Cybersecurity

Operation Technology (OT)

How to navigate successfully in a multivendor and multisite world

Productie Proces Automatisering

25 januari 2024 | Van der Valk Hotel, Vianen

Ari Rajamäki

- Product Manager, Cybersecurity at Valmet
  - LinkedIn @arajamak
  - Cyber security Engineer, Master of Engineer at JAMK University of Applied Sciences 2021

- Valmet - a leading global developer and supplier of process technologies, automation and services for the pulp, paper and energy industries https://www.valmet.com/
  - Automation ICS/DCS/IIoT technology and service Vendor

GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL GICSP

ISA/IEC 62443 CYBERSECURITY FUNDAMENTALS SPECIALIST ISA

ISA/IEC 62443 CYBERSECURITY RISK ASSESSMENT SPECIALIST ISA

Overview of presentation

- OT Cybersecurity threat landscape, Cybercrime vs Cyberwarfare
- EU Regulations NIS2 (Network and Information Security) and CRA (Cyber Resilience Act)
- IEC 62443 and risk management
- ICS/DCS technology and service vendor experience ongoing cybersecurity program targets and countermeasure improvements

Ransomware attacks vs Known attacks OT

Ransomware 2023

- LockBit:
  - The most active ransomware gang in 2023, with 273 victims named on leak sites in Q1 of 2023
- Clop:
  - Leaked 102 victims in Q1 of 2023
- BlackCat (AlphV):
  - Responsible for 87 listings on leak sites2
- RagnarLocker:
  - Targeted several companies worldwide in 2023

A ransomware-as-a-service (RaaS) that targeted several companies worldwide in 2023

- Avaddon
- Conti
- DarkSide
- Egregor
- Mespinoza
- NetWalker

10 most known OT cases

- **Stuxnet 2010**
- **Ukraine** power grid attack 2015
- **NotPetya** 2017
- TRITON 2017
- Dragonfly 2018
- GreyEnergy 2018
- LockerGoga 2019
- Ryuk 2019
- **WannaCry 2017**
- SolarWinds 2020

NIS2 requirement and obligations

secure processes

Areas of NIS2:

- Risk management
- Corporate accountability
- Reporting obligations
- Business continuity

Measures to minimize cyber risks:

- Incident management
- Supply chain security
- Enhanced network security
- Access control and encryption

CRA Cyber Resilience Act

product security

Targets of CRA:

- Obligations for manufactures of Products of Digital Elements
- Hardware and Software whole lifecycle
- Criticality and important categories?

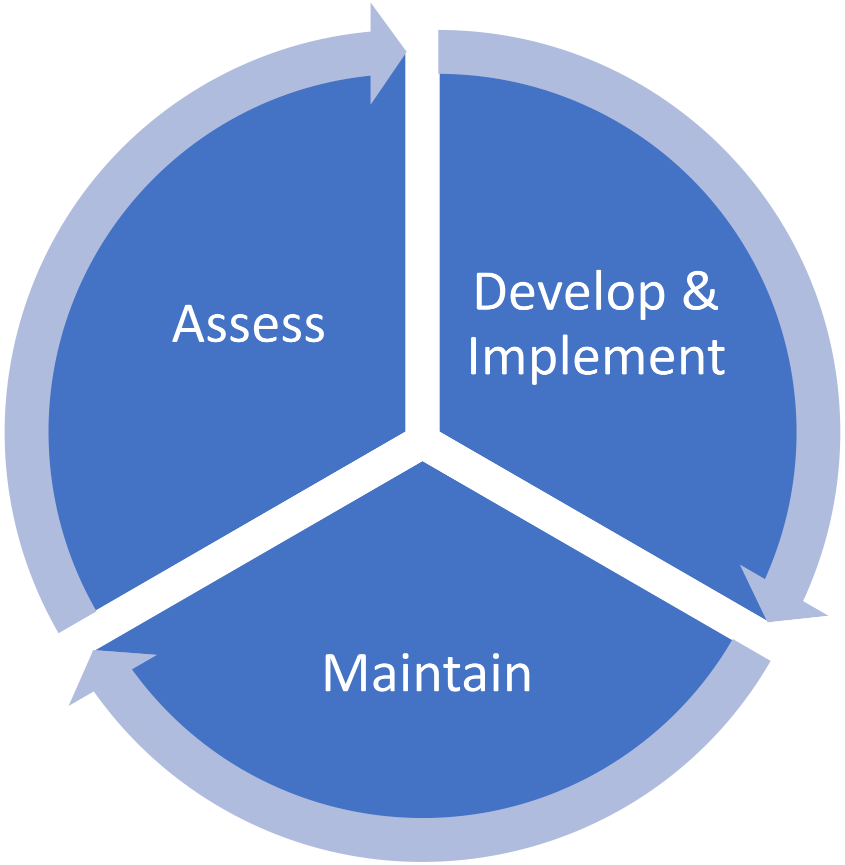
Elements in CRA:

- Secure design and assessments
- Vulnerabilities notifications
- Incidents notifications
- Penalties of non-compliance

IEC62443 Cyber Security Management System

- The security life cycle ISA 62443
  - Assess phase
  - Develop and Implement phase
  - Maintain phase

- Cybersecurity Management System
  - Continuous Processes
  - Policies, Procedures, Training and Awareness
  - Periodic Cybersecurity Audits



IACS IEC62443 Cybersecurity

Assess Phase

- Defining System Under Consideration (SUC) into **Zones and Conduits**
- **Assessing risk** for each Zone and Conduit
  - Use threats and vulnerability scenarios
  - Define Security Level Targets (Zone and Conduits)
- Documentation and Security requirements to **improve**
  - OT Asset list and System diagrams
  - Corporation policies and processes
  - **Cybersecurity Requirement specification**

High-Level Cyber Risk Assessment

what might be the impact of general types of cyber security vulnerabilities and the likelihood that a threat might exercise these vulnerabilities

Allocation of IACS Assets to Security Zones and Conduits

defining a security zone, an organization must first assess the security requirements (security goals) and then determine whether a particular asset should be considered within the zone or outside the zone

Detailed Cyber Risk Assessment

detailed vulnerability assessment that includes examining details such as existing technical countermeasures

Top cyber risk management priorities in OT

Service provider to maintain users, AD or verify security updates

Incident response or digital forensic support in process automation environment

Production resilience when IT services are lacking. Attack prevention capabilities instead of detection

OT Cybersecurity Fundamentals

- **OT Risk and threat detection integrations with ISMS/CSMS**
  - Business risk tolerance and cybersecurity requirements
  - SIEM and SOC OT Asset and threat detection and response
  - Resilience of IT services
- **Secure remote connection**
  - In person remote support
  - Machine to machine cloud and SOC connection
- **Secure Network Architecture**
  - Segmenting and FW between untrusted networks
  - Intrusion Detection/Prevention System and Virtual Patching
  - Threat and log visibility to CSOC
- **Endpoint Protection**
  - Endpoint detection and response
  - **Whitelisting vs Antivirus**
  - **Backup and recover**
  - Threat and log visibility to CSOC
- **User Identities and Privileges**
  - OT user management and password policies
  - Threat and log visibility to CSOC

