jamk.fi

Industrial control systems' integrations to Operation Technology and Information Technology Security Operation Center

Ari Rajamäki

Master's thesis
April 2021
Technology
Master's Degree Programme in Information Technology, Cyber Security

jamk.fi

Description

Author(s)	Type of publication	29 April 2021
Rajamäki, Ari	Master's thesis	Language of publication: English
	Number of pages 80	Permission for web publication: Yes

Title of publication

Industrial control systems' integrations to Operation Technology and Information Technology Security Operation Center

Degree programme

Master's Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Kokkonen, Tero and Hautamäki, Jari

Assigned by

Valmet Oy Automation Business line

Abstract

Risks of cybersecurity incident in the process automation systems have increased because more digitalization and connectivity are added to these environments. Cyber threats and attacks on industrial control systems have affected the enterprise organizations' risks and business continuity plans.

The risk of losing control system availability, integrity or continuity of critical infrastructure, a chemical process or a larger manufacturing facility is the main reason why these industrial control systems (ICS) are added to the scope of enterprise organizations' cyber incident risk management plans. Government and agency regulations and guidelines for critical infrastructure protection are driving this change also.

The topic of the thesis assigned by Valmet Automation was security monitoring for awareness, threat detecting requirements and response capabilities for industrial control system. Constructive research methodology was selected for organization to continuously improve the log management and security monitoring of the ICS products and system deliveries, improve service functionalities and skills needed to support incident response and forensic operations, used, for example, by an asset owner organization's security operation center (SOC) providers.

Industrial control system's monitoring interface availability and understanding the contextual security events and response activities can be different depending on the ICS vendor and the industry process. Customer enterprise SOC organizations require ICS vendor support and services to integrate and normalize the events of ICS environment to the SOC's threat analysis and incident response processes, originally planned for the enterprise operation information and communication technology (ICT) networks.

Keywords/tags (subjects)

ICS, OT, SIEM, SOC, Log management, Security, Critical infrastructure, Situation awareness

Miscellaneous (Confidential information)

jamk.fi

Kuvailulehti

Tekijä(t) Ari Rajamäki	Julkaisun laji Opinnäytetyö, ylempi AMK	29 Huhtikuu 2021
	Sivumäärä 80	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: Kyllä

Työn nimi
Industrial control systems' integrations to Operation Technology and Information Technology Security Operation Center

Tutkinto-ohjelma
Master's Degree Programme in Information Technology, Cyber Security

Työn ohjaaja(t)
Tero Kokkonen ja Jari Hautamäki

Toimeksiantaja(t)
Valmet Oy Automation Business line

Tiivistelmä

Kyberhäiriön riski prosessiautomaatiojärjestelmissä on kasvanut, koska digitalisaation myötä järjestelmiin on avattu ulkoisen järjestelmän tietoliikenneyhteyksiä. Automaatiojärjestelmiin kohdistuneet kyberhyökkäykset ovat vaikuttaneet myös organisaatioiden riskienhallintasuunnitelmiin sekä jatkuvuuden varautumissuunnitelmiin.

Kriittiseen infrastruktuuriin kuuluvan tai esimerkiksi suuren kemian alan teollisuuslaitoksen automaatiojärjestelmän riskit, jotka liittyvät laitosta ohjaavan järjestelmän saatavuuteen, eheyteen sekä luotettavuuteen ovat merkittävä tekijä miksi ICS (Industrial Control System) liitetään osaksi yritysten kyberhallintasuunnitelmia. Myös valtioiden sekä erilaisten virastojen määräykset, suositukset sekä ohjeet ohjaavat tähän suuntaan.

Automaatiojärjestelmän tietoturvatapahtumien monitorointi ja järjestelmän tietoturvatason tietoisuuden lisäämismahdollisuudet sekä näiden uhkien tunnistamiseen liittyvien toimintasuunnitelmien vaatimukset olivat tämän tutkimustyön aiheena. Konstruktiivinen tutkimusote valittiin metodologiaksi, jolla kohdeorganisaatio voisi parantaa keskitetyn lokihallintajärjestelmän käyttöä tietoturvan monitorointiin erityyppisissä ICS toimituksissa sekä parantamaan palvelukyvykkyyttä ja taitoja, joita tarvitaan, kun ICS järjestelmä liitetään osaksi SOC (Security Operations Center) valvontaa sekä tietoturvapoikkeamien selvitysprosesseja.

Automaationjärjestelmän tietoturvan monitorointirajapinnat sekä tietoturvatapahtumien ymmärtäminen voivat olla hyvin järjestelmätoimittaja- tai prosessikohtaista. SOC toimija vaatii tukea järjestelmän toimittajalta tai sen ylläpitäjältä, liittääkseen järjestelmän tapahtumat osaksi monitorointia sekä prosesseja, jotka ovat suunniteltu toteutettavaksi tieto- ja viestintätekniikan ympäristöissä sekä näiden järjestelmän ylläpitotaitojen avulla.

Avainsanat (asiasanat)
ICS, OT, SIEM, SOC, Log management, Security, Critical infrastructure, Situation awareness

Muut tiedot (salassa pidettävät liitteet)

Contents

Figures

Tables

Acronyms

AI	Artificial Intelligence
APT	Advanced Persistent Threat
BES	Bulk Electric System
CEE	Common Event Expression
CEF	Common Event Format
CEI/CBE	Common Event Infrastructure/Common Base Event
CEO	Chief Executive Officer
CIA	Continuity Integrity Availability
CIDF	Common Intrusion Detection Framework
DCS	Distributed control System
DNA	Dynamic Node of Applications
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Resource Planning
EU	European Union
FIM	File Integrity Monitoring
GDPR	General Data Protection Regulation
IACS	Industrial Automation and Control System
ICS	Industrial Control System
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IOC	Indicator Of Compromise
IODEF	Incident Object Description and Exchange Format
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Centre
IT	Information Technology
LEEF	Log Event Extended Format

MES	Manufacturing execution systems
NCSC-FI	National Cyber Security Center Finland
NERC CIP	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NIST CSF	NIST Cyber Security Framework
OODA-loop	Observation Orientation Decision Action -loop
OT	Operation Technology
PDCS	Plan Do Check Act
PLC	Programable Logic Controller
RTU	Remote Terminal Unit
SA	Situation Awareness
SCADA	Supervisory Control And Data Acquisition
SDEE	Security Device Event Exchange
SIEM	Security Information and Event System
SIS	Safety Instrumented System
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
SOC-CMM	SOC Capability Maturity Model
STIX	Structured Threat Information eXpression
TAXII	Trusted Automated eXchange of Indicator Information
VM	Virtual Machine
WELF	WebTrends Enhanced Log File Incident Object Description

1 Introduction to industry control system security monitoring

Monitoring of Information and Communication Technology (ICT) infrastructure by administrators is day to day continuous task. Administrators belong to an organization, are responsible for the infrastructure as an asset for the enterprise business continuity. Monitoring and the maintenance tasks such as the whole ICT infrastructure in this modern cloud computing era can be delivered also as a service. Cloud used as a platform for hosting ICT asset provides some advantages for example availability of the ICT asset. Distributed cloud service is the best possible redundancy and availability guarantee for the enterprise assets. Cloud provides endless capacity, and there is always available capacity for scaling up the performance or for the new services provisioning; however, is it always available, do you always have the internet connectivity to enable the cloud services? Example the enterprises operating industry production environments to control and monitor the machinery are usually missing this cloud connectivity and SaaS and PaaS (Software and Platform as a services) type of services.

