

Managing Cybersecurity in the Process Industries

A Risk-based Approach



WILEY

Managing Cybersecurity in the Process Industries

This book is one in a series of process safety guidelines and concept books published by the Center for Chemical Process Safety (CCPS). Refer to www.wiley.com/go/ccps for full list of titles in this series.

It is sincerely hoped that the information presented in this document will lead to a better safety record for the entire industry; however, neither the American Institute of Chemical Engineers, its consultants, CCPS Technical Steering Committee and Subcommittee members, their employers, their employers' officers and directors, nor exida, and its employees and subcontractors warrant or represent, expressly or by implication, the correctness or accuracy of the content of the information presented in this document. As between (1) American Institute of Chemical Engineers, its consultants, CCPS Technical Steering Committee and Subcommittee members, their employers, their employers' officers and directors, and exida and its employees and subcontractors, and (2) the user of this document, the user accepts any legal liability or responsibility whatsoever for the consequence of its use or misuse.

Managing Cybersecurity in the Process Industries

A Risk-based Approach

CENTER FOR CHEMICAL PROCESS SAFETY
of the
AMERICAN INSTITUTE OF CHEMICAL ENGINEERS

120 Wall Street, 23rd Floor • New York, NY 10005



WILEY

This edition first published 2022
© 2022 the American Institute of Chemical Engineers

A Joint Publication of the American Institute of Chemical Engineers and John Wiley & Sons, Inc.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by law. Advice on how to obtain permission to reuse material from this title is available at <http://www.wiley.com/go/permissions>.

The rights of CCPS to be identified as the author of the editorial material in this work have been asserted in accordance with law.

Registered Office

John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA

Editorial Office

111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Limit of Liability/Disclaimer of Warranty

While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials or promotional statements for this work. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or service the organization, website, or product may provide or recommendations it may make. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Library of Congress Cataloging-in-Publication Data Applied for:

ISBN: 9781119861782

Cover Design: Wiley

Cover Images: © Alexander Supertramp/Shutterstock, Travel mania/Shutterstock

10 9 8 7 6 5 4 3 2 1

Table of Contents

Table of Contents v

List of Figures..... xi

List of Tables xiii

Acronyms and Abbreviations..... xvii

Glossary..... xxiii

Acknowledgments..... xxix

Preface..... xxxiii

Part 1: Introduction, Background, and History of Cybersecurity 1

1 Purpose of this Book 1

1.1 Target Audience..... 6

1.2 What is Cybersecurity?..... 6

1.3 What is Operational Technology (OT)?..... 10

1.4 Which industries have OT? 13

1.5 Scope..... 15

1.6 Organization of the Book 17

2 Types of Cyber-Attacks, Who Engages in Them and Why 19

2.1 Types of Cyber-Attacks 19

2.2 Who Commits Cybercrimes and Their Motives 26

2.3 Summary 30

3 Types of Risk Receptors / Targets 33

3.1 What is Cybersecurity Risk 35

3.2 What are Common Cybersecurity Targets? 38

3.3 Types of Cybersecurity Consequences 43

3.4 Summary 45

4 Threat Sources and Types of Attacks 47

4.1 Non-Targeted Attacks 49

4.2 Targeted Attacks 53

4.3	Advanced Persistent Threats (APT)	58
4.4	Summary	62
5	Who Could Create a Cyber Risk? Insider vs. Outsider Threats.....	65
5.1	Insider Cybersecurity Risk	65
5.2	Outsider Cybersecurity Risk	69
5.3	Summary	71
6	Case Histories	73
6.1	Maroochy Shire.....	73
6.2	Stuxnet.....	77
6.3	German Steel Mill	81
6.4	Ukrainian Power Grid.....	84
6.5	NotPetya	91
6.6	Triton.....	95
6.7	Düsseldorf Hospital Ransomware.....	99
6.8	SolarWinds	101
6.9	Florida Water System	105
6.10	Colonial Pipeline Ransomware	107
6.11	Summary	110
	Part 2: Integrating Cybersecurity Management into the Process Safety Framework.....	113
7	General Model for Understanding Cybersecurity Risk.....	113
7.1	Cybersecurity Lifecycle	113
7.2	Integrated Cybersecurity and Safety Lifecycle	121
7.3	NIST Cybersecurity Framework	129
7.4	Summary	138
8	Designing a Secure Industrial Automation and Control System..	141
8.1	The Disconnect between IT and OT Risk Management	141
8.2	Inherently Safer vs. Inherently More Secure.....	146

8.3	Defense-in-Depth	149
8.4	Network Segmentation	153
8.5	System Hardening	173
8.6	Security Monitoring	176
8.7	Risk Compatibility Assessment	180
8.8	Summary	182
9	Hazard Identification and Risk Analysis (HIRA)	183
9.1	Use of Process Safety Tools to Identify and Manage Cybersecurity Risk	185
9.2	Qualitative Methods	187
9.3	Quantitative Methods	217
9.4	How to Prioritize Risk Reduction Measures?	231
9.5	Revalidation/Reassessment	232
9.6	Summary	233
10	Manage the Risk	235
10.1	Management Approach	235
10.2	Initial Steps	236
10.3	Cybersecurity Culture	240
10.4	Compliance with Standards	242
10.5	Cybersecurity Competency	246
10.6	Workforce Involvement	248
10.7	Stakeholder Outreach	251
10.8	Process Knowledge Management	252
10.9	Operating Procedures	256
10.10	Safe Work Practices	259
10.11	Management of Change	262
10.12	Asset Integrity and Reliability	266
10.13	Contractor Management	272
10.14	Training and Performance Assurance	275

10.15	Operational Readiness	278
10.16	Conduct of Operations	281
10.17	Emergency Management	285
10.18	Incident Investigation.....	290
10.19	Measurements and Metrics	295
10.20	Auditing	300
10.21	Management Review and Continuous Improvement	304
10.22	Summary	307
11	Implementing a Holistic Approach to Safety and Cybersecurity	311
11.1	Cybersecurity Management Systems (CSMS)	312
11.2	Integrating CSMS with Process Safety Management	327
11.3	Summary	334
Part 3: Where Do We Go from Here?		337
12	What's Next? A Look at Future Development Opportunities	337
12.1	Cybersecurity Adoption Trends	338
12.2	Emerging Technologies.....	350
12.3	Summary	353
13	Available Resources.....	355
13.1	Local, Regional, and Global Topics	355
13.2	Cybersecurity Incident Repositories	362
13.3	Competency Requirements and Training Availability	363
13.4	Administration vs. Accountability Functions	368
13.5	Summary	370

Appendix A Excerpt from NIST Cybersecurity Framework 371

Appendix B Detailed Cybersecurity PHA and LOPA Example.....377

 B.1 System Basis 377

 B.2 Initial Risk Assessment.....382

 B.3 Detailed Risk Assessment (Cyber PHA/HAZOP) 387

 B.4 LOPA/ Semi-Quantitative SL Verification 405

Appendix C Example Cybersecurity Metrics.....411

Appendix D Cybersecurity Sample Audit Question List 413

Appendix E Management System Review Examples.....419

References 421

Index 437

List of Figures

Figure 1-1 Major Industrial Cybersecurity Events in the Last Decade	1
Figure 1-2 Cybersecurity Management System Pillars	5
Figure 1-3 OT Reference Model.....	12
Figure 4-1 Distributed Denial of Service Attack Diagram	56
Figure 4-2 Man-in-the-Middle Attack Diagram	58
Figure 6-1 Simplified Maroochy Shire SCADA System	74
Figure 6-2 Petrochemical Site Simplified Network Architecture	97
Figure 7-1 Assess Phase	115
Figure 7-2 Implement Phase.....	118
Figure 7-3 Maintain Phase	120
Figure 7-4 NIST Framework Aligned with Integrated Lifecycle	132
Figure 8-1 IT vs. OT Priorities.....	143
Figure 8-2 Hierarchy of Controls	147
Figure 8-3 Defense-in-Depth for Cybersecurity	151
Figure 8-4 Example Network Architecture with Extreme Connectivity ..	154
Figure 8-5 Example Network Architecture with Complete Separation...	156
Figure 8-6 Example Network Architecture with DMZ (Single Firewall) ...	159
Figure 8-7 Example Network Architecture with DMZ (Dual Firewall).....	160
Figure 8-8 Network Segmentation with Data Diodes	162
Figure 8-9 Combined Control and Safety Engineering Workstation	163
Figure 8-10 Separate Control and Safety Engineering Workstations	164
Figure 8-11 Separate Control and Safety Zones with Data Diode.....	165
Figure 8-12 Multi-Step Remote Access to IACS Systems	166
Figure 8-13 Ring Configuration for Unmanned Remote Operations.....	169
Figure 8-14 Extending Logical Networks to Remote Sites.....	170
Figure 9-1 Determining the Scope of Cybersecurity Assessments	184
Figure 9-2 Process Safety and Cybersecurity Analysis Considerations ..	187
Figure 9-3 Initial Risk Assessment Methodology.....	189
Figure 9-4 Detailed-Level Risk Assessment Methodology.....	195
Figure 9-5 Network Architecture for FMEA	209
Figure 9-6 Cybersecurity Vulnerability Methodology	213
Figure 9-7 Bow Tie Diagram.....	219
Figure 9-8 Example Cybersecurity Bow Tie Diagram.....	220
Figure 9-9 Swiss Cheese Model.....	222

Figure 9-10 Semi-Quantitative SL Verification Methodology	223
Figure 10-1 Example Job Cyber Assessment.....	273
Figure 11-1 Implementing Holistic Cybersecurity and Safety Approach.....	312
Figure 11-2 Continuous Improvement Process for CSMS.....	325
Figure 12-1 Zero-Trust Architecture	342
Figure 12-2 Simple Example of Software Bill of Materials	346
Figure 13-1 Drivers for Facility Risk Management	355
Figure B-1 Simplified Isomerization Process Flow Diagram	378
Figure B-2 Simplified Network Architecture	379
Figure B-3 Identification of System Under Consideration	382
Figure B-4 Device Selection.....	383
Figure B-5 Consequence Severity Ranking	384
Figure B-6 Likelihood Ranking	384
Figure B-7 Initial Risk Ranking	385
Figure B-8 Security Level Target	385
Figure B-9 Initial Risk Assessment Results.....	386
Figure B-10 Updated Zone and Conduit Diagram	387
Figure B-11 BPCS Zone for Detailed Risk Assessment	388
Figure B-12 Updated Risk Ranking.....	396
Figure B-13 Updated Security Level Target.....	396
Figure B-14 Likelihood with Countermeasures	401

List of Tables

Table 1-1 RBPS Accident and Cybersecurity Event Prevention Pillars.....3

Table 3-1 Considerations for Consequence Risk Table 44

Table 4-1 Attack Characteristics by Threat Source Type 49

Table 4-2 Cyber Kill Chain® Steps and Description.....61

Table 4-3 Attack Characteristics by Threat Source Type 63

Table 5-1 Sub-Groups of Insider Cyber activities 66

Table 6-1 Major Victims of NotPetya Attack 93

Table 7-1 IEC 62443 Security Levels (SL).....116

Table 7-2 Lifecycle Steps for Process Safety and Cybersecurity 124

Table 7-3 NIST Framework Functions and Categories.....131

Table 8-1 Differences Between IT and OT.....142

Table 8-2 Attack Surface.....148

Table 8-3 Common Cybersecurity Protections.....149

Table 8-4 Typical SIEM Features and Descriptions 179

Table 9-1 Process Safety and Cybersecurity Techniques.....185

Table 9-2 Example Severity Matrix.....191

Table 9-3 Example Likelihood Matrix 192

Table 9-4 Example Corporate Risk Matrix.....192

Table 9-5 Risk Ranking to Security Level Target.....193

Table 9-6 Initial Risk Assessment Worksheet 194

Table 9-7 Threat Definition Examples 198

Table 9-8 Threat Likelihood by Threat Source.....200

Table 9-9 Detailed Risk Assessment Worksheet 204

Table 9-10 Cybersecurity Checklist 206

Table 9-11 Example Cybersecurity FMEA for Safety PLC.....211

Table 9-12 Target Attractiveness Estimates.....224

Table 9-13 Cybersecurity Countermeasures and Estimated PFD 226

Table 9-14 Semi-Quantitative SL Verification Worksheet.....228

Table 9-15 HIRA RBPS Principles and Cybersecurity Considerations 234

Table 10-1 Cybersecurity Culture.....242

Table 10-2 Industry Codes, Standards, and Practices 243

Table 10-3 Compliance with Standards.....245

Table 10-4 Cybersecurity Competency.....248

Table 10-5 Workforce Involvement.....251

Table 10-6 Stakeholder Outreach	252
Table 10-7 Process Knowledge Management	256
Table 10-8 Operating Procedures	260
Table 10-9 Safe Work Practices	261
Table 10-10 Management of Change	265
Table 10-11 Asset Integrity and Reliability	270
Table 10-13 Contractor Management	275
Table 10-13 Training and Performance Assurance.....	278
Table 10-14 Operational Readiness.....	282
Table 10-15 Conduct of Operations.....	284
Table 10-16 Incident Response Plan Considerations	286
Table 10-17 Emergency Management.....	291
Table 10-18 Incident Investigation.....	294
Table 10-19 Leading Indicator Metrics	297
Table 10-21 Measurements and Metrics	300
Table 10-22 Auditing.....	303
Table 10-23 Cybersecurity Assessment Stages	306
Table 10-24 Management Review.....	307
Table 11-1 Example RACI Chart for Cybersecurity Lifecycle Activities.....	319
Table 11-2 Example IACS Cybersecurity Audit Checklist	323
Table 11-3 Example Cybersecurity Lifecycle Procedures/ Templates	329
Table 13-1 IACS Cybersecurity Practices, Standards, and Regulations...	358
Table 13-2 Cybersecurity Competency Requirements Example	366
Table 13-3 Certification or Certificate.....	367
Table A-1 Example NIST Framework Structure	372
Table B-1 Example Severity Matrix	380
Table B-2 Example Likelihood Matrix	381
Table B-3 Example Corporate Risk Matrix	381
Table B-4 Risk Ranking to Security Level Target.....	381
Table B-5 Threat Definition Examples	390
Table B-6 Threat Definition Examples and Likelihoods.....	391
Table B-7 Consequence Definition per Threat	393
Table B-8 Consequence and Severity Definition per Threat.....	394
Table B-9 Cybersecurity HAZOP Worksheet with Countermeasures	398

Table B-10 Countermeasure Effectiveness 400

Table B-11 Completed Cybersecurity HAZOP Worksheet.....402

Table B-12 Target Attractiveness Estimates 406

Table B-13 Cybersecurity Countermeasures and Estimated.....407

Table B-14 Semi-Quantitative SL Verification Worksheet 408

Table B-15 Severity Level and Tolerable Frequency 409

Table D-1 Cybersecurity Sample Audit Checklist 413

Acronyms and Abbreviations

5G	Fifth generation technology standard for cellular networks
AIChE	American Institute of Chemical Engineers
API	American Petroleum Institute
APT	Advanced Persistent Threat
AWIA	America's Water Infrastructure Act
BAS	Building Automation System
BMS	Burner Management System
BPCS	Basic Process Control System
CCPS	Center for Chemical Process Safety
CEMS	Continuous Emissions Monitoring Systems
CFATS	Chemical Facility Anti-Terrorism Standards
CFR	Code of Federal Regulations
C-IRP	Cybersecurity Incident Response Plan
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CMMS	Computerized Maintenance Management Systems
CMR	Countermeasure
CMS	Configuration Management Systems
COTS	Commercial off the Shelf
CRC	Cyclic Redundancy Check
CSA	Cybersecurity Assessment
CSMS	Cybersecurity Management System
CVA	Cybersecurity Vulnerability Assessment
CVSS	Common Vulnerability Scoring System

DCS	Distributed Control System
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
FAT	Factory Acceptance Test
FERC	Federal Energy Regulatory Committee
FMEA	Failure Modes and Effects Analysis
HAZOP	Hazard and Operability Study
HIPPS	High Integrity Pressure Protection System
HIRA	Hazard Identification and Risk Analysis
IACS	Industrial Automation and Control Systems
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IoA	Internet of Automation
IoT	Internet of Things
IP	Internet Protocol
IPL	Independent Protection Layer
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology

KPI	Key Performance Indicator
LAN	Local Area Network
LOPA	Layer of Protection Analysis
MAC	Media Access Control
MCC	Motor Control Center
MDR	Managed Detection and Response
MFA	Multi-factor Authentication
MITM	Man-in-the-Middle
MOC	Management of Change
MTSA	Maritime Security Act
NCSC	National Cyber Security Center
NERC	North American Electric Reliability Council
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
NVD	National Vulnerability Database
OS	Operating System
OSHA	Occupational Safety and Health Administration
OT	Operational Technology
PDF	Probability of Failure on Demand
PHA	Process Hazard Analysis
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PSCAI	Process Safety Controls Alarms and Interlocks

PS-ERP	Process Safety Emergency Management Plan
PSM	Process Safety Management
PSSR	Pre-startup Safety Review
QRA	Quantitative Risk Analysis
RaaS	Ransomware as a Service
RACI	Responsible, Accountable, Consulted, Informed
RAGAGEP	Recognized and Generally Accepted Good Engineering Practice
RAN	Radio Access Network
RBPS	CCPS Risk Based Process Safety
RDP	Remote Desktop Protocol
RIK	Replacement-In-Kind
RTU	Remote Terminal Units
SAT	Site Acceptance Test
SBOM	Software Bill of Materials
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Networking
SIEM	Security Information and Event Management
SIEMS	Security Information and Event Management System
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SL	Security Level
SOC	Security Operation Center
SOP	Standard Operating Procedure
SUC	System Under Consideration

SVA	Security Vulnerability Assessment
SWP	Safe Work Practices
UK HSE	United Kingdom Health and Safety Executive
VLAN	Virtual LAN (Local Area Network)
VPN	Virtual Private Network
WAN	Wide Area Network

Glossary

This Glossary contains Process Safety terms unique to this CCPS publication. The CCPS Process Safety terms in this publication are current at the time of issue. For other CCPS Process Safety terms and updates to these terms, please refer to the CCPS Process Safety Glossary [1].

Audit	A systematic, independent review to verify conformance with prescribed standards of care using a well-defined review process to ensure consistency and to allow the auditor to reach defensible conclusions.
Backdoor	Any connection (often covert) that allows authorized or unauthorized users to bypass existing security measures and establish a high level of access to a software application, computer system, or network.
Bow Tie Model	A risk diagram showing how various threats can lead to a loss of control of a hazard and allow this unsafe condition to develop into a number of undesired consequences. The diagram can also show all the barriers and degradation controls deployed.
Competency	A PSM program element associated with efforts to maintain, improve, and broaden knowledge and expertise.
Computer virus	A common type of malware that inserts itself into a legitimate program or application and modifies the program or application.
Conduit	Logical grouping of communication assets that protects the security of the channels it contains. (Connections between security zones.)

Continuous Improvement	Doing better as a result of regular, consistent efforts rather than episodic or step-wise changes, producing tangible positive improvements either in performance, efficiency, or both. Continuous improvement efforts usually involve a formal evaluation of the status of an activity or management system, along with a comparison to an achievement goal. These evaluation and comparison activities occur much more frequently than formal audits.
Cyber Kill Chain®	A model for identifying the steps that adversaries must complete to achieve their objective in a cybersecurity attack on an IACS [2].
Cybersecurity	Prevention of illegal or unwanted penetration of, or interference with, the intended operation of an industrial automation and control system using computer-based systems.
Cybersecurity Hygiene	Basic cybersecurity practices (that can be followed by any authorized user) to protect the health of computer systems.
Cybersecurity Management System	Program designed by an organization to maintain the cybersecurity of the industrial automation and control system considering requirements for personnel security, cybersecurity procedures, and necessary documentation.
Firewall	Inter-network connection device that restricts data communication traffic between two connected networks [3]

Hazard and Operability Study (HAZOP)	A systematic qualitative technique to identify process hazards and potential operating problems using a series of guide words to study process deviations. A HAZOP is used to question every part of a process to discover what deviations from the intention of the design can occur and what their causes and consequences may be. This is done systematically by applying suitable guidewords. This is a systematic detailed review technique, for both batch and continuous plants, which can be applied to new or existing processes to identify hazards.
Information Technology (IT)	Hardware and software used to store, retrieve, transmit, or manipulate data or information in systems connected to the internet.
Layer of Protection Analysis (LOPA)	An approach that analyzes one incident scenario (cause-consequence pair) at a time, using predefined values for the initiating event frequency, independent protection layer failure probabilities, and consequence severity, in order to compare a scenario risk estimate to risk criteria for determining where additional risk reduction or more detailed analysis is needed. Scenarios are identified elsewhere, typically using a scenario-based hazard evaluation procedure such as a HAZOP Study.
Malware	Malicious software, designed to interfere with the expected functionality of a computer, system, or network.
Operational Technology (OT)	Hardware and software that detects or causes a change through the direct monitoring and/or control of industrial equipment.

Phishing	A fraudulent attempt to obtain sensitive information such as usernames and passwords by impersonating a trustworthy entity, often conducted via email.
Process Safety Controls Alarms and Interlocks (PSCAI)	Safeguards implemented with instrumentation and controls, used to achieve or maintain a safe state for a process, and required to provide risk reduction with respect to a specific hazardous event [4]
Replacement-In-Kind (RIK)	An item (equipment, chemical, procedure, etc.) that meets the design specification of the item it is replacing. This can be an identical replacement or any other alternative specifically provided for in the design specification, as long as the alternative does not in any way adversely affect the use of the item or associated items.
Risk Profile	Characterization of the nature and levels of threats faced by an organization considering the likelihood and impact of a security incident. A risk profile supports determination of control measures based on the effectiveness for different types of risks.
Risk Receptor	The entity experiencing harm such as a company, an individual, or the public.
Script Kiddie	Unskilled hacker who lacks the ability to write sophisticated programs on their own but can use readily available hacking tools to execute attacks.
Social Engineering	Methods used in cybersecurity attacks to obtain confidential data by tricking individuals into revealing secure information. (Phishing is a sub-type of social engineering.)

Spoofing	The process of disguising an unknown, often malicious source as a trusted and known source.
Watering Hole	A strategy used in cybersecurity attacks, where a website is compromised and used to infect those who visit the website with malware.
Zero-Day Vulnerability	Weakness or vulnerability in computer-software that is unknown to the system supplier and security professionals.
Zone	Grouping of logical and/or physical assets that share common security requirements.
Zone & Conduit	Architecture diagram for a network or system that identifies the security zones and conduits based on network segmentation devices.

Acknowledgments

The American Institute of Chemical Engineers (AIChE) and the Center for Chemical Process Safety (CCPS) express their appreciation and gratitude to all members of the *Managing Cybersecurity in the Process Industries, A Risk-based Approach* Subcommittee for their generous efforts in the development and preparation of this important guideline. CCPS also wishes to thank the subcommittee members' respective companies for supporting their involvement during the different phases in this project.

Subcommittee Members:

Seshu Dharmavaram, Chair	Air Products and Chemicals, Inc.
Hafiz Zeeshan Ahmed	Tronox – Australia
Blake Benson	ABS Group
John Biasi	1898 & Co.
Denise Chastain-Knight	exida
John Cusimano	Deloitte & Touche LLP
Chris DaCosta	Air Products
Felix Azenwi Fru	National Grid
Anil Gokhale	CCPS
Azmi B Hashim	Petronas
Kathy Kas	Dow
Walid Khayate	AON – Canada
Rafael Martinez	FMC – Barcelona
Dave Moore	AcuTech
Divyang Shah	Reliance Industries Limited
David Thaman	PPG – retired
Lu Yi	IRC
Jeff Young	Syngenta
Rich Santo	AcuTech
Jim Petrusich	Go-Arc Israel

The book committee wishes to express their appreciation to Patrick O'Brien, exida, Denise Chastain-Knight, exida, Shawn Statham, exida, Steve Gandy, exida, Mike Medoff, exida, and Iwan van Beurden, exida, for their contributions in preparing the guideline's draft manuscript.

Before publication, all CCPS books are subjected to a peer review process. CCPS gratefully acknowledges the thoughtful comments and suggestions of the peer reviewers. Their work enhanced the accuracy and clarity of this guideline.

Although the peer reviewers provided comments and suggestions, they were not asked to endorse this guideline and did not review the final manuscript before its release.

Peer Reviewers:

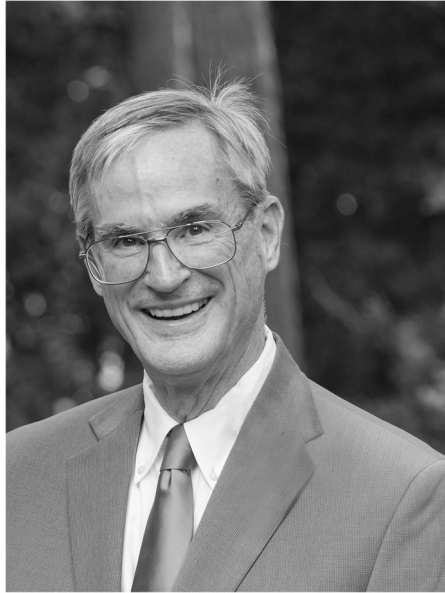
Spencer Casey Bitz, CISSP	OneNeck IT Solutions
Randy Woods	Dow
Craig Fisher	BP (UK)
Sharul A Rashid	Petronas

Managing Cybersecurity in the Process Industries

A Risk-Based Approach

is dedicated to

Dennis Hendershot



Dennis Hendershot has been a mentor for several generations of process safety professionals, through his long-time involvement in the Loss Prevention Symposium, to the founding of CCPS in 1985, to his expertise in Inherently Safer Technologies (IST) and even in “retirement”. It was no coincidence that former Secretary of State James Baker selected Dennis to serve on his panel to investigate the BP Texas City incident.

Always willing to help wherever needed, Dennis’ calm demeanor and obvious expertise, combined with a unique way of communicating even the most complex topics clearly and understandably have made him an icon in process safety circles.

From 2005 until 2019 he served as the staff consultant and editor for the Process Safety Beacon, generating a new monthly publication like clockwork.

Dennis always had a wealth of ideas that need attention and always had more than sufficient material to make the Beacon a 'must read' for thousands and thousands of readers across the globe. He continues to follow his passion for the Beacon by anchoring the development of the Book of Beacons.

Dennis is an AIChE Fellow and CCPS emeritus. CCPS is proud to dedicate this newest work to Dennis, as a small token of recognition for all he has given and continues to give to the process safety community.

Anil Gokhale & Pete Lodal

Preface

As this text was being finalized, the United States was again responding to a ransomware attack, this time against Colonial Pipeline. Although the disruptions to the public were minimal, and a significant portion of the ransom recovered by the FBI, it again pointed out the increasing threat of cyber-attacks against critical infrastructure, businesses, and governmental agencies. Like all near-miss events, the Colonial Pipeline incident is yet another “free” wake-up call pointing out the need for ever stronger and more robust cyber protections.

This book is intended to provide a framework for such protection in the process and related industries. One of the key concepts emphasized here is the relationship of, and differences between Information Technology (IT) and Operational Technology (OT). The gap between the two has been widely debated for the last 10 years but the fundamental issues remain, primarily due to lack of skill overlap. While both areas share similar protection goals against cyber-attacks, the risk-based assessment outlined in this text highlights significant differences, and how some approaches to IT security are simply not sufficient in the OT space.

Multiple audiences should find this book useful. For those who are looking for an overall framework, or who have managerial responsibilities in the cybersecurity world, the risk-based approach articulated here provides a management structure for evaluating, detecting, preventing, and responding to OT cyber-related attacks. For those who simply want to increase their knowledge of the topic, Chapters 1 and 6 (overview and case histories) provide a succinct overview of the subject, with real-world examples of what could happen if sufficient measures are not in place. And, for the practitioner, who will have to design, implement, test, and improve OT cybersecurity systems, this text provides methods and references to identify, evaluate, and implement effective solutions.

Cybersecurity did not exist 40 years ago. Its evolution has paralleled the increasing use of logic devices to improve process control, and overall process safety. As DCS vendors abandoned proprietary platforms in favor of commonly available ones, it served a commercial competitive goal. Like many other technologies, this migration to more computer and computer-like

controls has improved process safety immensely, while creating an unintended by-product, namely the ability to do harm in a chemical process at a distance. This is an evolving topic, but the authors and the CCPS committee who have created this text believe that this book sets a workable, risk-based approach for addressing the issue of cybersecurity in the process industries.

The American Institute of Chemical Engineers (AIChE) has helped chemical plants, petrochemical plants, and refineries address the issues of process safety and loss control since 1967. Through its ties with process designers, plant constructors, facility operators, safety professionals, and academia, the AIChE has enhanced communication and fostered improvement in the high safety standards of the industry. AIChE's publications and symposia have become an information resource for the chemical engineering profession on the causes of incidents and the means of prevention.

The Center for Chemical Process Safety (CCPS), a directorate of AIChE, was established in 1985 to develop and disseminate technical information for use in the prevention of major chemical accidents. CCPS is supported by a diverse group of industrial sponsors in the chemical process industry and related industries who provide the necessary funding and professional guidance for its projects. The CCPS Technical Steering Committee and the technical subcommittees oversee individual projects selected by the CCPS. Professional representatives from sponsoring companies staff the subcommittees and a member of the CCPS staff coordinates their activities.

A successful process safety program relies upon committed managers at all levels of a company, who view process safety as an integral part of overall business management and act accordingly.

September 2021

Peter N. Lodal

D&H Process Safety

Kingsport, TN

Part 1: Introduction, Background, and History of Cybersecurity

1 Purpose of this Book

Cybersecurity has quickly become an essential component in maintaining the safe and continued operations of industrial facilities. A survey of industrial control system operators in 2019 showed that 59% had experienced a cybersecurity incident in the past year [5]. The increase of cybersecurity incidents is not a phenomenon limited to a few specific companies or only the largest corporations. Over the last ten years, numerous attacks on automation systems such as those listed in Figure 1-1 continue to demonstrate that industrial facilities of all types and sizes are vulnerable to cybersecurity attack, and that these cyber-attacks can have significant financial, environmental, and process safety related consequences [6].

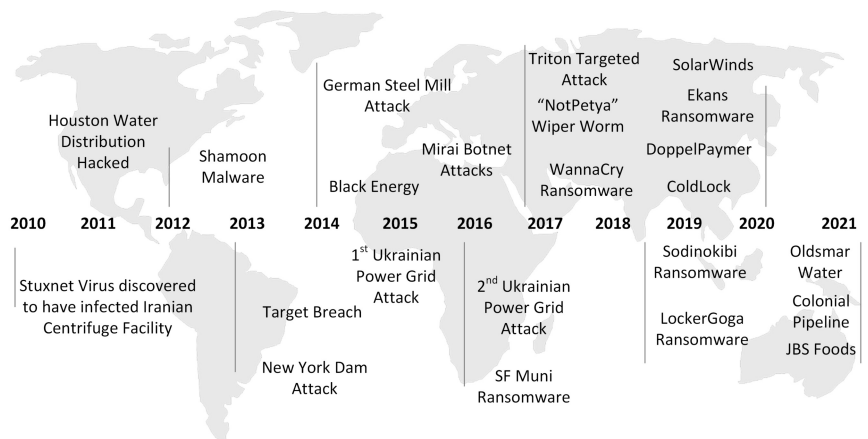


Figure 1-1 Major Industrial Cybersecurity Events in the Last Decade

Over the past 20 years, the conversation has moved from “Who could possibly target control systems for a cybersecurity attack?” to a continuing discussion of the many recent breaches and attacks. What has led to this drastic increase in cybersecurity attacks on industrial control systems? The following list provides several factors that could account for this increase:

- Increased interconnectivity of industrial control systems
- Increased convergence of OT and IT systems

- Increased use of Internet Protocol in OT applications
- Increased requirements for remote access
- Increased number of readily available hacking tools
- Desire to target critical infrastructure for political motives
- Increase in number of threat agents with skills to target control systems
- Better identification of cybersecurity attacks
- Increase in known software vulnerabilities
- Increase in known vulnerabilities in legacy systems
- Lack of sufficient cybersecurity awareness and training
- Potential for significant financial gain
- Desire to gain recognition of skills by targeting control systems

While no single cause drives the increase in cybersecurity attacks, it is likely that many of the factors in this list are contributing to the continually evolving cybersecurity landscape.

The purpose of this book is to introduce a risk-based approach for Managing Cybersecurity in the Process Industries and to help organizations design and implement more effective cybersecurity management system programs that are aligned with existing process safety management systems. This approach includes methods for:

1. Understanding cybersecurity risk for the process industry,
2. Integrating cybersecurity management into the existing process safety framework, and
3. Developing a path forward for the future of cybersecurity for the process industry.

The risk-based approach helps to provide an optimum comparison between cybersecurity risk and process risk so that informed decisions can be made. Not all hazards and risks are equal, and it is important to focus time and resources on the higher risks. Cybersecurity risk for the process industry can vary greatly, from potential business impact arising from denial of service or ransomware to the devastating real-world impact of a targeted attack that compromises process control and safety systems. The potential of cybersecurity attacks on the process industry to result in safety consequences

represents a fundamental shift in approach from traditional IT cybersecurity concerns. Adopting this approach for cybersecurity will help all industries that manufacture, use, or handle hazardous chemicals or energy to:

- Develop their approach to cybersecurity incident prevention.
- Continuously improve their management system effectiveness.
- Employ cybersecurity management for non-regulatory processes using risk-based design principles.
- Integrate the cybersecurity business case into an organization’s business processes.
- Focus their resources on higher risk activities.

This approach for cybersecurity management builds on the Guidelines for Risk Based Process Safety (RBPS) [7] and the RBPS Management System Accident Prevention Pillars:

Table 1-1 RBPS Accident and Cybersecurity Event Prevention Pillars

RBPS Accident Prevention Pillars	Cybersecurity Event Prevention Pillars
Commit to process safety	Commit to cybersecurity
Understand hazards and risk	Understand cybersecurity hazards and risk
Manage risk	Manage cybersecurity risk
Learn from experience	Learn from experience

These pillars remain central for preventing cybersecurity incidents. Leveraging existing risk assessment and management techniques to address cybersecurity reduces the time required to deploy a robust cybersecurity program and improves the alignment between process safety risk management and cybersecurity risk management. The following considerations for cybersecurity outline key steps for addressing cybersecurity risk through the RBPS pillars.

Top management ***commitment to cybersecurity*** is a pre-requisite to successful implementation. Without strong leadership and clear organizational commitment to improving cybersecurity, it is very difficult to make improvements. In addition to driving cybersecurity initiatives, management support is also helpful for establishing a robust cybersecurity culture. Cybersecurity culture is based on awareness (understanding of the cybersecurity impacts of employee actions) and hygiene (understanding of basic security best practices); with these two components in place, conscientious cybersecurity behavior can be promoted. After cybersecurity culture has been established, ongoing management support is critical for sustaining focus on cybersecurity excellence.

Organizations that ***understand cybersecurity hazards and risk*** are better able to allocate limited resources in the most effective way. Due to the many misconceptions about cybersecurity for the process industry, developing an accurate understanding of the potential risks is particularly important. This is a necessary step for incorporating cybersecurity risk into the business plan to lower the overall risk level of the organization and maintain safe and continuous operations.

Managing cybersecurity risk consists of multiple phases including the identification and analysis of cybersecurity risk, designing of cybersecurity protections, implementation of cybersecurity detection systems and procedures for responding to cybersecurity incidents, and recovering from cybersecurity incidents. Strategies such as implementing a cybersecurity lifecycle can help organizations to reduce unexpected downtime and decrease the potential for adverse cybersecurity impacts.

Learning from experience requires monitoring and acting on internal and external challenges. Common internal challenges include previous cybersecurity incidents and near misses, while external challenges include events at similar facilities, industries, technologies, and increased threat activity. Despite an organization's best efforts in implementing cybersecurity management, with the continually evolving threat landscape, cybersecurity attacks are more a question of "when" than "if." Responding effectively to these situations and improving defenses in the future are critical aspects of

cybersecurity management. An effective approach for learning from real world experience is to:

- 1. Apply industry best practices
- 2. Correct deficiencies identified from internal incidents
- 3. Apply lessons learned from other organizations

Monitoring Key Performance Indicators (KPIs) for cybersecurity throughout the life of the facility can provide useful information about how an organization's cybersecurity approach changes over time. In addition to tracking KPIs, periodic audits/ assessments of the current level of cybersecurity drive continuous improvement and sustained results.

The pillars of the risk-based approach for cybersecurity are shown in Figure 1-2:

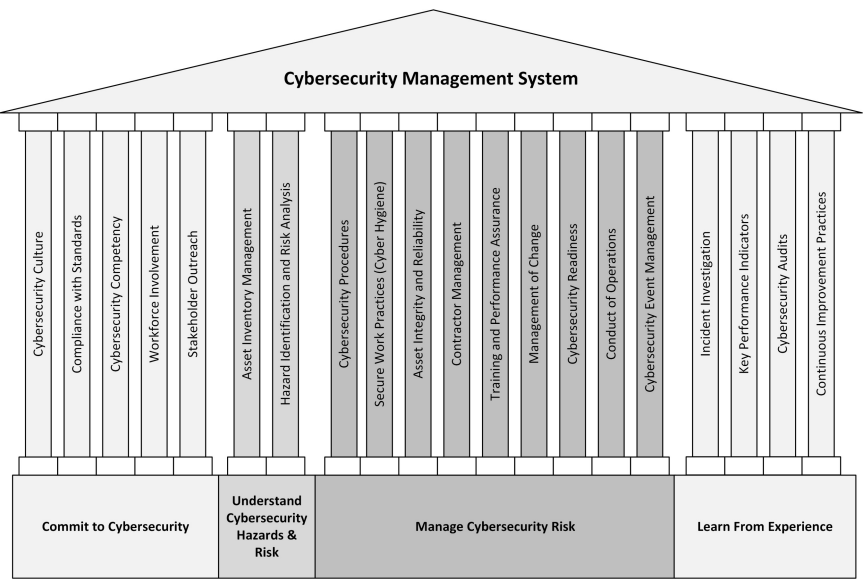


Figure 1-2 Cybersecurity Management System Pillars

Adapted from [7]

Focusing on the pillars of the risk-based approach for cybersecurity should enable an organization to improve its cybersecurity effectiveness, reduce the frequency and severity of cybersecurity incidents, and improve its long-term safety, environmental, and business performance. If the process control system is not secure, it cannot be operated safely. The risk-based approach helps avoid gaps and inconsistencies in the security approach to prevent common cause failures of the control and safety systems.

1.1 Target Audience

This risk-based approach for Managing Cybersecurity in the Process Industries is written for practitioners of the process safety lifecycle including process safety practitioners, process control engineers, instrumentation engineers, maintenance engineers, and process engineers, and others. For simplicity, these roles are referred to as process safety professionals throughout the remainder of this book. Additionally, this book is written for key stakeholders whose decisions can impact the implementation of the process safety lifecycle. The goal of this book is to improve awareness and resilience against cybersecurity attacks by leveraging existing techniques for process safety management. Although process safety professionals have a detailed understanding of process risk and operational technology for maintaining operations, they generally have limited experience with cybersecurity considerations. As such, before diving into the specifics of integrating cybersecurity and process safety management it is necessary to outline the fundamental aspects of cybersecurity.

1.2 What is Cybersecurity?

The IEC 62443-1-1 standard [3] defines security as:

1. Measures taken to protect a system.
2. Condition of a system that results from the establishment and maintenance of measures to protect the system.
3. Condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss.

4. Capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet ensure that this is not denied to authorized persons and systems.
5. Prevention of illegal or unwanted penetration of, or interference with, the proper and intended operation of an industrial automation and control system.

Essentially, security refers to the ability to protect something from various threats, and cybersecurity is focused on protection from unauthorized access for computer-based systems. Although cybersecurity is a relatively new concept, security in the broader sense has been relevant for as long as there have been things worth protecting.

One common analogy for security is that of the medieval castle. These strongholds of defense were designed with security at their core. The moat, walls, and towers were the measures taken to protect something of value from various threats, such as bandits or attacking armies. This example introduces a key concept for designing with security in mind: defense-in-depth. Defense-in-depth is the principle of maintaining independence across security measures, so that if one layer of defense is compromised, the others remain intact.

Moreover, for a moat to be effective, a drawbridge must grant access to authorized visitors. For security to be maintained, it is important that a gate is also included. This ensures that even if the drawbridge is compromised and cannot be raised, rendering the moat ineffective, the security measures of the wall and gate remain uncompromised.

It is important to note that the defenses of castles only worked until technology advancements such as gun powder and modern weaponry enabled the walls to be breached easily. Similarly, cybersecurity defenses must be maintained and kept technically current; otherwise, they become obsolete and ineffective against attackers.

The three main types of security are physical, personnel, and cyber. These three types of security are closely related and must be implemented together to develop a robust, integrated security policy. It is insufficient to evaluate only one area of security. To truly secure a facility from cyber risk, personnel and physical security must be evaluated in combination with cybersecurity.

1.2.1 What do Process Safety Professionals know about Cybersecurity?

Often when people (including process safety professionals) hear the term cybersecurity, they picture a hooded figure in a dark room “hacking” personal information on an IT network. These “stereotypical” attacks may consist of stealing a user’s password using phishing emails (emails designed to trick users into giving personal information and passwords to an attacker) with fake links or attachments that result in downloading/executing malware when clicked. These attacks could lead to identity theft or compromised financial information. Although these are types of cybersecurity attacks that happen on a regular basis, they do not provide the full cybersecurity picture for the process industry. Modern cyber-attacks can go far beyond stealing personal data and have the potential to inflict significant harm on personnel, equipment, and the environment.

A 2014 cybersecurity attack on a German steel mill highlights just how dangerous attacks on control systems can be. Attackers gained access to the corporate network through a phishing campaign intended to compromise operator accounts. They were then able to access the control network and caused multiple process controls to fail. As a result, a furnace at the steel mill was prevented from shutting down, which resulted in significant equipment damage. Fortunately, the site was able to identify the hazardous scenario and evacuate nearby personnel; however, similar incidents of industrial furnaces have resulted in loss of life [8].

1.2.2 What should Process Safety Professionals know about Cybersecurity?

The attack on the German steel mill introduces one of the fundamental differences between Information Technology (IT) and Operational Technology (OT) cybersecurity: attacks on OT can have **physical impacts**. These differing consequences are a primary driver for the conflicting IT and OT cybersecurity priorities.

For IT security, performance and confidentiality are paramount and outages, while undesirable, are acceptable. This is not true for the process industry, where the need for availability and integrity of the control and safety systems outweighs all other considerations. The priorities are not the only difference between OT and IT cybersecurity, and additional information on these differences is provided in Chapter 8.

Understanding the impact of OT cybersecurity attacks on the process control system is essential for process safety professionals. Particularly striking about the cybersecurity impact on process safety is the possibility for a cybersecurity attack to result in the common cause failure of multiple systems. Industry examples such as the German Steel Mill attack [8], Stuxnet [9], and the Saudi petrochemical facility attack [10] have shown that attackers target both the control and safety/protective functions to achieve the maximum consequence. (Additional information on these and other cybersecurity case studies are included in Chapter 6.) The potential for cybersecurity attacks to trigger the initiating event of a hazard and bypass multiple protection layers can lead to significant unmitigated risk if sufficient security protections are not in place.

Cybersecurity poses new challenges, but by leveraging existing risk assessment and risk management models with new insights, cybersecurity risk can be effectively evaluated. To support this approach, several tools and techniques have been developed for process safety professionals. The following list includes available industry best practice references and regulatory requirements:

- Guidelines for Risk Based Process Safety [7]
- NIST Cybersecurity Framework [11]
- IEC 62443 [12]
- ISA TR84.00.09 [13]
- Chemical Facility Anti-Terrorism Standards: Critical Infrastructure, United States [14]
- NERC CIP: Power, United States [15]
- AWIA: Water and Wastewater, United States [16]

Further discussion of the NIST cybersecurity framework and the IEC 62443 standard is provided in Chapter 7 as a baseline approach for adopting cybersecurity.

In the United States, OSHA's Process Safety Management (PSM) regulation, 29 CFR 1910.119 [17], is often viewed as synonymous with process safety. For many companies in the process industry, application of the IEC 61511 standard is used to demonstrate that OSHA safety requirements related to Safety Instrumented Systems are met. The updated IEC 61511 standard [18] released in 2016 does include new cybersecurity requirements. Any company claiming compliance with the IEC 61511 standard is now expected to complete mandatory cybersecurity activities, including a cybersecurity risk assessment for the Safety Instrumented System (SIS) and all connected networks. Many organizations conduct IT risk assessments of the corporate network, but these studies do not often focus on OT assets such as safety or control systems. As a result, a separate OT focused risk assessment is typically needed to comply with the IEC 61511 requirements.

The growing inclusion of cybersecurity requirements in regulations and international standards serves to underline the fundamental importance of cybersecurity for process safety engineers. Cybersecurity incidents have become a credible threat to controls, alarms, and SIS. Cybersecurity needs to be assessed since attacks can lead to common cause failure for all safety functions (SIFs) in an SIS. Without sufficient cybersecurity protection, traditional protection layers such as Basic Process Control System (BPCS) interlocks, SIS interlocks, and alarms cannot be relied on to raise operator awareness of an unsafe condition or automatically bring the process to the safe state. Simply put - without security, there is no safety.

1.3 *What is Operational Technology (OT)?*

OT cybersecurity is focused on the protection of operational technology, such as automation systems, industrial control systems, process control networks, and supervisory control and data acquisition systems, from compromise. This book includes information on OT cybersecurity as it relates to the process industry.

Operational Technology (OT) is any hardware or software that detects or causes a change directly to industrial equipment, assets, processes, and

events. Essentially, OT systems are capable of monitoring, controlling, and/or performing safeguarding of physical equipment. Common types of OT equipment/systems include:

- Basic Process Control System (BPCS)
- Safety Instrumented System (SIS)
- Programmable Logic Controllers (PLCs)
- Distributed Control System (DCS)
- Supervisory Control and Data Acquisition (SCADA)
- Fire and Gas Detection Systems
- Allocation and Custody Metering System
- Motor Control Centers (MCCs)
- Burner Management Systems (BMS)
- Building Management/ Automation Systems (BAS)
- Alarm Management System
- Continuous Emissions Monitoring Systems (CEMS)
- Machine Monitoring Systems (MMS)
- Pipeline Leak Detection Systems (PLDS)
- Terminal Automation System

Often, many of these different types of OT components are used in the same OT network to control a variety of different process equipment. Building a reference model, such as the one in Figure 1-3, is often helpful to show the interaction of OT equipment and more clearly illustrate the OT interface with the traditional IT network.

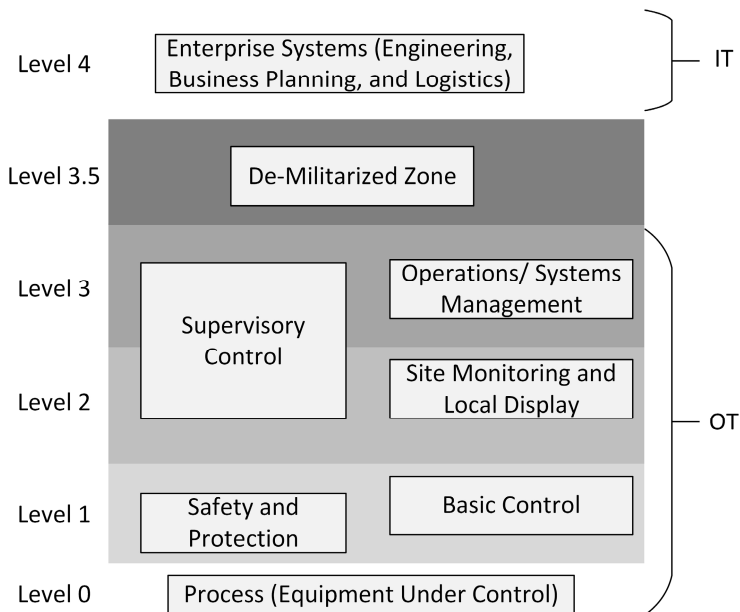


Figure 1-3 OT Reference Model

Source: IEC 62443-1-1 [3]

The traditional OT system is made up of levels 0 through 3:

- Levels 0 (process) contains the physical equipment being controlled or monitored by the OT network (e.g., actuated valve, pressure transmitter).
- Level 1 (basic control) contains the components that interface directly with process equipment, including the programmable logic controllers responsible for basic control (e.g., BPCS, DCS) and for safety and protection (e.g., SIS, BMS, safety PLC).
- Level 2 (area control) contains the site monitoring and local display (e.g., CEMS, operator workstations) that provide additional information about the components in level 1 and 0. Elements of supervisory control (e.g., SCADA) are also considered in this level.
- Level 3 (site operations) contains operations/ systems management that are not directly interfacing with equipment from level 1 (e.g., building management). In some applications, elements of supervisory control are also a part of level 3.

The assets in levels 1-3 have the potential to cause changes at level 0 and affect the physical process; as such, they need to be considered when addressing cybersecurity. When smart devices such as smart transmitters or valve positioners are used in level 0, they need to also be considered in the cybersecurity risk assessment.

Level 4 is composed of the enterprise systems that traditionally make up an internet connected IT network (or corporate wide area network (WAN)/ local area network (LAN)). It is important to protect these systems to achieve overall security; however, these enterprise systems are outside the scope of this guideline.

Level 3.5 (the demilitarized zone or DMZ) is often implemented in networks as a buffer between the IT network and the OT network to prevent direct traffic between the two systems. Often, the ownership of the DMZ is shared between IT and OT teams, and it is an important aspect in securing the perimeter security of the OT network. This is another area where coordination and a close working relationship between IT and OT team members is needed to achieve the organizations cybersecurity goals. More information on the use of a DMZ to improve network segmentation is provided in Chapter 8.

Another term that has become increasingly popular in industry, is Industrial Automation and Control Systems (IACS) . IACS is another name for OT and is defined in the IEC 62443 standard as “a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process” [3]. It is important to remember that securing the IACS goes beyond just the physical equipment and is dependent on the people and software/ applications as well. All of these areas have to be considered when implementing security protections for the IACS.

1.4 Which industries have OT?

Operational Technology is used in many industries such as chemicals, oil and gas, utilities, and manufacturing. Essentially, any industry where computer systems interact with physical systems uses OT. In some cases, OT is used for control; however, OT can also include monitoring systems for industries that are not typically associated with OT such as building automation systems (BAS), heating, ventilation, and air conditioning (HVAC), fire and gas, and even

transportation systems. Sections 1.4.1, 1.4.2, and 1.4.3 discuss the common OT systems used in various industry groups.

1.4.1 Chemical Processing

Many chemical processing facilities, including petrochemicals, pharmaceuticals, refineries, specialty chemicals, bulk chemicals, and even food and beverage, use OT for critical control and safety applications. In many cases, the control is handled in a connected BPCS or DCS system that may or may not be segmented from a separate safety system or SIS. Numerous real-world incidents have highlighted the potential for consequences resulting from the compromise of chemical processing facilities such as the Saudi Arabia Petrochemical attack [9]. (Additional information on this case study is included in Chapter 6.)

1.4.2 Utilities

Utilities also use OT for a variety of applications, including control and monitoring. While some utilities such as power generation (nuclear, coal, gas, etc.) may have network configurations similar to traditional chemical processing sites, many utility providers such as water supply or natural gas/oil pipelines have much more distributed networks. These networks are often referred to as Supervisory Control and Data Acquisition systems (SCADA). SCADA systems often make attractive targets because of their places in critical infrastructure and the need for everyday activities. SCADA systems need rigorous cybersecurity protection as well and have already been targeted for numerous attacks such as the Maroochy Shire Wastewater incident [19], Ukrainian Power Grid attacks [20] [21], and Oldsmar Water System Attack [22]. (Additional information on these and other cybersecurity case studies are included in Chapter 6.)

1.4.3 Discrete Manufacturing

Manufacturing systems including vehicle production and line manufacturing also rely on OT for essential functions. In many cases, machinery and robotics applications may rely more heavily on segmented OT networks, with PLCs used for control of individual lines or sections of lines. However, even in these segmented networks, growing reliance on digital systems has led to a movement of greater interconnectivity to improve monitoring and advanced control of manufacturing processes.

1.5 Scope

To better focus this information on the most important aspects for process safety professionals, it is important to formally define what is included and what is excluded from this risk-based approach.

1.5.1 Cybersecurity

Cybersecurity is the aspect of security relating to the prevention, detection, and mitigation of accidental or malicious acts on or involving computers and networks. Cybersecurity has multiple focus areas such as IT and OT cybersecurity.

IT cybersecurity is related to the protection of enterprise or business networks that are designed to be connected to the internet. This is the area many people traditionally think of when hearing cybersecurity. The field of IT has been wrestling with cybersecurity for longer than the field of OT, in large part because of the greater interconnectivity of IT systems.

The predominant standard adopted for IT cybersecurity is ISO/IEC 27002:2013, *Information technology - Security Techniques - Code of practice for information security controls* [23], which is a comprehensive catalog of general IT security practices for cybersecurity risk management. IT cybersecurity is primarily concerned with the protection of confidentiality and integrity of internet facing computer systems and often has very different priorities than OT cybersecurity. As such, IT cybersecurity is largely outside the focus of this book.

OT cybersecurity as introduced in Section 1.3 is focused on preventing the compromise of operational technology, such as automation systems, industrial control systems, and process control networks. This book will include information on OT cybersecurity as it relates to the process industry.

1.5.2 Physical and Personnel Security

Three main types/ categories of security are necessary for full protection of assets. These are physical, personnel, and cyber. To truly secure a plant from cyber risk, personnel and physical security must be evaluated in combination with cybersecurity.

Physical security refers to protections against unauthorized in-person access to the physical process and the process control system. Although often

overlooked, numerous industry events have shown that poor physical security can increase the likelihood of both internal intentional attacks (e.g., disgruntled employee) and unintentional incidents (e.g., mistake, accessing incorrect part of system). Physical security is largely outside the scope of this guideline, but it is important for process sites to implement the three key aspects of physical security:

- Access control (e.g., fences, locked gates, access control cards)
- Surveillance (e.g., security cameras, security guards, 24/7 occupancy of control room)
- Policies and procedures (e.g., guidelines for physical security, audits of locked buildings/rooms)

Additional information on physical security can be found in the IEC 62443-2-1 standard [12] as well as in sector specific standards (e.g., CFATS [14], API 1164 Pipeline SCADA Security [24]).

Personnel security refers to the thoroughness of screening and training plant personnel (e.g., operators, engineers, supervisors) before providing access to critical systems. Personnel security requirements are driven by concerns that an employee may abuse their trust and deliberately cause harm to the company or that an employee may unwittingly cause an accident (e.g., inattention, unqualification, substance abuse). People are often the weak link when designing cybersecurity protections and need to be considered in an effective cybersecurity strategy. Requirements for personnel security often include identity verification, background checks prior to employment or on-site access, terms of use agreements for access to the IT and IACS networks, roles and responsibilities, and awareness training.

Even with trusted personnel, cybersecurity hygiene can still be a major factor in achieving cybersecurity goals. Phishing continues to be a major source of cybersecurity incidents, and the accidental downloading unwanted software when accessing file sharing sites (e.g., equipment information, music, movies) is unfortunately common.

Further discussion of personnel security is outside the scope of this guideline, but information can be found in the best practice and industry standard documents from the lists in Section 1.2.2.

1.6 *Organization of the Book*

This book will provide information in three main parts:

- Part 1: Introduction, Background, and History of Cybersecurity
 - o Purpose of this Book (this chapter)
 - o Types of Cyber Activities, Who Engages in Them, and Why (Chapter 2)
 - o Types of Risk Receptors/ Targets (Chapter 3)
 - o Threat Sources & Types of Attacks (Chapter 4)
 - o Who Could Create a Cyber Risk? Insider vs. Outsider Threats (Chapter 5)
 - o Cybersecurity Case Histories (Chapter 6)
- Part 2: Integrating Cybersecurity Management into the Process Safety Framework
 - o General Model for Understanding Cybersecurity Risk (Chapter 7)
 - o Designing a Secure Industrial Automation and Control System (Chapter 8)
 - o Hazard Identification and Risk Analysis (Chapter 9)
 - o Manage the Risk (Chapter 10)
 - o Implementing a Holistic Approach to Safety and Cybersecurity (Chapter 11)
- Part 3: Where Do We Go from Here?
 - o A Look at Future Development Opportunities (Chapter 12)
 - o Available Resources (Chapter 13)

Part 1 introduces process safety professionals to the many different types of cybersecurity events, threats, and attacks that have the potential to negatively impact the process control system. These serve as the foundation for Part 2, which introduces strategies for integrating cybersecurity management into existing process safety activities to better understand, identify, and manage cybersecurity risk by tailoring existing process safety assessment methodologies to address cybersecurity concerns. Finally, Part 3 covers future development opportunities and supporting resources so that companies in the process industry can become better prepared to adjust to and defend against the continually changing cybersecurity landscape.

2 Types of Cyber-Attacks, Who Engages in Them and Why

Organizations face a growing threat as IT and OT environments converge to form truly digital environments. Recognizing the severity of the cybersecurity threat is an important step to drive implementation of countermeasures and risk mitigation strategies necessary to protect Industrial Automation Control Systems (IACS) - the people, hardware, and software that make up OT systems.

As the threats to IACS systems increase, the risk of a serious event rises as well. If a cyber-attack can successfully penetrate these critical systems, hackers may be able to cause a physical event that compromises safety to personnel and surrounding communities.

This chapter will cover various kinds of cyber-attacks on a deeper level, the perpetrators who commit them, and their motives. This will form the foundation for categorizing cybersecurity incidents as part of the risk assessment process.

2.1 Types of Cyber-Attacks

One of the first steps to evaluate the potential impacts of cybersecurity attacks on IACS is to understand the different objectives, motives, and strategies for each type of attack. Depending on the attacker's goals, an attack on an IACS could result in the loss of confidential information, unexpected downtime, destruction of equipment, or even potentially unsafe conditions. In this Section, we will evaluate four of the most common types of cyber-attacks: espionage, sabotage, extortion, and show of skills.

2.1.1 Espionage

Cyber Espionage, also known as Cyber Spying, is the effort to obtain sensitive and classified information or intellectual property from governments, public agencies, and private industry. These acts can use technology via the internet, networks, and software, as well as human elements, to attack and penetrate the security of critical systems, devices, and networks.

Targets of cyber espionage vary depending on the motives and the perpetrators of the activity. Theft of government secrets and sensitive or classified information is often carried out by nation states (state sponsored or supported hacking groups) attempting to gain a military, political, technological, or economic advantage. Cyber espionage happens today on a

global scale, and the threats to governments include nation states, organized crime groups, and individuals.

One recent example of cybersecurity espionage was discovered in May of 2020. The attack, attributed to Naikon advanced persistent threat (APT) Group, successfully took advantage of a backdoor to compromise multiple national governments: Australia, Indonesia, the Philippines, Vietnam, Thailand, Myanmar, and Brunei [25]. Attackers were able to collect significant information from compromised networks including specific documents, information from connected removable drives, screenshots, and key logs. (More information on APTs is provided in Chapter 4.)

A critical example of cybersecurity espionage was discovered in December of 2020. The attack, which targeted an IT network management company called SolarWinds, left as many as 18,000 customers vulnerable to attack [26]. Prominent victims of the attack include the Pentagon, nuclear laboratories, United States Treasury, U.S. Commerce and Energy Departments, and several private cybersecurity firms [27]. The attack has been attributed to an APT associated with the Russian government and demonstrated the potential for sophisticated actors to compromise many different victims by targeting common supply chain elements.

Cyber espionage is not just a concern for government agencies, as many hacking groups target private companies to steal intellectual property, sensitive data, and technology. The ability of attackers to avoid detection and remain anonymous when executing remote cyber espionage activities has continued to incentivize attackers to rely on computer-based methods. Unlike physically stealing information, cyber espionage can be conducted anywhere in the world, and often little evidence can be found to track the attack back to individuals. As a result of the low risk and potential for significant rewards, hacking groups continue to engage in a variety of cyber activities.

IACS contain much confidential and proprietary information, including process data, information on technologies, batch recipes, research and development information, design and engineering information, formulas, and other intellectual property. This information can be desirable to many different perpetrators. For example, a competitor may aim to acquire a

competitive advantage, or a nation state may want to monitor or steal military technology or information about critical infrastructure.

The value of IACS targets is not lost on cyber criminals, and an analysis of the hacking group Leafminer - well known for conducting cyber espionage - showed that the energy/ petrochemical sector was the third most targeted industry (15%), narrowly behind government agencies (17%) and the financial sector (17%) [28].

An espionage attack named "Operation Sharpshooter" targeted nuclear, defense, energy, and financial companies [29]. This attack affected 87 organizations world-wide, primarily targeting English-speaking organizations or regional offices. The attack worked in two stages. First, after an initial foothold was established, then information was gathered about connected network devices, including network adapter information, computer name, username, IP address, native system information, and operating system (OS) product name. Data was then encrypted and transferred to the attacker's server without authorization. This attack is just one of many that highlights how sophisticated attackers routinely target the process industry and critical infrastructure.

Although the consequences of data theft and loss of intellectual property can sometimes be severe on their own, many espionage attacks on IACS do not stop there. Cyber espionage is often done to collect detailed information about the target to develop a future attack. Many of the common malware (malicious software) used for cyber espionage allow attackers to gain better insight into the network architecture of IACS and even steal passwords for use in future attacks. For example, the GreyEnergy malware allowed attackers to collect information about the system, event logs, screenshots, keystrokes, passwords, and windows credentials for multiple IACS [30]. This type of information is invaluable to attackers as they attempt to learn more about targets and expand their foothold in the network. The process of collecting information about a target prior to executing an attack is referred to as reconnaissance and has been a common strategy for major attacks against IACS, including Stuxnet, the Ukrainian Power Grid, and a Petrochemical facility in Saudi Arabia. More information about the steps for reconnaissance in these attacks and the attack methods employed is provided in Chapter 6.

2.1.2 Sabotage

Cyber sabotage is a deliberate and malicious act that disrupts normal processes and functions or causes the destruction or damage of equipment or information. Cyber sabotage is not focused on theft; rather, it is a weaponized form of cyber-attack designed to damage, destroy, and disrupt. While many consider the biggest target to be military and governments, there is growing evidence of cyber sabotage against private industry, organizations, and private citizens.

The sophistication required to commit these acts was once quite high, limiting the threat to nation states and state sponsored groups. However, the techniques and tools have become more accessible and readily available, often finding their way into the hands of lower-level criminals and hacktivists (hackers with political motivation). As the sophistication required to commit these acts is lowered, the threat continues to grow each year from criminals with various motives including terrorism, anarchy, or simply financial gain.

IACS are increasingly targeted for cyber sabotage - a serious threat, which can lead to unexpected downtime and interruptions to productivity, or even significant damage and increased risk to safety. These types of cyber-attacks can come from many sources including nation states, private industry, hacktivist groups, and private citizens. Most often, the motive is the potential for economic gain or a desire to cause significant disruption or damage. Disrupting or damaging the IACS of competing nations or private industry could potentially impact their production capabilities, allowing the perpetrators to gain a tactical or military advantage. In other cases, the desired outcome may be market manipulation and economic advantage.

Distributed denial of service (DDoS) attacks are commonly used for sabotage attacks that focus on disrupting the normal processes. In this case, target networks or servers are flooded with such a large wave of internet traffic that the operating system is overwhelmed by the sheer number of requests for access. This can result in lagging service or complete inability to access critical systems and, in some cases, prevent legitimate users from accessing the service at all. Although DDoS attacks do not require a high-level of sophistication, they still have the potential to be one of the most disruptive and most powerful types of cyber-attacks by taking websites and digital

services offline for significant periods of time. Further information on DDoS attacks including industry examples and the potential impacts to IACS is provided in Chapter 4.

Two attacks on the Ukrainian power grid in 2015 [31] and 2016 [21] further highlighted the ability of attackers to disrupt critical functions in industrial control systems. In 2015, attackers gained remote access to the utility network and began to manually switch off power to electrical substations resulting in a power outage affecting roughly 230,000 residents. The strategy was changed for the 2016 attack that has been named “CrashOverride.” Once the CrashOverride malware was introduced to the system, it automatically triggered at a specified time and did not require further manual intervention. Although the 2016 attack only caused a power outage for about 20% of the city of Kiev, it introduced the potential for the same attacker to target many different sites at the same time. In both attacks, temporary blackouts were triggered affecting thousands of users.

Further analysis of the CrashOverride malware identified an even more disturbing possibility than a power outage. The malware had functionality to communicate directly with grid equipment, including the ability to disable a protective relay designed to shut down the system if high power levels are reached. This functionality, used in combination with overloading grid components, could have had the potential to damage transformers - resulting in a longer, potentially cascading outage [21].

Many other examples of cyber sabotage activities have attempted to trigger physical damage or disruption. In 2000, a disgruntled employee of a water system integrator triggered a spill of raw sewage, damaging the environment in Maroochy Shire Australia [19]. In 2010, the Stuxnet virus impacted a nuclear enrichment facility in Iran, leading to the physical degradation of at least 1,000 machines [9]. In 2014, an attack on a German steel mill led to significant damage to a blast furnace [8]. In 2017, attackers attempted to trigger a deadly explosion in a Saudi petrochemical facility [10]. Sophisticated cyber-attacks such as these certainly have the potential to cause significant harm to process facilities if not prevented. Additional information on these cybersecurity case histories is provided in Chapter 6.

2.1.3 *Extortion*

Cyber extortion is typically a crime perpetrated by hacker's intent on achieving financial or material gain. These criminals use malware (e.g., ransomware) or another malicious strategy to gain access to sensitive data, information, and other critical systems. This sensitive information or access to critical systems is then held hostage until some form of payment is received. While the motive is most often financial, the demands can vary depending on the type of attack. Hackers may threaten to release sensitive information or withhold access to information until demands are met. In other incidents they have threatened to damage systems or destroy sensitive data if payment is not received.

Cyber extortion most often involves ransomware, a type of malware that utilizes encryption to prevent an organization from accessing their critical data by blocking access to files, databases, and applications. Typically, a ransom is then demanded to restore access. Ransomware is often designed to spread across a network and target databases and file servers and can ultimately affect an entire organization. It is a growing threat, generating billions of dollars in payments to cybercriminals and inflicting significant damage and expense on businesses and governmental organizations.

A review of cybersecurity insurance claims for a North American based was cited in claims more often than any other type of cybercrime [32]. The same study also showed that the frequency of ransomware attacks against policy holders increased 260% over the first half of 2020 [32]. Unfortunately, cyber extortion will likely continue to grow as ransoms are paid, providing a steady source of income for cyber criminals with limited risk of repercussions.

Two of the many cities affected by ransomware in recent years were Pensacola, Florida and New Orleans, Louisiana. In Pensacola in 2019, Maze ransomware was used to encrypt critical files. The group behind the attack demanded a payment of \$1 million to reverse the encryption [33]. This attack went even further than typical ransomware as it also resulted in the theft of confidential information. The group placed further pressure on the city by releasing a sample of the stolen data. During the same timeframe in New Orleans, an attack using Ryuk ransomware led to a state of emergency and the shutdown of 4,000 government servers and computers [34]. By this point, the Ryuk ransomware had already been used to successfully collect over \$1.6

million in ransoms from other municipal governments including Jackson County, Georgia, Riviera Beach, Florida, and Lake City, Florida [34].

Targets of ransomware are not limited to government agencies, and there have been multiple notable incidents of ransomware attacks on IACS. One of the most widespread ransomware incidents affecting IACS was the WannaCry attack in May of 2017. The WannaCry ransomware spread world-wide, affecting computers with the Microsoft Windows operating system. The incident infected over 200,000 computers across 100 countries [35]. A security patch to remove the Microsoft vulnerability exploited in the WannaCry attack was quickly deployed, but many organizations were not able to immediately install the patch. Such updating can be particularly challenging for process control systems because of the potential downtime necessary for patching. The WannaCry ransomware continues to infect unpatched systems to this day, although not nearly as many as when it was first released. In 2021 a ransomware attack on the Colonial pipeline resulted in a significant disruption of critical infrastructure and resulted in the pipeline being shut down for multiple days [36]. Additional information on the Colonial pipeline ransomware attack is provided in Section 6.10.

2.1.4 Show of Skills

Those who commit cybercrimes have many possible motives. While the desire for monetary or political gain can be clearly linked with some attack outcomes, other attackers conduct cyber activities purely to show off their skills. Attacks completed simply for the thrill or to demonstrate their own skill and earn “bragging rights” in the hacking community can often be harder to predict or track because no clear link can be found between the attacker and the target.

The level of sophistication for these types of attacks - commonly referred to as “Show of Skills” - can vary widely based on the individual hacker’s knowledge. Some possess significant knowledge in the tradecraft and others leverage readily available online tools. Malware and other malicious scripts and protocols can easily be downloaded and deployed even by an unsophisticated hacker. These hackers are often not part of an organized group but are looking to establish some level of credibility in the hacking community.

While the threat of cybercrime for bragging rights is typically less sophisticated, it continues to be an area of growing concern. A recent study by the National Crime Agency in the United Kingdom revealed that 61% of hackers begin engaging in this activity before 16 years of age [37]. The increased exposure of children and teenagers to technology related fields can be very beneficial when channeled in a positive way such as developing skills for a career in a technical field; however, at this stage, many learn by exploring and testing their skills. In cybersecurity, this type of technical exploration can have unintentional consequences.

The skill barrier for executing cyber-attacks is lower than ever with a vast array of publicly available hacking tools. Minimal expertise is necessary to use these tools, and they are often available for little or no cost. In addition, young hackers are often emboldened by a perceived anonymity and lack of legal consequences.

Although there has yet to be a major cybersecurity incident in the process sector connected to a Show of Skills attack, it is more likely a question of “when” than “if.” The many vulnerabilities in IACS systems, associated with the potential to cause significant financial and physical damage, make them a desirable target for cybercriminals looking to achieve notoriety. As the hacker population continues to grow, so does the potential for attacks on IACS systems.

2.2 *Who Commits Cybercrimes and Their Motives*

In addition to knowing the common types of cybersecurity activities, understanding the different types of groups that commit these activities and their individual motives can help to better identify why organizations may be targeted for attack and to prepare adequate security defenses. Groups of possible attackers include the following, which will be discussed in more detail in the subsequent sections:

- Competitors
- Nation states
- Hacktivists
- Criminals
- Disgruntled employees
- Rogue wizzes
- Script kiddies

One common method of describing hackers is to identify them as black hat or white hat. Black hat hackers are those who attempt to gain access to computer networks with malicious intent such as espionage, sabotage, or extortion. White hat hackers on the other hand are often described as ethical hackers that work with companies as employees or contractors to identify security vulnerabilities and help mitigate them before they lead to an incident. In these subsections different types of attackers are discussed that would largely be considered black hat hackers.

2.2.1 Competitors

In some cases, cyber-attacks may be initiated by companies competing in the same industry, typically looking to achieve a competitive advantage. This advantage can take multiple forms. Competitors engaging in cyber espionage may hope to steal sensitive information such as proprietary technology, process data, design information, trade secrets, or formulas. In cases of cyber sabotage, competitors may be attempting to hinder production from similar companies in a desire to improve market share, damage competitor's reputation, and potentially even secure supplier contracts. Recent studies have shown that as many as 43% of distributed denial of service attacks may be attributable to competitors [38]. The potential benefits to competitors from either espionage or sabotage make them an important source of attacks to consider in a cyber risk assessment.

2.2.2 Nation States

Of the groups that complete cyber activities, nation states (state sponsored or supported hacking groups), are often the most sophisticated attacks based on the level of skill, resources, and motivation. Nation states engage in a variety of activities, including espionage and sabotage, to further a national agenda. This could consist of the theft of government secrets or classified information to gain a military, political, technological, or economic advantage. The threat of nation states is not limited purely to government agencies or the defense industry, and nation states have been suspected of completing multiple attacks on IACS including the Stuxnet [9] and two Ukrainian power grid attacks [31] [21]. Attacks focused on the disruption or damage of critical infrastructure also have the potential to support a national agenda by inflicting financial damage on adversaries or impacting policy decisions.

Nation state attacks are particularly difficult for organizations to defend against because they frequently exploit zero-day vulnerabilities, which are vulnerabilities that were not previously documented. Although discovering and exploiting unknown vulnerabilities is a time and cost intensive process, government sponsored groups often have the necessary resources to develop these types of sophisticated attacks.

2.2.3 *Hacktivists*

The term Hacktivists refers to those who use legal and illegal digital tools in pursuit of political ends, free speech, and social agendas. Unlike many groups who commit cyber activities, hacktivists are not interested in financial gain; instead, they seek to disrupt and damage targets as a means of making a stance or demonstrating support of a cause. For example, companies in the process control industry may be targeted by hacktivist groups who focus on environmental issues or other geopolitical causes.

Although the skill level of individual members in hacktivists groups may not be particularly high, hacktivist groups are known to use crowdsourcing, or input enlisted from a large number of people over the internet, to develop their attacks. In this way, hacktivist groups can receive significant support from individuals who share their political or social views anywhere in the world. Through this shared effort, many hacktivist groups are effective at executing DDoS attacks or conducting similarly disruptive behavior.

2.2.4 *Criminals*

Cybercriminals are individuals or teams of people who commit malicious attacks on digital systems or networks. The primary objective of cybercriminals is financial gain. As such, they target a variety of targets with financial resources, including government agencies, financial companies, health institutions, industrial companies, and sometimes even individuals.

Ransomware is one of the most commonly used methods for cybercrime, and many criminal groups have found ways for this to be a successful business model. In some cases, it is not only a single group involved in the attack; rather, one group invests in the development of a sophisticated ransomware program, which is then shared with a variety of attackers in exchange for a portion of the successful ransom payments. This structure, known as

ransomware-as-a-service or RaaS, was believed to be used for the Sodinokibi ransomware attack in 2019. Throughout this attack, a number of companies in the food, services, and healthcare sectors were infected with an average ransom demand of \$260,000 U.S. Dollars [39].

In addition to requesting ransom payments, cybercriminals may also seek to sell stolen information such as intellectual property, company information, or personal data for financial gain. In the 2013 Target hack, attackers gained initial access to the system through a third party refrigeration contactor, before ultimately compromising Target's point of sale system [40]. From the point of sale system attackers successfully compromised personal financial information from over 100 million credit/ debit card using shoppers [40]. In addition to companies with sensitive financial information, companies in the process industry may often make attractive targets to cybercriminals based on their size and the criticality of information available on IACS systems.

2.2.5 Disgruntled Employees

Disgruntled employees and contractors are different from the other groups evaluated in this chapter in that they often already have access to the IACS systems under consideration. They tend to pose a high risk based on their access and detailed knowledge of the system and security features. The potential for damage from an internal threat seeking revenge or financial gain can be significant and must be considered when developing security practices and protocols. Further analysis of intentional internal attacks and effective protections is included in Chapter 5.

2.2.6 Rogue Wiz

Surprisingly, some cyber criminals are not motivated by financial gain or any form of activism but purely from the enjoyment of the challenge. This group of cyber criminals is most likely to conduct a show of skills attack such as those described in Section 2.1.4. These types of hackers are sometimes referred to as gray hat, because they fall somewhere in between white hat and black hat hackers. Many gray hat hackers will investigate vulnerabilities in an organization without permission to demonstrate their hacking ability or to emphasize the need for better cybersecurity protections. Although gray hat hackers do not operate with malicious intent, they may still violate laws or ethical standards.

In 2010, a Japanese man was arrested for creating the Ika-tako or “squid-octopus” virus [41]. The virus was estimated to have compromised between 20,000 and 50,000 computers, replacing the files of victims with cartoons of squid, octopus, and other sea life created by attackers. When arrested, the hacker told police “I wanted to see how much my computer programming skills had improved since the last time I was arrested.”

Another attack conducted in San Francisco in 2014 exploited a vulnerability in traffic signs to replace traffic warnings with fictitious warnings such as “Godzilla Attack” or “Nearby Zombies” [42]. Although some attacks by rogue wizzes may seem to be harmless, the potential for very real damage exists if a hacker chooses to test their skills on an IACS network. In this case, the attack could easily lead to unexpected downtime and financial loss or even the potential loss of critical systems.

2.2.7 Script Kiddies

A script kiddie is an unskilled person who uses tools developed by others to hack computer systems and networks. In many cases, script kiddies are juveniles or other unskilled hackers who lack the ability to write sophisticated programs on their own. Instead, they use readily available programs developed by skilled hackers to execute their own attacks. Often, script kiddies may hope to impress friends or gain credibility in hacking communities for their exploits and do not fully understand the implications and potential damage of their actions.

Due to the large number of readily available hacking tools, script kiddies are a quickly growing group and may already make up a large portion of cybersecurity attacks. Although they do not have sophisticated skills for penetrating secure networks, script kiddies can use social engineering techniques such as emails with malicious links and available databases of compromised passwords. In this way, script kiddies can compromise many unprotected networks, including internet facing networks for companies in the process industry.

2.3 Summary

In this chapter, we discussed the most common types of cybersecurity activities, groups who are likely to commit them, and their possible motives.

Developing an understanding of types of cybersecurity activities is an important foundational element for accurately determining the potential consequence of a cybersecurity event. Furthermore, knowledge of the various perpetrators and their intents behind cybersecurity incidents is a key step in assessing sources of cybersecurity risk and developing effective countermeasures.

3 Types of Risk Receptors / Targets

Understanding cybersecurity hazards and risk is one of the pillars in the RBPS approach for cybersecurity. To effectively consider cybersecurity as part of business planning activities, it is necessary to develop a common language for discussing, comparing, and prioritizing risks from any source – including cybersecurity and process safety incidents.

Risk is defined as the possibility of injury or harm and is a measure of the likelihood (frequency) and consequence (severity) of an adverse effect. Depending on the risk receptor, or the entity experiencing harm, the severity of the consequence can be expressed in different ways. Process safety focuses on the management of hazardous materials and energy where loss of containment events can result in fire, explosion, and toxic effects. These consequences may cause harm to the health and/or safety of people and damage the environment. An organization may also be impacted financially by property damage and business interruption.