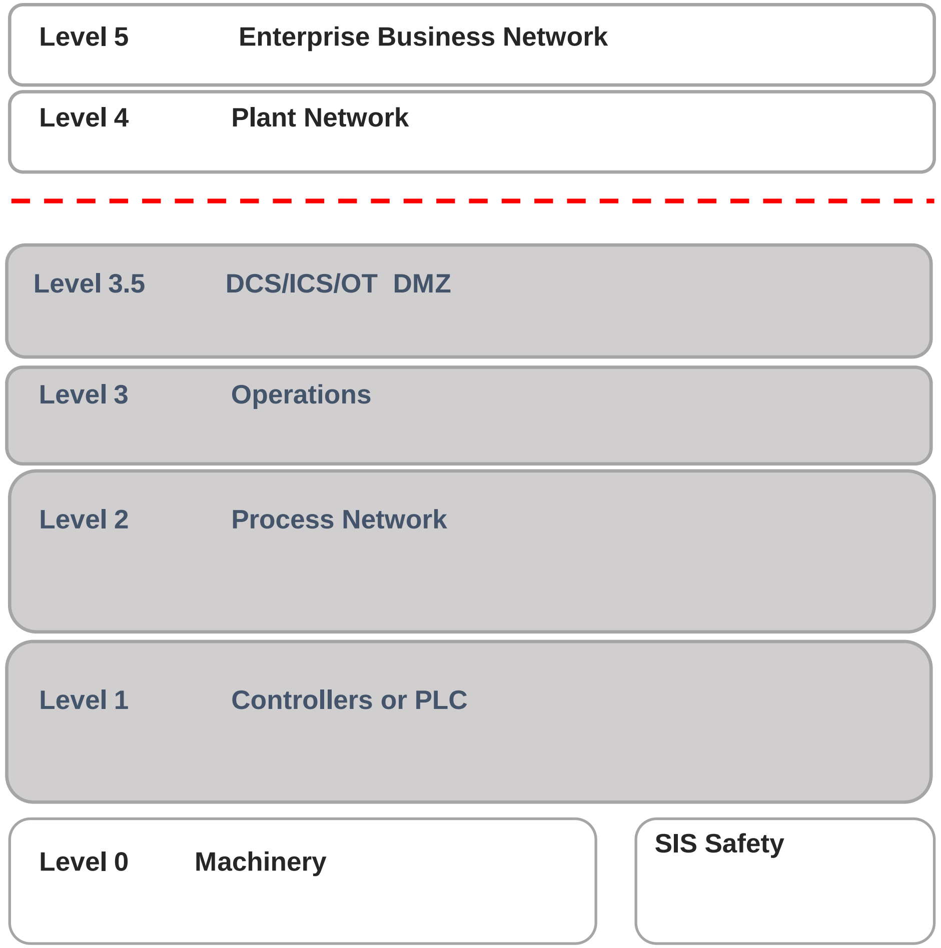
Risk and Threat detection and management processes

Cyber resilience and Security Level Target of connectivity and IT services

Security Level Target, and countermeasures based on Risks, criticality and assets type

IEC62443
Risk = Threats x Consequences x Likelihood

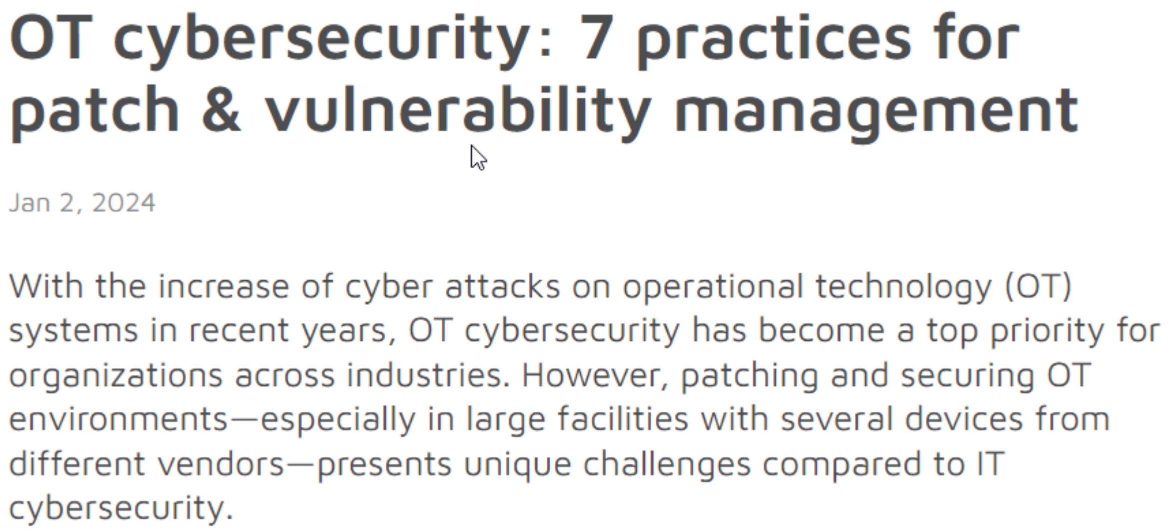
Security Level Target, and countermeasures based on Risks, criticality and assets type



ISA/IEC-62443 purdue model

OT cybersecurity patch and vulnerability management

Valmet Automation article January 2024



OT cybersecurity: 7 practices for patch & vulnerability management

Jan 2, 2024

With the increase of cyber attacks on operational technology (OT) systems in recent years, OT cybersecurity has become a top priority for organizations across industries. However, patching and securing OT environments—especially in large facilities with several devices from different vendors—presents unique challenges compared to IT cybersecurity.

Valmet

ot-cybersecurity-7-essential-practices-for-patch-and-vulnerability-management