Monitoring the ICT infrastructure health and availability is not the only required service that the Information Technology (IT) administrator organizations are responsible for providing. Protecting and monitoring the security of ICT infrastructure and information data is a critical requirement when enterprise ICT and data assets security risks are managed. Best practices for threats and risks management also require services to provide threat intelligence capabilities and functionalities. Operations for threat intelligence, incident response and incident forensic are usually responsibility of Security Operations Center (SOC) organization. SOC operations provided by outsourced services utilizing the cloud services for threat intel and asset information data aggregation, machine learning and even for artifact intelligence is again very cost efficient and even a practical strategy to provide the intelligence and awareness of the threats. Industry production environments can provide same asset and security information to a SOC organization and there is also threat intelligence available for industry control systems. What are usually missing are the connectivity and skill sets for SOC organization teams to do required

integrations, incident response and incident forensic in the industry production ICT environment.

Manufacturing and process industry facilities' computer infrastructure are commonly known as Operation Technology (OT) environments. OT and IT differences are in the critical assets and the information that environments are managing for the enterprise business continuity. OT environment deals with physical processes and production information. In the OT networks, Industrial Control Systems (ICS) computers are the network devices that are closest to the physical processes and the machinery. ICS is used to control and monitor the facility processes and machinery.

Industry production OT environment's ICT infra and IT services are close to common standards, technologies and services used in the upper level of production automation computers like servers, and security controls are many times similar as in the ICT enterprise infra; however, ICS are segregated installations in the OT network and are usually located in the factory premises or office locations from where factory production operations are managed. Lower level of the production systems, networks where ICT computer systems are controlling and monitoring the machinery, standard technologies, services and required skills differ from the normal enterprise ICT infra. Understanding production automation and industry processes engineering and controls is an asset that is usually not included in the enterprise IT administrators or SOC team member skillsets. (Searle, 2018)

Security protection and monitoring of the Industrial Control Systems (ICS) is beginning to be a more important part of the information security management programs and strategies in the production enterprises. Industrial control systems' security management can be even government or agency regulated for the industry sector's part of critical infrastructure of the cities, environment areas or countries. Critical infrastructure is usually referred to the energy production or transfer, clean and wastewater treatment, and transportation as for short list of examples. ICS security monitoring and security awareness of known and unknown ICS threats is a modern requirement for all production environments, production where industry automation technologies are used. The ICS production environment is not necessary part of any critical infrastructure; however, any distribution such as downtime of safety system or inactivity or maloperation in these ICS environments may cause

huge local environmental consequences, risk of human safety or financial local or global consequences. (Behrens, 2021)

Enterprises can be trying to push same security polices for control systems protection and monitoring as they are using for enterprise ICT and services. Usually, the organizations responsible for control systems, automation or OT networks and IT personnel cannot be sure if production environment availability and operations are guaranteed when same security policies with the controls are implemented into the ICS. It is also possible that automation system vendors' equipment, ICS controlling and monitoring the production does not provide the needed support for implementing enterprise security policy required security controls and security software applications.

Security information monitoring is one example of the passive security measure that usually can be implemented into the industry control systems. ICS security information events and logs from ICS network endpoint devices can be provided to the enterprise IT organized SOC. ICS endpoint can be protected and monitored with ICS vendor supported security controls and security software applications that are offering the security events and information. SOC operator can be missing the important security information event that can be a vendor or system specific device. For example, information from process applications' set or target points and safety system modifications are example events that should in many cases indicate a red alert in the SOC monitoring the ICS. Incident response and forensic operations in the production environments having alerts like these usually require a set of skills that only the ICS automation engineers, and operators' personnel have. (Dragos Inc, 2017)

Let's concern the above introduction to the ICS security monitoring and incident responses. The knowledge of cyberattacks is targeted to the enterprise IT infrastructures, from where the connectivity to the production OT exists and there are also targeted ICS attacks. This thesis will focus on researching and developing the ICS vendor systems and products' security monitoring capabilities and services needed to support implementations of the ICS to be part of SOC operations and incident response plans.

Valmet Automation Business line develops, deploys, and maintains automation technology SW and HW products. Valmet Automation is vendor of computers systems used in process industry sector to monitor and control machinery, measure performance and quality of the machinery, processes and end products or production. Cybersecurity requirements of the SW and HW products, deliveries and services have been increasing. Due the known ICS targeted cyberattacks or espionage campaigns against critical infrastructure's production environments.

Security monitoring and detection capabilities are an increasing requirement for the ICS environment. Security visibility and awareness must be part of the processes, systems and services delivery cross the supply chain. Enterprise IT organizations' SOC operators are commonly added to be responsible for detecting and responding to the security events also from the production automation environment if the enterprise has them. Therefore, passive monitoring and security events and logs forwarding are also required from Valmet Automation products, from new and existing maintained production automation system deliveries.

Valmet Automation service organizations must increase capabilities to provide services for implementing security monitoring technology into the maintained ICS. Service organization need to support implementing SOC connectivity for detecting and responding cybersecurity incident identified example from the Valmet Automation maintained production environment. This will also possibly improve the situation awareness of the Valmet ICS systems detected threats.

2 Thesis research target and methods

2.1 Research objectives

The thesis research will focus on the globally published cybersecurity requirements, guidelines and best practices for the ICS cybersecurity threat detection and monitoring capabilities. The research results will provide information of support services and implementations required to detect and forward ICS security event information to the ICS external Security Information and Event Monitoring (SIEM) systems. The ICS external SIEM can be provided by Operation Technology (OT) or IT organization to comply new security risk management policies of the asset owner organization. Support services' availability and capabilities are required to support the Security Operation Center (SOC) personnel in their processes of detection, incident response and forensic tasks. These tasks are carried out in the live production ICS environment, in use for manufacturing and process industry purpose. Because of this, special ICS/OT skills may be required to ensure ICS availability.

