CUTAWAY SECURITY
INFOSEC CONSULTANTS

Architecting Safety using Cybersecurity Requirements and Assessments

Don C. Weber - @cutaway
Principal Consultant, Founder

1

Cutaway Security, LLC / Don C. Weber

- Masters Degree in Information Assurance
- IACS Security Program Maturity
- IACS Security Assessments
- Penetration Testing
- Security Research

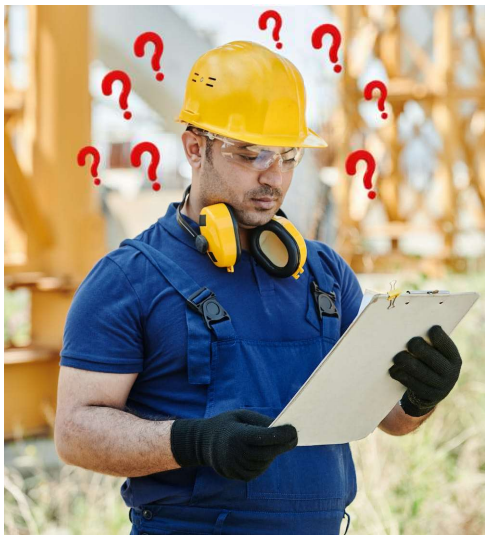
SANS ICS410: ICS/SCADA Security Essentials

Assessing and Exploiting Control Systems

2

Agenda

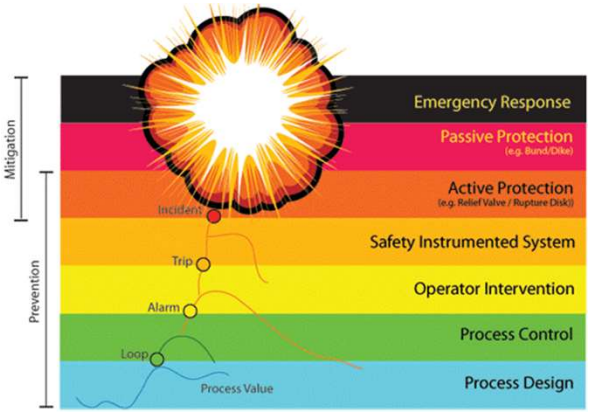
- The Cybersecurity Safety Challenge
- Starting the Architecture Conversation
- Starting the Assessment Conversation
- Summary
- Questions (possibly afterwards)



3

Safety and Protection Systems

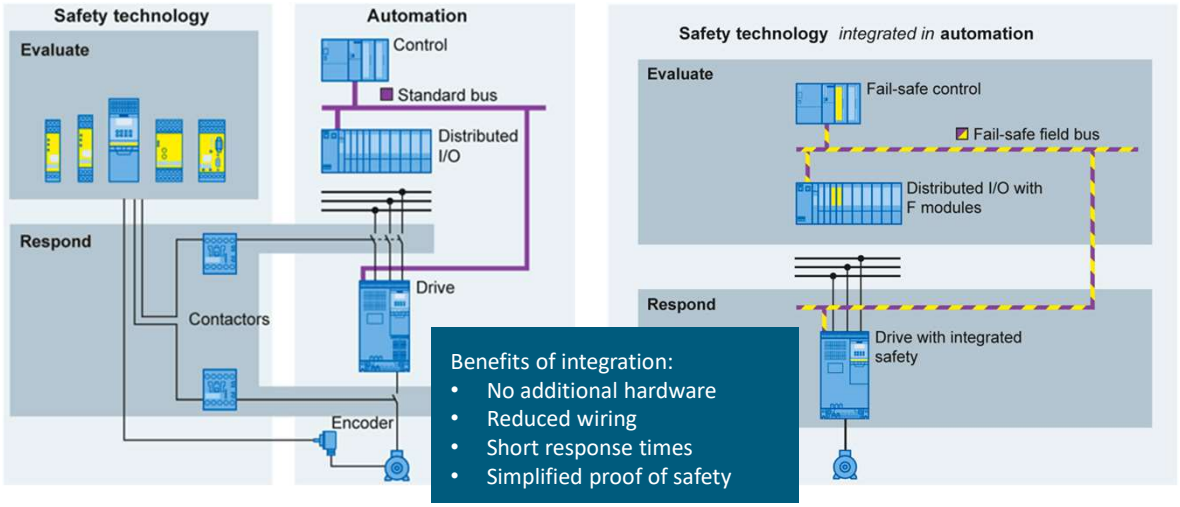
- Safety and protection systems
  - Prevents worse-case scenarios
  - Great lines of last defense
  - Implemented in your most critical processes
  - Requires full manual reset after triggered
  - Failures: https://www.csb.gov/videos/
- SIS systems include automated protection:
  - Leak detection equipment
  - Tank/sump alarms
  - Hazardous gas detectors
  - Burner management
  - Nuclear safety detection systems



