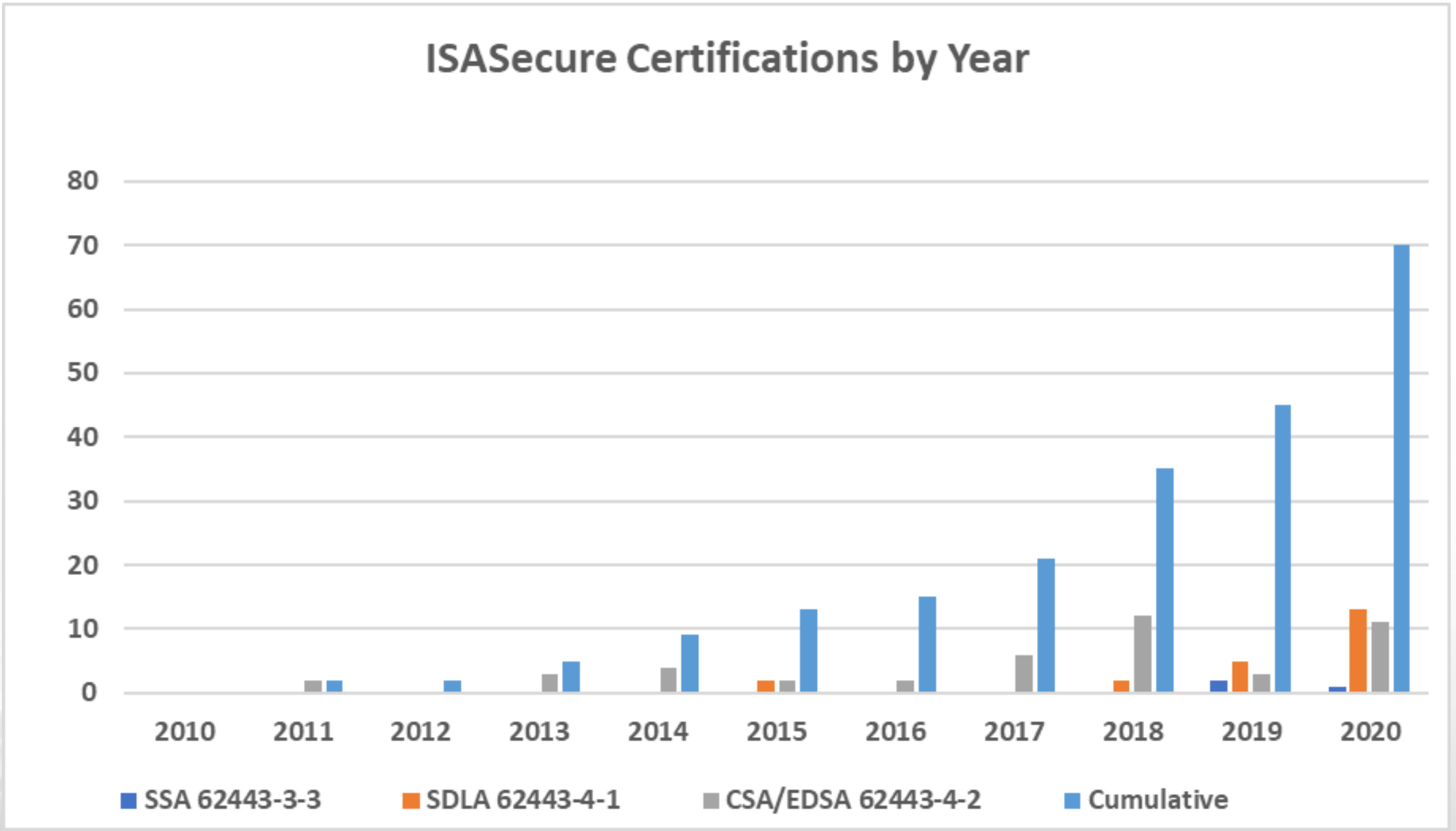
Applied Risk | Critical Infrastructure Made Secure.

Industrial security trends and adoption of IEC 62443

February 17th, 2021

Classification: restricted

ISASecure®



ISASecure®

ISASecure Certifications in Calendar Year 2020

SDLA – Development Lifecycle Certification
ISA/IEC 62443-4-1

1. Emerson Austin, TX
2. Emerson Pittsburgh, PA
3. Emerson Manilla, Philippines
4. ABB Cleveland, OH
5. ABB San Jose, CA
6. ABB Malmo/Vasteras Sweden
7. Honeywell Process Solutions Companywide Phoenix, AZ
8. Johnson Controls Inc Companywide (Cork Ireland)
9. Wartsila Herndon, VA
10. Schneider Electric Lake Forest, CA
11. Schneider Electric Company Wide (Rueil-Malmaison, France)
12. Yokogawa Musashino Tokyo Japan
13. GE Power Conversion Rugby England

SSA – System Certification
ISA/IEC 62443-3-3

1. Emerson DeltaV

CSA/EDSA – Component Certification
ISA/IEC 62443-4-2 & 4-1

1. Honeywell PLC
2. Honeywell Safety Manager
3. Honeywell Safety Manager SC
4. Honeywell Control Edge RTU
5. GE Power Controller
6. ABB Controller
7. ABB Safety controller
8. ABB DCS Controller
9. Schneider Electric Triconex TCM
10. Schneider Electric Tricon Comm Module
11. Schneider Electric Tricon Comm Module 695
12. Wartsila Power Plant Controller