When process safety risk is evaluated, the frequency is determined by considering the likelihood that an initiating event could occur. Example causes include equipment failure, instrument or valve failure, and human performance issues. The likelihood for these causes to produce an initiating event are statistically determined based on long industry experience. The consequence is determined by following a chain of events from the initiating event to the potential ultimate outcome in absence of safeguards that could reduce the consequence or halt the chain of events entirely. For an individual event, the equation is shown in Equation 3-1.

$$R = C \times F \quad \text{Equation 3-1}$$

Where:

R is risk

C is the consequence

F is the frequency

In process safety, a third factor - defined as operational discipline - has been identified to have a significant impact on process risk. Operational discipline is an outcome of an effective conduct of operations program (see Section 10.16). A conduct of operations program addresses the potential of human behavior to introduce risks by enforcing the use of required systems and procedures correctly, every time [43]. As the operational discipline improves it leads to a reduction in overall risk as shown in Equation 3-2. In process safety, operational discipline focuses on reducing the likelihood of human performance issues initiating a potentially hazardous scenario. In cybersecurity, operational discipline can also have a significant impact on risk by improving cybersecurity hygiene (awareness and adherence to best practices) which reduces the exposure or vulnerabilities of and IACS.

$$R = \frac{C \times F}{f(\text{Operational Discipline})} \quad \text{Equation 3-2}$$

Where:

R is risk

C is the consequence

F is the frequency

$f(\text{Operational Discipline})$ is a function based on the implementation of the operational discipline program

Companies may experience harm in a number of different areas including human, environmental, and financial impact. To determine the total level of risk to which a company is exposed, a risk integral is used to account for all consequences to all risk receptors. This is mathematically expressed in Equation 3-3.

$$RI = \sum_{i=1}^n C_i \times F_i \quad \text{Equation 3-3}$$

Where:

RI is the total risk (risk integral)

n is the number of hazardous events

C is the consequence of the individual event

F is the frequency of the individual event

Accurately determining the overall risk to a process facility cannot be understood solely by evaluating process safety risk; other sources of risk – including cybersecurity risk – need to be considered to develop a complete organizational risk profile. Chapter 2 identified common cybersecurity activities that have the potential to result in adverse effects on the process control system. These cyber incidents can also have an effect on risk receptors currently considered in a Risk Based Process Safety program and have the potential to introduce new risk receptors or levels within existing risk receptors.

3.1 What is Cybersecurity Risk

Process safety risk is concerned with the management of hazardous materials and energy where loss events can result in fire, explosion, and toxic effects. Industrial (OT) cybersecurity risk is concerned with intentional or unintentional interference with the potential to compromise industrial automation and control systems by means of computer connected systems. To account for the potential of compromise the likelihood of a successful attack, L_{AS} , is substituted for initiating event frequency in the process risk equation and is expressed by Equation 3-4.

$$R = C \times L_{AS}$$

Equation 3-4

Where:

C is the consequence of the attack

L_{AS} is the likelihood of a successful cybersecurity attack

The likelihood of a cybersecurity event can come from either a malicious attack (intentional) or an operator error (unintentional). The likelihood of a successful cyber-attack (L_{AS}) [44] is the product of threats, vulnerabilities, and target attractiveness and is expressed by Equation 3-5.

$$L_{AS} = T \times V \times A_T \quad \text{Equation 3-5}$$

Where:

L_{AS} is the likelihood of a successful cybersecurity attack

T is the threat; any person, indication, circumstance, or event with the potential to cause loss of, or damage to an asset

V is vulnerability; any weakness that can be exploited by an adversary to gain access to an asset

A_T is target attractiveness; an estimate of the value of a target to an adversary

Incorporating the components that lead to the L_{AS} into the risk equation yields Equation 3-6.

$$R = C \times T \times V \times A_T \quad \text{Equation 3-6}$$

Consequence severity (**C**), threats (**T**), vulnerabilities (**V**), and target attractiveness (**A_T**) are the four factors that determine the level of risk for a cybersecurity scenario.

The **consequence severity** of a cybersecurity incident is dependent on the inherent characteristics of the target (e.g., quantity of hazardous chemicals, type of hazardous chemicals), objective of the attacker, and the components of the process control system that are compromised. Section 3.2 will review the common targets on the IACS for cybersecurity attack and evaluate the potential consequences associated with the compromise of different targets. The consequence severity can be further refined by considering which risk receptor is affected and will be discussed in additional detail in Section 3.3.

Threats in cybersecurity can come from many different sources including individuals, organizations, and even government sponsored groups. In Chapter 2, a number of potential threats to IACS were discussed and the types of cybersecurity activities each group is most likely to conduct were introduced. The frequency at which threats conduct cybersecurity attacks are based on a number of additional factors such as the required sophistication for an attack and whether the attack is conducted by an insider or an outsider. In general, the higher the level of sophistication required for an attack, the lower the frequency at which the attack will be executed. Chapter 4 will further evaluate the level of sophistication for common attack types. The impact of internal vs. external cybersecurity threats will be evaluated in Chapter 5.

When considering **vulnerabilities** in the cybersecurity context, it is important to understand the difference between a cybersecurity risk and vulnerability. A vulnerability is defined as: “a design flaw or weakness in a device, application, or system such that its operation and management could be exploited to advance a cyber-attack” [45]. While risk represents both the likelihood and consequence of a cyber event, a vulnerability is related to a weakness in the cybersecurity defense of a system that can be exploited during a cybersecurity attack. As such, a vulnerability, while not creating a cybersecurity risk, does increase the risk for a control system by increasing the likelihood that an attack would be successful. Vulnerabilities are commonly rated based on criticality and exploitability. The criticality is a measure of the significance of the impact of an attack on the affected software program or operating system (e.g., can an unauthorized user make change?). The exploitability is a measure of how easy it is for an attacker to take advantage of the vulnerability. Vulnerabilities with a high criticality and a high exploitability represent the most serious concerns.

The **target attractiveness** is a measure of how likely an attacker is to target a specific facility. It is a combination of the entity's public image or reputation, industry sector, and how much it assists the threat agent's goal, be it business, political, or personal. For example, CFATs facilities are critical to national infrastructure and, as such, are more attractive than a small regional plant. Like many factors involving cybersecurity, target attractiveness can change drastically in a very short period of time. Media exposure and the potential for information to spread rapidly online can also cause target

attractiveness to change rapidly. A published report about a chemical company performing legal but unpopular animal testing could quickly raise the attractiveness of their facility to hacktivist groups. A similar trend can be observed for organizations with a record of environmental spills or other activities that may be seen as undesirable by hacktivist groups.

Target attractiveness also depends on the intelligence available. If a plant's control system plans have been leaked online, compromising that plant may be much easier, making the plant a much more attractive target. Unskilled hackers such as Script Kiddies can search the peer-to-peer networks and use tools from the dark web (encrypted online content that is not indexed by search engines and can only be accessed through specific browsers) to find intelligence on the plant with minimal effort. This can allow someone with even relatively low skill easy access to its internal networks if it is in line with their motives.

Chapter 9 will discuss in detail considerations for conducting a cybersecurity Hazard Identification and Risk Analysis (HIRA) including how to identify threat vectors, utilization of tools such as the National Institute of Standards and Technology (NIST) Common Vulnerability Scoring System (CVSS) to assess vulnerability and factors that influence the attractiveness of a target.

3.2 *What are Common Cybersecurity Targets?*

The process industry has many targets that may be attractive to cybercriminals. Depending on their motivation, attackers will target different components on the process control system. Furthermore, the higher the extent of damage that can be caused by successfully compromising a target, the more desirable or attractive that target is to the attacker. The specific methods used by attackers to compromise systems will be evaluated in greater detail in Chapter 4, while this section focuses on the common cybersecurity targets in IACS.

3.2.1 *Process Safety Controls, Alarms, and Interlocks (PSCAI)*

Process Safety Controls, Alarms, and Interlocks (PSCAI) are safeguards implemented with instrumentation and controls. PSCAI are used to achieve or maintain a safe state for a process, and are required to provide risk reduction

with respect to a specific hazardous event [4]. These critical components often comprise multiple layers of protection used to achieve process safety. Numerous case studies including Stuxnet [9] illustrate how cyber-attacks can penetrate IACS and compromise PSCAI, impacting multiple layers of protection at the same time. Using the Stuxnet malware, attackers seized control of the uranium centrifuge process and introduced control upsets that caused the centrifuges to damage themselves. The objective of Stuxnet was to damage equipment, had the objective been more aggressive such as a safety impact, the outcome could have been much more severe. One particularly unsettling aspect of Stuxnet is that the attackers were able to feed the operator fake process data that suggested that the process was operating normally when it was actually impaired. This type of action, called a “man-in-the-middle” attack, is described further in Chapter 4.

Disruption of PSCAI has the potential for the highest safety consequences in a process facility. The BPCS provides primary control of the process hazards. If an unauthorized party were to gain access to the BPCS, they could command the system to perform any number of operating deviations that might initiate a major loss of containment scenario. The results could potentially include the release of hazardous and/or toxic chemicals, fire, explosion, or fatalities. Such an event could impact the safety of site personnel and the public, damage the environment and physical equipment, sully business reputation, and have enormous costs to mitigate damages and repair or rebuild the facility.

A cyber-attack does not need to initiate an event directly; rather, they can disable a protective measure and wait for an initiating event to occur. A Safety Instrumented System (SIS) and a High Integrity Pressure Protection System (HIPPS) are examples of independent protection layers that are designed to prevent or mitigate the consequences of a hazard scenario due to initiating events such as control system failure. The interlocks and controls within these systems are designed to provide protection for specific scenarios. They stand by passively until a specific process deviation occurs and then take action. Cyber-attacks on this type of system need not be sophisticated. Simply changing an interlock trip point or placing an interlock in bypass can permit a process upset to propagate into a high consequence loss of containment event with safety, environmental and financial implications.

An alarm is “an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response” [46]. Alarms are commonly used in the process industry to help operators respond to process upsets before they lead to unsafe operating conditions or negative financial impacts. In addition to sending incorrect process data to human machine interfaces, sophisticated attackers can also disable process alarms and effectively impair the view of the control room operators to the current state of the running process.

Configuration Management Systems (CMS) are often a combination of company procedures and software tools that are used to maintain traceability and accuracy for configured systems including PSCAI. CMS allow for changes to the configuration for controllers and other types of network equipment to be documented, tracked, and deployed more efficiently. CMS can make attractive targets for attackers looking to hide the tracks of their attacks or gain a better understanding of configured elements. Modifying control or safety interlock settings in the CMS is one method of compromising PSCAI. Compromising any one PSCAI layer of protection can lead to a significant increase in risk, but the potential for a single cybersecurity attack to lead to a common cause failure of multiple protection layers is particularly concerning.

3.2.2 *Other Connected Systems*

Although PSCAI are attractive targets for those looking to complete cyber sabotage because of the magnitude of damage that can be done, they are not the only options for attackers looking to disrupt the IACS. Targeting computers or servers on the IT or OT networks may in some cases be easier targets than compromising the PSCAI directly.

It is often necessary to have some connectivity between the IACS and the business systems (often through firewalls inter-network connection devices that restrict data communication traffic between two connected networks [3]) to provide means for software updates, recipe management, and production reporting. Such pathways should be carefully managed to perform specific communication tasks between the IT and OT networks. Leveraging these pathways, an attacker may seek to affect the PSCAI indirectly by altering documents on the IT network or non-control devices on the OT network and allowing authorized communication processes to carry the incorrect

information across firewalls to the desired target. Non-PSCAI systems a cybercriminal may seek to exploit include:

1. Digital Twins
2. Recipe inputs (e.g., downloads from enterprise management system)
3. Computerized Machine Management Systems (CMMS)
4. Digital procedures and checklists

A digital twin is a digital copy of a process used to train operators and optimize the process with dynamic simulation. An attacker might access the twin directly or intercept information between the twin and the live process. If the twin is accessed directly, it can be used by the attacker to better understand the process and develop a plan for initiating complex event scenarios that could overwhelm the operating staff and safety systems. The plan may be used during a BPCS attack, potentially increasing the consequences beyond the level anticipated for a single initiating event scenario. If the attacker is unable to access and control the twin directly, they may intercept and alter communication between legitimate users and the process. Digital twins often receive real-time information from the operating process, and disrupting communications (such as a denial of service attack) can lead to loss of analysis/insight from the simulation or potentially even alter the results.

Batch chemical processes rely on process recipes to produce a suite of chemicals that may require common raw materials but create finished product with different properties and performance characteristics. For example, in a resins process, the recipe composition includes raw material charge quantity, charge rate, heating and cooling cycles, hold times and solvent strip rate and quantity. Incorrect measures or operations can lead to quality issues, over-reaction coagulating a batch in the reactor, or a runaway reaction with the potential for vessel rupture. Recipes are often developed on the IT network, where they may be more vulnerable to access. Compromising recipe formulation or operating parameters before they are transferred to the OT

network is a viable means of causing process upset or initiating a high consequence event.

Another potential target is a CMMS. These are widely used in industry for tracking maintenance-related activities for process control equipment, safety critical components, and rotating equipment. An attacker could delete or modify maintenance work orders or request to delay both preventative and reactive maintenance activities. In the event of significant delays, this can lead not only to financial harm due to wear out beyond allowable limits but could create safety and environmental concerns due to the catastrophic failure of incorrectly maintained equipment.

Other information and documents may be created and managed within the IT network that are intended to support the success of the human layer of protection. Some examples include operating procedures and checklists. These documents could be altered in ways to provide incorrect information that may not be noticed when used. Some possible alterations include:

- Changes to setpoints, control limits, or safe operating limits on a standard operating procedure (SOP).
- Modification or deletion of steps in an alarm response procedure.
- Addition to, deletion of, or reorganization of, steps in a checklist.
- Alteration of methods or targets in a proof test procedure.

3.2.3 *Interconnection Vulnerabilities*

As the connectivity of industrial automation control systems continues to grow, process safety professionals must be aware that anything digital and interconnected is susceptible to cybersecurity attack. PSCAI and connected systems are not only attractive targets for sabotage purposes, but due to the critical nature of the information stored in these devices, they can also be attractive for attackers looking to conduct espionage or receive ransom payments for the return of encrypted data.

Espionage or extortion attacks can also target business information for process industry companies. This type of information usually resides on the IT network to accommodate the many systems feeding information into the centralized location. This also makes it easier for users to extract data from the business information repository and perform analysis activities. These databases often include intellectual property (formulations, production

methods), commercial information (pricing, customer list), logistics (supply chain, product shipping) and business plans. Obtaining access to the information could provide a competitor with a competitive advantage resulting in a loss of sales revenue.

IT networks are not the only peripheral network typically connected to process control systems. The Internet of Things (IoT) consists of any device with an embedded sensor, software, or technology for the purpose of communication. The IoT provides multiple potential entry points to the control system. IoT devices are so common that they are often connected to the OT system without an awareness that they can be potential back doors inviting cyber-attack. Examples include smart factory equipment, process instrumentation, wireless shipping container trackers, printers, photocopiers, and cell phones. During the Stuxnet investigation, cases were identified where print drivers were used to install and spread malware on the process network [9]. The potential security implications of connecting IoT devices to the control environment is further explored in Chapter 8. In some cases, control systems across physically separate sites will even be connected using cellular or satellite networks further increasing the interconnectivity and access vulnerability.

3.3 *Types of Cybersecurity Consequences*

Unlike cybersecurity incidents on IT systems, which tend to result almost exclusively in economic consequences, OT cybersecurity incidents can create a number of potential consequences, depending on the objectives of the attacker. These include traditional process impacts to safety, the environment, and business risk. In some cases, an organization's risk matrix may require modification to consider other impacts such as reputational damage or loss of intellectual property/ competitive advantage. Table 3-1 provides a summary of information that should be considered when updating a process safety consequence severity table to apply to cybersecurity risk assessment.

Table 3-1 Considerations for Consequence Risk Table

Types of Consequences	Consideration
Safety	• Injuries/fatalities • Off-site consequence
Health	• Exposure onsite or off-site • Long- or short-term effects
Environment	• Release or spill • Reversibility of consequences • Remediation • Regulatory consequences
Community	• Exposure • Shelter in place • Evacuation • Property damage • Business reputation • Media coverage
Economic	• Potential to impact multiple units • Equipment and property damage • Government/ authority fines • Business interruption, unplanned shutdown • Loss of intellectual property • Profit erosion
Company Image/ Reputation	• Negative media coverage • Loss of privacy • Loss of stakeholder confidence • Loss of license to operate

3.4 *Summary*

This chapter introduced the equations for determining process safety and cybersecurity risk. Understanding how the consequence, type of threat, attractiveness of the target, and number of vulnerabilities affects the likelihood of a cybersecurity attack is a key step in performing cybersecurity risk assessment and applying a risk-based approach for cybersecurity. Additionally, common targets in the IACS system were identified and a wide range of possible consequences resulting from a cybersecurity attack were reviewed. Unlike traditional IT systems, attacks on IACS can have many possible outcomes including consequences for humans, the environment, businesses, and the community.

4 Threat Sources and Types of Attacks

Threat sources are the people or groups that may attempt to gain unauthorized access to the process control system in order to execute an attack. In Chapter 2, we identified groups that commit cybercrimes and identified multiple potential threat sources to control systems such as competitors, cyber criminals, and nation states. This chapter will cover threat sources in more detail and examine how the type of threat source is related to the attack complexity, possible types of attack, and likelihood of attack.

Understanding the motives and types of threat sources is an important aspect of cybersecurity because the level of skill and motivation of a threat source is directly related to the type and sophistication of the cyber-attack. Three broad classifications for attack types are: Non-Targeted, Targeted, and attacks by advanced persistent threats (APT). For each type of attack, we will evaluate the most common methods for introducing the attack and the possible outcomes.

Whether an attack is targeted or untargeted, it will often involve malware or software designed to interfere with the expected functionality of a computer, system, or network. Many kinds of malware are present in today's cybersecurity ecosystem, with the most common types being viruses and worms.

A computer virus is a type of malware that inserts itself into a legitimate program or application. The virus modifies the program, usually by deleting or corrupting files, and the computer system itself can be damaged. The virus is able to replicate and spread to other systems on the network once the program is run. Computer viruses can spread easily when someone visits a website and downloads files or opens an image. A common virus tactic is to read the victim's email contact list and then send itself to each person on the list in an email. The virus then spreads to the recipient's computer when the recipient opens the email attachment or clicks on an included link. Spoofing is the process of disguising an unknown and often malicious source as a trusted and known source. Spoofing is a commonly used technique to increase the likelihood of a user triggering a virus. In this chapter, examples of spoofing as a social engineering technique (e.g., email phishing) will be introduced.

Spoofing can also be used to execute complex attacks such as man-in-the-middle attacks (discussed in Section 4.2.2).

A computer worm is similar to a virus, with the key difference being that it can self-replicate without any human action. To infect a computer, a virus requires a step such as clicking on a link, enabling a macro, or allowing a program to make changes; however, a worm can spread without any of these actions. In some cases, the only step necessary for a worm to spread is to visit an infected website or be connected to an infected device or network. As a result, computer worms such as NotPetya (discussed in Chapter 6) can propagate rapidly through networks once they are introduced.

Depending on how the malware is executed on the system and its intended function, many further subtypes may be found, such as those listed in Table 4-1. Although the type of malware depends on the behavior and intended objective of the malicious software, malware is generally designed to take advantage of known vulnerabilities or weaknesses in software and can impact any system which contains the vulnerability, as demonstrated in the WannaCry attack [35] introduced in Chapter 2.

Table 4-1 Attack Characteristics by Threat Source Type

Malware Type	Definition
Trojan Horse	Any malware that misleads users of its true intent, typically by disguising itself as legitimate software.
Spyware	Malware that enables a user to obtain confidential information about the victim’s computer activities by transmitting the data from the infected device.
Ransomware	Malware that encrypts to critical files on an organization network, preventing them from accessing devices, databases, and applications unless a ransom is paid to the attacker.
Rootkit	A set of software tools that allow an unauthorized user to gain access and control of a computer without being detected.

Cyber-attacks can be general (non-targeted) or specific (targeted) to an individual victim. Attackers need to consider their desired objectives: is the malware intended to target one specific company or is it intended to infect as many different companies as possible? Non-targeted malware is opportunistic in nature and depends on affecting a sufficient number of possible victims to achieve the intended outcome (e.g., ransomware payment from five companies). Targeted malware attacks are designed to achieve a specific outcome on a specific victim. Attacks by advanced persistent threats (APT) are a subset of targeted attacks, but often have a higher level of resources and skill behind the attack, making it beneficial to consider APT specific concerns.

4.1 Non-Targeted Attacks

Non-targeted attacks are the most common types of attacks because non-targeted malware has the potential to impact a high number of targets/systems, and the malware can sometimes be used by many different attackers. Designing malware typically requires a high-level of sophistication and skill, which limits the number of attackers able to create it. However, now many malware kits containing the malware source code and instructions on

how to deploy the malware are readily available. With these kits, even unskilled attackers such as script kiddies can use sophisticated malware in their attacks. The source codes of major industrial attacks, such as Stuxnet, are also readily available on the dark web and can provide a detailed blueprint for future attacks.

Although the probability of success of a non-targeted attack on any one system is low, by expanding the number of possible targets, attackers can increase the likelihood of achieving their goals. The more widely used an operating system, the higher the number of possible targets and the more attractive it is for an attacker to exploit.

Beginning as far back as the mid 1990's, there was a growing trend to move automation systems to a Microsoft Windows-based platform. Although this had a number of positive effects, such as increased functionality and easier integration, it also greatly increased the potential for non-targeted attacks to affect automation systems including process control systems. This potential is furthered by the frequent use of Commercial Off-the-Shelf (COTS) products in automation systems of all types (e.g., Microsoft Office, Personal Computers, and Programmable Logic Controllers). By using readily available products, companies can significantly reduce the upfront purchase cost over customized solutions. However, if a vulnerability is present in the COTS product used, malware designed to exploit this vulnerability has the potential to impact each system where the product is used.

4.1.1 Non-Targeted Attack Methods

Non-targeted attacks can be introduced to networks in a variety of ways, including:

- Social engineering
- Watering hole attacks
- Poorly configured segmentation between control and IT networks
- Internet facing/ wireless devices and brute force attacks
- Removable media

Social engineering is the manipulation of people into providing confidential or personal information and is commonly used in cybersecurity attacks. Phishing is one common social engineering technique that uses email to attempt to acquire sensitive information (e.g., passwords) or trick users into

clicking on a link that loads malware onto the affected computer. Other types of social engineering attacks are common, such as the attacker calling a support helpline while pretending to be someone in the organization and asking for a password or a new access account. In many cases, support personnel want to be helpful and may provide this information if not properly trained to detect potential social engineering techniques. A phishing benchmarking study showed that, without awareness training, the average number of phishing emails where the link was clicked was 37.9% across all industries and all size organizations [47]. The percentage of phishing emails where the link was clicked was even higher in large manufacturing companies at 46.8% [47]. In other words, nearly half of employees at large companies were susceptible to phishing type attacks.

A watering hole attack or drive-by is when malware is downloaded to a victim when a website is visited. This can be done by either compromising a website (adding code that automatically downloads the malware when visited) or by unknowingly directing victims to a different website. In either case, the victim does not need to perform any action other than visiting the affected website. One relevant example of drive by attacks affecting control systems is the NotPetya attack; this attack is analyzed in more detail in Chapter 6.

Poorly configured or non-existent segmentation can be used by attackers to move from the IT network to the IACS. Although IACS are not intended to be connected to the internet, in many cases attackers first gain a foothold on the enterprise network before compromising the more isolated control network. This can happen when a compromised device communicates with a computer on the control network through an allowed firewall rule. For example, if a firewall allows a connection to be made from the IACS to a data historian on a corporate network and the historian is compromised, the attacker has the ability to communicate with devices on the IACS from the historian and can potentially introduce the malware using the allowed connection.

Another common strategy for non-targeted attacks is to scan lists of internet-facing devices using specially designed search engines to identify if any IACS devices have been unknowingly connected. Shodan, one such search engine, is commonly used by hackers and security engineers alike. Shodan

contains information on hundreds of millions of internet-connected devices and includes specific sections dedicated to Industrial Automation Control Systems [48]. The IACS section allows for searches based on control system-specific communication protocols including Modbus, Ethernet/IP, and other proprietary protocols, and researchers have collected over one million unique IP addresses for IACS or IACS related devices [48]. Internet-facing industrial devices with default accounts and security settings can be easily compromised using brute force attacks that can automatically attempt hundreds of thousands of possible passwords to gain access.

Removable media is another common source of unintentional malware introduction. Even in cases where the control network is “air-gapped” or fully isolated from the enterprise network, if an infected flash drive is connected to the system, it is possible for malware to spread. Removable media is frequently used in IACS because even isolated networks require that information be shared with external systems (e.g., historian data, process logs, anti-virus definitions, system updates). When external devices, such as removable media or temporary network connections, are connected to the control system, the potential exists to introduce malware if the connected devices have already been infected.

Regardless of what method is used to first introduce malware to an IACS, once introduced it has the potential to result in significant problems for the control environment including loss of data, hardware failure, or an inoperable system. Non-targeted attacks are designed to affect as many targets as possible, and as such are not designed to modify specific controller setpoints or disable safety critical functions. This is not to say that non-targeted attacks do not have a significant impact on the system; in many cases, even non-targeted attacks can result in significant financial consequences due to the loss of critical data or unintended downtime. Any impact on the availability of safety and control-related functions has the potential to negatively affect the reliability and safety of a process plant even if the attack is not specifically designed to trigger a hazard scenario.

4.1.2 Ransomware

Another commonly employed method for non-targeted attacks is ransomware. Ransomware is a common type of malware that encrypts user

data, causing it to be unusable until the victim pays the attacker and receives the decryption key. In Chapter 2, ransomware was introduced as the most frequent cause in cybersecurity insurance filings [32] and was the type of malware used in the WannaCry attack. The prevalence of ransomware is likely due to a number of factors; among these are the ease in which ransomware can be deployed by hackers with limited skill and the financial benefit for attackers when a ransom payment is made (often in a digital currency that is difficult to trace such as bitcoin). If the victim does not pay the ransom, the encrypted data cannot be recovered, and the victim must attempt to recreate the lost data from other means such as manual backup files. More advanced ransomware attacks often encrypt the backup mechanism or the network locations where the backups are stored, making it difficult for users to recover the information themselves (unless separate offline backups are maintained). This leaves victims in a difficult position of either paying the ransom or losing the encrypted data. In either case, there is a financial consequence related either to the cost of the ransom payment or the cost of lost operations until critical data can be restored.

In Chapter 2, the potential for ransomware-as-a-service (RaaS) was also introduced. In this case, unskilled attackers can use a sophisticated ransomware program developed by skilled attackers in exchange for a portion of the ransom payment. This strategy benefits both groups involved because it allows for a higher number of targets to be affected, increasing the total ransom payments received.

4.2 Targeted Attacks

In targeted attacks, the attacker has a particular victim or type of victim in mind. These attacks generally require victim-specific information to be deployed effectively. Obtaining this type of information and incorporating it into the malware design requires a higher level of skill and motivation than non-targeted attacks but increases the likelihood that the attackers will successfully compromise the target.

As introduced in Chapter 2, cyber espionage is often the first stage in targeted attacks to provide greater information about the target. This information allows the threat source to operate on the victim in a way to increase the likelihood of success. Information about the physical plant setup

such as equipment type and location, as well as network specifics such as IP addresses, personnel information, and security policies, can be used to improve the specificity of the attack and ensure that it exploits vulnerabilities present in the target system.

Targeted cybersecurity threats can be aimed at individuals or organizations. An attack targeting a specific individual will use personalized information to make the attack seem as though it came from a credible source. For example, if the attacker successfully obtained credit card information from an attack on a business used by the victim, then the attacker can create an email appearing to be from the victim's credit card company with an attached receipt to be validated. This email could contain a link to a website where the user would enter identification information or could include a virus that is downloaded when the link is clicked. This type of highly focused phishing is commonly referred to as spear phishing and requires a higher level of sophistication to create than traditional phishing emails. Spear phishing can be effective against organizations as well as individuals. In many cases, spear phishing is targeted at users with privileged access to the control system and can be even more effective than traditional phishing attacks.

When designing targeted attacks, attackers have the option to pick from any of the introduction methods discussed for non-targeted attacks, but attackers have the added benefit of selecting the methods most likely to succeed at compromising a specific target based on their knowledge of the network and user behavior. Just as spear phishing is a more targeted version of typical social engineering, watering hole attacks can be made more specific by targeting the websites that the target or type of target is known to visit frequently. Brute force attacks can be done against exposed internet-facing devices by using a search engine to identify specific devices on a company's network. Even protections for securing remote access such as two-factor authentication can be overcome by targeting contractor and employee remote workstations and connecting over the VPN once access is established. With the right precautions, these types of attacks can avoid detection and go unnoticed for significant periods of time.

Targeted attacks are not just more sophisticated in their means of gaining access to a system, but in many cases, they can also have a more severe impact

on an organization because the attack is intentionally designed for that target. Attackers also have the option to try and manipulate settings for control or safety critical assets because the attack is designed specifically for the target. Two types of attacks designed to specifically affect an individual target are denial of service and man-in-the-middle attacks.

4.2.1 Denial of Service

Denial of service (DoS) attacks interrupt the access of authorized users to computers or web services by causing a scarcity of resources (e.g., overwhelming network connections or device memory). This can result in lagging services or a complete inability to access critical systems, in some cases preventing legitimate users from accessing the service at all. The most common DoS attacks work by generating so much traffic that the requests from authorized users cannot be processed. In some cases, malware can also lead to denial of service by improperly using a computer's resources until it experiences insufficient memory, processing, or storage space available to complete necessary activities. Each of these types of DoS attacks can be made against an IACS network if network devices are exposed to the internet, the malware is introduced to the IACS (e.g., removable media), or the attack is initiated from a compromised business asset.

Some malware is designed with the ability to launch DoS attacks from infected machines. If multiple infected machines are used to launch an attack, it is referred to as a Distributed Denial of Service (DDoS) attack. DDoS attacks are particularly effective because few services or devices can cope with an attack from thousands - or in some cases, hundreds of thousands - of infected machines. Figure 4-1 illustrates how attackers can infect and leverage multiple machines in a DDoS attack on an identified target.

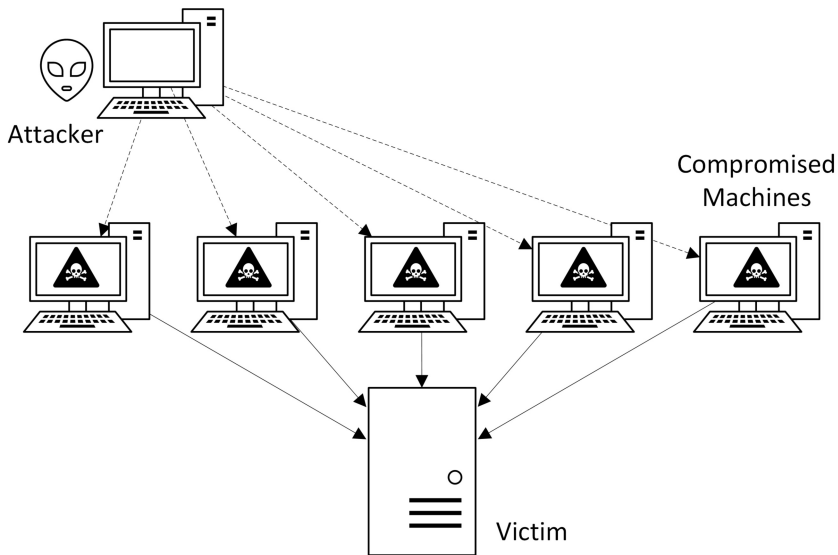


Figure 4-1 Distributed Denial of Service Attack Diagram

DDoS attacks are one of the most common attack types for sabotage on critical systems, web sites, and operational systems. In the past, it took a good deal of sophistication to infect computers to establish a botnet - a grouping of infected machines controlled by an attacker through instructions sent from a command-and-control server.

However, as exploit kits and other hacking tools have become more common, the following trends have been seen in DDoS attacks:

- The skill required to execute a DDoS attack is decreasing, and
- The average size of botnets is increasing.

As introduced in Chapter 2, script kiddies are inexperienced hackers who have limited ability to write code, but even they are capable of using exploit kits to launch effective DDoS attacks. While a DDoS attack is one of the least sophisticated types of cyber-attack, it also has the potential to be one of the most disruptive and most powerful by taking websites and digital services offline for significant periods of time.

Part of the disruptiveness of DDoS attacks can be attributed to growing botnet size. In the 2000's to early 2010's, botnets typically only contained a few

hundred infected machines. However, with the rapid expansion of internet users in recent years, botnet size has also increased. Botnets today can include hundreds of thousands of infected machines. These counts include different types of internet-connected machines including personal computers, laptops, servers, and Internet of Things (IoT) devices. Cybercriminals gain access to these devices and other network resources and then leverage them without the owner's knowledge to facilitate the attack.

One of the largest DDoS attacks to date was the 2016 Mirai Botnet. This attack was one of the first major attacks to target IoT devices including digital video recorders, digital video cameras, routers, and printers [49]. At its peak, the Mirai Botnet had over 600,000 compromised devices and was used to launch over 15,000 attacks against security firms, service providers, and telecommunications providers. A series of attacks ranging from a few seconds to a few hours were conducted against Dyn, a Domain Name System (DNS) supplier for popular sites including Amazon, Netflix, PayPal, Reddit, and Twitter [49]. This attack caused some of these sites to be unreachable for many users trying to reach the site over that period.

4.2.2 *Man-in-the-Middle*

A man-in-the-middle (MITM) attack occurs when the communication between two parties is intercepted and manipulated by a third party. Generally, one of the parties in the attack is a human user and the other is a device or website; however, it is possible to conduct a MITM attack for any combination (e.g., human user to human user, device to device, website to website, or device to website.) A key element of a MITM attack is to avoid detection so that the user does not realize the information is being manipulated. A general cybersecurity example for a MITM attack is the case where an attacker compromises a website and can steal credentials for a user trying to log on to the website.

MITM type attacks can be particularly effective in an OT setting when the operator is shown an altered view of the process compared to what is actually taking place. This was the technique used in the Stuxnet attack to provide fake process data showing normal operation of the centrifuges when the operation was in fact in an abnormal state [9]. By leading operators to believe the centrifuges were within the operating limits, the Stuxnet attack was able to go undetected for a longer period and cause more significant damage to the

uranium enrichment facility. Figure 4-2 illustrates how attackers can block the original connection in an OT setting and provide incorrect data to the workstation.

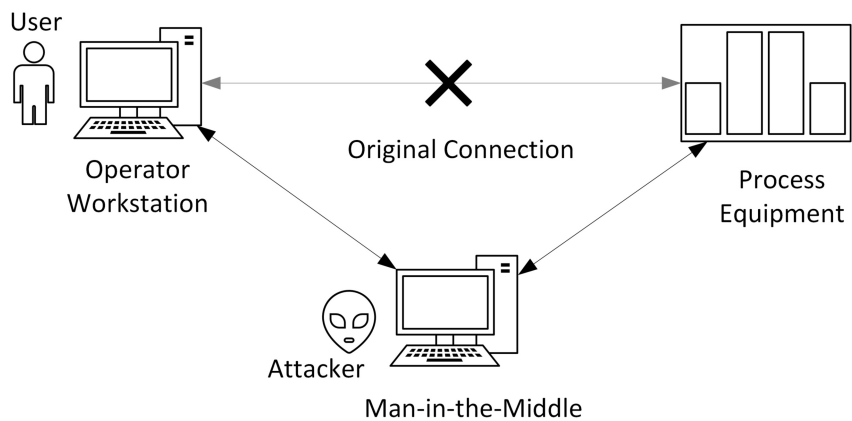


Figure 4-2 Man-in-the-Middle Attack Diagram

In addition to blocking operator visibility to actual process conditions, MITM attacks can change the commands to the process. This can lead operators to think a small change in a parameter is being made when a much larger change is actually made. To be effective, the MITM needs to be implemented and executed in such a way as to not alert operators. This generally involves extensive reconnaissance into typical operating conditions and the creation of realistic replacement data (e.g., feeding a constant value, which does not change at all, for a process variable would quickly be identified as a potential fault). Digital twins are a particularly attractive target for attackers conducting MITM attacks because they provide a detailed look at the typical system response to different process conditions and can be used to generate realistic replacement data. The level of specificity for MITM attacks can only be achieved in targeted attacks focused on a single or limited number of similar targets and requires a high level of sophistication behind the attack.

4.3 *Advanced Persistent Threats (APT)*

Advanced persistent threats (APTs) are groups of skilled attackers that will often conduct extended attack campaigns over months or years against

identified targets. In many cases, APT threat sources are government-sponsored or affiliated groups known as “nation state” attackers, although it is possible that some APTs are unaffiliated. As introduced in Chapter 2, nation states engage in a variety of cyber activities such as espionage and sabotage to support a government agenda, whereas unaffiliated APT groups may behave more similarly to cybercriminals looking for financial gain. APTs have the skills and resources to use any introduction methods from previous attack types and can execute more sophisticated strategies to attempt to gain access to target systems.

In addition to the common types of social engineering attacks previously discussed, APTs often engage in one or more highly focused spear phishing campaigns targeted at individuals across an organization. APTs will often focus on many different individuals with engineering credentials to access a desired target. If any one of these individuals is deceived into entering their account information, this may be all the information the attackers need to establish their initial access.

APTs can also engage insiders within an organization in cyber-attacks or force them to take part in the attack. Attackers can compromise insiders in many ways, including leveraging political allegiances/ philosophies, bribery, extortion, and threats of physical or financial harm against the individual if they do not agree to help. Although these types of social engineering activities require significant resources to execute, the possibility of obtaining an inside source of information and a direct vector to introduce an attack can make this worthwhile for APT groups. The potential for insiders to introduce cybersecurity risk is explored in greater detail in Chapter 5.

Another area where typically only APTs have sufficient sophistication and resources to target is the supply chain. There are numerous places in the supply chain where an attack may occur: at component suppliers, at equipment manufacturers, in transit, at reception, at installation, via patches and upgrades, and at disposal. If an attack can be successfully completed while the item is in the supply chain, then it is difficult to identify the attack has occurred because the documentation and mitigations for prevention or discovery of tampering will have been bypassed, disabled, and/or replaced by valid surrogates. Supply chain attacks are among the most sophisticated

methods for introducing an attack and, in many cases, require support from an insider. The recent SolarWinds attack demonstrated the potential for supply chain attacks to impact many different organizations. By compromising a software supplier whose tools and services are used by many organizations, the APT group responsible had the potential to compromise as many as 18,000 customers, including government agencies and cybersecurity firms [26].

Of the attack types reviewed in this chapter, attacks by APTs have the highest sophistication and motivation. Unlike the non-targeted attacks identified in Section 4.1 and the majority of targeted attacks in Section 4.2, which activate as soon as they are able to, attacks by APT groups are intentionally designed to lay dormant until called into action. This delayed activation allows APT groups to avoid detection until the attackers are ready to execute the attack. Often, the objective of APT attacks is to establish remote “command and control” of the system. The process that APTs follow when looking to achieve command and control of a system is called the Cyber Kill Chain® [2]. The Kill Chain consists of seven steps that must be followed for attackers to successfully gain control. Table 4-2 has been adapted from [2] to show the steps of the cybersecurity kill chain and common methods used.

Table 4-2 Cyber Kill Chain® Steps and Description

Step	Description	Notes
Reconnaissance	Gathering information for an attack (e.g., account information, system information, physical layout information).	The cyber espionage activities discussed in Section 2.1.1 are commonly used for the reconnaissance step.
Weaponization	Developing malware that includes the ability to exploit a known vulnerability with deliverable payload.	APTs design malware to exploit known vulnerabilities in target systems. In some cases, previously unknown or zero-day vulnerabilities have also been exploited by APTs.
Delivery	Delivering malware to the victim.	Delivery methods were introduced by varying methods of sophistication in Sections 4.1, 4.2, and 4.3.
Exploitation	Leveraging vulnerability on victim’s system to execute malicious code.	In the exploitation stage, the malware takes advantage of the vulnerabilities identified in the weaponization stage.
Installation	Installing malware on the victim's systems.	The malware will often automatically download once infected, and in some cases even check for the most recent version.

Table 4-2 continued

Step	Description	Notes
Command and Control	Create remote command channel to allow for manipulation of victim's system.	Once a set of predetermined conditions are met, the malware will establish a remote command channel for the attackers.
Actions on Objectives	With remote control of the system, attackers can accomplish their ultimate goals.	With remote control of the victim's system, the attackers can now modify configurations and setpoints to achieve their objectives.

Once an APT has established command and control of an IACS system, the attacker has the flexibility to modify setpoints and manipulate the physically connected components of the control system to achieve their ultimate objective. Depending on the motivation of the attack, harm can be initiated for any of the risk receptors introduced in Section 3.3. Examples of detailed case studies of attacks designed to target each of these different risk receptors will be further explored in Chapter 6.

4.4 Summary

In this chapter, information was provided on three categories of cybersecurity attacks: non-targeted, targeted, and APTs. For each type of attack, common methods for introduction and types of consequences or impacts on the system were presented. Each of these types of attacks has the potential to damage IACS systems. As shown in Table 4-3 (adapted from *Mitigating Covert Compromises* [50]), the frequency and number of targets for non-targeted attacks is much higher than targeted or APT attacks, but the sophistication in targeted and APT attacks is much higher, making these attacks more likely to be successful when they do occur. When implementing a risk-based approach for cybersecurity, organizations need to develop adequate protection layers against all three categories of threat sources.

Table 4-3 Attack Characteristics by Threat Source Type

Attack Characteristics	Non-Targeted	Targeted	Advanced Persistent Threats
Frequency of Attack	High	Low	Very Low
Number of Targets	High	Low	Very Low
Skill/ Effort Required	Low	High	Very High
Probability of Success	Low	High	Very High

5 Who Could Create a Cyber Risk? Insider vs. Outsider Threats

Experts have identified multiple ways to categorize the sources of threats, types of attacks, and the level of cybersecurity risk with the hope of more accurately modeling and predicting cybersecurity incidents. At the core of this effort is the question “Who could create a cyber risk?” One fundamental method of categorizing the potential sources of cybersecurity risk is to consider if they are an insider (internal) or outsider (external) threat. To better understand the similarities and differences of insider and outsider attacks, we will consider the following information for each type of attack:

- Level of access,
- Motive,
- Common types, and
- Case studies/ examples.

5.1 *Insider Cybersecurity Risk*

An insider cybersecurity risk is created by someone who is permitted logical and/or physical access to the system, whether they are an employee, contractor, or 3rd party (e.g., integrator, service provider). Common roles with access to the industrial control system include:

- Administrators
- Engineers
- Technicians
- Supervisors
- Operators
- Contractors/Vendors
- Electricians

These roles - and any other personnel with access to the control system - are critical elements in maintaining the security and safety of the site. Other roles, such as HR personnel and administrative staff with access to confidential information on the business network, can also lead to potential insider risk. The number of personnel with in-person and remote access is a key measure of the cybersecurity exposure for a site: the greater the number of personnel with access, the greater the exposure and the greater the risk.

Insider cybersecurity risks can be particularly difficult to protect against with traditional cybersecurity measures because the source of the risk is allowed to access the system. In this case, the application of personnel security controls, including background checks and identity verification, as well as improved cybersecurity awareness and training, are critical steps for reducing the likelihood of both insider intentional and unintentional cybersecurity events.

Insider attacks can be further segmented based on whether there is an intent or motive to cause harm and/ or whether a decision to act inappropriately is made. Insider activities can be grouped into three categories based on the answer to these questions, as shown in Table 5-1 adapted from *Insider Threats* [51].

Table 5-1 Sub-Groups of Insider Cyber activities

	Accidental	Negligent	Malicious
Decision to act inappropriately?	No	Yes	Yes
Motive to cause harm?	No	No	Yes

For an insider source of cybersecurity risk to be malicious, an intentional decision to act inappropriately or outside of normal acceptable behavior is made in conjunction with an intent to cause harm. Unintentional sources of insider risk can be classified as accidental or negligent, depending on whether a conscious decision to act inappropriately was made.

5.1.1 Insider Intentional Harm

An intentional insider attack (often referred to as a disgruntled employee in the cybersecurity field) is an act of sabotage in which someone with access to the process control system intentionally damages the integrity of the system. The motives for intentional insider attacks can include a workplace disagreement, failure to achieve a desired promotion, unfavorable

termination, outside influence, or desire for monetary gain. Insider sabotage can take many forms:

- Intentionally modifying setpoints/ configurations,
- Creating new remote access connections for future activities,
- Deleting critical data,
- Stealing intellectual property,
- Attempting to damage company image,
- Attempting to cause physical harm to safety, environment, and business assets.

One such example in the relatively early days of cybersecurity occurred in Maroochy Shire Australia. A wastewater treatment facility was compromised when an employee from Hunter Watertech Pty Ltd, the 3rd party company responsible for the system design and integration, was not selected for a direct position at the Maroochy Shire treatment plant. After his termination, the attacker took advantage of weak physical security at his former office to steal a laptop with the required configuration to connect remotely into the Remote Terminal Units (RTUs) for controlling the network of the treatment system. By manipulating the control system, raw sewage was released to a variety of residential and park areas, causing significant environmental damage. The 3rd party contractor was determined to be liable, and the cleanup cost exceeded half a million dollars [19]. Although this attack resulted in a considerable negative impact, the outcome could have been significantly worse if the former employee had decided to target the safety of the drinking water at the facility.

5.1.2 *Insider Unintentional Harm*

Often overlooked, but equally important, sources of insider cybersecurity risk include unintentional mistakes. A 2018 study by the Ponemon Institute of over 150 companies across 13 industries found that nearly 80% of all insider cybersecurity incidents were unintentional [52]. The most common sources of unintentional cybersecurity incidents were employee or contractor negligence (64%) and credential theft (13%) [52].

Unlike intentional attacks, unintentional harm is not driven by a formal motive. Instead, it is often the result of accidental or negligent behavior. Competency requirements for cybersecurity are critical to reduce the potential

for unintentional harm resulting from both accidents and negligent behavior; they improve awareness of the potential impact on the system and outline correct behavioral practices. The need for competency requirements is particularly important as industrial companies continue to face challenges with workforce development, employee turnover, and finding enough skilled personnel for technical roles.

Common types of insider accidental cybersecurity incidents involve connecting a previously infected USB or device to the control network. A common strategy is to perform USB “drops” - leaving infected USBs in high traffic areas such as the parking lot of an industrial facility. When a curious employee plugs in the USB to see what is on it, the malware can infect the connected device. This pathway can lead to the introduction of general malware not specifically intended to damage control systems as well as the introduction of attacks specifically targeting industrial control systems. Studies of infected malware have shown that malware used in large scale previous attacks such as Stuxnet and WannaCry are still commonly found in today's cybersecurity ecosystem [53].

Another common source of unintentional cybersecurity incidents are mistakes in the configuration of network or control devices. In one case, operators of a nuclear power plant were forced to initiate an emergency shutdown following the failure of two reactor recirculation pumps [54]. The root cause of the failure was identified as excessive traffic, likely resulting from the incorrect configuration of network devices. The excess traffic caused normal transmissions to be disrupted, and the continual storm of data caused the controller connected to the pumps to become “locked up” or non-responsive [54]. The situation was resolved by disconnecting the pump variable frequency drives (VFDs) from the IACS network and installing firewalls to better segment the control network.

Determining whether unintentional insider activities should be considered accidental or negligent can depend on the larger context. For example, connecting an unauthorized USB device to a control network in one organization may be considered an accident if no removable media policies are in place or enforced. In a second organization, with strict policies for handling removable media and consequences for failing to adhere to these

procedures, the use of an unauthorized USB device would be considered negligent. Developing organizational procedures for cybersecurity best practices - sometimes referred to as cyber hygiene - is a necessary step in properly training individuals and reducing the likelihood of an accidental cybersecurity incident. Likewise, consistent enforcement of penalties for failing to adhere to these policies is important to reduce the likelihood of negligence leading to a cybersecurity incident.

5.2 *Outsider Cybersecurity Risk*

An outsider cybersecurity risk is posed by someone who is not permitted logical or physical access to the control system. As introduced in Chapter 2, several possible types of outside cybersecurity risks include:

- Competitors
- Nation states
- Hacktivists
- Criminals
- Rogue wizzes

Although these outsiders are not given access to the system intentionally, they are often able to exploit poor security features and known vulnerabilities in industrial control networks to establish access remotely and execute cybersecurity attacks.

Similar to insider threats, outsider threats can also be segmented based on the intent or motive to cause harm. While the most outsider threats are intentional, it is still possible for outsiders to cause unintentional harm.

5.2.1 *Outsider Intentional Harm*

Most outsider attacks are intentional in nature. The underlying motive behind the attack is often the key determiner in the type of attack executed. Outsiders are primarily driven by one of three broad types of motives:

- Financial (desire to receive financial gain, steal sensitive information, competitive advantage)
- Political (targeted nation state activity, activism)
- Personal (show of skill, grudge/revenge)

Attacks driven by financial gain often deploy ransomware, a type of attack where critical information is encrypted on infected devices. Victims are

instructed to wire payments to the attacker with the hopes of receiving a password key to unlock the information. As mentioned in Chapter 2, WannaCry is a recent example of a ransomware attack that had significant impacts on several industrial control systems compromising over 200,000 devices across 100 countries [35].

Some nation state or APT threats attempt to go beyond financial impact and have attempted to manipulate the physical process to cause equipment damage and safety concerns. Case studies for these types of attacks are described in more detail in Chapter 6.

Personal motives can also drive outsider (as well as insider) attacks, and these attacks may employ a variety of means, depending on the specific objectives. The level of impact of an individual attacker is largely dependent on the skills and resources of the hacker. Although, the number of hackers with detailed knowledge of industrial control systems is still relatively small, several disturbing trends may indicate a future increase. These include the rapid growth of hacking tools (e.g., ransomware kits), which allows even unskilled attackers to deploy sophisticated attacks.

5.2.2 *Outsider Unintentional Harm*

Unintentional outsider cybersecurity incidents can also have the potential to result in downtime and other negative consequences for the control system. The most common types of unintentional harm are from “updates gone bad” or patches that introduce compatibility problems between network components. These issues can often result in system unavailability and unexpected reactions from the control system such as downtime or even loss of control. A rigorous patch management methodology, including testing of patches by the equipment supplier and by individual sites in secure test environments or on lower criticality systems, can help to limit the likelihood of this type of incident. Additional information on patch management activities can be found in Chapter 8.

Mistakes or negligent behavior can also result in unintentional outsider threats or incorrect physical protections (e.g., leaving gates open or doors unlocked). A common mistake is leaving unneeded accounts in place, which can leave the system open to access by outsiders such as unapproved contractors, equipment/ software vendors, or even members of the general

public. Since these outside parties may not have any cybersecurity awareness training or knowledge of the significant potential impacts of connecting to the control system, it is possible for them to unknowingly introduce cybersecurity risk. Although these issues can be mitigated within the site's fence line by applying standard physical security measures, for some remotely located systems such as distant tank farms and pipelines, preventing access to unauthorized personnel can be more challenging. When equipment is located outside of the fence limit, it should be kept in locked cabinets whenever possible. If physical constraints make the use of a locked cabinet difficult, physical port blocking can be implemented as an alternative.

5.3 *Summary*

Examples from many previous cybersecurity attacks demonstrate that both insider and outsider cybersecurity risks have the potential to significantly impact both the continued operations and safety of industrial control systems. To adequately assess and protect against this risk, it is important to follow a consistent methodology for risk assessment that considers all applicable sources of risks and the most effective means against protecting each type. Further detail on conducting cybersecurity risk assessment is included in Chapter 9.

6 Case Histories

In the first 5 chapters of this book, core principles for industrial cybersecurity have been established including the importance of cybersecurity for OT systems, cybersecurity risk, types of cybersecurity activities, threat agents, attack methods, and those who can pose a cybersecurity risk. This chapter shifts the focus to previous cybersecurity events that have impacted operational systems with the potential to negatively impact health and safety. These example incidents give a clearer understanding of the types and impacts of previous cyber-attacks, demonstrate the importance of protecting process control systems from cybersecurity attacks, and include practical guidance on how a similar attack could be prevented for current IACS. For each of the following incidents, the background, threat agent, attack method, and impact will be presented and categorized:

1. Maroochy Shire
2. Stuxnet
3. German Steel Mill
4. Ukrainian Power Grid
5. NotPetya
6. Triton
7. Düsseldorf Hospital Ransomware
8. SolarWinds
9. Florida Water System
10. Colonial Pipeline Ransomware

6.1 *Maroochy Shire*

A total of more than 750,000 gallons of raw sewage was spilled following a series of cyber-attacks on the Maroochy Shire wastewater treatment facility located in Queensland Australia in early 2000 [9]. The most severe incident occurred in March when 264,000 gallons of raw sewage spilled into a tidal canal and the Maroochy River [9], [19]. The attacker was able to remotely stop pumps from running when needed, start the pumps when they were not required, block relevant alarms, trigger nuisance alarms, and trigger a loss of

communication to remote stations [19]. The Queensland Environmental Protection Agency (EPA) described the incident as “causing significant harm to an area enjoyed by young families and other members of the public, marine life died, the creek water turned black, and the stench was unbearable” [19]. The incident cost the city over \$175,000 U.S. dollars in repairs and clean-up activities, and the incident cost Hunter Watertech Pty Ltd. - the system integrator - over \$500,000 U.S. dollars in incident investigation costs, additional security activities, and cleanup efforts [19]. This represented the first known instance of a cybersecurity attack on an industrial control system resulting not only in an impact on the computer itself but also a consequence to the physical process under control. Today, the Maroochy Shire spill remains one of the clearest examples of a cybersecurity attack having an adverse impact on the environment.

Background: Hunter Watertech Pty Ltd. had been awarded a project to install Remote Terminal Units (RTUs) at 142 pump stations. RTUs are used to interface between physical objects and SCADA systems. SCADA systems are a type of IACS that are commonly used in physically dispersed applications such as water systems and pipelines. In this instance, the RTUs were intended to allow for remote monitoring and control of a number of physically spread-out pump stations. Figure 6-1 shows the simplified network architecture for the Maroochy Shire SCADA System.

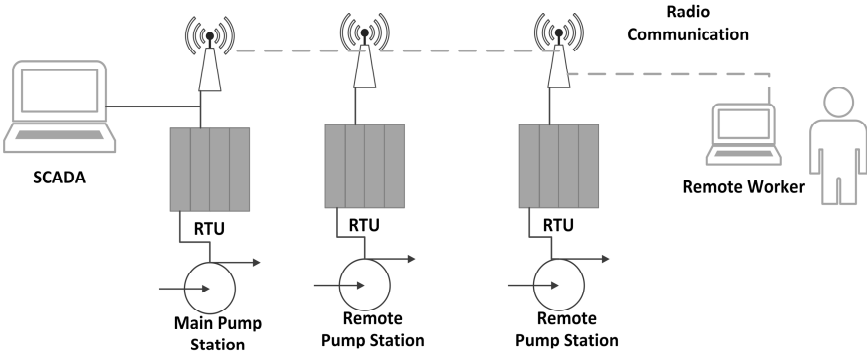


Figure 6-1 Simplified Maroochy Shire SCADA System

Source: MIT Cybersafety Analysis of Maroochy Shire Spill [19]

The RTUs allowed for centralized control of the remote pump stations as well as the ability for users to connect remotely in the field. Vitek Boden was hired as the project manager by the integrator (Hunter Watertech Pty Ltd.) to serve as the site supervisor. However, at the end of 1999, Boden got into a serious disagreement with Hunter Watertech Pty Ltd. and resigned. Subsequently, Boden tried twice, unsuccessfully, to secure direct employment with the Maroochy Shire Council.

Threat Agent: The threat agent in this attack was clearly a **disgruntled employee**. Upon investigation, it was determined that Boden was responsible for the attacks after private investigators monitoring the Maroochy Shire Council site identified Boden's vehicle exiting the area around the pumping station immediately following one of the attacks. Police were alerted and pulled over Boden's car. The suspect was in possession of the same type of RTU used for the pumping stations, a two-way radio, and a laptop containing proprietary control system software. The RTU and radio had previously been stolen from Hunter Watertech Pty Ltd. This is an example of an internal intentional attack; Boden leveraged the equipment he had stolen as well as his detailed knowledge of the system and his knowledge of the Hunter Watertech Pty Ltd. facility. The motive in this case was most likely revenge due to the degradation of his relationship with his previous employer and his subsequent inability to gain direct employment from the Maroochy Shire Council.

Attack Method: The incident represented a **targeted attack**. Boden used the stolen equipment to remotely connect to the RTUs and modify setpoints, leading to repeat malfunctions of the equipment. Maroochy Shire first suspected foul play in the malfunctions after resetting the device configurations did not correct the issues. At times, the control system operators were unable to correct malfunctions as they occurred because the radio network traffic was clogged with Boden's communications. This resulted in a similar effect to a **DoS attack** because authenticated users were unable to connect to the system.

Impact: There was significant environmental damage, and financial damage was incurred by Hunter Watertech Pty Ltd. as well as by the city of Maroochy Shire. The impact could have been significantly worse if Boden had targeted the drinking water system and triggered consumer safety concerns.

The Chief Executive for Hunter Watertech Pty Ltd. observed: “With unlimited command of 300 control nodes for both sewage and drinking water, his attacks were actually quite restrained. He could have done anything he liked to the fresh water. He faced virtually no obstacles to breaking in” [19].

Key Points

Physical Consequences – Maroochy Shire was the first confirmed cybersecurity attack on an OT system. This event demonstrated the potential for cybersecurity incidents to lead to environmental consequences. Had the attacker targeted the drinking water systems, the results could have been much more severe.

Insider Attack – The ease with which a former insider was able to complete the attack demonstrated the potential for disgruntled employees and contractors to cause significant harm. Additionally, the incident highlighted the poor physical security of the integrator and the lack of security barriers for the SCADA system.

Preventing the Attack – The attack on the Maroochy Shire water treatment facility could have been prevented by improving security barriers for personnel security, physical security, and system hardening (as explained in Section 8.5). From a personnel and physical security perspective, steps could have been taken to immediately remove Boden’s credentials and ensure that he did not have access to steal the proprietary software and hardware necessary to connect remotely to the SCADA system. Additionally, requiring user authentication for remote access could have provided another barrier. For current systems, best practices such as multi-factor authentication for remote access and requiring onsite approval for remote access should also be considered.

6.2 Stuxnet

The attack campaign targeting the Natanz Uranium Enrichment Facility in Iran from 2007 to 2010 was the first example of malware designed specifically to target IACS [9]. The Stuxnet malware, developed to compromise Siemens PCS7 controllers, led to significant disruptions in facility operations from 2007 to 2010 [9]. Multiple versions of the malware caused physical damage to the plant over this period by disabling protective functions, manipulating the position of valves at the inlet and outlet of the centrifuges, and changing the speed at which the centrifuges rotated. The end result was costly damage to over 1,000 centrifuges (possibly as many as 2,000 centrifuges [9]) and reduced production capacity throughout the attack duration.

Background: The potential for cybersecurity attacks to cause physical damage to IACS systems was first demonstrated in an experimental setting with the Aurora Generator Test in 2007. For this test, a few lines of code were intentionally modified by research personnel to determine the impact on a generator system. Ultimately, the 27-ton diesel generator was destroyed in roughly 3 minutes [55]. Although the potential for physical damage may have been demonstrated in experimental settings, nothing like Stuxnet had ever been seen before in an operational system.

Threat Agent: The level of sophistication involved in the Stuxnet attack made it clear that it was the work of a *nation state*. The attack development was likely started as early as 2005 and was conducted and maintained over multiple years. The attack has been widely attributed to the United States and Israel, with some security experts suggesting that other allied nations may have been involved in the effort as well [9].

Attack Method: The Stuxnet attack was another example of a *targeted attack*. Extensive reconnaissance was carried out to prepare for the attack, including monitoring the sale and global movement of parts that ultimately were used in the facility. This tracking enabled the attackers to identify the versions of the Siemens logic controllers used at the facility so that they could design the appropriate code [9].

The OT network for the Natanz facility was air gapped (completely separated) from internet-connected IT and corporate systems, so the attackers needed to find a way to cross this gap. Universal Serial Busses (USBs)

or flash drives are commonly used at industrial sites to move information between the IACS and external networks, and the attackers took advantage of this technology to cross the air gap. It is believed that the virus was introduced from a USB flash drive used by an insider working with the Dutch intelligence agency [56]. Once the attack was first introduced into the network, it spread rapidly and was unintentionally transferred between different computers on the Natanz IACS network via USB flash drives on many occasions.

The Stuxnet virus took advantage of at least four **zero-day vulnerabilities** - vulnerabilities that are not known by the software/ system vendor or the security community (such that no patches for the vulnerability are available or under development). These types of vulnerabilities are rare, often requiring significant research and effort to find, and are particularly difficult to protect against because no patches or fixes are available.

The vulnerabilities allowed Stuxnet to spread more easily throughout the system and gain administrative privilege, and allowed for changes to be made to control setpoints. Once installed, Stuxnet automatically established communication between isolated PCs and internet-connected PCs on the Natanz network to access a central command server and download the latest version of itself. The virus was designed to automatically trigger a predetermined set of actions and did not require manual intervention to damage the centrifuges.

Impact: The Stuxnet virus was designed with a number of key functionalities to avoid detection and ensure that the disruptive impact continued for as long as possible. The virus was designed to impact only a portion of the centrifuges at one time following a randomized selection process. Before the control valves were manipulated or other settings were changed, healthy process variables were recorded and then played back to the operators during the time that the disruption was occurring. This is known as a **man-in-the-middle attack**, as previously described in Chapter 4. Additionally, the attack was designed to stop after 90 minutes or after a set pressure was reached in the affected centrifuge. This step was taken to prevent catastrophic damage that may have revealed the presence of the virus and prevented the damage that subsequently occurred to a larger number of centrifuges over time.

Careful planning led to the physical degradation of as many as 2,000 centrifuges and a significant disruption and of the facility's enrichment capabilities over a 2-year period [9]. The attack was successful in that it caused significant financial consequences and delays in the Iranian nuclear program. However, had the attackers chosen to cause more significant damage to the centrifuges, they would have faced virtually no obstacles in triggering a safety incident. Not only was the control system compromised, but the operators did not have correct visual representations of the process conditions and the protective relays for the centrifuges had also been compromised.

Key Points

The First, but not the Last – Stuxnet was the world's first "digital weapon," a string of code developed with the intention of causing physical damage to industrial systems. It was the first case of malware being designed specifically to target IACS, but it was not the last. Stuxnet served as a proof of concept for the potential impact that cybersecurity attacks could have on IACS, and with the source code readily available, it provided a blueprint for future IACS-targeted malware.

Air gaps are not infallible – The Stuxnet attack also demonstrated how skilled attackers can circumvent "air gaps," or total isolation between OT and internet-connected systems. Using removable media such as USB flash drives and potentially a compromised insider, the attackers were able to install malware onto an isolated system.

Wakeup Call – Stuxnet was the first major cybersecurity incident affecting IACS. It provided a major wakeup call to system owners and operators and catalyzed a growing focus on cybersecurity for OT systems. The Stuxnet cyber-attack was a major factor in the development of international standards and best practices for security IACS systems.

Preventing the Attack – Although it is difficult to prevent attacks that exploit zero-day vulnerabilities, the following steps could have been taken to limit the likelihood of Stuxnet being introduced:

- Formal policies for USB flash drive management could have limited the opportunities to spread the virus within the network.
- Background checks for employees could have indicated that an insider may have had ties to a foreign intelligence agency.
- Application whitelisting could have helped to limit the ability of malware (even malware that exploits unknown vulnerabilities) to run on a system by restricting applications to only a pre-approved list.

Improved network monitoring techniques could have indicated that an ongoing issue was occurring reducing the amount of time that the virus was active on the network.

6.3 German Steel Mill

A cyber-attack on an unnamed steel mill in Germany in 2014 resulted in a control system failure. Due to either a failure of individual control components or the entire system, the site was unable to safely shut down a blast furnace. The outcome of the incident was described by authorities as “massive damage to the plant” [57]. Fortunately, no one was injured during the incident, but similar safety incidents at other blast furnace sites have resulted in severe injuries [58] and fatalities [59]. The cyber-attack on the German steel mill is an important cybersecurity incident because it represented just the second confirmed example of a cyber-attack leading to physical impact as a result of a compromised IACS.

Background: Little information has been released about the identity of the steel mill targeted in the attack. A number of steel mills in Germany, operated by 15 different companies, were responsible for producing over 40 Million U.S. tons of crude steel in 2014 [60]. The majority of the crude steel was produced by integrated steel mills, the same type of mill targeted in the attack [57]. Integrated steel mills are comprised of a blast furnace, steelwork, and rolling mills.

Threat Agent: A *targeted attack* was most likely carried out by an *advanced persistent threat* (group of skilled attackers) based on the high-level of skill demonstrated in the attack and the objective of triggering physical damage. Per the Federal Office for Information Security in Germany “The technical capabilities of the attackers are highly advanced...The know-how of the attackers was not only very pronounced in the field of classical IT security, but also extended to detailed expertise on the industrial controls and product processes used” [57].

Attack Method: The initial introduction of the attack was completed using *spear phishing* (targeted malicious emails) to gain access to the mill’s IT network. Once the attackers were established on the IT network, they worked their way onto the OT network and established the ability to remotely modify components of the mill’s control system [57].

Impact: After access to the control system was established, the attackers manipulated the configuration or setpoints, resulting in the failure of individual control components - and potentially of the entire system. As a

result of this degree of system compromise, the equipment was in an “undefined state” in the control system and local staff was unable to safely shut down the blast furnace. Ultimately, the attack resulted in “massive” physical damage at the site, but fortunately no personnel were in the surrounding area of the furnace when the damage occurred [57].

Key Points

Physical Consequence – The attack on the German steel mill was just the second cyber-attack to result in equipment damage, but it showed what can happen when attackers are able to successfully take over process control and protection systems while preventing the local staff from operating or shutting down the system safely. Fortunately, no one was injured in the incident; however, as previous incidents with blast furnaces have shown, the event had the potential to trigger a serious safety consequence as well.

Exploiting Connectivity – This attack showed how attackers can often transition from the IT network to the IACS network even if a firewall is in place. Compromising user accounts through phishing is an easy means of gaining initial access. Once they have gained access to the IT network, attackers can perform reconnaissance until they are able to access a remote account for the IACS or determine another means to compromise the system.

Preventing the Attack – The initial compromise of the steel mill occurred as the result of a spear phishing campaign. The most effective controls for preventing this type of attack are interactive cybersecurity hygiene training on phishing activities and email-filtering solutions to reduce the number of malicious emails received by personnel. (Of these steps, improving the human element through training tends to be the most critical.) The attack also required movement from the IT network to the OT network; robust network segmentation between these networks such as a demilitarized zone (see Chapter 8 for more details) could have reduced the likelihood of attackers gaining access to the OT network. Lastly, it appears as though a control system failure led to the inability to safely shut down the blast furnace; had an independent safety system also been a part of the IACS, this could have potentially brought the system to a safe state even after the cybersecurity intrusion.

6.4 *Ukrainian Power Grid*

Two attacks on the Ukrainian power grid in 2015 [31] and 2016 [21] represent the only confirmed cases of cyber-related power blackouts to date. Both attacks demonstrated the ability of attackers to disrupt critical infrastructure and provided important wakeup calls to those responsible for the operation of critical infrastructure around the globe. In 2015, attackers gained remote access to the utility network and began to manually switch off power to electrical substations. They were also able to overwrite firmware for essential network components, further exacerbating the damage [31]. The strategy employed in the 2016 attack was different. Once the CrashOverride malware was introduced to the system, the code automatically triggered at a specified time and did not require further manual intervention [21]. The reduced manual effort in triggering the blackout introduced the potential for the same attacker to target many different sites at the same time. In both attacks, hundreds of thousands of Ukrainian residents were left without power for one to six hours. Although the results of the attacks on the Ukrainian power grid were not catastrophic, similar techniques have the potential to cause cascading and more widespread blackouts, and the learnings from this attack helped to shape the methods for protecting power grids and critical infrastructure.

6.4.1 *First Ukrainian Power Grid Attack*

The first Ukrainian power grid attack occurred in 2015.

Background: The country of Ukraine has 24 regions, further divided into provinces. A separate company is responsible for power distribution for each region. The 2015 attack impacted three of these companies, including the one responsible for supplying the Ivano-Frankivsk region in Western Ukraine [20].

Threat Agent: The first attack on the Ukrainian power grid required significant resources, skill, and the knowledge of both IT and OT systems. The level of sophistication in the attack suggests a **targeted nation state attack**. Forensic analysis of the attack identified clear differences during the different phases of the attack, opening the possibility of separate groups working together (e.g., collaboration by both **cyber-criminals** and a nation state) [20].

Ukraine quickly identified Russia as the culprit for the attack, and although it is difficult to definitively attribute the attack, many security professionals consider Russia to be the most plausible source [20]. Political tensions between Ukraine and Russia rose after the annexation of Crimea in 2014, and a pro-Ukrainian activist had previously physically attacked a substation, shutting off power to 2 million Crimean residents. It is possible that this prior attack on an electrical substation may have triggered or accelerated the timeline of the 2015 Ukrainian cyber-attack [20]. Later analysis of the attack led to the attribution to the **APT** group Sandworm, known to have Russian ties [21].

Attack Method: The initial intrusion of the network was achieved through a **spear phishing** campaign targeting IT staff and system administrators. The phishing emails contained a malicious Microsoft Word document. When the attachment was opened by workers, a popup asked the user to enable macros for the document. If the workers agreed to enable the macros, the BlackEnergy3 malware was downloaded onto the machine and created a back door for the attackers [20]. However, the first stage of the attack only led to the compromise of the corporate network, which was segmented by firewall from the IACS network for the power grid.

Between the spring and December of 2015, the attackers conducted widespread reconnaissance, collecting information on the network structure and user credentials [20]. Some of these credentials pertained to remote access accounts that allowed operators to access the OT network remotely through a Virtual Private Networks (VPNs). Although VPNs do require authentication and provide confidentiality, once a user has been authenticated, no other security measures are in place. With this account information, the attackers were able to remotely compromise the IACS system and prepare for the attack [20].

Once the attackers created a foothold in the IACS network, they took a number of steps before initiating the attack:

- Disabling the control center's uninterruptible power supply (UPS) to ensure that, when power was lost, the operators would lose power as well.
- Overwriting the firmware on serial-to-Ethernet converters used to translate commands from the IACS system to substations. Once power was restored, this step would prevent operators from remotely controlling to the affected substations and force them to manually operate the breakers.

Impact: With these advance preparations, the attackers began a coordinated series of manual actions:

- Disabling the reconfigured UPS system
- Launching a telephone **DoS attack** against the customer call center for the power companies
- Manually opening circuit breakers to shut-off power
- Launching the **malware** program KillDisk to delete files from operating systems, causing them to crash and be unable to reboot.

The resulting power outage affected roughly 230,000 residents for one to six hours. Although the power outage was not long, for more than two months after the attack, operators were still forced to control the breakers manually because of the overwritten firmware.

Key Points

Blackout – The 2015 Ukraine power grid attack was the first confirmed blackout caused by a cybersecurity incident. It highlighted the vulnerabilities of power grids and other critical infrastructure systems and demonstrated how cybersecurity attacks could disrupt the general public. The targeted attack also demonstrated the potential for political motivations to raise the target attractiveness of a site based on its location.

Preventing the Attack – The initial compromise of the power grid occurred as the result of a spear phishing campaign. The most effective controls for preventing this type of attack from resulting in compromise are interactive cybersecurity hygiene training on phishing activities and email-filtering solutions to reduce the number of malicious emails received by personnel. (Of these steps, improving the human element through training tends to be the most critical). The attack also required movement from the IT network to the OT network. There was a single firewall in place between the networks, but a dual-firewall demilitarized zone might have provided improved security (see Chapter 8 for more details). Additionally, the attackers connected via VPN to the OT network; requiring multi-factor authentication for all VPN connections could have provided another means to prevent the attack. Lastly, improved network monitoring could have identified a potential network intrusion prior to the blackout being triggered.

6.4.2 Second Ukrainian Power Grid Attack

The second Ukrainian power grid attack occurred in 2016.

Background: Almost exactly one year after the original attack on the Ukrainian power grid, a second attack was triggered, leading to the second confirmed cyber-related blackout [21].

Threat Agent: Security researchers believe it likely that the same group was responsible for both the first and second attacks on the Ukrainian power grid. They have most commonly attributed the attack to Sandworm [21], believed to be a Russian **nation state** hacking group. The Ukrainian president Petro Poroshenko spoke after the second blackout, stating that the attacks

were conducted with the “direct or indirect involvement of secret services of Russia” [21].

Attack Method: The strategy for the second attack on the Ukrainian power grid was different from the first attack in that it triggered automatically. This has been described as a “**logic bomb**” functionality because the attack was programmed to occur at a predefined time without any further input required from the hackers.

The **malware** used in the second attack, commonly known as “CrashOverride” or “Industroyer,” was the second case of malware being designed specifically for IACS systems. The malware was identified to have four payload components that could be modified based on the type of system being targeted. The version of the malware used to target the power grid was designed with functionality to communicate directly with switches and circuit breakers at electric distribution substations and other IACS devices [61]. The wiper component and one of the payload components were tailored for use against commonly used equipment in the Ukrainian power grid, including certain industrial power control products by ABB and the Siemens SIPROTECT devices used in electrical substations and other related fields of application [61].

The automation of the second power grid attack was significant in that it greatly improved the scalability of the attack, allowing hackers to trigger more blackouts quicker and with less preparation. “Crash Override” was only the second identified malware specifically designed to disrupt IACS systems, Stuxnet being the first.

Impact: The blackout triggered in 2016 only lasted for about one hour and impacted around 20% of the city of Kiev. Although the impact of the attack was much less severe than it could have been, the automation and modularity of “CrashOverride” introduced the very real potential for multiple blackouts to be triggered simultaneously and result in a much longer lasting outage. It is estimated that around 20 hackers were needed to conduct the 2015 attack; however, with the improved scalability demonstrated in the 2016 attack, experts estimate that “those 20 people could target ten or fifteen sites or even more, depending on time” [21].

Another disturbing possibility identified was that “CrashOverride” could potentially have been used to cause physical damage to power equipment. The SIPROTECT digital relay is used to gauge the charge of grid components and can open circuit breakers automatically to prevent thermal overload. Pairing the functionality to disable the protective relay with commands to overload the charge could have led to overheating and physical damage to transformers and other components [61].

The worst-case scenario for the “CrashOverride” malware could well have been to pair the automated logic bomb capability for a more widespread attack with the commands to trigger physical damage at the substation. If deployed correctly, this pairing could have resulted in significant cascading blackouts, which could have affected multiple regions and made it much harder to recover from the upset [21].

In response to the growing cybersecurity threat to power grids, some countries have made the decision to implement “retro” technologies to decrease reliance on critical systems [62]. The shift is the reverse of the general trend of IACS systems towards greater connectivity and digitalization. Although moving towards more manual operation may help to limit the cybersecurity exposure, manual operations are not immune to cybersecurity attack. As the Stuxnet attack showed, it is possible to overcome a traditional air gap through removable media and physical access.

Key Points

IACS-Specific Malware – The “CrashOverride” attack was only the second known case of malware purpose built to disrupt IACS. (Stuxnet was the first.) The increased scalability has increased the potential that a similar size group could cause significantly more outages, triggering a larger and longer blackout.

Disabling Protective Relays – The ability of the “CrashOverride” malware to communicate directly with IACS devices, including protective relays, introduces the possibility of an attack resulting in physical damage by disabling protective measures and manipulating controls to overheat the equipment. The potential for long-lasting physical damage can result from the common cause failure of multiple systems during a cybersecurity attack.

Preventing the Attack – It is believed that a spear phishing campaign was used to gain initial access for both the first and second power grid attacks. The previously mentioned steps of interactive cybersecurity hygiene training on phishing activities and email-filtering solutions to reduce the number of malicious emails received by personnel could have helped in this case as well. Organizations that are determined to have a higher attractiveness to targets based on previous incidents and threat agent trends (such as critical infrastructure in the Ukraine) may want to consider more detailed training on spear phishing activities, as they may be more likely to be targeted by sophisticated threats. In addition to preventing the initial intrusion, improved network monitoring could have identified the malware on the system prior to the “logic bomb” functionality being triggered. Application whitelisting could also have been an effective measure at preventing the malware from running on the IACS.

6.5 NotPetya

The NotPetya malware was designed to delete critical components of a system's memory, permanently preventing affected workstations and servers from being restored. The 2017 attack first started in Ukraine, where over 300 companies were affected and an estimated 10% of all computers in the country were wiped. What started as a compromise of one company's accounting software quickly spread into one of the widest reaching cybersecurity incidents of all time. Within six hours of the release of the malware, an estimated 2,000 companies were infected [63], including many organizations with OT systems. The ultimate damage caused around the globe is estimated at \$10 Billion U.S. dollars [64].

Background: The company first targeted in the NotPetya attack was the Linkos Group, a small Ukrainian software company. The company's primary product, named "M.E.Doc," is a tax preparation software and is used by nearly every business in the Ukraine [64]. Hackers compromised the "M.E.Doc" update server and created a backdoor (a covert connection that allows authorized or unauthorized users to bypass existing security measures and establish a high level of access to a computer system or network). They used the backdoor to release NotPetya directly to thousands of computers globally that had the program installed.

Threat Agent: Similar to the other recent cybersecurity attacks on Ukraine, definitive proof confirming the attackers is difficult to find. However, many security professionals have identified the most likely culprit as the APT Sandworm, again linking the activity to the political tensions between Russia and Ukraine. U.S. Intelligence agencies have also confirmed Russia's involvement in the incident [64].