Source: SANS ICS410 | ICS/SCADA Security Essentials

4

Traditional Safety System vs. Integrated Safety System



Benefits of integration:
- No additional hardware
- Reduced wiring
- Short response times
- Simplified proof of safety

Source: SANS ICS410 | ICS/SCADA Security Essentials

5

The Cybersecurity Safety Challenge

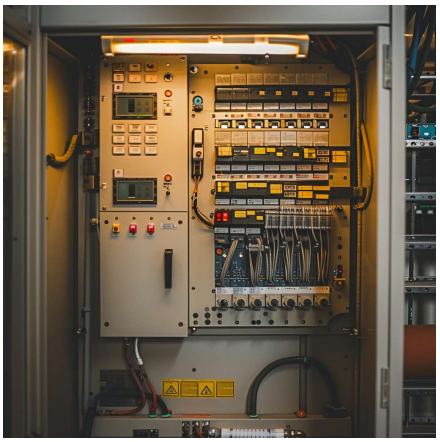


Image Source: AI generated on MidJourney on March 13, 2024

- Safety is traditionally NOT considered a cybersecurity task
  - PHA/HAZOP, FEMA, and LOPA are process safety evaluation techniques
  - ISA/IEC 62443 initial and detailed risk assessments meet these criteria, separately
- Vendors / integrators deploy and maintain
  - Consider example of rides at amusement parks where responsibility-lines with owner/operator blur
- Safety equipment *might* be air-gapped
  - Consider consequence prioritization if / when assets are connected to a network
- International standards, by sector, are trying to catch up
  - Consider ISA TR 84.00.09, Cybersecurity Related to the Functional Safety Lifecycle (approved April 10, 2017)
  - Consider ISO/TR 22100-4 "Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects"
  - ASTM F24 Cybersecurity for Safety-Related Controls Task Group

6

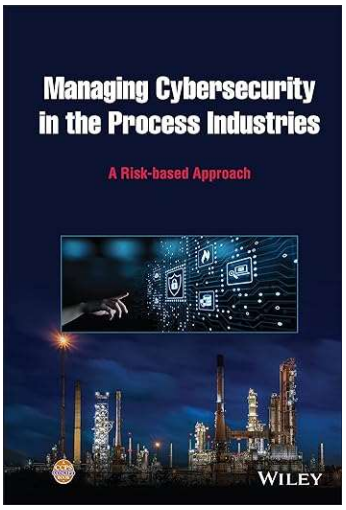
They Wrote a Book About This*

* I just bought it and started reading it

Managing Cybersecurity in the Process Industries: A Risk-based Approach

- By: Center for Chemical Process Safety
- https://www.amazon.com/Managing-Cybersecurity-Process-Industries-Risk-based/dp/1119861780

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.