Industry sector's business opportunities and modern cybersecurity requirements available for the ICS deployments are key commitments for the thesis assigner to comply and provide solutions for the automation products, projects, and services. There is a risk of losing process industry project and service opportunities or some of them to the competitor or 3rd party company organizations. There are cybersecurity companies who are developing and targeting more research work toward the OT sector security monitoring systems and related services. Using 3rd party security products in the ICS environment deliveries require also new roles and responsibilities to be defined when systems are delivered or maintained.

The thesis focuses on requirements of providing managed security monitoring interface and services for new and existing Industrial Control System deliveries. The results are used in the projects the thesis assigner is implementing Valmet Automation DNA (Dynamic Network of Application) ICS product and related maintenance services.

Security monitoring and service requirements of the Industrial Control System are rapidly increasing. Organizations and asset owners must provide security awareness

information from the production system the enterprise plant or mill is using. ICS vendors developing and deploying the computer technology, infrastructure and software applications to these OT environments must comply with cybersecurity requirements that are targeted to OT sector. Vendors must support globally, and industry sector diversely defined cybersecurity policies and regulations. The thesis will try to find answers to the problems of implementing, managing, and developing technology for log management and security monitoring solutions by using organization's existing processes and resources for creating and delivering products and services, considering the existing organizations' knowledge of the cybersecurity domain and the technology provided for the ICS environments and SOC operations.

The thesis will research the requirements and solutions used for security monitoring of ICS and OT environments. The research project will also identify how the SOC operations are planned and offered for the ICS asset owners in the plant or mill OT environment. The thesis will provide required technical implementation and documentation of Valmet Automation Central Log Management product and security services for the ICS security monitoring implementations, risks detection and response. The research project will develop capabilities to continue the improvement and development the security monitoring capabilities and services into the assigner organization's products and deliveries.

The thesis will answer the following research question:

- Can ICS vendor implement and maintain the log management system used as source for OT SIEM and SOC capabilities?

The main research question is divided into the following sub-questions:

- What interfaces and protection features the log management must provide?
- What skills are needed to implement the log management used for SOC operations in ICS?
- What services can the ICS vendor provide to support SOC capabilities for threat - and risk detection and incident response in the ICS environment?

2.2 Research methodology

The selected research methodology for the thesis is the constructive research approach and the methodology's possibilities of using different methods for innovative research work. Because the constructive research innovation method provides the possibility to create multiple or endless number of constructions (solution), it is a good methodology to use in the Valmet Automation products and organizations.

Valmet Automation organizations have long traditions of developing process industry products and services. Constructive research methodology will provide the best possibilities for Valmet Automation organizations for continuous development of security monitoring capable products. The methodology will also support maintenance services development work. These services are performed in the field of globally distributed production environments using Valmet Automation DNA DCS. Constructive approach can also be considered as a continuous learning process (Lukka, 2014) and methodology offers field research possibilities, and both modes are excellent approaches in the assigner's organization and product developing processes.

Cybersecurity requirements for security visibility, log forwarding and SOC services from the industry customers RFPs' (request for proposal), industry standards and guideline policies can be used for benchmarking process. Benchmarking is used as part of constructive and innovative research work process. Benchmarking is a process that help to answer the research question, what is needed for ICS security monitoring interfaces. Benchmarking method can be used together with the PDCA (Plan Do Check Act) method. Similar data collection and implementation planning processes were used in the study of (Narayanamurthy & Gurumurthy, 2016), where the authors were following Xerox benchmarking model techniques.

Process of several iterations to implement the improvements in the PDCA driven development is very well known and used in the thesis assigner's organization development projects and processes. PDCA's Check-part could utilize steps from the benchmarking process and create new targets for the Do-part iteration. Benchmarking process can also be conducted in continuous PDCA cycles. When

planning the benchmarking process, the information is collected from the references after which checking, and analyzing the information follows. After benchmarking the improvement implementations are included into the project backlog (Laine, 2007).

The risks of constructive research approach are the issues that get uncovered during the research work. For example, during the process of benchmarking and PDCA phases new challenges might be discovered. For this reason, the constructive approach takes longer to conduct the construction. (Lukka, 2000) Lukka's opinion and experience expresses that the most typical problem is that the organization's commitment for the research work cannot be maintained. Commitment or lack of commitment from the stakeholders in the organization may decrease because of the significance of the research work or the reprioritization of the organization's resources to more important projects due to business reasons.

Commitment and reprioritization risk can be realized in the assigner's organization because of the rapidly increasing security requirements for the ICS products and services. The reason can also be that service organization's resources used for field-based research work are required for other projects and constructive approach will be delayed.

The principles of the PDCA method and backlog usage are good methods for the research project. Implementation and development can be paused, or iteration speed can be slowed down when the resources or commitment are needed elsewhere in the resource organizations. The research project's benchmarking method can define the backlog list of issues requiring implementation work. Planning of the new PDCA iteration can be conducted later when the resources are available again. Commitment risk and the dilemma of losing control of business secret (Lukka, 2000), is managed because the author of the research is working as an employee in the target organization.

2.3 Research ethics

The research integrity of the thesis is partly managed by author's contract of employment with Valmet Automation Oy, where author is working as on industry security specialist. The contract agreement also includes a part where the client's

business and trade secrets are protected during and after the employment. The agreement also covers the thesis and research work. The thesis does not publish any personal data, and the research did not require to process any GDPR (General Data Protection Regulated) information. Data and information to be protected by the author's contracts of employment are Valmet DNA product and service-related information like agreements and environment details of the Valmet customers. To protect Valmet Automation's and its customer trade secrets and environment details, the thesis does not present or refer to any of the information nor are they published in this public thesis paper (Finnish Advisory Board on Research Integrity, 2012).

Primary the research work used reliable observations and studies conducted by industry asset owners and requirements and guidelines published or regulated by government organizations for the OT industry. The research also used publications and studies from the industry companies for ICS technology, Universities, and consultancy/research workers' whitepapers and publicizations.

Constructive approach's field-based research studies and work were carried out in the customer environment together with interviews of the service people using and integrating the log management system and related services. These findings are not published in the thesis. In terms of good research, practices and respects details from the customer environments or the customer organization are not published (ALLEA - All European Academies). Publishing all the research work details may cause unwanted risks of identifying vulnerabilities of the environments and components used in these or similar ICS deployments.

The research and the thesis report do not violate any agreements between the author and Valmet Automation Oy. Copyrights are not violated, and all the references and citations are presented and marked according to the JAMK Master thesis project and reporting instructions. The thesis follows sources: clear, concise, and credited paraphrasing (Ylönen, 2021). JAMK' pedagogical and ethical principles targets' were followed during the thesis project (JAMK, 2017).

