Kriittinen infra tietomurtojen kohteena

4.6.2025

M.Tyynelä
Valmet Automation

Valmet Automation

Proven automation performance - Key segments and Offering

Pulp and paper

Energy

Process industries

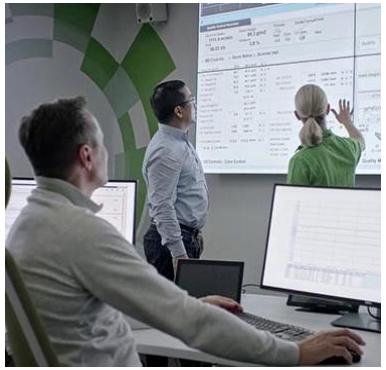
Marine

Distributed control systems

Industrial applications

Quality management

Analyzers and measurements



Industrial internet solutions

Automation services

https://www.valmet.com/

Colonial Pipeline ransomware attack

- On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that afflicted computerized equipment managing the pipeline. The attack primarily targeted the company's billing infrastructure. However, the oil pumping systems remained operational. The inability to bill customers was cited as the reason for halting pipeline operations.
- The attackers gained access to the system using a compromised password for an inactive virtual private network (VPN) account, which did not have multi-factor authentication enabled.
- Overseen by the FBI, the company paid the amount that was asked by the hacker group (75 bitcoin or $4.4 million USD) within several hours; upon receipt of the ransom, an IT tool was provided to the Colonial Pipeline Company by DarkSide to restore the system. However, the tool required a very long processing time to restore the system to a working state.

Panic buying caused widespread gasoline shortages

Some filling stations were without fuel for several days

https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

20 percent more ransomware attacks on ICS systems

3. October, 2024 08:26

Facebook X LinkedIn Reddit WhatsApp Pocket

This article is also available in German.

Industrial companies worldwide continue to be a popular target for cyber criminals, as the latest analysis by Kaspersky ICS CERT for the second quarter of this year shows.

For example, 23.5% of ICS computers worldwide were exposed to cyber threats; although this represents a slight decrease of 0.9 percentage points compared to the first quarter of 2024, there was a significant increase in ransomware attacks. The proportion of ICS computers affected by ransomware rose by 20% compared to the previous quarter.

https://www.it-daily.net/en/it-security-en/cybercrime-en/20-percent-more-ransomware-attacks-on-ics-systems

Customer challenges

Security Awareness

What is our employees', Suppliers' and Vendors' cybersecurity awareness level?

Connection security

Do we know who and when they are taking remote connections to our sites?

Assets to protect

Do we know our OT assets from all the vendors?
Are there any cybersecurity controls installed in these assets?
Are assets and our data in Suppliers' systems and premises secured?

Supported security controls and updates available

Can we patch all the assets all the time?
If not, will network level protection save us?