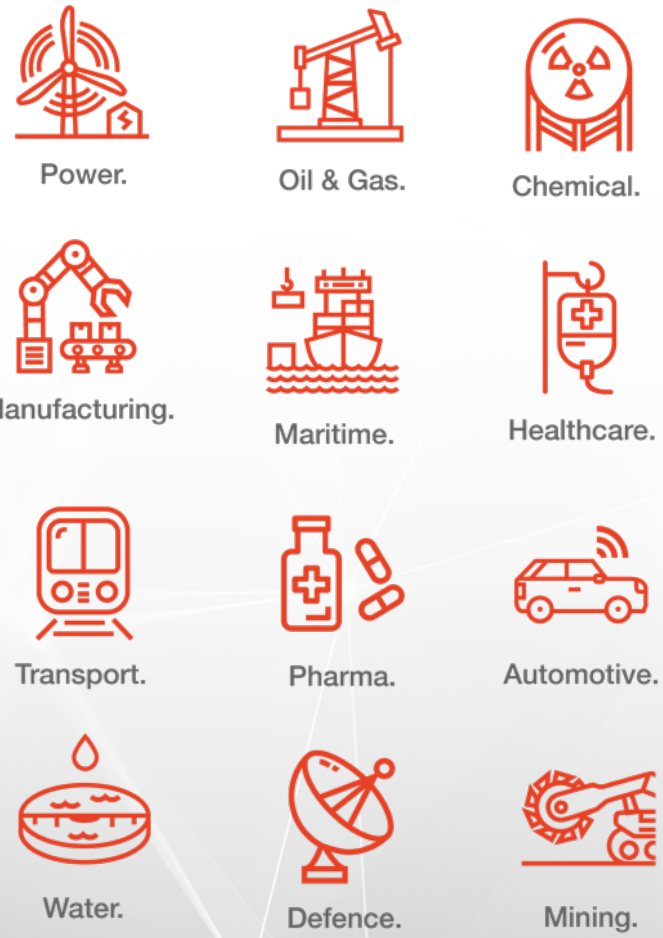
ISASecure®

About Applied Risk

Applied Risk provides cyber security solutions for securing critical infrastructures, including Industrial Control Systems (ICS) and Industrial Internet of Things (IIoT).

Due to our extensive knowledge and experience we are creating safe, secure and reliable solutions for end users and suppliers throughout the whole lifecycle of their assets.

Our solutions are available worldwide.



CREST

ISASecure®

Who We Are

Chris Sandford
Director OT Security Services

Karl Williams
Head of OT Security Services

State of Industrial Cyber Security 2020 Report

This presentation discusses the findings from “The State of Industrial Cyber Security 2020” report, which was based on:

- Applied Risk’s technical and non-technical assessments
- Examination of third-party material
- Consultation with specialists in OT security.

Deliverables from this work include a 34-page report with findings, field observations and practical recommendations for the industry.

https://applied-risk.com/resources/the-state-of-industrial-cyber-security-2020

Agenda

01 Introduction

02 Top Trends in OT Security

03 Research findings and field observations

04 IEC 62443 adoption and how industrial security frameworks are affected

05 Recommendations and IEC 62443 adoption for securing OT

06 Q&A

Top Trends in OT Security

Top Industrial Cybersecurity Trends

Market Trends

- Mergers & Acquisitions
- Investment in OT security
- Maintaining core operations
- Insurance