3 Industrial Control System and Security

3.1 Security Monitoring

Security monitoring of any computer system fundamental principle is same as it is for security protection of any computer system: you need to know what to monitor and you need to know what you are protecting. This principle should always be taken care with asset inventory technology implementations. This is usually true with ICT systems managed by IT organization. Industrial control systems' computer technologies lifecycles are long and asset inventories are not implemented or the inventory data do not contain all the devices (Searle, 2018). This makes it more challenging to know what to protect in ICS network. Even though latest cybersecurity requirements and solutions offered into these critical environments are slowly degreasing this gap.

When the enterprise production environments' factories, mills or plants have been in operation for several decades. Environment of computer system could contain technology implementations from 20 years back or even more. Because of technologies and digitalization have gone forward, also new device installations have implemented during these decades. For these reasons factories using multivendor industrial control systems in the production system are heterogeneous environments. Cybersecurity protection services and products for ICS markets are usually providing passive asset inventories to help understanding of *know what to protect*. Security monitoring of ICS requires planning, determining what to monitor (Knapp & Langill, 2018).

There are plenty of studies and research work published for ICS threats and know attacks. Reports exists how these attacks have been executed and how sophisticate ICS attacks and adversary groups are evolving. The research will focus on the ICS vendor security detection capabilities and requirements. Because of above risks and the threats of adversary groups targeting attacks to countries and cities critical infrastructures' control systems is increasing and ICS vendor must comply to the requirements of mitigating the risks.

3.2 Industrial Control System

Operation Technology (OT) term is rather new synonym that has gain popularity in 21st century and during last year's when author was writing this thesis in 2020-2021 it is started to be more popular than ICS or SCADA although these later ones are still in use in valid sentences. There are industrial systems where proper term is to use SCADA, ICS or DCS as example. When someone is presenting or marketing industrial control system cybersecurity products and capabilities, they are more using common OT term for the target of the product, more than anything else. IT / OT differences, requirements and merging these two or cybersecurity policies of them are usually popular topic or argument with the cybersecurity professionals of IT and OT people. What is the difference and what is the OT environment? Simple explanation by Dragos Founder and CEO (Chief Execution Officer) Robert M. Lee is like follows

> *OT = IT + PHYSICS*
>
> *Physics in this equation stands in for the physical processes that OT systems control—whether it is machines and robots in manufacturing facilities, pumps and valves at water stations, or electrical grid equipment run by the power plant.*(Lee & Alperovitch, 2019)

Author of the thesis would also describe that Industrial control system is part of large OT network in manufacturing or process factories and ICS concepts can be summarized as a large or huge complex system of automation - and networks, devices, sensors, valves, and motors on top of large field or area.

Combining the computer programs and people (operators) who control and supervises the system, production, and process. ICS components or functionalities and common terminology at high level can be divided and described as follow (Harp & Gregory-Brown, 2016);(Searle, 2018).

- SCADA (Supervisory control and data acquisition system) what can be spread to larger geographic areas from where different automation or example power grid substations are operated and controlled
- DCS (Distributed Control System) is plant level automation system to control different processes of production.
- PLC (Programmable Logic Controller) can be smaller part of DCS to control real-time process via Multiple I/O field bus connections

- SIS (Safety Instrumented System) is detecting unsafe situations in the production process and safety of personnel and environment.

In the thesis author will use more ICS and DCS (Distributed Control System) term to scope the target down to be more of one production process controlling system instead of whole OT system where scope could include also Manufacturing execution systems (MES) and even Enterprise Resource Planning (ERP) type of systems.

Lower levels of ICS assets in the field, usually contains I/O (Input/Output) Devices, RTU (Remote Terminal Unit) and IED (Intelligent Electronic Devices) hardware equipment's used in process controlling and monitoring, sending and or receiving data to and from the process. In the Field bus of these IED, RTU devices and upper DCS/ICS level, there are also components used for building a network architecture and topology, containerizing media converters, network switches and routers (Kang, Kim, & Na, 2014).

Modern ICS environments or factories where cloud services are integrated into factory operations may contains also IIoT (Industrial Internet of Things) category devices. All the above component's devices and operations executed can provide security events for monitoring and storing. In the OT cybersecurity control and measure industry, there are new requirements to add more devices for security. Devices like Intrusion Detection System (IDS) support and implementations are requested for ICS. These security control devices and measures are naturally an important source for security events and threat visualization of the ICS. (More, Jamadar, & Kazi, 2020)

NIST (National Institute of Standards and Technology) Specific Publication 800-82 Guide to Industrial Control System (ICS) Security, describes ICS Operations as in figure 1. Operator and Engineering people are using the HMI (Human – Machine Interface) to monitor and control process by configuring setpoints, programming control loops executed by the Controller. The controller is a device using Sensors to read variables from the process, the controller uses actuators (valves, breakers, switches, and motors) to manipulated process. The controller executes loops and algorithms programmed and supervised by humans, operators, and engineers (National Institute of Standard and Technology, 2015).

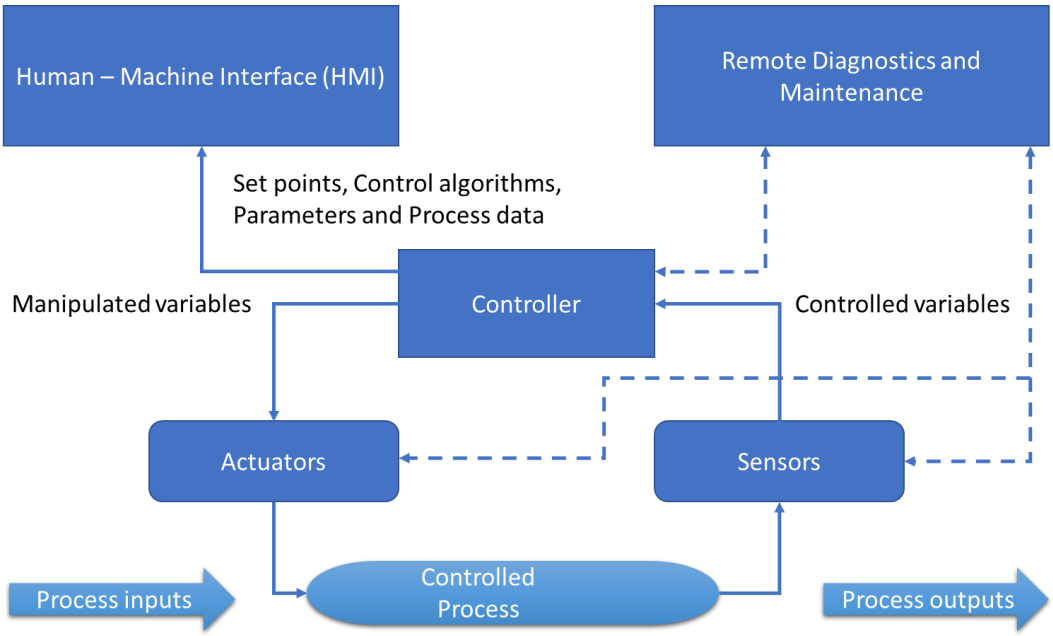


Figure 1. ICS Operations described in NIST SP 800-82 (National Institute of Standard and Technology, 2015)