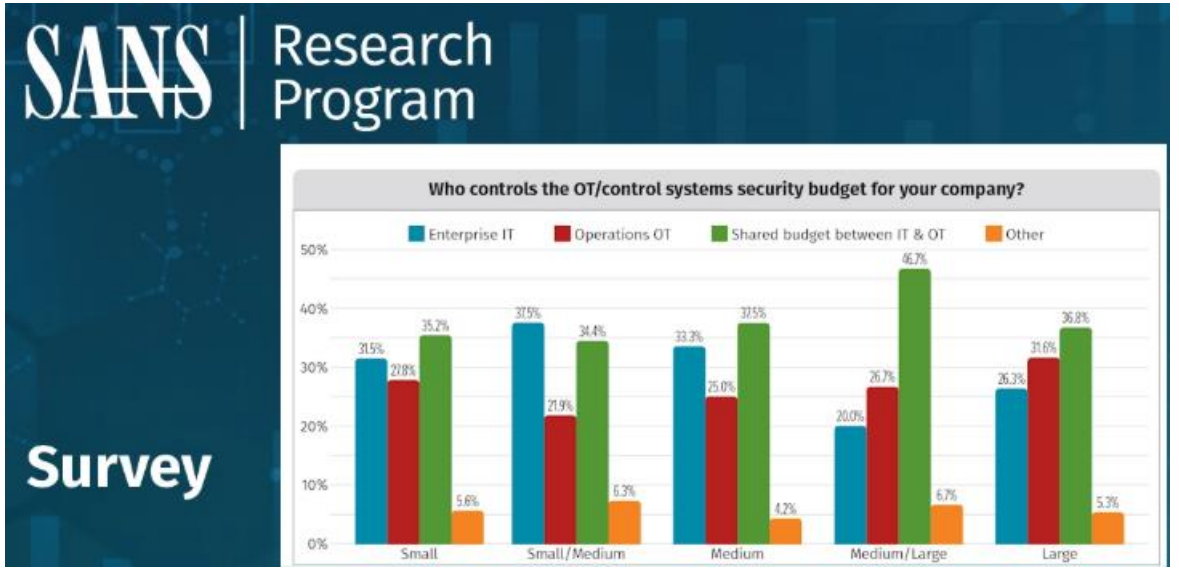
Recovery and business continuity

But if still something happens, can we recover everything, how long will it take to get production back on?

New OPSWAT-SANS survey detects growing gap in ICS/OT cybersecurity budgets amid rising threats

A report from OPSWAT and the SANS Institute disclosed that ICS/OT (industrial control systems/operational technology) cybersecurity budgets lag as attacks surge, exposing critical infrastructure to risks. The financial shortfall is particularly alarming given that over 50 percent of organizations have reported experiencing at least one security incident within their ICS/OT environments. The OPSWAT-SANS report also identified a lag in budgetary support that heightens the vulnerability of essential services and underscores the urgent need for organizations to reassess their cybersecurity strategies to safeguard against potential disruptions and breaches.

In a report titled '2025 ICS/OT Cybersecurity Budget: Spending Trends, Challenges, and the Future,' disclosed that among the top vulnerabilities exploited were internet-accessible devices (33 percent) and transient devices (27 percent), often used to bypass traditional defenses. Despite the growing recognition of OT cybersecurity as a priority, only 27 percent of organizations place budgetary control under CISOs or CSOs. Without dedicated leadership, budget allocation often overlooks critical ICS/OT-specific needs, exposing infrastructure to evolving threats.



https://industrialcyber.co/reports/new-opswat-sans-survey-detects-growing-gap-in-ics-ot-cybersecurity-budgets-amid-rising-threats/

https://www.opswat.com/resources/reports/ics-ot-cybersecurity-budget

Changing environment

Towards more regulated industrial environments

- 25 - 10 years ago – Products

- Main interest how ICS security has been managed in products
- Patch management, Malware protection, Hardening
- Maintenance Services

- 10 - 5 years ago – Processes

- Interest of how information security and cybersecurity has been managed in Valmet Automation's processes
- Requirements for product and offering cybersecurity increasing
- Various requirements as each customer has its own kind of requirements

- 5 years -Today – Comprehensive

- Interest of how Valmet as a corporation manages information and cybersecurity in all levels of organization
- Requirements for some evidence that Valmet is working as it says (i.e. certifications)
- Integrations to Customer own system (e.g. SIEM) systems increasing
- Requirements more commonly based on standards, e.g. ISO 27001 and IEC 62443

- Today – Tomorrow – Regulated

- National laws & legislations
- **NIS2 Directive**
- Cybersecurity Act
- Data Act
- **CRA Cyber Resilience Act**
- RED Radio Equipment Directive
- Machinery Directive/Regulation
- NIST
- ISO 27001
- **IEC 62443**

(Vendors, Products, Plants)

EU NIS2 Directive

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2).

NIS2 Directive is aimed to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents.

The Directive sets out the baseline for **cybersecurity risk-management measures** (all-hazard approach) and **reporting obligations** across the sectors that fall within its scope.

By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from 18 October 2024. (Article 41)

Responsibility

The NIS2 entity is responsible to make necessary risk-based decisions and actions to maintain the entity-specific security level.