Attack Method: The strategy for compromising multiple victims through a common compromised website, also known as a **watering hole or drive-by attack**, was first introduced in Chapter 4. Based on the prevalent use of the M.E.Doc software throughout the Ukraine, it is widely believed that the primary targets of the NotPetya attack were companies in the Ukraine. However, the ultimate reach of the attack went much further.

The NotPetya attack was able to spread so rapidly because it effectively combined two separate hacking tools (EternalBlue and Mimikatz). EternalBlue

was an exploit (code that takes advantage of a vulnerability) originally developed by the U.S. National Security Agency that was leaked in 2017 and quickly used by many different hacking groups [63]. The exploit allowed the malware to self-replicate on unpatched Windows systems. If there was even one unpatched workstation on a network, it was possible for the worm to gain an initial foothold and then use another program called Mimikatz to spread. Mimikatz is a tool that can be used to search system memory for passwords, greatly increasing the ease of lateral movement of malware within a network [65].

Impact: The initial objective was to execute a **targeted attack** on Ukraine, and the damage from this attack was significant. Over 300 Ukrainian companies were affected, and a number of them were associated with critical financial, governmental, and social functions. These included six power companies, four hospitals, two airports, transport systems, government agencies, and over 22 banks [64]. Ultimately, 10% of all computers in the Ukraine were rendered inoperable.

Although the attack's target was the Ukraine, the impact radius was much wider. Tom Bossert, a security adviser for the Department of Homeland Security at the time of the attack, described it as: "the equivalent of using a nuclear bomb to achieve a small tactical victory" [64]. The worm was not designed with any measures in place to limit the spread or damage to selected systems, and the result was more than \$10 billion U.S. dollars in total damages. For companies outside of the Ukraine, NotPetya was an example of a **non-targeted attack** with the potential to cause significant damage. A number of companies with OT systems were hit very severely by the worm, as shown in Table 6-1 [64].

Table 6-1 Major Victims of NotPetya Attack

Company	Industry	Estimated Cost
Merck	Pharmaceutical	\$870 Million
FedEx / TNT express	Delivery	\$400 Million
Saint Gobain	Construction	\$384 Million
Maersk	Shipping	\$300 Million
Mondelez (Nabisco, Cadbury)	Food & Beverage	\$188 Million
Reckitt Benckiser (Lysol)	Consumer Goods	\$129 Million
Others	Multiple Industries	Approximately \$8 Billion
Total		\$10 Billion

The cybersecurity incident cost for OT companies was not just limited to the replacement cost for wiped network equipment; it also extended to the lost production during the incident and the resulting disruption to the supply chain. For the Maersk shipping company, the NotPetya worm left multiple shipping terminals inoperable, resulting in hundreds of trucks lined up outside of the terminal gates with nowhere to unload their cargo [64].

Although the financial consequences associated with unexpected downtime is significant, the loss of critical systems such as basic control system networks, protective systems for chemical manufacturers, and hospital patient health systems could have resulted in safety consequences as well.

Key Points

Collateral Damage – Although the original target of the NotPetya attack was the Ukraine, companies worldwide were severely impacted. The attack on the Linkos Group, for example, was clearly the result of a skilled targeted attack. However, for many of the companies hardest hit, the incident was not the result of a targeted attack. Instead, the malware spread because of poor segmentation between networks.

Major Cost – The NotPetya attack also demonstrated how significant cybersecurity attacks can be from a financial perspective. At more than \$10 Billion U.S. dollars, the NotPetya attack was likely the most damaging cybersecurity incident of all time. Several companies that had IACS systems vulnerable to potential compromise experienced losses of over \$100 million U.S. dollars resulting from network equipment replacement and the high financial cost of unexpected downtime for operational systems.

Preventing the Targeted Attack – The method for the initial compromise of the Linkos group update server is not publicly known, but the application of best practices for designing a secure system defined in Chapter 8 can help to limit the likelihood of a targeted attack successfully gaining access. Network segmentation using well-managed firewalls, a robust patch management strategy, implementing system hardening, and developing a network monitoring and response strategy could have helped make it more difficult for the threat agent to gain access, or helped to identify that the compromise has occurred.

Key Points Continued

Preventing the Non-Targeted Attack – For the companies not initially targeted in the attack, patch management and effective network segmentation are the most important controls. The EternalBlue exploit was only effective on unpatched Windows systems; had companies updated all servers and workstations on their network to the current patch-level (available prior to the incident), they could have been fully protected from the spread of NotPetya. Additionally, providing segmentation between physically separate business networks, as well as better segmentation between business and OT networks, would have limited the NotPetya infection to a smaller portion of the network, significantly reducing the financial impact of the compromise.

6.6 Triton

The Triton cyber-attack targeted a petrochemical facility in Saudi Arabia in 2017 and triggered a process shutdown - but the attack had a much more sinister goal. The malware that was introduced was specifically designed to target the site's Safety Instrumented System (SIS), which provided critical protection against hazard scenarios such as loss of containment of flammable and toxic materials. The attackers successfully compromised the site's Basic Process Control System (BPCS) and modified the configuration on one of the unit's SIS controllers; however, they unintentionally triggered a shutdown because of the redundant SIS configuration [66]. Had the attackers accounted for the redundant SIS configuration, they may have been successful in triggering a cybersecurity hazard scenario resulting in significant harm to personnel.

Background: Petrochemicals have become a core part of Saudi Arabia's plans for economic growth and diversification. Saudi Arabia has looked to reduce its overall crude oil output in an effort to support global oil prices (avoid a surplus of crude oil supply). In order to maintain economic growth with less crude oil output, Saudi Arabia has worked to increase the production of higher value petrochemicals. In this way, the cyber-attack seemed to be focused on sending a clear political message and complicating plans for private

investment. Amy Myers Jaffe, a Middle East expert for the Council on Foreign Relations said: “Not only [is] it an attack on the private sector, which is being touted to help promote growth in the Saudi economy, but it is also focused on the petrochemical sector, which is a core part of the Saudi economy” [10].

Threat Agent: The attack required significant skill and sophistication to complete and, because there was no clear profit motive, many experts believe that a *nation state* was responsible for the attack [66] [10]. Each piece of the code used in the attack appears to have been custom built, requiring significant time and resources [10].

The only countries believed to have the technical sophistication to execute such an attack are the United States, Israel, China, Russia, and Iran [10]. In addition to assessing capability, it is important to consider motive. Both the United States and Israel have taken steps to further cooperate with Saudi Arabia to limit Iran’s influence in the region, whereas China and Russia have begun to make more energy deals with Saudi Arabia in recent years [10]. Iran has been identified by many experts to be the most likely culprit based on the growing tensions between Iran and Saudi Arabia [10]; however, others maintain that Russia may have been responsible, although the motive remains unclear [67].

Attack Method: The intrusion originated in the corporate network, where the initial compromise potentially occurred as early as 2014 [67]. Although the exact method of the initial intrusion is not known, it is believed that a phishing campaign may have been the most likely source. The attackers then spent time transitioning to the site’s IACS network, where they successfully compromised an engineering workstation that was connected to the site’s Safety Instrumented System (SIS) [67].

It is believed that the connection between the engineering workstation and safety controllers was used to complete reconnaissance and determine the make and model of the controller hardware and the firmware version [67]. It is believed that the hackers then purchased the same version of the Schneider Electric Triconex™ safety system to better understand how it worked, explore it for vulnerabilities, and design and test the malware [10], [67].

A **zero-day vulnerability** found in the Triconex firmware allowed attackers to inject code, making it possible for them to access the controllers remotely whenever desired. The Triconex controllers had a physical key-switch for changing between “run” and “program” modes, and it is likely that either the controller was accidentally left in “program” mode or that the zero-day vulnerability allowed the attackers to bypass this functionality [10], [67].

Impact: Attackers were able to compromise both the BPCS and SIS controllers at the facility. Researchers have determined that the intent of the attack was most likely more severe than triggering a process shutdown, such as triggering a deadly explosion or release of toxic gas, because the attackers did not attempt to shut down the safety controllers. Instead, they attempted to insert functioning control logic that would have allowed attackers to modify the SIS controllers [66].

The attack resulted in an inadvertent shutdown of plant operations as the attackers attempted to trigger their intended consequence. The shutdown occurred because the three SIS controllers were not modified at the same time, causing a failed validation check between the redundant processing units [66]. As shown in Figure 6-2, the attackers did successfully compromise the BPCS system and one SIS controller in the pair. Had the attackers modified all SIS controllers at the same time, it is possible that they could have successfully achieved their ultimate objective.

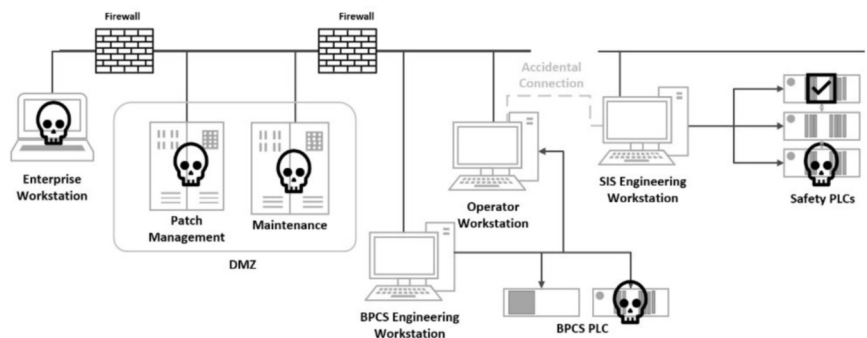


Figure 6-2 Petrochemical Site Simplified Network Architecture

Although the attack was not successful, it served as a chilling reminder that cybersecurity attacks have the potential to trigger common cause failures of both control functions and protective safety layers. This can lead to significant process hazards such as explosions or toxic releases, which can pose a serious threat to personnel safety.

Key Points

Targeting Safety – The attack on the Saudi petrochemical facility was the first confirmed attack that targeted SIS. (Previous attacks had compromised protective measures in the control system but not separate Safety Instrumented Systems.) Additionally, it was the first attack to specifically attempt to trigger a safety consequence. The incident provides a roadmap to future attackers looking to compromise safety and control systems.

Overcoming a Physical “Lock and Key” – The attack also demonstrated how no countermeasures are perfect; given enough time and resources, skilled attackers have the potential to compromise any system. By leveraging a zero-day vulnerability and an accidental connection, the attackers were able to remotely modify the safety controller configuration.

Preventing the Attack – Even after the initial compromise occurred, there were a number of steps that could have limited the effectiveness of the Triton attack. First, maintaining the network segmentation as originally intended to provide isolation between the safety and control systems would have limited the ability of the attackers to make modifications to the safety controller. Additionally, for the physical switch of the Triconex controller, ensuring that the switch was always kept in the run position could have potentially prevented the configuration being updated for the safety controller. Application whitelisting is one effective method for preventing even malware with zero-day vulnerabilities from running on the system. Additionally, network monitoring and response capabilities could have allowed the facility to identify the attack after it gained an initial foothold or after it compromised the control system - but prior to when the safety system was targeted.

6.7 *Düsseldorf Hospital Ransomware*

A ransomware infection at the Düsseldorf University Hospital disrupted emergency care at the facility in September 2020. As a result of the ransomware, patients had to be diverted to nearby hospitals for treatment. While in transit, one patient died. Had it been determined that the ransomware at the hospital was a contributing cause of this, it could have been the first fatality directly attributed to a cybersecurity incident [68].

Background: Hospitals and health systems have been shown to be vulnerable to serious cybersecurity threats, such as the significant financial impact on the UK's National Health Service as a result of the 2017 WannaCry ransomware incident [69]. Additionally, in October of 2020 as the number of coronavirus cases were rising, a wave of ransomware attacks crippled a number of American hospitals [70]. Although the objective of these ransomware attacks was to make money, the attacks also stopped the affected systems from working. For hospital systems, the potential for adverse patient health outcomes is a very real possibility. Similar attacks had already resulted in several near misses across Europe [68].

Threat Agent: Authorities have identified *cyber-criminals* as the most likely type of attacker for the *ransomware* incident [68]. Unlike other incidents with potential safety consequences, ransomware is typically perpetrated for monetary gain, making it a valuable method for cyber-criminal groups (as introduced in Chapters 2 and 4).

Attack Method: The initial breach was achieved by taking advantage of a **widely known vulnerability** in Citrix VPN software. The vulnerability allows attackers to gain access to internal networks through the VPN and establish remote connections [68]. Patches for the vulnerability had been made available. However, availability/ uptime requirements for hospitals are high, and it is not uncommon for patches to be delayed for extended periods of time. Once the vulnerability was exploited and the connection to the network was established, the hackers deployed ransomware, crippling critical systems.

Impact: The ransomware attack led to the inoperability of essential medical services at Düsseldorf University Hospital. As a result, a female patient had to be transferred 19 miles for treatment at a nearby hospital. The patient

died in transit, and police launched a negligent homicide investigation into the hackers.

After a months-long investigation it was determined that the patient's "medical condition was the sole cause of the death, and this is entirely independent from the cyber-attack" [70]. Although the loss of life in this case was the result of the medical condition, investigators noted that it seems like only a matter of time until a cybersecurity incident results in such a tragedy [70].

During the incident, the hackers provided the decryption key to the hospital prior to demanding any ransom payment [68]. This has led many to believe that the hospital was likely not the intended target of the attack and that the hospital may have been mistakenly compromised instead of another university. This development has twofold importance. First, it highlights the potential for hackers to trigger unintended and severe consequences in systems other than the intended target. Second, it demonstrates that poor perimeter defenses can lead to OT systems being compromised even if they are not specifically targeted in an attack.

Key Points

Possible Safety Consequences – Although the most likely motive for the Ransomware attack was financial gain, the loss of availability of critical health systems had the potential to result in safety concerns as well. Even though the cause of the fatality was determined to be solely the medical condition and not the cyber incident, there have been multiple near misses as a result of cybersecurity incidents at hospitals.

Any System Can Be Affected – The ransomware incident was most likely the work of a cyber-criminal organization but, based on the decryption code being provided prior to a ransom demand, it is possible that the hospital was targeted by mistake. The Dusseldorf University and NotPetya attacks are two examples of cybersecurity incidents affecting OT systems other than the original target. This emphasizes the need for every OT system to take adequate cybersecurity measures.

Preventing the Attack – The initial breach occurred from a known vulnerability in the VPN software used. Effective patch management practices would have prevented the attackers from gaining access and having the opportunity to deploy the ransomware on the system. Additionally, a robust system backup and restoration procedure (including offline backups) for the hospital could have limited the amount of time required to restart the system and limit the disruption to patients.

6.8 SolarWinds

The SolarWinds cybersecurity incident was discovered in December of 2020. SolarWinds, an IT network management company based in Texas, was compromised, leaving as many as 18,000 customers vulnerable to attack [26]. Prominent victims of the attack include the Pentagon, nuclear laboratories, United States Treasury, Commerce, and Energy Departments, and several private cybersecurity firms [27]. The attack has been attributed to an advanced persistent threat (APT) associated with the Russian government and demonstrates the potential for sophisticated actors to compromise many different victims by targeting common supply chain elements.

Background: The SolarWinds incident is an important example of a supply chain attack. There are numerous places in the supply chain where an

attack may occur: at component suppliers, at equipment manufacturers, in transit, at reception, at installation, via ongoing patches and upgrades, and at disposal. If an attack can be successfully completed while the item is in the supply chain, then there is often no way for asset owners to identify that an attack has occurred because the means for prevention, discovery, and tampering will have been bypassed, disabled, and/or replaced by valid surrogates.

Threat Agent: Supply chain attacks are among the most sophisticated methods for introducing an attack and typically require high skill levels consistent with an *APT* or *nation state*. The SolarWinds attack has been linked by multiple sources to an APT group with ties to the Russian government [26], [27], [71]. In many cases, supply chain attacks also require insider support; however, no insider involvement was suspected in the SolarWinds incident.

Attack Method: The first identified access vector for the breach was a supply chain compromise of the SolarWinds Orion Dynamic Link Library (DLL), which exposed as many as 18,000 customers to the attack dating back to March 2020 [26]. An advisory issued by the Cybersecurity and Infrastructure Security Agency (CISA) identified “evidence that there are initial access vectors other than the SolarWinds Orion platform,” meaning that even organizations without the SolarWinds monitoring software could have been affected by the attack [72].

Based on the currently available information about the incident, it appears that the attack methods were focused solely on reconnaissance activities. However, the widespread nature of the hack and the success of the attack for penetrating deep into organizations business networks introduced concerns that, if they desired, the attackers could have denied access to authorized users, deleted or corrupted critical data, or even gained control of IACS computer systems [26].

Impact: The full extent of the SolarWinds incident is not yet known, and it will likely be years until a complete picture of the incident is available. Initial estimates are that, based on the SolarWinds supply chain vector alone, as many as 18,000 customers were exposed to the attack including an emphasis on U.S. government agencies, IT cybersecurity firms and software suppliers, as well as organizations with IACS connected systems [26]. At least nine U.S.

government agencies and at least 40 private sector companies have been determined to be affected [26] [71]. Recent information indicated that “a small number of employees’ accounts were targeted in the breach;” among these email accounts was Chad Wolf, the acting Secretary of the Department of Homeland Security [71].

Brad Smith, the president of Microsoft, stated in response to the incident that “Governments have long spied on each other but there is a growing and critical recognition that there needs to be a clear set of rules that put certain techniques off limits. One of the things that needs to be off limits is a broad supply chain attack that creates a vulnerability for the world that other forms of traditional espionage do not.” [71] One long lasting impact from the attack is a re-evaluation of the methods used by nation states when conducting espionage activities as well as the methods for responding to large-scale cybersecurity incidents.

Unfortunately, the SolarWinds incident is not an isolated example, and the potential of supply chain-based attacks to compromise many different targets will only continue to grow. Even as many organizations continue to grapple with the SolarWinds incident, four vulnerabilities found in Microsoft’s Exchange software for organizations running self-hosted servers have reportedly led to the compromise of emails for over 30,000 U.S. government and private sector organizations [73]. This second attack has been attributed to an APT group with ties to the Chinese government and provides yet another example of nation state supported groups implementing a broad supply chain-based attack.

Key Points

Supply Chain Vulnerabilities – Supply chain attacks require a high level of skill to execute, but they can be invaluable to APT or nation state groups because they provide access and potential back doors to many possible targets. These recent incidents highlight the need for effective supply chain management as a foundational part of an organization's cybersecurity strategy. When a company allows a connection to a third-party vendor or software provider, it allows for the potential introduction of a previously unidentified risk.

Any System Can Be Affected – Although a supply chain-based attack may be focused on compromising a specific user or set of users for a hardware or software product, any company using the affected version of the product can also be affected. This means that any company using the third-party product could experience the impact of the data breach/espionage, deployment of ransomware or other attack method. This is highlighted by the large number of companies potentially affected by the recent attacks 18,000 (SolarWinds) and 30,000 (Microsoft Exchange).

Preventing the Attack – Supply chain attacks are particularly difficult to protect because the documentation and barriers for prevention or discovery of tampering will have been already compromised, making it difficult for asset owners to identify an attack. Effective supply chain risk management and emerging strategies such as Software Bill of Materials (SBOM see Chapter 12) are essential for reducing the likelihood of a supply chain attack affecting multiple sites. Additionally, each site can take steps to isolate any networks connected to third-party platforms or networks from the rest of the IT and IACS networks; this is one method that can help to limit the effectiveness of a supply chain-based attack on common software applications by restricting the number of devices that can be compromised. Application whitelisting can also provide protection against malware introduced from the supply chain by preventing any unauthorized applications from running on the IACS

6.9 *Florida Water System*

The Oldsmar Water Treatment Facility in Pinellas County Florida was compromised by hackers on February 5th of 2021. Hackers took advantage of the TeamViewer remote access application that was installed on the water facilities network to gain remote access [22]. The attackers successfully gained control of the process and were able to increase the concentration of water treatment chemicals with the potential to cause illness to the public and lead to significant corrosion and piping damage.

Background: The Oldsmar attack, was not the first attack in recent years to target drinking water. In 2016, another attack led to the successful modification of chemical flows for the “Kemuri” Water Company (Kemuri is a pseudonym used for the incident as the utility’s identity was not publicly announced) by a group of politically motivated hackers with ties to Syria [74].

Threat Agent: The specific threat agent responsible for the Oldsmar, Florida water hack is not known, but many experts believe it was not executed by a highly skilled agent such as a nation state or cybercriminal group. Instead it may have been a show of skills motivated attack, or an attack executed by a relatively unskilled hacker such as a script kiddy. The evidence supporting this theory is that no vulnerabilities were required to compromise the system (so it was susceptible to hackers of various skill levels) and the attackers did not attempt to disguise their behavior or maximize the damage (e.g., make the concentration change in the middle of the night or during a holiday weekend when the water treatment system may have been unmanned) [75].

Attack Method: The attackers used a compromised TeamViewer account to gain remote access to the water facilities network [22]. TeamViewer was originally installed on the water system network to allow for status checks and troubleshooting of alarms or other issues, but it had not been used for at least six months prior to the attack [22]. Additionally, each computer used to monitor the system remotely shared a single TeamViewer account and password. This meant that once that account was compromised, any computer on the network could be accessed. Furthermore, there was not a firewall separating the water system SCADA network from the internet, leaving virtually no barriers between the attackers and the SCADA network.

Impact: After the attackers gained access to the system, they were able to modify the concentration of water treatment chemicals and increase the amount of sodium hydroxide (lye) by a factor of 100 [75]. This much higher concentration had the potential to cause illness to the public and lead to significant corrosion and piping damage [75]. This differed from the previous Kemuri Water Company attack, where although hackers gained access to the chemical dosing system, they were unable to trigger a meaningful change in the water composition.

Fortunately, for the Oldsmar facility, although the sodium hydroxide concentration was changed to hazardous levels, the operator noticed the issue was able to reset the system to the proper level [22]. In this case the operator's awareness or operational readiness was one of the final barrier to prevent a cyber-attack from contaminating public drinking water. Additional details on operational readiness and how to effectively prepare operators to be aware of cybersecurity concerns is provided in Section 10.16.

Key Points

Critical Infrastructure Vulnerabilities– The Oldsmar water facility attack differed from other attacks on critical infrastructure, in that it not only could have resulted in loss of availability of a critical function but could have also led to significant illness in the public. This is important because it demonstrates how significant consequences from industrial cyber-attacks could be when looking at health and safety.

Preventing the Attack – Applications should be removed from the IACS as soon as they are no longer needed, and this is particularly true of remote access programs. Poorly secured remote access connections offer an easy pathway for attackers looking to gain access. The TeamViewer account used by attackers to compromise the Oldsmar facility was not only unused, but also shared a single account for the entire network. Additionally, there was no firewall separating the SCADA network from internet connected networks. The first step towards preventing the attack would be to establish effective network segmentation and separate the SCADA assets from non-critical assets. Additionally, remote access applications that are currently being used and required for the system to operate should be configured for maximum security. Examples of configuring the remote connection for additional security include requiring multi-factor authentication, and more stringent password controls such as requiring the use of strong unique passwords and periodic changes to passwords.

6.10 Colonial Pipeline Ransomware

The Colonial Pipeline Ransomware incident was discovered on May 7th, 2021, when a ransom note was sent to the pipeline. After the ransom note was received, the pipeline was shut down for nearly one week as an extensive review was conducted to determine the extent of the attack and check for physical damage to the pipeline [76]. The incident and subsequent weeklong shutdown of the pipeline represented one of the most significant cybersecurity incidents affecting critical infrastructure. The attack has been attributed to the criminal hacking group DarkSide, believed to be located in Russia [77].

Background: The Colonial Pipeline runs for 5,500 miles from Houston, Texas to the eastern seaboard. It transports 2.5 million barrels per day or roughly 45% of all gasoline, diesel, and jet fuel for the east coast of the United States [78]. This attack represented the first time that the pipeline had been fully shut down in its 57-year history [76].

Threat Agent: The Colonial Pipeline incident has been linked to the cybersecurity criminal group DarkSide that is believed to be operating out of Russia [77]. This group followed the ransomware as a service (RaaS) model and developed ransomware that can be used by many different threat agents in exchange for a portion of the ransom payment. In the nine months the group was active, the attackers received roughly \$90 million U.S. dollars in ransom from 47 different victims [36].

Attack Method: The attackers gained access to the corporate IT network for the Colonial Pipeline through an unused Virtual Private Network (VPN) that allowed for remote access to the corporate network. The VPN account did not require multi-factor authentication, and the attackers were able to establish remote access with just a compromised username and password [76]. The exact way in which the attackers found the login credentials is unknown; a detailed review during the cybersecurity response did not identify any evidence of phishing, but the password for the VPN account was found in a list of compromised passwords on the dark web. It is possible that the password had been reused by an employee for another site [76].

The initial intrusion into the Colonial Pipeline network occurred on April 29th, and a little more than one week later on May 7th, the initial ransom demand was sent. In addition to encrypting files, the attackers stole approximately 100 gigabytes of data from Colonial Pipeline and threatened to release the data publicly if the ransom was not paid. This practice of not only encrypting data, but also stealing confidential data and threatening to release it, is known as double extortion - and is becoming increasingly common for criminal hacking groups.

Impact: Although it is currently believed that the ransomware incident was fully limited to the IT network and that the operational IACS assets were not impacted, the decision was made to shut down the Colonial Pipeline to determine the full extent of the attack on the system. Only after completing a

complete visual verification of pipeline assets to confirm that no physical damage had been triggered, and conducting a thorough review of the IACS assets to confirm that they had not been impacted by the attack, was the decision made to restore pipeline operations [76].

The attack represents one of the most significant cybersecurity impacts to date on critical infrastructure systems. The outage for the pipeline - supplying nearly half of all gasoline, diesel, and jet fuel to the northeast United States - led to widespread concerns of fuel availability, long lines at gas stations, and increasing prices. Several steps were taken to minimize the disruption resulting from the attack, including relaxed rules for the transportation of petroleum fuel by road to allow increased shipment of fuels by truck. Over the week in which the attack occurred, oil prices rose six cents per gallon and continued to rise even after the pipeline operations were restored as suppliers struggled to meet demand [78].

Colonial Pipeline also paid roughly \$4.4 million U.S. dollars in ransom as a result of the attack. Although many governments, including the United States, have public positions that discourage the payment of ransomware demands since they may incentivize future attacks, many companies are left in an extremely difficult position of facing longer outages if encrypted data is not restored [77]. The United States Justice Department (DOJ) has reported that \$2.3 million U.S. dollars in cryptocurrency has been recovered from the ransom paid to DarkSide as part of a collaborative effort between the Federal Bureau of Investigation (FBI) and the DOJ after Colonial Pipeline notified them of the breach and ransom demand [77]. Additionally, DarkSide is believed to have ceased operations after it lost access to its internal servers and cryptocurrency wallets [36]. The efforts to disrupt DarkSide appear to be an attempt to discourage future attacks by cyber-criminal groups against critical infrastructure, but it is not yet clear if disruptions after the fact will prove to be an effective deterrent.

Key Points

Critical Infrastructure Vulnerabilities– The Colonial Pipeline incident highlighted yet again the many vulnerabilities present in critical infrastructure systems and showed how cybersecurity attacks can cause significant disruption to the public. What set the Colonial Pipeline incident apart from other attacks on critical infrastructure, such as the Ukrainian power grid, is that the attack was not specifically designed for IACS systems or developed to cause specific damage to the pipeline. This is important because it demonstrates that even IT based cybersecurity attacks and more general malware can lead to significant physical impacts if sufficient security protections of critical infrastructure or effective segmentation between the IT and IACS network are not present or available. Additionally, if critical functions, such as financial tracking and invoicing, on the IT network of an IACS organization are compromised this can have negative effects, even if segmented properly.

Preventing the Attack – Poorly secured remote access connections offer an easy pathway for attackers looking to gain access. The VPN used by attackers to compromise the IT network of the Colonial Pipeline was no longer in use and should have been disabled as soon as it was no longer needed. Additionally, the security settings for the VPN could have been improved by requiring multi-factor authentication, and more stringent password controls such as requiring the use of strong unique passwords or periodic changes to the password would have limited the possibility of the password being compromised from another account.

6.11 Summary

For over twenty years, cybersecurity attacks on IACS systems have been shown to represent a real and present threat to automation systems, with the potential for failures of both control and safety systems. Incidents have shown that cybersecurity can have physical impacts resulting in financial, environmental, and safety-related consequences. Although no cybersecurity attacks to date have led to a confirmed loss of life, the recent attacks on the Saudi petrochemical facility and the Düsseldorf Hospital show just how serious the potential safety consequences of cybersecurity events could be. An

important step in preparing for cybersecurity threats is to stay informed about recent attacks. One reliable source for updates on recent attacks is the Cybersecurity and Infrastructure Security Agency (CISA) Alerts, which can be subscribed to via email [79]. The second part of this book will shift the discussion from the basic concepts of industrial cybersecurity and focus on a risk-based approach for understanding, managing, analyzing, and protecting against cybersecurity risk.

Part 2: Integrating Cybersecurity Management into the Process Safety Framework

7 General Model for Understanding Cybersecurity Risk

The first part of this book introduces the concepts of industrial cybersecurity and cybersecurity risk, including examples of cybersecurity activities, types of targets, sources of cybersecurity risk, and incident case studies. The second part of this book builds on this foundation and demonstrates how cybersecurity can be integrated into process safety management. Before discussing methods for integrated safety and cybersecurity, it is helpful to understand some existing models for managing cybersecurity risk.

Similar to the approach adopted for managing process and functional safety, a lifecycle approach is also appropriate for cybersecurity. A number of different approaches for understanding cybersecurity risk have been developed in industry best practices, international standards, and regulatory requirements. The model introduced in this chapter has been built from a number of references, including:

- IEC/ISA 62443 [3]
- ISA TR 84.00.09 [80]
- NIST Cybersecurity Framework [11]

The resulting process for addressing cybersecurity risk, built from this model, is consistent with best practice in the process and related industries. The process can be adapted by each company to meet their specific safety and cybersecurity targets.

7.1 *Cybersecurity Lifecycle*

A lifecycle is defined in the CCPS Glossary as “The stages that a physical process or a management system goes through as it proceeds from birth to death. These stages include conception, design, deployment, acquisition, operation, maintenance, decommissioning, and disposal.” [1] It is important to consider a lifecycle-based approach for cybersecurity because of the potential for serious consequences if the IACS is compromised at any stage: detailed system design, during the production of individual components, or during facility operation. The cybersecurity lifecycle introduced in IEC 62443-1-1 [3]

consists of three phases: Assess, Implement, and Maintain. If cybersecurity is not addressed in each of these phases, the safety and integrity of the IACS may not be achieved.

7.1.1 Assess Phase

The first phase of the cybersecurity lifecycle is the assess or analysis phase. In this phase, the IACS is identified, segmented into zones, and analyzed for risk. The requirements for design are then defined. In process safety, the assess phase is dominated by Process Hazard Analysis (PHA), whereas in the cybersecurity lifecycle, a cybersecurity risk assessment is conducted.

The objective of the assess phase is to identify any shortcomings in the current cybersecurity of the facility. In a greenfield project, this is completed before the implementation and maintenance stages to ensure that the IACS can be operated safely and securely. For brownfield facilities, or sites already in operation, it is still important to first complete the assess phase to identify the current level of risk for the facility and prioritize remediation actions. Figure 7-1 documents the assess phase as defined in IEC 62443-1-1, with each major step numbered [3].

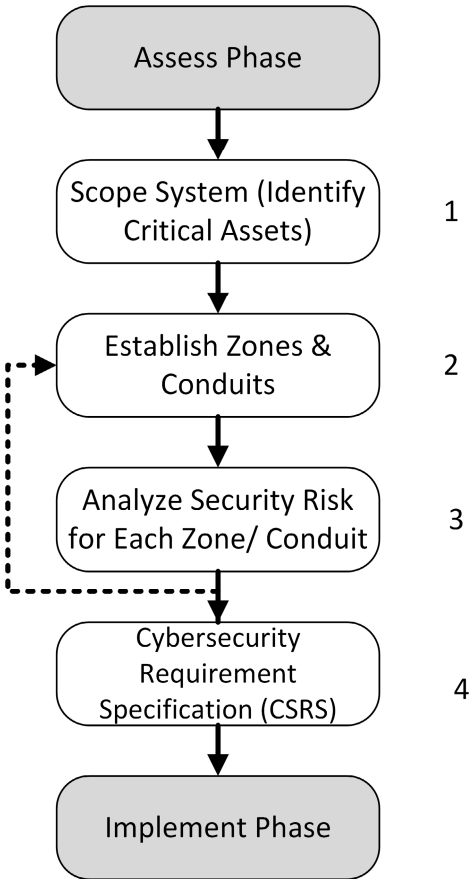


Figure 7-1 Assess Phase

Source: IEC 62443-1-1 [3]

The first step in the assess phase is to identify the scope of the system under review and set the boundary limits for the study. Next, the Zone & Conduit diagram, a network architecture diagram that identifies the security zones (grouping of logical and/or physical assets that share common security requirements) and conduits (connections between zones with network segmentation devices) is created. Additional information on network segmentation strategies is provided in Section 8.4.

Once the scope of the system is identified, a baseline cybersecurity risk assessment is necessary for both greenfield and brownfield facilities to

identify the most critical areas requiring mitigation. Chapter 9 provides additional details on various cybersecurity risk assessment methodologies.

The results of the risk assessment are formalized in the Cybersecurity Requirement Specifications (CSRS), which serves as the guiding design document in the implement phase. CSRS requirements for each zone can be standardized using a security level (SL) target, with four distinct levels correlating to different cybersecurity protections as shown in Table 7-1.

Table 7-1 IEC 62443 Security Levels (SL)

Security Level (SL)	Skills	Motivation	Means	Resources
SL 1	No Attack Skills	Mistakes	Non-intentional	Individual
SL 2	Generic	Low	Simple	Low (Isolated Individuals)
SL 3	IACS Specific	Moderate	Sophisticated (attack)	Moderate (Hacker Groups)
SL 4	IACS Specific	High	Sophisticated (campaign)	Extended (Multi-Disciplinary Teams)

Source: IEC 62443 Part 3-3 System security requirements and security levels [81]

Each increasing security level is intended to represent an increase of security by a factor of 10, similar to the difference in risk reduction between each Safety Integrity Level (SIL) in functional safety standards [18]. One way of defining Security Levels is to identify the types of attackers that can be protected against by a system of a given SL (e.g., unintentional mistake for SL 1, sophisticated attack for SL 3). The security requirements for a zone are

determined during the risk assessment phase based on the worst-case consequence of a cybersecurity compromise in a zone and, in many cases, are correlated to an organization's tolerable risk criteria. Further details on this approach to risk management are included in Chapter 9.

7.1.2 Implement Phase

The objectives for the implement phase are to have a complete design that meets the requirements of the CSRS and to have those designed countermeasures and systems implemented in the physical equipment. To ensure that the requirements have been implemented as intended, a Cybersecurity Factory Acceptance Test (Cyber FAT) and Site Acceptance Test (Cyber SAT) are completed. Not only are the cybersecurity countermeasures designed in this phase, but they are also tested and validated to ensure that the design goals are met when the countermeasures are installed. The implement phase is adapted from IEC 62443-1-1 [3] with each step numbered in Figure 7-2.

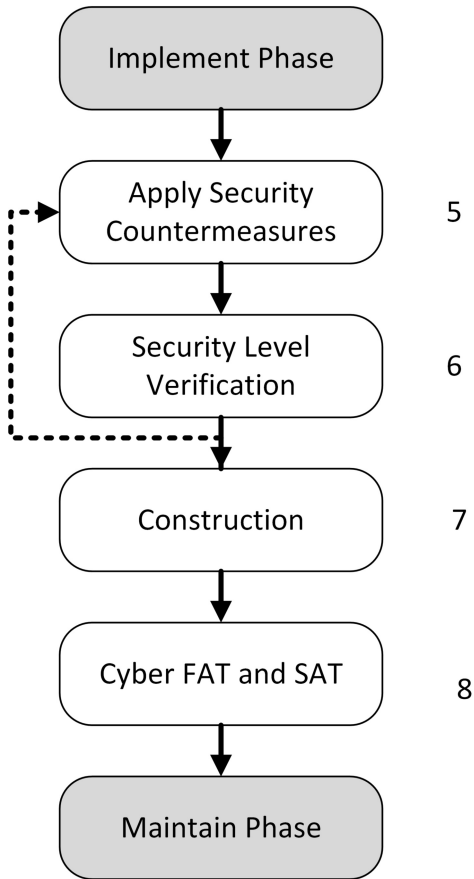


Figure 7-2 Implement Phase

Source: IEC 62443-1-1 [3]

The implement phase of the cybersecurity lifecycle includes the application of countermeasures, security level verification, and testing activities that make up the bulk of an upgrade, retrofit, or new project. Countermeasures are cybersecurity protections to prevent or detect a cybersecurity incident, and may include elements such as access control, network segmentation, system hardening, and defense-in-depth. Additional information on practices for designing a secure system and implementing countermeasures is included in Chapter 8. After these countermeasures are applied, SL verification is performed to ensure that adequate countermeasures are in place to provide

the necessary cyber risk reduction based on the organization's tolerable risk criteria. At the Cyber Factory Acceptance Test (FAT) and Site Acceptance Test (SAT) stages, the presence of the countermeasures in the configured system can be tested to validate that all countermeasures are in place and are functioning properly. Additionally, the Cyber FAT and SAT provide an opportunity for rigorous vulnerability scanning and potentially penetration testing to identify any cybersecurity weaknesses prior to beginning operations.

7.1.3 Maintain Phase

In the functional safety lifecycle, the maintain phase begins with the installation, commissioning, and validation of the Safety Instrumented Functions (SIF) [18]. In contrast, the cybersecurity lifecycle defines the maintain phase as beginning with the actual operation of the plant or equipment. Therefore, the first step in the maintain phase is startup, followed by maintenance activities, ongoing security monitoring, periodic audits, and modification/ decommissioning.

The objective of the maintain phase is to ensure that the level of cybersecurity for the IACS can be managed consistently throughout the lifecycle of the facility. The hardware assets of the IACS require periodic maintenance to maintain their cleanliness and correct operations. In addition to the maintenance of physical systems, periodic steps are required to maintain the health and proper function of software-based systems, including the patching of security vulnerabilities in applications and operating systems as well as updates to anti-virus definitions. The full maintain phase of the cybersecurity lifecycle is adapted from IEC 62443-1-1 [3] with each step numbered in Figure 7-3.

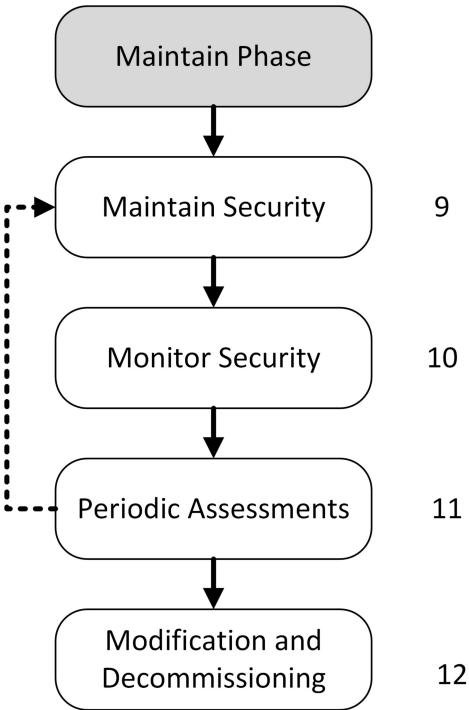


Figure 7-3 Maintain Phase

Source: IEC 62443-1-1 [3]

The IEC 62443 standard is performance based; this means that adherence to the standard requires ongoing measurements of security against key metrics. This may include tracking the current system patch level, anti-virus definitions, and the proper functioning of cybersecurity countermeasures. It is impossible to ensure that cybersecurity is achieved unless a feedback loop is in place to demonstrate that the cybersecurity countermeasures are still operating properly. Through the correct use and monitoring of cyber metrics, it is possible to maintain an up-to-date awareness of the operating state of countermeasures and overall cybersecurity health of the network (see Section 10.19).

The last portion of the maintain phase covers management of change and decommissioning activities. Cybersecurity countermeasures require more frequent attention than many Safety Instrumented Functions (SIFs) because of

the rapidly changing cybersecurity landscape. Thinking back to the castle analogy from Chapter 1, cybersecurity countermeasures can quickly become outdated if not frequently updated to protect against emerging threats - similar to the decline in effectiveness of castle walls after the introduction of gun powder and modern weaponry. For example, software patches to protect Microsoft systems against the Eternal Blue vulnerability were available prior to the NotPetya [64] and WannaCry [35] cybersecurity events and could have mitigated an organizations exposure to the malware. Management of change procedures are particularly important for cybersecurity because changes may have opposing impacts on achieved security. Unfortunately, not all patches can be deployed immediately. Not only does patching IACS have the potential to lead to system downtime, but insufficiently tested patches can even introduce compatibility issues between applications from different vendors. Only patches that have been tested and approved by the control system vendor should be considered. Care must be taken to balance availability and security needs to mitigate known vulnerabilities while avoiding changing the system too rapidly, which can result in decreased security and operational issues.

In the cybersecurity lifecycle, partial decommissioning is common; when this occurs, a risk assessment is required to ensure that the new control system setup is not at a greater risk of a successful cyber-attack due to the changes. For example, partial decommissioning may occur when a historian server is removed from the OT network. If this functionality is moved from the OT network to the IT network as a shared business server, it may have an impact on the achieved security by introducing another communication pathway between the IT and OT networks. Any partial decommissioning activity should trigger the same level of review as standard management of change activities.

7.2 *Integrated Cybersecurity and Safety Lifecycle*

The cybersecurity lifecycle introduced in Section 7.1 was originally designed and completed as a separate exercise, decoupled from the process and functional safety lifecycle evaluations. Often, IT personnel were responsible for cybersecurity concerns, while plant controls, process, and safety engineers had responsibility for safety activities. The lack of communication between

these groups represented a weak point in the achieved security of IACS. A lack of understanding of the required communications between IT and OT networks can lead to poorly configured firewall rules segmenting the networks (e.g., permitting traffic from all or many sources from the corporate IT network to connect to the OT network). These rules could result in unnecessary traffic between the enterprise and automation networks, significantly increasing the system exposure to malware and other attacks. Similarly, conducting frequent or automated patching activities of controllers on the automation network (similar to patching methods used for IT assets) can have major consequences for system availability because of the potential for a system level patch to lead to an unintentional shutdown of control equipment. Due to the potential for unintentional downtime, the patch management approach for OT needs to be different from the IT environment.

As awareness of the potential safety consequences related to an industrial cyber-attack rose, it became clear that closer coordination between security and safety activities is needed. One effective measure for improving communication between these groups is to connect the two lifecycles into a single integrated lifecycle, encompassing all safety and cybersecurity lifecycle tasks. The objective of this combined process is to optimize system design and prevent or detect analysis / design errors while avoiding excess documentation. This provides an opportunity for more efficient design, more effective solutions, and the potential for cost reduction.

The Technical Report ISA TR 84.00.09 *Cybersecurity Related to the Functional Safety Lifecycle* [80] was one of the first industry efforts to align the cybersecurity and safety lifecycles. This report, in combination with the IEC 62443 and IEC 61511 standards, represent the currently accepted best practices for:

- Identifying the level of consequence associated with a process or piece of equipment.
- Identifying the level of vulnerability for a control system and likelihood of a cyber-attack.
- Setting safety and cyber risk reduction targets to manage those risks to an acceptable level.

- Designing Safety Instrumented Functions (SIFs), countermeasures, and other means of risk reduction to meet those risk reduction targets.
- Testing, operating, and maintaining the SIFs and countermeasures to ensure that the SIL and SL targets are met.

The integrated safety and cybersecurity lifecycle is a mechanism used to meet specific safety and cybersecurity targets set by each company. A key step in both lifecycles is the independent validation of previous work completed through periodic assessments. In IEC 61511, five stages of Functional Safety Assessments (FSA) are introduced as key steps in the functional safety lifecycle [18]. In ISA TR 84.00.09, five stages for Cybersecurity Assessments (CSA) are defined as part of the integrated lifecycle and occur at the same lifecycle stages as the safety lifecycle equivalents [80]. Completing the FSA and CSA activities in parallel provides another opportunity to improve communication and coordination between personnel completing safety and cybersecurity tasks.

Adopting an integrated lifecycle approach that combines multiple industry best practices and international standards is an important step for any company looking to address both cybersecurity and safety risk. The framework of integrated lifecycle activities introduced in Table 7-2 can be used to ensure that all required tasks are completed and provides the information necessary to align tasks between the process safety and cybersecurity teams.

The integrated lifecycle provides guidance on how to integrate cybersecurity into the existing process safety risk management process. Every facility is unique, and the risk-based approach should be tailored to meet corporate risk criteria and site-specific hazards to create an effective risk management workflow.

Table 7-2 Lifecycle Steps for Process Safety and Cybersecurity

No.	Lifecycle Step	Process/ Functional Safety Activity	Cybersecurity Activity
Assess Phase			
1	Define Project Scope	Determine the physical equipment and chemical components under consideration.	Determine the industrial control system equipment and critical assets under consideration.
2	Determine System Under Consideration	Determine nodes for process hazard analysis.	Develop the Zone & Conduit diagram based on physical and logical groupings of devices from the network architecture.
3	Hazard Identification and Risk Analysis	Complete a process hazard analysis and Layer of Protection Analysis (or another SIL selection method) to ensure that a tolerable risk level is achieved, identify safeguards, and determine SIL targets for SIFs.	Complete an initial risk assessment to determine security level targets for zones. Complete Detailed Risk Assessment to determine residual risk with current and planned countermeasures.

Table 7-2 continued

No.	Lifecycle Step	Process/ Functional Safety Activity	Cybersecurity Activity
Assess Phase			
4	Document Requirements	Develop safety-critical equipment list (e.g., pressure relief valves, check valves). Develop a Safety Requirement Specification (SRS), with all the functional and safety integrity requirements of the SIFs identified.	Develop CSRS with cybersecurity specific requirements for safety critical systems (e.g., SIS, BPCS).
4a	Validation of Assess Phase	Functional Safety Assessment 1, independent assessment of all assess activities including risk assessment, SIL determination, and SRS.	Cybersecurity Assessment 1, independent assessment of all assess activities including cybersecurity risk assessment and requirement documentation.
5	Conceptual Design	Select equipment for safety critical items and Safety Instrumented Functions.	Select countermeasures for cybersecurity protections and select equipment with suitable security capabilities.

Table 7-2 continued

No.	Lifecycle Step	Process/ Functional Safety Activity	Cybersecurity Activity
Implement Phase			
6	Design Verification	Complete safety integrity level verification to ensure that SIL targets have been achieved.	Complete security level verification to ensure that security level targets have been achieved.
7	Detailed Design	Application programming development and verification. Detailed design documentation.	Device configuration and software asset inventory development. Detailed design documentation.
7a	Validation of Design Activities	Functional Safety Assessment 2, independent assessment of all design activities including conceptual design, SIL verification, and detailed design.	Cybersecurity Assessment 2, independent assessment of all design activities including conceptual design, countermeasure selection, SL verification, and detailed design.
8b	Installation and Commissioning	Installation of SIS and BPCS equipment and mechanical IPLs (Independent Protection Layers).	Installation of network equipment including boundary devices, switches, servers, SIS, and BPCS.

Table 7-2 continued

No.	Lifecycle Step	Process/ Functional Safety Activity	Cybersecurity Activity
Implement Phase			
8c	Site Acceptance	Site Acceptance Test to confirm correct functioning of SIS and BPCS on-site.	Cyber Site Acceptance Test to confirm cybersecurity resilience and correct functioning of countermeasures on-site.
8d	Pre-Startup Safety Review	Functional Safety Assessment 3, independent assessment of all safety activities completed prior to the introduction of hazards to ensure the safe condition of the system.	Cybersecurity Assessment 3, independent assessment of all cybersecurity activities completed prior to the introduction of hazards to ensure the secure condition of the system.
Maintain Phase			
9a	Startup	Start of the operations phase - chemical and physical hazards are introduced to the system.	Start of the operations phase - IACS is now connected to equipment with the potential to cause chemical or physical hazards.

Table 7-2 continued

No.	Lifecycle Step	Process/ Functional Safety Activity	Cybersecurity Activity
Maintain Phase			
9b	Operation	Reliability and integrity of safety functions and other IPLs is required to achieve availability and safety goals.	Security countermeasures are required to achieve availability and safety goals.
9c	Preventative Maintenance	Proof testing of SIFs and other required maintenance activities (e.g., calibration, mechanical integrity program).	Anti-virus updates, periodic patching of IACS.
10	Monitoring and Metrics	Tracking of key safety metrics (e.g., demand frequency, failure rates of safeguards).	Tracking of key security metrics (e.g., attack frequency, failure rates of countermeasures).
11	Periodic Assessment	Functional Safety Assessment 4, review of achieved safety based on operating experience.	Periodic vulnerability assessments (Cybersecurity Assessment 4), snapshot of achieved security.

Table 7-2 continued

No.	Lifecycle Step	Process/ Functional Safety Activity	Cybersecurity Activity
Maintain Phase			
12	Modification & Decommissioning	Management of Change procedures and evaluation of potential safety impacts of changes/ partial decommissioning (less common). Site decommissioning represents the end of the lifecycle. (Functional Safety Assessment 5)	Management of change procedures and evaluation of potential security impacts of changes/ partial decommissioning (common). Site decommissioning represents the end of the lifecycle. (Cybersecurity Assessment 5)

Sources: ISA TR 84.00.09 [80], IEC 62443-1-1 [3], IEC 61511 [18]

Comparing the process/functional safety and cybersecurity lifecycles at each stage, it is clear that significant commonality and overlap exists between the approaches used to ensure the safety and security of industrial systems. Each of these areas of overlap provides an opportunity to reduce the cost of deployment by completing the activities in a coordinated way to remove the need for duplicate work. This, in combination with the improved management of risk, are fundamental components of the business case for integrating safety and cybersecurity.

7.3 NIST Cybersecurity Framework

As discussed in the last section, key activities in the cybersecurity lifecycle include assessing potential threats and designing an effective protection strategy to guard against those threats. The National Institute of Standards and Technology (NIST) has provided a useful framework to help users identify their risks and develop appropriate countermeasures to improve cybersecurity. The framework can assist users as they develop their analysis

of potential threats, design/implement robust security measures, and operate/maintain management policies, standards, and procedures for the various phases of the lifecycle. While the NIST framework does not provide detailed guidance on how to accomplish each task, it does facilitate a common understanding of risk and enable users to develop customized measures appropriate to the particular organization. The NIST framework has a taxonomy that divides cybersecurity into five key pillars or functions:

1. Identify (I), develop an organizational understanding of cybersecurity risk to systems, people assets, data, and capabilities and implement an effective management strategy considering business needs.
2. Protect (P), implement sufficient countermeasures to ensure the security of critical assets and services.
3. Detect (D), develop appropriate capabilities to support the timely identification of potential cybersecurity events.
4. Respond (R), implement the necessary activities and strategies to take action to mitigate and limit the impact of a detected cybersecurity incident.
5. Recover (R), implement appropriate plans to restore any capabilities or services that were impaired due to a cybersecurity incident, with considerations for continuous improvement of cybersecurity resiliency.

The identify and protect functions are preventive in nature, whereas the detect, respond, and recover functions are mitigative. Each function has categories that describe specific aspects of the lifecycle that are relevant to the particular function, as shown in Table 7-3.

Table 7-3 NIST Framework Functions and Categories

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security & Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communication
Risk Assessment	Information Protection processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	

Source: NIST Cybersecurity Framework [11]

Each category has subcategories that describe numerous activities and performance criteria that are related to the category and function. Finally, the framework provides industry references for each subcategory, where more detailed information can be found that an end user might find useful when developing their management systems. An example of the framework structure and taxonomy for one category in each of the functions is provided in Appendix A.

The five functions in the NIST framework can be aligned with the phases of the integrated lifecycle, as shown in Figure 7-4. The assess phase of the lifecycle aligns with the NIST identify function, the implement phase aligns with the protect and part of the detect functions, and the maintain phase aligns with the remainder of the detect function and with the respond and the recover functions.

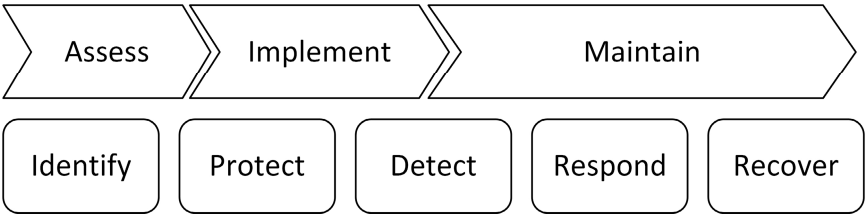


Figure 7-4 NIST Framework Aligned with Integrated Lifecycle

Source: IEC 62443-1-1 [3] and NIST Cybersecurity Framework [11]

Understanding the functions of the NIST Cybersecurity Framework are a beneficial step in implementing cybersecurity for IACS, because they provide a consistent taxonomy and approach for evaluating cybersecurity capabilities at different phases in the cybersecurity lifecycle. The framework is not intended to function in isolation but is meant to enhance existing cybersecurity strategies by providing an efficient methodology for identifying gaps and prioritizing mitigation measures.

7.3.1 *Identify*

The first NIST function, Identify, is consistent with the assess phase from the integrated lifecycle. As shown in Table 7-3, the key objectives of the Identify function are:

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

The Asset Management activity includes identifying critical assets and defining the scope of the activities. It also provides added details on the types of information that should be considered when developing asset lists. This information includes both physical (devices and systems) and software (software platforms and applications) assets, as well as the communication/ data flow between assets and external information systems.

The Business Environment activity is an important step to understand the facility's position in the supply chain and critical infrastructure. Understanding

the potential impacts of a cybersecurity attack is important to determine how attractive a site may be to attackers and to ensure that appropriate measures of risk reduction are implemented.

Governance is related to the organizational policies within a company. Effective policies document the roles and responsibilities for personnel and demonstrate how regulatory requirements and organizational objectives for cybersecurity are met. One of the most effective methods for managing cybersecurity is to align these policies with existing process safety management. This strategy is discussed in depth in Chapter 11.

Risk Assessment is a fundamental step in any risk-based approach. An effective cybersecurity risk assessment needs to consider the likelihood of a cybersecurity attack as well as the potential consequence of a cybersecurity attack. Detailed methodologies for completing a cybersecurity risk assessment are introduced in Chapter 9.

The Risk Management Strategy refers to the established policies for identifying, managing, and accepting risk. Corporate risk criteria are a key piece of the risk management strategy. In many cases, the risk criteria for process safety can be leveraged for cybersecurity considerations as well. Information on adapting safety risk matrices for safety and cybersecurity consideration is introduced in Chapter 3.

Overall, the different elements in the identify function help organizations to define and understand the current cybersecurity risk for the system and highlight the important steps needed to manage the risk based on the organization's business environment and governance structure.

7.3.2 *Protect*

Once the potential cybersecurity risks have been identified in the assess phase of the lifecycle, it is important to design and implement effective cybersecurity protections or countermeasures. The Protect function of the NIST framework identifies different steps for safeguarding the control system, including access control, user awareness and training, data security, information protection, maintenance, and protective technology.

The key objectives of the Protect function are:

- Access Control
- Awareness and Training
- Data Security
- Information Protection
- Maintenance
- Protection Technologies

Access Control consists of managing physical and logical access to the IACS. Logical access (the ability to log onto a computer-based system) is commonly secured following the philosophy of granting the least privilege - by creating user accounts with the minimum amount of access necessary to complete specific job functions. Logical access also relies on authentication (or means of verifying a user's identity prior to allowing access), such as the use of passwords or biometric scans. Physical security is often implemented at the site perimeter as well, such as locked doors or cabinets to restrict access to hardware. Remote access is also important to secure, as the increasing connectivity of IACS drives a greater risk of cybersecurity incidents.

The next activities for the protect function are Awareness and Training. These activities are essential to ensure that all employees have appropriate cybersecurity hygiene and are aware of the potential cybersecurity risks posed by both external hackers and accidental or malicious internal behavior.

Data Security is achieved by implementing sufficient countermeasures to protect data-at-rest (stored data) and data-in-transit (transferred data between two different systems). A robust data security strategy typically includes formal asset management, encryption, protection against data leaks, and integrity checking mechanisms.

Information Protection is an important extension of data security for the overall IACS and includes elements such as developing a baseline configuration, implementing configuration management, maintaining backups (both on and off network), and tracking the effectiveness of protection measures.

Maintaining organizational assets is necessary to protect against network intrusions. In particular, securing remote access and maintenance activities are important steps in limiting the potential for compromise of the IACS.

Lastly, Protection Technologies should be implemented to ensure that communications, removable media use, and access to the control system are controlled. Maintaining audit logs is necessary to evaluate the performance of protective technologies and other designed countermeasures to ensure that the credit given in the design and implementation phase can be maintained throughout the operations and maintenance phase.

The primary objective of the protect phase is to ensure that adequate cybersecurity countermeasures are defined that consider the different entry points for attackers and the different components of the IACS that require safeguarding. Protect is the final preventative measure in the framework; if the designed countermeasures prove to be ineffective, organizations will need to rely on mitigative measures from the Detect, Respond, and Recover stages.

7.3.3 *Detect*

The Detect function in the framework is based on identifying anomalies in network activity that are potential cybersecurity events via continuous security monitoring or other detection processes. Considerations for system monitoring are often completed during the implement phase. In the maintain phase, these considerations are used as a baseline against which events are evaluated.

The key objectives of the Detect function are:

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Detecting Anomalies and Events typically requires analysis of activity against a baseline to determine if an event is outside normal limits or established thresholds. Once an event crosses this threshold, it is important to analyze the attack methods and target, as well as the potential impact.

Security Continuous Monitoring is the process of monitoring logical and physical access to the IACS as well as traffic on the network. Key aspects of

security monitoring include the detection of malicious code, unauthorized mobile code (e.g., removable media), external connections, periodic vulnerability scans, and analysis of user behavior.

Detection Processes are the policies implemented that define what roles are responsible for detection activities and the necessary steps for carrying out the process in the event of a cybersecurity event. Best practices for detection processes include periodic testing, continuous improvement based on testing as well as on real-world performance, and clear communication to appropriate parties.

The Detect function represents both the transition from the Implement to the Maintain phase in the lifecycle model as well as the transition from preventative to mitigative measures in the NIST framework. So far, the activities discussed for the Identify, Protect, and Detect functions are preventative in nature; that is, they can be used to prevent a cybersecurity event from occurring or reduce the likelihood that an event will occur. The last two functions of the NIST framework are mitigative in nature; they reduce the consequence of a cybersecurity event once it has occurred.

7.3.4 *Respond*

Responding to a cybersecurity event consists of communicating, analyzing, and mitigating the event.

The key objectives of the Respond function are:

- Response Planning
- Communication
- Analysis
- Mitigation
- Improvements

Response Planning involves developing pre-plans on how to respond to a variety of potential cyber threats. The cybersecurity response plan often incorporates a mixture of cybersecurity specific aspects (e.g., response to compromise or failure of a network-based system) and process safety related aspects (e.g., emergency response procedure for fire or loss of containment), because of the potential of IACS systems to have physical impacts when compromised.

Communication in an incident response is enabled by personnel who have a clear understanding of their roles and responsibilities. Effective communication helps to maintain a clear chain of command and ensure that the necessary information is shared with all internal members coordinating the response. Communication also refers to the external communication necessary for incident reporting and voluntary information sharing, to improve cybersecurity awareness.

Analysis activities during a response are triggered by a notification of the detection system. The process of performing incident forensics and understanding the full impact of the incident. This analysis allows for events to be categorized, allows for the best response for the situation, and helps companies mitigate the incident as soon as possible.

Mitigation is the process of containing the incident, limiting the impact, and correcting the vulnerability that was exploited in the incident. This process helps to minimize the negative impact of the cybersecurity consequence and allows for a quick return to operation.

The last step in the response process is a mechanism for continuous improvement. The response plan should be re-evaluated based on lessons learned from real-world events and the results from testing the response procedures. Continually updating the response strategies is an important step in maintaining the technical currency of the plan in the continually evolving threat landscape.

Timely response to cybersecurity incidents is a major element of mature organizations approach to cybersecurity. Although it is not possible to design a system that is completely invulnerable to cybersecurity attack, conducting response planning and being prepared to quickly respond and minimize the impact of a cybersecurity incident can significantly limit the negative impact of an incident.

7.3.5 *Recover*

The final function in the NIST Framework is Recover. Once the incident has been responded to and the potential for further damage has been stopped, recovery activities including planning, improvements, and communications with external parties, are identified as the next steps.

The key objectives of the Recovery function are:

- Recovery Planning
- Improvements
- Communication

Recovery Planning, similar to response planning, can be conducted prior to or during an event. The results of proactive recovery planning activities or lessons learned from recovering from real-world cybersecurity incidents can be used to improve the recovery plan and ensure the strategies remain current. Recovery of the network components of the IACS may be handled via the use of backup files (if needed from a secure off network location), whereas the recovery from process safety effects, such as environmental cleanup or process equipment replacement, may take longer.

The final step of recovery is the communication with the public regarding the event. Cybersecurity events often have unseen consequences regarding a company's image and reputation that can have long-term financial consequences. Managing public relations throughout an incident and taking steps to repair the company's reputation after onsite recovery is complete are essential for minimizing the long-term impact of the incident.

Similar to the iterative nature of the integrated lifecycle, the NIST framework is also intended to operate as a continuous process. As such, the lessons learned from the response and recover activities can be incorporated into the cybersecurity risk identification process to ensure the protection and detection processes are sufficient to manage cybersecurity risk. This continuous improvement-based approach is an important component of the strategies for managing both process safety and cybersecurity risk.

7.4 Summary

Developing a robust model for understanding cybersecurity is a useful step in implementing a risk-based approach. It enables a common language and a shared understanding of cybersecurity activities. The model discussed in this chapter has been built from a number of sources, including the cybersecurity lifecycle and NIST Cybersecurity framework. The cybersecurity lifecycle provides a step-by-step methodology for implementing cybersecurity across the assessment, implement, and maintain phases. The lifecycle can be further

strengthened by considering the functions from the NIST cybersecurity framework (identify, protect, detect, respond, and recover). The cybersecurity lifecycle can be aligned with the process safety lifecycle to improve the efficiency of safety and cybersecurity activities.

8 Designing a Secure Industrial Automation and Control System

As Industrial Automation and Control Systems (IACS) continue to become more closely integrated with traditional IT networks, it is important that the unique risks and challenges faced by the IACS are adequately considered during the system design. Applying adequate security during the design process requires an understanding of the differences between IT and OT risk management strategies, a review of related process safety techniques, and the implementation of cybersecurity best practices such as defense-in-depth, network segmentation, system hardening, and security monitoring.

8.1 *The Disconnect between IT and OT Risk Management*

The IT world has been wrestling with cybersecurity risk for longer than the OT world, with a significant focus on cybersecurity for more than the last two decades. Many different organizations have been involved in addressing cybersecurity. These include the U.S. National Institute of Standards and Technology (NIST), which published *An Introduction to Computer Security: The NIST Handbook* in 1995 [82], and the Internet Engineering Task Force (IETF), which has created documents such as *RFC 2196 - Site Security Handbook* [83].

The dominant standard in the IT security field is ISO/IEC 27002:2013, *Information technology - Security Techniques - Code of practice for information security controls* [23], which is a comprehensive catalog of general IT security practices for cybersecurity risk management.

Although much work has been done to develop security practices for IT, these practices do not always directly transfer to OT systems. The disconnects between IT and OT occur because of technological differences between IT and OT systems and the differing priorities of these systems. Table 8-1 highlights some of the key differences between IT and OT environments.

Table 8-1 Differences Between IT and OT

	IT	OT
Vocabulary	IT specific	Process Safety specific
System Response Time	Most users require response times of one or two seconds, although longer times are tolerated	Often must be real-time based upon process dynamics, e.g., milli-seconds or seconds
System Availability	Outages tolerated	Outages are extremely costly and often not tolerable
Data Confidentiality	Data privacy is critical and may result in serious business loss	Data privacy is generally less critical
Data Integrity	Critical	Critical
System configuration and/or software integrity	Critical	Critical
Technology Obsolescence	3 – 5 years	20+ years
Upgrade Costs	Moderate	Significant
Patching	Timely	Less Frequent / As Required
Anti-virus	Common	Depends on system age
Changes	Easy to implement	Difficult to implement
Cybersecurity Awareness	Good	Poor / Improving
Process Safety Awareness	Poor	Good
Revalidation Requirements	No explicit requirement	No greater than 5 years

Source: Implementing IEC 62443: A Pragmatic Approach to Cybersecurity [84]

Understanding the differences in consequences for IT and OT cybersecurity incidents is the key to adapting security policies from the IT sector to the OT sector, as well as to adopting a risk-based approach for cybersecurity. The IT security culture and the technologies that it has created are based on the idea that performance and confidentiality are paramount and outages, while undesirable, are acceptable. This is clearly not true for the industrial world, where the need for the availability and integrity of a system typically dominates all other considerations.

8.1.1 Differing Priorities

The Confidentiality, Integrity, and Availability (CIA) model is commonly used to identify the order of priority for IT systems. Confidentiality is followed by integrity and finally availability in order of importance. As such, IT cybersecurity is primarily focused on preventing and responding to data breaches. Events impacting integrity and availability are undesirable but are ultimately tolerable. OT systems have reverse priorities, with availability being the most critical, followed by integrity and lastly confidentiality. These differing priorities are highlighted in Figure 8-1.

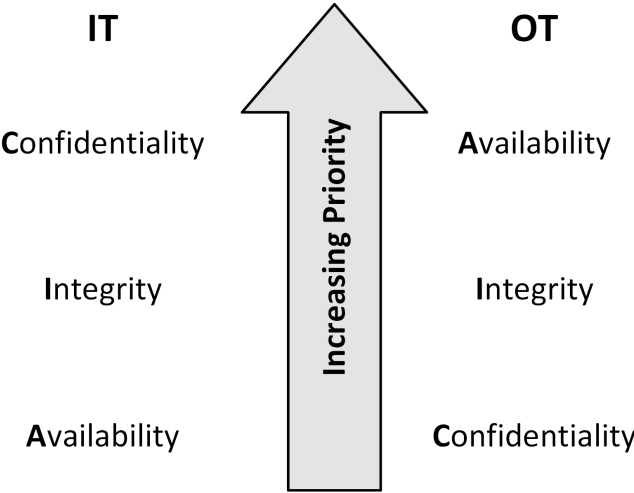


Figure 8-1 IT vs. OT Priorities

Occasional outages are common and tolerated in business systems, whereas control systems are expected to operate for years without interruption. Similarly, the tradition of beta testing new IT products in the field and recovering from problems by simply rebooting servers or switches is in sharp contrast to standard control system practices. This is not surprising considering the difference in consequences of outages for IT and OT systems. The impact of outages in business systems are typically loss of data or delay in activities, while outages in the process environment can result in loss of operations and production and may cause damage to equipment and the environment—or even illness, injury, or fatality. The impacts of process safety incidents are often evaluated for the impact on P-E-A-R or:

1. People safety i.e., worker injury/fatality and risk to public health due to toxic gas release, explosion, etc.
2. Environmental degradation due to pollution into air/sea/ground and contaminated food chain
3. Asset loss
 - a. Cost escalation due to repairing/replacing damaged equipment.
 - b. Profit erosion due to unsold off-spec products, production stoppage/slowdown, etc.
4. Reputational damage due to loss of stakeholder/client/customer confidence

The impact on these areas can be significantly costlier for OT systems than IT systems. If we consider the cost impact of a generic ransomware attack on an IT and OT system, we can see that the consequence may be very different between the two types of systems. Assuming a ransomware payment demand of around \$300,000 on average, the cost of the ransom or the time necessary to recreate the encrypted configurations/ data for an IT network is likely the highest cost component of the incident. However, for OT systems, if the ransomware affects systems necessary for operations, the cost of lost production will often quickly outweigh the ransom demand. For example, a

typical mid-size styrene plant (approx. 90,000 lbs./hr.) could result in approximately 1 million dollars per day of lost production [85]. After just eight hours of unplanned downtime the operational cost would exceed the ransom demand. In the worst-case scenario, if a safety-critical component is compromised and fails to act when needed, the resulting cost of a release or safety incident can be many orders of magnitude higher.

8.1.2 Information Technology (IT)—Extreme Connectivity

It is not just the priorities that differ between IT and OT - the network architecture and structure often vary significantly. IT networks are examples of extreme connectivity. IT networks often have a shared enterprise network across many locations and sites, interface with the internet, and frequently use 3rd party cloud hosts. Remote access is also very common for enterprise networks and serves to increase the level of access to IT networks.

From an attack surface perspective, IT networks tend to have many potential entry points and large numbers of different software and applications that could be exploited by attackers. This leads to lower inherent security for IT networks. Due to the lower consequences of cybersecurity events on IT networks, organizations are often willing to accept the risk of greater connectivity to allow for rapid communication between different sites, to improve information sharing and monitoring capabilities. Security measures such as frequent patching, anti-virus software, other end point protection, and continuous monitoring technology can be more easily deployed for IT networks. The reduced negative impact of a temporary outage resulting from a required countermeasure update or unexpected interaction with new applications makes these steps much easier to manage.

8.1.3 Operational Technology (OT) – Extreme Compartmentalization

Unlike IT networks, OT networks were originally designed to operate in extreme compartmentalization, with the use of specially designed computer-based systems to control individual parts of processes. Some types of OT, such as individual package PLCs and MCCs, are still local or hardwired; however, control systems, such as BPCS, have become more interconnected with monitoring and reporting functions. The range of compartmentalization can also be seen in safety-critical components. Safety instrumented systems are essential to maintaining the safe operation of many process plants. On some

networks, they are maintained on a network that is fully segmented from control and other functions; on other networks, they can be part of a connected safety and control network. The most compartmentalized type of safety instrumentation is the use of hardwired relays for safety functions; this has the security benefit of not being susceptible to cybersecurity compromise but can be very difficult to maintain over time (potentially defeating the required safety integrity).

8.2 *Inherently Safer vs. Inherently More Secure*

When considering how to design and protect OT systems as they become more interconnected with traditional IT systems, it is helpful to consider traditional strategies for risk mitigation. In process safety, there are multiple means for reducing risk, ranging from the elimination/ minimization of hazards or addition of safeguards to administrative procedures. Depending on the specific scenario, each of these steps may be necessary to achieve tolerable risk goals. However, when possible, the most effective of these methods is to apply the principles of inherently safer design, as shown in Figure 8-2.

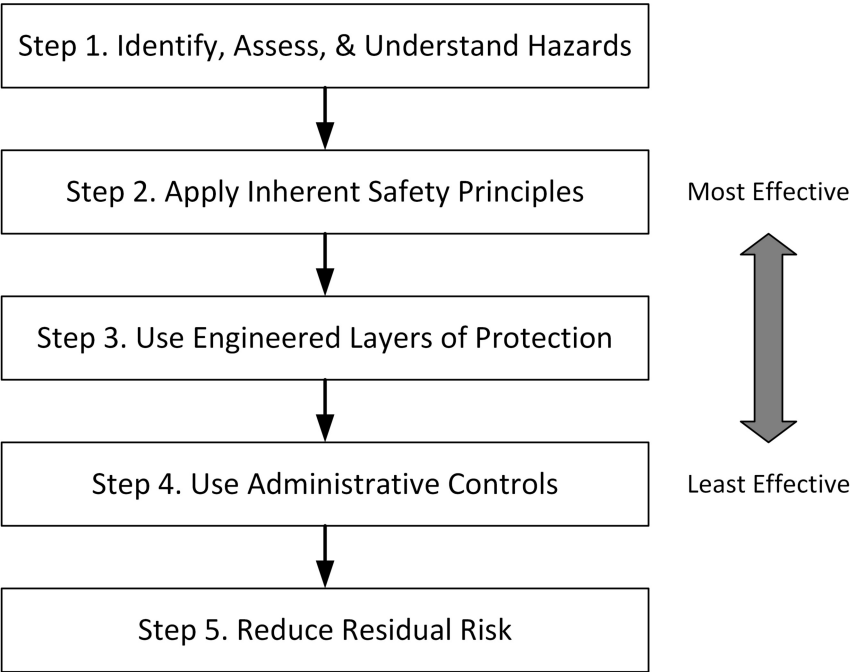


Figure 8-2 Hierarchy of Controls

Source: CCPS Inherently Safer Chemical Processes, A Life Cycle Approach [86]

Recognized and Generally Accepted Good Engineering Practice (RAGAGEP) suggests first eliminating the risk through good design. The greatest impact on the overall risk reduction. can be made when the hazard is physically removed. Although eliminating the risk is the most effective method, it may not be possible to fully eliminate all risk from process facilities. As introduced in Chapter 3, the presence of flammable and toxic materials at process sites creates the potential for harm. Steps can be taken through good design to reduce this risk as much as possible, and the remaining risk is then mitigated by subsequent applying risk controls such as engineered layers of protection (e.g., safety instrumented functions or alarms) and administrative controls such as awareness and training activities.

While inherently safer design focuses on process design to limit physical hazards, inherent security focuses on limiting cybersecurity hazards through

proper network design. One metric for measuring the inherent security of a system is attack surface. Attack surface is the number of available vulnerabilities or weak points that can be accessed and exploited by a cybersecurity threat. It can be determined in many different ways but should, at a minimum, consider the areas in Table 8-2.

Table 8-2 Attack Surface

Attack Surface Type	Considerations
Network	• Network Segmentation • Number of Devices on the Network • Internet-exposed Devices
Software	• Removal of All Unneeded Applications • Known Vulnerabilities in Current Operating System or Applications • Patch Management
Social Engineering	• Least Privilege Access • Cyber Hygiene/ Awareness Training • Personnel Security Measures • Physical Access

Designing an inherently more secure system does not involve the changing of the physical process conditions; instead, it focuses on reducing these areas of attack surface. Limiting the number of network devices, applications, and personnel with access can help to improve the inherent security. Steps such as system hardening or blocking unnecessary ports and removing applications not required for the IACS are also consistent with an inherent security approach and reduce the susceptibility of individual devices to cyber-attack. Although it is impossible to completely eliminate cybersecurity risk, following the hierarchical approach and taking steps to make the system as inherently secure as possible helps to mitigate the remaining risk. Adopting

a defense-in-depth approach and implementing the practices outlined in the remainder of this chapter can help to significantly improve the security and resiliency of the IACS network. Reduction in cybersecurity risk often consists of a combination of inherently secure design practices and following secure practices. Additional information on developing inherently safer/ more secure practices is presented in Section 10.9 (Operating Procedures) and Section 10.10 (Safe Work Practices).

8.3 *Defense-in-Depth*

Defense-in-depth is described as "an approach to defend the system against any particular attack using several independent methods [3]." Defense-in-depth is the essential principle for securing an IACS network to withstand a cyber-attack for a prolonged period. It is an extension of the principle of engineered protection layers in that, by ensuring the independence of each defensive layer, it is possible to limit the likelihood of common mode failures across multiple layers. Common cybersecurity protections used to implement a defense-in-depth approach are listed in Table 8-3.

Table 8-3 Common Cybersecurity Protections

Protection	Description
Virus Scanners/ Anti-Virus	Software program designed to detect and remove viruses/ other malicious programs. Additional information provided in Section 8.5.2.
Patch Management	Applying security patches in a timely manner to address known vulnerabilities. Additional information provided in Section 8.5.1.

Table 8-3 continued

Protection	Description
Access Control	Process of restricting access to only required personnel. Use of strong authentication methods for personnel establishing access.
Network Segmentation (e.g., Firewalls, DMZ)	Using barrier devices to block all non-essential communication between security zones. Additional information provided in Section 8.4.
System Hardening	Removing unnecessary applications or features to improve security. Additional information provided in Section 8.5.
Security Monitoring	Monitoring network traffic to identify potential cybersecurity incidents requiring response. Additional information provided in Section 8.5.1.
Policies & Procedures	Security policies and procedures for cybersecurity hygiene and adhering to cybersecurity best practices. Additional information provided in Chapter 11.
Physical Security	Methods for preventing unauthorized physical access to IACS assets such as perimeter security, locked buildings, locked cabinets, and security cameras.

As presented earlier, a good analogy for defense-in-depth is a medieval castle. These fortresses were designed to provide protection against invading forces. To do this, layers of defense—from moats, outer walls, and castle walls to well-manned gates and the garrison—repelled attackers. The idea was that even if one layer were to be bypassed (e.g., the attacking army got past the moat), there would still be multiple layers left to defend the castle. Figure 8-3 shows the defense-in-depth concept for implementing common cybersecurity protections (similar to the process safety onion model for protection layers).

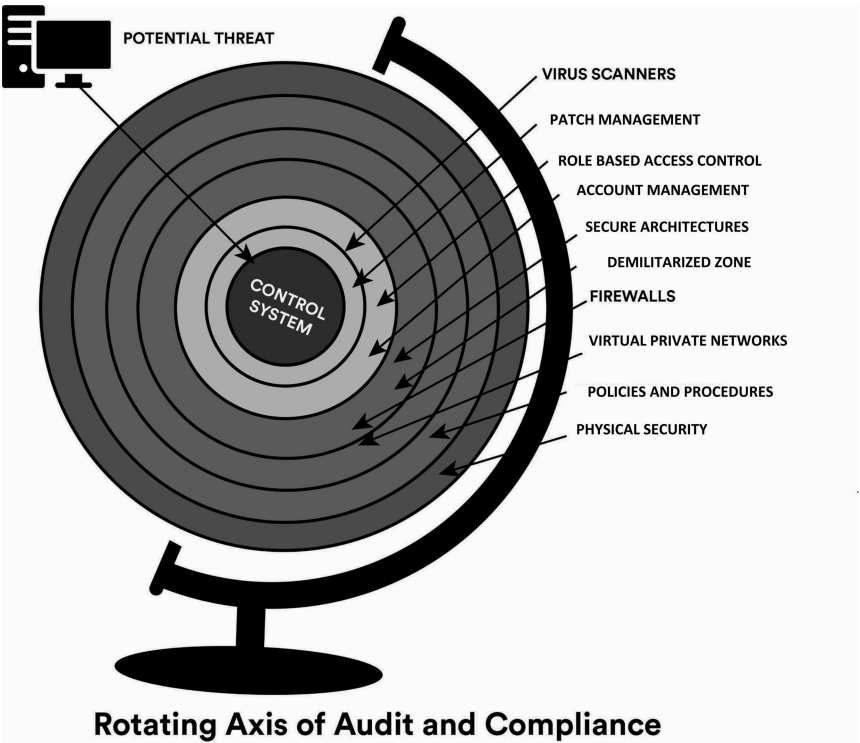


Figure 8-3 Defense-in-Depth for Cybersecurity

Source: Implementing IEC 62443: A Pragmatic Approach to Cybersecurity [84]

This definition for defense-in-depth introduces key concepts that will be carried throughout the rest of the design process. First, it demonstrates the

need for independent layers of security and detection (even on a single system) to protect the system from cyber threats. It also reinforces the understanding that every layer (and system) can be hacked, given enough time and skill. This is similar to process safety in that no one layer of protection can fully eliminate the risk as some probability of failure exists for each individual layer - whether it is a SIF, pressure relief valve, or even a physical barrier such as a dike.