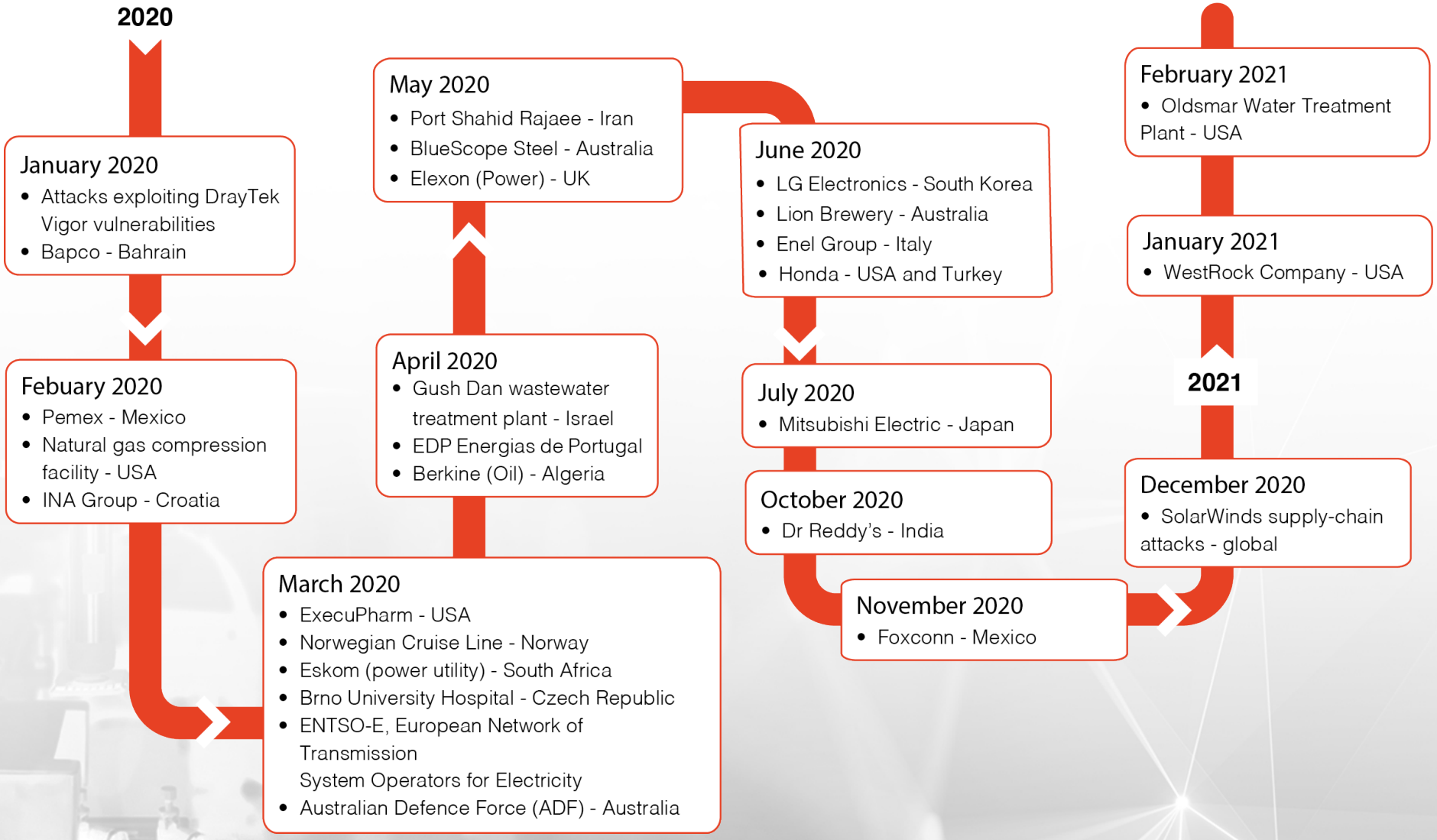
Technology Trends

- IT/OT Convergence
- Cloud Adoption
- Remote Access

Ongoing Trends

- OT security skills shortage
- Shadow OT
- Compliance: laws and regulations

Attacks in Industrial Sectors



Research Findings and Field Observations

Field Operations

Top 5 Technical Observations

1. Outdated and vulnerable software

The use of unpatched and unsupported operating systems and software remains one of the primary challenges encountered in the field.

2. Inadequate network segmentation

A large discrepancy in the segmentation approaches between IT and OT networks has been observed.

3. Weak access control

This issue was observed of both physical and logical access control and can become agravated with the rise of remote access.

4. Focus on protecting rather than detecting and responding

OT managers often lack focus on detection and response to suspicious activities in their networks and on hosts.

5. Cutting corners

Lack of a formalised configuration management method and deployment with insufficient security controls are some examples of issues observed.

Field Operations

Top 5 Non-Technical Observations

1. Governance

Responsibilities related to OT security are often poorly defined and clear company wide policies rarely exist.

2. Knowledge management

Knowledge of OT processes and measures is often neither properly documented nor shared between colleagues and departments.

3. Poorly defined supplier requirements

The lack of OT security requirements defined to vendors and suppliers is causing security gaps.

4. Lack of strong OT security culture

Regular OT security training is not provided or limited, or is provided but poorly reinforced.

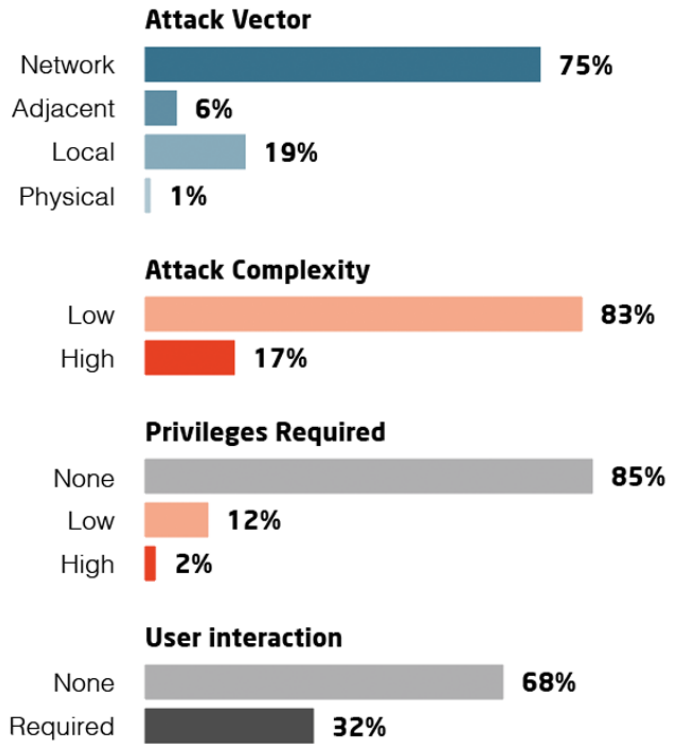
5. OT Security during greenfield and brownfield projects

When adding, modifying or upgrading a system, OT security is often regarded as an afterthought during a project.