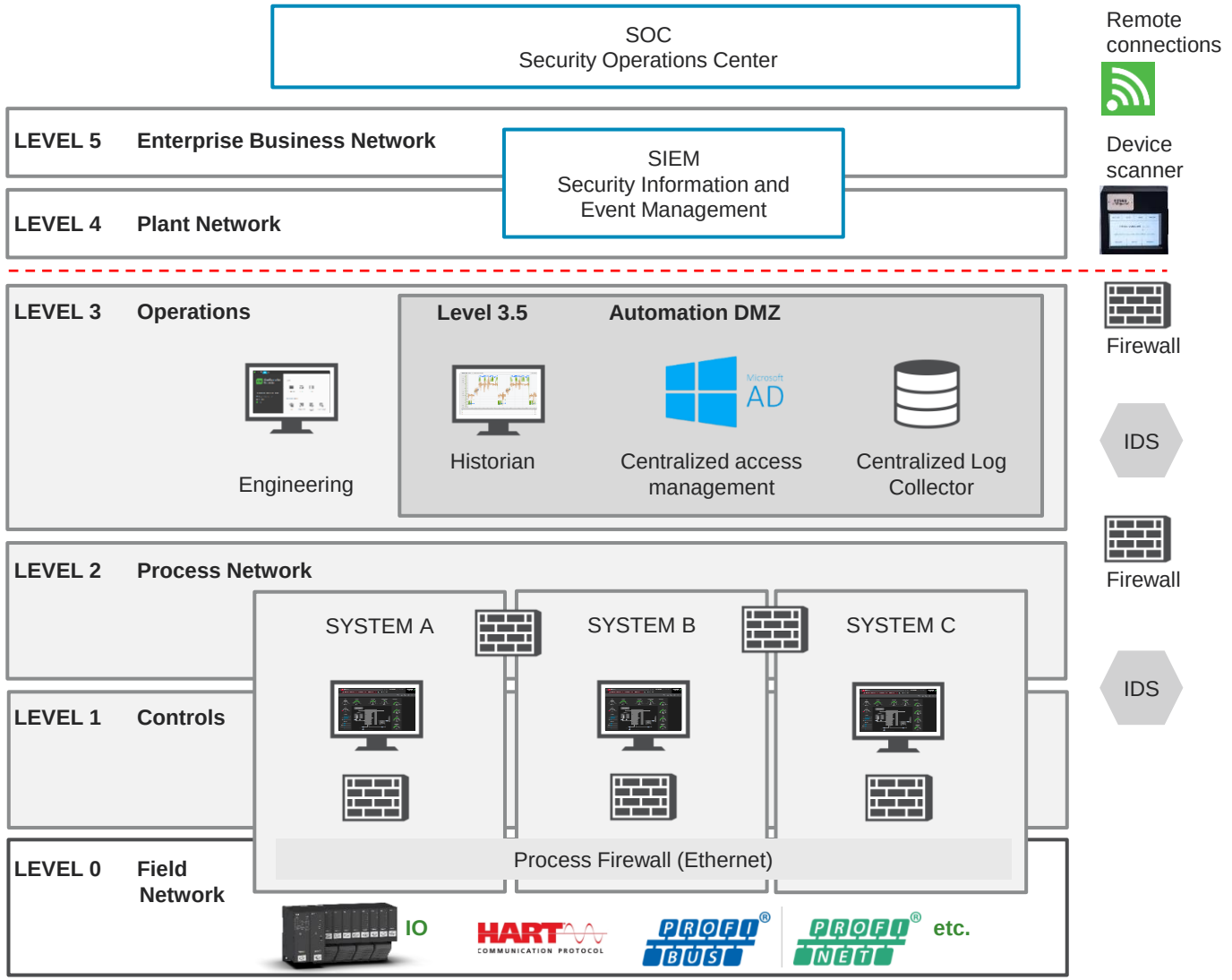
https://eur-lex.europa.eu/eli/dir/2022/2555/oj
https://traficom.fi/fi/ajankohtaista/kyberturvallisuuslaki-hyvaksytty-eduskunnassa-nis2-direktiivin-mukaiset-velvoitteet

CASE

SUPPLY CHAINS
PARTNERS AND SUBCONTRACTORS

Secure by Design

- Integration with IT security
  - ✓ SIEM and SOC
  - ✓ Secure remote connections
- Secure product development methodologies (SDLA)
  - ISA/IEC 62443-4-1 Secure Development Lifecycle
- Secure communications (all levels)
- Secure Network Architecture
  - ✓ ISA/IEC-62443 Purdue model (reference architecture)
  - ✓ DMZ with firewalls between IT and OT and between subsegments
  - ✓ (Optional) Intrusion Detection/Prevention Systems (IDS/IPS)
  - ✓ Secure (encrypted) communication
- Endpoint Protection
  - ✓ Secure configuration and hardening
  - ✓ Virus/malware protection with tested updates
  - ✓ Whitelisting for allowed software
- Centralized access management (AD)
- Log management (integration with SIEM when needed)
- Backup and Recovery
  - ✓ Backups & Regular backup testing
  - ✓ Recovery Plan & Exercises



EU Cyber Resilience Act (CRA)