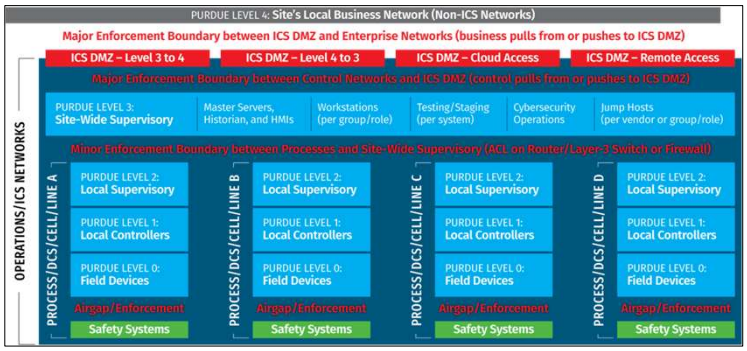


Starting the Architecture Conversation

- ISA/IEC 62443
  - Reference Models
  - Reference Architecture
  - Zone / Conduit Models
  - Risk Assessment Methodology
  - Detailed Risk Assessment

Image Source: AI generated on MidJourney on March 13, 2024

Reference Models



Reference Models establish a frame of reference for more detailed information about the IACS environment.

NOTE: The SANS ICS410 Reference Model is based on the ISA/IEC 62443 standards

Reference Architectures

Reference Architecture are diagrams that describe the physical and logical deployment of assets of an organization, location, or scope of evaluation.

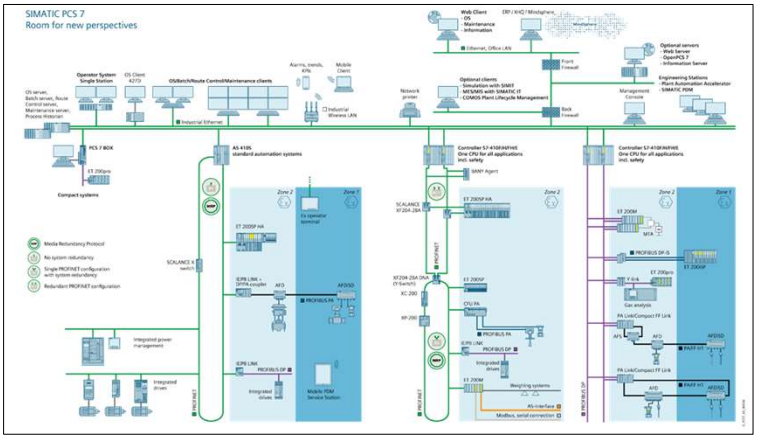
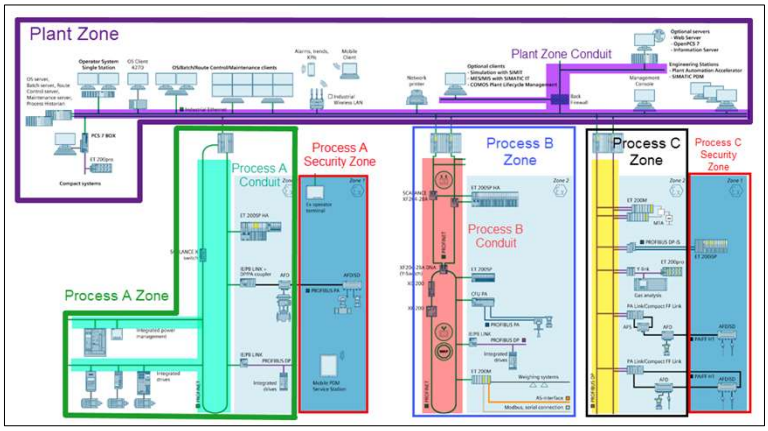


Image Source: Siemens architecture SIMATIC PCS7: https://www.automation.siemens.com/bilddb/download.aspx?reqInsID=1502504

Zone / Conduit Model



Zone / Conduit Models are logical groups of assets, typically nested, that define characteristics and communications of the assets which can be used to analyze security requirements.