Deploying a layered defense method forces the attacker to go through each level individually, making the process of gaining entry more difficult. When considering that attackers must also avoid being detected while bypassing each layer, the addition of new layers further increases the time required to gain access and increases the possibility of staff identifying the intrusion prior to actions on objectives.

Additionally, the use of a tiered defense allows for deficiencies in one layer to be addressed by another layer. A good example of this is the demilitarized zone firewalls (DMZ). The firewall from the business network to the DMZ must be configured to allow some internet-facing traffic through, which exposes the system to potential threats. The firewall between the DMZ and the control network is configured to disallow all internet-facing traffic, preventing any threat from going directly from the business network to the control network. This layered firewall approach allows for efficient engineering, while maintaining network security.

For true independence, each layer should be able to operate autonomously and use different functionality. This helps reduce the likelihood that an attacker can bypass multiple layers of defense using a single technique or method. Following this and the aforementioned principles allow for the effective design of layered system security, which is a key component of the overall defense system.

Each cybersecurity protection must be monitored and maintained. One exercise to review the current level of monitoring for cyber-protective functions is to draw a simple graphic of the design in question, list the countermeasures, and then document what metrics, diagnostics, or alarms are in place for each countermeasure. A countermeasure with no metrics, diagnostics, or alarms is equivalent to a safety function with no alarms, proof

tests, or inspections. The metrics, diagnostics, and alarms for countermeasures comprise the “rotating axis” (shown in Figure 8-3) required to maintain the integrity of cyber-protective functions.

8.4 *Network Segmentation*

Network segmentation is an effective approach to enhance both security and performance. A network is divided into zones considering security requirements for applications and data, and the access needs of users. Proactive security measures are put in place to prevent unauthorized access to the zone and to securely manage access by trusted users. The equipment and methods used to protect each segment are determined by the risk potential posed, and the requirements for information flow and user access into the segment.

For OT networks, as with all networks, there is a trade-off between security and operability. As connections are increased, the configuration and operation of OT systems has been made easier. Following the standardization of OT systems on the Windows OS, the question of whether to connect or not has become even more important for OT systems.

Each new communication path has the opportunity to provide better insight into the process leading to improved monitoring capabilities and operational efficiency, but also has the potential to serve as an entry point for attackers. The fewer connected devices and systems a network has or the fewer communication paths, the inherently more secure it is. As the number of connected devices grows, the larger the attack surface becomes, which presents more opportunities for attackers to gain access to the system.

The extreme of allowing every connection and directly interfacing OT systems with internet-based systems (Figure 8-4) is not sustainable due to the increased probability of unexpected downtime and potential for unexpected interactions between external and internal systems.

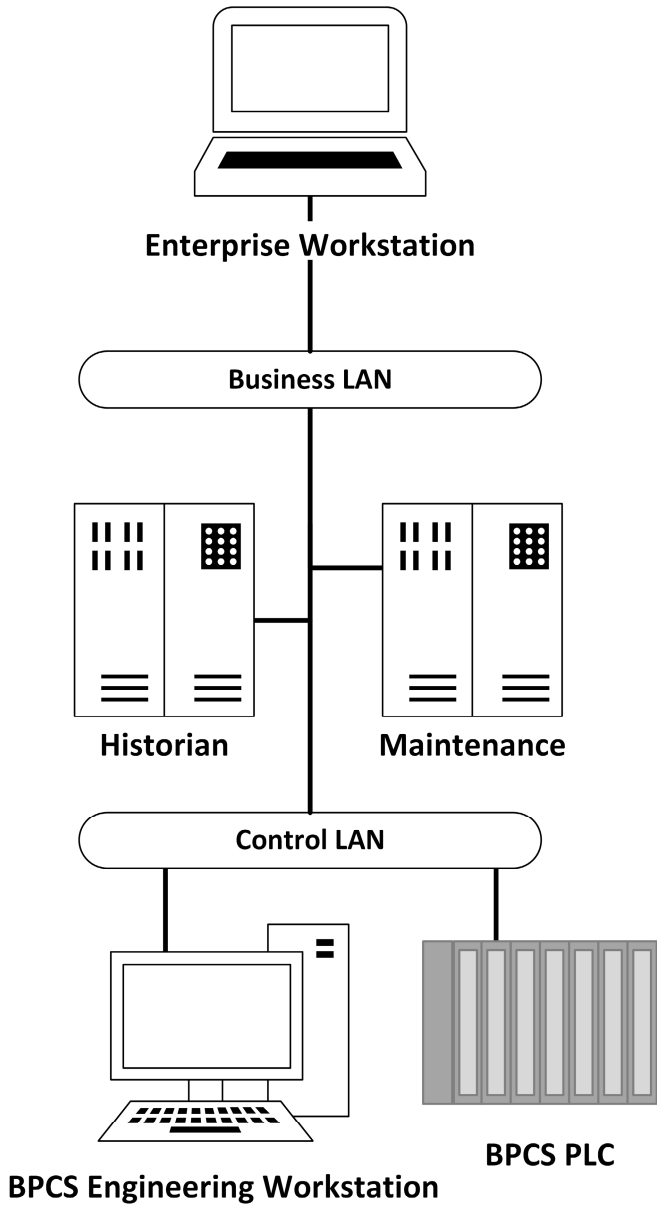


Figure 8-4 Example Network Architecture with Extreme Connectivity

The other extreme of a network operating in total isolation is equally unsustainable (Figure 8-5). A traditional air gap between the OT and the IT network is intended to prevent security concerns from crossing over into the OT space. While having complete network segmentation with no connections between the IACS and internet connected networks seems like a good approach, it has several major drawbacks:

- There is no “true” air gap; all systems require some information input or output, even if it is not normally connected to the network a computer or if a USB is often needed to transfer information.
- Isolated systems can quickly become unpatched and unsupported.
- Lack of automated backups can make fully isolated systems more difficult to restore.
- Business demands are driving greater connectivity to improve operational efficiency.
- False sense of security can lead to poor cyber hygiene.

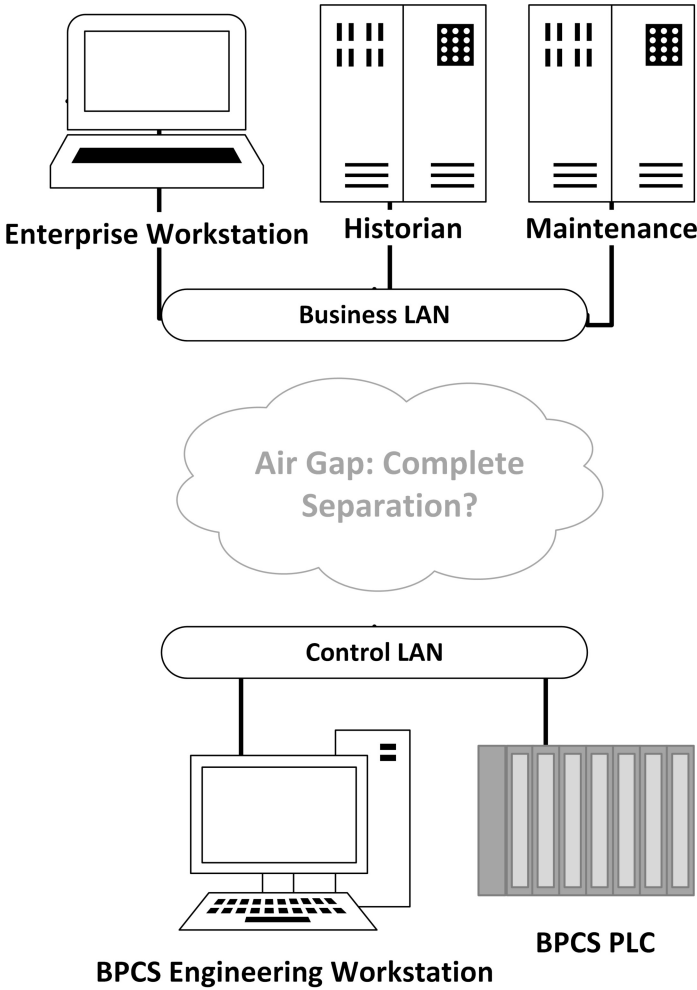


Figure 8-5 Example Network Architecture with Complete Separation

Although some automation systems have remained isolated, for many remaining fully isolated is no longer an option. Instead, they must navigate how the connections can be managed safely and securely. Similar to inherent safety, it is not possible to fully eliminate cybersecurity risk, and actions must be taken to maintain the required network connectivity as securely as possible (to achieve tolerable risk). For OT networks, key aspects of a risk-based

approach for establishing a network architecture are network segmentation, defense-in-depth, and system hardening.

8.4.1 Types of Network Segmentation

A well-planned network architecture is one of the most important technical factors in determining if a control system facility can be effectively secured from cyber-attack. If the architecture is properly designed, then a layered defense will be feasible, and the cybersecurity countermeasures deployed will achieve their maximum effectiveness.

One commonly used networking device is a network switch (a hardware device that forwards data packets to an individual specified device). Switches are commonly used to connect devices on a Local Area Network (LAN), which is any computer network within a small geographical area. One application of a network switch is to split up the LAN into smaller virtual segments known as VLANs. Breaking the physical network into smaller logical networks helps to increase performance, improve manageability, and simplify network design.

If configured properly VLANs can allow switches to provide some segmentation between networks. However, switches and VLANs are susceptible to many common types of cybersecurity attacks, and do not provide the same level of segmentation as traditional firewalls. As a result, switches should not be considered as a fully effective cybersecurity mechanism and should instead be used to help manage traffic flow within a zone.

It is critical to be able to segregate the overall network according to services, users, and systems. This is only possible if the network architecture is properly designed to allow for segregation and permit the deployment of effective controls such as firewalls between zones.

The first step for network segmentation is to deploy a countermeasure strategy using security zones based on risk level for all cyber assets. High-risk zones (e.g., zones with critical cyber assets such as SIS and BPCS) should be isolated or segmented with well-managed and maintained barrier devices from zones with lower security requirements. These barrier devices should block all non-essential communications into and out of high-risk zones.

In addition to these basic steps, current industry best practice calls for the control system network to be clearly separated from regular IT network segments (e.g., the business network). This is implemented using independent switches isolated behind a business or control system network firewall [87]. Many companies have adopted a third network or demilitarized zone (level 3.5) for shared business or control system assets, such as data historians as shown in the reference model in Figure 1-3. The reference architecture drawing in Figure 8-6 illustrates this type of structure.

The shared nature of the DMZ between the IT and OT network can sometimes make administration and management of the intermediate zone difficult. In many cases, it is beneficial to have the OT technology team manage access through the control system firewall to ensure that the proper permissions have been granted to any individuals getting system access to the control system workstations/servers.

Understanding the ownership of specific zones is a key point for design. As the system is deployed, designers and operators must appreciate what is owned by local plant personnel and what is managed by others (e.g., what devices or systems have contractors providing maintenance and support). Countermeasures should be designed to segment zones that are managed internally from zones managed by third parties, while still allowing the necessary communications for operations.

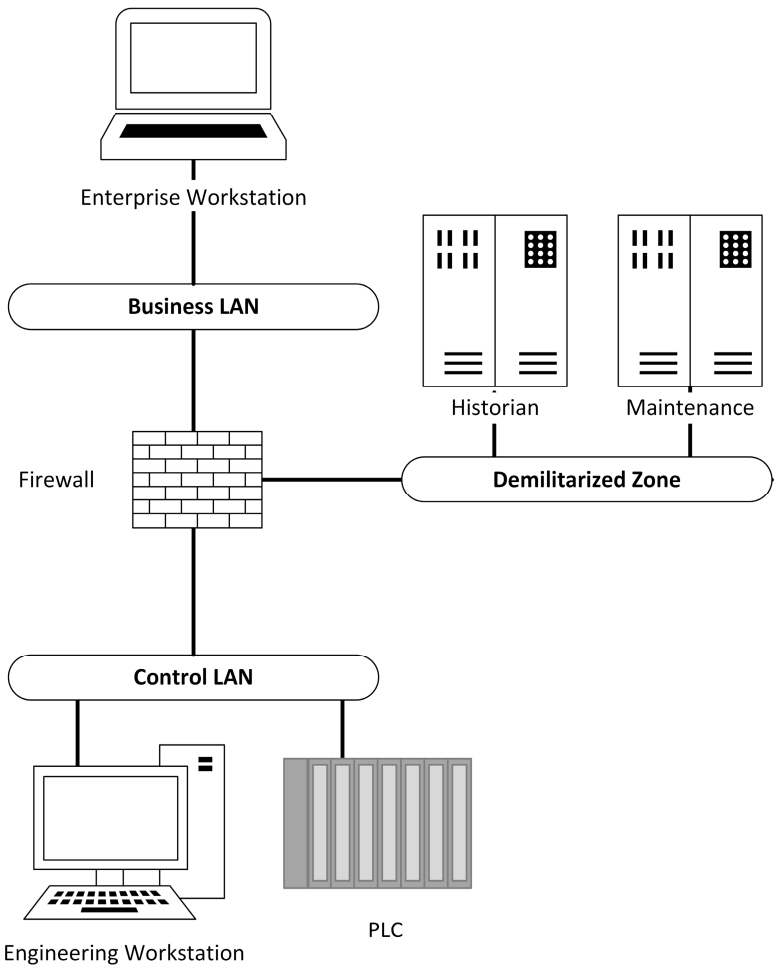


Figure 8-6 Example Network Architecture with DMZ (Single Firewall)

For optimum cybersecurity, two firewalls, ideally from different vendors, can be used. This makes it more difficult for an attacker to access the control system network, because even if they are successful in getting through the firewall from the IT network, they would need to gain entry through a second firewall type. The reference architecture drawing in Figure 8-7 illustrates this type of structure.

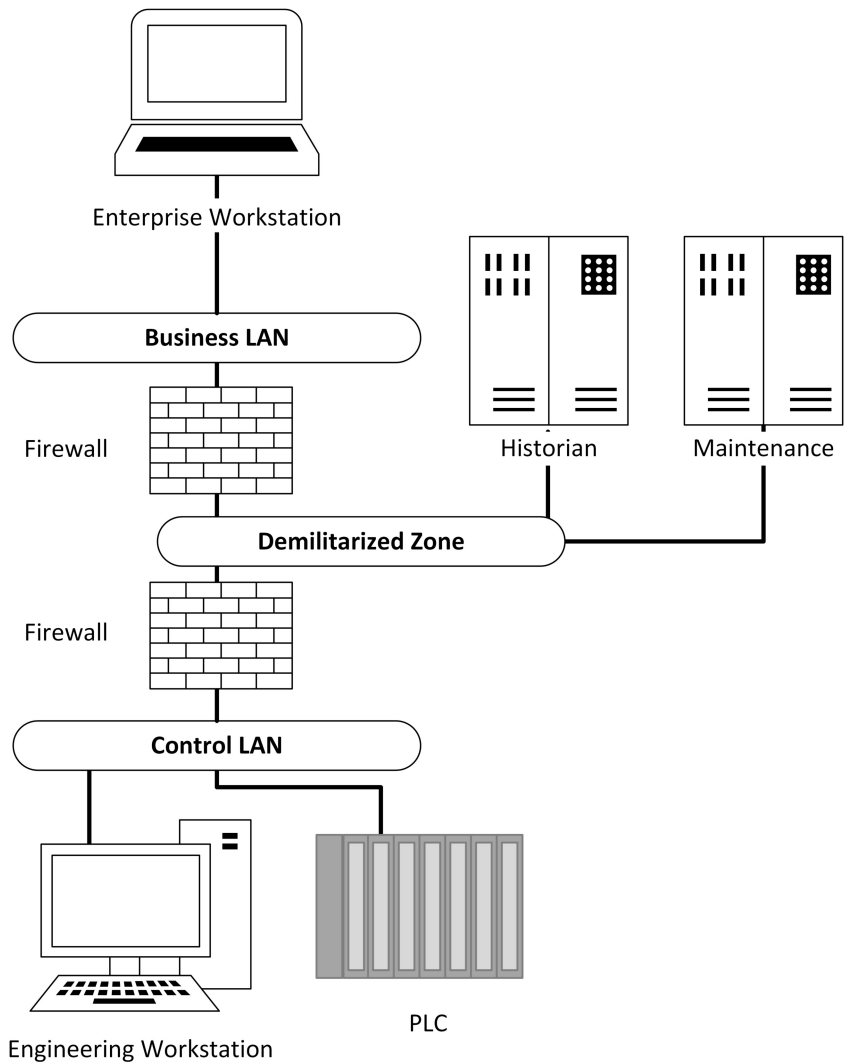


Figure 8-7 Example Network Architecture with DMZ (Dual Firewall)

Another network segmentation strategy that can be considered is the use of data diodes or unidirectional security gateways. Data diodes are a hardware device that ensures that network traffic can only travel in one direction. Typically, this is used to transmit information from a more secure zone (such as an IACS) to a less secure zone (such as the IT network), as shown in Figure 8-8. The benefit of a data diode is that it ensures a cybersecurity compromise of the less secure zone will not lead to a compromise of the more secure zone. A drawback of the data diode model is that many networks still require two-way traffic for operational purposes, so it may not be feasible to prevent any traffic from less secure zones to the IACS. In these cases, a data diode may still be beneficial for separating safety critical zones from the rest of the control network, as discussed in Section 8.4.2. Although data diodes provided a greater degree of segmentation between zones, they are not an infallible protection method. For example, security provided by a data diode could be unintentionally defeated by an insider setting up a temporary bypass connection (around the data diode) from the less secure zone to the more secure zone to transfer needed data from the less secure to the more secure zone.

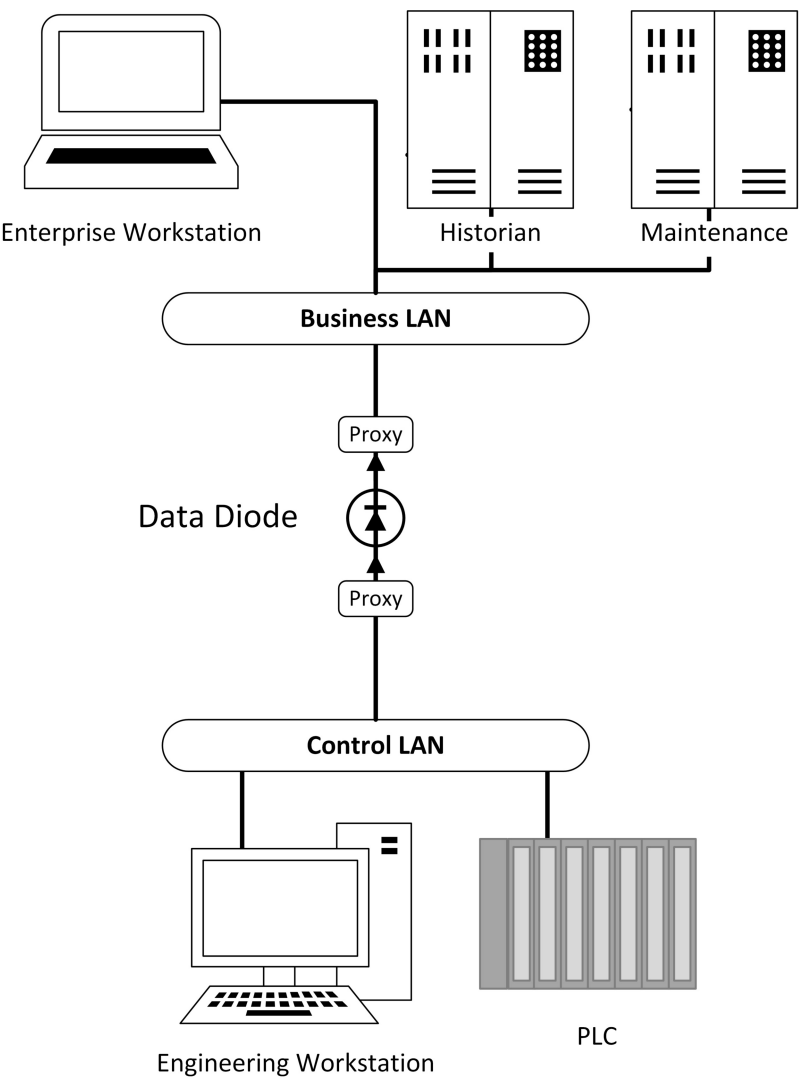


Figure 8-8 Network Segmentation with Data Diodes

8.4.2 Separating Safety and Control Systems

Network segmentation is not only important for protecting the IACS from compromises on the IT network, but also for separating zones with different security requirements within the control system. In some systems, the safety and control PLCs may share the same engineering workstation, as shown in Figure 8-9. In these cases, the engineering workstation can represent a single point of failure for both the control system and the safety system. This means that if an attacker gains access to the engineering workstation, they could not only disable safety productions but also manipulate control settings to trigger a hazardous event.

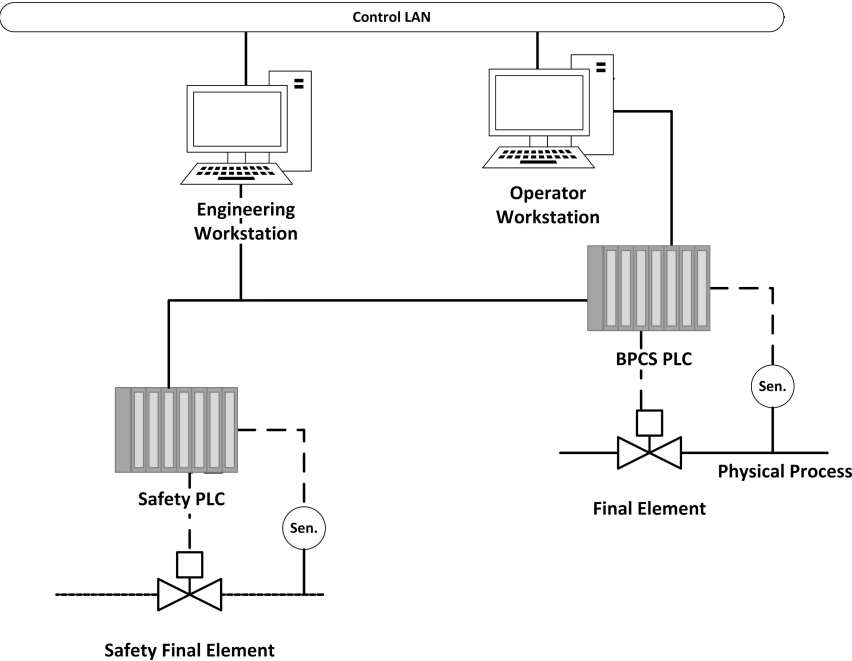


Figure 8-9 Combined Control and Safety Engineering Workstation

Where possible, safety critical elements of the IACS should be segmented from non-safety critical elements, as shown in Figure 8-10. This helps to reduce the chance that an attacker could compromise multiple elements from a single point in the IACS network, which is an important aspect of implementing the defense-in-depth approach. Using a firewall to segment the control and safety parts of the network can lead to improved security while still allowing required communications to the safety engineering workstation (e.g., anti-virus updates). When communications from external zones to the safety zone are not typically needed, a data diode could be considered to provide an even higher level of security, as indicated in the architecture shown in Figure 8-11.

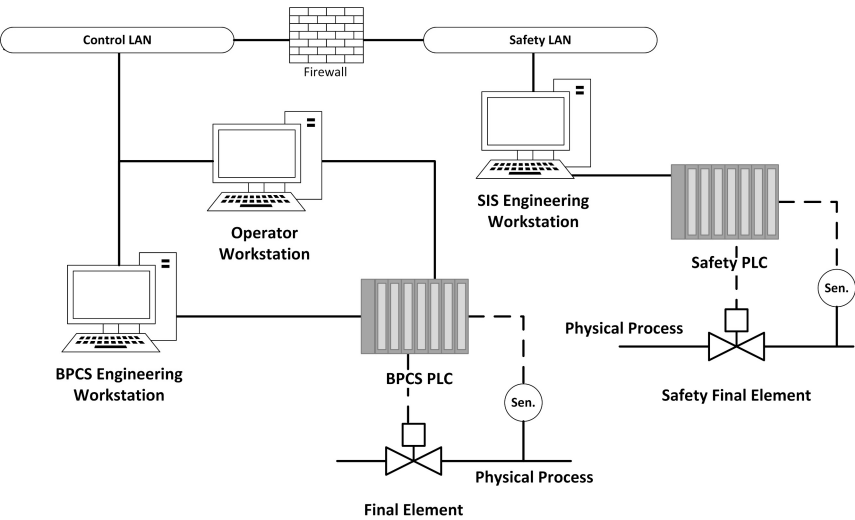


Figure 8-10 Separate Control and Safety Engineering Workstations

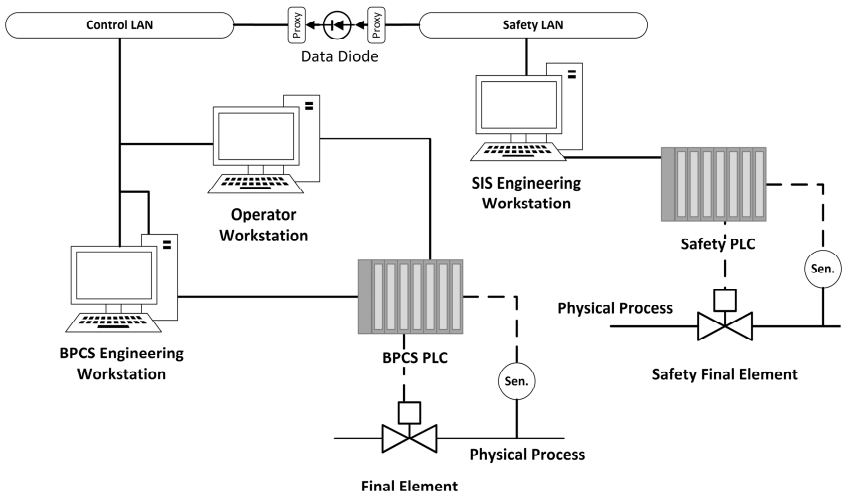


Figure 8-11 Separate Control and Safety Zones with Data Diode

8.4.3 *Securing Remote Access*

In 2019, approximately 70% of all IACS required at least some type of remote access [88]. With the ongoing increase in teleworking and the use of VPNs and Remote Desktop Protocols (RDPs), this percentage will only continue to grow. In the future, nearly all organizations will need to protect and secure remote access as a critical component of IACS systems. Strategies for securing remote access continue to evolve in an effort to protect against the potential for remote unauthorized access to hackers. Easy-to-implement steps such as configuring remote access programs for maximum security, minimizing the number of users with remote access credentials, only allowing company owned and maintained devices to connect remotely, and requiring multi-factor authentication (MFA) should be considered for all organizations with remote access.

Further industry best practices for securing remote access are built that is known as a jump host. This jump host is the only device that is allowed to establish remote access to the IACS and serves to limit the added exposure of the remote connection. The final connection from the jump host requires a second set of credentials and typically takes advantage of Remote Desktop Protocol (RDP) to provide two independent steps using diverse technology Figure 8-12.

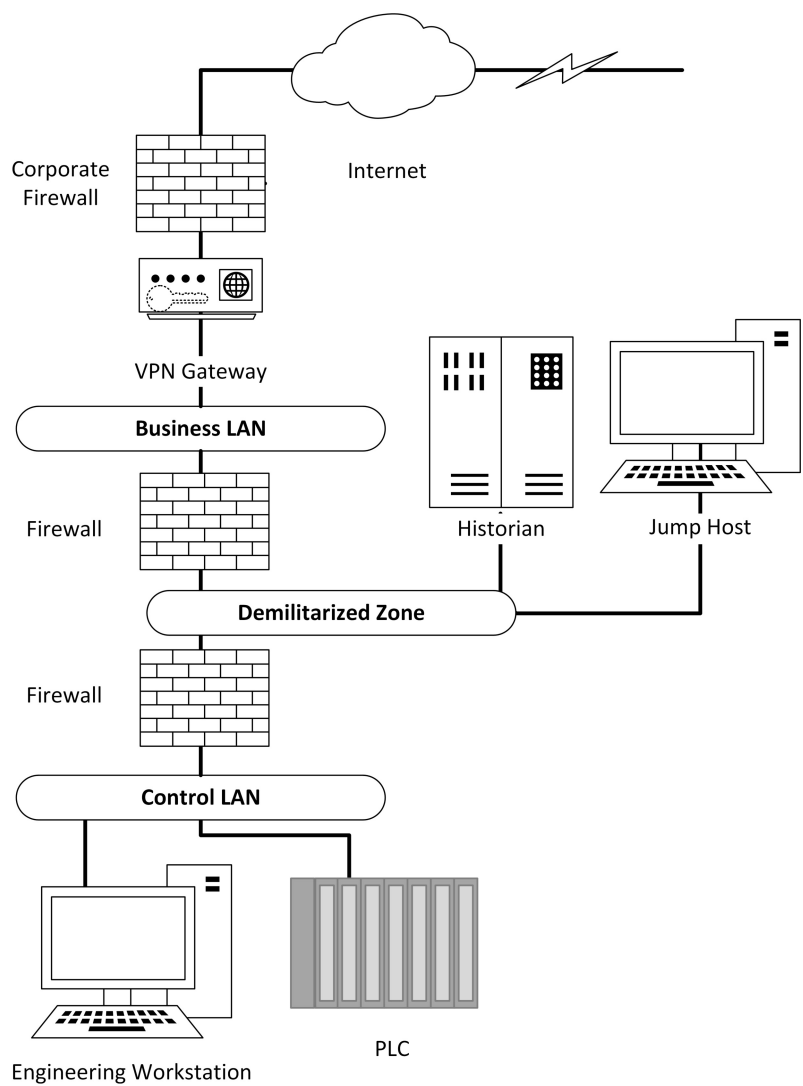


Figure 8-12 Multi-Step Remote Access to IACS Systems

Using a multi-step process for establishing remote access, paired with other strategies such as multi-factor authentication (MFA), carefully managed accounts, session recording, and one-click disconnection can allow organizations to meet operational and security needs. Ushered access, when onsite personnel must provide approval before a remote session can be

started, is another strategy that can be implemented to secure remote access. As the prevalence of remote access continues to grow, organizations must also become more sophisticated in implementing strategies to protect remote access to systems.

8.4.4 *Securing Continuous Remote Operations*

For many systems, remote access is used to provide better visibility into the operating process and allow for troubleshooting activities should any issues arise. However, there are a subset of applications that rely on remote access for continuous control functions. These include the remote operation of offshore platforms and the management of remote pipelines and terminals. The operating philosophy (how an organization plans to operate an asset) has a major impact on the design and network architecture for the remote site. The following questions are useful in defining the operational philosophy and requirements for the remote site:

- Where is the remote facility located?
 - o Is it close to the central control room?
 - o Is it on-shore or off-shore?
- What is the extent to which remote operations are used?
 - o Is remote monitoring used for process optimization (see Section 8.4.3)?
 - o Is the remote site operated fully remotely?
 - o What control activities are completed from the central control room?
 - o Does the process require continuous operators at the central control room?
 - o Are routine tasks automated?
 - o Can the remote site be fully started up and shut down without onsite manual intervention?

The operational philosophy will play a central role in the identification of the communication and network segmentation strategy for the remote site. For all remote sites, a robust communication strategy is needed to ensure the reliability, safety, and security of the remote operation. In many cases for offshore installations, subsea cables with single mode optical fiber are used to provide reliable communications [89]. In other applications, communication technologies such as line of sight communication (e.g., satellite communications, radio, and microwave) are used. As the name implies, a

physical line of sight is required between the signal transmitter and receiver for communications, which can lead to reduced reliability. Very Small Aperture Terminals (VSATs) are a specialized type of two-way satellites that have an antenna smaller than 3 meters and have the potential to offer a scalable and mobile system for network connections. Ultimately, the decisions on the communication medium and level of redundancy must consider the operational philosophy and required reliability of the application as well as the implementation cost.

One strategy to improve reliability is to implement multiple layers of redundancy. A redundant ring network has two layers of redundancy; the first is that two physical cables are used to connect each node or area of the network, the second is that each node of the network is connected to two other nodes. Connecting each node to two other nodes (in a ring or circle) ensures that loss of communication between any two nodes does not lead to an overall loss of communications. This approach is commonly used for fully remotely controlled offshore platforms is shown in Figure 8-13 [89].

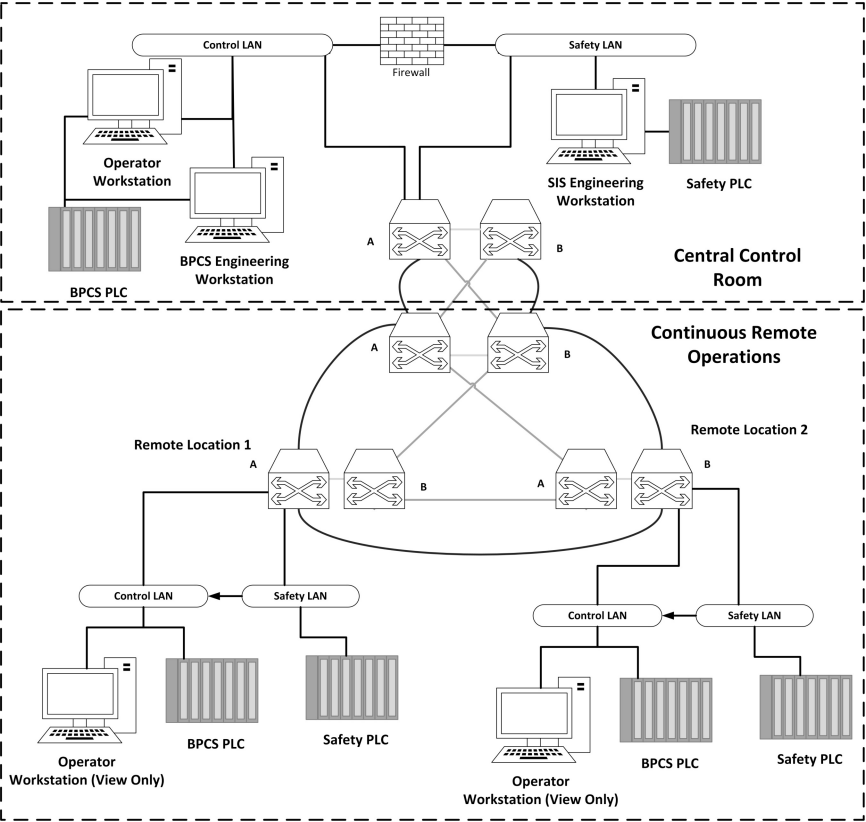


Figure 8-13 Ring Configuration for Unmanned Remote Operations

Regardless of the communication methods selected, it is important to consider the automatic actions taken by the system when communications are lost, possibly from a reliability issue or as the result of a DDoS type attack. Should the system automatically shut down or continue steady-state operation? This decision is often made based on the complexity of the system being controlled. If frequent setpoint changes or modifications from the central control room are needed it is typically safest to shut down the system automatically; however, if only infrequent modifications are made or the behavior of the remote system is well understood, it may be acceptable to allow operations to continue for a period of time. Depending on the action on loss of communications, a DDoS attack has the potential to trigger downtime and financial loss or to lead to potential safety or environmental consequences

if the remote site continues to operate without communications from the central control room.

In addition to considering the physical reliability of the communications with the remote site, it is also important to consider the logical connectivity between the remote site and the central site. One approach is to consider the continuous remote operations as a physical extension of the centralized process control network. For this approach, the network is not segmented between the central and remote locations; rather, segmented zones at the central site (e.g., control LAN and demilitarized zone) are extended to retain the separation of critical assets such as the example shown in Figure 8-14. This allows for a consistent network segmentation strategy to be achieved at the remote site with a single network cable and limits the potential for a boundary device located remotely to unintentionally block any needed communications. An important consideration when extending the logical zones is how to segregate communications to the remote site. Several possible segregation strategies can be considered, such as using separate physical channels (e.g., different cables), separate media channels (e.g., different frequencies), or separate logical channels (e.g., different addressing). The selection of channel segregation type should be based on the operational and risk-based requirements for the remote site [89].

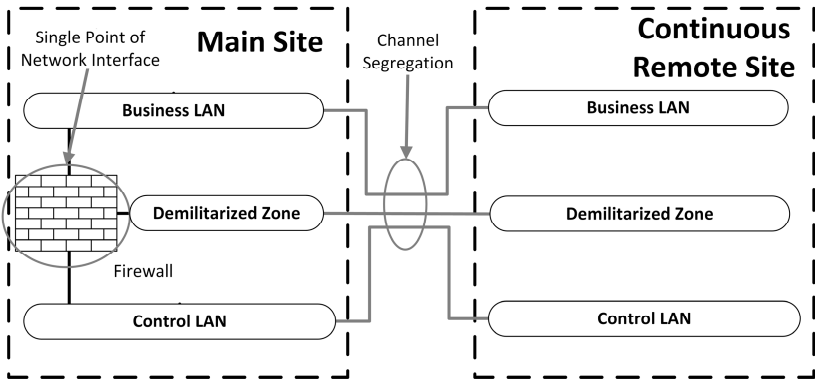


Figure 8-14 Extending Logical Networks to Remote Sites

In some applications (e.g., multiple remote terminals or pumping stations), it may be possible to implement network segmentation between the central and remote locations using a firewall or other boundary device. If this strategy is employed, it is important to consider where the firewall should be physically located (at the central location or at the remote site) as well as what steps should be taken to minimize the potential for the firewall to block necessary traffic between the central and remote sites. When a potential cybersecurity incident is identified (e.g., suspected ransomware, anti-virus alert, unusual traffic), a decision may be made to intentionally disconnect communications from the other zones to the control network for the main and remote sites. In these cases, it is important to have incident response plans (see Section 10.17) that define how to disconnect communications and what types of scenarios warrant this level of response.

Similar to the way that having more devices or applications connected to the control network at a single site increases the overall attack surface by providing more opportunities for an attacker to gain access, extending the control network to remote locations not only provides more connected devices that can be targeted but also provides a separate physical location where an attacker may be able to establish access. Physical security is a double-edged sword for normally unmanned operations. On one hand, it is often difficult to physically gain access to the site, and there is a lower likelihood of an internal unintentional incident at the remote location leading to an incident. On the other hand, during the times when maintenance personnel and vendors are present, there may be less oversight to monitor for potentially malicious activities. To help manage the risk of physical security issues at remote sites, closed-circuit television (CCTV) cameras or video surveillance can be used to provide live monitoring.

Ensuring the security of continuous remote operations is needed to prevent attackers moving laterally from the central location to remote assets as well as from remote assets to the central location. Although the geography and architecture for continuous remote operations are different from standard IACS, the security fundamentals from this chapter need to be applied to continuous remote operations in the same way as a traditional (non-remote) site. Defense-in-depth protections that consider the network segmentation, control of access accounts, multi-factor authentication, system

hardening (Section 8.5), and security monitoring (Section 8.6) are needed to ensure continued safe and secure operations. In particular, establishing a baseline for network communications of the remote asset and implementing an effective security monitoring solution are important steps in provide visibility into the current state of the remote site to operators or security personnel at the central location. This allows for an effective incident response plan to be developed and for actions to be taken to minimize the impact of a potential compromise at the remote location. Additional security protections that should be considered for continuous remote operations are the use of view only operator workstations at the remote site, screen savers and automatic screen locking after a defined period of inactivity, and unique operator accounts for improved tracking of changes made to the remote system.

8.4.5 Types of Connectivity

Another emerging trend for both IT and OT systems is the growing connection of Internet of Things (IoT) devices or physical devices connected to the internet. IoT first began with consumer products such as smart thermostats, lighting fixtures, and home appliances that leverage real-time sensors, monitoring, analytics, and machine learning to improve performance. Although the possible performance benefit is positive, IoT has the same security and privacy concerns with growing connectivity discussed previously. The poor system hardening of traditional IoT devices was clearly highlighted in the Mirai Botnet attack, when hundreds of thousands of IoT devices were compromised and used to execute DDoS attacks [49].

In some cases, IoT devices can even be used to gain access to connected networks. In 2017, attackers were able to steal 10 gigabytes worth of data from a North American casino after gaining initial access to a fish tank control system [90]. The new fish tank smart system was connected to a network via a PC and had multiple sensors regulating parameters such as tank temperature, cleanliness, and food [91]. It is likely that the organization was not aware of the full functionality of the smart sensors and did not disable internet access or provide sufficient protective measures. This made the fish tank the easiest entry point into the network.

When IoT devices are used in automation networks, they are often referred to as Industrial IoT (IIoT) or as the Internet of Automation (IoA). The use of smart sensors or position monitors in industrial applications has the potential to offer performance benefits but introduces additional cybersecurity concerns at Level 0 of the reference model (see Section 1.3). A misconfigured wireless smart transmitter, or a transmitter with a default web server that has not been disabled, could be used as an entry point to the OT network in much the same way that the fish tank sensors were used to gain access to the Casino's network. If a decision is made to use IoA equipment, increasing the attack surface, it is important that the steps for network segmentation and system hardening are taken to make the application as secure as possible.

8.5 *System Hardening*

System hardening is another important aspect of inherent security. System hardening is the practice of applying tools, techniques, and best practices to reduce system vulnerabilities and the attack surface that can be exploited by an attacker. It involves locking down the functionality of the various components in the IACS to prevent unauthorized access or changes, removing unnecessary functions or features, and patching any known vulnerabilities. This is especially important in modern control systems which utilize extensive commercial off-the-shelf (COTS) technology. In such systems, it is critical to disable unused functions and to ensure that configurable options are set to their most secure settings.

COTS Windows machines are a common choice for engineering and operator workstations; however, often many unnecessary applications and services are included in the default installation. These unnecessary applications should be removed for a control system application (e.g., default games, blue tooth, wireless connectivity, Microsoft Office programs). It is also important to disable or block unused or unnecessary communication interfaces and the services available on those interfaces.

Workstations and servers are not the only components of a control system that require hardening. Network equipment and embedded control products also require secure configurations, blocking of unused communication interfaces, and software maintenance. If network

segmentation is the key for minimizing the network attack surface, system hardening is essential for reducing the attack service of control system hardware and software. The final element of inherent security for IACS systems is the people provided access. Proper access control and cybersecurity awareness training are the most important steps for reducing this attack surface.

8.5.1 *Patch Management*

Patch management is an important layer for defense-in-depth; it allows organizations to mitigate known vulnerabilities in the operating systems and applications installed on the IACS. Patches or software updates are used to correct security vulnerabilities, fix errors in the previous software version, and introduce new functionality. In many case histories, such as the WannaCry Ransomware (see Chapter 2) and NotPetya Wiper Worm (see Section 6.5) incidents, the malware exploited known vulnerabilities (which had patches available) to gain access and spread across IACS systems. Had these systems been at the most current patch level, the malware from these attacks would not have been able to infect the system; this would have prevented the incident and resulting consequences.

Although patching can prevent significant security consequences, new patches cannot be automatically deployed to the IACS environment without risking a disruption of operations. The potential to negatively impact the availability of operations is why many IACS systems are patched infrequently. While automatically deploying patches in the process environment is problematic, it does not remove the need for patch management. Patch management practices instead need to balance the needs for both availability and security consistent with the site's operating philosophy and consider what additional protection layers are in place for a device. For example, a device that has multiple protection layers such as segmentation in an isolated part of the network, monitored for suspicious activity, and with whitelisting applied would have a lower patch priority, than a similar device without protections.

Effective patch management starts with an understanding of what vulnerabilities exist in the IACS. A risk-based approach is then applied to compare the benefit of correcting the vulnerability to the risk of the patches leading to an availability issue and determine if the patch should be installed.

Before patches are deployed on an IACS, they need to be reviewed and approved by the IACS vendor to confirm that the changes in the patch are compatible with the control system application. After the patch for a known vulnerability has been released and approved by the vendor, sites should track the level of risk from the vulnerability in the system as a key factor in determining when to patch.

One commonly used practice to limit the availability concerns from patching is to adopt a tiered approach. In a tiered approach, the order in which patches are installed is based on the criticality of the asset. Commonly used criticality levels include "Operations Critical" and "Early Adopter." Early adopters are devices in a test environment or on a less critical part of the control network, where an unexpected interaction between the patched system and the control system would not trigger a downtime event. After a patch has been successfully installed on early adopter systems for a predefined period without negative impacts, it can then be installed for operations critical assets. Some organizations may use additional criticality categories to further define the order in which patches are applied.

8.5.2 *Anti-Virus*

An analysis of the IACS threat landscape showed that the number of malware related incidents rose between 2018 and 2019, with an increase in attacks involving both ransomware and malware designed to bridge the gap from IT systems to IACS [88]. Another survey conducted in 2019 saw that malware related attacks were viewed as the number one threat for IACS, with 70% of organizations identifying ransomware/ malware as a major concern [5]. These results underscore that malware presents a continually present risk to IACS and has the potential to result in significant downtime, financial losses, and even safety concerns.

Anti-virus and other endpoint protection strategies are designed to protect IT and IACS assets from known malware attacks by maintaining an up-to-date blacklist of malicious programs which are prevented from running. This type of protection from malware is an important element in system hardening and can reduce the probability of a known attack resulting in a loss event.

Unfortunately, the use of anti-virus for IACS poses two primary challenges: it is only effective against known attacks added to the blacklist and many companies do not use anti-virus software on their IACS computers. The first challenge limits the effectiveness of anti-virus against novel or new attacks, including attacks that exploit zero-day vulnerabilities. Additionally, if the virus definitions are not frequently updated, the anti-virus software will become significantly less effective for even current known attacks that are not being added to the blacklist. For the second challenge, IACS system administrators may be hesitant to deploy anti-virus software for several reasons. One of the primary concerns has been system reliability and the potential for additional software on the IACS to cause availability issues. Although this has been a valid concern in the past (particularly for older legacy systems), the stability of anti-virus management has improved significantly, and nearly all major IACS software suppliers now have tested, qualified, and approved anti-virus software that can be used on their Windows-based platforms.

The benefits of running anti-virus software on IACS hosts typically outweigh the risk that the anti-virus software will have a potential negative impact on the system availability. However, continued support and updates of the anti-virus software is needed to maintain it as an effective layer for defense-in-depth. Following a regular virus definition frequency is an important step in maintaining the effectiveness of the software. Staggering the deployment of anti-virus updates between non-critical and critical systems (similar to patch management) can further reduce the likelihood of a potential negative impact on availability.

8.6 *Security Monitoring*

Although steps like network segmentation and system hardening can help to reduce the attack surface of the IACS, it is often not possible to fully mitigate the potential for cybersecurity compromise. As such, organizations with a mature cybersecurity approach also focus on measures to identify anomalous network activity that could be an indication of a cybersecurity event. Effective detection and emergency response (additional information provided in Section 10.17) can help to identify an initial cybersecurity compromise before it escalates into a major negative safety or financial event.

Several technologies are currently being used to monitor unusual activity for IACS including:

- Intrusion Prevention/ Detection Systems
- Network Monitoring
- Continuous Security Monitoring
- Security Information and Event Management

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are commonly implemented in combination with a firewall at the entry points to critical zones. IDS is a security service that monitors and analyzes system events for the purpose of finding and providing real-time or near real-time warning/ alarms of attempts to access system resources in an unauthorized manner. IPS are similar to IDS in that they monitor and analyze system events to detect potential unauthorized access, but they have the added feature of automatically blocking potentially malicious communication. Although this feature can provide an added cybersecurity benefit, organizations should be cautious when implementing IPS because intrusion detection can be prone to a high rate of false positives; this can lead to blocking necessary network traffic and potentially impacting the availability of the system. A number of commercially available IDS/IPS protections as well as some free open source options. One such open source option is Open Source Security (OSSEC), which provides intrusion detection capability, log monitoring, and file integrity monitoring to support the identification and response of potential security events [92]. For many organizations where security monitoring is not currently in place, the use of open source tools can provide a way to kickstart their monitoring capability.

Another option for security monitoring is the completion of periodic network scans. The objective of network monitoring is primarily to identify cybersecurity incidents that require a response, and in some cases can support a secondary goal of maintaining an up-to-date asset inventory. Network monitoring can be either passive or active. Passive monitoring captures and analyzes live network traffic and doesn't require the generation of any additional network traffic, meaning there is no risk of disrupting essential processes on the IACS. Passive monitoring programs do take longer to analyze the entire network as they need to wait for traffic to be generated

to or from each device; however, passive network monitoring can be run continuously and evaluated at a set frequency. Wireshark is an open source and widely used protocol analyzer that provides detailed visibility into network traffic. It uses only passive scanning techniques and can support live data capture and later offline analysis [93].

Active monitoring works by generating test traffic on the network to gather basic profile information. This allows for faster results but does have the potential for disruption of the IACS, particularly for legacy components that may be sensitive to network traffic. NMAP or “Network Mapper” is an open source, commonly used active scanning tool that can discover what hosts are connected to a network, their services, operating system, and other characteristics [94]. When employing either passive or active monitoring, it is useful to have a baseline of the typical network traffic that can be used to determine if the latest scans indicate any unusual activity.

Continuous security monitoring is slightly different than network monitoring in that it tends to be more focused on identification of cybersecurity vulnerabilities and primarily supports an up-to-date asset inventory and detection of any potential security concerns in the current software version or configuration. It may also provide indication of cybersecurity threats such as unapproved changes or modifications to an IACS asset; however, it is not as focused on threat detection as network monitoring. Many organizations are now adopting a combined approach of both network monitoring and continuous monitoring to improve visibility into both the systems vulnerabilities and potential cybersecurity incidents.

Security information and event management (SIEM) systems are another method for detecting unusual activity on the IACS. SIEMs take advantage of logs that are already generated (from nearly every device on the IACS) to analyze network conditions and correlate them with possible cybersecurity events and threats. Once potential threats are identified, they can be used to generate automatic alerts and trigger an investigation into the potential issue. SIEM reports are another feature that allow organizations to better track how their system performance is changing over time. Common features in SIEM systems and a description of the usefulness in cybersecurity monitoring are provided in Table 8-4 [95]. Security Onion is another free tool that combines

network intrusion detection with a full range of SIEM capabilities; it can be a good first step for organizations considering implementing a more robust approach for monitoring [96].

Table 8-4 Typical SIEM Features and Descriptions

Typical SIEM Features	Description
Log Management	Logs are generated from many devices on the IACS including workstations, network devices, and controllers. Collecting, standardizing, and monitoring log activity is the basic function of SIEM systems.
Event Correlation	Cybersecurity threats typically affect multiple parts of the IACS. SIEMs can identify unusual behavior from multiple different logs and correlate them into a single cybersecurity event.
Identification of Threats	SIEMs can generate alerts when cybersecurity events are identified. These alerts can be fed to a Security Operations Center (if one is in place) or to the network architect responsible for the IACS system.
Threat Intelligence	Many SIEMs now include the capability of incorporating ongoing threat intelligence into their monitoring and threat identification behavior.
Reporting	SIEMs typically offer customizable reports that allow for network architects to have improved visibility into network activity and can improve the tracking of network behavior and cybersecurity metrics.
Incident Response	SIEMs are effective at collecting information related to potential cybersecurity incidents. This can support both the initial identification and response to a cybersecurity incident, as well as support the detailed incident investigation once the immediate threat has been resolved.

Security monitoring can be an important step in implementing a defense-in-depth approach and responding to any cybersecurity incidents that make it past perimeter defenses. Additional information about how organizations are continuing to adapt their security monitoring approach and implement more robust response activities is provided in Section 12.1.2.

8.7 *Risk Compatibility Assessment*

At their core, both cybersecurity and process safety risk management are fundamental to ensuring the continued safe operation of industrial sites. Without security there is no safety, and if attackers are able to easily access and compromise safety critical systems, it is likely that the process facility affected has significant unmitigated risk that it may not have identified. In this way, there is a basic synergy between cybersecurity and process safety risks.

In general, actions taken to improve the cybersecurity of an OT system will reduce the likelihood of compromise of safety critical systems and thus support the reduction of overall risk. However, in some cases, additional security protections can have an inverse effect on achieved safety. If the resource requirements for additional security protections such as real time monitoring, frequent patching, and advanced anti-virus protection consume a large enough portion of a safety critical system's processing capacity, the response time of that safety system - or its ability to function normally - can become negatively impacted. Additionally, sometimes security protections, such as Intrusion Prevention Systems (IPS) that automatically block traffic believed to be malicious or automatic log-off requirements for operator workstations, have the potential to delay site personnel from completing safety critical tasks. This highlights that, although there is synergy between the processes and approaches for cybersecurity and process safety management, the potential also exists for conflict between cybersecurity countermeasures and critical safety functions. Any potential adverse effects to critical safety functions need to be documented in the Cybersecurity Requirement Specification (CSRS), to ensure that the impact is clearly documented, and reviewed to ensure that it does not affect the achieved safety of the system. If it is determined that a negative impact on overall safety is caused, a suitable alternative cybersecurity protection should be evaluated.

The potential conflict between advanced cybersecurity measures and safety requirements further emphasizes the need for inherent security in OT systems. It is likely not possible to implement all protections necessary to achieve tolerable risk if OT systems are connected directly to internet-facing systems without network segmentation and/or adequate protection. Additionally, system hardening and restriction of access following the least privilege principle help to further reduce the attack surface of the network to make it inherently more secure. Engineered layers of protection and administrative procedures remain core steps for achieving tolerable cybersecurity risk, but they cannot be solely relied upon to achieve cybersecurity.

Although total isolation of the OT network may at first appear to be the most inherently secure solution, the inability to patch known vulnerabilities, make configuration updates, and transfer important data to enterprise systems likely outweigh the initial benefits. When addressing the question of how to connect OT systems, it is important to retain a risk-based approach. Security decisions regarding a small manufacturing site with limited hazardous material may vary drastically from security decisions for a large petrochemical facility processing explosive components. No single best network architecture or system hardening practices will apply to all OT systems; there is a diversity of OT technology, applications, and industries - and no "one fits all" solution.

Instead, companies need to understand the potential security risks and operational benefits of the connections between traditional OT and IT systems and make strategic decisions about how to manage this risk and achieve operational goals. By defining what connectivity is required and limiting access to only those users and applications that require it, companies can make systems as inherently secure as possible. The remaining risk reduction required can be achieved following a defense-in-depth approach for security protections. How many security layers are required, and how effective do they need to be? These are two important questions that will be addressed in Chapter 9, when methodologies for analyzing and quantifying cybersecurity risk are introduced.

8.8 *Summary*

Just as process safety uses a hierarchical approach using the principles of inherently safer design, cybersecurity risk mitigation also focuses on improving the inherent security of a system design to achieve cybersecurity objectives. Although extreme isolation for OT networks is not sustainable, taking steps to reduce a system's attack surfaces by limiting the number of users with access, network connected devices, and applications on the system is a key step. The techniques of defense-in-depth, network segmentation, system hardening, and security monitoring are critical to ensure that, as OT systems in many industries become more connected, safety and security objectives can be met.

9 Hazard Identification and Risk Analysis (HIRA)

Understanding cybersecurity hazards and managing risk are key to preventing cybersecurity events. Without an appreciation for Hazard Identification and Risk Analysis, companies will be unable to allocate resources to the most effective protections or determine if currently implemented protections have achieved tolerable risk. Identifying potential cybersecurity hazards and estimating risk can be a difficult undertaking for OT systems due to a number of factors, including:

- Misconceptions about cybersecurity as it relates to the process industry
- Limited industry databases on cybersecurity events
- Rapidly changing technology
- Continually evolving threat landscape

Although it can be challenging to assess cybersecurity risk, some techniques have been developed. While similarities exist between techniques for assessing process safety and cybersecurity risk, the contributors to risk are somewhat different. In process safety, risk is assessed based on the likelihood of a hazardous event occurring and the potential consequence of the event (based on the process hazards present). In cybersecurity, risk is assessed based on four key factors:

- Threat likelihood
- Vulnerabilities
- Target attractiveness
- Consequence severity

Several techniques will be discussed in this chapter to assess cybersecurity risk based on these four key factors.

One of the first steps in evaluating cybersecurity risk is to select the correct technique for the study. A number of different assessment techniques may be selected based on the objective of the assessment (Risk Identification or Design Confirmation) and the level of detail (Quantitative or Qualitative). Typically, when process sites are completing cybersecurity risk assessments, the main objective is to identify potential cybersecurity risks. In some cases, when equipment manufacturers or system integrators complete cybersecurity

risk assessments, the intent is to demonstrate that the planned design conforms to or achieves a certain level of security based on international standards or industry best practices. The results of the design confirmation can take the form of a documented security capability or as recommendations for standard countermeasures and configuration steps to be taken. For either outcome, the design confirmation can help to jump-start the asset owners risk assessment process by providing a clear system basis. Depending on the desired level of detail for the risk assessment, qualitative methods that provide categorization of cybersecurity risk such as high, medium, or low may be granular enough to support the risk-based approach. In cases where a more detailed understanding of the current cybersecurity risk is desired, quantitative (or semi-quantitative) techniques can help to define the likelihood of a successful cybersecurity incident and the expected impact on the system. Figure 9-1 maps cybersecurity risk assessment methods based on the focus of the study and the level of detail:

	Quantitative	Qualitative
Risk Identification	Bow Tie, Semi-Quantitative SL Verification, QRA Use Cases: • Determine likelihood of security events • Determine consequence severity	Cyber HAZOP, Checklist, Cyber-FMEA, Threat Analysis Use Cases: • Document potential sources of compromise and mitigation
Design Confirmation	Quantitative Threat Modelling Use Cases: • Verify appropriate resilience in component/ system design	Checklist, Cyber-FMEA Use Cases: • Identify weak points in system design and potential mitigation

Figure 9-1 Determining the Scope of Cybersecurity Assessments

The remainder of this chapter will focus specifically on risk identification techniques. Additionally, these techniques will be grouped based on the granularity of assessment, with qualitative techniques being presented in Section 9.2 and quantitative techniques being presented in Section 9.3.

9.1 Use of Process Safety Tools to Identify and Manage Cybersecurity Risk

In many cases, process safety tools and techniques can be readily applied to cybersecurity risk management. By leveraging existing process safety tools, companies can conduct an evaluation of cybersecurity scenarios without reinventing the wheel and developing a new methodology. In fact, many of the methods used to evaluate and manage cybersecurity risk are directly based on process safety equivalents, as shown in Table 9-1.

Table 9-1 Process Safety and Cybersecurity Techniques

Process Safety	Cybersecurity	Section
Process Hazard Analysis (PHA)/ Hazard and Operability Study (HAZOP)	Cybersecurity HAZOP	9.2.1
Checklist (e.g., facility siting)	Cybersecurity Checklists	9.2.2
Failure Modes and Effects Analysis (FMEA)	Cybersecurity FMEA	9.2.3
Bow Tie	Cybersecurity Bow Tie	9.3.1
Layer of Protection Analysis (LOPA)	Semi-Quantitative Security Level Verification	9.3.3
Quantitative Risk Analysis (QRA)	Quantitative Risk Analysis (QRA)	9.3.4

Some techniques can be directly applied to both process safety and cybersecurity analysis, such as consequence modeling and quantitative risk assessment (QRA). Coordination between the process safety and

cybersecurity teams can ensure that each type of HIRA activity is completed once, and the results are communicated to both parties.

In other cases, such as PHA/HAZOP or LOPA, process safety techniques can be modified to evaluate cybersecurity scenarios. HAZard and OPerability studies (HAZOPs) are a commonly used technique to assess the process hazards for industrial sites. The technique is based on using pre-configured guidewords to determine the possible causes and ultimate consequences of a process upset. For Cybersecurity PHAs/ HAZOPs, the guideword approach is adapted to identify potential causes of cybersecurity compromise.

The Venn diagram in Figure 9-2 shows similarities and differences between the process safety and cybersecurity approaches to risk management. Process safety risk assessment typically focuses on process control deviations, equipment failures and human performance issues as the primary causes of deviations and considers safeguards such as Safety Instrumented Systems. Cybersecurity risk assessment focuses on cybersecurity compromise as the initiating event and considers countermeasures as protective functions. In cybersecurity, Security Levels (SL) can be used to formalize the requirements for countermeasures. Security Levels are similar to Safety Integrity Levels (SIL) used in functional safety and represent order of magnitude improvements in cybersecurity protection from SL 1 being the lowest to SL 4 being the highest.

In addition, it is also important to understand the potential for common cause failure of multiple systems. In process safety, common cause failures typically result from a systemic issue such as plugging of a pressure sensor taps and plugging of a vent line. Cybersecurity attacks can also lead to common cause failure, such as by compromising both control and safety protections from a shared engineering workstation. However, cybersecurity driven common cause failures have the potential to occur even more frequently, because they are the result of an intentional action taken by an attacker.

Both cybersecurity and process safety risk assessment follow similar core principles such as a guideword-based methodology and the definition of worst-case consequences. Additionally, some information defined in process safety risk assessments can be directly translated to cybersecurity risk

assessments. For example, safeguards not susceptible to cyber-attacks, such as mechanical pressure relief devices, can be considered as effective protections in both analyses. A pressure relief device will reduce the likelihood of overpressure and vessel rupture whether the cause is a process upset or a cybersecurity incident. Likewise, conditional modifiers from a LOPA study, such as the probability of ignition or of someone being present when a hazardous event occurs, are generally still applicable to cybersecurity scenarios.

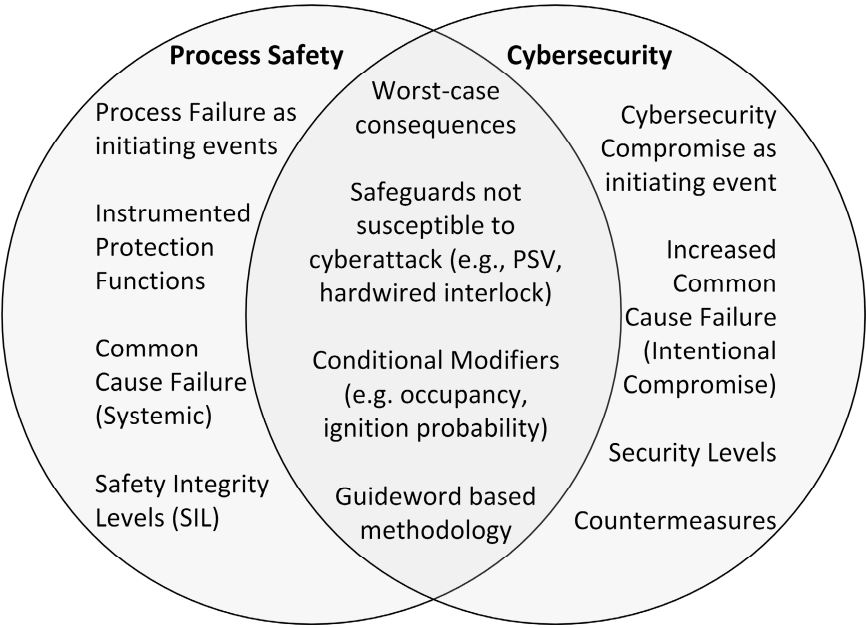


Figure 9-2 Process Safety and Cybersecurity Analysis Considerations

9.2 Qualitative Methods

Qualitative methods for hazard identification and risk analysis use categories to estimate the likelihood and consequence severity of cybersecurity events. These categories can help to identify how well cybersecurity risks are being mitigated and are often an important first step in addressing cybersecurity risk. Typically, qualitative methods are most effective for hazard identification and can be applied to a variety of scenarios and applications. In cases where

a more detailed understanding of a scenario is required, it can often be beneficial to pair a qualitative method with one of the more quantitative approaches presented in Section 9.3. Many methods for identifying potential hazards have been defined for process safety and other types of risks, ranging from predefined checklists to component-level assessments. In this section, four qualitative methods for hazard identification and risk analysis of varying granularity will be introduced:

1. Cybersecurity PHA/ HAZOP
2. Cybersecurity Checklists
3. Failure Modes and Effects Analysis (FMEA)
4. Cybersecurity Vulnerability Analysis

9.2.1 Cybersecurity PHA/ HAZOP

When the need for cybersecurity risk assessments was initially identified for industrial automation systems, the PHA/HAZOP methodology was one of the first methodologies considered. A HAZOP-based approach is introduced in the IEC 62443-3-2 standard Security Risk Assessment for System Design [97]. In this approach, the risk assessment is split into two components: the initial risk assessment and detailed risk assessment.

9.2.1.1 Initial Risk Assessment

The initial risk assessment focuses solely on consequence determination to identify the most critical assets requiring protection. This is an important step in determining the best network segmentation strategy for an OT network and can be completed following the methodology in Figure 9-3. A detailed example of how to complete the initial risk assessment is presented in Appendix B.

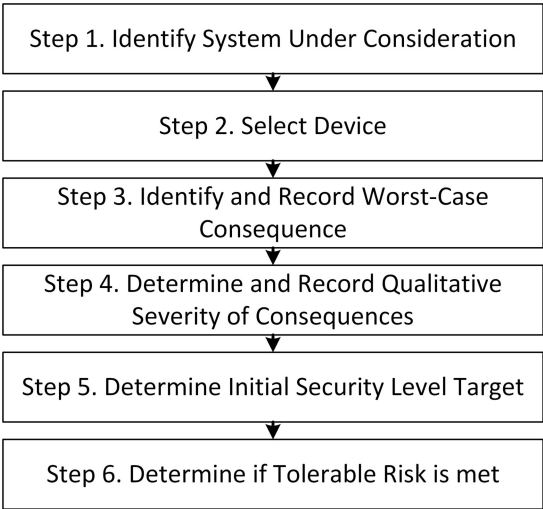


Figure 9-3 Initial Risk Assessment Methodology

Step 1: Identify the System Under Configuration

The first step is to identify System Under Consideration (SUC) or the scope of the assessment. Clearly defining which systems within the Industrial Automation and Control System (IACS) are being reviewed as part of the current risk assessment is important for bounding the study. IACS typically contain at least one control system zone, but larger sites may contain many.

Step 2: Select the Device

Once the scope is clearly defined, a specific device is selected to be the focus of a multi-step analysis. A cybersecurity device or asset is any computer-based or programmable device that is connected to the IACS. Examples of cybersecurity assets include engineering workstations, operator workstations, programmable logic controllers, servers, and network equipment.

Step 3: Identify and Record the Worst-Case Consequence

Consequences are considered for each device individually, excluding countermeasures, with the following assumptions:

- There is no response from a control system or operator in response to this failure.
- All countermeasure devices failed (e.g., firewalls, anti-virus scanning).
- The equipment fails if its design limits are exceeded.

Similar to process safety risk assessments, it is important to determine the worst-case unmitigated consequence. In many cases, cybersecurity compromises can trigger the hazard scenarios that are considered in the process safety assessment. Referencing the results of previous process risk assessments helps to ensure consistency between assessments and supports the accurate determination of risk.

Step 4: Determine and Record the Qualitative Severity of Consequences

Once the consequence is clearly defined, the severity of the consequence is determined for each applicable element of risk (e.g., safety, environmental, financial) based on the corporate risk criteria.

Step 5: Determine the Initial Security Target Level

The consequence severity and likelihood rankings, based on the assumed probability of compromise of one or a threat likelihood of once per year (see Chapter 3), determine the risk ranking for the device (Table 9-2, Table 9-3, and Table 9-4). Numbers between 1 and 16 are used to identify different levels of risk in the risk matrix (Table 9-4). The specific numerical values used in the risk matrix are commonly used as a way to communicate the organization's risk tolerance and will vary from organization to organization. This risk ranking can be coordinated to the four IEC 62443 security level targets introduced in Chapter 7 that provide increasing orders of magnitude for cybersecurity protection requirements. An example of how to coordinate risk ranking with example corporate risk criteria and security level is shown in Table 9-5.

Table 9-2 Example Severity Matrix

Severity Level	Severity		
	Business	Environment	Safety
1	Compromise resulting in negligible impact. (Less than \$50K)	Compromise resulting in negligible impact.	Compromise resulting in negligible impact.
2	Interruption of authorized user access resulting in minor business consequence. (\$50K to \$1M)	Interruption of authorized user access resulting in minor environmental impact.	Interruption of authorized user access resulting in minor safety impact.
3	Critical information stolen or locked from authorized users with moderate business consequence. (\$1M-\$25M)	PC affected resulting in temporary release and cleanup within weeks.	PC affected resulting in recordable injury.
4	Significant business consequence. (\$25M-\$100M)	Temporary damage to the environment and cleanup with months to a few years.	Single on-site fatality.
5	Severe business consequence. (Greater than \$100M)	Severe damage to the environment, cleanup greater than a decade.	Multiple on-site fatalities.

Table 9-3 Example Likelihood Matrix

Level	Likelihood
	L
VL	Very low, 10 ⁻³ per year or less
L	Low, 10 ⁻² per year
M	Medium, 10 ⁻¹ per year
H	High, 1 per year
VH	Very High, 10 or more times per year

Table 9-4 Example Corporate Risk Matrix

Risk Matrix		Severity Level				
		1	2	3	4	5
Likelihood	Very High	5	9	12	13	16
	High	4	8	9	12	13
	Medium	4	5	8	9	12
	Low	1	4	5	8	9
	Very Low	1	1	4	5	8

Table 9-5 Risk Ranking to Security Level Target

Risk Ranking	Security Level
Minimal (1-4)	Security Level 1
Moderate (5-8)	Security Level 2
Significant (9-12)	Security Level 3
Severe (13-16)	Security Level 4

Step 6: Determine if the Tolerable Risk Criteria are Met

For each device, the current risk ranking is reviewed to determine if it is tolerable. Based on the rankings in these tables, devices determined to have minimal risk would not require further investigation, whereas devices with significant and severe risks would require additional investigation in the detailed risk assessment. Devices with moderate risk should be reviewed to determine if the risk is currently as low as reasonably practical or if further steps should be taken. The security level targets can be used to group assets into zones based on cybersecurity criticality and support the determination of network segmentation.

An example Initial Risk Assessment worksheet is shown in Table 9-6.

Table 9-6 Initial Risk Assessment Worksheet

Cyber Asset	Likelihood	Consequence of Compromise	Severity	Risk	Security Level Target
Turbine BPCS Controller	High	Potential overspeed with potential rupture and multiple fatalities.	5	13	SL-4
Reactor BPCS Controller	High	Potential runaway. High Pressure Protection System (HIPPS) failure potential for rupture and single fatality	3	9	SL-3
Cooling Water BPCS Controller	High	Potential for long-term corrosion	1	4	SL-1

Source: Implementing IEC 62443: A Pragmatic Approach to Cybersecurity [84]

9.2.1.2 Detailed Risk Assessment

Once the initial assessments are completed, detailed risk assessments are conducted on the systems with higher potential risk. The detailed risk assessment serves as a more rigorous, guideword-driven evaluation of the IACS. The purpose of this more systematic analysis is to ensure that adequate security protections are implemented for cyber-critical or high-consequence zones. The cybersecurity HAZOP methodology used for detailed risk assessment is provided in Figure 9-4. A detailed example of how to complete the detailed risk assessment is presented in Appendix B.



Figure 9-4 Detailed-Level Risk Assessment Methodology

Step 1: Select the Zone or Conduit

The inputs to the cybersecurity HAZOP include the Zone & Conduit diagram created during the initial risk assessment as well as updated system architecture (such as those shown in Chapter 8). This information provides the

basis for grouping the assets into zones and evaluating the security requirements for assets based on the network segmentation strategy. These diagrams should, in combination with any applicable procedures related to cybersecurity, provide the cyber equivalent of process safety information needed for the risk assessment.

Step 2: Select the Cyber Node

Once a Zone or Conduit has been selected for review, the assets within the zone should be evaluated as cybersecurity nodes. This allows for the assessment to consider the impact of a cybersecurity threat on each asset within the zone. If very similar or “clone” zones are in an IACS, the detailed risk assessment only needs to consider one of the zones. Similarly, if multiple similar assets are within a zone, only the first needs to be fully evaluated and the rest can be identified as “clones.”

Step 3: Select the Threat Vector

When assessing the risk associated with a cyber node, determining the correct set of cybersecurity guidewords is critical. To be effective, the list of cybersecurity threats evaluated should include all threats needed to comprehensively evaluate the system without being redundant in nature. Some security analysts use lists containing hundreds of threat vectors when evaluating all possible pathways into a system, but this is a long and intensive process that often provides diminishing returns. Some example threat vectors that may be included in this type of list are:

- User Spoofing – Network Sniffing
- User Spoofing – Social Engineering
- User Spoofing – Credential Cracking
- User Spoofing – Replay Communications
- IACS Device Spoofing – Rouge Device
- Unauthorized Access – Unprotected Access Point
- Unauthorized Access – Session Stealing
- Unauthorized Access – Exploit Industry Known Weaknesses
- Unauthorized Access – Hack Common Software Weaknesses
- Data Disclosure – Social Engineering
- Data Disclosure – Network Sniffing
- Modification of IACS Control – Modify IACS Data in Transient
- Modification of IACS Control – Modify IACS Data at Rest

- Modification of IACS Firmware / Software – Unauthorized Update
- Malicious Code Insertion – Virus Propagation from IT Network
- Bypass / Compromise Physical Access Controls
- Authorized Individual – Error in Judgment
- Authorized Individual – Accidental Error
- Authorized Individual – Social Engineering
- Disable Integrity Protection Measures
- Disable Intrusion Detection Measures
- Disable Logging of Security Event Records
- Deletion / Modification of Security Audit Records
- Denial of Service – Data Flooding
- Denial of Service – Compromise Weak Software infrastructure

This is a small fraction of the list of all possible cybersecurity threat vectors, but it emphasizes how the guidewords for cybersecurity studies can quickly become large and difficult to manage. A more practical approach is to consider logical groupings of threats to reduce the number of guidewords needed. Two common ways to group threats are by the threat source (such as those introduced in Chapters 4 and 5) or by the mechanism used to gain access.

When grouping threats based on threat source (such as those introduced in Chapter 4), the following guidewords are typically considered:

- Internal Unintentional (e.g., unknowingly plugging in an infected USB)
- Internal Intentional (e.g., disgruntled employee)
- External General/ Unskilled (e.g., script kiddy)
- External Targeted/ Skilled (e.g., cyber criminals, show of skills)
- External Attack Campaign (e.g., advanced persistent threat, nation state)

When grouping threats based on the mechanism used to gain access, the following areas will typically be considered:

- Social Engineering (e.g., phishing, spear phishing)
- Communications (e.g., denial of service, man-in-the-middle)
- Supply Chain (e.g., compromise of service provider)
- Physical Access (e.g., logging onto an unguarded workstation)
- Software (e.g., exploiting a known software vulnerability)
- Hardware (e.g., connecting a USB to an unsecured port)

Organizations have the ability to customize their specific guideword lists to adapt the methodology to its systems and work processes. Often an additional guideword for “Other” threats can help to capture the knowledge and experience of the risk assessment team. The “Other” guideword is particularly useful for capturing information from previously seen events or events that may not fit easily into the other guidewords (e.g., compromise of a system through an authorized 3rd party connection).

Step 4: Identify and Record the Threats

Once the guidewords have been determined for the study, specific threats are evaluated for each zone or node. When defining threats in the study, it is important to include the threat source, skill level of the threat source, threat vector (pathway), and the potentially affected asset as shown in the “detailed threat definition” in Table 9-7.

Table 9-7 Threat Definition Examples

Guideword	Poor Threat Definition Example	Detailed Threat Definition Example
Social Engineering	Compromise of stream drum BPCS	Phishing campaign from skilled attacker results in compromised administrator BPCS Engineering Workstation credentials
Internal Unintentional	Mistake leading to compromise	Unintentional configuration error by controls engineer on the BPCS Engineering Workstation leads to potential compromise

Step 5: Identify the Vulnerabilities

For a cybersecurity threat to be successful, it must exploit a vulnerability or hole in the security of the asset. An analysis of known system vulnerabilities is often conducted prior to the cybersecurity HAZOP as a separate study. The vulnerability is distinct from a risk assessment in that it is not concerned with the consequence or likelihood of a potential cybersecurity event and only focuses on weaknesses or vulnerabilities that could be exploited. The vulnerability analysis feeds the cybersecurity HAZOP as an input and provides information on what specific entry points could be leveraged by attackers to compromise the system. This serves to further refine the list of identified cybersecurity threats and improve the estimated likelihood of an attacker exploiting a given vulnerability. Additional details on the methodology for cybersecurity vulnerability assessments (CVA) are provided in Section 9.2.4.

Step 6: Record the Qualitative Threat Likelihood

The threat likelihood is defined considering the threat source, level of skill required, and pathway only. At this stage, the unmitigated system risk is being assessed, so risk reduction from countermeasures is not considered. Unfortunately, the level of industry data available for cybersecurity incidents is not as mature as for process safety incidents. No reference books are currently available for determining the actual frequency of cybersecurity attacks. Currently, the industrial security industry is divided on the best method for considering likelihood. One position is that risk-based cybersecurity should only be focused on the attack consequence severity because the actual likelihood is unknown. In this approach, an attack frequency of 1/yr. is typically considered for all threat types. However, this approach is conservative and may not lead to the optimal use of cybersecurity resources. For example, targeted/ skilled cybersecurity attacks that may cause the most significant consequences often occur at a lower frequency than unskilled internet-based attacks. This introduces a second option for determining threat likelihood based on order of magnitude estimates for different types of threat sources and skill levels, as shown in Table 9-8.