NIST SP 800-82 summarizes and defines guidelines of ICS topologies and gives methods and controls for protecting the ICS from cyber threats (Hao, Zhou, & Chen, 2016). The ICS operations described in NIST SP 800-82 can also describe the ICS safety instrumented system operations, the SIS is a system that is composed of the sensors and the controllers. The SIS is used to take the process to a safe state when preconfigured risk conditions are met. This can be a situation where the ICS operators have failed to stabilize the process using the ICS controls and controllers.

The SIS systems are usually segmented to be separated network in the ICS, for the reason of protecting the SIS against cyberattacks. The SIS cyberattacks are targeted to physical damage facilities by compromising and altering the SIS controller or it is configuration to misbehave in defined emergency situations. Example of the SIS targeted cyberattack in Saudi Arabian known as TRISIS (M. Geiger, 2020) where attacker got access to special engineering workstation, the HMI used for TRITON attack targeting to the Triconex SIS, the controller of process safety system (Johnson, et al., 2017).

The ICS operations security monitoring and events sources could be partly the same as in the ICT environment. Example the authentications, privileged executions or any security event of a workstation or server environments and applications. The ICS important operations of the controller configurations or operator's control mode updates like setpoints altering or manual mode selections (instead of automatic valve or motor controls) could be prioritized as severe events in the ICS. The industry processes' ICS environments have hundreds of parameters that could be monitored for security reasons. In a fact an automation system of industry processes is built to digitalize process statuses and the values are used to monitor and control process. These values are used by the operators in the control rooms of smaller DCS or larger SCADA systems. (Searle, 2018)

The control room is much like a SOC room with screens and visualization of trends and alarms to monitor the asset or in the ICS case also the process stability and quality are monitored, and alarms are interpreted and responded. SOC analyst monitoring of IT infrastructure and has responsibility of confidentiality, integrity, and availability (security). The control room operator monitoring of physical processes and has responsibility of uptime, max of production/profit, and safety and pollution (safety) (Kotofil & Kopeytsev, 2019).

3.3 OT and IT Systems security

IT and OT risks differs, for IT environment almost always protected asset is the data in the systems and high risks are related to lose of business-critical digitalized information for example during the cyber espionage or ransomware attack. For the OT environment protected asset is the ICS process controls and high risks are related to the loses of human life or the environmental hazards because of physically damaged industry factory. Even the risks are different in the IT and OT domain the threats for attacks can be the same especially with the modern industrial systems where multiple connections between the ICS and the ICT exists. Connections will continue to be added with the cloud and IIoT (Industrial Internet of Things) related products and services offered are increasing in the control systems to improve production monitoring capabilities. (Lee & Alperovitch, 2019)

Industrial environment to be used for training and learning are rare to have, and OT cybersecurity knowledge and experience is not so common as it is with IT domain (Lee & Alperovitch, 2019). In Lee's and Alperovitch's white paper it is also mentioned that OT mission, systems, threats, and organization impact are different than IT. OT and IT threats can be different; however, vulnerabilities exploited in IT network attacks can be successful exploited also to the connected OT environment computer systems.

For the IT, network high throughput is important and delays in the networks are okay or can be easily solved by expanding computing power or memory. This workaround can be implemented even if it requires short maintenance shutdown or restart of system services. What obviously is not huge problemed in the IT where several maintenance windows can occur, out of the office time. In the OT production environments system shutdown maintenance periods are not always possible or they must be planned beforehand, production can is running many times a 24h per day several months nonstop.

Usually computing power and available memory and storage are constrained within the devices part of ICS environment. ICS lifecycle is long and old generation devices exits. Into these legacy devices, implementing new security measures, protocols and technologies are challenging. These were only few samples of challenges in the ICS environments when security implementations or monitoring capabilities are added. Table 1 is listing more challenges and differences between IT and OT domains' security management (Searle, 2018).

Table 1. IT vs OT security management (National Institute of Standard and Technology, 2015);(Searle, 2018)

IT: Security > Availability	**ICS: Availability > Security**
Risk of losing data • High throughput • No similar redundancy requirements • Cloud technologies available	Risks of Environmental and life danger • Production targets • real-time controls and safety systems • Malfunction not to stop production • Redundancy required

Standard IT systems	Proprietary systems
• Continuous, automatic updates • Booting of PCs' is not a problem • Expandable computing power and storage • Standard workstations, servers and network solutions and technologies • General IT skills and competencies available	• Static, automatic updates not possible • Embedded systems, field buses and field devices with industrial protocols • Various generations of technologies • Multivendor environments • Specific engineering roles and skills
Responsibilities and life cycle	Responsibilities and life cycle
• short lifecycle • IT is responsible	• Long lifecycles • IT, OT and Automation people are responsible from business continuity

OT and IT Cyber domains' information security's and cybersecurity's common object is to gain strong confidentiality, integrity, availability (CIA) and nonrepudiation of the information (data) and the systems (technology). In the OT, sometimes spoken as A-I-C for a reason of thinking about the organization or business prioritizes where most important object is the data or system availability in means of business continuity.

Critical infrastructure protection (CIP) or commonly in the ICS environments, availability is top priority for high reasons like environmental safety or life lost danger. Risks for losing the money can also be the prioritization reason and unwanted production stops are minimized. These situations or hazards can also occur if important process data is not available or data is invalid, and integrity of information is compromised. Integrity is compromised if information used for control process is not actually coming from the device (data source) where control function or program is thinking it is coming from. (Searle, 2018)

Availability and confidentiality of the SIS is high and example, integrity of updates in any computer or program is also important. The SCADA communication integrity or nonrepudiation between the SCADA and the substation is important (Li, Niu, Li, Ma, & Shen, 2014). The DCS availability or operator controls based on the tampered data might lead to environment or people safety danger. The PLC sensor data or firmware integrity could lead similar situations when processes are controlled wrongly.