Products with digital elements must conform with “*essential cybersecurity requirements*” which are presented in Annex I	Risk based approach Secure by Design and Secure by Default Products shall “*be made available on the market without known exploitable vulnerabilities*” Requirements secure by default configuration, security updates, access control, encryption, data integrity, data minimization, availability, attack surface minimization, activity recording
Manufacturers shall also conform with “*vulnerability handling requirements*” in Annex I	Documentation, possibly including software bill of materials, remediation including security related fixes, testing, public disclosure of vulnerabilities, channel for receiving vulnerability reports, delivery of security updates free of charge (with limited exceptions for tailor-made products)
Information and instructions to the user	Contact information, product documentation, technical support details,…
EU Declaration of conformity	Conformity Assessment

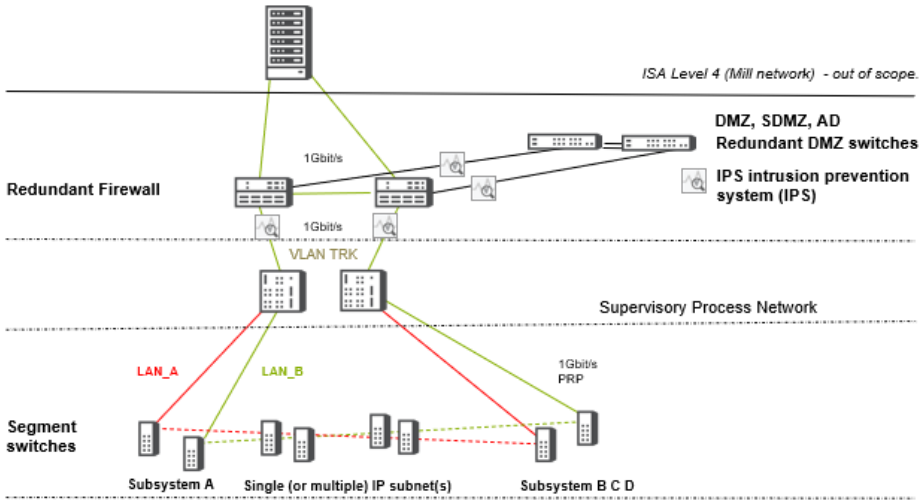
VULNERABILITY MANAGEMENT

CASE

Certified systems (IEC 62443 SSA, ACSSA) ?

- ISA/IEC 62443-3-3 (System security requirements and security levels , SSA) certifications are becoming more common (provides the evidence that the system is secure-by-default)
- Certifications based on the specific pre-defined reference architecture
- The reference architecture includes the defined network architecture and all hardware and software components of the system
- The certification is valid ONLY for the specific reference architecture, changing/adding any part will result in the loss of the certification

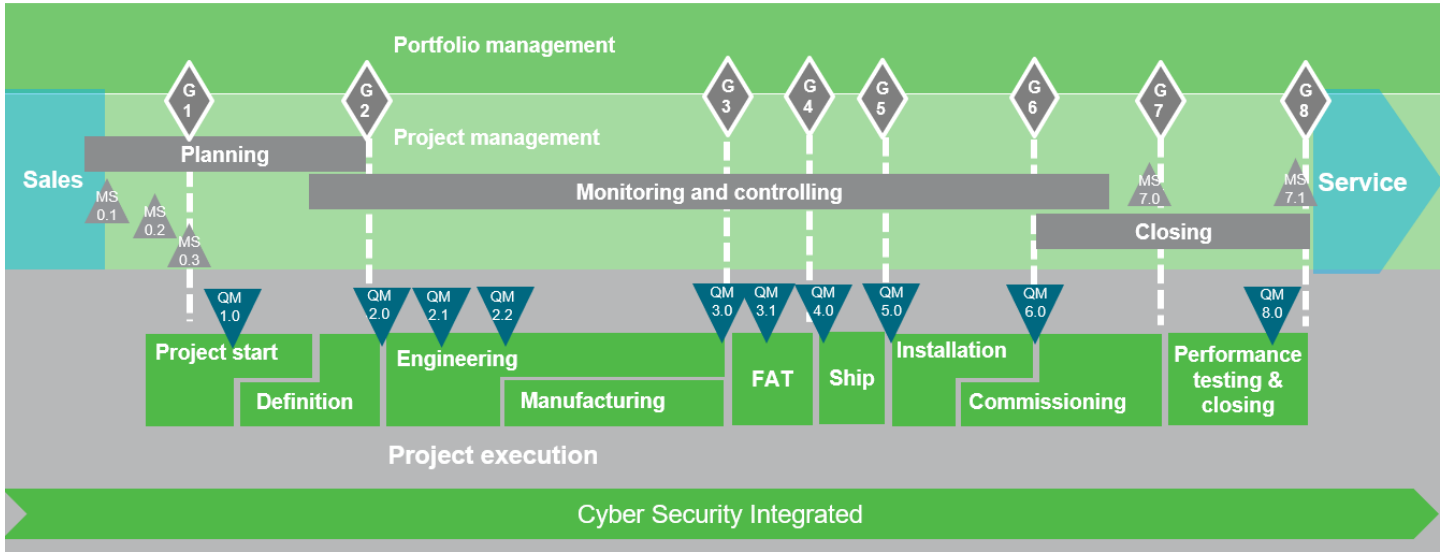
- Automation and Control Systems Security Assurance (ACSSA) Certification Based on ISA/IEC 62443 (for Asset owners) ?
  - The requirements relevant to the following parts of IEC 62443:
    - IEC 62443-2-1 – Security program requirements
    - IEC 62443-2-4 – Service providers
    - IEC 62443-3-2 – Risk assessment and system design
    - IEC 62443-3-3 – System requirements and security levels