Table 9-8 Threat Likelihood by Threat Source

Threat Source	Qualitative Likelihood	Estimated Frequency
Non-Targeted Attacks (e.g., script kiddie)	Very High	10 per year
Internal Unintentional (e.g., accidental use of an infected USB)	High	1 per year
External Targeted (e.g., cyber criminals)	Medium	0.1 per year
Internal Targeted (e.g., disgruntled employee)	Medium/ Low	0.1 – 0.01 per year
External Campaign (e.g., Nation State)	Low/ Very Low	0.01 per year

When considering the relative likelihood of possible threat sources, it is important to make conservative estimates. The true likelihood of attack for a site will vary based on the level of system exposure and vulnerabilities as well as the target attractiveness of the site. The size, industry, and location of a site are particularly important when considering the likelihood of targeted attacks and can lead to significantly differing results.

Step 7: Determine the Worst-Case Consequence (without Countermeasures)

After determining the likelihood of the threat, the consequence should be defined for the node or asset being evaluated. In many cases, the worst-case consequence defined in the initial risk assessment may be applicable and can be easily referenced. If a specific threat vector does not have the potential to lead to the worst-case consequence estimated in the initial assessment, then the credible worst-case consequence resulting from that threat vector should be documented. As with the initial risk assessment, the following assumptions are made:

- There is no response from a control system or operator in response to this failure.
- All non-mechanical countermeasure devices failed (e.g., firewalls, anti-virus scanning).
- The equipment fails if its design limits are exceeded.

However, mechanical devices that are not susceptible to cyber-attack such as pressure relief devices, can be considered in the likelihood estimate at this stage. The severity of the consequence is determined for each applicable type of consequence (e.g., safety, environmental, financial) based on the consequence without considering countermeasures.

Step 8: Determine and Record the Qualitative Severity of Consequences

The consequence severity and likelihood are ranked based on the corporate risk criteria. (Examples are provided in Table 9-4, Table 9-2, and Table 9-3.) In many cases, the same consequence severity ranking can be used from the initial risk assessment and the threat likelihood is updated based on the type of threat being considered.

Step 9: Determine the Security Level Target

The updated security level target is determined based on the unmitigated threat likelihood and consequence severity based on the organization's corporate risk criteria. Correlating the risk category to the security level as shown in Table 9-5 allows the same approach to be used for the initial and detailed risk assessments.

Step 10: Identify and Record the Countermeasures

The next step is to document what countermeasures are in place to decrease the likelihood of the attack being successful or reduce the severity of the consequence. Common countermeasure types that may be considered for various cybersecurity threats include:

- Firewalls/ Network Segmentation
- Access Control
- Intrusion Detection/ Prevention
- System Hardening
- Encryption
- Administrative Procedures
- Physical Security
- Cybersecurity Alarms

Many possible countermeasures can be adopted following a defense-in-depth approach to cybersecurity. Often, these countermeasures are a combination of technical solutions and company policies and procedures.

Step 11: Determine the Likelihood with Countermeasures

Based on the type and number of countermeasures, the mitigated likelihood of an event - including consideration of countermeasures - can be estimated. The following rules of thumb can be considered when determining how much the likelihood should be reduced with countermeasures:

- For manual countermeasures (e.g., cybersecurity alarms with operator intervention, manual monitoring activities), two independent actions should be identified to reduce the likelihood category by one.
- For automatic countermeasures (e.g., firewalls, hard-coded endpoints in controller), one independent countermeasure can be used to reduce the likelihood category by one.
- For safeguards not susceptible to cyber-attack (e.g., pressure relief devices or other mechanical devices), the likelihood with countermeasures can be estimated in the same way as in a traditional HAZOP/LOPA. For example, a pressure relief valve can be used to reduce the likelihood category by two.

When credit is taken for these countermeasures, it is important to ensure independence of the protections; otherwise, a single technique/action by the attacker could potentially overcome multiple countermeasures. For example, if the same access accounts are used for both the IT and IACS networks, an attacker could compromise both networks with a single set of credentials.

An example cybersecurity HAZOP worksheet is shown in Table 9-9. In this example, the likelihood of the social engineering threat can be reduced three steps (from high to very low) in the following way.

- The access restriction limits the number of accounts that can be compromised and automatically reduces the likelihood of the attack being successful by one likelihood level (high to medium).
- The pressure relief valve reduces the likelihood of the attack by two levels (medium to low, low to very low).

In the second example, the likelihood of an unintentional physical threat is reduced from very high to high based on the use of a locked cabinet (prevents attack automatically without manual detection and response during the event) that can reduce the likelihood one level.

Table 9-9 Detailed Risk Assessment Worksheet

Threat	L	Consequence	Sev.	Risk	Countermeasures (CMR)	L w/ CMR	R w/ CMR
Social Engineering: Spear Phishing campaign as part of a targeted attack (skilled) leading to stolen SIS engineer credentials.	H	Compromise of Safety Instrumented Function that protects against turbine overpressure. Potential for catastrophic overpressure of steam turbine and piping leading to loss of containment and potential multiple fatality event following a BPCS failure or process upset.	5	13	Restrict access to only required personnel with individual access account. Access is reviewed on a yearly basis. Pressure relief valves reduce likelihood of catastrophic overpressure and are not susceptible to cybersecurity threats.	VL	8
Physical: A contractor (unknowingly) attempts to connect ransomware infected equipment to the SIS engineering workstation.	VH	Inability to access SIS application program, potential business impact due to the cost of replacing SIS engineering workstation and application program, or potential for spurious trip and unexpected downtime.	2	9	The SIS engineering workstation is kept in a locked cabinet that only required personnel may access.	H	8

Where:

- L is the Likelihood.
- Sev is the Consequence Severity.
- CMR is Countermeasure.
- L w/ CMR is the likelihood with countermeasures.
- R w/ CMR is the risk with countermeasures.

Step 12: Determine if the Tolerable Risk Criteria are Met

The current level of risk resulting from the consequence severity and likelihood with countermeasures is compared with the corporate risk criteria to determine if the risk exceeds tolerable levels. When the risk is determined to be high, recommendations are made to improve the cybersecurity protections. This is a fundamental part of adopting a risk-based approach for cybersecurity as it focuses time and resources on reducing the highest risk scenarios first. In cases where a more detailed understanding of the cybersecurity risk is desired, or for scenarios with extremely high consequence severity, a semi-quantitative approach such as a LOPA based approach in Section 9.3.3 can be useful.

9.2.2 *Cybersecurity Checklists*

Checklists are often used in process safety as an additional step when conducting a HAZOP or other method of risk identification to ensure that common issues that have contributed to previous industry incidents have been properly mitigated and addressed. In some cases, these questions may be addressed throughout the HAZOP process, while other considerations may not logically fit into the HAZOP approach for risk identification.

The most common format for process safety checklists is a list of questions that must be answered, sometimes grouped by category. The checklist is completed by documenting the answer to each question and providing recommendations if any concerns are identified.

A cybersecurity checklist can provide a similar function during cyber risk assessment to ensure that common issues are appropriately addressed and to identify necessary actions to improve the inherent security of the system. An example cybersecurity checklist is provided in Table 9-10. This checklist can

be used and adapted by companies to ensure that it covers all relevant areas of concern.

Table 9-10 Cybersecurity Checklist

Item	Question	Response	Recommendation
General Cybersecurity Management			
1	Is a cybersecurity management system in place and aligned with process safety management?		
2	Is there a current audit program for cybersecurity controls in place?		
3	What is the emergency response plan in the event of a cybersecurity event?		
4	Are contractors trained with basic cyber hygiene requirements?		
5	Does the management of change work process for EH&S include relevant cyber content?		
6	What cybersecurity standards have been applied to the system?		
7	Is an updated hardware and software inventory maintained?		

Table 9-10 continued

Item	Question	Response	Recommendation
Design Phase			
8	Is the business network segregated from the IACS network? Please comment on how ownership is defined between the two.		
9	How are firewalls and firewall rules managed?		
10	How is remote access governed?		
11	How is wireless governed?		
12	Are diagnostics and alarms for countermeasures employed? If yes, provide examples.		
13	Are default passwords required to be removed from network equipment? If yes, is there a follow-up audit process to ensure it occurs? Are metrics documented relative to this and periodically analyzed?		
14	Are autorun and auto-play features disabled on tools for removable media devices?		
15	How is portable media (e.g., USB sticks/ports) managed?		
16	How is content downloaded from the internet managed?		

Table 9-10 continued

Item	Question	Response	Recommendation
Operations and Maintenance Phase			
17	How is the patching work process handled? Are only vendor approved patches applied?		
18	How are upgrades conducted for firmware in network equipment, Windows-based systems, and embedded devices?		
19	How are applications updated for Windows-based systems, 3rd part software, and embedded devices?		
20	Is anti-virus or whitelisting used on the IACS?		
21	Where is the engineering workstation located and how is access controlled?		
22	Are stand-alone engineering tools kept up-to-date (e.g., contain only whitelisted software), patched, and employ anti-virus protection?		
23	Who has access to the operating console?		
24	Is there clear identification between IT/Business and IACS computers?		
25	Is an active log of networks accessed on this site?		

9.2.3 Failure Modes and Effects Analysis (FMEA)

Failure Modes and Effects Analysis (FMEA) is a qualitative methodology for identifying potential problems and their impact. It can be used for either risk identification or system validation, depending on the stage in the lifecycle at which it is completed. Similar to HAZOP, FMEA is a systematic method for hazard identification and risk analysis, but instead of applying guidewords, FMEA starts with a set of potential failure modes for each device.

The first step in an FMEA is to list all of the components in the system under consideration: this will list typically be based on the Zone & Conduit map or asset inventory for the system. Typically, a FMEA would be selected if a more detailed analysis of the potential failures and impacts for a particular device or system is desired. In the example system in Figure 9-5 the Safety network has been identified for analysis, starting with the Safety PLC.

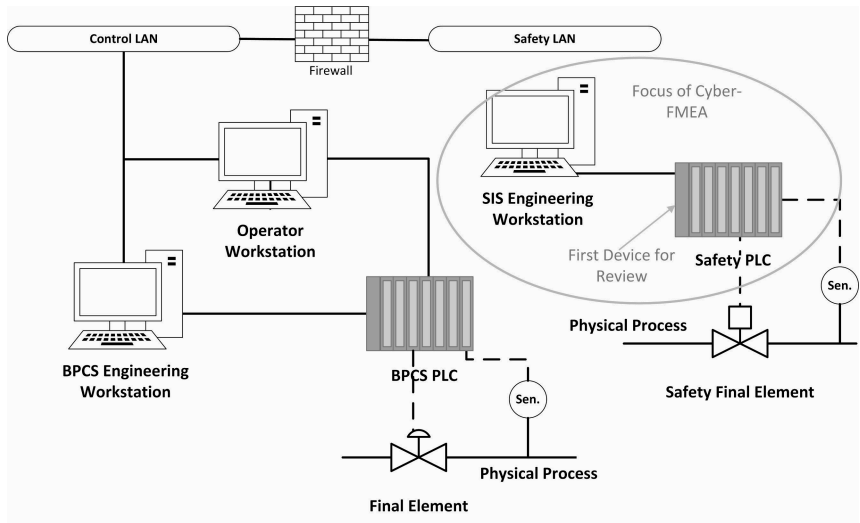


Figure 9-5 Network Architecture for FMEA

Once the list of components is agreed upon, possible failure modes are established for review. A failure mode is any means by which something could go wrong with a component. For example, when conducting an FMEA for a traditional safety analysis, common failure modes of a solenoid valve would include open coil, binding, loss of reset force, and external leak. For

cybersecurity assessments, typical failure modes include unauthorized access, inability to establish authorized access (Denial of Service), loss of communication, loss of data integrity, and loss of data confidentiality. Depending on the component in which the failure is experienced, the effect will vary. The effect in an FMEA is similar to the consequence in a cybersecurity HAZOP in that it defines the possible outcomes of a scenario. For each effect, existing controls or countermeasures that prevent or limit the severity of the negative impact can be listed. An example output from the FMEA methodology for the Safety PLC is included in Table 9-11.

Table 9-11 Example Cybersecurity FMEA for Safety PLC

Component	Failure Mode	Effect	Controls/ Countermeasures
Safety PLC	Unauthorized access	Unapproved changes to SIS logic, potential loss of protection for overpressure and overspeed protection.	Access control list SIS application program review
	Denial of Service	Inability to make approved changes to SIS controller and temporary delay.	
	Loss of Communication	Individual safety functions fail to safe state, process trip.	Redundant communication paths
	Loss of data integrity	Unapproved changes to SIS logic, potential loss of protection for overpressure and overspeed protection.	Redundant CPUs SIS application program review
	Loss of data confidentiality	Limited impact, with the potential for information to be leveraged in future attacks.	Encryption

Similar to the methodology presented in Section 9.2.1, the likelihood of failure modes and the severity of effects can be recorded during the assessment to determine the risk for each scenario. Depending on the criticality of the failure mode, actions can then be recommended to mitigate the highest areas of risk.

9.2.4 *Cybersecurity Vulnerability Analysis (CVA)*

A vulnerability assessment provides an overall review of potential weaknesses in the protection plan for a site or asset. Methods for traditional security vulnerability analysis (e.g., physical, personnel) have been developed in industry guidelines such as *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites* [98]. Cybersecurity Vulnerability Analysis (CVA) is distinct in that it specifically focused on assessing the existing IACS cybersecurity environment (physical, technical, and policy-related). The goal of the CVA is to identify current vulnerabilities and create recommendations for possible improvements. Typically, an initial CVA is conducted during the project phase for new facilities and ongoing vulnerability assessments are completed periodically for operating plants. For a vulnerability assessment to be most successful, it should be completed as an input to a cybersecurity HAZOP/ risk assessment, as discussed in Section 9.2.1. A methodology for completing a CVA considering all aspects of attack surface (network, software, and social engineering) is provided in Figure 9-6.

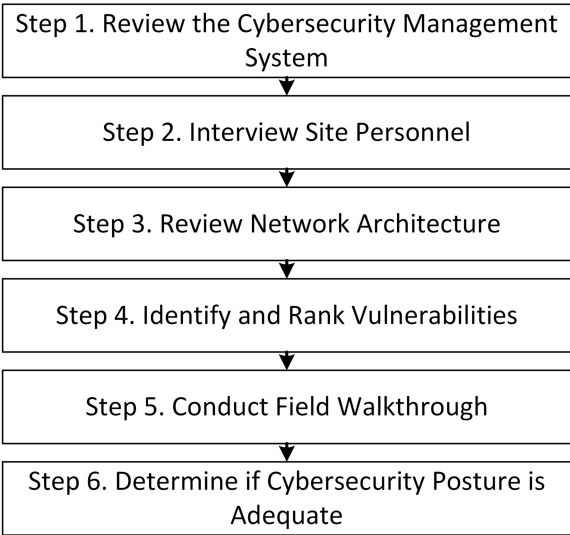


Figure 9-6 Cybersecurity Vulnerability Methodology

Step 1: Review the Cybersecurity Management System

The first step in the vulnerability analysis is to review the organization’s cybersecurity management system (CSMS) and supporting cybersecurity policies and practices. The purpose of this analysis is to determine how the organizational approach compares to industry standards (e.g., IEC 62443-2-1) and best practices (e.g., NIST Cybersecurity Framework) to determine if improvements are required to improve security. Effective policies and competency development are important steps in managing the human factors that influence cybersecurity readiness. A holistic approach to implementing cybersecurity in coordination with process safety management is introduced in Chapter 11.

Step 2: Interview Site Personnel

For operational facilities, it is also important to interview site personnel to gain insight into the application of security measures for the system. The leader of the CVA should interview personnel with access to the IACS to ensure that cybersecurity policies and practices are being implemented and to determine the level of cybersecurity awareness and hygiene practiced at the site. The interviews should include a representative from each group with

access to the IACS or sensitive information about the network, including all insider roles identified in Section 5.1.

Step 3: Review Network Architecture

The network architecture is the next area to be reviewed. In the project-phase analysis, the network architecture is assessed from the conceptual design. The proposed segmentation is reviewed to determine if the current design increases cybersecurity risk for critical devices by pairing them lower criticality systems in the same zone. During the periodic CVA for an operational facility, an approved network scanning tool is used to determine the actual “as found” network architecture and network traffic pattern. This information is compared to the updated Zone and Conduit diagram to assess if the network segmentation strategy has been maintained and if any unidentified devices are connected to the network. The review of the network architecture and current network traffic baseline is an important step in understanding the level of exposure of the current network strategy and can identify deficiencies in the network aspect of attack surface. Additional information on security monitoring and network scanning tools can be found in Section 8.6.

To assess the software-based aspects of the attack surface, the configurations for devices on the IACS (e.g., workstations, servers, firewalls, and switches) need to be reviewed against baseline configurations. In the initial CVA, the configuration data is assessed based on the plan hardware and software versions to be used in the IACS. These versions are assessed against databases of known vulnerabilities such as the National Vulnerability Database [99] to identify if any mitigation actions are required. During the periodic CVA for an operational facility, devices in cyber critical zones are scanned using an approved tool to collect the current device configuration and assess vulnerabilities in the current hardware/ software. One free to use open source tool that can support this review is DumpSec [100]. DumpSec creates a concise, easy-to-read export detailing the permissions and audit settings for the file system, registry, printers, and network shares of devices with Windows-based operating systems [100].

Step 4: Identify and Rank Vulnerabilities

As introduced first in Chapter 3, a vulnerability is: “A design flaw or weakness in a device, application, or system such that its operation and management could be exploited to advance a cyber-attack” [3]. Vulnerabilities are the weaknesses in the cybersecurity defenses of a system that can be exploited during a cybersecurity attack. Vulnerabilities are commonly rated based on exploitability and impact. The exploitability is a measure of how easy it is for an attacker to take advantage of the vulnerability. A vulnerability related to establishing remote access from an external device would likely be easier for attackers to exploit than a vulnerability on an application in the IACS that could allow the escalation of all general users to administrator credentials. The impact is a measure of the significance of the vulnerability on the affected program (e.g., can an unauthorized user make a change?). Vulnerabilities with a high exploitability and a high impact represent the most serious concern. The impact will be determined based on the type of vulnerability and the level of access granted by exploiting the vulnerability. For example, operating system (OS) command injection vulnerabilities allow attackers to execute arbitrary OS commands on a server running an application; these typically lead to the total compromise of the application (and its data). This would correspond to a high impact score.

To support the easy comparison of different vulnerabilities, many organizations have adopted the Common Vulnerability Scoring System (CVSS) framework so that vulnerabilities can be graded consistently. Vulnerabilities are given a base score between 0 and 10 based on factors relating to exploitability and impact. A list of known vulnerabilities sorted by affected operating system/ program and the associated CVSS score can be found at the National Vulnerability Database [99].

Some external factors also have the potential to impact the criticality of a vulnerability. For example, if source code for an attack is released that leverages a vulnerability, it can facilitate attackers exploiting this vulnerability and ultimately increase the overall criticality of the vulnerability.

Vulnerability scanning tools offer an easy way for organizations to scan many devices to identify the presence of any known vulnerabilities based on installed applications and patch levels for operating systems. A number of

vulnerability scanning tools are commercially available. One free to use open source tool for vulnerability scanning that contains features for a variety of internet and industrial protocols is OpenVAS (Open Vulnerability Assessment Scanner) [101].

Step 5: Conduct Field Walkthrough

In addition to these steps, a plant walkthrough or physical inspection is also completed as part of the periodic CVA. This gives the assessor an opportunity to review how physical security measures are implemented in the field. A walkthrough helps assessors to verify that cybersecurity policies have been adopted and that good cybersecurity hygiene is practiced. It also provides an opportunity to review the physical state and protections of IACS devices and to confirm that no undocumented devices are connected in the facility. The operations and maintenance questions from the cybersecurity checklist in Section 9.2.2 provide a good list of considerations to check during the field walkthrough.

Step 6: Determine if Cybersecurity Posture is Adequate

The results of the policy, architecture, and device configuration analyses should be compared against the security requirements for the system to identify any deficiencies in the current cybersecurity posture. The CVA report should clearly communicate the results from each area, including both strengths and weaknesses, to provide an accurate snapshot of security at that point in time. This is an essential input to the risk assessment process and can be used to determine what vulnerabilities are present that could be exploited by attackers. The number and types of vulnerabilities present will influence the overall likelihood of a successful attack.

A cybersecurity vulnerability analysis does not take the place of a cybersecurity risk assessment. Vulnerability assessments are only focused on identifying weaknesses in system security and do not provide information on the likelihood of an attack or the potential consequence if these vulnerabilities are exploited. The risk assessment is a foundational step in identifying the most important risks to mitigate first and is necessary to apply the RBPS to cybersecurity applications.

9.3 *Quantitative Methods*

Quantitative risk analysis methods differ from qualitative methods in that they use numerical values to model the likelihood and severity of a cybersecurity scenario instead of categories. Quantitative analysis methods typically take longer to complete than their qualitative counterparts but provide a higher level of precision when analyzing cybersecurity scenarios. Typically, this added level of detail is most important for high-risk scenarios. In this section, three quantitative methods for analyzing cybersecurity risk will be introduced:

1. Bow Tie
2. Layer of Protection Analysis (LOPA)
3. Quantitative Risk Assessment (QRA)

9.3.1 *Availability of Cybersecurity Databases*

The effectiveness and accuracy of quantitative methods are highly dependent on the quality of the database used to estimate the likelihood of each factor in the analysis. If inaccurate sources are used as inputs, the quantitative methods will not return accurate results. Unfortunately, it is often difficult to gather detailed information about cybersecurity concerns, in part due to confidentiality concerns and the sensitivity of the information. As a result, there is no central, well-maintained database where statistics can be found for:

- Attack likelihood
- Target attractiveness of a site
- Effectiveness of countermeasures

Without this information, the methods presented in the following subsection largely represent a future state of more rigorous cybersecurity analysis. The semi-quantitative estimates provided in Section 9.3.3 provide the current best practice for estimating the likelihood of a successful cybersecurity attack. As the cybersecurity field continues to evolve and defensive technologies are better able to track information about cybersecurity incidents, it is possible that the data to support more robust quantitative estimates will be collected. Additional information on efforts to develop a

centralized cybersecurity incident repository that would support a more detailed database for these factors is provided in Section 13.2.

9.3.2 *Bow Tie*

Cybersecurity scenarios often have multiple initiating events progressing to multiple outcomes. A diagram, referred to as a “bow tie” diagram, is commonly used in process safety analysis and can be very useful in analyzing this type of scenario. As the name implies, the diagram shows multiple initiating events leading to one incident, which then leads to multiple potential outcomes and consequences. The center knot represents the hazardous event of concern. The left side of the bow tie diagram is called the pre-event side and the right side of the diagram is called the post-event side.

Each initiating event progresses to intermediate events based upon the success or failure of safeguards/ countermeasures capable of preventing the incident. If a preventative protection functions as intended, the incident will not occur. Once the incident occurs, various outcome paths are possible depending on the success or failure of safeguards capable of mitigating the consequences of the incident. The bow tie diagram shown in Figure 9-7 includes the following elements [102]:

1. **Hazard:** The bow tie diagram begins with the hazardous event of concern.
2. **Top Event:** The point in time at which loss of control of the hazard occurs.
3. **Threats** are depicted on the left side of the bow tie diagram.
4. **Consequences** of loss of control of the hazard are depicted on the right side of the bow tie diagram.
5. **Prevention barriers** shown on the left side of the diagram are barriers which stop threats from resulting in the top event.
6. **Mitigation barriers** shown to the right of the top event are barriers which mitigate the top event (i.e., reduce the scale of the undesired consequences).
7. **Degradation Factors** can be applied to both prevention and mitigation barriers, and these can lead to impairment or failure of the barrier to which they are attached.

- 8. **Degradation Controls** act to mitigate the degradation factors, helping maintain the main pathway barrier at its intended function.

Barriers and degradation controls are fundamental elements of safety and cybersecurity management systems. Steps need to be taken to maintain the effectiveness of these layers to ensure that an organization's risk targets are met. Altogether, bow tie diagrams demonstrate a holistic picture for process safety or cybersecurity risk management [102].

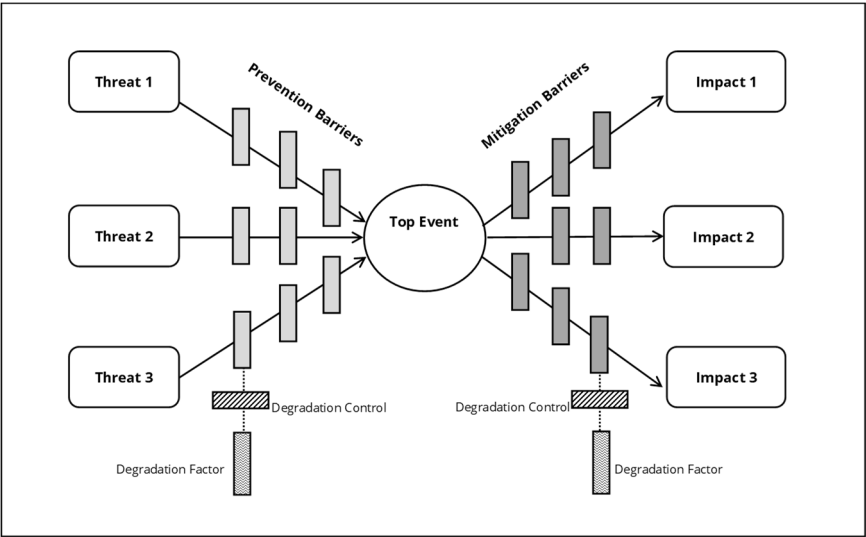


Figure 9-7 Bow Tie Diagram

Source: Adapted from Bow Ties in Risk Management: A Concept Book for Process Safety [102]

Cybersecurity countermeasures can be assigned as either preventative or mitigative barriers, depending on where they fall in the chain of events. In the NIST cybersecurity framework first introduced in Chapter 7, protections from the identify, protect, and parts of the detect stages of the framework are preventative in that they block attackers from triggering a consequence. Protections from part of the detect and the respond and recover stages of the framework are mitigative because they help to minimize the negative impact

of a cybersecurity incident once the top event has occurred. Traditional process safety protections that are not susceptible to cybersecurity compromise, such as pressure relief valves (preventative) and dikes (mitigative), can also be considered in cybersecurity bow ties.

Cybersecurity emergency response procedures are particularly important for mitigating the consequences of compromise because it is very difficult to prevent skilled and motivated attackers from gaining access. The common adage for cybersecurity is that compromise is question of “when” and not “if.” With this in mind, organizations that are able to detect intrusions more quickly and respond effectively will be much more effective at mitigating cybersecurity risk than organizations who cannot. The speed at which intrusions are detected is often a function of the implemented cybersecurity monitoring or continuous monitoring applications that can generate cybersecurity alarms based on unusual activity and the level of cybersecurity awareness for plant personnel responsible for responding to an alarm. Organizational cybersecurity readiness can also be improved by developing procedures that document unusual activity that could constitute a cybersecurity incident and providing plant personnel with a clear chain of command for cybersecurity related issues. An example bow tie diagram for a cybersecurity scenario is shown in Figure 9-8.

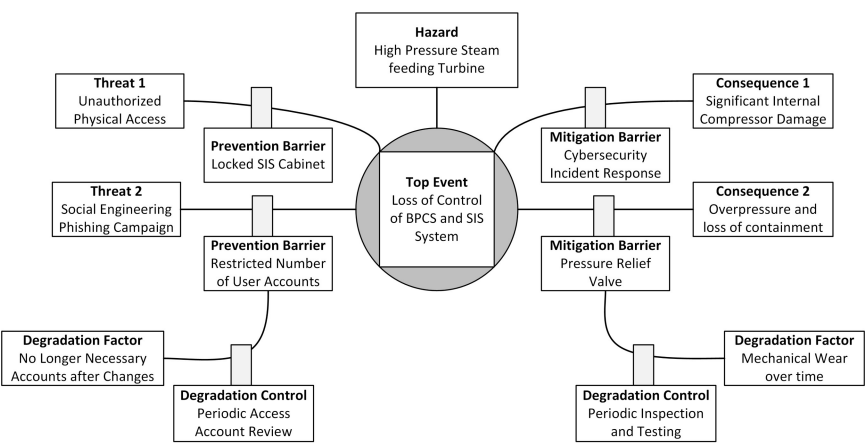


Figure 9-8 Example Cybersecurity Bow Tie Diagram

Bow ties are particularly effective at visualizing the relationships between threats and possible outcomes. The graphical depiction of the relationship between cybersecurity controls and the outcome scenarios can provide a clearer picture to a wider range of users as compared to other more complex analysis methods. Additionally, bow ties clearly connect the cybersecurity management activities necessary to maintain the effectiveness of barriers to the risk assessment and can help to maintain focus on important management activities. Metrics and data collected for individual threats, consequences, and barriers that make up the bow tie can be used to support the quantification of probabilities using the LOPA and QRA based methodologies.

9.3.3 *Layer of Protection Analysis (LOPA)*

Layer of protection analysis (LOPA) is a semi-quantitative method for analyzing risk; details on this methodology are provided in *Layer of Protection Analysis (LOPA): Simplified Risk Assessment* [103]. It is commonly used in process safety to determine if an organization's tolerable risk criteria are met for a given hazard scenario. In a typical chemical process, multiple safeguards are used to reduce the frequency of an undesired consequence, including inherently safer design, instrumented protections (SIS and BPCS), operator response to alarms, other non-instrumented engineered safeguards, and emergency response [103]. Not all of these safeguards, however, meet the standards necessary to credit them as Independent Protection Layers (IPLs) in LOPA. To be considered an effective layer of protection, safeguards must meet seven core attributes: independent, functional, integrity, reliable, validated, maintained and audited, access security, and management of change.

If all of these requirements are met, then a safeguard can be applied in the LOPA scenario and considered as an independent protection layer. This means that the likelihood of each protection failing is independent, and the likelihood of a hazardous event occurring is the initiating event frequency multiplied by the probability of failure on demand of each protection layer. For scenarios with multiple initiating events, the total likelihood of the hazardous event occurring is the sum of the mitigated frequencies for each cause. The LOPA methodology is commonly modeled using the "Swiss cheese diagram"

to demonstrate that the consequence is only possible if each layer fails, as shown in Figure 9-9.

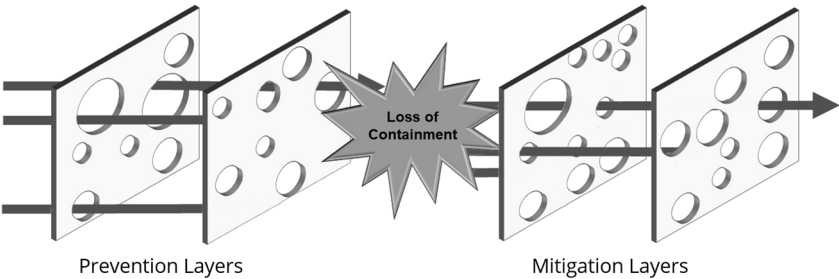


Figure 9-9 Swiss Cheese Model

Source: “Swiss cheese model” adapted from original proposed by James Reason, U. Manchester, 1990

A similar approach can be taken for cybersecurity scenarios to verify that the mitigated likelihood of a cybersecurity attack resulting in a defined hazard scenario meets an organization’s tolerable risk criteria. This approach is sometimes referred to as semi-quantitative Security Level (SL) verification [84] and can be used as one approach for justifying that adequate security has been achieved for critical zones. The methodology for completing semi-quantitative SL verification is included in Figure 9-10. A detailed example of how to apply the semi-quantitative approach is presented in Appendix B.



Figure 9-10 Semi-Quantitative SL Verification Methodology

Step 1: Initial Risk Screening

The first step in semi-quantitative SL verification is to identify which scenarios from the cybersecurity HAZOP require further evaluation based on consequence severity or residual risk. For each of these scenarios, the threat likelihood, consequence severity, and cybersecurity countermeasures are transferred to the SL Verification worksheet and provide the basis for the evaluation.

Step 2: Determine Threat Likelihood

The likelihood level from the cybersecurity HAZOP is converted into a quantitative frequency based on an organization’s defined methodology. A basis for estimating threat likelihood is provided in Section 9.2.1, and the frequencies from Table 9-8 can be considered as a starting point for organizations implementing a semi-quantitative method.

Step 3: Determine Target Attractiveness

The next factor that needs to be considered is a site’s target attractiveness. First introduced in Chapter 3, target attractiveness is a factor indicating how likely a facility is to be targeted for attack considering industry, size, company, political and personal motives, and the overall value of the target to an attacker. The target attractiveness is modeled as a multiplier of 1 or greater that can be used to model how much more likely a site is to be targeted based on its attractiveness. The levels of target attractiveness in Table 9-12 can be considered depending on a site’s size. These estimates can be further refined by considering the impact of an organization’s location and any company specific media coverage.

Table 9-12 Target Attractiveness Estimates

Name	Description	Assumptions	Multiplier
Small Impact Target	Multi-source plant with limited production impact.	Normal level of media coverage	1
Regional Impact Target	Product impact for a specific region.	Normal level of media coverage	1.5
Large Impact Target	Single source critical company assets.	Normal level of media coverage	3
Critical Infrastructure Target	National infrastructure with extensive impact.	Normal level of media coverage	5

Step 4: List Countermeasures

Cybersecurity countermeasures defined in the cybersecurity HAZOP are re-evaluated to ensure that they apply to a given threat vector / consequence pair; this is analogous to applying protection layers to a given cause /

consequence pair in a process safety LOPA. In addition to being specific to the threat vector and consequence, the protection layer must be independent from the initiating event and all other protection layers. Otherwise, a single action by the attacker could potentially overcome multiple countermeasures. Cybersecurity attacks can be a large source of common cause failure for traditional layers, and a well-designed attack may successfully circumvent multiple countermeasures. It is important that different types of countermeasures are considered to build a defense-in-depth approach. This ensures that attackers must bypass multiple diverse layers to achieve their goal and provides increased opportunity to detect and respond to an intrusion before the ultimate consequence is reached. Similar to process safety, where the diversity of protections helps to reduce the probability of a common cause failure for protection devices, diversity in countermeasures reduces the likelihood that multiple countermeasures would be susceptible to the same exploits. Lastly, the countermeasures need to be shown to be dependable and auditable so that the attained security can be assured over time.

If a countermeasure meets the criteria for independence, dependability, and auditability, credit can be taken in the SL Verification. Credit is taken in the form of assigning a probability of failure on demand (or PFD) for the countermeasure. No protection layer is perfect, and the Probability of Failure on Demand represents the likelihood that the protection layer will fail when it is called upon to prevent scenario propagation. PFD is a multiplier less than one that reduces the likelihood of a successful cybersecurity attack. Unlike in traditional LOPA analysis, no industry data on countermeasure effectiveness is available for determining the PFD. As a result, it is recommended that conservative estimates are made based on the type of countermeasure employed. Estimates for the PFD of different countermeasure types are provided in Table 9-13. As the industrial cybersecurity field continues to evolve, it is expected that improved data gathering will support more granular determination of countermeasure effectiveness as well as other factors considered in semi-quantitative SL verification.

Table 9-13 Cybersecurity Countermeasures and Estimated PFD

Countermeasure Type	Description	Estimated PFD
Active	The countermeasure can automatically prevent or reduce the severity of the ultimate consequence (e.g., pressure relief valves).	0.1
Passive	The countermeasure requires manual intervention to avoid the ultimate consequence (e.g., cybersecurity alarm with operator response, network monitoring).	0.2
Safeguards not susceptible to cyber-attack	Traditional process safety IPLs that are not susceptible to cybersecurity compromise (e.g., pressure relief valves, hardwired interlocks).	Same probability of failure from existing LOPA databases.

Step 5: Apply Conditional Modifiers

After determining effective countermeasures, conditional modifiers can be considered. Conditional modifiers are probabilities of possible outcomes that can support risk calculations. Examples of conditional modifiers that may be considered for a loss of containment scenario resulting in a potential fatality include probability of ignition, probability of explosion, occupancy (probability of personnel presence), and probability of injury or fatality. Similar to their use in LOPA for process safety risks, conditional modifiers can be considered if appropriate based on the consequence description and the operating environment. For example, in the German steel mill incident, the severe equipment damage and loss of containment at the blast furnace did not result in a fatality because no operator was present in the hazard area [8].

Additional information on the use of conditional modifiers in process safety can be found in *Guidelines for Enabling Conditions and Conditional Modifiers in Layers of Protection Analysis* [104].

Step 6: Calculate the Likelihood of Successful Attack

Once all factors have been considered for a cybersecurity hazard scenario, the likelihood of a successful cybersecurity attack is calculated. An example semi-quantitative SL verification worksheet is shown in Table 9-14.

Table 9-14 Semi-Quantitative SL Verification Worksheet

Attack Likelihood	Target Attractiveness	Countermeasure 1	Countermeasure 2	Countermeasure 3	Likelihood of a Successful Attack
Targeted (Skilled)	Single Source/ Large Impact	Restrict access to only required personnel with individual access account. Access is reviewed on a yearly basis.	The Application Program for the SIS PLC is reviewed yearly to identify if any unapproved changes have been made.	Pressure relief valves reduce likelihood of catastrophic overpressure and are not susceptible to cybersecurity threats.	--
0.1/yr.	3	0.1	0.2	0.01	6E-5/yr.

Step 7: Determine if the Tolerable Risk Criteria are Met

This likelihood of a successful attack is compared to the tolerable frequency based on corporate risk criteria to determine if the cybersecurity requirements are sufficient to achieve the identified Security Level. If the risk exceeds a tolerable level, recommendations are made to reduce risk and increase the security capabilities. The amount of residual risk can be determined as shown in Equation 9-1. When the residual risk is determined to be 1 or less, no further action is required. When the residual risk is higher than 1, further action may be required to achieve risk goals.

$$\text{Residual Risk} = \frac{\text{Likelihood of a Successful Attack}}{\text{Tolerable Frequency}}$$

Equation 9-1

If the tolerable frequency for the cybersecurity scenario evaluated in this worksheet was set at 1 x10⁻⁵/yr., the residual risk would be 6, and recommendations would be needed to reduce the risk further. The addition of another automatic countermeasure, such as two-factor authentication for all administrative accounts or remote logins, could help to reduce the risk further and meet the organizational risk criteria.

The benefit of a semi-quantitative LOPA approach over using only a qualitative HAZOP based method is that it provides a more precise estimation of the current risk and can better guide activities for reducing the residual risk. This is an important aspect of the risk-based approach, as it is critical to apply an organization's limited resources to the highest risk scenarios first. The drawbacks of the semi-quantitative approach are that, as discussed in Section 9.3.1, data is not readily available for countermeasure effectiveness or threat likelihood. This limits the certainty of the estimated likelihood of a successful attack. Additionally, a semi-quantitative approach requires more time to complete than a purely qualitative analysis. Despite these drawbacks, the semi-quantitative approach is an important step for identifying the optimal cybersecurity protections for high-risk scenarios, and in some very high-risk cases, integrating cybersecurity concerns with fully quantitative risk assessments can be beneficial.

9.3.4 Quantitative Risk Assessment

The Quantitative Risk Assessment (QRA) methodology is a systematic approach to quantifying risk [105]. It provides improved granularity for high-consequence scenarios and is a more rigorous method of evaluating risk and identifying areas for cost-effective risk reduction. The methodology originated from probabilistic risk analysis practices in the nuclear industry and has been applied to the process industries since the 1980's [105]. *Guidelines for Chemical Process Quantitative Risk Analysis* [105] demonstrates how the methodology for quantitative risk assessment can be adapted to include specific parameters in the chemical, petrochemical, and oil processing industries such as:

- Involvement of chemical reactions
- Consideration of multiple chemicals
- Impact of plant type, age, and location on failure frequencies
- Possibility of multiple outcomes from a single event (e.g., fire, explosion, toxic release)

QRA is different from other risk identification and analysis methods presented in this chapter because it uses information from analysis databases to provide quantitative estimates for initiating event likelihood and consequence estimation. For traditional process safety, a number of well-maintained databases that extract from decades of operational experience provide accurate quantitative estimates for individual component failures and the likelihood of an incident resulting in possible consequences. For example, the release of a flammable material may result in no ignition, immediate ignition, or delayed ignition based on a number of factors; the probabilities of the various outcomes can be incorporated into a QRA [106].

The best application of QRA principles for cybersecurity risk analysis is to update an existing process safety QRA study to include cybersecurity considerations. This includes both confirmation that the possible worst-case consequence for the cybersecurity scenario has been evaluated and the addition of cybersecurity event frequencies to the model. Unlike other techniques presented in this chapter, a QRA model is not typically built just for cybersecurity.

Although the QRA method cannot yet be fully leveraged for calculating the likelihood of a cybersecurity attack, determining the expected consequence

outcome is largely unaffected by the initiation of the hazard (e.g., process failure or cybersecurity intrusion). As such, using traditional QRA techniques for consequence analysis can help to improve the understanding of the expected risk outcomes of a cybersecurity incident and support more accurate identification of the highest cybersecurity risks requiring protection.

9.4 *How to Prioritize Risk Reduction Measures?*

A key outcome of understanding cybersecurity hazards is to prioritize risk reduction measures and ensure that resources are allocated to the most effective protections. Being able to answer the question “how good is good enough?” is fundamental in prioritizing risk management. The use of corporate risk criteria (e.g., Table 9-4, Table 9-2, and Table 9-3) provides a clear and consistent approach for answering this question.

Using this example criteria, when a risk is brought to the Minimal (1-4) ranking, an organization's risk requirements may have been met. For risks that are Severe (13-16), or Significant (9-12), further risk reduction measures should be considered. The order in which these risk reduction measures are implemented should be based on the risk ranking, with the highest scored scenarios being addressed first. This helps to ensure that resources are focused where they will have the most impact. One benefit of completing traditional process safety and cybersecurity risk assessments using the same tolerable risk criteria is that the risks from each scenario can be accurately compared when completing prioritization. (For example, a level 16 cybersecurity risk would be a higher priority than a level 12 safety risk.)

For scenarios that are determined to be Moderate (5-8) risk, the determination of whether further action is necessary can be determined using the As Low as Reasonably Practicable (ALARP) principle. With this approach, the possible benefit in terms of risk reduction for implementing additional security controls is compared to the cost of implementation. If it is possible to implement an effective control for limited additional cost, this step should be taken. If the countermeasure is significantly more costly than the added benefit, the ALARP principle can be used to justify acceptance of the current risk.

Aggregating the results of the risk assessment can help to provide a better comparison of the risk between different systems and help to answer

questions such as: “How much risk is each system/ area contributing? Which systems/areas are contributing the most overall risk?” This facilitates an optimized approach for assigning resources to the highest areas of risk first so that additional cybersecurity protections can be implemented in the most effective manner. Although risk aggregation supports a clearer comparison, it is only as reliable as the data upon which it is based. Changes to the underlying data for the analysis can have a significant impact on the relative priorities.

9.5 *Revalidation/Reassessment*

When a risk assessment is conducted, it is based on the current system as documented at the time of the assessment. Any changes to the design or to the credited protections may impact the result of the assessment. Typically, this is addressed through a periodic reassessment of hazards. Global regulatory requirements frequently specify that PHA should be revalidated every 5 years. However, cybersecurity assessments should be revalidated at a higher frequency because of the fast pace of change in the cybersecurity threat landscape. Also, it is not uncommon for changes to be made to the IACS at a much higher frequency than the assessment revalidation time period. In these cases, the management of change (MOC) work process is used to ensure that the proposed change will not negatively impact the achieved safety or security of the system. As such, change management is an essential component for maintaining both process safety and cybersecurity over time. It is often beneficial to supplement existing MOC procedures with cybersecurity-specific considerations. The following types of changes should be evaluated for cybersecurity impacts:

- Changes to the Zone & Conduit Diagram
- Changes to firewall rules
- Changes to the hardware and software asset management list
- Changes to the IACS access control list
- Changes to cybersecurity countermeasures (endpoint protection, security monitoring, system hardening)
- Changes to the configuration of IACS assets
- Changes to the logic of Process Safety Controls Alarms and Interlocks (PSCAI).
- Software and firmware patch updates

In general, any change made to the system that has the potential to impact the achieved safety and security of the IACS requires a management of change program. This means that the analysis of the change impact should be evaluated, and the change itself should be performed in accordance with the MOC policy. Even “replacement-in-kind” changes can have impact. From a cybersecurity context, “replacement-in-kind” means the same hardware and software version for an asset. In some cases, the same IACS component may have a different level of cybersecurity exposure, depending on the firmware version. One example is the introduction of web servers for wireless smart transmitters. If a web server is enabled in the replacement sensor, but not in the original sensor, this could significantly increase the exposure to compromise following the change. Additional information on MOC is provided in Section 10.11.

Periodic assessment also provides an opportunity to review the achieved security of the system more frequently than the typical five-year revalidation PHA time frame. Completing an independent review of all MOCs over the past year, as well as testing cybersecurity countermeasures to ensure proper function, can support the identification of potential security concerns before they become major issues. As introduced in Chapter 5, human performance issues and unintentional vulnerability introduction continue to be major contributors to cybersecurity incidents. Setting a periodic review schedule gives organizations an opportunity to reduce the likelihood of unintentional incidents negatively impacting the IACS.

9.6 Summary

Identifying and analyzing risk is a core part of adopting the RBPS approach for cybersecurity. Although accurately assessing cybersecurity risk poses a number of unique challenges, adopting commonly used process safety techniques and calibrating them for cybersecurity studies can help to provide consistent risk assessment across safety and cybersecurity scenarios and reduce the necessary development time for the cybersecurity risk identification and analysis method. Core principles of Hazard Identification and Risk Analysis, as well as cybersecurity specific considerations, are summarized in Table 9-15.

Table 9-15 HIRA RBPS Principles and Cybersecurity Considerations

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	Ensuring consistency between assessments is critical for maintaining an accurate picture of an organizations risk, and implementing risk assessment procedures under the process safety/ cybersecurity management system is an effective approach.
Identify hazards and evaluate risk	Selecting the appropriate risk identification method is critical for an effective cybersecurity risk assessment. Common methodologies for identifying cybersecurity risk include cybersecurity HAZOP, cybersecurity checklists, and Cybersecurity FMEA.
Assess Risk and make risk-based decisions	Selecting the appropriate risk analysis method is critical for an effective cybersecurity risk assessment. Common methodologies for analyzing cybersecurity risk include cybersecurity bow tie, LOPA/ semi-quantitative SL verification, and QRA. The use of a methodology adopted for cybersecurity analysis is particularly important because of the current limitations of data sources for probability estimation in the cybersecurity industry.
Follow through on assessment results	Regardless of the methodology used for the hazard identification or risk analysis, it is essential that the recommendations resulting from the study are implemented in a complete and consistent manner.

10 Manage the Risk

Chapter 7 describes the integrated safety lifecycle and illustrates how process safety activities and cybersecurity lifecycle activities map to this model. Chapter 9 provides an in-depth discussion on the cybersecurity Hazard Identification and Risk and Analysis element for Risk Based Process Safety (RBPS). This chapter discusses implementation of a management system for cybersecurity risk within the balance of the other RBPS elements. Chapter 11 will provide additional details on how to implement the management program.

10.1 Management Approach

Like Process Safety Management, the success of cybersecurity management is dependent upon strong leadership that drives a committed culture. The organization's management needs to clearly appreciate the potential for cybersecurity attacks and understand the safety and business risks of a successful attack. *Guidelines for Risk Based Process Safety* [7] identifies the key principles of Risk Based Process Safety (RBPS) and describes the essential features of each element. Cybersecurity risk management is integrated into the RBPS program by aligning cybersecurity management activities with the key principles of the 20 RBPS elements and implementing each activity as part of the existing management system. Understanding the cybersecurity considerations begins with the following questions:

- What constitutes a cybersecurity attack?
- How can cybersecurity be compromised?
- What are the consequences of a successful attack?
- How often might an attack occur?
- What barriers must be maintained to repel attacks?

The first question – understanding the nature of cybersecurity attacks – was addressed in Chapter 4, and the Hazard Identification and Risk Analysis (HIRA) element discussed in Chapter 9 addresses the second and third questions. Other RBPS elements address the last two questions. In this chapter, cybersecurity risk management considerations are developed for each element, considering the activities covered under the process safety element and the expected behaviors of personnel within that element. Although cybersecurity activities are managed more heavily in some elements

than others, cybersecurity considerations are present in every element. This chapter will discuss:

- Initial steps common to all elements
- Cybersecurity concerns associated with the element and their relative importance.
- Element specific cybersecurity activities

10.2 Initial Steps

Establishing the Site Security Lead role and the competencies required to fulfill the responsibilities of that role are important first steps. The Site Security Lead role is responsible for site adoption of IACS cybersecurity and for staying up-to-date on standards and risks. Individuals that will hold key roles pivotal to effective cybersecurity management should also be identified. It is important to document the roles and responsibilities as described in Section 11.1.1 and develop a Responsible, Accountable, Consulted, and Informed (RACI) chart. The individuals assigned to these roles will likely require some additional training to meet the full scope of competency requirements. Competency plans should be prepared to address needs, obtain training, and seek out the experience opportunities necessary to develop personnel.

Another important early step is to conduct a cybersecurity gap assessment to identify gaps between an organization's current and desired cybersecurity state. Typically, the scope of a gap assessment includes a review of existing policies and procedures (such as those outlined in Chapter 11), as well as a review of the existing network architecture and security measures. Pairing a gap assessment with the cybersecurity Hazard Identification and Risk Analysis (HIRA) as described in Chapter 9 is an effective method to establish a clearer understanding of the threats, vulnerabilities, and potential consequences of a cyber-attack. The initial risk assessment method outlined in Section 9.2.1 can be completed at the same time as the gap assessment to provide a high-level snapshot of current cybersecurity risk and jumpstart the use of a risk-based approach. Conducting a cybersecurity gap assessment enables an organization to prioritize initial and longer-term actions based on risk and helps to ensure that recommended practices are rolled out in the most effective manner.

10.2.1 Enhanced Control of Access

Improving the control measures that manage access to the IT and OT systems is another powerful step that can be taken early in system implementation.

Methods include:

- Implementation of an improved password policy requiring stronger passwords and periodic password changes.
- Two-factor authentication.
- Implementation of a least privilege access policy, ensuring all users have the minimum access required to complete their job.
- Removing all “backdoor” access (access that bypasses security) into the IT and OT systems.
- Separating IT and OT accounts for users of both systems.
- Conducting a user account review on both the IT and OT system and disabling accounts that do not have a current business purpose.

10.2.2 Training and Orientation

Chapter 4 cited data from a phishing benchmark study [47] where the link in a phishing email was clicked between one third and one half of the time. It is important to train employees to recognize these phishing attempts, so they do not click on such links. General awareness training is an important early step to reach the largest number of personnel. Conducting early effective awareness training will instill a sense of vulnerability and can help to improve cybersecurity hygiene. Training can also inform personnel of new cybersecurity protection measures to facilitate effective implementation.

Topics include:

- Outlining the content of top-level policies and procedures for cybersecurity management.
- Setting expectations for personnel responsibilities and behaviors.
- Communicating HIRA results, including a description of cybersecurity risks.
- Summarizing potential pathways for attack.
- Summarizing short-term and long-term activities in the cybersecurity implementation plan.

The initial awareness training should also include guidelines for improving cybersecurity hygiene such as:

- How to identify common email attacks such as phishing, ransomware and spyware and the proper response to these threats.
- Procedures for usage of removable media devices (e.g., USB drives, memory cards, smart phones).
- Precautions to be taken when downloading files from the internet.
- Rules for what downloads are permitted for business purposes (e.g., instrument maintenance manual, Safety Data Sheets) and what is forbidden (e.g., movies, music, games).
- Procedures for the use of secure file transfer sites for project file sharing.
- Password security techniques such as how to select robust passwords and the frequency with which passwords should be changed.

The workforce includes not only employees and site-embedded contractors, but also contractors and visitors that may visit the site periodically. The site orientation should be periodically refreshed to communicate the updated cybersecurity policies and procedures, including a description of the expected behaviors and defined rules of conduct for cybersecurity-related activities.

10.2.3 Initiate Continuous *Reinforcement*

The awareness training described in Section 10.2.2 provides a starting foundation of cybersecurity knowledge. Other methods may be employed to provide continuous reinforcement and keep cybersecurity awareness in mind.

- Prepare short modular training sessions to reinforce behavior expectations.
- Develop easily accessed guidance instruction on threat detection to supplement awareness training. Examples include a webpage that provides guidance on how to identify malware, instruction on how to safely report the attack, and steps to remove the email or file from their computer.
- Implement tools and activities that provide continuous reminders to be mindful of cybersecurity issues. For example, email bulletins, handouts, posters, cybersecurity puzzles, games, and quizzes all can help to build awareness.

- Incorporate cyber incident discussion and cybersecurity talks into safety meeting topic rotations.
- Periodic communication such as newsletters can include a cyber-related success story.
- Develop resources such as a cyber webpage as part of the internal company network.
- Email notifications to communicate new threats as they become known (e.g., new malware email attack).
- Establish cybersecurity metrics and share the scorecard with personnel.
- Consider celebration of a cybersecurity awareness month, etc.

10.2.4 *Design to Secure IACS*

Chapter 8 provides information on techniques to design a secure Industrial Automation and Control System (IACS). The objective of these techniques is to provide network segmentation and implement multiple layers of protection to deflect potential cybersecurity attacks. Implementing the measures described in Chapter 8 will require careful planning and will likely be implemented over a period of time. The following are some activities that can be executed quickly and will support the planning stage of system redesign:

- Prepare an inventory of process automation and control assets. Identify safety critical assets so they can be separated from general control assets.
- Conduct a survey for all computerized system to confirm that antivirus protection is in place.
- Launch a program to update and manage patches such as function and security updates for IACS assets.
- Complete a physical review of the spaces where contractors are permitted physical access can also help to identify potential points of exposure. Simple steps such as port blocking can help protect any locations where a portable data device could be plugged in.
- Confirm that printers, copiers, and similar equipment are connected only to the IT network and that proper firewalls are in place between the IT and OT network.
- Physically secure IACS hardware in locked cabinets or rooms. Consider installation of closed-circuit TV cameras to monitor cybersecurity-sensitive spaces.

10.3 *Cybersecurity Culture*

10.3.1 *Culture: Cybersecurity Concerns*

Building a strong cybersecurity culture is a primary line of defense. In the past, many organizations had limited awareness of OT cybersecurity incidents and believed that their IT department could sufficiently handle the OT environment. Often in these cases, manufacturing equipment was not adequately protected from cyber-attacks because of the differences in required cybersecurity hardening between OT and IT equipment. This cultural disconnect resulted in a higher facility exposure to cybersecurity incidents.

An organization's culture needs to have a firm foundation on which to build and must be fueled by management commitment. Personnel need to be trained to recognize a potential threat, understand the risk associated with a cyber-attack, know what action to take to prevent/ stop the attack, and be empowered to take steps necessary to stop the attack quickly. Training should be reinforced through Conduct of Operations reviews and behavior adjustments to drive operational discipline for cybersecurity similar to the approach taken for process safety.

Features present in a strong process safety culture include sustaining a sense of vulnerability, maintaining open and effective communication, and enabling timely response. Process safety scenarios primarily result from unintentional sources such as human performance issues, failed instrumentation or equipment, and acts of nature. Cybersecurity scenarios may originate from a premeditated intent to do harm or from an unintentional human performance issue. The cybersecurity culture needs to expand awareness to include potential sabotage as a credible source of risk, recognize attack attempts, and take appropriate and immediate action to address the situation.

10.3.2 *Culture: Cybersecurity Activities*

The cybersecurity culture is built with the same level of dedication as the process safety culture. Some activities to build a strong cybersecurity culture can occur quickly; others will require longer-term development. The top-level policy and procedures define the objective, but the underlying procedures for management of cybersecurity must be developed to provide clear guidance for cyber activities. Procedures should address items such as email, internet

usage, patch and update management, hardware changes and obsolescence. (See Chapter 11 for additional details.)

Organizations should establish a formal plan for cybersecurity management that defines roles and responsibilities. Developing a business continuity plan to address activities and systems that must be in place to restore and recover from an attack is another important part of the management system. Techniques such as tabletop exercises can be used to practice and refine recovery procedures. It is important to make personnel aware of the recovery plan and train them on routine activities, such as system backups, needed to support recovery.

Providing personnel with the tools needed to effectively manage cybersecurity and holding them responsible for complying with the procedures are also critical steps in a successful implementation. Cybersecurity training for personnel, including how to recognize an attack and the appropriate response, should also be considered as part of building a culture of cybersecurity. Culture can be strengthened by utilizing the continuous reinforcement techniques discussed in Section 10.2.3. Organizations can also establish a good cybersecurity culture by establishing a mechanism for safe reporting of untargeted attacks such as spoofing and phishing (e.g., a report button to highlight potential phishing emails for IT review). Periodic review exercises with OT personnel and operators to provide updates on new types of threats can also help to improve threat recognition skills. Lastly, establishing measurements and metrics to evaluate cybersecurity management performance monitoring is essential for tracking. These metrics should be reviewed regularly and shared with personnel. Celebrating success moments by highlighting positive behaviors can help to further boost engagement. Core principles of a strong Cybersecurity Culture, as well as cybersecurity-specific considerations for building the culture, are summarized in Table 10-1.

Table 10-1 Cybersecurity Culture

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	Establish policy and cybersecurity procedures and enforce compliance with the procedures.
Develop and implement a sound culture	Maintain a sense of vulnerability to cyber-attacks. Provide employees with the knowledge to recognize attacks and tools to respond quickly and effectively.
Monitor and guide the culture	Monitor cybersecurity management performance using leading and lagging indicators and provide feedback to personnel.

10.4 Compliance with Standards

10.4.1 Compliance with Standards: Cybersecurity Concerns

Chapter 1 provided a list of industry best practice references and regulatory requirements. The NIST Cybersecurity Framework [11] and IEC 62443 [107] standard, as discussed in detail in Chapter 7, establish the basis for the cybersecurity lifecycle model. This framework provides a structure for cybersecurity management for most organizations. Some examples of cybersecurity regulations and recommended practices are summarized in Table 10-2.

Table 10-2 Industry Codes, Standards, and Practices

Core Cybersecurity Standards
• IEC 62443 Industrial communication networks – IT security for networks and systems • NIST Cybersecurity framework • NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security • 6 CFR Part 27: Chemical Facility Anti-Terrorism Standards (CFATS)
Industry Focused Cybersecurity Standards
• 18 CFR Part 40: Federal Regulatory Commission (FERC) • NERC CIP: Power, United States • AWIA: Water and Wastewater, United States
Cybersecurity Implementation Focused Standards
• ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements • ISO/IEC 27009 Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements • ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security
IACS Standards with Cybersecurity Requirements
• IEC 61511 Functional safety - Safety instrumented systems for the process industry sector

Some industries, such as the nuclear, power and water industries in the United States, must comply with additional regulations specific to the industry and the authority having jurisdiction. Individual countries may have a cybersecurity governing agency authorized by that country's government. Organizations should conduct a search to identify any additional standards that are relevant to a site's industry, physical location, and regulatory authority. Refer to Chapter 13 for further discussion on available resources regarding regulations and industry standards.

The first steps in any effort to comply with standards are to identify which standards apply, obtain copies of these relevant standards, and make them accessible to personnel responsible for cybersecurity implementation. For organizations looking to get started with limited IACS cybersecurity

experience, the NIST Cybersecurity Framework [11] provides an effective starting point for assessing and improving cybersecurity posture.

10.4.2 Compliance with Standards: Cybersecurity Activities

Cybersecurity standards do provide some prescriptive guidance, but much of the content is performance-based. The standards indicate what is to be accomplished, leaving the end user to determine how to best achieve compliance. For example, IEC 62443 [107] requires monitoring and maintenance of security, but it does not prescribe specific actions to do so. Each organization should first determine what standards apply at both the corporate and site-specific levels, then develop policy and procedures for implementation that include detailed interpretation of the guidance. Personnel competent in cybersecurity are drawn upon to define an organization's program and develop the detailed procedures that will be put into practice.

Personnel that execute the procedures should be trained in regulatory standard requirements and recommended industry guidance, as well as in the implementation of specific company procedures. Additionally, competency requirements for personnel in positions of responsibility for cybersecurity implementation should be updated periodically to ensure that key managers are aware of relevant regulatory requirements and industry standards.

A measurement and metric system should be implemented to monitor performance and establish action to be taken to when the metrics indicate that goals are not being achieved. Finally, it is important to monitor the changing cybersecurity landscape to identify new standards and guidance and maintain currency with existing standards as they are updated. Most process safety standards are mature, are revised infrequently, and rarely have major updates. On the other hand, cybersecurity is evolving rapidly in response to the changing technology and growing threat vectors, and companies need work processes to keep pace with these changes in regulations and standards. Core principles of Compliance with Standards, as well as cybersecurity specific considerations, are summarized in Table 10-3.

Table 10-3 Compliance with Standards

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	• Incorporate the cybersecurity lifecycle into process and functional safety lifecycle (see Section 7.2). • Identify and implement standards and good engineering practices specific to the industry and jurisdiction. • Monitor implementation performance and revise procedure detail as needed to establish consistent implementation practice. • Maintain and improve personnel competency.
Conduct compliance work activities	• Provide personnel access to standards and recommended procedures. • Evaluate new standards and recommended practices for applicability, and review updates to implemented standards for changing guidance. • Periodically complete audit and management review to ensure that a compliance focus is addressing risks adequately.
Follow through on decisions, actions, and use of compliance results	• Follow prescribed practices fully and maintain work records. • Monitor compliance and update practices to address gaps and implement improved practices. • Monitor and report compliance status.

10.5 Cybersecurity Competency

10.5.1 Competency: Cybersecurity Concerns

Cybersecurity competency encompasses the knowledge, skill, expertise, and training needed to qualify personnel for effective cybersecurity management. Competency requirements relate directly to the roles and responsibilities with which personnel are tasked. These competencies are developed through a combination of education, training, and experience. In general, competency requirements may be grouped into a few categories:

- **Expert level** - Cyber technical experts include the Site Security Lead (Cybersecurity Champion), IT Personnel, and Controls Engineer. The roles include day-to-day management of systems that are subject to cybersecurity threats. These experts will also be instrumental in developing policies, procedures, and training materials, and they are front line defenders in the event of cybersecurity attack. The expert level requires deep knowledge of a broad range of computer systems and cybersecurity management techniques. This group will require the highest level of competency and should consider cybersecurity certification.
- **Intermediate level** – This level includes personnel responsible for the design and specification of IACS and IT equipment. They assure that systems are maintained and operating as intended and conduct cyber-attack response assessment and threat management. This level requires in-depth knowledge in specific areas and sufficient breadth to effectively work across responsibility boundaries.
- **Awareness level** – All personnel require awareness level competency at a minimum. Cyber-attack attempts can target a system in many ways. Personnel should be able to identify potential attacks and know the appropriate response and notification action to take when a threat is identified. Knowledge of the policies and procedures is required to maintain control of access to computerized systems and assure proper hygiene.

Table 11-1 in Chapter 11 is a sample RACI chart for cybersecurity lifecycle activities. A similar chart should be prepared very early in the development of the cybersecurity management program. Competency requirements for each role in the chart and other responsible individuals should be identified early and adjusted as the cybersecurity management program develops.

10.5.2 Competency: Cybersecurity Activities

The initial steps in Section 10.2 discussed competency plans for employees requiring cybersecurity awareness as well as for cybersecurity technical leaders. The competency plan needs to include provisions for moving personnel from the awareness level to the expert level and closing any competency gaps. Resource depth is required to assure that personnel with appropriate competency are available 24/7 to respond to threats quickly. Cross training is recommended with identified backups to prepare for attrition and address the transition needs for those moving into key roles. Sources of competency development include:

- IACS cybersecurity training
- Industry webinars and workshops
- Industry literature
- Certification programs (see Section 13.3.2)

In addition to training, competency aides can be developed that describe the structure of work processes and reduce the likelihood of human performance issues. For example, a checklist detailing the steps of installing a software update can be created, including verification documentation requirements at key confirmation steps. Developing a list of outside resources that can be consulted to address specific needs can further support competency development.

Using cybersecurity measures and metrics to monitor the effectiveness of the competency program and adjust the program as needed helps to ensure success. The percentage of phishing attempts that are repelled versus those that are successful is a good indicator of whether personnel know how to identify emails that represent a possible attack. The number of reports of suspect emails may be another good indicator that personnel do know how to respond and report properly.

Finally, user feedback on the procedures and tools helps an organization to understand what is working about the process and what is troublesome. For example, does the software update procedure work smoothly, or do users report issues when attempting to perform the update? Problems may indicate additional training is required or that an issue with the procedures or tools

needs correcting. Core principles of Cybersecurity Competency, as well as cybersecurity specific considerations, are summarized in Table 10-4.

Table 10-4 Cybersecurity Competency

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	Identify the knowledge and skills required to execute cybersecurity responsibilities. Develop and periodically update the training plan.
Execute activities that help maintain and enhance process safety competency	Appoint an IACS site security lead. Prepare resources “in depth” (e.g., identify a backup). Consult experts.
Evaluate and share results	Document each attack and response experience and communicate the learnings. Evaluate cybersecurity activities to obtain feedback and improve process.
Adjust plans	Continuously monitor the organizational response performance to cybersecurity threats and adjust protocols as needed.

10.6 Workforce Involvement

10.6.1 Workforce Involvement: Cybersecurity Concerns

The 2014 steel mill attack [8] described in Section 6.3 illustrates the importance of workforce involvement in managing cybersecurity risk. The attack began with a spear phishing email and ultimately resulted in the attackers gaining access to the mill’s control system, where they were able to modify settings. This resulted in massive damage to the furnace [8]. In the NotPetya attack [64] (Section 6.5), hackers gained access through a website, causing considerable damage to over 300 companies’ business systems. The Saudi petrochemical facility attack [10] (Section 6.6) was introduced via the IT system. The attackers were able to gain direct access into the IACS, including the Safety Instrumented System (SIS), and the attack was only thwarted because of a lucky programming error. There are many pathways by which an

attacker can target an organization, and these three incidents illustrate that the protection layers can be compromised without strong workforce engagement. To limit these pathways, the entire workforce should be fully involved in preventing and identifying attacks to prevent successful intrusion.

10.6.2 Workforce Involvement: Cybersecurity Activities

For the purpose of this discussion, workforce refers to all personnel - direct and indirect - whose role has a potential to impact cybersecurity. It includes employees and contractors working at a site, those working offsite performing duties that affect the design and implementation of cyber and process engineering controls, and personnel who may require remote access.

Workforce engagement is a critical aspect of a successful cybersecurity program. The engagement should be structured and targeted to gain the most benefit; therefore, it is important to develop a written plan for workforce involvement. The workforce engagement plan should include a description of the workforce roles, a detailed inventory of their respective responsibilities, and a path to obtaining the required competencies to fulfill the role's responsibilities.

Members of the workforce should be included in developing the procedures and practices for cybersecurity management. Creating an environment that empowers workers to speak up when addressing a suspected cybersecurity threat is an important part of establishing trust.

One of the workforce challenges is changing the engagement between IT and OT personnel. As stated previously the differing priorities in cybersecurity risk management, must be overcome so the two groups can learn from each other and collaborate. Developing trust between these two groups is an important step in breaking down the siloes which may currently exist in the organization. Managing cybersecurity risks requires looking from a single enterprise lens, teamwork, and alignment between processes (OT) and technology (IT) can help to ensure that shared company KPIs are met.

The following list includes a summary of behaviors that can accelerate workforce involvement and build cybersecurity culture (adapted from [108]).

- Conduct cybersecurity awareness during safety talk and mass gatherings
- Conduct training on cybersecurity to target specific groups
- Conduct assurance audits for cybersecurity compliance
- Practice cyber-hygiene at all times
- Provide visual reminders of proper behaviors
- Be attentive to and aware of cybersecurity concerns
- Embrace cybersecurity as a responsibility for all personnel
- Continue to enhance digital programs

Metrics to monitor workforce involvement, such as the number of untargeted attack attempts reported each month, help to measure the progress of the engagement. Sharing results of the monitoring with the workforce, such as celebrating the success by highlighting the 'wins' where threats were recognized and repelled, can help to continue to grow buy-in for workforce engagement. Core principles of Workforce Involvement, as well as cybersecurity specific considerations, are summarized in Table 10-5.

Table 10-5 Workforce Involvement

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	Develop a written plan for workforce involvement, including definition of roles and responsibilities. Provide easy access to threat response guidance instruction. Execute a plan to ensure that personnel develop the required competencies for assigned cybersecurity roles.
Conduct work activities	Involve workforce in the development and maintenance of cybersecurity procedures. Foster an environment of individual empowerment and trust.
Monitor the system for effectiveness	Develop and monitor metrics for workforce involvement.
Actively promote the workforce involvement program	Share workforce involvement metrics. Celebrate success stories.

10.7 Stakeholder Outreach

10.7.1 Stakeholder Outreach: Cybersecurity Concerns

In part, the success of a cybersecurity program is dependent upon a level of secrecy regarding the specific tools and techniques used to repel attacks. As such, the level of information shared with stakeholders may need to be guarded. Certainly, the organization should communicate that it does have a formal cybersecurity program. However, a company should carefully choose what details are shared with industry peers - and what information is kept confidential - to avoid handing a system roadmap to potential attackers. It may also be appropriate to share details with regulatory bodies that may not be appropriate for public disclosure. Details of the cybersecurity plan should be considered to be business confidential information.

10.7.2 Stakeholder Outreach: Cybersecurity Activities

Existing stakeholder outreach programs can be updated to include cybersecurity considerations and communication tools (e.g., brochures,

training programs). Updating training programs to include guidance about what information can be publicly shared regarding cybersecurity management is another important step in furthering stakeholder outreach. Core principles of Stakeholder Outreach, as well as cybersecurity specific considerations, are summarized in Table 10-6.

Table 10-6 Stakeholder Outreach

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	Continue existing stakeholder outreach activities and communications.
Identify communication and outreach needs	Determine the scope of information to share with stakeholders.
Conduct communication and outreach activities	Update communications to include cybersecurity in the formal risk management toolset.
Follow through on commitments and actions	Continue to follow-through on commitments to stakeholders.

10.8 Process Knowledge Management

10.8.1 Process Knowledge Management: Cybersecurity Concerns

Cybersecurity incidents like those perpetrated against the Natanz uranium enrichment facility (Section 6.2) [9] and the Saudi Petrochemical facility (Section 6.6) [10] illustrate the damage that can be done by a cyber-attack when detailed information becomes known about the process. Espionage attackers, like those who perpetrated the GreyEnergy malware (Section 2.1.1) [30], can obtain information such as confidential formulations and commercial information that could impact a company's competitive advantage. Information collected under the process knowledge element can be an incredibly attractive target for a cybersecurity attack. While this information needs to be available for legitimate users, care must be taken to block access by unauthorized intruders. Information provided by cybersecurity codes and standards (Section 10.4) and the Hazard Identification and Risk Analysis

(Chapter 9) can be helpful in determining what information is potentially at risk for cybersecurity attack.

A cyber-attack targeting process knowledge may have many objectives, including business interruption for ransom, theft of intellectual property for resale, access to business information to gain a competitive advantage, and sabotage. Identification of the type of process knowledge that may be subject to a cyber-attack - and understanding the attractiveness to cyber-attackers - is necessary to prioritize work activities and close gaps. Examples of process knowledge that may be of interest to attackers include:

- Process hazards information
 - o Reactive System Screening Tool/Vent Sizing Package/combustible dust testing data
 - o Chemicals and inventories
 - o HIRA records (process and cyber)
- Process technical information
 - o Material and energy balances
 - o Piping and Instrumentation Diagrams
 - o Process models
- Business information
 - o Raw material suppliers and pricing
 - o Product cost and profit margin
- Hardware & software
 - o Control systems updates and upgrades
 - o Firmware update
 - o Equipment make and model
 - o Network segmentation diagram
- Contractor access and security – e.g., design engineers, fire protection
- How to control, protect, and update control system logic, interlock tables and alarm tables etc.

Once a list of potentially cyber sensitive information is developed, the following questions should be answered:

- What else needs to be added to the scope of process safety knowledge?
- How is process knowledge stored?
- Who uses the process knowledge?

- What are the security and process risks?
- Who might want the information?
- What would a cyber-attacker do with this information?

10.8.2 Process Knowledge Management: Cybersecurity Activities

Implementing cybersecurity protections for process knowledge is complicated because the information is stored in many locations, often with different people or departments managing the information. The first step is to complete a system survey and catalog the locations where process knowledge is stored and the potential risk(s) if the knowledge is compromised. The Hazard Identification and Risk Analysis (HIRA) is a good starting place to identify critical process information so that the security status of information can be evaluated and the opportunity for unapproved access can be minimized. Methodologies for protecting process information will vary based on the answers to questions in Section 10.8.1. Written policies and procedures need to be developed to provide consistency to data management and ensure that cyber countermeasures are maintained.

One of the questions posed is “What else needs to be added to the scope of process safety knowledge?” The question could be rephrased as “What other knowledge do I need to secure in order to properly protect my process safety knowledge?” This knowledge may include information in hardcopies as well as information that is stored in multiple electronic locations. For example, the IACS may include devices that are identified by tag in the maintenance management system; however, the software version and patch control are managed in a separate spreadsheet. Also consider the information housed in a non-operations department. For example, IT is likely to manage the list of printers connected to the OT system with wireless capability. Consider what information may be stored off site under the control of vendors and contractors; how do the vendors and contractors protect the information against compromise?

Examples of information that may be stored by outside firms include:

- Engineering and design contractors – all types of engineering design and specification documentation.
- Controls and configuration contractors – detailed information about IACS hardware and software information.

- Fabrication contractors – detailed mechanical information on equipment and piping systems.
- Construction contractors – all types of engineering documentation, including construction details.
- Testing and analysis laboratories – Information regarding the properties of raw materials, intermediates and final products, including combustibility and reactivity potential.

Developing policies and procedures to manage the control of information with contractors is an important part of managing the exposure of process knowledge. An assessment of contractor cybersecurity program in the contractor qualification process can help to identify potential issues prior to beginning the project. Establishing requirements and expectations for the handling and security of such information while in the hands of contractors can help to protect sensitive information throughout the engagement.

Process knowledge needs to be secured against potential cyber-attack; however, it is important to assure that recovery of the information is possible should the data become compromised. The Business Recovery Plan should include process safety knowledge in the backup and the associated recovery scheme. A comprehensive list of process safety information and its storage location is also required to facilitate the identification of equipment for backup.

Establishing measures and metrics to monitor the health of process knowledge security management internally and with contractors can provide further information on the security of sensitive information. Routinely monitoring the metrics and periodically auditing the knowledge management and backup systems performance help to ensure that these processes work correctly when they are needed. Any issues or potential gaps identified during testing activities should be implemented in the procedures in a timely manner. Core principles of Process Knowledge Management, as well as cybersecurity specific considerations, are summarized in Table 10-7.

Table 10-7 Process Knowledge Management

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	Update the process knowledge management philosophy to address cybersecurity accessibility risks. Review and expand the scope of process safety knowledge to include relevant IACS equipment; assign responsibilities for the various types of process safety knowledge.
Catalog process knowledge in a way that facilitates retrieval	Incorporate newly scoped process safety information into catalog and retrieval systems.
Protect update process knowledge	Consider enhanced security requirements for documentation access. Ensure that documentation is kept up-to-date. Provide cybersecurity protection for backups of process safety information
Use process knowledge	Inform personnel about newly classified process knowledge and how to access it. Perform periodic reviews to confirm that process knowledge is current, accurate and complete.

10.9 **Operating Procedures**

10.9.1 *Operating Procedures: Cybersecurity Concerns*

The Maroochy Shire Sewage Spill case study given in Section 6.1 illustrates the potential harm that can be caused when a saboteur gains access to the control system [19]. The saboteur completed his attack by manipulating the setpoints of the process and process alarms [19]. In this case, process operators were able to recognize the process upset and attempt correction; however, they were unable to take sufficient action to avoid the incident. What if a saboteur were able to compromise the settings in an operating procedure or modify the step instructions, thus tricking the operators themselves into compromising process operation? Consider the potential impact if this approach leads to the

compromise of process safety alarm setpoints such that operators are not warned of a process upset. What if a Safety Instrumented Function (SIF) proof test procedure has the step “remove bypass” deleted, thus compromising the SIF availability?

Operating procedures are the written instructions that describe the routine activities associated with converting a raw material into a finished product. Examples include rail car connection, process operation modes (start-up, normal operation, shutdown, regeneration etc.) and routine in-process instrument calibration. Operating instructions and alarm management procedures are generally included in the scope of operating procedures. Procedures for non-routine activities like process troubleshooting and emergency shutdown are also included in the element scope. One might also extend the definition to include any procedure, such as a proof test procedure (often classified as a maintenance procedure), that assures the performance of the SIS during process operation. These types of procedures are written instruction providing detailed steps to complete each task and describing how the tasks are performed so that activities may be completed consistently. Personnel are trained to follow the procedures and learn to trust the guidance they provide. Unless the revision control has been updated, an operator may not recognize that the procedure content has been changed since it was last used. Unauthorized alteration of the procedure content could result in process upset, product compromise, or a safety incident.

10.9.2 Operating Procedures: Cybersecurity Activities

For the purpose of cybersecurity protection, an organization should consider expanding the definition of critical operating procedures to include those that safeguard operations or that could, if tampered with, results in unsafe operation. An organization could identify all procedures that if tampered with could result in unsafe operation and implement protective measures, similar to those discussed under Section 10.8, Process Knowledge Management. The risk assessment can be leveraged to evaluate the security status of procedures that contain sensitive information and reduce the opportunity for unapproved access.