Figure 2 presents security CIA Triad in ICS concept with nonrepudiation in the communication flow.

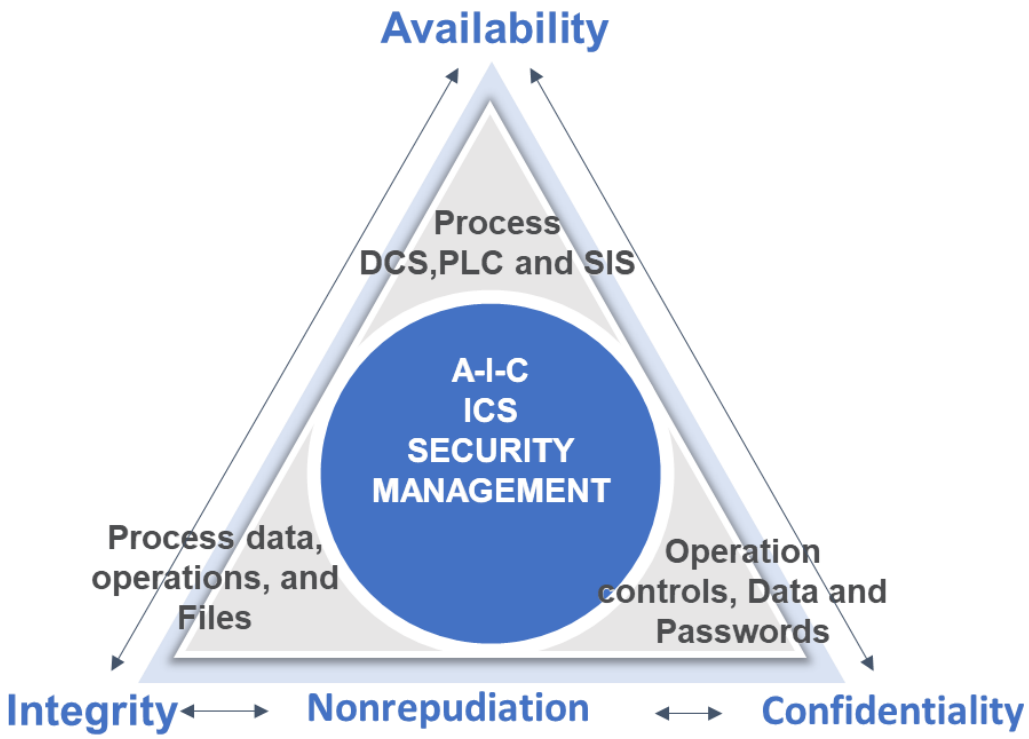


Figure 2. A-I-C of Industrial Control System and nonrepudiation in communication (Valmet Automation, 2021)

Secure by design and defense in depth can be used to describe security management of the systems or applications and components developed into them. The OT environment's ICS can be considered as insecure by design as expressed by Dale Peterson in his several post and talks (Peterson, 2013). Dale is referring to the design and feature documentation of the ICS and possibilities to attacker to use all the information build in the ICS and maliciously control the process or the devices used for process control. This possibility can make the ICS vulnerable for malicious actions or attacks without attacker need to exploit any software vulnerabilities, after attacker have food hold in the ICS networks, he or she need only know the valid commands towards the controller device.

3.4 NIST Guidelines for ICS security and log management

NIST SP 800-92 Guide to Computer Log Management discusses the most common types of challenges in log management and divides them in to three different sections:

- Log Generation and Storage,
- Log Protection and
- Log Analysis

Special Publication raises possible problems of generating logs in different type of endpoints, threats for logs CIA and inadequately and support of people who are analyzing the information of the logs. This means the ICS vendor devices may have lack of support for providing event for security monitoring system. Or the log format is following or including error or severity information numbers that only the ICS vendor engineer recognizes or is able of analyze, by knowing the device or process specific implementations.

Log Generation and Storage challenges in the multivendor ICS production environment are almost multiplied because of the different type and age of endpoint devices used for log sources. In multiple distributed control systems (DCS) large production facility's source devices connectivity to external log system is challenging because of process area and networks' segregations. Segmentation and communication segregation are implemented to clarify roles and responsibilities between ICS vendors, and improve the security within and between the ICS networks.

The vendor specific hardened endpoints for minimizing attack vectors is one typical challenge to be able add devices or systems as log source of OT or IT centralized system. Inconsistent of logs content and format originated from various vendors system is also challenge in the ICS environment. When comparing to the ICT challenges, the timestamp inconsistency in other hand may be challenge for the ICT environments. And because of the ICS are naturally time critical systems, time synchronous is not usually an issue. Time synchronization and accuracy is verified before production control or monitoring is stated with the system. (National Institute of Standard and Technology, 2006)

Similarly *Log Protection* in the ICS environment may be more challenging that it is in ICT environments. Because of the segregation of the multivendor environments and long life cycle of the ICS endpoint components, system might contain devises that does not offer any protection for logs, example cryptographic encoding of logs in transit or locally stored is not usually supported for older control system endpoints, nor they do not offer storage spaces long period logs storing. (National Institute of Standard and Technology, 2006); (Knapp & Langill, 2018); (Knapp & Samani, 2013)

Log Analysis for events severity originated from the ICS is difficult to do unless it is clear what role the endpoint device or the operation triggering the event has for the production process. Intrusion detection security event are naturally severe for ICS environment as it is for the ICT; however, false positivity quantity is usually bigger for the ICS. Or the deeper forensic action needs local access to endpoint or the ICS forensic is normally required to be executed by personnel who also have maintenance responsibility, toolkits, and permission to operate in the ICS environment. (National Institute of Standard and Technology, 2006); (Knapp & Langill, 2018)

NIST Special Publication (SP) 800-82 Guide introduces high level guidance for securing the ICS environments. Following SP 800-82 quoted recommendation is for the ICS security monitoring, logging, and auditing:

> *The security architecture of an ICS must also incorporate mechanisms to monitor, log, and audit activities occurring on various systems and networks. Monitoring, logging, and auditing activities are imperative to understanding the current state of the ICS, validating that the system is operating as intended, and that no policy violations or cyber incidents have hindered the operation of the system. Network security monitoring is valuable to characterize the normal state of the ICS, and can provide indications of compromised systems when signature-based technologies fail. Additionally, strong system monitoring, logging, and auditing is necessary to troubleshoot and perform any necessary forensic analysis of the system.* (National Institute of Standard and Technology, 2015)

NIST SP 800-82 risk management is divided to four parts (framing, assessing, responding, and monitoring). Monitoring is for continuous monitoring the system risks. Responding is for reaction to identified or detected risk. Responding actions should be done according to the processes in the risk management plan. Framing is framework for organization risk management to identify risks and example planning the response process. Assessing is a process to identify threats that might cause the risk to become real (Hao, Zhou, & Chen, 2016).