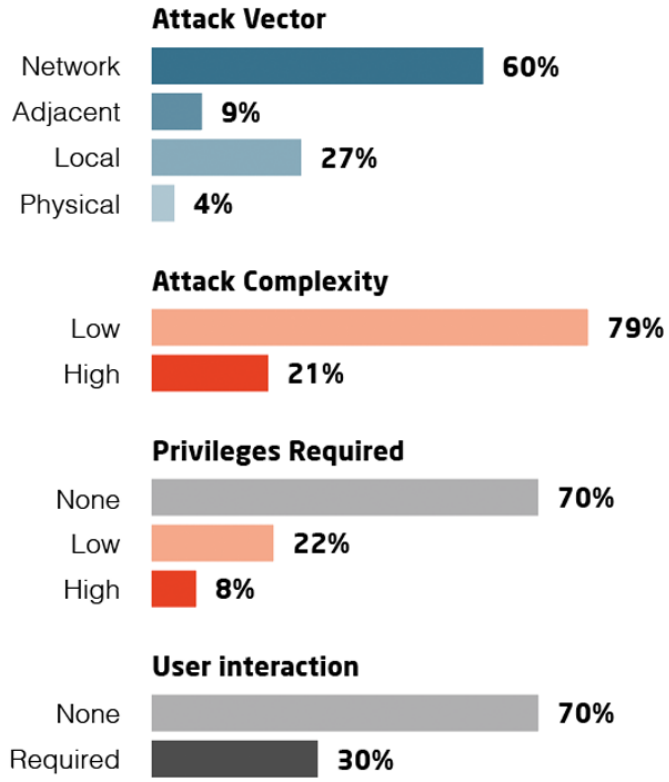
Vulnerability Metrics

Based on CVSS v3 scores from ICS-CERT

2018



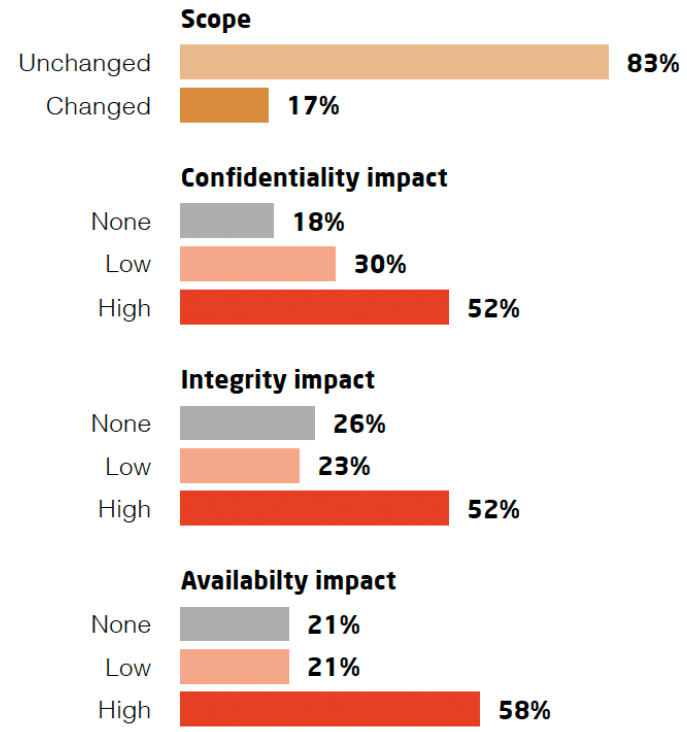
2019



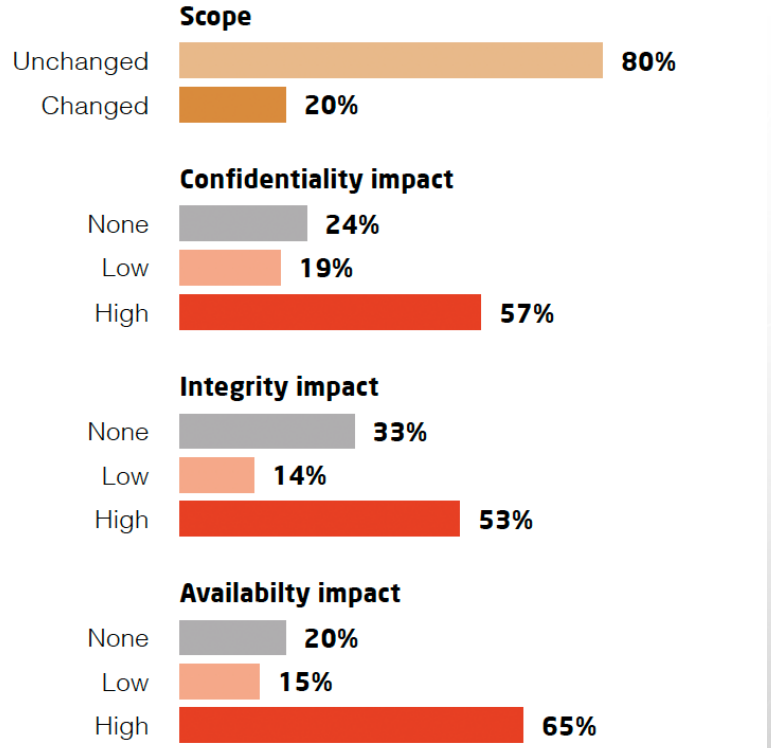
Vulnerability Metrics

Based on CVSS v3 scores from ICS-CERT

2018



2019

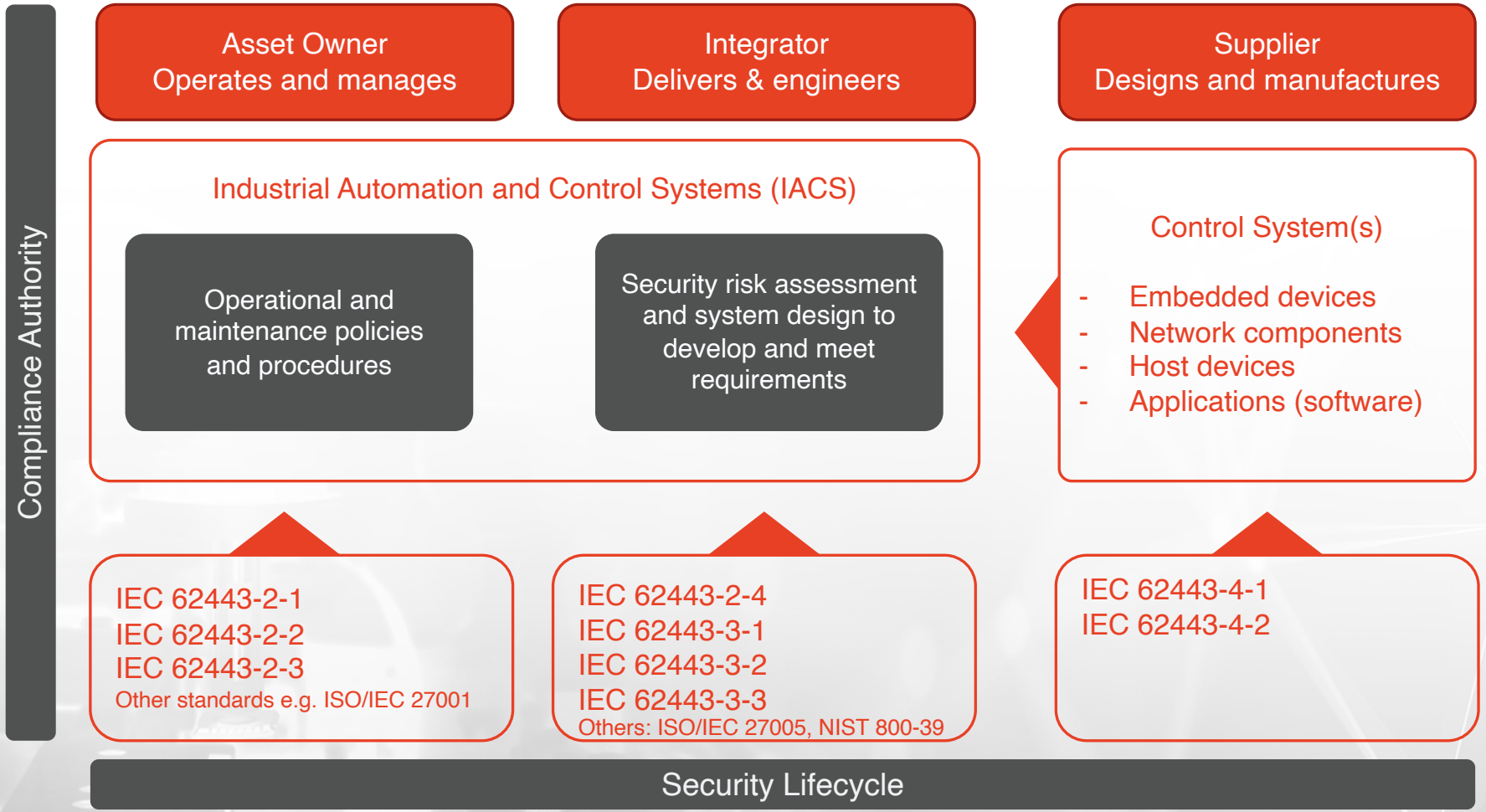


Conclusion

The main challenges observed in the field continue to stem from deficiencies in governance. Clear ownership must be properly defined in order to drive all the OT security improvements in the organisation within a strategic framework and maintain such commitment over the long term