The initial effort is geared toward identifying all procedures that need to be secured and improving the access controls to those documents. Procedures that should be considered for the list include:

- Process operating procedures.
- Alarm management procedures.
- SIS proof testing procedures.
- Procedures for software updates and patches to devices related to IACS.

The second effort puts a focus on making documents less susceptible to alteration or implementing a means to readily identify alterations. Consider providing additional separation between the master copies of procedures and a non-editable copy available to users. For example, an organization can maintain a master hardcopy of procedures that can be used to verify copies printed from an electronic system. Storing the master copies of procedures in a separate system with appropriate encryption and access control limiting access to only the users responsible for updating procedures can help to reduce the exposure.

While improving the security of procedures, an eye should be turned toward recovery in the event of a compromise. The procedure management system should include backup and recovery capabilities. For some procedures, this will include the document and the instruction within the document. For example, consider the procedure for performing an update to the BPCS software. The procedure likely includes a step-by-step checklist for the software update. Consider including a printed checklist where the user can record execution (using initials) of each step as it is performed. Some steps could also require documentation of system step confirmation feedback by recording the information by hand or capturing screen prints as part of the update log. This information may be useful if it is necessary to “rollback” the update or troubleshoot results.

Some procedures may be stored and used in a digital format. For example, SIS proof test procedures may be included in a software package designed to permit the procedure to be taken to the field on a tablet, where data can be entered real time and then uploaded to the software for tracking and analysis. Robust password protection and data encryption should be

considered to protect these types of systems. Core principles of Operating Procedures, as well as cybersecurity specific considerations, are summarized in Table 10-8.

10.10 Safe Work Practices

10.10.1 Safe Work Practices: Cybersecurity Concerns

Safe work practices (SWP) are a set of documents that, like operating procedures, describe the methods and tools to be used in executing a scope of work. Safe work practices differ from operating procedures in that they are more broadly applicable (e.g., multiple companies, sites, or process units), whereas operating procedures are typically defined specifically for an individual operating environment. The purpose of SWPs is to control hazards and manage risk associated with activities that are not part of the normal sequence of operation. Examples include interlock bypass management, lock out/tag out, hot work, line break, confined space, relief device removal for recertification, and other non-routine work.

SWPs are typically generated in a word processing format, and the master files are likely housed on a centralized server. While it is technically possible for a cyber-attacker to gain access to the procedures and modify the content, the potential for harm will vary with SWP. Altering the procedures themselves may not offer an attractive opportunity to do harm, but they could be used to collect intelligence information that could be used in preparing a targeted attack.

Table 10-8 Operating Procedures

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	Incorporate cybersecurity concerns to protect the integrity of operating procedures. Address backup and business recovery requirements for procedures.
Identify what operating procedures are needed	Complete a task analysis to determine the procedures that need to be revised or developed to address cybersecurity risk with respect to the safe operation of the process.
Develop procedures	Consider inclusion of a checklist that provides both guidance in step execution and means of documenting activity.
Use procedures to improve human performance	Incorporate cybersecurity considerations into existing practices: Ensure that procedures are available. Hold organization accountable for consistently following procedures.
Ensure that procedures are maintained	Incorporate cybersecurity considerations into existing practices: Correct errors and omissions in a timely manner. Conduct periodic review and formally manage procedure changes.

Some SWPs that may be of interest to cyber-attackers because alteration could cause an incident include:

- Cybersecurity procedures and practices
- Fire system impairment procedures and authorizations
- Interlock bypass procedure and authorizations
- Control systems procedures and authorization (abort keys, manual mode, process parameters)
- Valve locking procedure and management list (open or closed)
- Critical maintenance activities

- Equipment specific lockout and isolation procedures
- Procedures for maintaining integrity of cybersecurity countermeasures (see Chapter 11)

10.10.2 Safe Work Practices: Cybersecurity Activities

The first step is to identify all safe work practices and implement protective measures similar to those discussed under Section 10.8, Process Knowledge Management. Drawing from the risk assessment to evaluate the security status of information helps to prioritize steps to reduce the opportunity for unapproved access. Safe work practices subject to cybersecurity threat should be maintained in a manner similar to that described for operating procedures (Section 10.9). Limiting access, robust password protection and encryption should be considered. Core principles of Safe Work Practices, as well as cybersecurity specific considerations, are summarized in Table 10-9.

Table 10-9 Safe Work Practices

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	Incorporate cybersecurity countermeasures to protect the integrity of safe work practices.
Effectively control non-routine work activities	Review safe work practices where errors could result in impairment or compromise of a safety system and update to include additional steps for confirming function prior to return to service.

10.11 Management of Change

10.11.1 Management of Change: Cybersecurity Concerns

A recent case study illustrated that “replace in kind” is not as simple as matching model numbers for electronic components. During a planned outage at a manufacturing plant, switches in the alkylation unit Process Control Network (PCN) were replaced. The replacement switches were from the same manufacturer and had the same hardware model number; however, they had newer firmware. When the process was restarted, the PCN began to experience problems, including loss of view of six units and a loss of control across the network. This resulted in a seven-hour outage to roll back the switch upgrade. The event was initiated by a bug in the switch firmware, and the event escalated due to a previously unknown flaw in the overall system configuration that prevented reconciliation of the errors caused by the firmware bug. [109] This incident demonstrated that replacement-in-kind must consider not only the hardware but all aspects of the device (including firmware version and configuration), as well as the environment in which it will be used.

The objective of Management of Change (MOC) is to recognize change situations, evaluate the hazards associated with the change, determine whether to allow the change, and provide necessary risk control and follow-up. Integrating cybersecurity concerns into the MOC process assures that process safety systems remain protected against cybersecurity attack and that IACS remains fully functional. The scope of work requiring MOC may need to be revised as well to capture additional items related to cybersecurity. In addition, all cybersecurity changes should follow MOC procedures to ensure that existing cybersecurity protection measures are not compromised and to avoid the failure to put in place new countermeasures when systems are modified.

10.11.2 Management of Change: Cybersecurity Activities

The first step is to establish a cyber-competent MOC champion to function as the MOC review and approval authority. This champion should also participate in developing modifications to the MOC process and scope to incorporate cybersecurity concerns. Organizations should identify the types of changes

that may not currently be included in the MOC program and place a temporary hold on the activities until requirements are defined. Any “backdoor” access to IACS systems should be immediately closed to prevent unauthorized or unreviewed changes.

The existing MOC process should be updated to incorporate cybersecurity concerns. When evaluating the change, the cyber risk assessment can be used as a useful reference to identify if the proposed change will have an effect on the current level of risk, and if any additional countermeasures will be required to achieve an acceptable level of risk. Updating the MOC procedure with a checklist of the items requiring cybersecurity evaluation can help to ensure that no changes are missed.

The definition of “replace in kind” may need to be updated to address the cybersecurity point of view. The CCPS glossary [1] defines replacement-in-kind (RIK) as “An item (equipment, chemical, procedure, etc.) that meets the design specification of the item it is replacing. This can be an identical replacement, or any other alternative specifically provided for in the design specification, as long as the alternative does not in any way adversely affect the use of the item or associated items.” From a cybersecurity perspective, replacement-in-kind means the same hardware, software version and (where applicable) firmware version, as well as the same configuration for an asset. Different features can be enabled in different versions of firmware and software (even if the model number is the same), which may introduce faults or increase the cybersecurity exposure (e.g., addition of web servers in new firmware versions, more recent version of network equipment). Newer versions are not always safer versions. One method for ensuring that a new network device is truly replacement in kind is to compare the software hash for the program. A software hash is a unique digital fingerprint, which is generated from a mathematical function which converts the data in a computer program to a numeric value. If even one piece of data is different between the programs the software hashes will not match. When completing a hardware or software change that is not replacement in kind, it is often beneficial to include full verification testing (SIF proof test, interlock trip test, control function test) in the project scope to confirm function before restart.

Defining the scope of a cybersecurity change and the roles and responsibilities for managing the change are early requirements. Different individuals may be responsible for different types of change. The justification for change and methods to manage the change may vary as well; for example, some types of changes may be permissible on an emergency basis. Potential types of cybersecurity changes and associated points to consider include:

- Systems
- Cybersecurity countermeasures (endpoint protection, security monitoring, system hardening).
- Addition or removal of hardware
- Configuration of IACS assets
- Software and firmware patch updates
- Webserver firmware updates
- Controller downloads
- Procedural
- Responsibility for review and approval each type of change (e.g., BPCS software upgrade, connecting a new printer to IACS network).
- Avoiding unrecognized “change” (e.g., connecting phone to computer for charging, attaching new printer, instrument firmware update not vetted).
- Policy
- Firewall rules.

All changes need to include updates to the documentation used to manage cybersecurity information and communication of changes. Documentation to be updated includes:

- Zone & Conduit Diagram.
- Hardware and software asset management list.
- IACS access control list.
- Maintenance records to reflect instrument software update, including update of model numbers in equipment identification records to reflect change.
- Communication and training materials after major updates. For example, BPCS software update may provide new features or revise existing.

Cybersecurity Assessments are included in ISA TR84.00.09 as verification activities to be conducted at specific phases of the lifecycle [80]. Cybersecurity

Assessments 1-4 are typically initiated as part of other elements, as summarized in Section 10.21.2. Cybersecurity Assessment 5 is performed to confirm activities associated with modification and decommissioning. The scopes of all MOCs should be evaluated to determine if a Cybersecurity Assessment 5 is required. Core principles of Management of Change, as well as cybersecurity specific considerations, are summarized in Table 10-10 .

Table 10-10 Management of Change

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	Modify the MOC program to incorporate cybersecurity considerations and include cybersecurity changes. Establish and train an MOC approval authority for cybersecurity concerns. Close ‘backdoor’ access for modification. Include MOCs in cybersecurity periodic review and audits.
Identify potential change situations	Define ‘change’ with respect to cybersecurity. Establish guidance to define what changes may be permitted on an emergency basis.
Evaluate possible impacts	Conduct a cyber risk assessment as part of the MOC implementation and review.
Decide whether to allow the change	Designate one or more person(s) with cybersecurity competency to provide change authorization for MOCs with cybersecurity elements.
Complete Follow-up activities	Update records and communicate changes.

10.12 Asset Integrity and Reliability

10.12.1 Asset Integrity and Reliability: Cybersecurity Concerns

The purposes of the Asset Integrity and Reliability element are to prevent catastrophic release of chemicals or energy from the process and to assure the availability of critical safety and utility systems. Examples of the systems and equipment considered by this element include process equipment, IACS, mechanical prevention and mitigation measures (e.g., relief devices, containment dikes), utility systems, and fire detection and protection systems. The systems are managed with a combination of inspection, testing, preventative and predictive maintenance, and repair or replacement. The work is guided by written maintenance procedures, performed by specially trained personnel, and verified under a quality assurance program.

From a cybersecurity perspective, asset integrity and reliability are about assuring that the systems providing protection against cyber threats are available and perform reliably when needed. Asset integrity and reliability is also concerned with monitoring system performance to detect issues so that they may be addressed promptly. Without proper integrity and reliability management of cybersecurity assets, there is no barrier to prevent cyber-intrusion, leaving the organization open to potential theft, business interruption and physical damage.

10.12.2 Asset Integrity and Reliability: Cybersecurity Activities

Cybersecurity items should be integrated into the asset integrity management program and should undergo similar management activities. The first step is to define which assets, including those in maintenance stores, need to be considered under the program and what cybersecurity concerns are associated with those assets. Items to consider include:

- Network equipment (e.g., switches, routers), servers, workstations, boundary devices (e.g., firewall), access points, wiring and other equipment.
- Control system logic solver, workstations, configuration libraries, third-party access points, and support equipment.
- Safety Instrumented System logic solver, workstations, configuration libraries, third-party access points, and support equipment.

- Devices with wireless capability such as smart transmitters or IIoT devices
- Devices that are located outside the facility's physical security (e.g., pipeline sensor, remote pump station)
- Condition control and monitoring systems for spaces impacting process conditions and product safety. (e.g., clean rooms, cold storage)

One asset type - vendor package units - may require multiple approaches to maintaining integrity. Site-owned package units, such as compressors and boilers, may include a dedicated control PLC and sometimes have a separate safety shutdown logic solver. These generally communicate with the site control system. These systems may be generally isolated from direct communication outside the facility; however, they may be equipped to transmit maintenance monitoring information to the supplier (but are not typically intended to receive information). In this case, cybersecurity concerns may be entirely under the control of the plant. A facility may also have package systems that are owned by the vendor and leased to the operating facility. This type of system is generally connected to the plant control system for operational purposes but is also connected to the vendor systems for the purpose of monitoring raw material supply and equipment performance. In this case, there will be shared responsibilities for cybersecurity. It is important to ensure that the vendor has a cybersecurity management system in place as well to provide appropriate protection measures for the plant so that package communications cannot become potential points for cybersecurity intrusion.

Once the assets have been identified and the cybersecurity concerns are known, then the Asset Integrity Management Plan needs to be updated to include new or modified inspection, test, repair, and maintenance activities. Competency requirements for personnel conducting the activities need to be defined to ensure that they are appropriately trained and require certifications where appropriate. The plan should define any special tools or software required to execute the plan. The plan should also include a schedule for the execution of each activity.

Some topics to consider in the development of the plan and schedule include:

- How are the personnel competency requirements for each task determined? Many tasks require specialized training.
- What information needs to be tracked and analyzed to assess asset integrity and reliability? What analysis methods are appropriate for different types of data?
- Do existing maintenance and testing procedures need to be changed to incorporate cybersecurity concerns or improve existing methods? For example, consider including as found/as left documentation steps in SIF proof test procedures to provide data for analysis that better monitors the condition of the SIF.
- What process and maintenance data should be tracked and analyzed to monitor cybersecurity performance and support incident investigation? What is the appropriate data sampling rate and data retention timeframe for each data type? Consider process items such as demand information in BPCS, alarm performance, faults and false alarms, critical process conditions.
- What asset information is required to support an effective auditing program? A list of assets with detailed model numbers, firmware version, and software version, provides a basis for the audits. Revision tracking is used to confirm asset integrity management and update activities are conducted in accordance with procedures.
- What controls support may be required remotely? Vendor technical support may be required to troubleshoot operational problems. Controls group coverage is often staffed on-site during core business hours but handled on call on nights and weekends. How is the access managed to provide cybersecurity control and protections regarding who has access and what can be accessed through this pathway?
- How are wireless components documented and protected against undesired access? How can their security health be monitored?
- What assets may be accessed or updated by 3rd parties? For example, instruments are sometimes sent offsite for refurbishment, or calibrated in a mobile technician shop during a turnaround. How are 3rd parties vetted to confirm they have cybersecurity controls in place? What checks are required in house before returning these devices to service?

Cybersecurity introduces new considerations into the site asset management philosophy, procedures, and procurement process as well. Older devices may be at higher risk for cyber compromise, either because they were not designed to address cybersecurity issues or because they are so common that hackers have developed methods to exploit these devices in an attack. Steps to consider when updating the repair, replacement, and procurement guidelines include:

- Confirm that manufacture and installation date are recorded for assets where cybersecurity concerns are to be addressed for integrity management, along with the model number, hardware, firmware version and software version. Review the inventory against a resource such as the National Vulnerability Database (NVD) [99] to identify which items might have known vulnerabilities, thus posing a higher risk of exploitation. Develop a prioritized plan to patch or replace these items.
- Prepare an obsolescence management plan. Replacement of many items in a production facility is based on a run to failure (reactive) philosophy. Safety Instrumented System (SIS) components are examples of equipment that is proactively scheduled for replacement based on useful life. There may be cybersecurity considerations for some components that shift the replacement mode from the reactive to proactive philosophy. For example, legacy systems may no longer be supported by the manufacturer and lose their technical currency. An end user is sometimes unable to obtain updates and patch such systems to maintain security.
- Update the repair and replacement parts sourcing philosophy. Utilize authorized suppliers with established cybersecurity management programs. Resist purchasing items, new or used, from e-commerce sites or unauthorized supply houses where the cybersecurity, reliability and service life are unknown.
- With respect to cybersecurity, newer is not necessarily better. Section 10.11 discussed that replacement-in-kind means the same hardware, software version, and (where applicable) firmware version for an asset. New features and software and firmware updates can increase cybersecurity exposure. When specifying new equipment, consider cybersecurity considerations when selecting features and software version.

Reviewing cyber-attack reports should be an ongoing practice to support the identification of new vulnerabilities or changes to existing vulnerabilities. Consider the use of continuous monitoring or Security Information and Event Management systems that would provide visibility into the current state of the network and identify if assets have been compromised. Finally, consider if the existing integrity management system and support tools can effectively support cybersecurity concerns for asset integrity and if they can be properly protected from cybersecurity threats. For example, installing a computerized maintenance management system (CMMS) to manage workflow, capture data and support reliability analysis may be more cost-effective than hardening multiple legacy tools. Core principles of Asset Management and Reliability, as well as cybersecurity specific considerations, are summarized in Table 10-11.

Table 10-11 Asset Integrity and Reliability

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	• Incorporate cybersecurity items into the written asset maintenance and integrity program. • Confirm that repair parts and replacement items conform to specification. • Track and analyze maintenance and reliability data. • Ensure that personnel engaged in asset maintenance and integrity activities are fully qualified. • Stay abreast of cybersecurity attack reports and adjust plan as new threats become known.
Identify equipment and systems that are within the scope of asset integrity program and assign ITPM tasks	• Identify equipment and systems that may be at cybersecurity risk. Incorporate items with cybersecurity concerns into the inspection, testing, and preventive maintenance (ITPM) plan and schedule the appropriate activities.

Table 10-11 continued

RBPS Key Principle	Cybersecurity Considerations
Develop and maintain knowledge, skills, procedures, and tools	• Develop procedures for inspection, testing, repair, and other critical maintenance activities. • Train personnel and ensure that they obtain competency certifications where needed. • Obtain specialized tools and software, as needed, to support reliability and integrity activities.
Ensure continued fitness for purpose	• Schedule SIS component replacement/refurbishing before the end of useful life. • Monitor systems for anomalies and investigate to determine threat potential. • Plan, control and execute calibration, maintenance, and repair activities. • Confirm the quality of repair/refurbish parts and maintenance materials.
Address equipment failures and deficiencies	• Promptly repair all deficiencies and failures within IACS and systems that support IACS health. • Review test and inspection reports and track failures over time. Evaluate the reports to identify chronic failures and common cause concerns. • Perform timely inspection, testing and maintenance according to the plan.
Analyze data	• Collect and analyze data for IACS failure rates, process demands, alarm rates and system reliability metrics. • Investigate failures for availability, reliability, and common cause concerns. • Maintain data archives for established data retention periods.

10.13 Contractor Management

10.13.1 Contractor Management: Cybersecurity Concerns

The utilization of contractors is sometimes a necessity to augment staff and engage expertise that is not available within the permanent staff. However, many contractors perform activities that could have a cybersecurity impact. The controls system engineer performing updates to the BPCS software has a role with the obvious opportunity to do harm. However, what about the temporary receptionist, or the person who services the printer/copy machines? Should we be concerned about contractors installing equipment, piping, and instrumentation? The cybersecurity risk exposure associated with contractor roles will vary based on the level of access required to complete their jobs. Roles like the control system engineer or the temporary receptionist require login credentials to complete their work. The access level provided to the controls engineer could permit direct sabotage, with the possibility of very serious consequences. The receptionist has a more tightly controlled level of access, but even this level of access could lead to a security event in the IT system. The person servicing the printer/copy machine likely does not have credentials to login into the network; however, they could gain access through the computer interface of the machine being serviced. The contractors installing equipment, piping and instrumentation could easily connect a thumb drive to a computer, printer or copier while working in a restricted area. Potential consequences of improper cybersecurity management by contractors include theft, business interruption, property damage, and safety impacts.

10.13.2 Contractor Management: Cybersecurity Activities

The contractor management program should be updated to address cybersecurity risks that result from using contract personnel. The means to control the risk is dependent upon the role of the contractor and the access required for the scope of work. After developing a list of contracted service types, a Job Cyber Assessment (JCA) can be performed on each type, beginning with the roles that require the most direct system access. The JCA technique can identify cyber hazards related to job activities and identify a targeted implementation of preventative measures. Figure 10-1 is an example of a Job Cyber Assessment.

Job: Downloading IACS Controller Firmware		
Analysis By: <i>Instrument Technician</i>	Reviewed By: <i>Commissioning Supervisor</i>	Approved By: <i>Site Security Lead</i>
Date: 10/10/2020	Date: 10/10/2020	Date: 10/10/2020
Sequence of Steps	Potential Cyber-Hazard	Preventative Measures
<i>Connect DMZ workstation to enterprise workstation</i>	<i>Potential for malware on enterprise network</i>	<i>No direct connection between enterprise network and DMZ</i>
<i>Download ICS Controller Firmware</i>	<i>Potential for malware/ misconfiguration in firmware</i>	<i>Firmware is tested in next step</i>
<i>Test Firmware for known Malware</i>	--	--
<i>Connect engineering workstation to DMZ</i>	<i>Potential for malware on DMZ</i>	<i>No direct connection between enterprise network and DMZ</i>
<i>Download ICS Controller Firmware</i>	<i>Incorrect Functionality</i>	<i>Firmware is tested in next step</i>
<i>Test ICS Controller Functionality</i>	--	<i>Confirm Firmware version matches Manufacturer's recommendation</i>

Figure 10-1 Example Job Cyber Assessment

The contractor evaluation process and contractor management procedures should be modified to address the implementation of preventative measures. Cyber considerations can be added to the contractor qualification process, along with a decision guide to determine which criteria are applied based on the nature of the service. For example, for a controls system contractor, the qualification process might include a review of their cybersecurity program. How does the contractor ensure that the personnel working on an assignment are competent, trustworthy, and have no cyber-related criminal history? An organization can establish a procedure for vetting

contractor personnel individually if their role poses a cybersecurity risk. The procedure should include criteria to determine which personnel should be vetted and a list of background information to be provided. For roles where the contractor does not need access to computerized systems in execution of the job, the qualification process may be less focused on the contractor's cybersecurity program.

The contracting and onboarding process should make organizational cybersecurity expectations clear. The topics to be discussed will vary with the responsibilities of the contractor's job. For example, the general site safety orientation delivered to all site visitors may describe policies regarding use of mobile data devices and prohibit usage of a site computer. A contractor whose job requires access to computerized systems may receive a more in-depth orientation regarding the procedures and documentation requirements specific to the job task (e.g., software updates, patch management, proof test procedures).

The contractor management program needs to address special cases, such as arrangements whereby the facility leases a package system and relies on the vendor for servicing. The Maroochy Shire incident [19] summarized in Section 6.1 illustrates the type of event that can arise when using contractors. The event involved a former employee of an industrial control system integrator. In his role as site supervisor during the project, he was granted access to control systems and physical access to equipment systems. When his services were terminated, he was able to execute multiple attacks using equipment (a radio) stolen for the site and detailed knowledge acquired while on-site. Long-term arrangements have a risk whereby an embedded contractor has access to sensitive systems and process technology and has the knowledge to cause harm. Trust becomes an important part of the relationship. In most instances, the work the contractor was hired to do comes to an end and the work relationship is dissolved. The contractor management program should include provisions to bring long-term contractor relationships to a close in a way that limits the opportunity for an event like the Maroochy Shire incident. The program should include immediate termination of system access and the return of any assigned company equipment. An organization can limit the potential usage of items acquired through opportunistic theft by

good physical security practices, careful inventory control, and having the ability to disable electronic equipment remotely.

Periods such as a turnarounds or control system upgrade, with heavy contractor presence on site, provide an increased opportunity for systems access. Consider conducting a thorough systems check or an audit following these activities to confirm the ongoing health of cybersecurity systems. Core principles of Contractor Management, as well as cybersecurity specific considerations, are summarized in Table 10-12.

Table 10-12 Contractor Management

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	Establish cyber related contractor qualification criteria. Develop guidelines for cyber competency requirements of contractors.
Conduct element work activities	Establish expectations with contractors.
Monitor the contractor management system for effectiveness	Monitor and evaluate contractor performance. Perform a ‘health check’ on systems following contractor updates in addition to normal periodic reviews.

10.14 Training and Performance Assurance

10.14.1 Training and Performance Assurance: Cybersecurity Concerns

The Bayer Crop Science incident in Institute WV illustrated the consequences that can occur when operators are unfamiliar with or confused by control system information [110]. On August 28, 2008, a pressure vessel exploded, causing two fatalities and injuring eight people. The incident occurred during process startup following an extended outage to replace equipment and upgrade a control system. A number of control

system issues contributed to the event. There was an incomplete commissioning and calibration of DCS which resulted in centrifuge operation issues [110]. A malfunctioning relay caused centrifuge trips, and inadequate process tuning led to sluggish control response. The operating procedure had been revised to reflect equipment modification but did not include operating details for the new control system. At the time of the incident, revisions to the procedure were incomplete, so the operators were using an unapproved draft.

The operators had received some training on the DCS system (although on a different process) and were somewhat familiar with the display functions for the methomyl unit. However, these screens on the methomyl process were more complex, the method for command entry (mouse vs keyboard) was different, and some operating variables were displayed in different units than the previous DCS [110]. Inadequate training played a central role in the incident, contributing to several contributing factors: lack of experience with the newly installed control system, insufficient technical experience in the control room during startup, bypass of critical safety devices, and misalignment of valves [110].

The cybersecurity management techniques and countermeasures put in place will have limited effectiveness unless personnel are trained to use them effectively. This will require training on a wide variety of topics targeting specific audience groups. These include:

- General awareness training for all users.
- Organization specific training for those performing cyber duties, targeting access as well as the use of company procedures.
- Specific technical training addressing tools and techniques for cybersecurity management.
- Targeted training required to build competency level or achieve certification.
- Participation in cybersecurity conferences and workgroups.
- Refresher training.

An overall training plan should be developed, identifying who needs training, what type of training is required, and a schedule for implementation.

This will ensure that training is completed in a timely manner. Training content should be periodically reviewed and updated to maintain the currency of information about threats, vulnerabilities, and proper response behavior.

10.14.2 Training and Performance Insurance: Cybersecurity Activities

Training requirements for roles will vary with the responsibilities of the job role. Conducting a Job Cyber Assessment (JCA) is a good way to define the training plan for individual job roles, determine how to group training content for effective training delivery, and identify what training topics can be addressed in house and what topics need for outside training. (Refer to Figure 10-1 for a sample JCA worksheet.) Information documented in the JCA worksheet may include:

- List of jobs and task steps.
- List of related cyber hazards associated with each step.
- Hazard mitigation plan for each step, as applicable.
- Personnel accountable for mitigation.
- Participants in the JCA.
- Supervisor approval.

Confirming the effectiveness of training needs to go beyond a simple test at the end of class. Periodic assessment in the form of planned drills or random challenges can be very effective in reinforcing skills. For example, a phishing security test is conducted by sending an email to users and tracking responses. If the link is clicked, the user can be directed to a landing page where they are notified that they just participated in a test and are provided with some refresher training information on identification of phishing attempts and proper action to take. A similar test can be done with removable media by dropping a USB loaded with a tracking file in a parking lot, lobby, or breakroom and monitoring the response. The USB drop and other random challenges should also include a refresher training activity as well.

Cyber threats are constantly evolving. Attack methods change rapidly. Hackers are constantly working to exploit device vulnerabilities, and efforts to identify and close the gaps are ongoing. Modular training (small 20-minute sessions) can be an effective tool to quickly disseminate information about new threats and boost knowledge boost between formal training updates.

Core principles of Training and Performance Assurance, as well as cybersecurity specific considerations, are summarized in Table 10-13.

Table 10-13 Training and Performance Assurance

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	• Define the roles and responsibilities for cybersecurity concerns. • Document training and confirm training effectiveness. • Formally control the training program and the dissemination of knowledge bulletins
Identify what training is needed	• Conduct job/task analyses and regulatory reviews to identify minimum requirements. • Determine the training content for various responsibility level requirements
Provide effective training	• Develop training materials and update the content periodically. • Develop training options for specialized activities (expert level). • Provide initial training and refresher training on a defined schedule.
Monitor worker performance	• Monitor performance with security tests and drills. • Update qualification requirements periodically

10.15 Operational Readiness

10.15.1 Operational Readiness: Cybersecurity Concerns

The BP Texas City explosion and fire demonstrates the consequences of failed instrumentation. On March 23, 2005, an explosion occurred from a vapor cloud in the isomerization unit, causing 15 fatalities and injuring 180 people [111]. The explosion occurred when a raffinate splitter tower was overfilled during a restart of the isomerization (ISOM) unit following a lengthy turnaround. Inadequate instrumentation and ineffective

mechanical integrity were cited as causes of the incident [111]. The tower was equipped with a level transmitter (for control and high-level alarm) and a hardwired switch (alarm). The level transmitter was malfunctioning and was slated for repair after the startup, and a pressure control valve that vents pressure from the tower was also malfunctioning. The redundant hardwire switch failed, but the failure was not detected prior to the event.

Operational readiness is the verification activity confirming that all safety requirements have been met and all protections are in place prior to transitioning from a shutdown state to startup to normal operation. A discrete activity such as Pre-Startup Safety Review (PSSR) is a common tool that provides a framework to confirm the process is ready to start. Shutdown activities often include updates or modifications to control software or logic, updates and patches of component logic and repair, and replacement or upgrades to controls and instrumentation. These activities provide an opportunity for a cybersecurity incident; therefore, it is important to confirm that the systems are functional and free of cyber compromise before returning to normal operation. Failed and bypassed level instrumentation played a direct role in the 2005 Texas City explosion [111]. While the instrumentation issues were not due to a cyber-attack, the event serves as a reminder about the potential consequences that can result when critical instrumentation is compromised during startup.

Cyber considerations should be included in the process operational readiness procedures and checklists. Activities like confirming that bypasses are removed and verifying the correct function all SIFs which were modified (including changes to the application program) should already be in the PSSR. In addition, the PSSR checklist should be modified to require a review of cybersecurity specific concerns:

- What additional cybersecurity checks are advised that may not currently be considered?
- Should job specific checklists be developed for common activities?
- What should be included on a PSSR checklist where the control system was upgraded, version updated or patched?

- What are the competency requirements for personnel who sign off on cybersecurity aspects of the PSSR and MOC?

The ISA TR84.00.09 technical report [80] identifies steps in the cybersecurity lifecycle known as Cybersecurity Assessments (CSA) where an independent review of all previously completed lifecycle steps is conducted. The third CSA is designed to be completed in parallel with traditional PSSR activities. Completing a CSA 3 can support developing a robust method for answering cybersecurity questions prior to startup and ensure that all cybersecurity findings and recommendations are resolved prior to sign off.

10.15.2 Operational Readiness: Cybersecurity Activities

The first priority to address operational readiness for cybersecurity concerns is to establish the requirements that need to be addressed. What are the assets that need to be considered, and what are the potential consequences if a vulnerability is not detected? The asset list developed for the Asset Integrity and Reliability element described in Section 10.12 can provide consequence information useful for prioritizing operational readiness support tools. For example, the scope of work for the next scheduled turnaround may give a good indication of the operational readiness support tools that might be needed in the short term. For example, a generic check list for instrumentation with programmable capability may be a high priority because it will be utilized for multiple devices during the turnaround. On the other hand, developing a detailed, “ready to operate” checklist for a control systems upgrade may be a lower priority if there are no control system modifications planned for the next outage.

Another high priority step is to develop “ready to operate” decision gate criteria. Which checklist items must be completed prior to startup, and which may be deferred? Defining the documentation requirements for deferred items and tracking closeout of the items to completion is an important step in managing potential cybersecurity exposure.

For cybersecurity concerns, operational readiness may take on a different framework and may need to be addressed at different times and in different ways. Does the identification of a cyber-attack automatically trigger a ‘not ready to operate’ state (e.g., need to shut down), or does it trigger an

emergency state where the plant continues to operate, and additional controls are required?

The content of operational readiness checklists and the readiness review scope will vary based on the types of cyber related assets included in the outage scope. The list of checks and balances required when updating BPCS software will be extensive. Are the updates always done on a ‘clone’ system such as a digital twin (Section 3.2.2), tested, and then deployed? If not, what testing is required before the process is considered ready to operate?

The cybersecurity operational readiness checklist should include many of the same questions as the HIRA cybersecurity checklist (See Table 9-10), with a focus on how the concerns have been addressed. Some additional things that should be included in readiness review, regardless of the outage scope of work, include:

- Confirm that bypasses have been removed from interlocks.
- Confirm that controls have been tested and are password protected.
- Confirm that training has been completed.
- Update documentation for cybersecurity content (e.g., logic solver version control, instrument specification update software revision).

Core principles of Operational Readiness, as well as cybersecurity specific considerations, are summarized in Table 10-14.

10.16 Conduct of Operations

10.16.1 Conduct of Operations: Cybersecurity Concerns

On February 5, 2021, hackers compromised the Oldsmar Water Treatment Facility in Pinellas County Florida [75]. The hackers likely gained access to the control system through a remote access application that was no longer used but had not been uninstalled. The hacker was able to modify the concentration of sodium hydroxide (lye) by a factor of 100. Fortunately, an observant operator noticed the mouse moving across the screen and was able to regain control and reset the concentration to its correct value [75].

Successful cybersecurity management depends heavily on disciplined conduct of operations. Personnel need to be alert to the potential for cyber-attacks, use judgement to identify attacks, and properly act to contain the attack. The procedures for use, maintenance, and update of ‘all things computer’ must be followed faithfully. Good electronic hygiene and responsible password management are expected. An organization should define the expectations for personnel behavior in the governing policies and procedures and communicate the consequences for failure to follow procedures.

Table 10-14 Operational Readiness

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	• Incorporate cyber readiness checks into operational readiness procedures and checklists. • Determine what cybersecurity activities that occur in operating states other than shutdown should trigger a cyber operational readiness review. • Define scope(s) and personnel competency requirements for cyber readiness reviews. • Include cybersecurity requirements in the “ready to operate” decision gate and follow up tracking.
Conduct appropriate readiness reviews as needed	• Provide a detailed list of modification as input to the operational readiness review. • Define cyber roles and responsibilities for readiness reviews.
Make startup decisions based on readiness results	• Document (including potential consequences) cyber-related action items deferred to after startup. • Communicate the risks associated with incomplete cyber scope action items.
Follow through on decisions, actions and use of readiness results	• Follow through with timely resolution of cyber action items. • Update records for cyber content.

Reflected cybersecurity expectations in individual performance objectives and assessment criteria highlight the importance of cybersecurity. Key expectations include:

- Effective recognition of anomalies and proper response.
- Training workers to self-check and peer check.
- Adherence to policy and procedures including access controls.
- Prompt response, including the reporting of suspected attack and immediate correction of deviations.
- Maintaining instruments and tools to assure IACS remains in top performance condition.
- Maintaining accountability: celebrating the wins (attack recognition and correct action) and learning from the failures.

10.16.2 Conduct of Operation: Cybersecurity Activities

Procedures and tools need to be in place to guide personnel's behaviors in the desired direction and support personnel in conducting work activities. Maintaining up-to-date design documentation, labeling equipment and wiring in the field to match documentation, and providing quick reference tools are all important steps of developing proper operational conduct. Guidance such as decision trees to help personnel decide appropriate response to a suspected attack can further improve the response after an attack is identified.

Routinely monitoring system performance helps to identify when adjustments to improve the program are needed. Monitoring activities include:

- Observing systems to identify unauthorized activity.
- Scanning systems to evaluate if an attack has taken place.
- Performing field inspections to confirm design documentation and field conditions are consistent.
- Conducting routine audits.
- Implementing leading and lagging indicator metrics and sharing the results.
- Periodically conducting a Cybersecurity Assessment 4 to evaluate the current state of cybersecurity.
- Performing a periodic management review focused on cybersecurity.

Core principles of Conduct of Operations, as well as cybersecurity specific considerations, are summarized in Table 10-15.

Table 10-15 Conduct of Operations

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	• Define the roles and responsibilities for reporting and management of suspected cyber-attacks
Control operations activities	• Develop procedures that define actions required for monitoring system status and response to a suspected cyber-attack. • Assign and prioritize resources to conduct monitoring checks on a defined schedule. • Establish a formal protocol for communication with personnel. • Control access to cyber sensitive systems.
Control the status of systems and equipment	• Monitor for potential cyber incursions and attacks against barriers. • Maintain labeling, instruments and tools.
Develop required skills/behaviors	• Train personnel to recognize anomalies. • Maintain diligence in observation, reporting and follow-up of anomalies.
Monitor organizational performance	• Maintain accountability and strive for continuous improvement. • Conduct periodic inspections. • Promptly respond to reports of potential threats and correct deviations immediately.

10.17 Emergency Management

10.17.1 Emergency Management: Cybersecurity Concerns

Eventually, all organizations will likely experience some sort of cybersecurity incident. A Cybersecurity Incident Response Plan is necessary to properly prepare for the emergency response needed to mitigate the consequences and recover from the event. The response to potential attacks is similar to the response for industrial accident emergencies in that the same five actions are included:

1. Plan for possible emergencies.
2. Provide resources to execute the plan.
3. Train and inform personnel.
4. Practice and continuously improve.
5. Effectively communicate with stakeholders.

The objectives of cybersecurity incident response are to address the threat before it has an opportunity to escalate into a loss event and to quickly respond to an event once it has occurred to minimize the consequence and recover quickly. The scope of cybersecurity incident response lies in the management of both intentional and unintentional cybersecurity events. Should a cyber-attack escalate into a process safety event, then the process safety Emergency Management Plan should also be followed.

The Cybersecurity Incident Response Plan addresses an overall approach to addressing all types of incidents. The plan should include identification of incident types (malware, extortion, denial of service, espionage, sabotage). Topics and clarifying questions that should be defined for each type of incident are defined in Table 10-16.

Table 10-16 Incident Response Plan Considerations

Topic	Clarifying Questions/ Notes
Scope of the response effort	Which systems may be affected, and what is the operational consequence of a successful attack?
Tools and techniques to monitor for and identify potential attacks	What cybersecurity alarms, alerts, and diagnostics are needed, and how are they to be utilized?
Roles and responsibilities	The roles that may need to respond to a cyber-attack should all be identified and defined in the response plan. For example, response to an extortion attack may be addressed by a few IT people, and operations administration may be asked to cease normal activity. A targeted sabotage attack will require the engagement of both operation and process control personnel.
Operational response criteria	Responses to potential cyber events should be pre-defined. For example, depending on the nature of the attack and the target objective, is it necessary to take the process to a safe state - or to initiate a full shutdown?
Response procedure and contingency requirements	The initial response is generally to locate the threat and neutralize it. Should the procedure be prescriptive to be expedient? Or should the procedure include a guided decision tree to address multiple potential outcomes? Are the responses more global in nature (e.g., restore the control system to a previous version) or more surgical in nature (e.g., locate the bug and remove it without restoring to a previous version)?

Table 10-16 continued

Topic	Clarifying Questions/ Notes
Information and data capture to support follow-up forensic analysis and incident investigation	What information is needed to support future forensic analysis? How should this data be obtained and securely stored?
Training and communication requirements	Response preparation for phishing attacks requires brief training and routine refresher communications for all email users. However, the response to a malware attack may be managed by a few individuals with highly specialized training.
Communication requirements during and following an attack	What information needs to be communicated to internal stakeholders and in what timeframe? What information needs to be communicated to external stakeholders and in what timeframe?
Incident Escalation	How severe is the event? Does the event need to be escalated to senior management? Does the organizational crisis management strategy need to be implemented?
Identification of and plan to conduct cybersecurity attack drills	How frequently are incident response drills conducted? What types of scenarios should be included?

In addition to the Incident Response Plan, organizations should prepare a Business Continuity and Restoration Plan. The plan should include an assessment of the potential impact a cybersecurity event could have on the business model considering the financial and operational impacts. Will the facility be able to continue to operate? At what production rate? Establish a recovery timeline to support business continuity needs. Who needs to be notified of the incident and what information should be shared? Understanding the requirements to maintain business continuity will provide a basis for defining the recovery plan. Is it necessary to provide for switching

process controls to a fully redundant control system at another location, or can an outage be tolerated while restoring from backups? What backups are needed, and at what frequency should backups be made? Which backups are executed automatically, and which are manual? How long does it take to restore the system from backups? Define the backup requirements and set a schedule for performing the backups. Determine where the backups are stored (on or off site) and ensure that backups, license keys, and configuration data are readily available. Perform periodic testing of backup and restore activities. Finally, set requirements for periodic review and update of both the Incident Response Plan and the Business Continuity and Restoration Plan.

10.17.2 Emergency Management: Cybersecurity Activities

An organization can augment cybersecurity by improving system background monitoring to establish a baseline for 'normal' system traffic. This can enable the detection of abnormalities that could signal a potential attack. Once the baseline is established, the detection of an anomaly - either from security monitoring tools or from operator vigilance - could trigger the Cybersecurity Incident Response action. Some items to monitor include:

- Unusually slow internet or devices.
- Locked out accounts.
- Pop-ups and redirected websites when browsing.
- Unexpected software installs.
- Unexplained changes to files.
- Anomalies in normal network traffic patterns.
- Abnormal outbound traffic.
- Irregular access locations.
- Large number of requests for the same objects or files.
- Suspicious activity on the network after-hours.
- Multiple failed login attempts.
- Unknown/unauthorized IP addresses on wireless networks.
- Unexplained system reboots or shutdowns.
- Services and applications configured to launch automatically.

A change in network activity could indicate that the system is being probed for weaknesses or is actively under attack. Such changes should be considered as near misses and investigated accordingly. In addition to establishing background monitoring, personnel should be assigned to perform intelligence

gathering activities such as monitoring cybersecurity threat intelligence feeds to stay abreast of new threats or attack methods.

Developing the details of the Cybersecurity Incident Response Plan (C-IRP) and Business Continuity and Restoration Plan (BCRP) will involve tools and techniques that parallel a process safety Emergency Management Plan (PS-ERP). For example, the plan should have a defined program owner. Upon detection of a threat, the C-IRP owner, IT and IACS security leads, PS-ERP owner, and other key personnel are contacted to establish an incident command structure and initiate incident response activity. Determining when 3rd party resources may be needed on the response team (e.g., vendor providing BPCS software services) is another important step of the plan. The plan should also address requirements for the leadership roles as well as the makeup of the incident leadership and response team based on the type of attack.

A center of operations for the incident response or “war room” is often beneficial. An effective “war room” should have communications equipment and support secure access to support information such as the C-IRP procedures, asset integrity and reliability management records, and network diagrams. The communication plan and documentation needs will vary with the type of attack, so the C-IRP should include a global list of requirements as well as the means to identify specific needs based on the type of attack. Provisions should be made for a backup source of documents in the event that the primary source is inaccessible or compromised.

An immediate response action is to “secure the scene” or isolate the affected systems and establish quarantine procedures. The C-IRP should include procedures to block network ports or otherwise take the infected system offline. This immediate action may include physically disconnecting communications between zones at boundary devices such as firewalls to stop the network traffic. The criteria and the methodology for returning non-affected assets to operations as soon as possible should be established in advance.

The system should be equipped with message logging capability to capture pertinent information, both before and during the incident. The log should be stored in a protected location. Information captured in the log can

support incident investigation and provide data points to include in cybersecurity metrics.

The effectiveness of cybersecurity incident response is a direct result of good planning and robust preparation. The effectiveness of cyber emergency response execution is improved by:

- Implementing a formal backup and recovery procedure and an execution of backups on a routine and timely basis. The backup scope should include all information necessary support the safe resumption of business operations.
- Periodically performing tabletop exercises and cyber-attack response drills. Critique the results of the exercises and drills and modify the plan and procedures to incorporate learning and addresses gaps.
- Performing periodic audits of cybersecurity systems and addressing findings and recommendations.

10.18 Incident Investigation

10.18.1 Incident investigation: Cybersecurity Concerns

The objective of incident investigation is to learn from experience. The 2015 and 2016 Ukrainian Power Grid attacks [20] [21] (described in Section 6.4) illustrate this point. Although the attacks were executed in different ways and they were executed against different power companies, both are believed to have been executed by the same group and are suspected of being delivered by the same method (phishing campaign). Learnings from a detailed incident investigation of the first attack shared across the industry group could help to prevent subsequent attacks as seen in the Ukraine.

Core principles of Emergency Management, as well as cybersecurity specific considerations, are summarized in Table 10-17.

Table 10-17 Emergency Management

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	• Develop a cybersecurity incident response program and designate a program owner. • Define roles, responsibilities, and competency requirements.
Prepare for emergencies	• Identify the potential types of cybersecurity incidents and prepare response plans. • Inform and train personnel. • Establish contracts with 3rd party resources. • Periodically review and update plans.
Periodically test the adequacy of plans and level of preparedness	• Conduct cybersecurity incident drills and or tabletop exercises. • Critique drill and tabletop exercise results. • Perform periodic assessment and audits. • Address findings and recommendations.

Incident investigation is a formal process of studying incidents to determine root causes so that preventative and mitigating measures can be improved. An incident investigation should be performed for all significant cybersecurity incidents. Routine monitoring activities should be reviewed and a near miss investigation should be performed for any situation with a marked increase in threat attempts or other abnormal activity. The task of a cyber-attack incident investigation is to characterize the attack, identify attack mechanisms, identify security compromises, and improve defenses. Analysis activities to consider include:

- Security and event logs review
- Disk and file analysis (e.g., disk image)
- Memory analysis
- Network traffic analysis

The learnings from an incident investigation should be used to harden the network against future attacks. As with process safety events, recommendations from incident investigations should be addressed in a timely manner, documented, and tracked to closure. Findings should be communicated so that hardening implementation can move forward. Maintaining a searchable log of cyber incidents with investigation summary findings can improve the understanding of the site cybersecurity trends over time.

10.18.2 Incident Investigation: Cybersecurity Activities

The first step is to develop a plan for incident investigation of cyber-attacks and near misses. This can take the form of either an additional section to existing incident investigation plans within the organization, or as a separate cybersecurity specific plan. Part of the plan will include how to determine the scope and structure of the analysis based on the type of incident (e.g., apparent cause analysis, root cause analysis, or trend only). Another important aspect of the incident investigation plan is to identify which steps will be completed internally, and which steps will be completed externally. Typically, internal resources are responsible for preserving the data needed to investigate the incident as well as for implementing the recommendations and follow on activities from the investigation, in a similar approach to process safety incident investigation. For the cybersecurity specific analysis, including which devices were compromised, what vulnerabilities were exploited, and how the incident occurred, specialized third parties are most often used. Defining the roles and responsibilities for the investigation team in advance helps to improve the efficiency of analysis activities when they are required. Training for required team members should also be provided so that they can effectively fulfill their roles. Any tools required to conduct forensic analysis should be identified and either acquired for use of the on-site team or arranged for via contracted support from a 3rd party.

The scope of a near miss or incident investigation is likely to differ, depending on the type of incident and the consequences. The plan should provide guidance regarding the tools and techniques to be deployed in the investigation.

Some questions to address include:

- What are the techniques for data collection and analysis? Can these be pre-defined based on the type of attack? How do the techniques differ based on the relative risk?
- Is the investigation to be completed at one time or conducted in multiple stages? For example, are there a few basic items that are addressed when a phishing attack is identified (immediate response) and a more rigorous review conducted on a periodic basis to look for systematic concerns (monthly metric review)?
- What investigation methodology is best for a given type of incident? How should the investigation be structured? The scope and objective of the investigation may be comprehensive with a detailed analysis to identify the root cause, limited to determination of the apparent cause, narrow seeking to determine relevant trends only? The method(s) selected needs to lead to an action that will best provide improved countermeasures.
- What questions need to be asked in the investigation?
 - o How did the attacker get in?
 - o How far did they get in?
 - o What was the attacker's objective?
 - o What countermeasures failed and why?
 - o What management methods failed and why?

Following through on the results of the investigation and addressing recommendations helps to better protect the system against future incidents. An action plan identifying the countermeasures to be strengthened and a timeline for implementation should be developed. This plan should also define the resources needed for implementation (e.g., is enhanced training and awareness sufficient or is a capital project needed to strengthen countermeasures).

Lessons should be focused on specific target audiences and communicated to applicable parties. Internal communication of lessons learned may be focused on improving existing countermeasure performance or expanding the recognition of types of attacks. External communication may occur at conferences or industry groups to provide improved knowledge about evolving attack methods and to learn from others' experiences.

Establishing trending capability for cyber incidents data can help to identify recurring events and systematic causes. The effectiveness of new and improved countermeasures should also be monitored to ensure that they are achieving the desired effect. Performing periodic management reviews to assess the incident investigation plan and adjust to correct deficiencies or incorporate new tools and techniques further supports robust deployment. Core principles of Incident Investigation, as well as cybersecurity specific considerations, are summarized in Table 10-18.

Table 10-18 Incident Investigation

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable incident reporting and investigation practice	• Implement a program to formally review each cybersecurity incident or attempt as a near miss incident. • Define guidance that identifies what is to be reported, how to report, and how to establish the scope and depth of investigation. • Develop trained personnel with the competencies needed to perform effective investigations. • Monitor the effectiveness of the root cause analysis. Are repeat events observed?
Identify potential incidents for investigation	• Train personnel to report all suspected cybersecurity incidents and attack attempts. • Review all reports and determine the depth and type of investigation required promptly.
Use appropriate techniques to investigate incidents	• Define data collection techniques and data analysis methods for cybersecurity incident investigations. • Perform objective investigations with the appropriate technical rigor. • Develop effective recommendation and a suggested action plan.

Table 10-18 continued

RBPS Key Principle	Cybersecurity Considerations
Document incident investigation results	• Document the review of all cyber incidents, providing clear links between the cyber-attack attempt and the recommendations,
Follow through on results of investigations	• Follow through with the disposition of recommendations and document the results. • Communicate the lessons learned. • Maintain complete investigation records.
Trend data to identify repeat incidents that warrant further investigation	• Maintain a complete incident log and analyze the data for trends. • Complete a periodic management review.

10.19 Measurements and Metrics

10.19.1 Measurements and Metrics: Cybersecurity Concerns

Metrics provide the basis for evaluating cybersecurity system performance and the benchmark against which the system will be audited. They also determine the thresholds for normal operation and identify the conditions for the diagnostics and alarms that indicate a potential cybersecurity incident, triggering emergency response action. The metrics may be qualitative or quantitative. A combination of leading (pre-event) and lagging (post-event) metrics should be considered. In order to most effectively assess system effectiveness, careful consideration should be given to selecting the metrics that best monitor the condition of the system.

Cybersecurity is implemented in an industrial setting for two basic purposes: 1) to protect the content and preserve business function and 2) to secure the safety and integrity of process operations. The metrics chosen to monitor these systems as the basis for Key Performance Indicators (KPI) should support these two primary purposes.

10.19.2 Measurements and Metrics: Cybersecurity Activities

Implementation of one or more monitoring tools will facilitate metric data collection. The data from these tools provides information that will be helpful in determining the usefulness of a particular metric while also establishing a system benchmark. A written description for each metric should be prepared, including the data collection methods (continuous or periodic scan), collection and analysis frequency, and reporting requirements. The roles and responsibilities of personnel collecting and analyzing the information should also be established. The required competencies of personnel with monitoring responsibilities should be defined, and familiarity with tools should be supplemented as needed. Establishing a schedule for routine metric review (weekly, monthly) and in-depth management reviews (annual, biannual) helps to ensure that the cybersecurity key performance indicators (KPIs) are kept relevant.

Leading and lagging indicator metrics should be established for monitoring cybersecurity performance and as basis for auditing. (Auditing metrics will be discussed in more detail in Section 10.20.) The IEC 62443-2-1 [12] standard provides additional cybersecurity metrics which can be used to assess the current cybersecurity environment for physical security, access security, authorized change management, and unauthorized network communications.

Leading indicators are the metrics that indicate a potential problem before it occurs. These ‘warning signs’ should monitor the effectiveness of preventive measures intended to block or deflect attack attempts. They can also indicate the rigor with which activities are conducted in the cybersecurity management system. Targets for leading indicators are summarized in Table 10-19.

Table 10-19 Leading Indicator Metrics

Target Area	Metric Questions
Email management effectiveness	• What percentage of attack attempts are being detected by email filtering? • What percentage of untargeted attack attempts are being identified and reported? • What is the phishing test success rate?
Access management effectiveness	• What percentage of user accounts are overdue for password changes? • What is the time between the notice to terminate access and closure of the account? • What percentage of accounts are closed for users who no longer have access authorization?
Physical security effectiveness (see Section 10.20 for additional discussion)	• Is all portable media scanned for malware prior to connecting with the IACS? • Are all doors of the cabinets locked? Are all USBs/CDs/DVDs disabled?
Cybersecurity hygiene effectiveness	• How many suspect files were introduced to the network? • What is the distribution of introduction paths (e.g., email, internet downloads, USBs)? • Are all temporary connections to control networks managed using cyber hygiene procedures?

Table 10-19 continued

Target Area	Metric Questions
Cybersecurity management effectiveness	• How many IACS and network patches are pending implementation? • What is the duration between patch availability notification and implementation? • What is the update status of threat tracking tables (e.g., malware, email scams)? • Are backups being performed on time? What is the duration between fault detection and repair? • Is restoration of backups being checked as per plan? • Are tabletop drills being carried out as per plan? • Are audits being carried out as per plan? • How many security advisories are pending for implementation? • How many devices are not complying to minimum baseline security standards?

Lagging indicators are the metrics that indicate that an incident has already occurred. Metrics that identify and successfully deflect a potential incident are positive indicators of cybersecurity performance. Metrics that evaluate the consequences of a successful intrusion illustrate weaknesses in the cybersecurity system that need correction. Some lagging indicator metrics include:

- Number of intrusion attempts
- Mean time to detect an intrusion
- Percentage of successful intrusion attempts
- Mean time to recover from an intrusion attempt

Intrusions should be investigated as near miss incidents to understand how the intrusion occurred and identify the weakness that permitted

successful intrusion. Additional example cybersecurity metrics are provided in Appendix C and can be used as a starting point for developing a company-specific list of metrics to track.

Diagnostic measures should be used to monitor the health of system components. Network equipment and IACS devices can be equipped with diagnostic capability that provides either real time notification or data logging that can be periodically analyzed. Metrics should be tracked to assure that component failures identified diagnostic faults are addressed promptly. Some diagnostics to consider include:

- Automatic diagnostics:
 - o Switch or router fault alarms
 - o Firewall fault alarms
 - o Intrusion detection (IDS/IPS) fault alarms
 - o Cyclic Redundancy Check (CRC) alarms
- Periodic diagnostic procedures:
 - o System log review
 - o Controller diagnostic buffer review
 - o Review of IACS alerts
 - o Group policy review

The value of passive metric and diagnostic information is limited by the frequency and thoroughness with which it is analyzed. Alarms provide an opportunity to elevate lagging indication to a timely proactive response. The alarms and setpoints should be selected judiciously to avoid creating nuisance alarms. Sound alarm management practices, such as those described in ANSI/ISA 18.2 [112], should be applied to cybersecurity alarms. Annunciation of fault alarms on critical devices such as firewalls, routers and critical process sensors is recommended. Consider the implementation of Cyclic Redundancy Check (CRC) alarms for identification of unauthorized system changes. Core principles of Measurements and Metrics, as well as cybersecurity specific considerations, are summarized in Table 10-20.

Table 10-20 Measurements and Metrics

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	• Develop a written description of cybersecurity metrics, data collection methodology, collection frequency, and reporting requirements. • Maintain the competency of personnel who collect and analyze data and provide training to personnel using the results.
Conduct metrics acquisition	• Define effective metrics that provide real-time monitoring of important concerns. • Faithfully collect and analyze data and communicate the results.
Use metrics to make corrective action decisions	• Establish acceptable limits for metrics and define corrective actions required when trending toward limits. • Evaluate metric effectiveness and revise or replace metrics that are not meaningful.

10.20 Auditing

10.20.1 Auditing: Cybersecurity Concerns

The objective of audits is to determine if the management system is performing as intended. Auditing is a periodic evaluation to review the management system elements and prepare findings, observations, and recommendations to improve the system. The audit element should consider a combination of techniques, including self-assessments and formal 3rd party audits. A checklist-guided self-assessment can be a useful tool for more frequent reviews and as preparation for formal audits.

10.20.2 Auditing: Cybersecurity Activities

The first step to developing an effective auditing practice for cybersecurity is to incorporate cybersecurity concerns into the overall site management system. Establishing an audit protocol for each element of the management system helps to ensure that the cybersecurity concerns are effectively implemented. The competency requirements for auditors addressing cybersecurity scope should also be formally defined. What format should be used to conduct the audit? A single trained auditor may be able to effectively address both cybersecurity concerns and process safety concerns for some management system elements (e.g., Workforce Involvement). Other elements may require auditors with different expertise (e.g., Asset Integrity and Reliability). Several questions should be addressed when applying existing process safety audit techniques to cybersecurity including: Would a multi-element, cyber-focused format provide a more comprehensive perspective than a standalone safety audit? Should cybersecurity audits be conducted on a higher frequency than other audits to keep pace with fast-paced change of cyber threats?

Facilities may have limited cybersecurity-competent resources on a given site. Utilization of the same resources to manage the system and to also audit the system may result in an ineffective audit, with important vulnerabilities potentially overlooked. It is prudent to use resources from another location within the organization or carefully vetted 3rd party resources to provide appropriate staff for audits and assure independence in the auditing process.

For each audit, a written plan should be prepared and should include:

- Scope and objectives:
 - o Where (physical scope) – What is the physical location to be audited? What IT/OT systems, email system, physical devices etc. are in scope for review?
 - o What (analytical scope) – What standards, procedures, policies, and management control mechanisms are the basis for audit?
 - o When (temporal scope) - Should some aspects of cybersecurity be audited more frequently based on metric observation and frequency of threat? For example, is email is subject to frequent untargeted attack, whereas the IACS devices have a much lower attack frequency?

- Depth of review criteria. How much audit time should be allocated to topics that merit a more detailed review? Which audit topics can be audited in less depth?
- Resources. Will the audit be staffed by internal or external resources? What competencies (type and level) are required to cover the audit scope?
- Roles and responsibilities. What roles have responsibilities in the auditing process as auditors, participants, consultants, or responsible management?
- Requirements for resolution of findings and recommendations. What is the work process for defining and assigning action items? How will they be tracked to completion?
- Documentation requirements. What documentation will be generated during the audit? Where will the audit documentation be archived, and for how long will it be retained? How will access to audit documentation be restricted?

In some cases, special conditions may trigger an audit outside the scheduled frequency. For example, it may be beneficial to perform audit whenever upgrades are carried out. Special audits can be particularly useful to follow-up on implementation of a remedial measure. Consider preparation of a master self-assessment or audit checklist with questions grouped to facilitate matching the list to an audit scope. Appendix D provides a sample questions list for areas that may be covered in a cybersecurity audit.

While the same audit techniques, analysis, observation, and interviews can be used in both process safety and cybersecurity audits, the proportion of effort expended on each technique may differ. Determining what information is to be gathered in preparation of the audit and conducting as much data analysis as possible in advance of the onsite visit can help to save time during the actual audit and further focus the interview and observation activities.

Determining the appropriate sample size and preferred methodology is important because the detailed review may vary by element. For example, the Management of Change audit sample size may only consist of a few records that are analyzed in depth; however, the Asset Integrity and Reliability element may have a larger sample size of records that are randomly spot-checked.

Results of the audit are documented, and audit findings and recommendations are recorded and tracked to closure. At a minimum, the audit report should include:

- Scope of the audit.
- Audit team and qualifications.
- List of personnel interviewed.
- References used in the audit.
- Audit methodology.
- Findings, recommendations, and observations.

Core principles of Auditing, as well as cybersecurity specific considerations, are summarized in Table 10-21.

Table 10-21 Auditing

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	• Incorporate cybersecurity concerns into the written audit program, establishing the physical, analytical, and temporal scope and audit frequency. • Develop a cybersecurity audit protocol. • Utilize personnel with appropriate competency, experience, and objectivity.
Conduct element work activities	• Define the audit scope and the responsibilities of the audit team members. • Gather information for audit prework. • Plan and schedule on-site audit activities. • Document the audit results. • Address audit findings and recommendations.
Use audits to enhance RBPS effectiveness	• Monitor performance over time to confirm system effectiveness and adjust cybersecurity management system techniques as needed.

10.21 Management Review and Continuous Improvement

10.21.1 Management Review and Continuous Improvement: Cybersecurity Concerns

Management reviews are routine evaluations of the management system to confirm effectiveness. The reviews are formalized and scheduled health checks that bridge the gap between day-to-day activities and periodic audits. They are structured team reviews that are usually less formal than an audit and are generally 1st party reviews. Additional information on the continuous improvement approach is included in Section 11.1.3.

10.21.2 Management Review and Continuous Improvement Cybersecurity Activities

Scheduling a cybersecurity-focused review into the management system review rotation is beneficial to monitor cybersecurity performance. The review should consider cybersecurity concerns from a different perspective than day-to-day responsibilities and audits. The review may also consider different evidence than what is evaluated in an audit or previous review. Topics that might be considered for the session include:

- Why are attack attempts getting past an initial barrier?
- Are there places where following the procedures is difficult, tempting individuals to take shortcuts?
- Are there places where risk is not effectively addressed (e.g., interlocks bypassed)?
- Are phishing tests or dropped USB drills showing improvement in personnel behaviors?
- A review of potential threats and conducting an impact analysis to determine if additional countermeasures are needed.
- Is there changing legislation: If so, evaluate applicability relevant to cybersecurity.
- Is there an opportunity to benchmark cybersecurity activities and strategies, both within and outside of the industry?
- Has employee feedback on cybersecurity practices been requested, and what input has been received?

The scope of the management system review should be different than the scope of an audit. For example, the audit may focus on all RBPS elements with respect to cybersecurity activities, but the management review focus may be

as narrow as a single element or as broad as all elements and supporting management systems. Refer to Appendix E for example questions that may be used, depending on the scope of the management review. Defining standards of performance for the review including scope, objectives, review frequency and depth of scrutiny, requirements for resolution, and documentation help to maintain distinct scopes. Roles and responsibilities for participants should be defined, including who is responsible for what aspects of the review, who is accountable, and who are the decision makers. Prior to the meeting, preparing a presentation highlighting issues and upcoming challenges can help to align the management review team. This helps to focus the review and raise issues early.

The integrated cybersecurity lifecycle was summarized in Chapter 7. Table 7-2 includes five cybersecurity assessments conducted at specific stages of the lifecycle. These are important stage gate assessments for cybersecurity implementation and present opportunities to introduce periodic management system reviews. For each stage of the assessment the results of previously completed lifecycle activities should be evaluated by an independent team member. The cybersecurity assessments should be conducted to achieve specific objectives as identified in Table 10-22.

Table 10-22 Cybersecurity Assessment Stages

Assessment Stage	Objective
Cybersecurity Assessment 1	Confirm risk assessment and design basis activities. Consider conducting the cyber assessment in association with the HIRA element.
Cybersecurity Assessment 2	Validate design activities. Consider conducting the cyber assessment in association with the Asset Integrity and Reliability element.
Cybersecurity Assessment 3	Confirm cybersecurity concerns have been implemented prior to introduction of hazards. Consider conducting the cyber assessment in association with the Operational Readiness Element.
Cybersecurity Assessment 4	Evaluate status of cybersecurity through periodic vulnerability assessments. Consider conducting the cyber assessment in association with the Conduct of Operations element.
Cybersecurity Assessment 5	Confirm activities associated with modification and decommissioning are addressed. Consider conducting the cyber assessment in association with the Management of Change element.

Cybersecurity Assessments 1 through 3 help to support the effective implementation of cybersecurity controls during the project stage, while Cybersecurity Assessments 4 and 5 are conducted on an ongoing basis throughout operations. As such, Cybersecurity Assessment 4 is closely aligned with the continuous improvement element. This periodic assessment provides an opportunity to track key metrics and assumptions made throughout the cybersecurity lifecycle and to verify that forward progress is being made.

Following each cybersecurity assessment, team recommendations should be documented and tracked to closure. The review quality can be validated by

comparing results with previous reviews and audit cycles to understand if deficiency was previously overlooked or if there is a systemic concern. Performing periodic spot checks, such as drills or mini audits, to test cybersecurity effectiveness can provide further insights. Core principles of Management Review and Continuous Improvement, as well as cybersecurity specific considerations, are summarized in Table 10-23.

Table 10-23 Management Review

RBPS Key Principle	Cybersecurity Considerations
Maintain a dependable practice	• Incorporate cybersecurity concerns into the written management review program, including defining roles, responsibilities, and standard of performance. • Compare audit and management review results to validate the effectiveness of the program over time.
Conduct review activities	• Document the cybersecurity scope for the management review and define responsibilities for team members. • Gather information needed for the management review and prepare a status summary. • Plan and schedule the management review meeting. • Document the management review. • Promptly address management review findings and recommendations.
Monitor organizational performance	• Strive to continuously improve cybersecurity defense. • Perform periodic spot checks to test cybersecurity effectiveness.

10.22 Summary

Managing the risk associated with cybersecurity is an ever-changing journey, and it is important to have a defined management structure that facilitates effective implementation and ongoing robust secure operations. The

framework of Risk Based Process Safety is a good vehicle for the management of cybersecurity concerns.

An organization with a well-established commitment to process safety has a culture dedicated to maintaining dependable practices and continuous improvement of those practices. The workforce is engaged, competent, and accustomed to compliance with standards and procedures. Communication is open, and all employees are comfortable raising concerns. These behaviors that are used to manage process safety can be directly applied to cybersecurity issues.

The basis for a cybersecurity management program is to understand the hazards and risks. Many of the tools and techniques used to assess cybersecurity hazards are similar to process safety hazards assessment techniques. Risk-based decision making ensures that resources are dedicated based on risk reduction value rather than by arbitrary means. These management systems for cataloging, retrieving, updating, and using process knowledge are easily adapted to managing cyber knowledge.

Robust operational discipline is key to managing cybersecurity risk. The workforce is accustomed to following procedures and maintaining them, and they can apply that discipline to cybersecurity practices as well. Asset integrity and reliability, management of change, and operational readiness can be expanded to incorporate cybersecurity concerns without fundamentally changing how the elements function. The scope of contractor engagement should be broadened from a cybersecurity concept to consider any personnel that may have access to the IACS. Additional discipline should be maintained with respect to any services that have cybersecurity implications through the use of a consistent documented framework. Training and performance assurance programs should also be expanded to include new criteria for cybersecurity awareness and role-based competency development; however, they can follow the same guidelines and management approach as existing process safety training programs. Cybersecurity emergency management requires the development of new plans documenting the procedures, tools, and techniques needed for incident response, business continuity, and recovery. Where a cybersecurity attack could lead to a process incident, the

cybersecurity management plan engages process management resources early, possibly even before an incident occurs.

Learning from experience is a cornerstone of effective cybersecurity management. Investigation of cyber-attack incidents and near misses provides valuable information to harden defenses. Performing periodic checks, such as a phishing test or cyber-attack response drills, can confirm that personnel will respond to threats in a desired manner and timeline. Routine monitoring of targeted metrics and periodic management reviews and auditing maintain visibility to cybersecurity concerns and the condition of cyber defenses.

11 Implementing a Holistic Approach to Safety and Cybersecurity

Part II of this book has focused on how to effectively integrate cybersecurity into the process safety framework. First a model for understanding cybersecurity was introduced in Chapter 7. This model included the cybersecurity-specific lifecycle, as well as considerations for integrating the cybersecurity lifecycle with existing process safety and functional safety activities. Next, in Chapter 8, the concept of inherent safety was applied to cybersecurity to demonstrate how steps can be taken to reduce an organization's attack surface by limiting the number of personnel with access, devices on the network, and applications on the IACS. Additionally, the concept of defense-in-depth was introduced to demonstrate how independent layers can be established to protect against cybersecurity attacks. Chapter 9 focused on how existing process safety Hazard Identification and Risk Analysis (HIRA) techniques can be applied to cybersecurity and used to accurately identify and analyze cybersecurity risk. Finally, Chapter 10 provided guidance on how the Risk Based Process Safety (RBPS) framework elements can be applied to cybersecurity.

Each of these chapters provides a core building block for an integrated approach to safety and cybersecurity, and this chapter will focus on how to put these pieces together into an integrated cybersecurity program. The 8 steps for effectively implementing an integrated approach for safety and cybersecurity are provided in Figure 11-1.

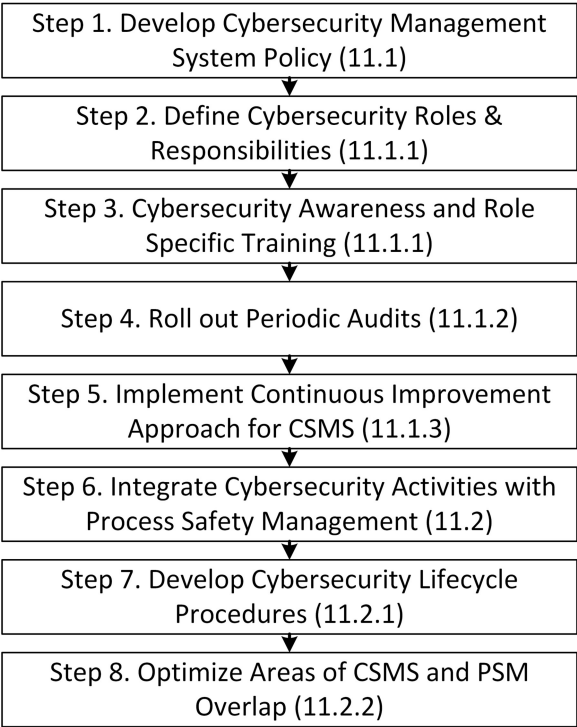


Figure 11-1 Implementing Holistic Cybersecurity and Safety Approach

11.1 Cybersecurity Management Systems (CSMS)

The first step for implementing a holistic approach is to develop a robust Cybersecurity Management System (CSMS). In any cybersecurity program, it is easy to get caught up in technological solutions and forget the soft aspects of cybersecurity such as policy development, responsibilities, and staff training. This human part of the equation is critical to the success of any cybersecurity program. Ensuring that trained personnel follow detailed procedures, and that all necessary paperwork is generated and stored, can go a long way in reducing the potential for errors throughout the cybersecurity lifecycle.

A cybersecurity management program should be centered on an IACS security policy that documents cybersecurity objectives, defines a lifecycle-based approach, and provides a timeline for implementation. The security policy is a statement of the goals, responsibilities, required activities, and acceptable behaviors necessary to maintain a secure production environment.

It demonstrates management support, gives broad guidance, and defines the direction for cybersecurity-related activities across the organization using a risk-based approach.

The following topics and questions are typically covered in the CSMS:

- Formal scope of the CSMS: What assets and systems are included? Is there a boundary between the IACS cybersecurity policies and the IT cybersecurity policies? Does the CSMS apply to multiple sites or a single site?
- Strategic goals, process, and timing of the CSMS: What is the objective of the CSMS? What is the time frame for implementing the policy?
- Lifecycle approach: What activities need to be completed to achieve a targeted level of cybersecurity (based on the corporate risk criteria and goals)? What is the planned order of activities for existing sites and new projects?
- Integration with process safety: Do existing process safety procedures apply to cybersecurity? How is cybersecurity risk addressed by the CSMS? How is cybersecurity to be integrated with existing risk management activities or managed as a separate activity?
- Organizational security structure: What group is responsible for implementing the CSMS? What roles have cybersecurity responsibilities?
- Business continuity: What actions should be taken if a cybersecurity event occurs? How will the negative financial impact of a cybersecurity incident be minimized?
- Enforcement: How will the new cybersecurity management system be enforced? How frequently will internal audits be conducted?
- Training and roll out: What type of training is needed on the new cybersecurity management system? How will roles be made aware of new cybersecurity responsibilities and provided with support to complete them?

The first step in developing an effective CSMS is to formally define the scope of the policy. Which systems are considered under the IACS cybersecurity policies and procedures, and which systems are maintained according to IT security policies? Typically, the local OT team will have responsibility for production assets in level 3 and in the OT Reference Model

(Chapter 8, Figure 8-2) and the IT team will be responsible for enterprise systems. However, ownership of the demilitarized zone may not be as clearly defined. Specifying the transition between IT and IACS ownership is critical to ensuring that security is enforced for all network zones and weak points are avoided in the design. Another important consideration in the scope of the CSMS is to identify if the document is intended for a single site or multiple sites. In many cases, it is beneficial to make the CSMS broad enough to apply to multiple operational sites. This approach helps to ensure that cybersecurity objectives are clearly defined for each site and to limit the development time by avoiding rework of the policy for each individual site. This approach also helps to drive organizational consistency in CSMS implementation.

The CSMS should be focused on the strategic goals for IACS cybersecurity and not necessarily on how to complete each step in the process. Not only is finding the right level of detail important in applying the CSMS to different sites, but it also helps to avoid overloading site personnel with information at the policy level. The CSMS should outline what is to be accomplished for IACS cybersecurity and the associated timeline. An example of a strategic goal would be: "To ensure the availability and integrity of critical assets in the IACS environment and safe and secure operations by implementing a robust cybersecurity management program by the end of 2021." The timeline for deployment should extend beyond when audits to the CSMS are set to begin to allow for a site-specific roadmap to be established that incorporates the initial audit results and the available resources of the site. The timeline should also include other key milestones such as cybersecurity training for site personnel, interactive workshops to review the new policy, and dates for implementing practical security controls.

As discussed in Chapter 7, the cybersecurity lifecycle is an important framework for implementing and managing risk that should be integrated into the organization's CSMS. Although the CSMS should not define the detailed method for completing each lifecycle activity, it is important to identify which lifecycle steps are necessary to achieve the organization's cybersecurity goals. A brief description of the lifecycle steps to be completed and a reference to a detailed procedure for completing the steps are typically all that is required in the top-level policy. Further discussion on the cybersecurity lifecycle is included in Section 11.2.

During development, it is also key to integrate the CSMS with existing process safety policies and procedures. This integration can be achieved in multiple ways. The first method is to explicitly reference related process safety procedures. This could be done with a simple reference to the top-level process safety management (PSM) document or to specific procedures (e.g., process safety risk assessment, management of change) that are related to cybersecurity. In addition to referencing existing procedures, cybersecurity policies can be created in a format similar to existing safety policies. Adopting the format of existing policies not only decreases the deployment time required, but it can also provide better integration of lifecycle steps by aligning with existing safety methods and improving the site review and acceptance process by using familiar language and methods.

Outlining the organizational security structure, or ownership of the security program, may be one of the most important factors for program success. The creation of an organizational structure that defines the roles and responsibilities for cybersecurity is critical to any cybersecurity program in the same way as it is for a process safety or functional safety program. It is important that both IACS and IT personnel are involved and that the boundary between IACS and IT security policies is defined. Additionally, communication between IACS roles such as controls engineers, process safety engineers, process engineers, and operators is essential to maintain the program. When defining roles and implementing the cybersecurity program, senior management support is essential for success. Without a defined structure in place and management support, many cybersecurity programs will lose traction over time. Company culture is another critical element of successful safety and cybersecurity programs, and the culture starts at the top of any organization. Further detail about defining the roles and responsibilities for the CSMS program is included in Section 11.1.1.

The final component of an effective CSMS is to identify the critical objectives for maintaining business continuity in the event of a cybersecurity incident. Business continuity management is a program designed to counteract interruptions to business activities and protect critical business processes from the effects of major failures or disasters. While important for all information systems, it is vital for control systems. Even with the best-designed cybersecurity policies and procedures, it is highly likely that, at some

point in the operation of a facility, there will be a loss of a device or server containing critical data. Regardless of whether this loss is due to accidental or malicious forces, a comprehensive backup and restore policy needs to be in place to recover this data. The business continuity plan serves to consolidate communications during a cybersecurity incident and promotes a more efficient response, including activities crucial to recovering data and restoring the process. The business continuity plan represents another opportunity for integration with existing site safety activities because many organizations have existing disaster response plans and procedures that can be updated to include cybersecurity scenarios.

11.1.1 Roles and Responsibilities

One of the most important factors in implementing a CSMS is a clearly defined organizational structure, including identifying which roles have cybersecurity responsibilities. IACS cybersecurity is still a relatively new topic for many organizations, and oftentimes ownership of cybersecurity activities is not yet established. Two primary approaches have been adopted successfully.

The first is a single cross-functional cybersecurity team with responsibility for both IT and IACS cybersecurity. The team is most often chaired by a senior manager (e.g., Chief Information Security Officer, CISO) who is responsible for information security. The team includes representatives of various functional departments of the organization (e.g., IT, operations, engineering, process safety). This approach can help to demonstrate commitment to IACS cybersecurity by combining IACS security efforts with existing cybersecurity management. Although the priorities between IT and IACS cybersecurity are not always in agreement (as introduced in Chapter 8), if senior management understands and addresses these nuances with IACS-specific cybersecurity policies, this can be an effective means of providing the needed resources for addressing IACS cybersecurity.

The second approach is to establish a second, separate team for IACS cybersecurity. The leadership of the IACS cybersecurity team can vary but typically falls to either the engineering, operations, or process safety group. The primary benefit of this approach is to ensure that the leadership of the IACS team has more detailed knowledge of the cybersecurity risks associated with the control system. If a separate IACS cybersecurity team is created, it is

critical that the team work closely with the IT cybersecurity team to ensure that boundaries between the IT and IACS system are protected.

Either approach can work effectively if the organization establishes buy-in, defines roles, and has accountability mechanisms in place. Defining the roles and responsibilities for IACS provides the anchor for any CSMS program. The roles range from the overarching duties of senior management to personal duties of new employees and contractors. Without this structure in place, most cybersecurity programs will collapse under the pressure of daily operational demands; unless the human element of cybersecurity is addressed, technical solutions will not be enough to achieve lasting results.

In addition to defining the cybersecurity responsibilities for existing roles, it is generally necessary to identify an internal champion for IACS cybersecurity. Commonly referred to as the site or IACS security lead, this member has responsibility for ensuring that cybersecurity risks are identified and addressed in the planning phase of the project. The IACS security lead is accountable to ensure that adequate countermeasures are maintained during plant operation. For organizations with multiple sites, it is generally beneficial to have a cybersecurity champion at each site.