Example of a reference architecture

End-to-End Cybersecurity in Delivery Projects

- Cybersecurity is a fundamental part of delivery projects and is integrated as an essential part of delivery project flow.
- Security part of project's risk management.
- **Communication and cooperation with all relevant parties, with clear responsibilities**.



Project Flow

- Sales phase
  - Customer's security requirements?
- Transfer from sales to projecting
- Quality assurance in project
- Manufacturing
- Acceptance Tests (FAT, On-Site & SAT)
- Transfer from projecting to service
- Service (Maintenance)
  - Service agreements

G PROJECT GATE

MS PROJECT MILESTONE

QM QUALITY MILESTONE

G1	Start delivery project
G2	Start detail engineering
G3	Start site operation preparations
G4	Start main shipments
G5	Start installation
G6	Start commissioning and start-up
G7	Start performance testing
G8	Close the project

MS0.1	Transfer from Sales
MS0.2	Project Plan
MS0.3	Project Budget
MS4.0	Site Risk assessment
MS7.0	Take over
MS7.1	Transfer to Service

QM1.0	Ready for definition
QM2.0	Ready for detail engineering
QM2.1	Ready for purchasing
QM2.2	Ready for Manufacturing
QM3.0	Ready for iFAT
QM3.1	Ready for cFAT
QM4.0	Ready for shipment
QM5.0	Ready for installation
QM6.0	Ready for commissioning
QM8.0	Ready for closing

CASE

RISK MANAGEMENT
CHANGE MANAGEMENT

Maintenance Services

- Integration with IT security
  - ✓ SIEM and SOC
  - ✓ Secure remote connections
- Secure product development methodologies (SDLA)
- Secure Network Architecture
  - ✓ ISA/IEC-62443 Purdue model - reference architecture
  - ✓ DMZ with firewalls between IT and OT and between subsegments
  - ✓ (Optional) Intrusion Detection/Prevention Systems (IDS/IPS)
  - ✓ Secure (encrypted) communication
- Endpoint Protection
  - ✓ Secure configuration and hardening
  - ✓ Virus/malware protection with tested updates
  - ✓ Whitelisting for allowed software
- Centralized access management (AD)
- Log management (integration with SIEM when needed)
- Backup and Recovery
  - ✓ Backups & Regular backup testing
  - ✓ Recovery Plan & Exercises
- Certified systems (IEC 62443 SDLA, CSA, SSA) ?
- **Up-to-date Service Agreements**

Cybersecurity Consultancy	Risk Assessment for new sites Cybersecurity exercise for customer key personnel Cybersecurity Assessment for existing sites Incident response support
Identity and Access Management	Active Directory management for Valmet standard setup Active Directory workshop for custom setup
Endpoint Protection	Hardening Antivirus Application lockdown (whitelisting)
Vulnerability Management	Asset Inventory and Lifecycle Planning Vulnerability inspection and reporting Patching services
Network Protection	Centralized log collection Intrusion detection/prevention system (Virtual Patching) Incident response support Security Operations Center visibility
System Recovery	Backups Recovery Plan Offsite backups hosting and recovery services


Valmet
FORWARD