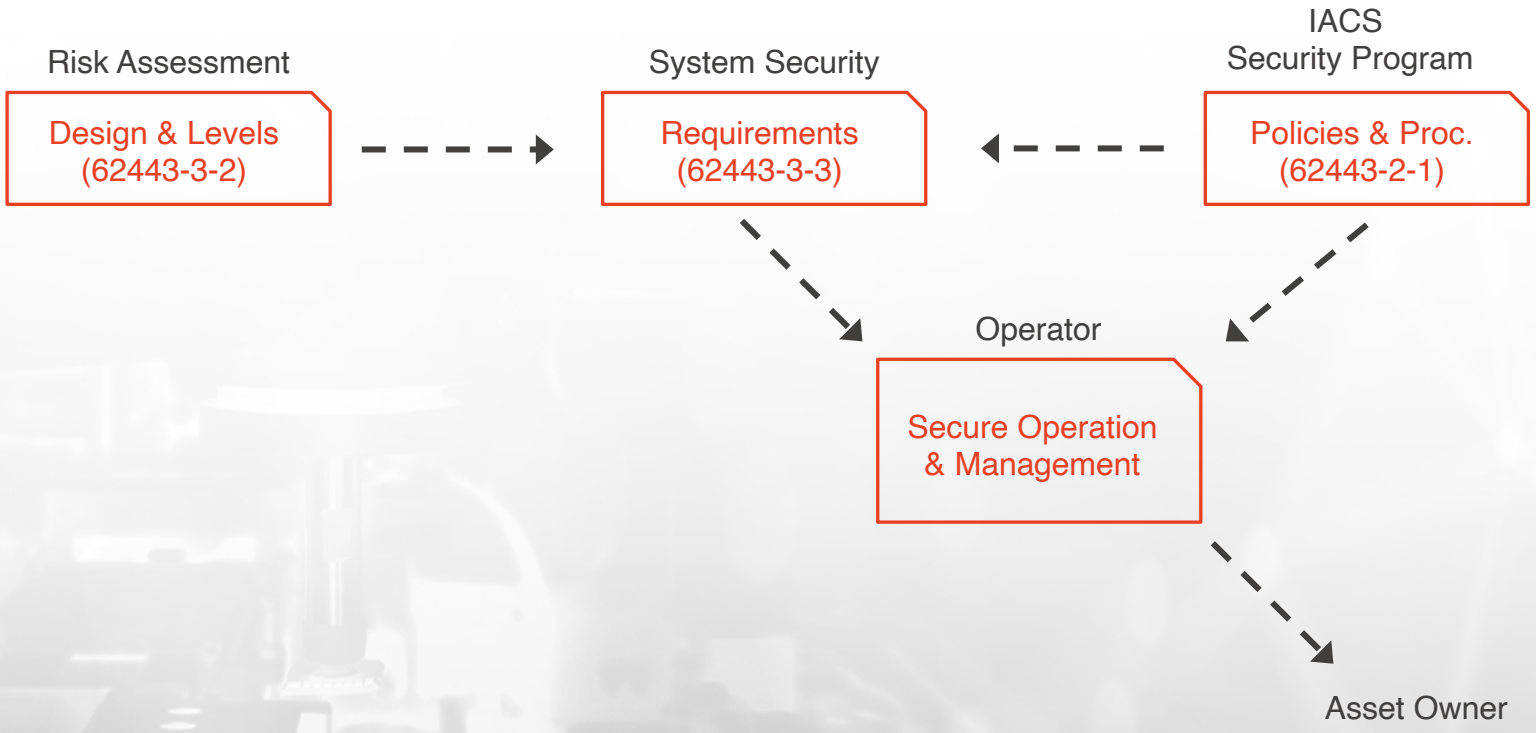
IEC 62443 Adoption and How Industrial Security Frameworks are Affected

IEC-62443 Series of Standards



Asset Owner, Operator (End User)

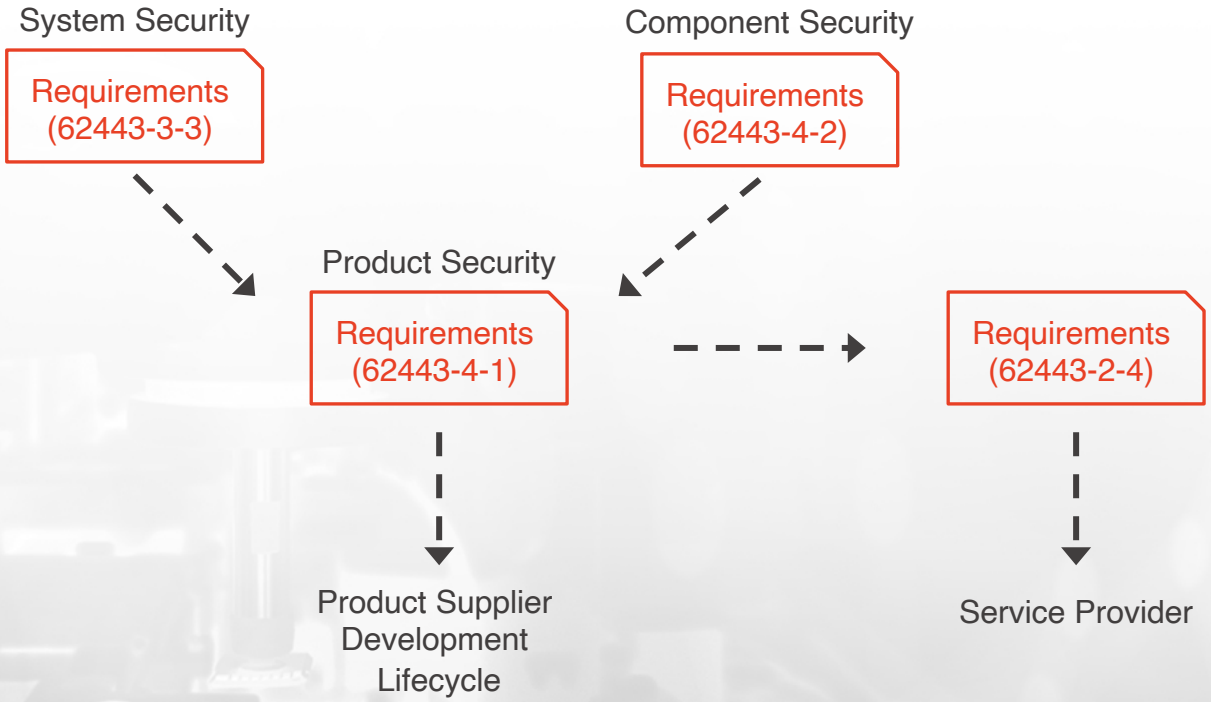
Framework Considerations



- Risk Assess (initial or detailed)
  - Threats
  - Initial or Detailed
- System Design
  - Zone & Conduit Model
- System Security Requirements
- Compliance Assessment
  - Internal
  - Regulatory Assessment
- Security Risk Management

