



# Tactical Risk Reduction in IACS Environments

Don C. Weber - @cutaway

Principal Consultant, Founder

© 2023 Cutaway Security, LLC. All Rights Reserved.

---



# Cutaway Security, LLC / Don C. Weber



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





# Agenda

- ISA/IEC-62443 Risk Assessments
- Strategic Vs Tactical Vulnerability Assessments
- Adapting the CutSec Cyber Vulnerability Assessment Methodology
- Cyber Vulnerability Assessment Reports
- Summary



# ICS62443 Risk Assessments - Requirement

- ISA/IEC-62443-3-2: Security risk assessment for system design
  - Perform a detailed cyber security risk assessment
    - Identify threats
    - Determine Consequence and Impact
    - Identify vulnerabilities
    - Determine unmitigated likelihood
    - Determine unmitigated cybersecurity risk
    - Determine Security Level Target (SL-T)
    - Compare unmitigated risk with tolerable risk
    - Identify and evaluate existing countermeasures
    - Re-evaluate likelihood and impact considering countermeasures
    - Determine residual risk
    - Compare residual risk with tolerable risk
    - Apply additional security countermeasures
    - Document and communicate results

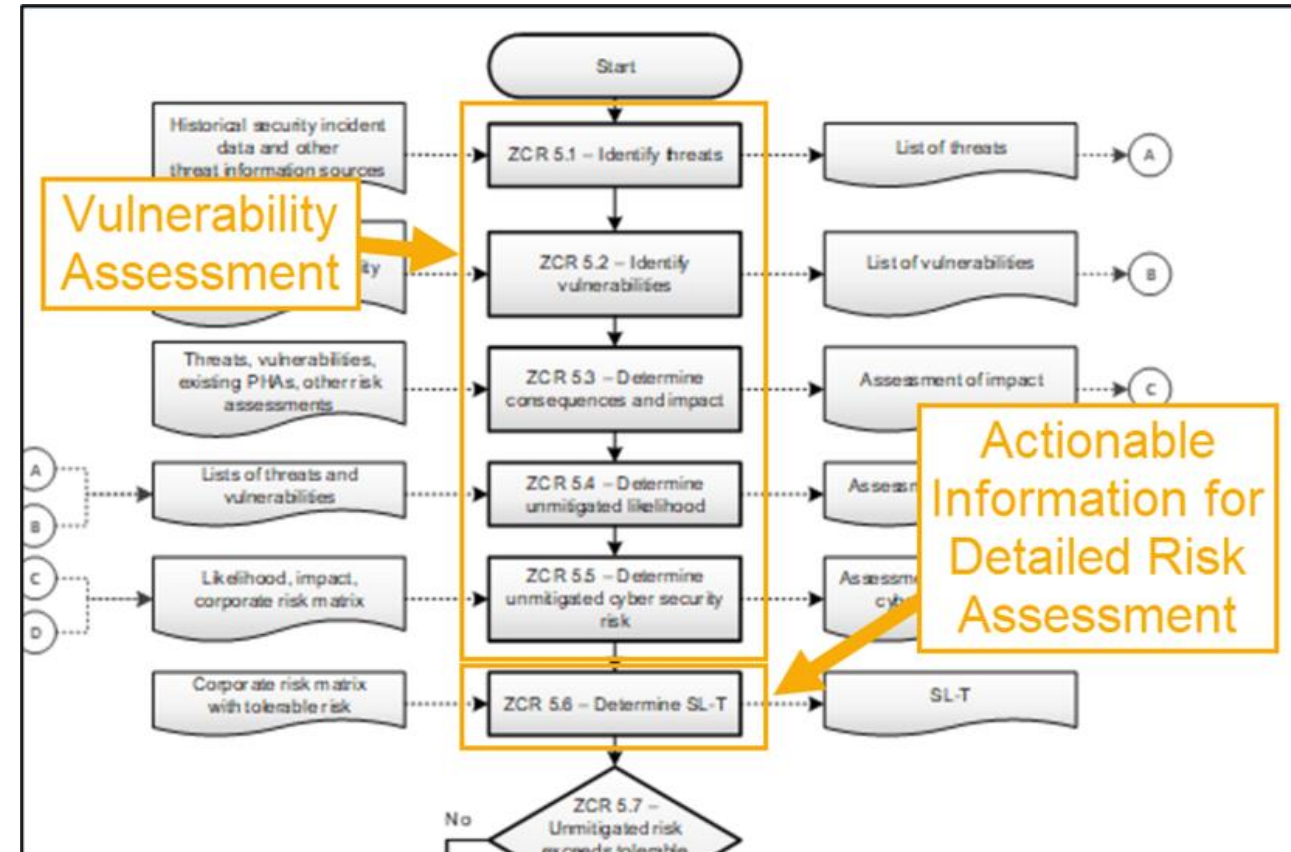
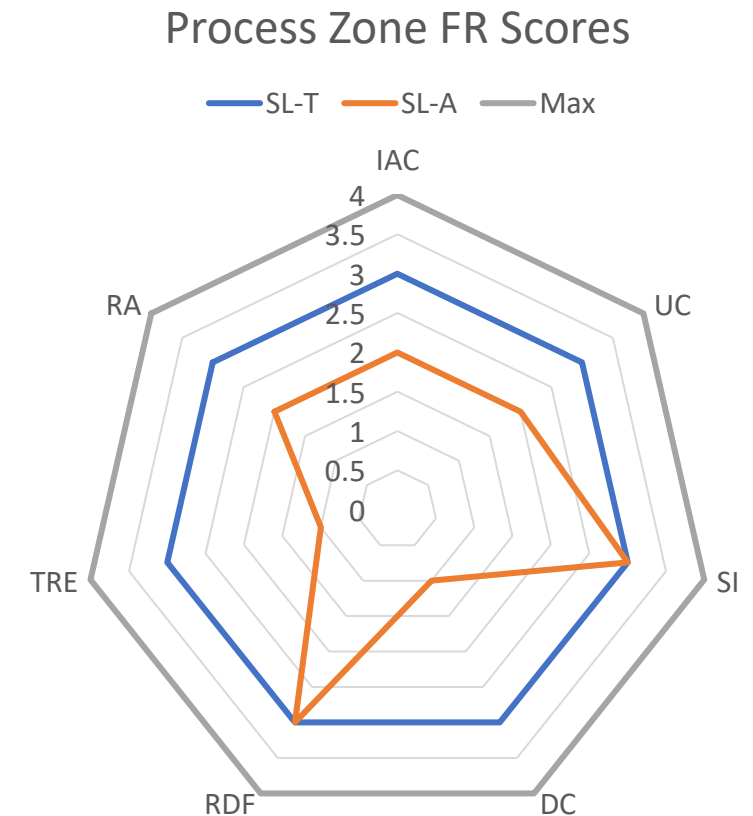


Image Source: White Paper Excerpt: Leveraging ISA 62443-3-2 For IACS Risk Assessment and Risk Related Strategies



# ICS62443 Risk Assessments - Implementation

- ISA/IEC-62443-3-3: System security requirements and security levels
  - Foundational Requirements (FRs)
    - Identification and authentication control (IAC)
    - Use control (UC)
    - System integrity (SI)
    - Data confidentiality (DC)
    - Restricted data flow (RDF)
    - Timely response to events (TRE)
    - Resource availability (RA)
  - Security Levels
    - SL 1 – ... protect against casual or coincidental access by unauthenticated entities.
    - SL 2 – ... protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation.
    - SL 3 – ... protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
    - SL 4 – ... protect against intentional unauthenticated access by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