ISA/IEC 62443-3-2
ZCR 3.3: Separate safety related assets

ZCR 3.3: Separate Safety-Related Assets

ZCR 3.3 "Separation of safety and related assets" refers to the process of ensuring that safety and related assets are isolated from other assets in the system under consideration (SuC). This is to reduce the risk of harm to human life in the event of a security breach. The results of the ZCR 3.3 phase should result in the safe and effective separation of safety and related assets within the SuC.

Image Source: https://novesh.com/blog/novesh-blog-7/understanding-iec-62443-3-2-zones-conduits-and-risk-assessments-27

ISA TR 84.00.09, Cybersecurity Related to the Functional Safety Lifecycle

Cyber Security Assessments (CSA) should be carried out that the following stages of a System-Under-Consideration's (SUC's) lifecycle:

- Stage 1: After the detailed risk assessment, countermeasure selection, and CSRS for the SUC has been developed to ensure the conceptual design reduces risk appropriately.
- Stage 2: After the IACS cybersecurity countermeasures have been integrated into project's conceptual design prior to construction, aka Cybersecurity Factory Acceptance Testing (CFAT).
- Stage 3: As a part of the Pre-Startup Safety Review (PSSR), aka Cybersecurity Site Acceptance Testing, to ensure the SUC is safe and secure for operations.
- Stage 4: Periodic or reactive activities during normal operations and maintenance of the SUC.
- Stage 5: As a part of change management and decommissioning of the SUC.

Two concerns drive cybersecurity safety considerations:

- Safety function failure to perform when needed
- Spurious operation that cause unauthorized activation, cause business interruption, or damage equipment

Physical safety considerations that are a part of the risk assessment process but not a part of the cybersecurity assessment consideration, for example:

- Safety controls not vulnerable to cyberattack
  - Other than validating they are not
- Hard wired interlock systems
- Pressure relief valves
- Check valves

Risk Assessment Methodology

Defined in ISA/IEC 62443-3-2

- High-Level Risk Assessment
  - Collects information about System Under Consideration (SUC)
  - Organizes SUC into Zones and Conduits
  - Completes documentation of SUC
- Detailed Risk Assessment
  - Vulnerability assessment of SUC's zones and conduits
  - Details unmitigated risk and countermeasures effectiveness to compare SL-A to SL-T
  - Provides actionable intelligence to produce CSRs

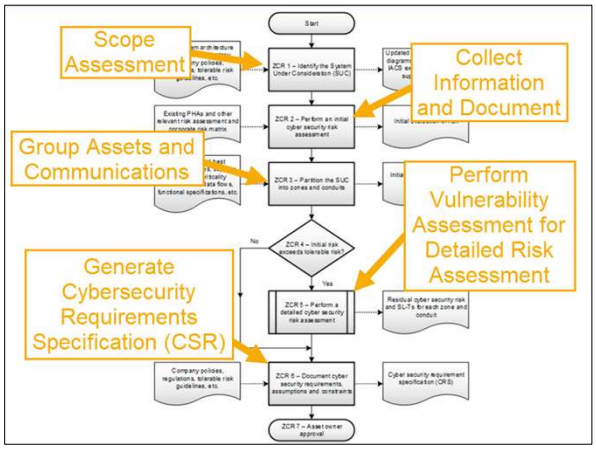


Image Source: White Paper Excerpt: Leveraging ISA 62443-3-2 For IACS Risk Assessment and Risk Related Strategies : https://gca.isa.org/blog/white-paper-excerpt-leveraging-isa-62443-3-2-for-iacs-risk-assessment-and-risk-related-strategies

Detailed Risk Assessment

Defined in ISA/IEC 62443-3-2

- Detailed Risk Assessment
  - Vulnerability Assessment
    - Security Assessment
    - Penetration Test
  - Compare Achieved Security Level (SL-A) to Target Security Level (SL-T)
  - Compare Residual Risk to Tolerable Risk
  - Identify and apply appropriate countermeasures
  - Document and Communicate