Suppliers/Vendors/System Integrators

Framework Considerations



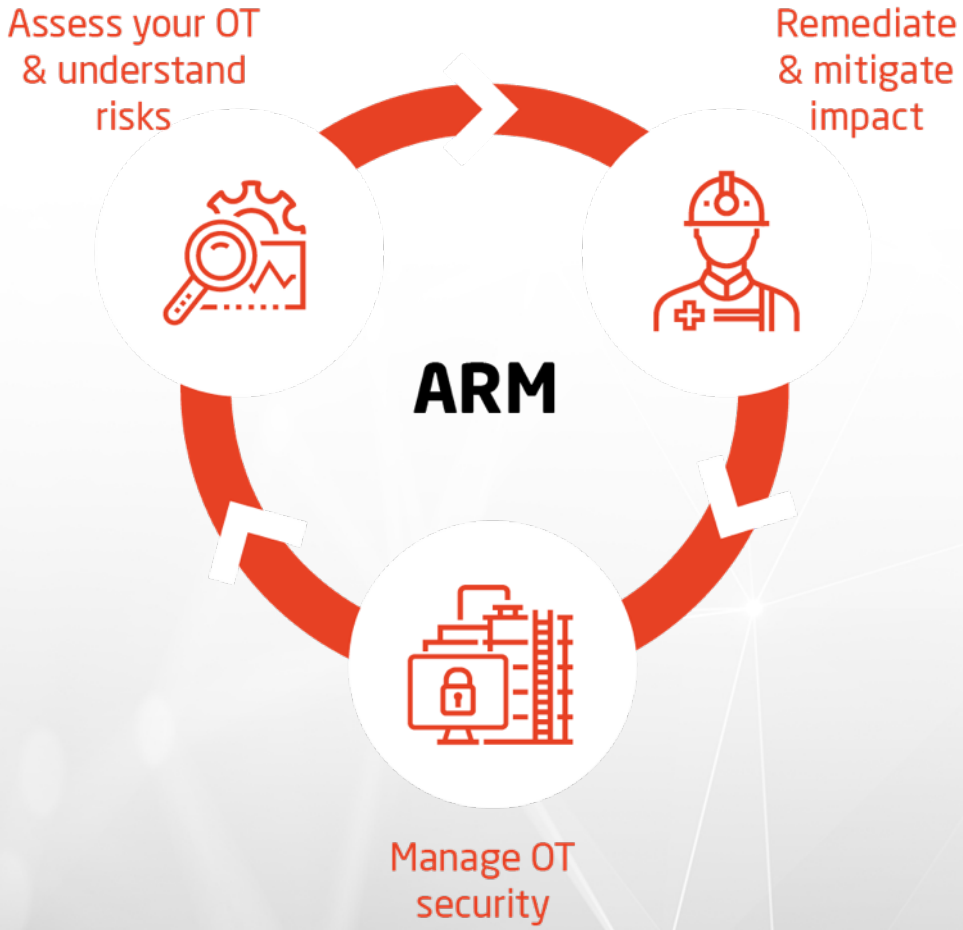
- Defined security requirements
- Security vulnerability assessments
  - Supply chain
  - Software applications & hardware
  - Functional security
- Validation against security requirements
  - Technical (penetration) testing pre-acceptance (FAT/SAT)
  - Implementation (post acceptance)