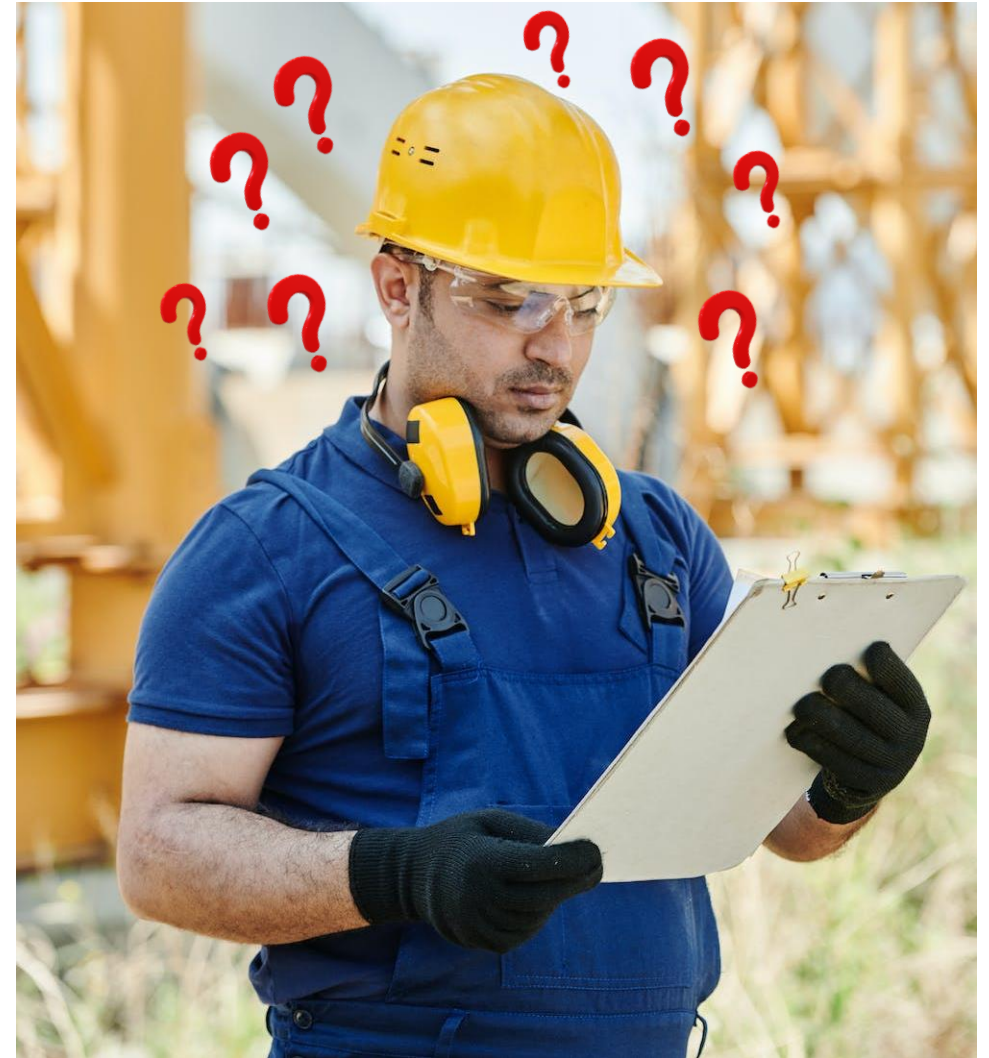






# Questions That Remain

- How do I safely gather cyber information about my process?
- How do I safely do a cyber security penetration test?
- What are these people going to be doing to my process?
- Fine, they find vulnerabilities, now what?
- Why don't you just tell me what to do?





# Strategic VS Tactical - Simplified

- Strategic decisions are designed to affect and affirm culture and address systemic issues.
- Tactical decisions directly impact the implementation of the physical processes.