3.5 IEC 62443 and NERC CIP

IEC 62443 is a series of specifications for Industrial Automation and Control System (IACS) and is originating from the International Society of Automation's (ISA) 99, Industrial Automation and Control System Security. IEC 62443 series consists of (General, Policies and Procedures, System and Component) and these describes roles for user, system integrator and product supplier. IEC describes concepts of system zones and conduits to partition of system according to the security levels of the equipment (Hao, Zhou, & Chen, 2016).

System zones and communication channels between the zones are implemented with security controls like network flow permission (segregation), monitoring and deep packet inspection capable devices. Figure 3 describes these ICS network zones (levels 0 – 4) in model that is named as Purdue Enterprise Reference Architecture (PERA) (Searle, 2018), to this figure author of thesis has added roles of asset owners, vendor - and SOC services, roles that can be distributed to IEC62443 users, system integrators and product suppliers. IEC 62443 endpoint devices and equipment's are protected and monitored according to the selected security levels (SL) SL1-4 targets (Knapp & Langill, 2018).

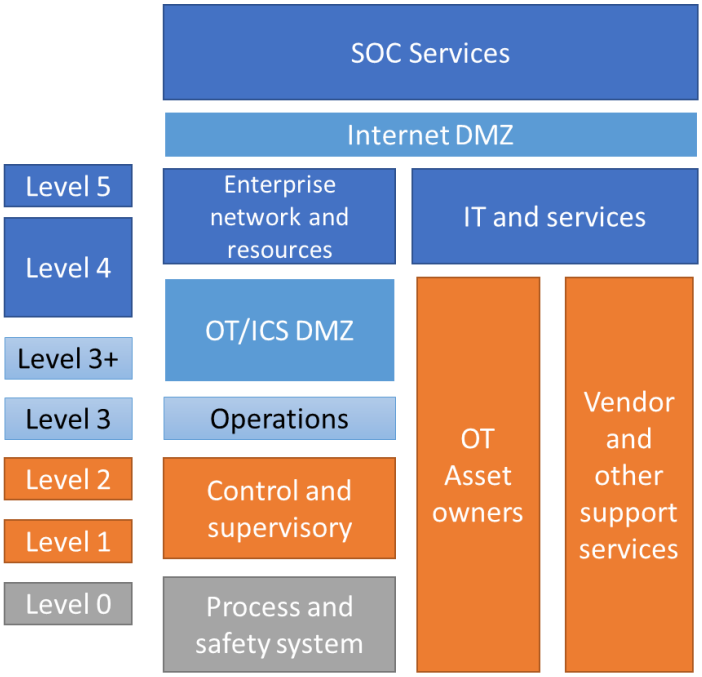


Figure 3. 62443 Purdue/reference model (Searle, 2018)

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Committee (CIPC) has role of developing standards that helps NERC to protect North America's critical electricity infrastructure physical security and cybersecurity. NERC CIP standards are highly referred also in other parts of the globe and together with IEC 62443 is one of the recommended guidelines for creating policies for Industrial control system cybersecurity protection and risks management. NERC CIP-007-6 defines requirements for System Security Management and Security Monitoring, see table 2.

Table 2. NERC CIP-007-6 R4 Security Monitoring, quoted from (NERC, 2014)

Title	**Cyber Security — System Security Management**
Number	CIP-007-6
Purpose	*To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against*

	compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
Background	*Standard CIP-007 exists as part of a suite of CIP Standards related to cyber security, which requires the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.*
Requirement part 4 Security Event Monitoring	*Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring*
4.1 Log events	• *Detected successful login attempts;* • *Detected failed access attempts and failed login attempts;* • *Detected malicious code.*
4.2 Generate alerts for security events	• *Detected malicious code from 4.1;* • *Detected failure of 4.1 event logging*
4.3 Where technically feasible	• *Retain applicable event logs identified in 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.*
4.4 Review a summarization or sampling of	• *logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents*

3.6 Security monitoring requirements and guidelines summary

Many of security guidelines and best practices are targeted to protect important assets security risks. Now these guidelines and practices have adapted as compliance controls by governments and organizations. Policies and technical controls that must be implemented or organizations are issued with fine of non-compliance. This might lead organizations to situation where they are high compliance scores but still be low in securing the assets. Using compliance standards as checklist to avoid penalty fines was one top issue in the report recommendations done by the University of Maryland (Stevens, et al., 2020). Report recommendation for standard and best practices authors was to define them to be used auditor checklists. Each security control requirement should be clear as possible to be used for checking compliancy of control or measure (Stevens, et al., 2020).

European Union Agency for Network and information Security (ENISA) the European Union (EU) Cybersecurity Agency is summarizing the matching the proposed industry sector specific security measure international standards, regulations and accepted good practices for example Energy and Drinking water supply and distribution as described in below table 3. Table 3 is a matrix table associating the standard, regulations, and guidelines of industry sectors giving detailed information especially for Security detection domain measures (Detection, Logging and Correlation and analysis) (ENISA, 2017).

From the ENISA's report the summary Table 3 list standards and guidelines, the ones with € (Euro) symbol identifies what of them are commercially locked and those ones require license fees for usage. Standards that are not referred in this thesis paper are the API STD 1164 (American Petroleum Institute) for the pipeline SCADA security and ONGC2M2 (Oil and Gas) Cyber security maturity model, both from Department Of Energy. ISO 27019 and 27001:2013 from International Organization for Standardization Information security controls for the energy utility industry and Information security management.

Table 3. ENISA baseline security measures for detection (ENISA, 2017, pp. 46 - 58)

		Domain & Measure (Detection)	Domain & Measure (Logging)	Domain & Measure (Correlation and analysis)
Energy (Electricity)	NIST SP 800-82	YES	YES	YES
	NERC CIP	YES	YES	YES
	ISO 27019 €		YES	YES
Energy (Oil & Gas)	API STD 1164 €	YES	YES	
	ONGC2M2	YES	YES	
Drinking Water	NIST CYBER SECURITY FRAMEWORK	YES	YES	YES
	ISA/IEC 62443 3-3 €	YES	YES	YES
	ISO 27001:2013 €	YES	YES	

Three of the table 3 standards or guidelines instructs or requires also collected information analyzing and correlation (NIST SP&CSF, NERC-CIP, ISO27019 and IEC). This requirement's purpose is for improving the forensic and threat identification capabilities, possible done as post-incident action in SIEM or SOC capable organizations.