All organizations need to balance operational and security needs, such as the operational need to maintain production and the security need to implement critical patches. This can be challenging when the same personnel are responsible for addressing both types of needs and they don't have clearly defined management support for security objectives. Where possible, having roles dedicated specifically to support IACS cybersecurity can be helpful in avoiding these conflicting responsibilities.

A responsibility assignment matrix is an effective means of depicting the participation of various roles in a project or lifecycle. The matrix identifies 4 types of involvement:

- **Responsible (R):** The team member that completes the task or does the work; typically, each task has only one responsible party.
- **Accountable (A):** The team member that delegates the work and reviews the project; there can only be one accountable party per task.

- **Consulted (C):** Team members who review and provide input into the task being completed; there may be many consulted members for each task.
- **Informed (I):** Team members who are not directly involved in the activity but should be kept aware of progress; there may be many informed members for each task.

The responsibility assignment matrix or RACI chart will vary for each organization implementing cybersecurity based on the organizational structure and the planned completion of cybersecurity lifecycle tasks. An example RACI chart is provided in Table 11-1. This example provides a starting point for defining responsibilities for lifecycle tasks but should be adapted to align with an organization's implementation approach.

Table 11-1 Example RACI Chart for Cybersecurity Lifecycle Activities

No	Cybersecurity Lifecycle Activity	Project/ Site Manager	IACS Security Lead	Process Safety Engineer	Control Engineer	Process Engineer	O&M Engineer	IT Personnel
Assess Phase								
1	Define Project Scope	A, R	C	C	I	I		I
2	Determine System Under Consideration, Develop Network Architecture	A	R	C	I	I		I
3a	HIRA: Initial Risk Assessment	A	R	C	C	C	C	I
3b	HIRA: Cybersecurity Vulnerability Analysis	A	R	C	C	C	C	I
3c	HIRA: Detailed Risk Assessment	A	R	C	C	C	C	I
4	Document Requirements: Cybersecurity Requirements Specification	A	C	R	C	I	I	I

Table 11-1 continued

No	Cybersecurity Lifecycle Activity	Project/ Site Manager	IACS Security Lead	Process Safety Engineer	Control Engineer	Process Engineer	O&M Engineer	IT Personnel
Design Phase								
5	Conceptual Design: Select Countermeasures		A	I	R	I		C
6	Design Verification: Security Level Verification		A	I	R	I		C
7	Detailed Design: Device Configuration and Software Asset Inventory		A	I	R	I	C	C
8a	Cyber Factory Acceptance Test		A	I	C	I	R	I
8b	Installation and Commissioning		A	I	R	I	C	I
8c	Cyber Site Acceptance Test		A	I	C	I	R	I
8d	Pre-Startup Safety Review: Cybersecurity Assessment		A	R	C	C	C	I

Table 11-1 continued

No	Cybersecurity Lifecycle Activity	Project/ Site Manager	IACS Security Lead	Process Safety Engineer	Control Engineer	Process Engineer	O&M Engineer	IT Personnel
Maintain Phase								
9a	Startup: Begin Operations	A	I	I	C	C	R	
9b	Operation: Use Countermeasures		A	C	C	C	R	I
9c	Preventative Maintenance: Anti-Virus Updates, Patch Management		A	C	R	C	C	I
10	Monitoring and Metrics: Tracking Security KPIs, Cybersecurity Monitoring		A	C	R	C	C	I
11	Periodic Assessment: SVA, Audits		A	R	C	C	C	C
12	Modification & Decommissioning: Management of Change		A	R	C	C	C	I

In addition to defining cybersecurity roles and responsibilities, training and awareness are also crucial steps in the implementation of any CSMS program. As introduced in Chapter 10, cybersecurity competency and workforce involvement are foundational steps in implementing the risk-based approach for cybersecurity. The necessary competency development activities for a CSMS program can typically be broken into two parts. First, general cybersecurity awareness training should be provided and reviewed on a periodic basis for all personnel at the site. Second, additional role-based training should be provided relating to the cybersecurity program requirements and the more detailed procedures/ methods used to meet the program requirements. Effective education programs should teach employees and contractors both the “how” and the “why” of appropriate cybersecurity behavior. Additionally, effective cybersecurity training programs are an important component of developing professional competency for cybersecurity positions. Knowledgeable and vigilant staff are one of the most important lines of defense in cybersecurity.

11.1.2 Audit

After developing a cybersecurity management system, the challenge of implementation and enforcement begins. Without a well-defined approach to system audits, it is difficult to ensure that cybersecurity requirements are being met consistently. Additionally, audits also provide opportunities to identify deficiencies in cybersecurity protections and allow for corrections to be made prior to an incident. By defining the audit methodology, timeframe, metrics, and management of corrective actions in the CSMS, an organization can ensure that all sites are made aware of the implementation responsibilities and that progress will be consistently tracked. Typically, this performance tracking involves three primary efforts:

1. Regular audits to ensure compliance with plant cybersecurity policies and standards (this section)
2. Updating of the Security Vulnerability Assessment to take into consideration changing threats, vulnerabilities technologies or consequences. (Chapter 9)

- 3. Re-evaluation of cybersecurity policy, standards, or procedures, considering any changes in the Cybersecurity Vulnerability Assessment results. (Section 11.1.3)

The effectiveness of regular audits can be improved by following a consistent audit method with an audit template or checklist. The checklist should be easy to use and focused on the most important elements of the CSMS program. An example IACS cybersecurity audit checklist is provided in Table 11-2 and can be adapted to meet a specific site’s cybersecurity program. A larger list of potential cybersecurity audit questions is included in Appendix D.

Table 11-2 Example IACS Cybersecurity Audit Checklist

IACS Cybersecurity Audit Checklist			
Requirement	Yes/No	Comments	Action Item?
Is an IACS Security Lead assigned?			
Has the CSMS been adopted by site?			
Are personnel completing cybersecurity lifecycle activities competent?			
Is the implementation of the cybersecurity policy monitored per Quality Assurance or Process Safety Management Procedures?			
Is MOC applied to all changes to the IACS or to all changes that can impact the IACS?			
Has a Cybersecurity Risk Assessment been completed?			
Have high risk scenarios from the risk assessment been addressed?			
Have steps been taken to limit the attack surface for the IACS?			

Table 11-2 continued

IACS Cybersecurity Audit Checklist			
Requirement	Yes/No	Comments	Action Item?
Is an up-to-date system architecture and inventory maintained?			
Is physical security enforced for IACS assets?			
Are access accounts to the IACS restricted and managed?			
Is patch management implemented to eliminate identified vulnerabilities?			
Is anti-virus protection used where feasible in the IACS?			
Is all documentation kept for the cybersecurity lifecycle, accurate, traceable, fit for purpose, accessible, uniquely identified, and kept with version history?			
Manager:	Signature:		Date:
Auditor:	Signature:		Date:

11.1.3 Continuous Improvement of CSMS

Continuous improvement as defined in the CCPS Glossary is a strategy for “Doing better as a result of regular, consistent efforts rather than episodic or step-wise changes, producing tangible positive improvements either in performance, efficiency, or both. Continuous improvement efforts usually involve a formal evaluation of the status of an activity or management system, along with a comparison to an achievement goal. These evaluation and comparison activities occur much more frequently than formal audits” [1].

Similar to process safety, adopting a continuous improvement style approach can also be a useful supplement to the risk-based framework. Continuous improvement can be looked at as an extension of the “Learn from Experience” foundational block. Defining the conformance metrics for the

CSMS program helps to support this approach. Cybersecurity metrics (or key performance indicators) were introduced as a core element of the risk-based approach in Chapter 10.

The cybersecurity program needs to continually evolve to stay current with the ever-changing cybersecurity threat landscape and the rapid pace of change for protective technologies. The most effective method to maintain the currency of the CSMS is to track, measure, and improve cybersecurity efforts over time. This continual process of reviewing, improving, and maintaining the CSMS facilitates the conformance of the cybersecurity system throughout the life of the facility.

The typical steps in a continuous improvement cycle are to plan, do, check, and act as shown in Figure 11-2.

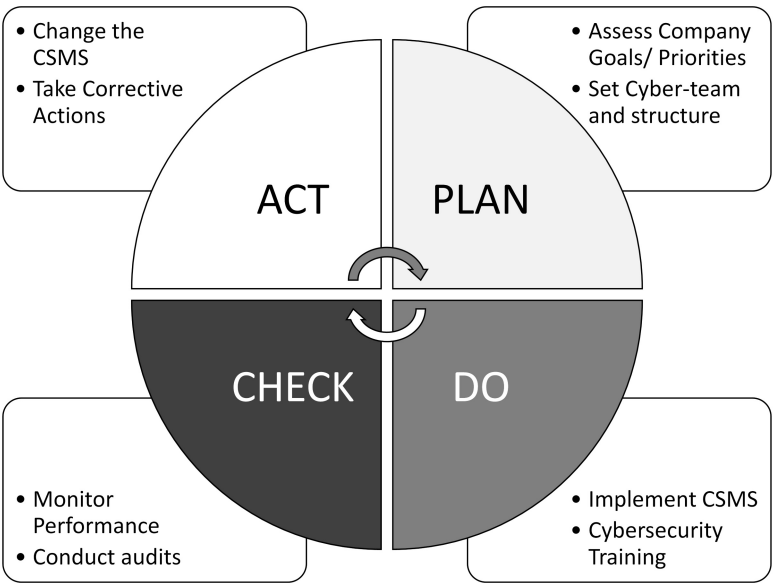


Figure 11-2 Continuous Improvement Process for CSMS

The first step in the continuous improvement process is to plan. This activity begins with the assignment of the organization or role responsible for managing changes to the CSMS. This step should be included in the considerations for organizational security in Section 11.1 and the RACI chart

developed for the organization. The plans for implementing the CSMS should also be communicated with stakeholders and affected personnel.

The next step in the continuous improvement process is to do. This step includes the implementation of the cybersecurity management system including the deployment schedule, cybersecurity training activities, and addition of cybersecurity protections.

The third step in the continuous improvement process is to check. Many metrics are available to track the performance of the CSMS. (For an example list of cybersecurity metrics, see Appendix C.) The following are commonly employed strategies for checking the performance of the CSMS:

- Review of potential threats to the IACS and conduct impact analyses.
- Review cybersecurity incidents, both internal and external to the organization.
- Monitor and evaluate changing legislation and industry standards relevant to cybersecurity.
- Analyze, record, and report operational data for key performance indicators of the CSMS.
- Investigate ineffective CSMS policies and procedures to determine root causes for problems.
- Validate that actions from previous audits have been implemented.
- Benchmark cybersecurity activities and strategies, both within and outside of the industry.
- Request and report employee feedback on security suggestions.
- Adapt standard plant business methodologies (i.e., Six Sigma) to measure, analyze, improve, and sustain cybersecurity improvements.

It is not expected that every possible method for checking CSMS performance is implemented by every organization. However, reviewing the strategies provided and identifying which approaches will offer the best synergy with existing quality and process safety management systems can substantially increase the likelihood of cybersecurity improvements being made.

The last step in the continuous improvement process is to act. Acting includes making changes to the CSMS to rectify issues identified during periodic evaluations. For each identified deficiency, corrective or preventative

actions should be identified and implemented as part of this phase. Often, establishing triggers or thresholds for cybersecurity metrics can make it clear when changes to the organization's technology, business objectives, or cybersecurity activities are needed. Defining formal action triggers also helps to maintain the consistency of audits across multiple sites.

The continuous improvement process provides an effective way to learn from a site's operating experience and ensure that this learning is translated to improvements in the overall CSMS program. Following a step-by-step methodology not only leads to consistent deployment, but it can also support the tailoring of the CSMS to meet any organization's strategic goals and risk tolerance.

11.2 Integrating CSMS with Process Safety Management

Although in the past it was unusual for a process safety engineer and the IT architect to possess detailed knowledge of both functional safety and cybersecurity, it is no longer possible for safety and security activities to operate effectively in separate silos. Cybersecurity incidents such as Stuxnet [9], the German steel mill [8], the Ukrainian power outages [21], and the Saudi petrochemical facility [10] clearly demonstrate that safety objectives and cybersecurity objectives are intrinsically interconnected. It is important for both process safety and cybersecurity-oriented roles to understand the implications of cybersecurity incidents and the potential to cause safety-related and financial harm.

Improving the integration of cybersecurity and process safety activities has two clear hurdles. The first is technical vocabulary. As first introduced in Chapter 8, IT and OT personnel have different priorities and different contexts. For example, a typical frequency for a demand on a safety critical system may be around once in 10 years, whereas the IT security analyst may see persistent threats of cyber-attacks continually for each hour of each day. The second hurdle is the traditionally separated work processes. During a traditional HIRA study, operations, engineering, safety, IACS, and process engineers are all relevant working partners who participate during the review. To add an IT resource on top of those roles often seems overwhelming and may not be the best use of time for the IT architect.

The CSMS can go a long way towards minimizing the impact of both hurdles. First, by defining the organizational structure of the IACS security team, the CSMS can identify which activities require IT support and provide key touch points between the IT and OT security teams and disciplines of the combined security team. Additionally, adopting a lifecycle-based approach can help to facilitate smoother integration between IT-focused security activities, IACS-focused security activities, and process safety-related activities. An integrated work process consolidates communications and fosters improved understanding across the disciplines.

As the need for cybersecurity in IACS becomes increasingly clear, both security and safety disciplines need to understand the similarities and differences between the groups to ensure that both security and safety can be achieved. This change in mindset requires a cultural shift – a recognition that critical process safety and security goals cannot be achieved without the collaboration of both disciplines. The risk-based approach defined in *Guidelines for Risk Based Process Safety (RBPS)* [7] is critical for addressing both areas. Maintaining consistent risk criteria across both disciplines allows for a clear comparison of the risks resulting from process safety incidents and cybersecurity incidents, and it allows for one integrated approach in reducing overall facility risk. Involving stakeholders from all affected groups during the development of the CSMS program is a core step in meeting the safety and cybersecurity needs of all parties.

11.2.1 Lifecycle Approach

A lifecycle-based approach is one of the best opportunities to integrate cybersecurity into the existing process safety risk management process. As first introduced in Chapter 7, the cybersecurity and process safety lifecycles were originally designed and intended to be operated separately. Over time, it became clear that better alignment of safety and cybersecurity activities was needed, and a number of industry efforts have been taken to demonstrate how this can be achieved (such as the technical report ISA TR-84.00.09 [80]). The full integrated lifecycle was presented in Table 7-1.

A key activity in the CSMS is to identify the subsequent lifecycle steps to be completed. Although the CSMS should not go into detail for each step, it is beneficial to reference the subsequent procedures needed to achieve the

cybersecurity objectives. Depending on the differences between the technologies employed and the operations of multiple sites, these procedures can be defined centrally or may need to be written for specific sites. Example procedures/ templates that may be needed underneath the CSMS are documented in Table 11-3.

Table 11-3 Example Cybersecurity Lifecycle Procedures/ Templates

Procedure Title	General	Site/System Specific
Project Cybersecurity Plan Template	X	
Personnel Security and Competency Procedure	X	X
Competency Log	X	
Action Item Template	X	
Cybersecurity Assessment Procedure	X	X
Cybersecurity Audit Procedure	X	
Management of Change Procedure	X	X
Configuration Management Procedure		X
Data Security and Cryptography Procedure	X	
Initial Risk Assessment Procedure	X	
Network Segmentation Procedure	X	
Cybersecurity Vulnerability Analysis Procedure	X	
Cybersecurity Detailed Risk Assessment Procedure	X	
Cybersecurity Requirement Specification Procedure & Template	X	X

Table 11-3 continued

Procedure Title	General	Site/System Specific
Firewall Configuration and Management		X
Device Hardening		X
User Security/ Access Control		X
Security Level Verification Procedure	X	
Cyber Factory Acceptance Test Procedure/ Plan	X	X
Installation and Commissioning Procedure	X	X
Cyber Site Acceptance Test Procedure/ Plan	X	X
ICS Maintenance Plan		X
Site Training		X
Patch Management Procedure		X
ICS Backup Procedure		X
Emergency Response Plan		X
Business Continuity Plan	X	
Quality Assurance Procedure	X	
Supplier Quality Assurance Procedure	X	
Document Control Scheme	X	

For many of these cybersecurity activities, existing process safety and functional safety procedures can either be referenced in the cybersecurity procedure or adapted to cover both safety and cybersecurity considerations. Both methods of integrating lifecycle activities can be effective. The goal is to find the easiest method for creating and maintaining robust systems for the CSMS and process safety management. In some cases, the preferred approach

can be governed by which groups are responsible for process safety and cybersecurity documents.

The objective for adopting an integrated lifecycle approach is to better manage safety and cybersecurity risks and ensure that optimal risk reduction measures are taken. Following a step-by-step lifecycle ensures that no critical activities are missed. Additionally, by aligning the process safety and cybersecurity lifecycles, costs can be reduced by avoiding duplicate effort and rework. This synergy has been identified by many high-performing organizations in industry that have already implemented - or are in the process of implementing - a work process for integrating cybersecurity and safety activities. One factor that seems to play a significant role in the ability or willingness of an organization to undertake an integrated approach is the maturity of the organization with their process safety and cybersecurity activities. As companies build a clearer understanding of the required activities and implement more robust programs, the need for an integrated work process and the resulting benefits become clearer. A comprehensive work process, which includes all necessary safety and cybersecurity tasks, is critical to the success of the integrated lifecycle. By pulling the unique requirements from the safety and cybersecurity lifecycle and integrating the overlapping requirements, one unified approach can be employed.

11.2.2 Areas of Overlap between CSMS and PSM

The integrated lifecycle provides guidance on the most effective ways to incorporate cybersecurity into the existing process safety risk management process. An important step in adapting the lifecycle to a specific organization is to clearly define the areas of overlap or commonality between the CSMS and PSM programs. Every facility is unique, and the risk-based approach should be tailored to meet corporate risk criteria and site-specific hazards in order to create an effective risk management workflow.

Some core activities, such as the definition of organizational risk tolerance and the specification of the corporate risk matrix and risk criteria, are clearly shared between both lifecycles. Other activities, such as the development of personnel competency and the selection of suitable equipment, also have considerations for both safety and cybersecurity. By taking the steps necessary to complete these core activities in a cohesive way, organizations

can build a solid foundation for both safety and cybersecurity activities. Identifying the common requirements for process safety and cybersecurity and clearly communicating these to other groups within the organization such as procurement (equipment selection) and human relations (competency) can further improve the effectiveness of the integrated approach.

After optimizing the foundational activities for safety and cybersecurity, it is useful to consider each key overlap point in the lifecycle to identify a practical approach to managing each task.

1. **Hazard Identification:** The first step to implement both the process safety or cybersecurity lifecycle is to develop a thorough understanding of the hazards present in the facility and the level of risk presented by that hazard. Hazards may result from equipment failure or cybersecurity sabotage and may have the potential to impact many risk receptors. As identified in Chapter 9, transferring results of the traditional process hazard analysis to the cybersecurity risk assessment can help to reduce the time required to define consequence severity in both the initial and detailed risk assessments. Additionally, the cybersecurity risk assessment can be used to identify any scenarios where a cybersecurity threat could compromise multiple process safety independent protection layers, resulting in higher residual risk unless sufficient security actions are taken.
2. **Hazard Data to Design Processes:** The results of the hazard identification are used as an input for the conceptual design of independent protection layers and cybersecurity countermeasures. The objective of the design phase is to ensure that the overall risk for both safety and cybersecurity scenarios are mitigated to within the organization's risk tolerance.
3. **Hazard Data to Validation Processes:** The next step is for the SIL (safety) and SL (security) targets to be evaluated and verified for the functional safety and cybersecurity lifecycles. These two requirements represent the validation of the design phase. The validation steps require that the information from the risk assessments is considered and that the choices made in the conceptual design phase are evaluated and provide a sufficient level

of risk reduction. These processes are surprisingly similar across disciplines; they rely on the same methodology of evaluating the effectiveness of a design against the original requirements documented.

4. The interface between the two lifecycle tasks does not stop here. An important requirement in the validation step is to ensure that no antagonistic relationships exist between safeguards and cybersecurity countermeasures (e.g., increasing the response time of a safety instrumented function). This can occur in some cases due to the additional software needed for countermeasures, which can result in a slow response from the programmable logic controller. If this results in a significant increase in response time, it needs to be documented and carefully monitored over time to ensure that the PLC response time remains acceptable.
5. **Management of Change:** Change management is essential for maintaining the achieved safety and security levels for a system. Changes that are not properly assessed can increase the frequency of demands on protection systems or even render them totally ineffective. Cybersecurity considerations for cybersecurity MOC were first introduced in Chapter 9, and it is critical that these are integrated into existing MOC activities, either as one shared procedure or as an additional cybersecurity procedure.
6. **Lifecycle Assessments:** The safety and cybersecurity lifecycle steps also follow a similar methodology in conducting periodic functional safety and cybersecurity assessments. These assessments are intended to provide an independent check of the lifecycle work completed to ensure that no mistakes were made and that all relevant scenarios have been properly evaluated. First introduced in ISA TR-84.00.09, cybersecurity assessments are intended to be completed at the same lifecycle stages as the safety assessments [80]. Integrating these safety and cybersecurity assessment activities into one comprehensive process can further reduce the time required to support lifecycle implementation.
7. **Abnormal Situation Management:** The last step is the development of event response for abnormal situation

management, including for both process safety and cybersecurity events. Abnormal situation management is relevant to each lifecycle. In the cybersecurity lifecycle, situation management is designed into the business continuity plan, whereas traditional emergency response plans are typically used for process safety incidents. For some events, it may not be immediately clear whether a process excursion is the result of an equipment failure or a cybersecurity event. In these cases, it is important that both possibilities are investigated and that the correct actions are taken to mitigate the potential harm.

8. Although the business continuity plan is a concept designed for cyber-related incidents, the same principles that govern this plan are also relevant to returning a plant to normal working order after a safety-related event or abnormal situation. This step further emphasizes the benefits that can be derived from additional collaboration across disciplines, by demonstrating the value which can be derived from applying core concepts across disciplines.

Optimizing the foundational activities for the safety and cybersecurity lifecycles, as well as effectively managing the interfaces between lifecycle activities, ensures that safety and security goals are achieved while providing the potential to reduce the time and cost associated with implementation. Adopting an integrated approach in the development, implementation, and monitoring of the cybersecurity management and process safety management systems provides the greatest efficiency gains.

11.3 Summary

Implementing a holistic approach for cybersecurity and process safety activities is necessary to ensure that both safety and cybersecurity objectives are met. Successful implementation of this approach starts with developing a robust cybersecurity management system, assigning responsible parties, and providing the training necessary for sites to be successful. Maintaining consistent tolerable risk criteria between safety and cybersecurity risk assessments further supports the adoption of a holistic approach. The use of periodic audits and a continuous improvement-focused approach can enhance the overall implementation of both safety and cybersecurity

activities. Finally, deploying a lifecycle-based approach, supported by necessary procedures and integrated into existing process safety activities, ensures that all necessary steps are completed to achieve both safety and cybersecurity objectives.

Part 3: Where Do We Go from Here?

12 What's Next? A Look at Future Development Opportunities

Part I of this book focuses on providing the background for cybersecurity as it is today. Part II focuses on strategies and techniques for effective implementation of cybersecurity protection and the integration of cybersecurity and process safety activities. Part III of this book takes this discussion a step further and covers where cybersecurity is likely to move in the future. Cybersecurity continues to evolve at a rapid pace, and achieving security and safety goals requires staying technically current.

As highlighted by the case histories in Chapter 6, IACS are becoming increasingly targeted for cybersecurity attacks. Stuxnet [9] and Triton [67] are just a few examples of malware designed specifically for use in attacks on IACS. Sophisticated attacks on IACS pose a dangerous threat that can result in safety incidents, material losses, and downtime. Damaging cybersecurity incidents on chemical sites and other critical infrastructure can have significant impacts on national stability, public welfare, the environment, and financial growth. The attacks on the Colonial Pipeline [36] and Oldsmar Water System [22] demonstrate the potential for cybersecurity incidents on critical infrastructure to trigger significant impacts to the supply chain.

Not only does the exposure to cybersecurity threats appear to be growing, but many organizations are also growing their digital presence online and migrating their infrastructure to the cloud - often outside the protection of firewalls and network security controls. This digital transformation has grown the enterprise attack surface and dramatically broadened the spectrum of threats and vulnerabilities that can affect the average organization. As connectivity to IACS systems shows no sign of stopping in the future, cybersecurity will continue to be an essential element to achieve safe operations.

Transformation is to be expected in the digital age; however, the global novel coronavirus pandemic, which began in late 2019, has had a significant impact on the rate of change for the cybersecurity landscape. Few could have predicted the changes and upheaval ushered in by the global pandemic. It has

completely changed how many live and work, with some organizations moving quickly to make permanent changes to behaviors as well as to IT and OT systems. It has driven a significant increase in teleworking and the use of Virtual Private Networks (VPNs). Rapid deployment of remote access and teleworking infrastructure is driving an unprecedented convergence of IT and OT ecosystems. It has also led to significant exposure of OT systems, with the number of internet-facing Remote Desktop Protocol (RDP) ports rising 50% from 3 million to 4.5 million [113]. When implemented securely, RDP can be a reliable way of establishing remote access; however, when used incorrectly, open RDP ports are a valuable resource to attackers.

The Cybersecurity & Infrastructure Security Agency (CISA) and the National Cyber Security Center (NCSC) have issued advisories warning of the accelerated risk of cybercriminal activity and advanced persistent threats APTs seeking to take advantage of this highly vulnerable ecosystem, and it has highlighted this risk to governments, organizations, and individuals [114]. An effective strategy for staying secure in a changing environment should consider changes in cybersecurity adoption (see Section 12.1), changes in technology (see Section 12.2), and changes in attacker behavior (see Section 13.1.3).

12.1 *Cybersecurity Adoption Trends*

Given the importance of IACS cybersecurity, it is important to understand the trends in cybersecurity adoption as organizations continually strive to be better protected against cybersecurity threats. New strategies have the potential to improve the effectiveness of existing methods and reduce the amount of time and energy required to achieve the same level of protection. Additionally, as cybersecurity threats change, strategies for adoption need to also adapt to ensure that the implemented cybersecurity approach provides adequate protection. A number of cybersecurity trends will be reviewed in this section, including:

- IT and OT convergence / Partnership
- Security Operation Centers (SOCs)
- Zero trust architecture
- Secure development practices/ Software Bill of Materials (SBOM)
- Cybersecurity insurance

12.1.1 IT and OT Convergence / Partnership

The fundamental differences between IT and OT systems were first introduced in Chapter 1, and the differences in IT and OT cybersecurity priorities and risk management strategies were analyzed in Chapter 8. IT's most important cybersecurity objective is confidentiality, with a definite focus on protecting network communication through improvements in encryption and authentication techniques, particularly for Industrial Internet of Things (IIOT) devices. In many cases, new cybersecurity technologies will first be deployed for IT systems before determining if they can be applied to OT systems. When applying cybersecurity controls to OT systems, it is important that the availability of the system be managed as the primary concern. However, as the connectivity and exposure of OT systems continues to grow, the IT and OT ecosystems are becoming increasingly co-dependent. This increasing integration of IT/OT systems is commonly referred to as IT and OT convergence.

In the past, the boundaries of IT systems and OT systems were more clearly visible. IT systems commonly included internet-connected storage devices, networking devices and other computers/servers, as well as processes to create, store, secure and exchange electronic data. On the other hand, OT systems were solely associated with isolated manufacturing and industrial environments and included a variety of technologies for the control of physical processes. Many OT devices for monitoring and process control were not computerized. In the past, devices utilizing computer processors generally used closed, proprietary protocols and programmable logic controllers rather than technologies that afforded full computer control.

While IT inherently included considerations for network connectivity communication and security requirements as a part of its scope, OT systems had not been traditionally designed with considerations for connections to larger networks - and especially not internet-connected systems. In the past, OT systems often relied on air gapping for security. With the increasing connectivity between IT and OT systems and the implementation of IIOT devices that leverage networking and communications, the lines between IT/OT will continue to become more muddled. This has posed challenges to traditional OT cybersecurity strategies and has led to significant changes to

address potential vulnerabilities. The growing convergence of IT and OT systems has also led to the need for closer partnerships to achieve the security and operational objectives of both systems.

The impact of IT and OT convergence can clearly be seen in the growing involvement of IT resources in OT cybersecurity discussions and the single security team approach discussed in Chapter 11. IT and OT convergence also provides better IT resource access to the OT group and can help improve the cybersecurity protections deployed in OT systems. In many cases, cybersecurity protections will first be tried in IT systems and then deployed to OT systems when it can be done with a low chance of negatively impacting system availability. Examples of the influence of IT and OT convergence can be seen in the cybersecurity trends for remote access, security operations centers, and the zero trust architecture.

12.1.2 Security Operations Centers

Continuous security monitoring is the process of monitoring logical and physical access to the IACS as well as traffic on the network. As introduced in Chapter 7, common aspects of security monitoring include the detection of malicious and unauthorized mobile code (e.g., removable media), the presence of external connections, periodic vulnerability scans, and the analysis of user behavior. A number of technologies and strategies are commonly employed in industry as companies are working to identify the most robust ways to monitor their systems for cybersecurity compromise.

One strategy that is being increasingly implemented in organizations with sufficient size and resources is a Security Operations Centers (SOC). The SOC is comprised of a team of experts responsible for the continuous monitoring and analysis of an organization's cybersecurity. This team works to detect, analyze, and mitigate cybersecurity incidents with a combination of technology solutions and proven processes. SOC teams typically consist of security analysts, engineers, and managers who work closely with incident response teams to make certain that security issues are addressed. These analysts are specially trained to help ensure that all issues requiring response are identified. SOC's also have detailed detection processes or policies documenting the necessary steps for carrying out the cyber response processes in the event of a cybersecurity event. IT and OT convergence has

also had a significant impact on the use of SOC's, and in many cases, companies are now leveraging these centers to monitor both their IT and OT assets.

Typical SOC infrastructure includes firewalls, Intrusion Prevention/Detection Systems (IPS/IDS), breach detection solutions, periodic probes, and a security information and event management (SIEM) system (first described in Section 8.6). The technology component is an important part of the SOC and often provides the information and insights necessary for the team to quickly identify and respond to potential cybersecurity incidents.

The developments in IACS include continuous security monitoring and threat detection to provide additional visibility into the control system network to the SOC. Continuous monitoring systems can provide continuous vulnerability modeling and advanced vulnerability detection to support a proactive response. Continuous monitoring solutions also define a clear baseline of the IACS normal network behavior; this baseline can be used to identify a variety of security and operational issues. In many cases, the outputs from continuous monitoring tools can directly interface with the SOC, supporting better visibility of network activity.

Organizations should continue to develop strategies to detect and mitigate cyber-attacks. In some cases, organizations without sufficient resources for an internal SOC are instead relying on external Managed Detection and Response (MDR) services. These services bring together the same elements for cybersecurity monitoring - event detection and response as an SOC - but rely on external security resources. This allows smaller organizations the ability to implement robust cybersecurity monitoring without incurring the ongoing cost of maintaining a full-time staff for the SOC.

12.1.3 Zero Trust Architecture and Software Defined Networks

Another strategy that was first implemented for IT systems, but which has the potential to significantly impact OT systems as well, is the concept of the zero trust architecture. A zero trust model works on the premise that trust or (access to a system) should never be granted implicitly; instead, it should be continually evaluated [115]. This is very different from the traditional network segmentation approach, where firewalls permit access to resources based on a systems IP address and the service/ application used.

In the zero trust approach, a device is not automatically able to access resources based on its intrinsic properties; instead, it must pass through a policy enforcement point that evaluates whether or not it is safe to allow the system to connect to the enterprise resources as shown in Figure 12-1.

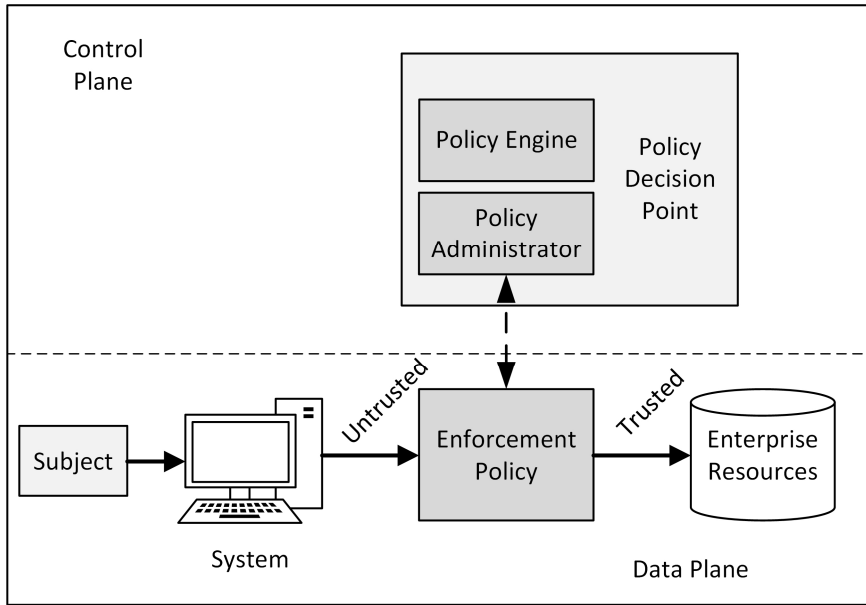


Figure 12-1 Zero-Trust Architecture

Source: NIST SP 800-207 [115]

For a zero trust architecture to be successful, it must reliably grant access to authorized users - allowing them to complete operational tasks - while consistently denying access to unauthorized or malicious actors. This effectiveness essentially comes down to how “good” the enforcement policy is at deciding whether a system can be trusted. This decision is reliant on a variety of external data sources, such as [115] [116]:

- Continuous diagnostic and mitigation systems that collect information about the current security state of a device, update the operating systems and security software as needed, and communicate the current state to the policy engine.
- Network monitoring/ Industry compliance checks, which ensures that the network traffic and behavior are aligned with industry/ organizational benchmarks and compliance rules.

- Ongoing threat intelligence feeds, such as malware definitions, blacklists for known malicious activities, common vulnerabilities and exposures, and other resources.
- Activity logs from network devices, which can indicate unusual activity for specific networks, devices, IP addresses, or other sources.
- Data access policies that are unique to each user and limit the ability to compromise multiple devices in the same zone for any malicious or unauthorized access.
- Public key infrastructure (PKI), which can be used to validate information about the device requesting access by authenticating a certificate issued by an organization to its devices against a certificate authority.
- Identification management, which are the processes followed for managing roles and access privileges for individual users; this is essential for defining rules about to which resources a user would be permitted access.
- Security information and event management (SIEM) systems (as introduced in Section 12.1.2), which can improve the accuracy of the decision-making process by collecting information from a number of the data sources identified in this list.

The zero trust model represents an important trend for securing IT systems and may play an important role in securing peripheral networks connected to the IACS as well. Adoption of a zero trust model approach for IACS applications is likely still in the future due to the potential for a zero trust architecture to block necessary communication on the IACS, leading to reduced system availability and compatibility issues with legacy IACS systems.

Similar to the zero trust model, a software-defined network (SDN) also works by separating the data plane (physical devices and communications) and the control plane (decisions on allowing or disallowing access) [117]. This allows for a single centralized network component to make decisions about which devices on the network should be allowed to communicate independently of the current physical connections for the network [117]. This introduces a potential to implement additional network segmentation using software-based firewalls - this could greatly reduce the upfront cost of implementing a secure network architecture by eliminating much of the physical hardware. Furthermore, even for networks with separated zones such as the enterprise network, DMZ, and control zone, SDNs can support micro

segmentation, or the ability to limit unnecessary traffic communication between devices on the same zone.

The application of SDN for industrial control systems has a number of possible benefits, including facilitating the configuration and automation of networking rules, easier management of network resources, better segmentation, and the mitigation of legacy control plane vulnerabilities [117]. Although SDN has the potential to lead to improvements in these areas, the potential for the failure of single centralized network component, leading to a significant disruption of system availability and compatibility issues with common legacy IACS systems, is a current barrier to widespread adoption.

12.1.4 Secure Development Practices/ Software Bill of Materials

The attack on SolarWinds, an IT network management company, highlights the importance of protecting the supply chain. By targeting SolarWinds, the attackers had the potential to compromise as many as 18,000 customers [26]. Prominent victims of the attack include the Pentagon, nuclear laboratories, the United States Treasury, Commerce, and Energy Departments, and several private cybersecurity firms [27]. This recent example demonstrates the need for secure development practices for components and software, as well as the need to continually protect the supply chain from sophisticated threats.

In many cases, IACS and IIoT devices restrict the ability for operators to make software changes or add security software after installation. This can limit the ability to implement security protections for these devices, and in some cases leaves them vulnerable to attack. To make up for security deficiencies, companies may try to “bolt on” security features from existing systems; however, this typically only has limited effectiveness. It is important to consider opportunities to build security into IACS devices starting with the manufacturers. Building in capabilities for classic security technologies like encryption, authentication, integrity verification, intrusion prevention, and secure update capabilities can provide opportunities for significant security improvements. As manufacturers become more aware of this need, further steps are being taken to secure components throughout development. In fact, even at the chip level, some manufacturers are already building security features into hardware. International standards such as IEC 62443 [107] provide requirements for the secure development lifecycle and security

capabilities that can be adopted to support built in security. Additionally, independent certification to relevant parts of IEC 62443 can provide confidence in the security of components.

The need for secure development goes beyond just hardware components, and hackers continually seek to compromise the software supply chain through penetration and attacks on vendors of software. Recent reports reveal that hacker attempts to inject malware into the software supply chain have increased at over 200% year over year [118]. This is not just a risk for desktop computers; it also applies to IACS and IIoT devices as well.

Most software depends on third-party components, such as libraries, executable files or programs, or source code; however, there is very little visibility into this software supply chain. It is very common today for software to contain numerous third-party components that may not have been clearly identified or even recorded. Software vulnerabilities are a byproduct of the human process of developing software and are being increasingly targeted in attacks in the software supply chain. If users are not aware of the components in their software, they may not be aware that patching is required. In some cases, users may have no way to know if their software is potentially vulnerable to an exploit due to an included component – or even know if their software contains a component that comes directly from a malicious actor. The reality is that, when a new risk is discovered, very few organizations can quickly and easily answer simple, critical questions such as: “Are we potentially affected?” and “Where is this piece of software used?” This lack of transparency into the composition of software across the digital landscape is an often-overlooked element that contributes substantially to cybersecurity exposure, as well as to the costs of development, procurement, and maintenance.

Implementing a Software Bill of Materials (SBOM), as recommended by the National Telecommunications and Information Administration (NTIA) [119], is one method for developing a nested inventory with the list of ingredients that make up software components. This approach, as shown in Figure 12-2, can help to significantly cut down on the amount of unknown code in the software supply chain.

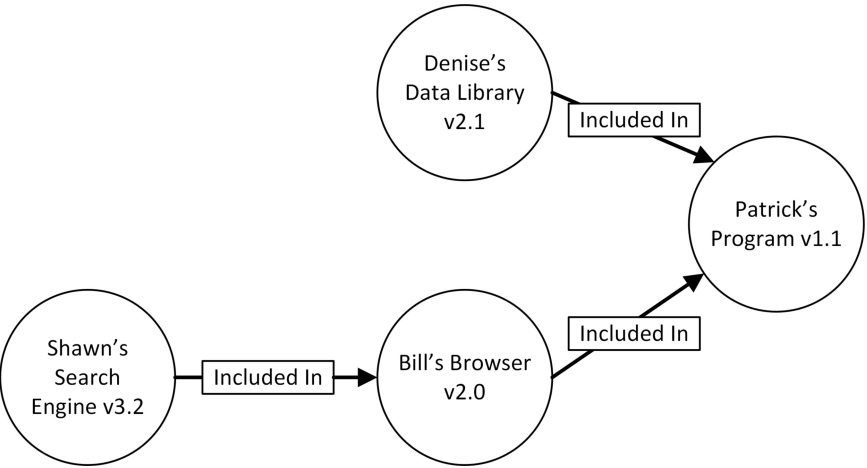


Figure 12-2 Simple Example of Software Bill of Materials

Source: NTIA Software Bill of Materials [119]

To be effective, it is important that the SBOM includes baseline software component information such as [119]:

- Name of the supplier
- Name of the component
- Name of the author
- Unique identifier
- Version and revision of the component
- Functional relationship with other components.

Software may span multiple industry groups, each with specialized needs, and contain components from open source and commercial software. As such, any solution for improving the software supply chain need to work across the entire ecosystem. The SBOM approach provides greater visibility into the software supply chain and allows for earlier identification and mitigation of potentially vulnerable systems. It also supports informed purchasing decisions by users and incentivizes the adoption of secure software development practices. A well-implemented SBOM can enhance software supply chain security and help to mitigate vulnerabilities before they are exploited - or help to respond more quickly once an incident is identified.

Additional industry efforts, such as the Open Process Automation Standards (O-PAS™), also outline steps for building cybersecurity directly into software and hardware components. The O-PAS standards are being released in three stages, with version 1 (interoperability) and version 2 (configuration portability) of the standard currently available, and version 3 (application portability) scheduled for release in 2021 [120]. The objective of these standards is to improve the openness and modularity of process automation solutions so that they can be more easily deployed in secure infrastructures [121].

12.1.5 Cybersecurity Insurance

Several strategies can be taken when companies evaluate risk. In part II of this book, methods for risk assessment countermeasures for mitigating risk were identified. One strategy of risk management that has not yet been discussed is that of risk transfer. Risk transfer is the practice of passing risk to another entity (such as an insurance company). Risk transfer almost always has a cost, such as an insurance premium, as part of the agreement for transferring the risk.

Cybersecurity insurance policies are specifically designed to allow companies to transfer the potential negative financial impacts of cybersecurity incidents such as data breaches, stolen funds, lost income (e.g., unscheduled downtime), ransomware, and computer replacement. Although insurance coverage is typically in the form of financial payment, coverage options are available to offset the costs of cybersecurity incidents resulting in other types of harm, including bodily injury and pollution damage. In some cases, coverage can even extend to intangible impacts, such as reputational harm loss and even reputational repair.

For organizations to choose to purchase cybersecurity insurance, either within a general policy or as a standalone policy, generally requires a perceived financial benefit between the cost of the insurance policy and the coverage limits in the result of an incident. The results of the hazard identification and risk analysis are often a valuable input into this decision-making process, and the expected loss from an incident may be determined by multiplying the expected likelihood by the potential cost of the incident (Equation 12-1).

$$\text{Expected Loss} = C(\$) \times L_{AS} \quad \text{Equation 12-1}$$

Where:

C is the consequence of the attack as a function of the financial impact

L_{AS} is the likelihood of a successful cybersecurity attack within a time basis (e.g., policy length)

If the expected cybersecurity loss is higher than the insurance premium and any potential deductions, it may be beneficial to purchase insurance. However, although this may seem like a straightforward comparison, a number of other factors may come into play, such as the details of what types of events are covered and any exclusions from the policy.

Current valuations for the global cybersecurity insurance market are slightly above \$7 billion U.S. dollars [122]. Multiple projections estimate that, in the next 5 years, this market could grow significantly to the size of \$20-\$25 billion U.S. dollars [122] [123]. Other estimates are less optimistic and project slower, although still positive, growth for the cybersecurity insurance industry [124].

Although the prevalence and visibility of cybersecurity incidents continue to rise, cybersecurity insurance has not grown as steadily as previously expected. In the United States, several factors have been identified that are believed to be slowing the adoption of cybersecurity [124]:

- Cost of insurance options is too high.
- Coverage limits are too low.
- Coverage terms and exclusions were unclear or too restrictive.
- Insurers and brokers are not promoting standalone cybersecurity insurance.
- Cybersecurity insurance viewed as a luxury but not a need.

A survey of U.S. companies ranging from revenue below \$100 million U.S. dollars to over \$1 billion U.S. dollars across multiple industries – including manufacturing, utilities, healthcare, financial, and retail – showed that 47% of organizations had cyber insurance in 2019 (up from 34% in 2017) [125]. Of the companies surveyed, larger companies (those with revenue above \$1 billion U.S. dollars) were much more likely to have cybersecurity insurance than

smaller companies (less than \$100 million U.S. dollars in revenue) at 57% and 36% respectively [125].

Cybersecurity insurance adoption also seems to be heavily dependent on an organization's region. The United States currently makes up a relatively large portion of the global cybersecurity market, but along with the rest of North America and the European region, appears to have only moderate growth [122]. The fastest growing market appears to be the Asia Pacific Region, while South America, Africa, and the Middle East appear to have the lowest growth rates [122].

The growth of the cybersecurity industry has the potential to support improved cybersecurity practices in several ways, according to the Cybersecurity and Infrastructure Security Agency (CISA) [126]:

1. Promoting the adoption of preventative measures in exchange for additional coverage.
2. Encouraging the implementation of best practices by basing premiums on an organization's level of self-protection.

Global insurance providers are continuing to become more knowledgeable about industrial cybersecurity concerns as a result of increasing engagement with government and industry groups [126]. This introduces the potential for insurance companies to be a major driver of cybersecurity implementation. This relationship is expected to be particularly strong in regions where the regulatory requirements for cybersecurity are limited. This correlation has already been seen in the field of functional safety in the United States, where insurance companies often drive adoption of industry best practice in exchange for improved premiums. In extreme cases, insurers may even refuse to extend policies if certain safety lifecycle activities are not completed.

Although cybersecurity insurance may still be viewed by many companies as a luxury and not a requirement, as insurers continue to adjust their coverage based on the implementation of cybersecurity controls – and as the frequency of cybersecurity incidents continues to increase – it is likely that the number of companies purchasing cybersecurity insurance will also rise. Even

if this increase in insurance policies is not as high as was originally projected [124], it is still likely that insurance companies will become a growing driver in the adoption of cybersecurity best practices.

12.2 Emerging Technologies

When looking at the future of IACS cybersecurity, organizations should consider the impact of emerging technologies on the cybersecurity landscape. Depending on the technology, the impact could either be a change in the level of exposure for IACS systems or changes in the ease/ effectiveness of security measures. Several advancements are poised to have major impacts on IACS systems, including:

- Implementation of 5G
- Edge computing
- Machine learning & Artificial Intelligence

12.2.1 Implementation of 5G

Implementation of fifth generation (5G) wireless technology represents one of the biggest critical infrastructure additions in many years, and 5G has the potential to further transform the digital landscape. It also has the potential to introduce new cybersecurity challenges, as tens of billions of smart devices are connected to the internet [127].

The Cybersecurity and Infrastructure Security Agency (CISA) has determined that the introduction of untrusted 5G components into the Radio Access Network (RAN) could expose core network elements to risks introduced by software and hardware vulnerabilities, counterfeit components, and component flaws caused by poor manufacturing processes or maintenance procedures [127]. Malicious actors can use these untrusted components to gain access to IIoT devices, which can be difficult to secure due to poor device management and platform diversity. Malicious actors may target IIoT devices by exploiting deficient configurations and then use those devices as initial access points to gain a foothold in RAN networks [127].

As industrial installations of IIOT devices continue to increase, combined with the transition to 5G, cybersecurity strategies need to be developed to mitigate this risk [128]. The 5G network will transition from centralized, hardware-based switching to distributed, software-defined digital routing.

This means inspection and control checkpoints will be pushed out to a web of digital routers throughout the network, leading to improved inspection capabilities and a reduction in chokepoints/ bottlenecks in connectivity. These software-based operating systems and protocols may lead to increased exposure. Ultimately, 5G will lead to an increased deployment of potentially hackable smart IIoT devices. Although 5G has benefits such as 100 times faster download speeds, 10 times decrease in latency (delay before data transfer begins), and 100 times increase in network capacity [127], it will be important to balance operational improvement with the potential increase in vulnerabilities to manage cybersecurity risk.

12.2.2 Edge Computing

Edge computing is transforming the way data is processed and stored by moving some of the core network functions closer to the end user at the network edge, rather than relying on a central location that may be a significant distance away. Gartner estimates that, by 2022, some three-quarters of enterprise data will be processed outside of central locations such as the cloud [129].

Moving data processing and storage closer to the point of origin minimizes the amount of long-distance communication required between client and server. Edge computing supports 5G emerging technologies by providing reduced latency and decreased core network traffic. For example, 5G will help autonomous vehicles that rely on immediate data processing and analysis to ensure near-instantaneous responses. An autonomous vehicle using edge computing sends data to a nearby access point where it is analyzed and returned, avoiding all the additional network hops it often takes to send information to a centralized data center. In a traditional network architecture, the autonomous vehicle communicates with a centralized data center, which could increase the number of network hops and impact time-sensitive applications like high-definition mapping, real time traffic flow, and industry specific logistical data.

In IACS applications, edge computing allows companies to balance the ever-increasing demand for computing power and internet bandwidth. While the benefits are considerable, the combination of cloud and edge computing introduces concern over the control of connected devices and could make

them a prime target for hackers interested in gaining access to IIoT devices from external networks. This has the potential to put critical data at risk as well as to provide an additional pathway for attackers to gain access to the IACS. Operators need to have a rigorous process for vetting devices and evaluating both the hardware and the software. A well-developed lifecycle-based strategy can help to ensure the security of edge computing devices and avoid a significant increase in the network exposure of the IACS.

12.2.3 Machine Learning and Artificial Intelligence

Machine learning and artificial intelligence are being increasingly used to identify patterns and signals, allowing for the detection of anomalies as they arise in real time. This technology allows businesses to detect attacks more quickly and accurately than ever before. This section will discuss two types of machine learning that can help to improve the effectiveness of cybersecurity protections: “standard” and stateful.

- Standard: raw data can be input directly into the machine learning model and the model makes a prediction considering only that data.
- Stateful: the machine learning model considers previous inputs when evaluating new data. It is possible for the model to look across historical information when making a prediction.

One example of machine learning in a cybersecurity application is the detection of malware. By inputting a portion of the program code into a machine learning model, it is possible to predict whether there is enough commonality with previously seen malware attacks to identify the behavior as malicious. One advantage of machine learning-based approaches is that machine learning tends to be relatively successful at ignoring any techniques used by the attacker to disguise the intention of the malware, which can significantly improve the speed and accuracy of the incident response. This is a “standard” application of machine learning in that a binary decision of malicious or non-malicious is made for the tested software program. Once the determination is made, it will not change over time, without a user action to approve or deny a specific program.

Unlike malware, human behavior changes over time making it more difficult to detect malicious activity. Sophisticated threats can often occur at the human layer when people use digital interfaces like email. Unfortunately,

entering raw email data into the model would not provide the full context of the individual's email history, so it would not be easy to predict if an employee is about to leak sensitive data or determine whether they have received a message from a suspicious sender. With stateful machine learning, it is possible to look across each employee's historical email data set and calculate important features by aggregating all the relevant data points leading up to that moment in time. This aggregated input can then be entered into the machine learning model. The introduction of time as a variable makes this a more complicated task, with some features being calculated outside of the model itself. As the complexity increases, the amount of computing power, infrastructure, and engineering involvement also increase. Applying stateful machine learning is difficult, but the benefits of improved anomaly detection and protection against the many diverse types of cybersecurity attacks can make it a worthwhile investment.

People are unpredictable and error prone. Training and formal procedures - while critical steps - cannot fully eliminate the potential for errors. As employees continue to control and share more sensitive company data, organizations need a more robust, people-centric approach to cybersecurity. Advanced technologies that understand how individuals' relationships and behaviors change over time could be very helpful in effectively detecting and preventing threats caused by human performance issues. In some cases, SIEM solutions such as those introduced in Section 12.1.2 include user behavior analytics, a functionality that leverages machine learning to better characterize user activity and identify potential malicious actors.

12.3 Summary

With the development of new technologies like 5G and the growing implementation of smart IIoT devices, the IACS cybersecurity landscape continues to grow in complexity. Addressing the challenges rising from increased connectivity and exposure will require significant commitment across the entire ecosystem. Strategies to mitigate cybersecurity risks will require continual assessment and the implementation of comprehensive standards that will provide organizations with the guidance necessary to develop and maintain an appropriate security program for their operations. Additionally, the growth of cybersecurity insurance may help to catalyze the

adoption of industry best practices based on insurance premiums and coverage options. The ever-changing nature of threats and technology will drive the need for appropriate cybersecurity programs that adapt to an ever-changing threat environment over time and support the adoption of the most effective trends in cybersecurity.

13 Available Resources

As cybersecurity continues to evolve, both in terms of the number and type of threats as well as the available protections, it is important to stay up-to-date with available resources and regulatory requirements. Leveraging these resources is one way to improve the efficiency of cybersecurity activities and ensure the success of the risk-based approach.

13.1 *Local, Regional, and Global Topics*

The implementation of cybersecurity measures and the adoption of the risk-based approach varies from company to company and from region to region, based on an organization's specific goals and objectives. Several core drivers for the mitigation of cybersecurity risk (as shown in Figure 13-1) need to be balanced while making decisions for risk management:

- Moral - Make the plant as safe and secure as possible, regardless of the cost.
- Financial – Minimize the capital and operating costs.
- Legal - Comply with regulations as written, regardless of cost or actual level of risk.

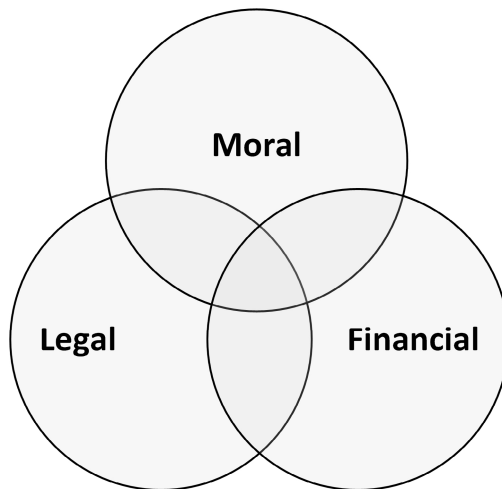


Figure 13-1 Drivers for Facility Risk Management

An effective risk-based approach identifies the area of overlap between drivers to find the right balance between all three factors. Any one obligation taken to the extreme would not be an effective strategy. For example, if the plant is made as safe and secure as possible without any consideration of the cost, the facility would likely be unable to stay in operation because the business would not be financially viable. These considerations need to be effectively balanced in relation to safety and cybersecurity to manage the facility's overall risk to an optimum level.

The financial and moral obligations of a facility are commonly driven by company culture and require a balance between achieving safety/ security targets and necessary financial benchmarks. The region and type of facility are important factors when considering the moral and financial drivers; however, in the case of legal requirements, region and industry are often the defining factors.

13.1.1 Shared Risk Profile

A risk profile is identified in the Chemical Facility Anti-Terrorism Standards (CFATS) as a combination of a facility's risk level, security issues, and physical characteristics [14]. The risk profile is an essential tool for determining the necessary level of performance or security that a facility needs to implement to achieve their organization's risk tolerance. The UK Health and Safety Executive (UK HSE) defines a risk profile slightly differently: "A risk profile examines the nature and levels of threats faced by an organization. It examines the likelihood of adverse effects occurring, the level of disruption and costs associated with each type of risk and the effectiveness of the control measures in place" [130].

The two key elements of the profile in both definitions are the likelihood of the adverse event occurring and the severity of the consequence. The exact risk profile for each site is unique and considers the results of the cybersecurity Hazard Identification and Risk Analysis (HIRA) and Security Vulnerability Analysis (SVA). Using a risk profile is one way to efficiently make decisions on how to best balance the different drivers for risk management and apply these decisions.

Shared risk profiles may be developed for use within a multi-site organization as a means of grouping sites to support easier identification and customization of the risk-based approach to cybersecurity. Sites may be grouped based on similarities in the network architecture, technologies used, or regions. This allows for the most efficient implementation of security controls across multiple sites. Alternatively, shared risk profiles may be developed in industry groups, international standards/ best practices, or regulatory requirements for use in multiple organizations.

Industry sharing forums such as Information Sharing and Analysis Centers (ISACs) help critical infrastructure facilities better protect their systems by communicating information about current cybersecurity threats. These sharing groups, paired with industrial cybersecurity alerts such as those issued by the Cybersecurity & Infrastructure Security Agency (CISA), help to further define the threat landscape. This makes a shared risk profile possible and ensures that organizations are as ready as possible to prevent and respond to cybersecurity incidents.

13.1.2 Regional Difference in Standards, Regulations, and Enforcement

Standards and regulation play a major role in how organizations choose to address cybersecurity risk. Regulatory requirements based on region or industry directly impact the legal driver for risk management, while standards and best practices provide guidance on how to implement cybersecurity protections.

The references in Table 13-1 are divided into four categories: Voluntary Industry Standards and Best Practices, Consensus Codes, U.S. Laws and Regulations, and International Laws and Regulations. These selected examples emphasize influential references that have helped to shape the current cybersecurity landscape. All organizations should review applicable regional regulations to identify if any additional regulatory requirements exist for cybersecurity.

Table 13-1 IACS Cybersecurity Practices, Standards, and Regulations

Voluntary Industry Standards and Best Practices		
Name	Applicability	Summary
IEC 62443 [107]	International Standard	Suite of standards that provide performance-based approaches and specific security capability requirements.
IEC 61511 [18]	International Standard	Performance-based functional safety standard. 2016 edition requires a cybersecurity risk assessment.
ISA TR84.00.09 [80]	International Best Practice	Technical Report on the integration of the cybersecurity lifecycle (IEC 62443) and functional safety lifecycle (IEC 61511).
NIST Cybersecurity framework [11]	International Best Practice	Framework for assessing and improving current cybersecurity posture.
NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security [82]	International Best Practice	Guidelines for industrial cybersecurity including detailed guidance on implementing security controls.
ISO/IEC 27001:2013 Information Security Management [131]	International Standard	Core standard for IT cybersecurity for developing Information Security Management Systems.
ISO/IEC 27002:2013 Code of Practices for Information Security Controls [23]	International Standard	Core standard for IT cybersecurity for implementing cybersecurity controls.

Table 13-1 continued

Consensus Codes		
Name	Applicability	Summary
API 1164 Pipeline SCADA Security [24]	Pipelines, North America	Prescriptive recommendations for achieving security in pipeline SCADA systems.
NERC Critical Infrastructure Protection Standards [15]	Power, North America	Series of standards with prescriptive requirements for cybersecurity in the power industry
U.S. Federal, State, and Local Laws and Regulations		
Name	Authority	Summary
America’s Water Infrastructure Act (AWIA) [16]	Environmental Protection Agency	Mandates completion of a risk and resilience study and an emergency response plan for water systems.
6 CFR part 27: Chemical Facility Anti-Terrorism Standards (CFATS) [14]	Department of Homeland Security	Prescriptive standard that mandates cybersecurity assessments and protections based on risk level for chemical facilities.
18 CFR Part 40: Federal Regulatory Commission (FERC) [132]	Department of Energy	Defines the applicability of mandatory reliability standards (including cybersecurity requirements) for the power industry.
Maritime Security Act (MTSA) [133]	Coast Guard	Prescriptive standard that mandates cybersecurity assessments and programs for maritime sites.
California SB-327 Cybersecurity for Internet of Things [134]	California State	Mandates cybersecurity requirements for manufacturers and asset owners with IoT devices.

Table 13-1 continued

International Laws and Regulations		
Name	Region/ Jurisdiction	Summary
The General Data Protection Regulation (GDPR) [135]	Europe (European Union)	Applies to all European Union member states, as well as to any companies operating elsewhere that market or provide services to people in the European Union. (Prescriptive)
UK HSE Cyber Security for Industrial Automation and Control Systems [136]	Europe (United Kingdom)	Mandates requirements for achieving cybersecurity of IACS and provides the basis for inspector audits. (Prescriptive)
ITSIG 2.0 (Information Technology Security Act) [137]	Europe (Germany)	Defines mandatory formal IT security requirements for Germany based on organization categories (some of which apply to IACS). (Prescriptive)
China Security Law [138]	Asia (China)	Defines mandatory security requirements for both IT and critical infrastructure systems. (Prescriptive)
National Industrial Control System Security Standard 3.1 [139]	Middle East (Qatar)	Defines mandatory security requirements for industrial control systems in Qatar. (Prescriptive)
National Critical Information Infrastructure Protection Centre (NCIIPC) [140]	India	Defines mandatory requirements for the protection of critical information infrastructure in India. (Prescriptive)

13.1.3 Where Are Attacks, and Do They Take on a Different Character?

Cybersecurity attacks continue to occur at a steady pace each and every day; an estimated 445 million attacks occurred globally in Q1 of 2020 [141], and 59% of industrial control systems from a recent survey had experienced a cybersecurity incident in 2019 [5]. Every region experiences cybersecurity attacks, but not necessarily the same types of attacks or at the same frequency. Several factors influence how likely a region will be impacted by a cybersecurity incident such as:

- Current level of cybersecurity protection
- Attractiveness of a region to targeted attacks
- Concentration of IACS
- Types of industry in the region
- Geo-political relations

For untargeted attacks, the most important factors in determining the likelihood of an incident are related to the cybersecurity preparedness of the organization and the preparedness of the individual sites to prevent and respond to cybersecurity incidents. Several websites have been developed that provide live tracking of cybersecurity incidents, including the country of origin and destination. Although these threat maps do not provide a complete picture of all cybersecurity activities, they can be very helpful in building a clearer model of the frequency and potential variability in cybersecurity attacks [142] [143].

Targeted attacks are more significantly influenced by target attractiveness and shifting geo-political relations; this is particularly true for advanced persistent threats or nation state type attacks. One method of reviewing the likelihood for advanced persistent threats to select a region based on their previously monitored activity. A 2019 Dragos report following 11 APTs with histories of targeting IACS found that North America was the region where the highest number of groups were currently active (8/11), followed by Europe (7/11), then Asia Pacific (5/11) and the Middle East (5/11), and lastly by Africa and South America [88].

Activity alone is not enough to develop a predictive model for the most likely location of attack. Although groups may be currently showing activity in multiple regions, the primary point of focus may be specific region or even an

individual country based on their current objectives. This has been demonstrated by a number of the major event case histories in Chapter 6 that illustrate how much of an effect geo-political relations can have on the likelihood of a targeted cybersecurity event.

One challenge with trying to accurately measure and categorize where cybersecurity attacks occur is the lack of a central, trustworthy incident repository. This can make it difficult to assess the accuracy of current attack estimates and limits the actionability of threat intelligence information. As discussed in Section 9.3.1, developing a central incident repository has the potential to significantly impact the metrics and techniques used for IACS risk management.

Another challenge with trying to define cybersecurity attacks by region is the potential for a single cybersecurity event to influence many victims in many separate locations. As demonstrated by both the NotPetya cybersecurity incident [64] and the recent SolarWinds hack [26], cyberspace operates under very different rules than the physical world, and even networks in remotely located regions can become intertwined and connected.

13.2 Cybersecurity Incident Repositories

An essential step to promote further development of cybersecurity risk assessment and management techniques is improved visibility and tracking of cybersecurity incidents. The development of a comprehensive database for cybersecurity incidents would support more robust semi-quantitative and quantitative methods for evaluating cybersecurity scenarios by providing more reliable information on the likelihood of a cybersecurity attack and the effectiveness of cybersecurity protections. One ongoing effort to develop a trusted repository of cybersecurity incidents is the Cybersecurity & Infrastructure Security Agency (CISA).

CISA identified six value propositions that having an incident repository would provide [144]:

1. Identifying top risks and effective controls
2. Informing peer-to-peer benchmarking
3. Showing return on investment for cybersecurity activities

4. Allowing for sector differentiation
5. Supporting forecasting, trending, and modeling
6. Advancing risk management culture

Implementing a standardized incident data repository is not without challenges; these include ensuring anonymity, protecting data security, assuring participation, and defining the necessary fields for data collection of events. Although adoption and participation in a centralized incident repository will likely take time, it is a crucial activity for advancing IACS cybersecurity techniques. Defining the correct information to be measured and stored for each cybersecurity incident will not only lead to further developments in cybersecurity techniques or tools, but it will also enable core metrics to be developed that can be tracked over time to measure how the continually shifting environment is influencing the cybersecurity risk for a facility.

The emerging cybersecurity trends introduced in Chapter 12, such as Security Operations Centers and improved cybersecurity monitoring, have a potential to significantly aid in the effort of data collection and characterization.

13.3 Competency Requirements and Training Availability

Professional competency is a cornerstone for every cybersecurity program and is necessary for the completion of lifecycle activities. Without knowledgeable individuals, no process—regardless of how well-crafted—will lead to the desired optimal outcome. When considering the overall attack surface for industrial systems, technical upgrades are central to reducing the network and software exposure; however, minimizing human performance issues is even more important. As first introduced in Chapter 5, accidents and negligent behavior can pose serious cybersecurity risks. Mistakes by employees and contractors contribute to around 80% of all internal cybersecurity incidents [52]. To successfully implement a risk-based approach, both capable individuals and well-defined company policies need to be brought together. Chapter 11 provided the key elements of a Cybersecurity Management System (CSMS) and the necessary planning and activities to implement a holistic approach for safety and cybersecurity. The development

of cybersecurity roles and responsibilities forms the basis for successful implementation of the CSMS. This section focuses on defining the competency requirements that should be assessed and documented for each role.

Personnel can demonstrate competency in several ways, such as completing training courses, documenting experience, earning certificates, and earning certifications. For successful implementation, it is important that both general cybersecurity awareness competency is developed for all personnel with access to OT and IT networks, as well as role-specific competency development for those involved in cybersecurity lifecycle steps. Defining the competency requirements within the CSMS framework helps to provide clear instruction on the necessary activities for personnel. For general cybersecurity awareness, training and/ or workshops may be all that is required, while role-specific requirements may dictate a combination of training, relevant experience, and certification. Documentation should be maintained for both general and role-specific competency, and a time period for revalidation/ refresher training should be identified based on the type of training (e.g., every year for awareness training and every 3 years for role-specific activities).

13.3.1 Role-Based Competency Requirements

Not every role involved in the cybersecurity lifecycle requires the same areas of competency. The competency development program should be adjusted based on an organizations RACI chart to ensure that each role is capable of completing assigned activities. Several factors should be considered when assessing or justifying the knowledge and experience of facility personnel:

- What cybersecurity lifecycle activities is the role responsible for leading (e.g., network architecture design, cybersecurity risk assessment, maintaining security)?
- What cybersecurity lifecycle activities is the role involved in as a consulted party?
- Does the role need IT-specific knowledge and experience to interface with the IT security team?
- With what IACS technology does the role need to be familiar?
- Are there process safety or functional safety activities with which the role must interface?

- What actions should the role take in the event of a cybersecurity incident?
- Does the role require an understanding of the potential consequences of a cybersecurity incident on the IACS?
- Does the role need knowledge of specific cybersecurity attack methods or defense techniques?
- Are there additional legal or regulatory requirements for competency based on the organizations location/ industry?

One approach for clearly documenting competency requirements is to define competency levels and list the necessary activities per lifecycle step based on the level of involvement. In general, roles that are informed or consulted have lower competency requirements than those responsible for facilitating the lifecycle step. The highest competency requirements are necessary for roles that have the ability to define the methodology and approach used for lifecycle activities. Listing requirements per step and the associated competency level helps to remove uncertainty in the required competency level and allow for easy tracking. An example of the competency requirements for the Cybersecurity Risk Assessment Activity is shown in Table 13-2.

Table 13-2 Cybersecurity Competency Requirements Example

Step	Competency Requirements	Competency Components
Cybersecurity Risk Assessment	(Consulted) Can participate as a member of the risk assessment team.	(Consulted) Understands cybersecurity risk assessment principles, where hazards can be introduced, and has attended relevant training
	(Responsible) Can lead risk assessment and generate output report.	(Responsible) Has experience participating in cybersecurity risk assessments and has led a cybersecurity risk assessment under supervision. Knowledgeable of the tools and methodology to be used in the assessment and has at least five years of relevant experience and professional competency certification or equivalent.
	(Expert) Can define new risk assessment approach and policies to follow.	(Expert) Has detailed experience with risk assessment techniques and risk assessment requirements from industry best practices and regulatory requirements, has led multiple risk assessments and has at least ten years of relevant experience and professional competency certification or equivalent.

13.3.2 Certification – What is Available?

Two common methods of documenting professional competency are certificate and certification programs. Although the names are very similar, distinct differences between the approaches are shown in Table 13-3.

Table 13-3 Certification or Certificate

Certificate	Certification
Results from an educational process.	Results from an assessment process that recognizes an individual's knowledge, skills, and competency in a particular specialty.
For newcomers and experienced professionals.	Typically requires professional experience.
Awarded by educational programs or institutions often for-profit (commercial).	Awarded by a third-party or standard-setting organization, typically not for profit.
Indicates completion of a course or series of courses with a specific focus (different than a degree-granting program).	Indicates mastery/ competency as measured against a defensible set of standards, usually by application or exam.
Course content determined by the specific provider or institution, not standardized.	Standards set through a defensible, industry-wide process (job analysis/ role delineation) that results in an outline of required knowledge and skills.
Usually listed on a resume detailing education.	Often results in credentials to be listed after one's name.
Demonstrates knowledge of course content at the end of a set period of time.	Has on-going requirements in order to maintain; holder must demonstrate he/ she continues to meet requirements.

Many competency programs specific to IT cybersecurity are available, but fewer options are available for industrial cybersecurity. In some cases, IT cybersecurity certifications can still be useful for industrial applications, particularly when paired with industrial control system training. Various certificate and certification programs for industrial cybersecurity training courses relating to the automation lifecycle, system integration, SCADA, and the secure development lifecycle are available [145] [146] [147] [148] [149] [150] [151] [152].

When considering certificate or competency requirements, it is important to ensure that all roles involved with the lifecycle have the appropriate level of competency. This requirement goes beyond internal stakeholders with cybersecurity responsibilities and also includes any contractors, vendors, or equipment suppliers that are involved the cybersecurity lifecycle. Facility operators should also define minimum competency requirements for external stakeholders, such as cybersecurity development certificates/ certification or appropriate experience and training. Only by ensuring competent personnel are involved at each stage of the lifecycle can successful implementation be achieved.

13.4 *Administration vs. Accountability Functions*

The rise of cybersecurity incidents has also led to important questions about which roles are responsible for ensuring that adequate cybersecurity protections are in place. While this question has no single answer, it is important to consider both the roles that are responsible for implementing and administering cybersecurity as well as the senior management roles responsible for assigning funding and having ownership for plant operations.

Although much of this book has focused on the specific technical details and strategies that should be considered by the roles implementing and administering cybersecurity, the importance of senior management support cannot be overstated. Senior management support is essential for establishing a mature cybersecurity culture and driving the direction of the organization with respect to cybersecurity.

In particular, senior management should understand:

- Why does cybersecurity affect multiple groups?
- What needs to be done to support effective implementation and ensure that cybersecurity isn't unintentionally undermined?

IACS cybersecurity is a complex issue that requires collaboration between many groups to be effectively achieved. The corporate IT group, OT team, process safety team, operations team, and HR department are just some of the groups needed to implement IACS cybersecurity. It is important for management to understand the necessary interactions between these groups and provide the support and guidance to help these groups communicate effectively together. A failure to understand the criticality of communications between these groups could lead to unclear guidance on the selected cybersecurity strategy.

In addition to supporting the collaboration of multiple groups, it is important for senior management to be aware of the potential pitfalls in IACS cybersecurity implementation. Just as seemingly small changes in process safety can significantly reduce the achieved safety of a system, the failure to secure remote access or provide adequate cybersecurity hygiene training could de-rail an otherwise successful cybersecurity program. It is critical for management to appreciate the need for continuous investment in cybersecurity when reviewing funding allocation; just because an incident has not occurred yet does not mean that a company has no risk of cybersecurity incidents.

Senior management adoption of the Risk Based Process Safety (RBPS) framework for cybersecurity can also help to provide a consistent rubric for decision making. Establishing clear commitment to cybersecurity, developing a detailed understanding of cybersecurity hazards and risks, taking effective steps to manage the cybersecurity risk, and learning from experience are all key steps in effectively implementing cybersecurity for all affected groups of the organization.

13.5 Summary

As cybersecurity continues to evolve, taking advantage of available resources becomes increasingly important to maintain adequate protection. Understanding the factors that drive adoption of cybersecurity practices, such as legal, moral, and financial responsibility, help to provide a clearer understanding of how cybersecurity implementation may differ by region. Available resources, such as shared risk profiles, industry references, and cybersecurity threat intelligence, help each organization to tailor their risk management approach. The development of a reliable repository for industrial cybersecurity incident data will be an important step in supporting the further development and optimization of cybersecurity analysis techniques. Cybersecurity competency is integral to the successful implementation and maintenance of a secure system, and a number of currently available training, certificate, and certification programs are available to improve cybersecurity competency within an organization. It is essential to define all roles involved in the administration or accountability of cybersecurity activities and provide training so that personnel are aware of their responsibilities to manage industrial cybersecurity risk.

Appendix A Excerpt from NIST Cybersecurity Framework

The NIST Cybersecurity Framework has five functions each containing multiple categories [11]. Within each category, subcategories are used to further segment the requirements and describe specific activities and performance criteria related to the category and function. The framework also provides industry references for each subcategory, where more detailed information can be found that an end user might find useful when developing their management systems [11]. An example of the framework structure and taxonomy for one category in each of the NIST Cybersecurity Framework functions is provided in Table A-1 to give a clearer picture of the framework structure.

Table A-1 Example NIST Framework Structure

Function	Category	Subcategory	Cross References
Identify (ID)	Risk Management (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.	CIS CSC: 4 [153] COBIT 5: APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 [154] ISA 62443-2-1: 4.3.4.2 [12] ISO/IEC 27001: Clause 6.1.3, Clause 8.3, Clause 9.3 [131] NIST SP 800-53: PM-9 [155]
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed.	COBIT 5: APO12.06 [153] ISA 62443-2-1: 4.3.2.6.5 [12] ISO/IEC 27001: Clause 6.1.3, Clause 8.3 [131] NIST SP 800-53: PM-9 [155]
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.	COBIT 5: APO12.02 [153] ISO/IEC 27001: Clause 6.1.3, Clause 8.3 [131] NIST SP 800-53: SA-14, PM-8, PM-9, PM-11 [155]

Table A-1 continued

Function	Category	Subcategory	References
Protect (PR)	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	COBIT 5: BAI03.10, BAI09.02, BAI09.03, DSS01.05 [153] ISA 62443-2-1: 4.3.3.3.7 [12] ISO/IEC 27001: A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 [131] NIST SP 800-53: MA-2, MA-3, MA-5, MA-6 [155]
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a way that prevents unauthorized access.	CIS CSC: 3, 5 COBIT 5: DSS05.04 [153] ISA 62443-2-1: 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 [12] ISO/IEC 27001: A.11.2.4, A.15.1.1, A.15.2.1 [131] NIST SP 800-53: MA-4 [155]

Table A-1 continued

Function	Category	Subcategory	References
Detect (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	CIS CSC: 1, 4, 6, 12, 13, 15, 16 COBIT 5: DSS03.01 [153] ISA 62443-2-1: 4.4.3.3 [12] ISO/IEC 27001: A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 [131] NIST SP 800-53: AC-4, CA-3, CM-2, SI-4 [155]
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	CIS CSC: 3, 6, 13, 15 COBIT 5: DSS05.07 [153] ISA 62443-2-1: 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 [12] ISA 62443-3-3: SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 [81] ISO/IEC 27001: A.12.4.1, A.16.1.1, A.16.1.4 [131] NIST SP 800-53: AU-6, CA-7, IR-4, SI-4 [155]

Table A-1 continued

Function	Category	Subcategory	References
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	CIS CSC: 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 COBIT 5: BAI08.02 [153] ISA 62443-3-3: SR 6.1 ISO/IEC 27001: A.12.4.1, A.16.1.7 [81] NIST SP 800-53: AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 [155]
		DE.AE-4: Impact of events is determined.	CIS CSC: 4, 6 COBIT 5: APO12.06, DSS03.01 [153] ISO/IEC 27001: A.16.1.4 [131] NIST SP 800-53: CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Incident alert thresholds are established.	CIS CSC: 6, 19 COBIT 5: APO12.06, DSS03.01 [153] ISA 62443-2-1: 4.2.3.10 [12] ISO/IEC 27001: A.16.1.4 [131] NIST SP 800-53: IR-4, IR-5, IR-8 [155]

Table A-1 continued

Function	Category	Subcategory	References
Response (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	RS.RP-1: Response plan is executed during or after an incident.	CIS CSC: 19 COBIT 5: APO12.06, BAI01.10 [153] ISA 62443-2-1: 4.3.4.5.1 [12] ISO/IEC 27001: A.16.1.5 [131] NIST SP 800-53: CP-2, CP-10, IR-4, IR-8 [155]
Recover (RC)	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	RC.IM-1: Recovery plans incorporate lessons learned.	COBIT 5: APO12.06, BAI05.07, DSS04.08 [153] ISA 62443-2-1: 4.4.3.4 [12] ISO/IEC 27001: A.16.1.6, Clause 10 [131] NIST SP 800-53: CP-2, IR-4, IR-8 [155]
		RC.IM-2: Recovery strategies are updated.	COBIT 5: APO12.06, BAI07.08 [153] ISO/IEC 27001: A.16.1.6, Clause 10 [131] NIST SP 800-53: CP-2, IR-4, IR-8 [155]

Source: NIST Cybersecurity Framework [11]

Appendix B Detailed Cybersecurity PHA and LOPA Example

An overview of qualitative and quantitative methods for cybersecurity hazard identification and risk analysis are provided in Chapter 9. In this appendix, a detailed example is developed for an isomerization system (defined in Section B.1). For this example, the following steps will be completed:

- Initial Risk Assessment (B.2)
- Detailed Risk Assessment/ Cybersecurity HAZOP (B.3)
- LOPA/ Semi-Quantitative SL Verification (B.4)

B.1 System Basis

The following example for a simplified isomerization unit is used for the detailed example. Isomerization is the conversion of a chemical from one molecular structure to another, without changing the molecular formula. Examples include changing from a straight-chain to a branched-chain hydrocarbon, such as butane to isobutane (both C_4H_{10}), or an alicyclic to an aromatic hydrocarbon [1]. Isomerization is a common process in the oil and gas and petrochemical industries, with over 200 isomerization units worldwide and a total processing capacity of more than 1.5 million barrels per day of light paraffins [156]. The higher-octane value of branched paraffins (over straight paraffins) makes this an important step in the production of gasoline. Isomerization is limited by a temperature-dependent thermal equilibrium, and a number of catalysts can be used to improve the equilibrium level [156]. A simplified process flow diagram for an Isomerization process flow diagram is shown in Figure B-1.