Image Source: <https://sprigghr.com/blog/alignment-direction/strategy-vs-tactics-how-do-they-work-together/>



# Types of Cyber Vulnerability Assessments

- Defining and communicating types of assessments reduces confusion
- Select assessment types based on the organization's goals
- Risk and cost vary by goals and experience
- Assessment results should improve process operational requirements

Project Initiation Data +  
Vendor Review =  
High-Level Risk Assessment

OT Risk	Assessment Type	Estimated Cost
	Vendor Review	\$
	Security Research	\$ \$
	Threat Modeling	\$ \$
☢	Security Assessment	\$ \$ \$
☢ ☢	Security Program Maturity	\$ \$ \$
☢ ☢ ☢	Penetration Test	\$ \$ \$
☢ ☢ ☢ ☢	Red Team	\$ \$ \$ \$





# CutSec CloudSec-IACS High-Level Risk Assessment

<https://github.com/cutaway-security/CloudSec-IACS>

## IACS High-Level Risk Assessment for Cloud Products and Services

The introduction of a cloud service into an industrial / automation control environment requires a Cyber Security Management System (CSMS)<sup>1</sup> to manage risk by creating policies and procedures, assignment of organization responsibilities, planning and implementation of awareness training, and selection of countermeasures to be implemented by the owner / operator. The CSMS initial high-level risk assessment requires gathering information about the cloud service, some of which must be provided by the product / service provider. Information gathering is a team effort between the owner / operator and product / service provider. Here is a breakdown of responsibilities for providing information during the initial high-level risk assessment. Overall, the owner / operator is responsible for ensuring all the information collected is complete. The owner / operator's project owner should review the data and ask clarifying questions until each section is completed.

- Project Overview – Owner / Operator
- Cloud Service Description – Product / Service Provider
- Product / Service Foundational Requirements – Product / Service Provider
- Zone and Conduit Characteristics – Owner / Operator

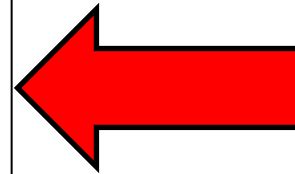
## Project Overview

Project Executive Sponsor	
Brief description of the project and cloud components	
Deployment Type	Testing Production Other:



# IACS Cyber Vulnerability Assessment Effort Prioritization

- Physical Security
- Segmentation and Isolation
- Access Control / Authorization
- Attack Surface
- Logging and Monitoring
- Asset Inventory
- Incident Response and Recovery



**Tactical IACS  
Security  
Starts Here**



# Vulnerability Analysis Via Process Familiarization

- Remote Scoping
  - Architecture Review
  - Basic Threat Modeling / Use Cases
  - Test Plan
- On-site
  - Site Walk Thru
    - Physical Security
    - Engineer / Operator Actions in Process
  - Interviews
    - Managers
    - Engineers / Operators / Programmers
    - IT Team
    - IT Security
  - Network Traffic Capture and Analysis
  - Attack Surface Enumeration
    - Network
    - System / Device Configuration
  - Asset Management
- Remote Reporting