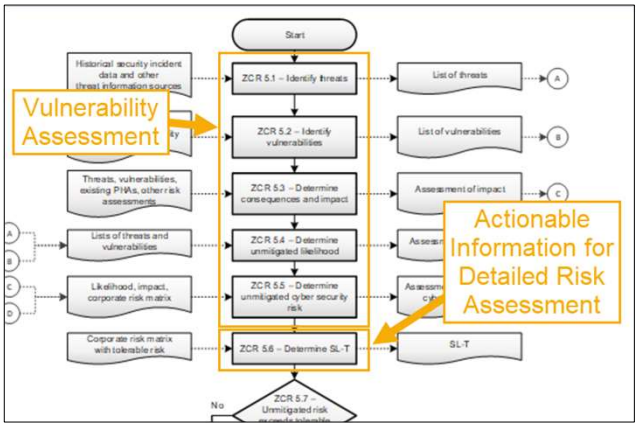


Image Source: White Paper Excerpt: Leveraging ISA 62443-3-2 For IACS Risk Assessment and Risk Related Strategies : https://gca.isa.org/blog/white-paper-excerpt-leveraging-isa-62443-3-2-for-iacs-risk-assessment-and-risk-related-strategies

Starting the Assessment Conversation

- SUC Assessment Information
- ISA/IEC 62443 Foundational Requirements
- SANS ICS Five Critical Controls

Image Source: AI generated on MidJourney on March 13, 2024

SUC Assessment Information

- System Under Consideration (SUC)
  - Name / Unique Identifier
  - Identify Stakeholders
  - Process / Environment Description
  - Assessment Goals
  - Safety and Criticality Description
  - List of Technologies
  - List of Deliverables
  - Timeframes
  - Locations
  - Testing Constraints

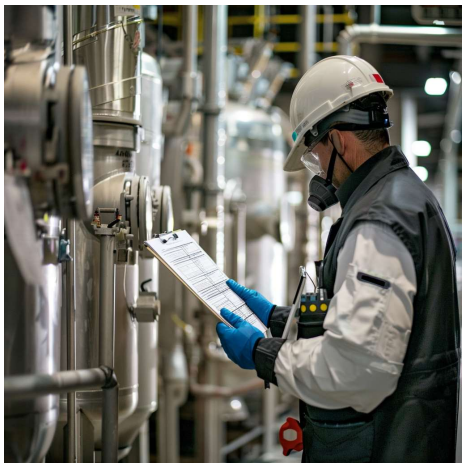
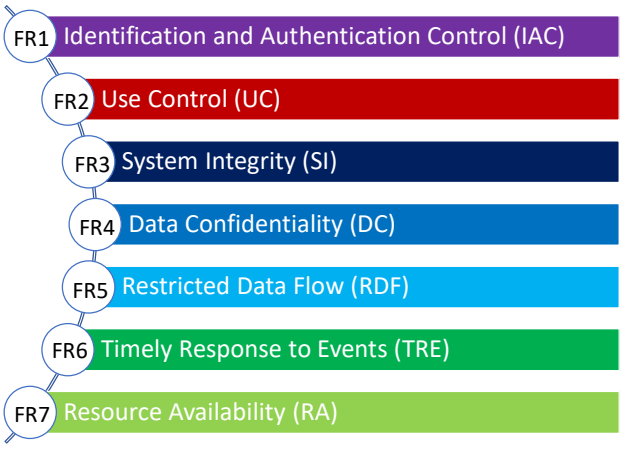


Image Source: AI generated on MidJourney on March 13, 2024

ISA/IEC 62443 Seven Foundational Requirements



SANS ICS 5 Critical Controls for ICS Cybersecurity

ICS INCIDENT RESPONSE
Operations-informed IR plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment