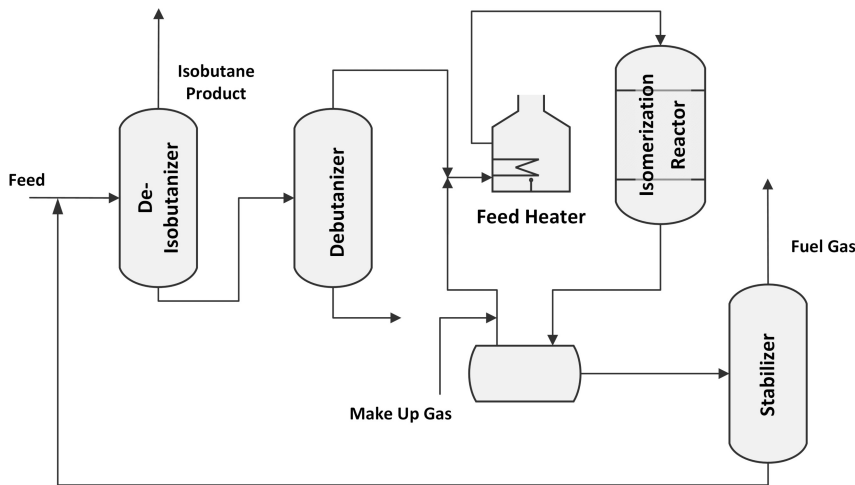


Figure B-1 Simplified Isomerization Process Flow Diagram

Due to the presence of high pressures and flammable hydrocarbons, the rupture of an isomerization reactor due to an overpressure could result in a significant process safety hazard with the potential for fatalities. Although the specific unit targeted in the Saudi petrochemical facility is not known, it is possible that an isomerization unit or other similar unit was the focus of the attack [10]. A simplified network architecture for the isomerization unit is shown in Figure B-2.

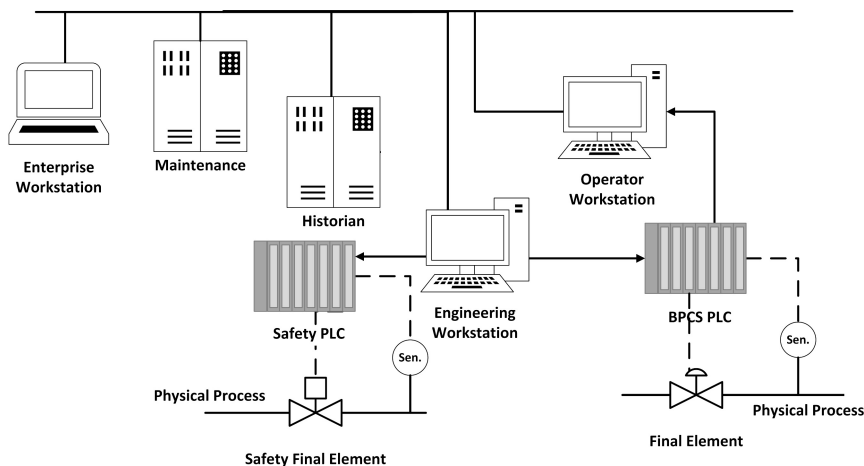


Figure B-2 Simplified Network Architecture

The risk criteria for use in the detailed example are included in Table B-1, Table B-2, Table B-3, and Table B-4. These tables will be referenced in the subsequent sections when completing likelihood or consequence severity rankings.

Table B-1 Example Severity Matrix

Severity Level	Severity		
	Business	Environment	Safety
1	Compromise resulting in negligible impact. (Less than \$50K)	Compromise resulting in negligible impact.	Compromise resulting in negligible impact.
2	Interruption of authorized user access resulting in minor business consequence. (\$50K to \$1M)	Interruption of authorized user access resulting in minor environmental impact.	Interruption of authorized user access resulting in minor safety impact.
3	Critical information stolen or locked from authorized users with moderate business consequence. (\$1M-\$25M)	PC affected resulting in temporary release and cleanup within weeks.	PC affected resulting in recordable injury.
4	Significant business consequence. (\$25M-\$100M)	Temporary damage to the environment and cleanup with months to a few years.	Single on-site fatality.
5	Severe business consequence. (Greater than \$100M)	Severe damage to the environment, cleanup greater than a decade.	Multiple on-site fatalities.

Table B-2 Example Likelihood Matrix

Level	Likelihood
	L
VL	Very low (Typically only considered after countermeasures), 10 ⁻³ per year or less
L	Low (Nation State), 10 ⁻² per year
M	Medium (Targeted Attack-Skilled), 10 ⁻¹ per year
H	High (Targeted Attack-Unskilled), 1 per year
VH	Very High (Internal Unintentional, Non-targeted), 10 or more times per year

Table B-3 Example Corporate Risk Matrix

Risk Matrix		Severity Level				
		1	2	3	4	5
Likelihood	Very High	5	9	12	13	16
	High	4	8	9	12	13
	Medium	4	5	8	9	12
	Low	1	4	5	8	9
	Very Low	1	1	4	5	8

Table B-4 Risk Ranking to Security Level Target

Risk Ranking	Security Level
Minimal (1-4)	Security Level 1
Moderate (5-8)	Security Level 2
Significant (9-12)	Security Level 3
Severe (13-16)	Security Level 4

B.2 Initial Risk Assessment

Step 1: Identify System Under Configuration

For this example, the System Under Consideration (SUC) includes the isomerization unit and all computer-based or programmable elements from the network architecture. The scope boundaries of the SUC are identified in Figure B-3.

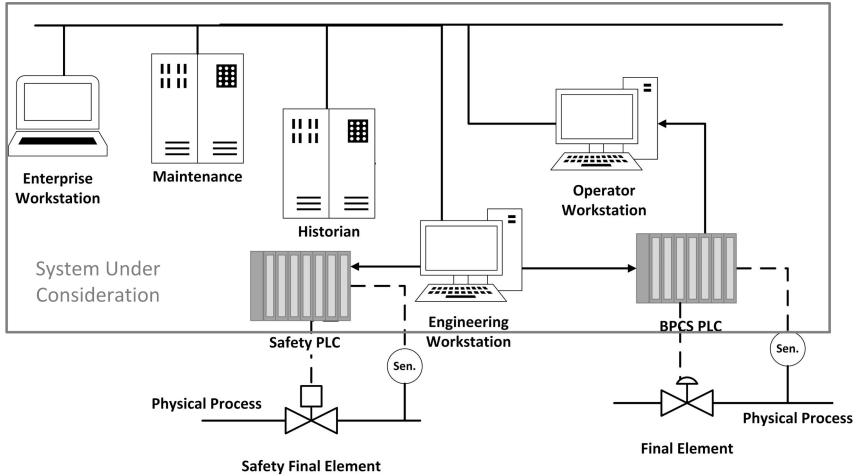


Figure B-3 Identification of System Under Consideration

Step 2: Select Device

After defining the SUC, each device under consideration is selected one at a time to complete Steps 3-6. For this example, the engineering workstation is selected as the first device as shown in Figure B-4.

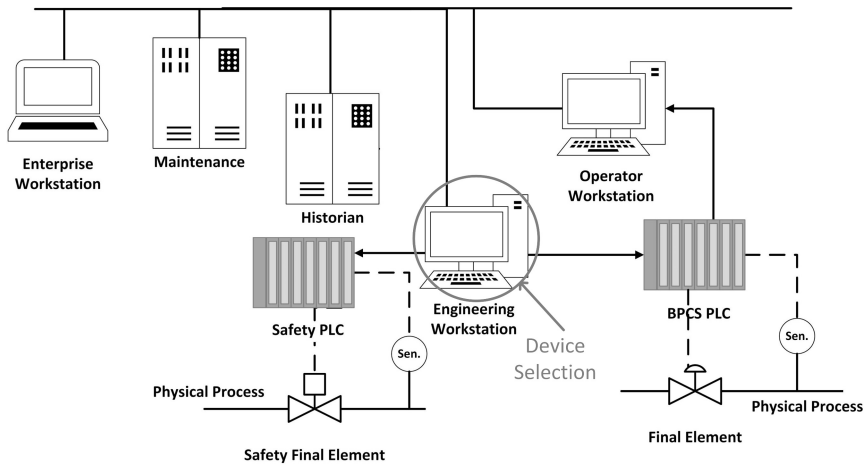


Figure B-4 Device Selection

Step 3: Identify and Record Worst-Case Consequence

The worst-case consequence is then defined for the engineering workstation the following consequence can be defined:

- Compromise of the engineering workstation leading to the potential compromise of both the basic process control and safety PLCs. leading to the potential to initiate a failure of the pressure control system and the failure of multiple protection layers including a high-pressure alarm and high-pressure safety interlock. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.

Step 4: Determine and Record the Qualitative Severity of Consequences

The worst-case consequence scenario described corresponds to a consequence severity of 5 for “safety” based on the risk criteria from Table B-1 as shown in Figure B-5.

Severity Level	Severity		
	Business	Environment	Safety
1	Compromise resulting in negligible impact. (Less than \$50K)	Compromise resulting in negligible impact.	Compromise resulting in negligible impact.
2	Interruption of authorized user access resulting in minor business consequence. (\$50K to \$1M)	Interruption of authorized user access resulting in minor environmental impact.	Interruption of authorized user access resulting in minor safety impact.
3	Critical information stolen or locked from authorized users with moderate business consequence. (\$1M-\$25M)	PC affected resulting in temporary release and cleanup within weeks.	PC affected resulting in recordable injury.
4	Significant business consequence. (\$25M-\$100M)	Temporary damage to the environment and cleanup with months to a few years.	Single on-site fatality.
5	Severe business consequence. (Greater than \$100M)	Severe damage to the environment, cleanup greater than a decade.	Multiple on-site fatalities.

Figure B-5 Consequence Severity Ranking

Step 5: Determine the Initial Security Target Level

After ranking the consequence severity, the initial security level target is determined considering a threat likelihood of 1. Based on the example likelihood matrix in Table B-2, a threat likelihood of 1 corresponds to the “high” likelihood ranking as shown in Figure B-6.

Level	Likelihood
	L
VL	Very low (Typically only considered after countermeasures), 10 ⁻³ per year or less
L	Low (Nation State), 10 ⁻² per year
M	Medium (Targeted Attack-Skilled), 10 ⁻¹ per year
H	High (Targeted Attack-Unskilled), 1 per year
VH	Very High (Internal Unintentional, Non-targeted), 10 or more times per year

Figure B-6 Likelihood Ranking

With the severity and likelihood rankings known, the initial risk level can be determined using the risk matrix in Table B-3 as shown in Figure B-7. A consequence severity of “5” and likelihood of “high” would correspond to a risk score of 13.

Risk Matrix		Severity Level				
		1	2	3	4	5
Likelihood	Very High	5	9	12	13	16
	High	4	8	9	12	13
	Medium	4	5	8	9	12
	Low	1	4	5	8	9
	Very Low	1	1	4	5	8

Figure B-7 Initial Risk Ranking

The final step is to correlate the risk level to the appropriate security level using Table B-4. For a scenario with a risk score of “13”, this would correlate to a Security Level 4 target as shown in Figure B-8.

Risk Ranking	Security Level
Minimal (1-4)	Security Level 1
Moderate (5-8)	Security Level 2
Significant (9-12)	Security Level 3
Severe (13-16)	Security Level 4

Figure B-8 Security Level Target

Step 6: Determine if the Tolerable Risk Criteria are Met

The risk for a compromise of the engineering workstation was determined to be severe. As a result, further risk mitigations would be necessary and a detailed risk assessment for the zone containing the engineering workstation would be required. Steps 3-6 should then be repeated for each device in the system under consideration. The outcome for each device is shown in Figure B-9.

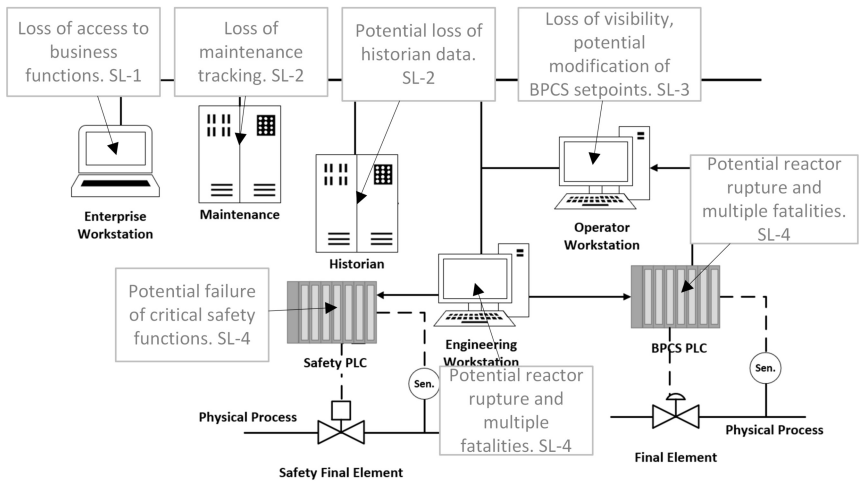


Figure B-9 Initial Risk Assessment Results

The initial security level targets can then be used to update the network segmentation strategy, by grouping devices with similar security requirements into zones. Often combining network segmentation techniques from Chapter 8, with risk-based targets from the initial risk assessment can drive an optimal strategy. Each zone is then given its own security level target based on the highest consequence device within the zone. Conduits or the connections between zones (including boundary devices such as firewalls) are given the same security level target of the highest security zone they are connected to. For example, if a firewall is used to separate a SL-2 zone from an SL-3 zone, the firewall would be given an SL-3 target. Following the addition of network segmentation between the IT and IACS zones as well as between the safety and control zones, the network architecture for the isomerization example is shown in Figure B-10.

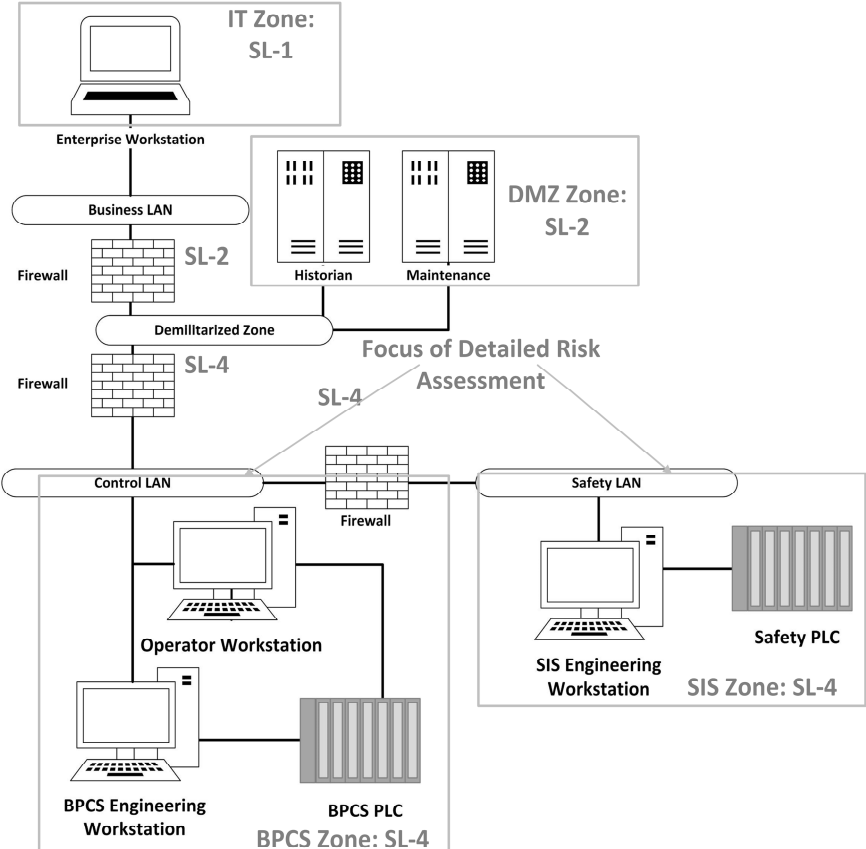


Figure B-10 Updated Zone and Conduit Diagram

The focus of the detailed risk assessment is then narrowed to zones that exceed the corporate risk criteria. In this example, these zones would be the BPCS zone and the SIS zone.

B.3 Detailed Risk Assessment (Cyber PHA/HAZOP)

Step 1: Select the Zone or Conduit

The first step in the detailed risk assessment is to identify which zone will be evaluated first. For this example, the BPCS zone from Figure B-11 will be identified as the focus for the study.

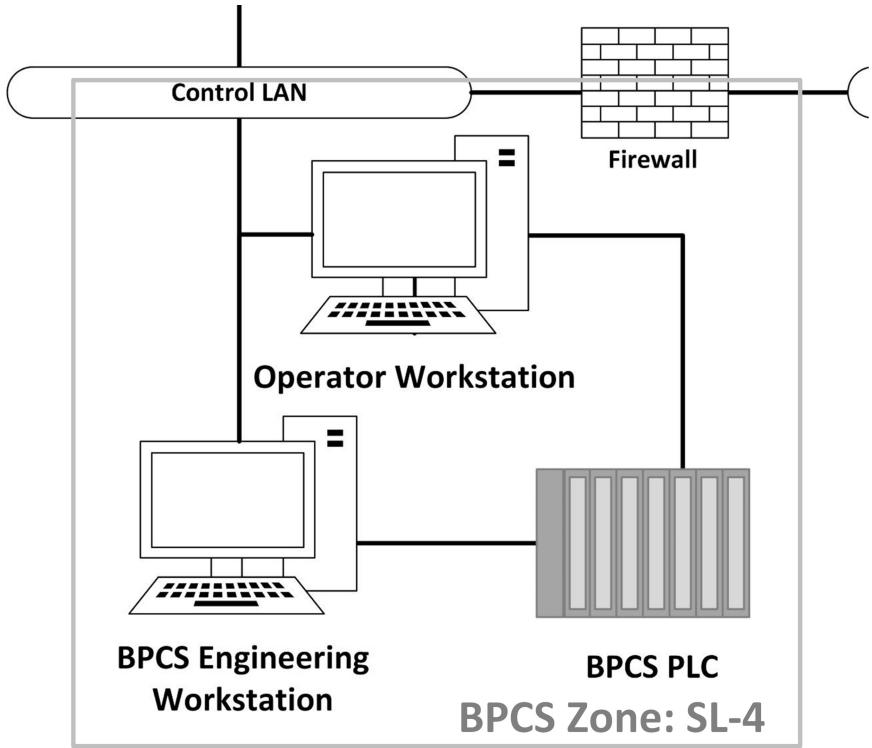


Figure B-11 BPCS Zone for Detailed Risk Assessment

Step 2: Select the Cyber Node

Once the zone is defined, the cybernode for review is selected. Often, each unique asset within the zone is defined as a node. The BPCS zone would consist of three nodes:

- BPCS Engineering Workstation
- BPCS PLC
- Operator Workstation

For this example, the BPCS engineering workstation will be the first node for review.

Step 3: Select the Threat Vector

After selecting the node for review, the threat vectors should be specified. Instead of using a list of hundreds of possible threat vectors, a list of relevant threat vector categories often drives a more efficient and effective study. For this example, the following six threat vectors will be used:

- Social Engineering (e.g., phishing, spear phishing)
- Communications (e.g., denial of service, man-in-the-middle)
- Supply Chain (e.g., compromise of service provider)
- Physical Access (e.g., logging onto an unguarded workstation)
- Software (e.g., exploiting a known software vulnerability)
- Hardware (e.g., connecting a USB to an unsecured port)

Cybersecurity risk assessment tools which support the use of “smart deviations” to populate automatically scenarios with pre-configured deviations are commercially available.

Step 4: Identify and Record the Threats

For each threat vector, specific threats should be identified that could lead to the compromise of the cybersecurity node. It is possible to have multiple threats defined per threat vector, depending on the node and the level of detail desired for the assessment. One example threat is defined for each threat vector to provide examples on this process in Table B-5.

Step 5: Identify the Vulnerabilities

The results of a Cybersecurity Vulnerability Analysis (CVA), following the approach defined in Section 9.2.4, is an important input to the cybersecurity HAZOP. Findings from the CVA can impact the types of threats identified and can, in some cases, impact the expected threat likelihood for different types of attacks as well. A CVA finding such as an improperly configured boundary device, known vulnerability in an application, or enabled web server (such as the example threat definition for the software threat vector) should be identified as part of the cybersecurity hazard identification process. Additionally, information such as the number of personnel with administrative and engineering accounts to the IACS will have an impact on how likely it is than an account with access may be compromised.

Table B-5 Threat Definition Examples

Threat Vector	Detailed Threat Definition Example
Social Engineering	Phishing campaign from skilled attacker results in compromised administrator BPCS Engineering Workstation credentials.
Communications	A targeted attack (unskilled) blocks network communication between BPCS and SIS zones.
Supply Chain	A remote backdoor is installed in the BPCS Engineering Workstation during manufacturing from a nation state level attack.
Physical Access	A contractor (unknowingly) attempts to insert ransomware infected equipment to the BPCS Engineering Workstation.
Software	A web server is enabled for the BPCS engineering workstation following a system upgrade, making the system vulnerable to unskilled attackers.
Hardware	A skilled attacker tries to gain access to the BPCS Engineering Workstation using a hardwired connection from a compromised business asset.

Step 6: Record the Qualitative Thread Likelihood

The likelihood of the threats should then be determined considering the level of skill required to execute that type of attack. Generally, the higher the level of skill and specificity required, the lower the likelihood of the attack. It is generally useful to define the correlation between different types of threat agents and an organization's likelihood matrix prior to completing the cybersecurity HAZOP. The likelihood levels defined in Table B-2 explicitly include references to the skill level of the threat and can be used to estimate the likelihood of each threat as shown in Table B-6.

Table B-6 Threat Definition Examples and Likelihoods

Threat Vector	Detailed Threat Definition Example	Likelihood (L)
Social Engineering	Phishing campaign from skilled attacker results in compromised administrator BPCS Engineering Workstation credentials.	Medium (M)
Communications	A targeted attack (unskilled) blocks network communication between BPCS and SIS zones.	High (H)
Supply Chain	A remote backdoor is installed in the BPCS Engineering Workstation during manufacturing from a nation state level attack.	Low (L)
Physical Access	A contractor (unknowingly) attempts to insert ransomware infected equipment to the BPCS Engineering Workstation.	Very High (VH)
Software	A web server is enabled for the BPCS engineering workstation following a system upgrade, making the system vulnerable to unskilled attackers .	High (H)
Hardware	A skilled attacker tries to gain access to the BPCS Engineering Workstation using a hardwired connection from a compromised business asset.	Medium (M)

Step 7: Determine the Worst-Case Consequence (without Countermeasures)

The worst-case consequence is then defined for each threat to the BPCS Engineering Workstation. For threats that can lead to a complete compromise of the BPCS engineering workstation the worst-case consequence from the initial risk assessment can often be considered. For some threats, the consequence may only be financial or environmental in nature and would need to be reviewed. Considering the updates to the network architecture the worst-case consequence can be re-written as follows:

- Compromise of the BPCS engineering workstation leading to the potential compromise of the basic process control PLC. leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.

Although the safety PLC is not directly communicated with from the BPCS Engineering Workstation, no countermeasures are credited when defining the worst-case consequence. The consequences of the cybersecurity threats identified in step 4 are shown in Table B-7.

Step 8: Determine and Record the Qualitative Severity of Consequences

Next the severity should be determined for each consequence considering all affected risk receptor categories. The consequence severity and categories are shown in Table B-8.

Table B-7 Consequence Definition per Threat

Threat Vector	Detailed Threat Definition Example	L	Consequence
Social Engineering	Phishing campaign from skilled attacker results in compromised administrator BPCS Engineering Workstation credentials.	M	Compromise of the BPCS engineering workstation leading to the potential compromise of the basic process control PLC, leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.
Communications (Comms)	A targeted attack (unskilled) blocks network communication between BPCS and SIS zones.	H	Loss of Communication between the BPCS and SIS zones. Loss of information from SIS controller/ engineering workstation to BPCS engineering workstation and operator workstation, loss of visual of safety system, negligible impact
Supply Chain	A remote backdoor is installed in the BPCS Engineering Workstation during manufacturing from a nation state level attack.	L	Compromise of the BPCS engineering workstation leading to the potential compromise of the basic process control PLC, leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.
Physical Access	A contractor (unknowingly) attempts to insert ransomware infected equipment to the BPCS Engineering Workstation.	VH	Inability to access BPCS Application program, potential business impact, due to cost of replacing BPCS engineering workstation and application program, or potential for spurious trip and unexpected downtime.
Software	A web server is enabled for the BPCS engineering workstation following a system upgrade, making the system vulnerable to unskilled attackers.	H	Compromise of the BPCS engineering workstation leading to the potential compromise of the basic process control PLC, leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.
Hardware	A skilled attacker tries to gain access to the BPCS Engineering Workstation using a hardwired connection from a compromised business asset.	M	Compromise of the BPCS engineering workstation leading to the potential compromise of the basic process control PLC, leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.

Table B-8 Consequence and Severity Definition per Threat

Threat Vector	Detailed Threat Definition Example	L	Consequence	Category (Cat.)	Severity (Sev.)
Social Engineering	Phishing campaign from skilled attacker results in compromised administrator BPCS Engineering Workstation credentials.	M	Compromise of the BPCS engineering workstation leading to the potential compromise of the basic process control PLC. leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.	Safety (S)	5
Communications (Comms)	A targeted attack (unskilled) blocks network communication between BPCS and SIS zones.	H	Loss of Communication between the BPCS and SIS zones. Loss of information from SIS controller/ engineering workstation to BPCS engineering workstation and operator workstation, loss of visual of safety system, negligible impact	Business (B)	1
Supply Chain	A remote backdoor is installed in the BPCS Engineering Workstation during manufacturing from a nation state level attack.	L	Compromise of the BPCS engineering workstation leading to the potential compromise of the basic process control PLC. leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.	Safety (S)	5
Physical Access	A contractor (unknowingly) attempts to insert ransomware infected equipment to the BPCS Engineering Workstation.	VH	Inability to access BPCS Application program, potential business impact, due to cost of replacing BPCS engineering workstation and application program, or potential for spurious trip and unexpected downtime.	Business (B)	2
Software	A web server is enabled for the BPCS engineering workstation following a system upgrade, making the system vulnerable to unskilled attackers.	H	Compromise of the BPCS engineering workstation leading to the potential compromise of the basic process control PLC. leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.	Safety (S)	5

Table B-8 continued

Threat Vector	Detailed Threat Definition Example	L	Consequence	Category (Cat.)	Severity (Sev.)
Hardware	A skilled attacker tries to gain access to the BPCS Engineering Workstation using a hardwired connection from a compromised business asset.	M	Compromise of the BPCS engineering workstation leading to the potential compromise of the basic process control PLC, leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.	Safety (S)	5

Step 9: Determine the Security Level Target

The security level target can be reviewed and updated for each threat based on the unmitigated likelihood. For the social engineering example, because the likelihood of a targeted attack leading to the consequence is medium the target in this case, the risk score would drop to 12 (as shown in Figure B-12) and the correlated security level would be SL-3 (as shown in Figure B-13).

Risk Matrix		Severity Level				
		1	2	3	4	5
Likelihood	Very High	5	9	12	13	15
	High	4	8	9	12	13
	Medium	4	5	8	9	12
	Low	1	4	5	8	9
	Very Low	1	1	4	5	8

Figure B-12 Updated Risk Ranking

Risk Ranking	Security Level
Minimal (1-4)	Security Level 1
Moderate (5-8)	Security Level 2
Significant (9-12)	Security Level 3
Severe (13-16)	Security Level 4

Figure B-13 Updated Security Level Target

Step 10: Identify and Record the Countermeasures

After defining the worst-case consequence countermeasures that can reduce the likelihood of the ultimate attack being successful or help mitigate the consequence severity can be considered. Each countermeasure identified should be reviewed to ensure that it is applicable to a given threat scenario. The following potential countermeasures were determined for the example system:

- Restrict access to only required personnel (3 automation and controls engineers) who each have their own individual access account. Access is reviewed on a yearly basis.
- The BPCS engineering workstation is kept in a locked cabinet that only required personnel may access.
- A firewall has been installed between the DMZ Zone and the BPCS zone.
- The Application Program for the BPCS PLC is reviewed yearly to identify if any unapproved changes have been made.

- A pressure relief valve is located on the isomerization reactor and is sized for the pressure control failure case.
- These countermeasures have been applied where appropriate for the threat scenarios in Table B-9.

Table B-9 Cybersecurity HAZOP Worksheet with Countermeasures

Threat Vector	Threat	L	Consequence	Cat.	Sev.	Risk	Countermeasures
Social Engineering	Phishing campaign from skilled attacker results in compromised administrator BPCS Engineering Workstation credentials.	M	Compromise of the BPCS engineering workstation leading to the potential compromise of the basic process control PLC, leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.	S	5	12	Restrict access to only required personnel (3 automation and controls engineers) who each have their own individual access account. Access is reviewed on a yearly basis.; A firewall has been installed between the DMZ Zone and the BPCS zone.; The Application Program for the BPCS PLC is reviewed yearly to identify if any unapproved changes have been made.; A pressure relief valve is located on the isomerization reactor and is sized for the pressure control failure case
Comms	A targeted attack (unskilled) blocks network communication between BPCS and SIS zones.	H	Loss of Communication between the BPCS and SIS zones. Loss of information from SIS controller/ engineering workstation to BPCS engineering workstation and operator workstation, loss of visual of safety system, negligible impact	B	1	4	None
Supply Chain	A remote backdoor is installed in the BPCS Engineering Workstation during manufacturing from a nation state level attack.	L	Compromise of the BPCS engineering workstation leading to the potential compromise of the basic process control PLC, leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.	S	5	9	The Application Program for the BPCS PLC is reviewed yearly to identify if any unapproved changes have been made.; A pressure relief valve is located on the isomerization reactor and is sized for the pressure control failure case

Table B-9 continued

Threat Vector	Threat	L	Consequence	Cat.	Sev.	Risk	Countermeasures
Physical Access	A contractor (unknowingly) attempts to insert ransomware infected equipment to the BPCS Engineering Workstation.	V H	Inability to access BPCS Application program, potential business impact, due to cost of replacing BPCS engineering workstation and application program, or potential for spurious trip and unexpected downtime.	B	2	9	Restrict access to only required personnel (3 automation and controls engineers) who each have their own individual access account. Access is reviewed on a yearly basis; The BPCS engineering workstation is kept in a locked cabinet that only required personnel may access.
Software	A web server is enabled for the BPCS engineering workstation following a system upgrade, making the system vulnerable to unskilled attackers.	H	Compromise of the BPCS engineering workstation leading to the potential compromise of the basic process control PLC. leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.	S	5	13	Restrict access to only required personnel (3 automation and controls engineers) who each have their own individual access account. Access is reviewed on a yearly basis; The BPCS engineering workstation is kept in a locked cabinet that only required personnel may access.
Hardware	A skilled attacker tries to gain access to the BPCS Engineering Workstation using a hardwired connection from a compromised business asset.	M	Compromise of the BPCS engineering workstation leading to the potential compromise of the basic process control PLC. leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.	S	5	12	Restrict access to only required personnel (3 automation and controls engineers) who each have their own individual access account. Access is reviewed on a yearly basis; A firewall has been installed between the DMZ Zone and the BPCS zone; The Application Program for the BPCS PLC is reviewed yearly to identify if any unapproved changes have been made; A pressure relief valve is located on the isomerization reactor and is sized for the pressure control failure case

Step 11: Determine the Likelihood with Countermeasures

The likelihood can then be determined considering the effectiveness of the identified countermeasures. Depending on the type of countermeasure (active or passive) different levels of credit can be considered. The number of steps the likelihood level can be reduced for each countermeasure is shown in Table B-10.

Table B-10 Countermeasure Effectiveness

Countermeasure	Reduction in Likelihood Level
Restrict access to only required personnel (3 automation and controls engineers) who each have their own individual access account. Access is reviewed on a yearly basis.	One likelihood level.
The BPCS engineering workstation is kept in a locked cabinet that only required personnel may access.	One likelihood level.
A firewall has been installed between the DMZ Zone and the BPCS zone.	One likelihood level.
The Application Program for the BPCS PLC is reviewed yearly to identify if any unapproved changes have been made.	Half of a likelihood level.
A pressure relief valve is located on the isomerization reactor and is sized for the pressure control failure case.	Two likelihood levels.

Using the information in Table B-10, the likelihood of a cybersecurity attack with countermeasures can be estimated. An example of determining the likelihood and risk reduction for the threat of an unskilled attacker compromising the system through an enabled web server is shown in Figure B-14. The access control countermeasure reduces the likelihood one level from high to medium, and the pressure relief valve reduces the likelihood two levels, from medium to very low.

Risk Matrix		Severity Level				
		1	2	3	4	5
Access Control Pressure Relief Valve	Very High	5	9	12	13	16
	High	4	8	9	12	13
	Medium	4	5	8	9	12
	Low	1	4	5	8	9
	Very Low	1	1	4	5	8
Likelihood with Countermeasures		Risk with Countermeasures				

Figure B-14 Likelihood with Countermeasures

Step 12: Determine if the Tolerable Risk Criteria are Met

The final step is to review the risk with countermeasures and determine if any scenarios exceed the corporate risk criteria. Recommendations can be made to provide additional countermeasures or take other actions to reduce risk to acceptable levels. In some cases, where a better understanding of the scenario is desired, a quantitative approach can be used. The complete results of the Cybersecurity HAZOP for the selected threats are shown in Table B-11.

Table B-11 Completed Cybersecurity HAZOP Worksheet

Threat Vector	Threat	L	Consequence	Cat.	Sev.	Risk	Countermeasures (CMR)	L with CMR	Risk with CMR
Social Engineering	Phishing campaign from skilled attacker results in compromised administrator BPCS Engineering Workstation credentials.	M	Compromise of the BPCS engineering workstation resulting in the potential compromise of the basic process control PLC, leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.	S	5	12	Restrict access to only required personnel (3 automation and controls engineers) who each have their own individual access account. Access is reviewed on a yearly basis.; A firewall has been installed between the DMZ Zone and the BPCS zone.; The Application Program for the BPCS PLC is reviewed yearly to identify if any unapproved changes have been made.; A pressure relief valve is located on the isomerization reactor and is sized for the pressure control failure case.	VL	8
Comms	A targeted attack (unskilled) blocks network communication between BPCS and SIS zones.	H	Loss of communication between the BPCS and SIS zones, leading to a loss of information from the SIS controller/ engineering workstation to the BPCS engineering workstation and operator workstation and loss of visual of safety system, with negligible impact.	B	1	4	None	H	4

Table B-11 continued

Threat Vector	Threat	L	Consequence	Cat.	Sev.	Risk	Countermeasures (CMR)	L with CMR	Risk with CMR
Supply Chain	A remote backdoor is installed in the BPCS Engineering Workstation during manufacturing from a nation state level attack.	L	Compromise of the BPCS engineering workstation resulting in the potential compromise of the basic process control PLC, leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.	5	5	9	The Application Program for the BPCS PLC is reviewed yearly to identify if any unapproved changes have been made.; A pressure relief valve is located on the isomerization reactor and is sized for the pressure control failure case.	VL	8
Physical Access	A contractor (unknowingly) attempts to insert ransomware infected equipment to the BPCS Engineering Workstation.	VH	Inability to access BPCS application program, with the potential for business impact (due to cost of replacing the BPCS engineering workstation and application program) or a spurious trip and unexpected downtime.	B	2	9	Restrict access to only required personnel (3 automation and controls engineers) who each have their own individual access account. Access is reviewed on a yearly basis.; The BPCS engineering workstation is kept in a locked cabinet that only required personnel may access.	M	5

Table B-11 continued

Threat Vector	Threat	L	Consequence	Cat.	Sev.	Risk	Countermeasures (CMR)	L with CMR	Risk with CMR
Software	A web server is enabled for the BPCS engineering workstation following a system upgrade, making the system vulnerable to unskilled attackers.	H	Compromise of the BPCS engineering workstation resulting in the potential compromise of the basic process control PLC, leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.	5	5	13	Restrict access to only required personnel (3 automation and controls engineers) who each have their own individual access account.; Access is reviewed on a yearly basis.; A pressure relief valve is located on the isomerization reactor and is sized for the pressure control failure case.	VL	8
Hardware	A skilled attacker tries to gain access to the BPCS Engineering Workstation using a hardwired connection from a compromised business asset.	M	Compromise of the BPCS engineering workstation resulting in the potential compromise of the basic process control PLC, leading to the potential to initiate a failure of the pressure control system. Ultimately leading to a possible overpressure and rupture of the isomerization reactor with hydrocarbon release and potential for multiple onsite fatalities.	5	5	12	Restrict access to only required personnel (3 automation and controls engineers) who each have their own individual access account. Access is reviewed on a yearly basis.; A firewall has been installed between the DMZ Zone and the BPCS zone.; The Application Program for the BPCS PLC is reviewed yearly to identify if any unapproved changes have been made.; A pressure relief valve is located on the isomerization reactor and is sized for the pressure control failure case.	VL	8

Where:

- L is the Likelihood.
- Sev is the Consequence Severity.
- CMR is Countermeasure.
- L w/ CMR is the likelihood with countermeasures.
- R w/ CMR is the risk with countermeasures.

B.4 LOPA/ Semi-Quantitative SL Verification

Step 1: Initial Risk Screening

The LOPA-based or semi-quantitative approach for cybersecurity risk assessment is typically only completed for scenarios determined to be high risk. This determination may be made based on the consequence severity or the overall level of risk. For the example isomerization unit, the semi-quantitative approach is applied for any scenarios with a mitigated risk of 12 or higher or a consequence severity of 5. From the example above, the following threats would warrant consideration using LOPA:

- Phishing campaign from skilled attacker resulting in compromised administrator BPCS Engineering Workstation credentials.
- A remote backdoor is installed in the BPCS Engineering Workstation during manufacturing from a nation state level attack.
- A web server is enabled for the BPCS engineering workstation following a system upgrade, making the system vulnerable to unskilled attackers.
- A skilled attacker tries to gain access to the BPCS Engineering Workstation using a hardwired connection from a compromised business asset.

Step 2: Determine the Threat Likelihood

The threat likelihood is then determined for each applicable threat. The likelihood of the threat can be estimated based on the qualitative likelihood level from the Cybersecurity HAZOP. For the web server example, the threat likelihood was high, based on the likelihood matrix in Table B-2; this corresponds to a frequency of once per year.

Step 3: Determine the Target Attractiveness

The target attractiveness of the site should then be estimated to determine the overall likelihood of a targeted attack. Using the target attractiveness description and estimates from Table B-12, the isomerization would most likely be categorized as a “Large Impact Target” given the size of the production facility.

Table B-12 Target Attractiveness Estimates

Name	Description	Assumptions	Multiplier
Small Impact Target	Multi-source plant with limited production impact.	Normal level of media coverage	1
Regional Impact Target	Product impact for a specific region.	Normal level of media coverage	1.5
Large Impact Target	Single source critical company assets.	Normal level of media coverage	3
Critical Infrastructure Target	National infrastructure with extensive impact.	Normal level of media coverage	5

Step 4: List the Countermeasures

Once the threat likelihood and target attractiveness are identified, countermeasures should be identified and credited based on the estimated probability of failure on demand (PFD). The countermeasures for the enabled web server example are shown in Table B-13. In addition to the access control and pressure relief valve, it was determined in the semi-quantitative review that the application program review would also be considered an effective countermeasure.

Table B-13 Cybersecurity Countermeasures and Estimated

Countermeasure	Type	Estimated PFD
Restrict access to only required personnel (3 automation and controls engineers), each of whom have their own individual access account. Access is reviewed on a yearly basis.	Active	0.1
The Application Program for the BPCS PLC is reviewed yearly to identify if any unapproved changes have been made.	Passive	0.2
A pressure relief valve is located on the isomerization reactor and is sized for the pressure control failure case.	Safeguards not susceptible to cyber-attack	0.01

Step 5: Apply Conditional Modifiers

Conditional modifiers can be applied in cybersecurity scenarios in a similar way to traditional LOPA analysis. For the isomerization unit example, an occupancy factor of 0.1 was assumed based on personnel being present in the vicinity of the reactor less than 10% of the time, during operator rounds. This modifier was reviewed and determined to be applicable for the cybersecurity scenario as well.

Step 6: Calculate the Likelihood of a Successful Attack

Once all of the factors that will have an impact on the likelihood of a cybersecurity attack resulting in the ultimate consequence are determined, the likelihood of the cybersecurity hazard scenario occurring can be determined as shown in Table B-14.

Table B-14 Semi-Quantitative SL Verification Worksheet

L	TA	CMR 1	CMR 2	CMR 3	CM	LAS
Targeted (Unskilled)	Large Impact Target	Restrict access to only required personnel (3 automation and controls engineers), each of whom have their own individual access account. Access is reviewed on a yearly basis.	The Application Program for the BPCS PLC is reviewed yearly to identify if any unapproved changes have been made.	A pressure relief valve is located on the isomerization reactor and is sized for the pressure control failure case.	Occupancy	--
1/yr.	3	0.1	0.2	0.01	0.1	6E-5/yr.

Where:

- L is Attack Likelihood
- TA is Target Attractiveness
- CMR is Countermeasure
- CM is Conditional Modifier
- LAS is Likelihood of a Successful Attack

Step 7: Determine if the Tolerable Risk Criteria are Met

The final step is to review the likelihood of the cybersecurity hazard scenario against the tolerable frequency to determine if an organization's tolerable risk is met. For each severity level in the severity matrix, a tolerable frequency is defined as shown in Table B-15.

Table B-15 Severity Level and Tolerable Frequency

Severity Level	Tolerable Frequency
1	1.00 E-2/ yr.
2	1.00 E-3/ yr.
3	1.00 E-4/ yr.
4	1.00 E-5/ yr.
5	1.00 E-6/ yr.

Using the likelihood of a successful attack from step 6 and the tolerable frequency from Table B-15, the residual risk for the scenario can be calculated using Equation B-1.

$$Residual\ Risk = \frac{Likelihood\ of\ a\ Successful\ Attack}{Tolerable\ Frequency}$$

Equation B-1

Substituting for the tolerable frequency of 1.00E-6/yr. for a severity level 5 consequence and the calculated likelihood of 6E-5/yr. a residual risk of "6" can be determined as shown in Equation B-2.

$$\text{Residual Risk} = \frac{6.00E-5/\text{yr}}{1.00 E-6/\text{yr}} \quad \text{Equation B-2}$$

The residual factor of 6 indicates that, even with the current countermeasures, the risk is not fully mitigated and additional recommendations for improving security are needed. Possible means for mitigating this risk could include the addition of additional cybersecurity countermeasures such as continuous threat monitoring. Alternatively, actions to mitigate the vulnerability of the enabled web server could also make the BPCS engineering workstation less susceptible to cybersecurity compromise and provide another option for reducing the risk. Providing a clear picture of the current risk is a critical part of employing the risk-based approach to manage risk and ensuring the optimal selection of cybersecurity protections.

Appendix C Example Cybersecurity Metrics

The following lists identify metrics in physical security, unauthorized access, change management, and unauthorized network management based on the IEC 62443-2-1 standard [12] that can be used as a starting point for developing company-specific cybersecurity metrics.

- Physical Security Metrics
 - o Are all logic solvers in an access-controlled environment?
 - o Are all logic solvers in a locked cabinet?
 - o Is authorized access reviewed at documented intervals?
 - o Are there controls in place to remove access immediately for someone that has become unauthorized?
 - o Are controls in place to prevent logic solvers from being programmed/configured remotely from a different network segment?
- Unauthorized Access Metrics
 - o Are roles and responsibilities for each type of account on the IACS system defined and documented?
 - o Are passwords changed at documented intervals?
 - o Are procedures followed to immediately remove access for users that no longer have authorization?
 - o What percentage of users have undergone cybersecurity hygiene training? Role-based training?
 - o How many unsuccessful login attempts have occurred?
 - o Have there been any successful unauthorized access attempts?
- Authorized Change Management Metrics
 - o Are there changes in the control of safety systems that have not been authorized by an approved MOC document that are discovered during a regular occurring audit?
- Unauthorized Network Communication Metrics
 - o Is all portable media scanned for malware prior to communicating with the IACS?
 - o Is all portable media used to communicate with the IACS authorized in a written cybersecurity policy?
 - o Are all USB ports on the IACS physically or logically disabled?

- o What percentages of IACS assets have anti-virus or endpoint protection installed?
- o What percentage of IACS assets have operating systems or applications with known vulnerabilities?
- o What percentage of IACS assets are currently maintained at the desired patch level?
- o Are there any unknown devices connected to the IACS?

Appendix D Cybersecurity Sample Audit Question List

The following is a sample of the topics and questions that may be addressed within an internal self-assessment or independent cybersecurity audit. The list is not all-inclusive. The audit questions list should be developed based on the standards, procedures, and practices in place within the organization.

Table D-1 Cybersecurity Sample Audit Checklist

Item	Question	Response	Recommendation
Cyber Hygiene			
1	Do personnel change passwords routinely?		
2	Do personnel know how to identify a phishing email?		
3	Do personnel know how to report a suspected phishing email?		
4	Are contractors trained with basic cyber hygiene requirements?		
Policies and Procedures			
5	Is a cybersecurity management system in place and aligned with process safety management activities?		
6	Are personnel awareness of policies and procedures, and are personnel adhering to recommended practices?		
7	Do tasks require a 'workaround' to address situations where system security makes their job more difficult?		
8	Do procedures address different cybersecurity requirements for networked and isolated systems?		

Table D-1 continued

Item	Question	Response	Recommendation
Policies and Procedures			
9	Are procedures for patch and software updates followed?		
10	Are the required records or logs updated to reflect changes?		
11	Is everything that should be backed up getting backed up on schedule?		
12	Is the MOC process being followed for all changes being done in control systems which can change cyber risk?		
13	Is remote connectivity being provided for control systems as per established procedure? Is restoration being checked? Are backups being stored at physically separate locations?		
14	What is the emergency response plan in the event of a cybersecurity event?		
Risk Assessment			
15	Is an updated hardware and software inventory maintained?		
16	Does risk assessment address the risk associated with non-compliant cybersecurity activities?		
17	Are risk assessment recommendations addressed in a timely manner?		

Table D-1 continued

Item	Question	Response	Recommendation
Cybersecurity Countermeasures			
18	Is the business network segregated from the IACS network? How is ownership defined between the two networks?		
19	How are firewalls and firewall rules managed?		
20	How is remote access governed?		
21	How is wireless access governed?		
22	Are autorun and auto-play features disabled on tools for removable media devices?		
23	How is portable media (e.g., USB sticks/ports) managed?		
24	How is content downloaded from the internet managed?		
25	Is anti-virus or whitelisting used on the IACS?		
Effectiveness of monitoring systems			
26	Do the routinely monitored metrics provide a good understanding of system performance when compared against periodic audit results?		
27	Are diagnostics and alarms for countermeasures employed? If yes, provide examples.		
28	Is an active log of network activity collected and reviewed (e.g. System Information and Event Monitoring)?		

Table D-1 continued

Item	Question	Response	Recommendation
Access Control			
29	Is authorized access reviewed at documented intervals?		
30	Are there controls in place to remove access immediately to someone that has become unauthorized?		
31	Are controls in place to prevent Process Safety Controls Alarms and Interlock (PSCAI) logic solvers from being programmed/configured remotely from a different network segment?		
Physical Security			
32	Are all PSCAI logic solvers in an access-controlled environment inside locked cabinets?		
33	Are all USB ports on a PSCAI system physically or logically disabled?		
34	Are all logic solvers put in RUN state instead of PROGRAM state wherever it is applicable?		
35	Are fire detection and mitigation equipment installed and working in the area where control systems are installed?		

Table D-1 continued

Item	Question	Response	Recommendation
Equipment Conformance to Design			
36	Is the installed equipment consistent with what is identified in the design documents?		
37	Are systems connected as shown on network diagrams?		
38	Is there equipment in the field that is not shown on network diagrams?		
Update and Improvement			
39	Are recommendations from the cybersecurity risk assessments, incident investigations and prior audits documented, tracked, and closed in a timely and effective way?		
40	Has system hardening and policy configuration been completed for standalone assets (e.g., package PLCS)?		
Risk of Obsolescence			
41	Does the system include equipment that is obsolete or no longer supported by vendor?		
42	Are equipment and parts procured from reliable sources?		
43	Is cyber equipment being disposed of safely?		

Appendix E Management System Review Examples

The scope of the management review may vary depending on the objective and desired level of detail. Example questions are identified in this appendix for three different types of management reviews with varying levels of frequency.

Metrics reviews conducted at high frequency:

- How are the metrics trending?
- Are hazards analysis being completed on schedule?
- Are preventive maintenance (PM) and inspections being done per schedule?
- How many open PHA recommendations are there?
- How many MOCs are there open longer than six months? Longer than one year?
- What PHAs are due to be performed this year, and what is the timeline and status of those?
- What PSM audit open action items are there, and what is status?
- Are procedures and standards being reviewed on schedule?

Document review conducted on a defined schedule:

- What do audit results indicate about my management system? Are systemic changes needed?
- Is this procedure or standard effective?
- Is this procedure or standard still applicable? Does anything need to be updated?
- Are the metrics that are tracked effective? Are they correlated to system performance and security?
- Are cybersecurity risk assessment and incident investigation recommendations realistic and actionable?
- What resources are needed to address these action item?

Regional or business segment level reviews conducted quarterly:

- What is the performance in one of the RBPS Pillars (rotation over the course of a year)?
- Is risk being managed as intended?
- Are the barriers to manage risk still in place and healthy?
- Are there safety/ security incidents or near miss events?
- What metrics are tracked, and how is the performance?

- What are the gaps that need to be addressed, or elements that need to be improved?
- What are forthcoming regulatory, industry, or ESG (Environment, Sustainability, Governance) changes that need to be addressed?
- What is the status of the current infrastructure and technology? Is it well-maintained? Is it falling behind industry benchmarks?
- What are the corporate objectives – do changes need to be made, or is further evolution required to meet corporate goals?
- Based on the gaps, evolving regulatory/industry standards, infrastructure needs, corporate projects, etc., what are the goals for the next several years?
- What is the existing organizational structure – is the right structure in place to address those challenges?
- What is the competency level of the organization – are the right skills to address those challenges in place?
- Is there a sufficient budget to meet the defined goals?

References

- [1] CCPS, "CCPS Process Safety Glossary," Center for Chemical Process Safety, 2021. [Online]. Available: www.aiche.org/ccps.
- [2] Lockheed Martin, "Seven Ways to Apply the Cyber Kill Chain® with a Threat Intelligence Platform," Lockheed Martin, Bethesda, MD USA, 2015.
- [3] International Electrotechnical Commission, IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, Geneva, Switzerland: International Electrotechnical Commission, 2009.
- [4] International Society of Automation, "ISA 84.91.01 Identification and Mechanical Integrity of Safety Controls, Alarms, and Interlocks in the Process Industry," International Society of Automation, Research Triangle, NC, 2012.
- [5] Kaspersky, "The State of Industrial Cybersecurity," ARC Advisory Group, Dusseldorf, 2019.
- [6] K. E. Hemsley and R. E. Dr. Fisher, "History of Industrial Control System Cyber Incidents," Idaho National Laboratory, Idaho Falls, 2018.
- [7] CCPS, Guidelines for Risk Based Process Safety (RBPS), Hoboken, NJ USA, NY: John Wiley & Sons, 2007.
- [8] R. M. Lee, M. J. Assante and T. Conway, "ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack," ICS SANS, Rockville, MD, 2014.
- [9] K. Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, New York, NY, USA: Crown Publishing Group, 2014.

- [10] N. Perlroth and C. Krauss, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," The New York Times, New York, NY USA, 2018.
- [11] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Gaithersburg, MD USA: National Institute of Standards and Technology, 2018.
- [12] International Electrotechnical Commission, IEC 62443 Part 2-1 Establishing an industrial automation and control system security program, Geneva Switzerland: International Electrotechnical Commission, 2010.
- [13] International Society of Automation, Cybersecurity Related to the Functional Safety Lifecycle, Research Triangle, NC USA: International Society of Automation, 2017.
- [14] "6 Code of Federal Regulations Part 27 Chemical Facility Anti-Terrorism Standards," Washington, DC USA, 2007.
- [15] NERC, "CIP-002-5.1a - Cyber Security - BES Cyber System Categorization," North American Electric Reliability Corporation, Washington, DC USA, 2015.
- [16] "America's Water Infrastructure Act (AWIA)," Washington, DC USA, 2018.
- [17] "Occupational Safety and Health Standards 29 CFR 1910.119," Washington, DC USA, 1999.
- [18] International Electrotechnical Commission, "IEC 61511 Functional Safety - Safety instrumented systems for the process industry sector," International Electrotechnical Commission, Geneva, Switzerland, 2016.
- [19] N. Sayfayn and S. Madnick, "Cybersafety Analysis of the Maroochy Shire Sewage Spill," Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, Cambridge, MA USA, 2017.

- [20] K. Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, San Francisco, CA USA, 2016.
- [21] A. Greenberg, "'Crash Override': The Malware That Took Down a Power Grid," Wired, San Francisco, CA USA, 2017.
- [22] A. Greenberg, "A Hacker Tried to Poison a Florida City's Water Supply, Officials Say," Wired, San Francisco, CA USA, 2021.
- [23] International Organization for Standardization, "ISO 27002 Information technology- Security techniques - Code of practice for information security controls," International Organization for Standardization, Geneva, Switzerland, 2013.
- [24] American Petroleum Institute, API 1164 Pipeline SCADA Security, Washington, DC USA: American Petroleum Institute, 2016.
- [25] Check Point Research, "Naikon APT: Cyber Espionage Reloaded," Check Point Research, San Carlos, CA USA, 2020.
- [26] L. H. Newman, "No One Knows How Deep Russia's Hacking Rampage Goes," Wired, San Francisco, CA USA, 2020.
- [27] D. E. Sanger and N. Perlroth, "More Hacking Attacks Found as Officials Warn of 'Grave Risk' to U.S. Government," New York Times, New York, NY USA, 2020.
- [28] Kaspersky Lab ICS CERT, "Threat Landscape for Industrial Automation Systems," Kaspersky Lab, Moscow, Russia, 2018.
- [29] McAfee, "Operation Sharpshooter Campaign Targets Global Defense, Critical Infrastructure," McAfee, Santa Clara, CA USA, 2018.
- [30] A. Cherepanov, "GreyEnergy a sucesor to BlackEnergy," ESET, Bratislava, Slovakia, 2018.
- [31] Reuters, "Ukraine Utility Cyber Attack Wider Than Reported: Experts," NBC News, New York, NY USA, 2015.

- [32] C. Cimpanu, "Ransomware accounted for 41% of all cyber insurance claims in H1 2020," ZD Net, Indian Land, SC USA, 2020.
- [33] L. Matthews, "Ransomware Hackers Have Started Leaking City of Pensacola Data," Forbes, New York, NY USA, 2019.
- [34] B. Freed, "New Orleans latest apparent victim of Ryuk ransomware," Scoop News Group, Washington, DC USA, 2019.
- [35] NAO Comptroller and Auditor General, "Investigation: WannaCry cyber attack and the NHS," National Audit Office, London, England, 2018.
- [36] R. Browne, "Hackers Behind Colonial Pipeline Attack Reportedly Recieved \$90 Million in Bitcoin before Shutting Down," CNBC, Englewood Cliffs, NJ United States of America, 2021.
- [37] Cyber Security Challenge UK, "Cyber Security Challenge UK Helps Youngsters Use Cyber Skills in Positive Ways," Cyber Security Challenge UK, Hertfordshire, England, 2020.
- [38] S. Evans, "Businesses Blame DDoS Attacks on Rival Companies," Infosecurity Group, London, England, 2017.
- [39] Symantec, "Sodinokibi: Ransomware Attackers also Scanning for PoS Software, Leveraging Cobalt Strike," Symantec, Mountain View, CA, 2020.
- [40] M. Kassner, "Anatomy of the Target data breach: Missed opportunities and lessons learned," ZDNet, San Francisco, CA USA, 2015.
- [41] D. Geere, "Japanese virus replaces files with pictures of squid," WIRED, San Francisco, CA, 2010.
- [42] A. Brown, "Godzilla Attack or Road-Sign Hack?," The Atlantic, Washington, DC USA, 2014.

- [43] J. A. Klein, "Turn Up Process Safety Performance," Chemical Processing, Cincinnati, Ohio USA, 2019.
- [44] CCPS, Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites, Hoboken, NJ USA: John Wiley & Sons, 2003.
- [45] K. Ruan, Cybercrime and Cloud Forensics: Applications for Investigation Processes, University College Dublin, Ireland: IGI Global, 2012.
- [46] International Society of Automation, ANSI/ISA-18.2-2016, Management of Alarm Systems for the Process Industries, Research Triangle Park, NC, USA: International Society of Automation, 2016.
- [47] KnowBe4, "Phishing By Industry 2020 Benchmarking Report," KnowBe4, Clearwater, FL USA, 2020.
- [48] Info Security, "Scariest Search Engine on the Internet Just Got Scarier," Info Security Group, London UK, 2014.
- [49] M. Antonakakis, T. April and M. Bailey, "Understanding the Mirai Botnet," in *26th USENIX Security Symposium*, Vancouver, BC, Canada, 2017.
- [50] A. Laszka, B. Johnson and J. Grossklags, "Mitigating Covert Compromises," in *Web and Internet Economics. WINE 2013. Lecture Notes in Computer Science, vol 8289*. Springer, Berlin, Heidelberg, Germany, 2013.
- [51] Imperva, "Insider Threat," Imperva, Redwood Shores, CA, 2020.
- [52] Ponemon Institute, "2018 Cost of Insider Threats: Global," Ponemon Institute, Traverse City, MI USA, 2018.
- [53] Kaspersky, "USB Threats from Malware to Miners," Secure List, Moscow, Russia, 2018.

- [54] U.S. Nuclear Regulatory Commission, "Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations," U.S. Nuclear Regulatory Commission, Rockville, MD USA, 2007.
- [55] A. Greenberg, "How 30 Lines of Code Blew Up a 27-Ton Generator," WIRED, San Francisco, CA, 2020.
- [56] P. Muncaster, "Dutch Insider Deployed Stuxnet: Report," Infosecurity, London, England, 2019.
- [57] Federal Office for Information Security, "The Situation of IT Security in Germany 2014," Federal Office for Information Security, Bonn, Germany, 2014.
- [58] S. Erler, "Steelworker Recounts Accident at Blast Furnace," Times of Northwest Indiana, Munster, Indiana, 2006.
- [59] Occupational Safety and Health Administration, "Accident: 200101251 - Employee Killed When Furnace Explodes," Occupational Safety and Health Administration, Washington, D.C. USA, 2001.
- [60] World Steel Association, "World Steel in Figures 2014," World Steel Association, Brussels, Belgium, 2014.
- [61] D. Raywood, "Industroyer Malware Detected, Linked to Kiev Attack," Infosecurity, London, England, 2017.
- [62] K. O'Flaherty, "U.S. Government Makes Surprise Move to Secure Power Grid from Cyberattacks," Forbes, New York, NY USA, 2019.
- [63] Z. Whittaker, "Six Quick Facts to Know About the Petya global ransomware attack," ZD Net, Indian Land, SC USA, 2017.
- [64] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," WIRED, San Francisco, CA USA, 2018.

- [65] J. Porup, "What is Mimikatz? And How to Defend Against This Password Stealing Tool," CSO Online, Needham, MA USA, 2019.
- [66] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker and C. Glycer, "Attackers Deploy New ICS Attack Framework "Triton" and Cause Operational Disruption to Critical Infrastructure," FireEye, Milpitas, CA USA, 2017.
- [67] M. Giles, "Triton is the World's Most Murderous Malware, and it's Spreading," MIT Technology Review, Cambridge, MA USA, 2019.
- [68] J. Tidy, "Police Launch Homicide Inquiry After German Hospital Hack," BBC News, London, England, 2020.
- [69] A. Smith, S. Smith, N. Bailey and P. Cahill, "Why "WannaCry" Malware Caused Chaos for National Health Service in UK," NBC News, New York, NY USA, 2017.
- [70] P. H. O'Neill, "Ransomware did not Kill a German Hospital Patient," MIT Technology Review, Cambridge, MA USA, 2020.
- [71] A. Suderman, "AP sources: SolarWinds hack got emails of top DHS officials," Associated Press, New York, NY USA, 2021.
- [72] Cybersecurity & Infrastructure Agency, "Alert (AA20-352A)," Cybersecurity & Infrastructure Agency, 17 December 2020. [Online]. Available: <https://us-cert.cisa.gov>.
- [73] M. Clark, "Move over, SolarWinds: 30,000 orgs' email hacked via Microsoft Exchange Server flaws," The Verge, 5 March 2021. [Online]. Available: <https://www.theverge.com>.
- [74] J. Leyden, "Water Treatment Plant Hacked, Chemical Mix Changed for Tap Supplies," The Register, 24 March 2016. [Online]. Available: <https://www.theregister.com>.

- [75] J. Peiser, "A Hacker Broke into a Florida Town's Water Supply and Tried to Poison it with Lye," Washington Post, Washington, D.C. USA, 2021.
- [76] W. Turton and K. Mehrotra, "Hackers Breached Colonial Pipeline Using Compromised Password," Bloomberg, New York, NY United States of America, 2021.
- [77] C. Bing, J. Menn and S. N. Lynch, "U.S. seizes \$2.3 mln in bitcoin paid to Colonial Pipeline hackers," Reuters, London, UK, 2021.
- [78] M.-A. Russon, "US Guel Pipeline Hackers 'Didn't Mean to Create Problems'," BBC, London, United Kingdom, 2021.
- [79] Cybersecurity & Infrastructure Security Agency, "Alerts," Cybersecurity & Infrastructure Security Agency, [Online]. Available: <https://us-cert.cisa.gov>.
- [80] International Society of Automation, "IS-TR84.00.09 Cybersecurity Related to the Functional Safety Lifecycle," International Society of Automation, Research Triangle, NC, 2017.
- [81] International Electrotechnical Commission, IEC 62443 Part 3-3 System security requirements and security levels, Geneva Switzerland: International Electrotechnical Commission, 2013.
- [82] National Institute of Standards and Technology, NIST SP-800-12 An Introduction to Computer Security: the NIST Handbook, Gaithersburg, MD USA: National Institute of Standards and Technology, 1995.
- [83] Internet Engineering Task Force, "RFC 2196 Site Security Handbook," Internet Engineering Task Force, Fremont, CA, 1997.
- [84] D. G. Gunter, M. D. Medoff and P. C. O'Brien, Implementing IEC 62443: A Pragmatic Approach to Cybersecurity, Sellersville, PA: exida, 2018.

- [85] Echemi, "Styrene Price Analysis," Echemi, [Online]. Available: <https://www.echemi.com>.
- [86] CCPS, *Inherently Safer Chemical Processes, A Life Cycle Approach*, Second Edition, Hoboken, NJ USA: John Wiley & Sons, 2009.
- [87] British Columbia Institute of Technology, "Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks," National Infrastructure Security Co-Ordination Centre, London, England, 2004.
- [88] Dragos, "2019 Year in Review, The ICS Landscape and Threat Activity Groups," Dragos, Hanover, MD USA, 2019.
- [89] C. Fisher, Interviewee, *Control & Automation Engineering Technical Authority*. [Interview]. 18 June 2021.
- [90] A. Schiffer, "How a fish tank helped hack a casino," Washington Post, Washington, D.C. USA, 2017.
- [91] L. Matthews, "Criminals Hacked a Fish Tank To Steal Data From a Casino," Forbes, New York, NY USA, 2017.
- [92] OSSEC, "About OSSEC Host Intrusion Detection," OSSEC, [Online]. Available: <https://www.ossec.net>.
- [93] Wireshark, "Wireshark," Wireshark, [Online]. Available: wireshark.org.
- [94] NMAP, "NMAP," NMAP, [Online]. Available: <https://nmap.org/>.
- [95] ControlScan, "SIEM: A Guide to Security Information & Event Management," ControlScan, Atlanta, GA USA, 2020.
- [96] Security Onion Solutions, "Security Onion 2," Security Onion Solutions, [Online]. Available: <https://securityonionsolutions.com>.

- [97] International Electrotechnical Commission, IEC 62443 Part 3-2 Security Risk Assessment for System Design, Geneva Switzerland: International Electrotechnical Commission, 2020.
- [98] CCPS, Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites, Hoboken, NJ USA: John Wiley & Sons, 2003.
- [99] NIST, "National Vulnerability Database," [Online]. Available: <https://nvd.nist.gov/>.
- [100] SomarSoft, "Free Utilities & DumpSec," SomarSoft, [Online]. Available: <https://www.systemtools.com>.
- [101] Greenbone, "OpenVAS - Open Vulnerability Assessment Scanner," Greenbone, [Online]. Available: <https://www.openvas.org>.
- [102] CCPS and the Energy Institute, Bow Ties in Risk Management: A Concept Book for Process Safety, Hoboken, NJ USA: John Wiley & Sons, 2018.
- [103] CCPS, Layer of Protection Analysis (LOPA): Simplified Risk Assessment, Hoboken, NJ USA: John Wiley & Sons, 2001.
- [104] CCPS, Guidelines for Enabling Conditions and Conditional Modifiers in Layers of Protection Analysis, Hoboken, NJ USA: John Wiley & Sons, 2014.
- [105] CCPS, Guidelines for Chemical Process Quantitative Risk Analysis, Second Edition, Hoboken, NJ USA: John Wiley & Sons, 2000.
- [106] CCPS, Guidelines for Determining the Probability of Ignition of a Released Flammable Mass, CCPS/AIChE, 2014, Hoboken, NJ USA: John Wiley & Sons, 2014.
- [107] International Electrotechnical Commission, IEC 62443 Security for Industrial Automation and Control Systems Parts 1-4, Geneva Switzerland: International Electrotechnical Commission, 2007.

- [108] S. A. Rashid and A. B. Hasim, "Accelerating Cybersecurity Culture Maturity in the Workplace," ISA Global Cybersecurity Alliance, [Online]. Available: <https://gca.isa.org/blog>.
- [109] S. Stock and J. Cusimano, "Addressing Common Process Control Network (PCN) Misconfigurations Will Increase Availability, Security and Safety," in *SANS ICS security Summit & Training*, Greenville, SC, 2019.
- [110] U.S. Chemical Safety and Hazard Investigation Board, "Investigation Report Number 2008-08-I-WV," U.S. Chemical Safety and Hazard Investigation Board, Washington, D.C. USA, 2011.
- [111] U.S. Chemical Safety and Hazard Investigation Board, "Investigation Report Number 2005-04-I-TX," U.S. Chemical Safety and Hazard Investigation Board, Washington, D.C. USA, 2007.
- [112] American National Standards Institute/ International Society of Automation, "ANSI/ISA 18.2 Management of Alarm Systems for the Process Industries," International Society of Automation, Research Triangle Park, NC USA, 2016.
- [113] D. Palmer, "Jump in Vulnerable RDP ports is Leaving Networks Open to Hacking and Cyberattacks," ZDNet, San Francisco, CA USA, 2020.
- [114] Cybersecurity & Infrastructure Security Agency (CISA), "Alert (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors," Cybersecurity & Infrastructure Security Agency (CISA), Arlington, VA USA, 2020.
- [115] S. Rose, O. Borchert, S. Mitchell and S. Connelly, "NIST Special Publication 800-207 Zero Trust Architecture," National Institute of Standards and Technology, Gaithersburg, MD USA, 2020.
- [116] B. Vigliarolo, "Zero trust security: A Cheat sheet," TechRepublic, Louisville, KY USA, 2020.
- [117] M. Cooney, "What is SDN and where Software-Defined Networking is Going," Network World, New York, NY USA, 2019.

- [118] Symantec, "Internet Security Threat Report Volume 23," Symantec, Tempe, AZ USA, 2018.
- [119] National Telecommunications and Information Administration (NTIA), "Software Bill of Materials," National Telecommunications and Information Administration (NTIA), Washington, D.C. USA, 2020.
- [120] The Open Group, "Open Process Automation Standards," The Open Group, [Online]. Available: <https://publications.opengroup.org>.
- [121] D. Emerson, "The Open Process Automation Standard Takes Flight," International Society of Automation, Research Triangle Park, NC USA, 2019.
- [122] Mordor Intelligence, "Cyber Security Insurance Market - Growth, Trends, Covid-19 Impact, and Forecasts (2021-2026)," Mordor Intelligence, Hyderabad, India, 2020.
- [123] Allianz Global Corporate and Specialty, "A Guide to Cyber Risk: Managing the Impact of Increasing Interconnectivity," Allianz, Munich, Germany, 2015.
- [124] J. Bernard, "Overcoming Challenges to Cyber Insurance Growth," Deloitte, London, UK, 2020.
- [125] Marsh, "Global Cyber Risk Perception Survey Report 2019," Marsh, New York, NY USA, 2019.
- [126] Cybersecurity & Infrastructure Security Agency (CISA), "Cybersecurity Insurance," Cybersecurity & Infrastructure Security Agency (CISA), [Online]. Available: <https://www.cisa.gov>.
- [127] Cybersecurity & Infrastructure Security Agency (CISA), "5G Security and Resilience," Cybersecurity & Infrastructure Security Agency (CISA), [Online]. Available: <https://www.cisa.gov/5g>.
- [128] Cybersecurity & Infrastructure Security Agency (CISA) , "Edge vs. Core - An Increasingly Less Pronounced Distinction in 5G Networks,"

- Cybersecurity & Infrastructure Security Agency (CISA) , Arlington, VA USA, 2020.
- [129] R. van der Meulen, "What Edge Computing Means for Infrastructure and Operations Leaders," Gartner, Stamford, CT USA, 2018.
- [130] Health and Safety Executive, "Profiling your health and safety risks," Health and Safety Executive, [Online]. Available: <https://www.hse.gov.uk>.
- [131] International Organization for Standardization, "ISO 27001 Information Technology - Information Security Management Systems," International Organization for Standardization, Geneva, Switzerland, 2013.
- [132] Federal Energy Regulatory Commission (FERC), "18 CFR 40 - Mandatory Reliability Standards for the Bul-Power System," Department of Energy, Washington, D.C. USA, 2016.
- [133] "Maritime Transportation Security Act," Washington, D.C. USA, 2002.
- [134] "Senate Bill No. 327 Security of Connected Devices," Sacramento, CA USA, 2018.
- [135] "General Data Protection Regulation 2016/679," European Parliament and Council of the European Union, Brussels, Belgium, 2016.
- [136] Health and Safety Executive, "Cyber Security for Industrial Automation and Control Systems (IACS) Edition 2," Health and Safety Executive, Bootle, Merseyside, UK, 2016.
- [137] "Information Technology Security Act (ITSIG2.0)," Berlin, Germany, 2020.
- [138] "China Security Law (CSL)," Beijing, China, 2016.

- [139] Ministry of Transport and Communications, "National ICS Security Standard Version 3.1," Ministry of Transport and Communications, Doha, Qatar, 2019.
- [140] National Technical Research Organization, "National Critical Information Infrastructure Protection Centre," National Technical Research Organization, 15 April 2021. [Online]. Available: <https://nciipc.gov.in/>.
- [141] Arkose Labs, "Arkose Labs Reveals 20% Spike in Fraud as Digital Behavior Shifts During COVID-19," Arkose Labs, San Francisco, CA USA, 2020.
- [142] Checkpoint, "Live Cyber Threat Map," Checkpoint, [Online]. Available: <https://threatmap.checkpoint.com/>.
- [143] FireEye, "FireEye Cyber Threat Map," FireEye, [Online]. Available: <https://www.fireeye.com>.
- [144] Cybersecurity & Infrastructure Security Agency, "Enhancing Resilience Through Cyber Incident Data Sharing and Analysis," Cybersecurity & Infrastructure Security Agency, Arlington, VA USA, 2015.
- [145] Cybersecurity & Infrastructure Security Agency (CISA), "Training Available Through CISA," Cybersecurity & Infrastructure Security Agency (CISA), [Online]. Available: <https://us-cert.cisa.gov>.
- [146] exida, "exida Functional Safety Services, Cybersecurity," exida, [Online]. Available: <https://www.exida.com>.
- [147] International Society of Automation (ISA), "ISA/IEC 62443 Cybersecurity Certificate Programs," International Society of Automation (ISA), [Online]. Available: <https://www.isa.org/training-and-certification/isa-certification/isa99iec-62443/isa99iec-62443-cybersecurity-certificate-programs>. [Accessed 25 February 2021].

- [148] TÜV Rheinland, "Cyber Security Specialist- CySec Specialist (TÜV Rheinland)," TÜV Rheinland, [Online]. Available: <https://www.tuv.com>.
- [149] Global Information Assurance Certification (GIAC), "Cyber Security Certification: GICSP," Global Information Assurance Certification (GIAC), [Online]. Available: <https://www.giac.org>.
- [150] Global Information Assurance Certification (GIAC), "Cyber Security Certification: GRID," Global Information Assurance Certification (GIAC), [Online]. Available: <https://www.giac.org>.
- [151] Global Information Assurance Certification (GIAC), "Cyber Security Certification: GCIP," Global Information Assurance Certification (GIAC), [Online]. Available: <https://www.giac.org>.
- [152] Information Assurance Certification Review Board (IACRB), "Certified SCADA Security Architect (CSSA)," Information Assurance Certification Review Board (IACRB), [Online]. Available: <https://www.iacertification.org>.
- [153] Center for Internet Security Inc., "CIS Controls," Center for Internet Security Inc., East Greenbush, NY USA, 2019.
- [154] ISACA, COBIT 5: Enabling Processes, Schaumburg, IL USA: ISACA, 2012.
- [155] National Institute of Standards and Technology, "SP 800-53: Security and Privacy Controls for Information Systems and Organizations," NIST, Gaithersburg, MD USA, 2020.
- [156] C. J. Cleveland, "Oil Refining and Products," in *Encyclopedia of Engery*, Amsterdam, Netherlands, Elsevier Science, 2004, pp. 715,721.

Index

A

Access Control 134, 150, 237

Advanced Persistent Threat 20, 58

Anti-Virus 175

Asset Integrity and Reliability.. 266

Attack Surface 148, 153, 173

Audit.....300, 322, 413

Auditing 300

B

Bow Tie 218

C

Colonial Pipeline Ransomware 107

Competency 246, 363

Compliance with Standards 242

Computer Virus.....47

Conduct of Operations 281

Continuous Improvement304, 324

Contractor Management 272

CSMS 328, 363

Cyber PHA/HAZOP 387

Cybersecurity Competency 246

Cybersecurity Culture 240

Cybersecurity Framework129, 371

Cybersecurity Lifecycle ... 113, 118, 119, 121, 328

Cybersecurity Management System..... 312

Cybersecurity Risk Assessment 188

Cybersecurity Vulnerability Analysis 212

D

Data Diode 161

DDoS See Denial of Service

Decommissioning..... 120

Defense-in-Depth 149, 151

Demilitarized Zone 13, 158

Denial of Service 22, 55, 56

Disgruntled Employee..... 29, 66

Düsseldorf Hospital Ransomware 99

E

Emergency Management 285

F

Firewall.....40, 152, 157

First Ukrainian Power Grid Attack 84

Florida Water System 105

G

German Steel Mill 81

H

Hacktivist 28, 38

Hazard and Operability Study 185, 188

Hazard Identification and Risk
Analysis 183
HAZOP *See* Hazard and Operability
Study

I

IACS *See* Industrial Automation
and Control Systems
Incident Investigation..... 290
Industrial Automation and Control
Systems..... 13, 141
Information Technology 145
Internet of Things 43

K

Kill Chain® 60

L

Layer of Protection Analysis.... 405

M

Management of Change.. 120, 262
Management Review and
Continuous Improvement ... 304
Maroochy Shire.....73
Measurements and Metrics 295
Metrics 295, 324, 411

N

Nation State 27, 77, 96
Network Segmentation... 153, 157,
170, 341

NIST Cybersecurity Framework
..... 129, 132, 219, 244, 371
Non-Targeted Attacks 49
NotPetya 91

O

Operating Procedures..... 256
Operational Readiness 278
Operational Technology 10, 13,
145

P

Patch Management 122, 174
Personnel Security.....16
PHA... *See* Process Hazard Analysis
Phishing 50, 54
Physical Security 15
Process Hazard Analysis.. 185, 188
Process Knowledge Management
..... 252

Q

Quantitative Risk Assessment. 230

R

Ransomware 24, 52, 69
Reference Model 11, 158
Remote Access..... 165, 167
Remote Operation..... 167
Risk 33, 35
Rogue Wiz 30

S

Safe Work Practices..... 259

Script Kiddies 30, 38, 50, 56

Second Ukrainian Power Grid

 Attack 87

Security Level 116

Security Monitoring..... 176, 178

Semi-Quantitative Security Level

 Verification..... 221, 222

Semi-Quantitative SL Verification

 405

Social Engineering 50, 198

Software Defined Networks 341

SolarWinds 101

Spear Phishing..... 54, 81

Stakeholder Outreach..... 251

Stuxnet.....77

System Hardening 173

T

Target Attractiveness 37, 38

Targeted Attacks.....53

Training and Performance

 Assurance 275

Triton.....95

U

Ukrainian Power Grid.....84

V

Vulnerability 37, 215

W

Workforce Involvement 248

Z

Zero Trust Architecture..... 341

Zero-Day Vulnerabilities 78

Zone & Conduit..... 115, 195

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.