Recommendations and IEC 62443 Adoption for Securing OT

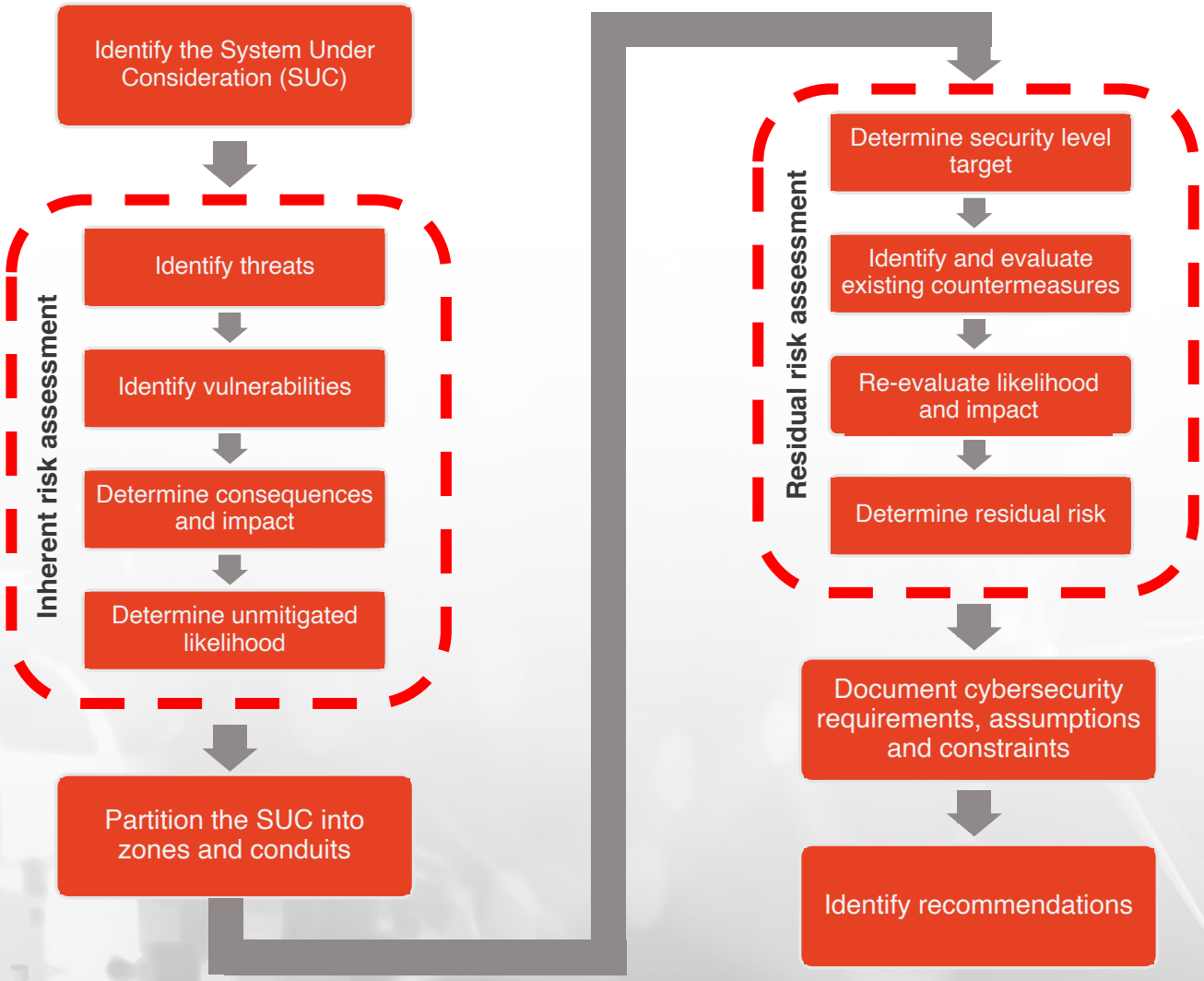
ARM™

Building a long-term OT security strategy

- **Assess:** Understand the current security posture, security framework, assets and criticality within a facility.
- **Remediate:** Develop a prioritised approach to overcoming or eliminating the security vulnerabilities.
- **Manage:** Ability to securely manage the OT infrastructure, and to maintain and improve the cyber security processes.



Risk Assessment Methodology



Risk Assessment Matrix

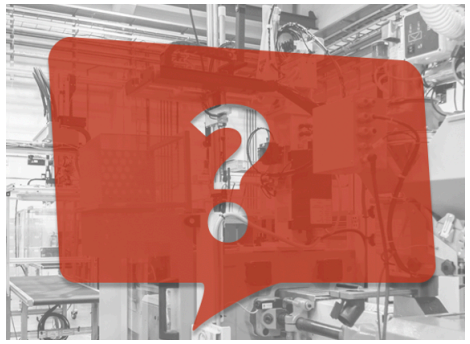
Alignment to Security Level (Target) – Prioritisation based on Criticality and Impact

Inherent Risk Rating	SL-T Ranking
Low	SL-1
Medium	SL-2
High	SL-3
Very High	SL-4

SDL Practice Areas – ISA/IEC 64443-4-1

1	Security Management (SM)	The purpose of the security management practice is to ensure that the security-related activities are adequately planned, documented and executed throughout the product's lifecycle
2	Specification of Security Requirements (SR)	The processes specified by this practice are used to document the security capabilities that are required for a product along with the expected product security context
3	Secure by Design (SD)	The processes specified by this practice are used to ensure that the product is secure by design including defense in depth.
4	Secure Implementation (SI)	The processes specified by this practice are used to ensure that the product features are implemented securely.
5	Security Verification and Validation Testing (SVV)	The processes specified by this practice are used to document the security testing required to ensure that all of the security requirements have been met for the product and that the security of the product is maintained when it is used in its product security context.
6	Security Defect Management (DM)	The processes specified by this practice are used for handling security-related issues of a product that has been configured to employ its defense in depth strategy (Practice 3) within the product security context (Practice 2)
7	Security Update Management (SUM)	The processes specified by this practice are used to ensure security updates associated with the product are tested for regressions and made available to product users in a timely manner
8	Security Guidelines (SG)	The processes specified by this practice are used to provide documentation that describes how to integrate, configure, and maintain the defense in depth strategy of the product in accordance with its product security context

Polls



- Have you carried out a Risk Assessment in the past two years?

a. Yes

b. No

c. Currently under consideration

- From the top 5 technical issues observed, which one is most affecting your organisation?

a. Outdated and vulnerable software

b. Inadequate network segmentation

c. Weak access control

d. Focus on protection rather than detecting and responding

e. Cutting corners

Questions?

Applied Risk | Critical Infrastructure Made Secure.

Contact

+31 (0) 20 844 4020

csandford@applied-risk.com

kwilliams@applied-risk.com

www.applied-risk.com

Amsterdam The Netherlands