Taught to me by two major, unrelated, Electrical Utilities

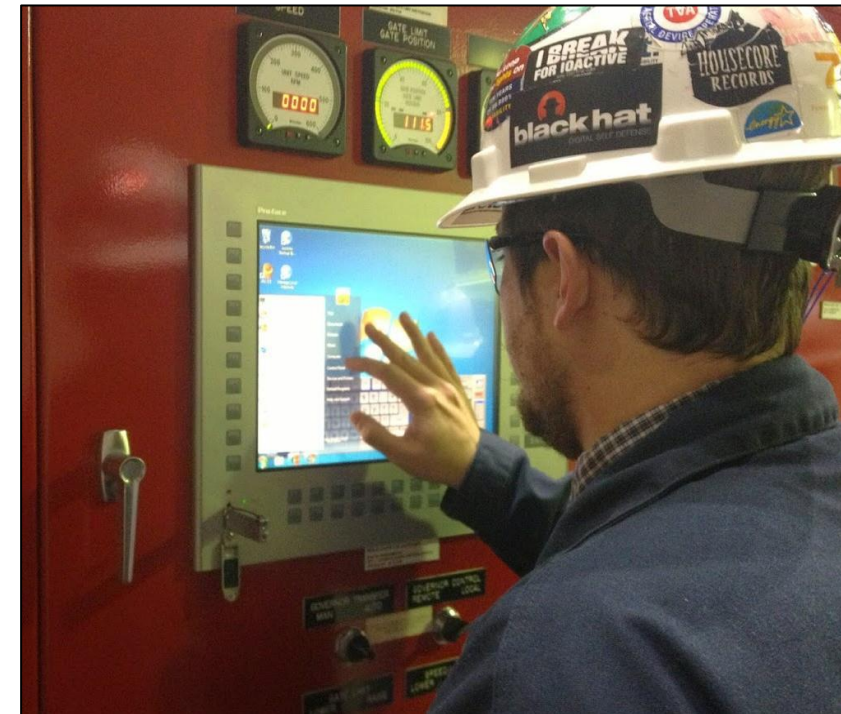
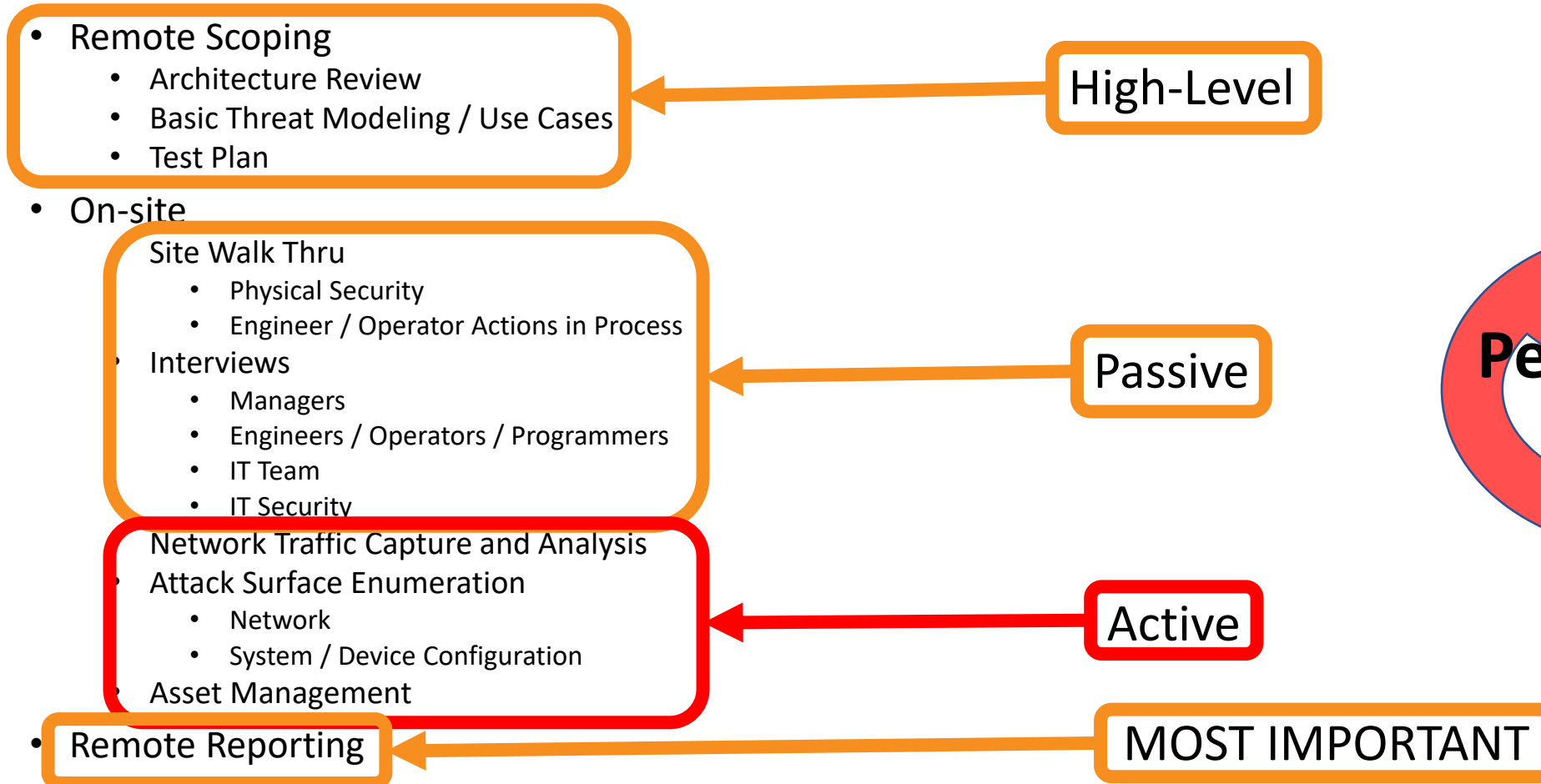