DEFENSIBLE ARCHITECTURE
Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs, process-communication enforcement

ICS NETWORK VISIBILITY MONITORING
Continuous network security monitoring of the ICS environment with protocol-aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control

SECURE REMOTE ACCESS
Identification and inventory of all remote access points and allowed destination environments, on-demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment

RISK-BASED VULNERABILITY MANAGEMENT
Understanding of cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact, or monitor for possible exploitation

Image Source: Five ICS Cybersecurity Critical Controls Whitepaper: https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

Safety Cybersecurity Assessment Focuses

- Secure Remote Access
  - Third-Party
  - Employees
  - Cloud
- Defensible Architecture
  - Network Segmentation / Isolation
  - Attack Surface
  - Communications
- Risk-Based Vuln Management
  - Hardware / Software Asset Inventory
  - Configuration Management
  - CISA KEVs
- ICS Network Monitoring
  - Countermeasure Efficacy Testing
- ICS Incident Response
  - Does your team understand the consequences of any of these things?

Image Source: AI generated on MidJourney on March 13, 2024

Multipart Summary

- Outsource Operations
- Quick Start vs Cybersecurity Program
- Incident Response

Image Source: AI generated on MidJourney on April 2, 2024

21

Outsourced Operations

Owners / Operators

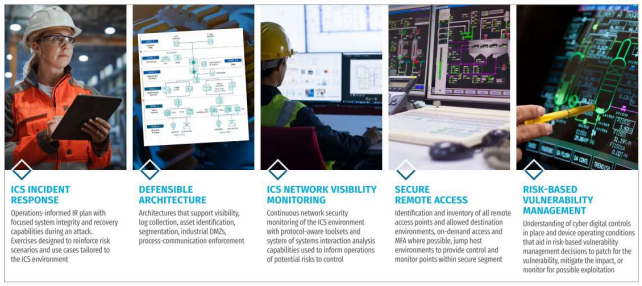
- YOU are ultimately responsible
- You MUST require vendors / integrators provide you cybersecurity details

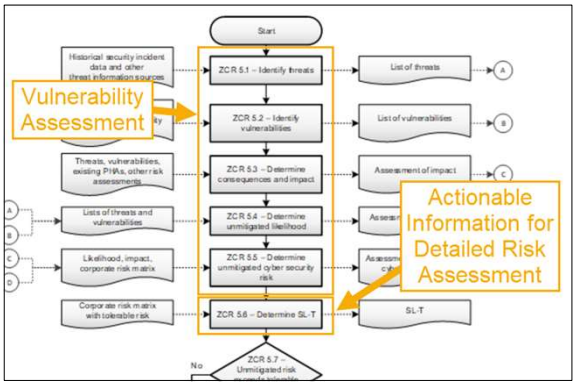
Vendors / Integrators

- You MUST provide details about cybersecurity to owners / operators

22

Quick Start vs Cybersecurity Program





Both Require a High-Level Risk Assessment to define team and scope.
Future standards will require more of vendors, integrators, and owner / operators.

Incident Response

Physical segmentation is ideal, as you can air gap and not impede functionality of the SIS should a threat warrant that response.- Gavin Dilworth (zDHD)

- You can island (i.e. remove remote access)

Prevention is ideal, but detection is a must; however, detection without response has minimal value. – SANS ICS410

Image Source: AI generated on MidJourney on April 2, 2024

CUTAWAY SECURITY
INFOSEC CONSULTANTS

Special Thank You To:

Gavin Dilworth (zDHD)
CutSec Discord
Beer-ISAC
Other OT/IT/Infosec Professionals

25

CUTAWAY SECURITY
INFOSEC CONSULTANTS

Don C. Weber - @cutaway
info@cutawaysecurity.com
https://www.cutawaysecurity.com
https://www.linkedin.com/in/cutaway/
Cutaway Security Discord

26