Image Source: <https://www.controlthings.io/> - Accessing and Exploiting Control Systems



# ISA/IEC-62443 Vulnerability Assessment Types



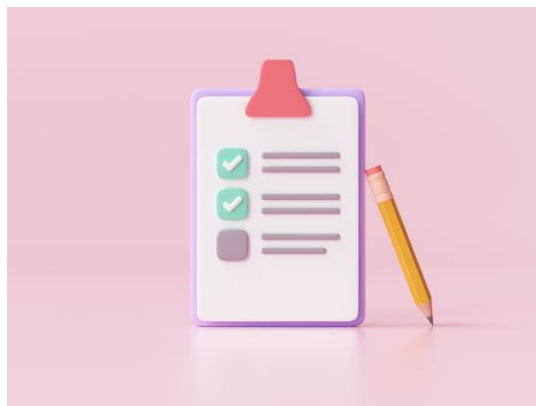


# Cyber Assessment Reports

Taught to me by two major, unrelated, Electrical Utilities

- Traditional Assessment Report

- Executive Summary
- Scope
- Methodology
  - Detailed Activity Log
- Findings
  - Observation
  - Risk
  - Recommendations
- Summary / Conclusion
- Supporting Data



- IACS Cyber Assessments

- Activity Log
  - Secondly provides details about assessment activities.
  - Primarily provides details about activities that made changes or left artifacts. For clean-up.
- Findings
  - Observation
  - Risk
  - Consequences
  - Recommendations





# IACS STAR Methodology

## IACS System Testing and Assessment Rating Score Calculator

### Likelihood Factors

#### Threat Actor Factors

##### Skill Level

5 - Advanced IT, moderate network, and

##### Motive

3 - Physical and remote access is possibl

##### Opportunity

3 - Physical and remote access is possibl

##### Size

8 - Physical malicious users

Threat Actor Factor:  
Medium (TAF: 4.75)

#### Vulnerability Factors

##### Ease of Discovery

2 - Requires physical access to environm

##### Ease of Exploit

3 - Denial-of-Service possible but no coc

##### Awareness

3 - Not publicly known but common con

##### Intrusion Detection

3 - Centrally logged with alerts and form

Vulnerability Factor: Low  
(VF: 2.75)

### Consequence Factors

#### Technical Impact Factors

##### Loss of Confidentiality

4 - Minimal network configuration data l

##### Loss of Integrity

2 - Modification of historical data used fr

##### Loss of Availability

8 - All production services completely lo

##### Loss of Accountability

2 - Central logging, Multifactor Authenti

Technical Impact Factor:  
Medium (TIF: 4)

#### Safety Impact Factors

##### Environment Damage

3

##### Process Damage

4 - Device damaged requiring manual up

##### Safety Equipment

6 - Safety equipment vulnerable and ren

##### Recoverability

1 - Process will automatically recover wit

Safety Impact Factor:  
Medium (SIF: 3.5)

Likelihood Factor: Medium (LF: 3.75)

Consequece Factor: Medium (CF: 3.75)

Overall Risk Severity: Medium

Score Vector: (SL:5/M:3/O:3/A:8/EA:2/EE:3/AW:3/DR:3/LC:4/LI:2/LA:8/LAC:2/ED:3/PD:4/SE:6/R:1)

- [https://github.com/cutaway-security/IACS\\_STAR\\_Methodology](https://github.com/cutaway-security/IACS_STAR_Methodology)
- <https://iacs-star-calculator.com/>



# Distribute Cyber Vulnerability Assessment Reports

- Identify Partner Organizations to Share Reports (ISACs / Munis / Co-ops?)
- For Each Cyber Assessment
  - Generate a sanitized report of findings and recommendations
  - Distribute to other business units / process owners in your organization
  - Distribute to partner organizations
- Receiving Sanitized Cyber Assessment Reports
  - Distribute to other business units / process owners in your organization (quarterly?)
  - Require leaders to review assessments with their teams and provide summary of comments or actions taken



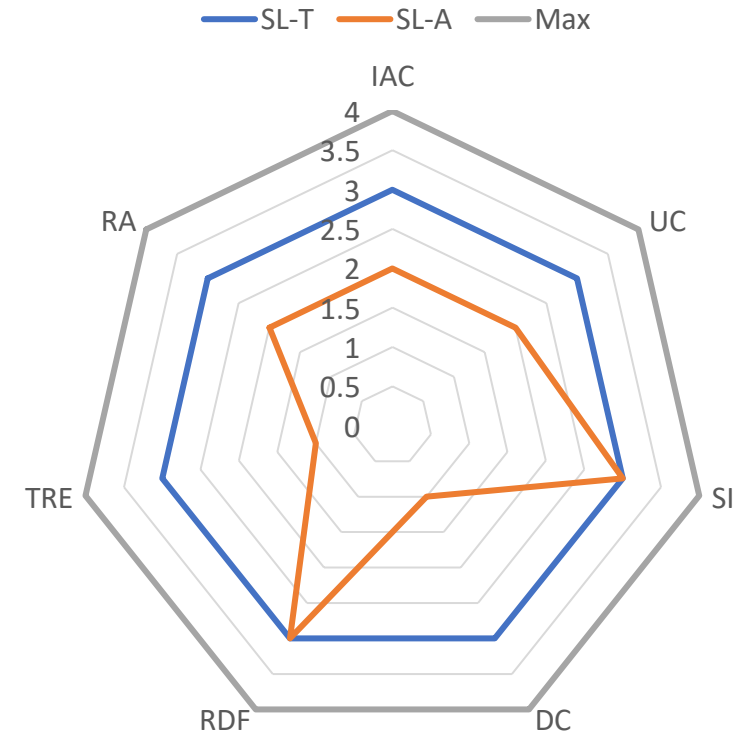


# ISA/IEC-62443 Risk Assessments

## Strategic

- ISA/IEC-62443-3-3: System security requirements and security levels
  - Foundational Requirements (FRs)
    - Identification and authentication control (IAC)
    - Use control (UC)
    - System integrity (SI)
    - Data confidentiality (DC)
    - Restricted data flow (RDF)
    - Timely response to events (TRE)
    - Resource availability (RA)
  - Security Levels
    - SL 1 – ... protect against casual or coincidental access by unauthenticated entities.
    - SL 2 – ... protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation.
    - SL 3 – ... protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
    - SL 4 – ... protect against intentional unauthenticated access by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

Process Zone FR Scores





# Summary

- Tactical Vulnerability Assessments help teams become familiar with the cyber security risk assessment process.
- Tactical Vulnerability Assessments are designed to QUICKLY identify gaps for teams to plan with vendors / integrators.
- Tactical Vulnerability Assessments feed information into the ISA/IEC-62443 Detailed Risk Assessment.
- Risk Assessments MUST still be performed after the Vulnerability Assessment and should be done following the ISA/IEC-62443 standards.
- Distribution and review of sanitized reports are like a **FREE** Vulnerability Assessment.



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



### ICS410 ICS/SCADA Security Essentials

A mix of hands-on and theoretical class, being driven by a high skilled instructor, makes this the best training in ICS security.

**Rafael Issa, Technip**

#### About the course

ICS410 is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

**REGISTER TODAY**



ICS410 Challenge Coin