3.7 Log Management and SIEM

Log management is a process of log collection from whatever sources are producing log output, storing, and protecting them example in centralized log management system. Log event collection can be implemented example by directing the events from the local host or device's log files or events storage to the centralized log management IP (Internet Protocol) address, using syslog messages and syslog protocol (Knapp & Langill, 2018).

Events can be also collected from the network traffic. Network traffic monitoring is performed example by using passive probes or similar devices to capture the network packets and send the logs or identified events to the central log management system (Knapp & Langill, 2018).

In the ICS, network monitoring is usefully approach to use for monitoring the resource limited IED, PLC and RTU type of devices. These ICS devices does not necessary provide syslog or syslog type daemon service for outputs of the events. The ICS asset inventory products are usually using this passive network traffic monitoring processes to create awareness of the whole holistic asset of network devices communicating in the network (Knapp & Langill, 2018).

Network traffic monitoring and the logs for security events are commonly provided from the firewall and the Intrusion Detection System (IDS) devices. For the ICS availability, it is important that these devices are providing the network events passively to avoid all possible disturbance in the network communication or in the device resources, especially in the process networks where the ICS real-time communication controls and protocols are in use (Dragos Inc, 2017). In the ICS networks many devices are communicating only with the devices connected in the same switch and therefore it's is important to monitor network traffic also closer to the devices, or there will be gap in the visibility (Behrens, 2021).

Collected security and other log information quality depends on what are logged and from where the logs are available. Quality of collected information also depends on how the logging is implemented into the applications or into the devices operating in the network. This is explicitly true for the applications and the devices used for security controls and monitoring. Overall, these defines the quality for the security forensics and analysis work that can be carry out using the collected logs.

> *From a high level, the best logs tell you exactly what happened, and when, where, and how* (Chuvakin & Peterson, 2010).

Into the below table 4 are collected the information what to log and what to include to the logs as it is discussed in the article "How to Do Application Logging Right (Chuvakin & Peterson, 2010). In the article Chuvakin and Peterson are describing ideas how the manual, automated and semi-automated analysis ideally can be improved with right type of critical logging, and without threat or forensic analyzer to deeply understand the application or the system. This same approach could be utilized for the ICS and the process specific logs. With right type of critical logging the OT SOC analyzer does not need to understand the industry process to threat

detection and only the roles working with the response action process, would need to have skills or knowledge of the ICS environment or the production process criticality.

Table 4. What to do for logging, quoted from (Chuvakin & Peterson, 2010)

What to Log		What to include	Reason for log
Authentication, authorization and access events	*Successful and failed authentication*	*Username*	*Who was involved?* *What happened?*
Changes	*System or application Data changes* *Application and component installations*	*Object (file, user account or data source),* *Status (succeed or failed)*	
Availability issues	*startups and shutdowns* *faults and errors,* *backup successes and failures*	*System, application, or component,* *Source (from where)*	*Where did it happen?*
Resource issues	*Exceeded capacity, resources* *connectivity issues and* *researched limits*	*Time stamp,* *Reason (password invalid)*	*When did it happen?* *Why did it happen?*
Threats	*Invalid inputs* *Other security issues*	*Action (how) and Priority*	*How did it happen?*

The logging types described in table 4 can be used as taxonomy rules for SIEM integrations. ICS asset specifically theses taxonomies could identify information such specified in the below list.

- Success and failed logins for ICS HMI, engineering, and network devices
- Changes of ICS HMI, engineering and controller applications and configurations
- Startup and shutdown of ICS processes in HMI, engineering, and controller devices
- Connectivity and resource limits from ICS HMI, engineering, and controller devices
- Threat detected from the passively monitored ICS network traffic or endpoint devices

Useful log information to be added from the ICS for the SOC analyzer to handle may be challenging because the SOC person skills may not be equipped with process specific information. Where for the ICS operator this information is probably very useful detail when analyzing incidents or doing post forensics task.

Security Information and Event Management (SIEM) System adds the threat identification and visualization capabilities to the log management systems by enabling analytical and contextual functions of processing the events (Knapp & Langill, 2018). The SIEM and Log Management systems differences can be sometime challenging to recognize and, in many times, the SIEM system can include the log management service as storage for the logs used for analyzing process.

Dr, Anton Chuvakin is analyzing and comparing the log management and the SIEM system relationships and functionalities in year 2010 published Whitepaper (Chuvakin D. A., 2010). In High-level Dr, Chuvakin is listing following functionalities between these two systems, SIEM and Log Management, list is quoted from (Chuvakin D. A., 2010).

SIEM

- *log collection*
- *aggregation*
- *normalization*
- *retention*
- *context data collection*
- *analysis (correlation, prioritization)*

- *presentation (reporting, visualization)*
- *security-related workflow and relevant security content.*

Log management

- *comprehensive log collection*
- *aggregation*
- *original (raw, unmodified) log retention*
- *log text analysis*
- *presentation (mostly in the form of search, but also reporting)*
- *related workflow and content.*

(Chuvakin D. A., 2010)

Uses cases for log management and SIEM systems may be the same or they can be the same technology solutions in the network. SIEM focuses on the security monitoring and Log management usage offer wide variety of use cases by providing auditing access for the logs and events collected from the OT and IT networks (Chuvakin D. A., 2010)

In the context of cybersecurity, the SIEM tools creates situational awareness to the process of perception. Collecting and aggregating the information from all the systems, enables the assessment of the reaction to the situation (Knapp & Samani, 2013). The SIEM tools provides' many automated processes to detect threats and risks from the monitored system using large amount of collected data.

- Correlating the data against known threat patterns
- Baselining the activities and alerting abnormalities or deviations from the baseline
- Calculation, filtering and visual measures of the asset risks indicators

In the ICS facilities, different security communication zones or the large SCADA network and the system distributions exits and some of these systems' local data collections or even the SIEM systems might exits. There might also be network segments where one-way unidirectional communication is only allowed. Some industries, external communications are not allowed at all, like in some level in the nuclear facilities the networks are completely isolated (Knapp & Langill, 2018).

When the ICS network zones connections are not totally restricted, secure cryptographically protected unidirectional connections can be established and used to provide the log data to the upper-level OT or IT SIEM system. This way, security information dataflows from the local collections (zone to zone) are encrypted. Encryption of log data in transit, protects from data tampering or espionage attempts (Searle, 2018).

When data is ingested in to the centralized SIEM system, events information normalization is required. Normalization of different events from source systems is classification process according to defined taxonomy. Normalization is needed for the data correlation process because there is no common log format or standard. Output of the events from the different source systems for example successful logon does not look the same and normalization process for the logon attempt is needed (Knapp & Samani, 2013);(Knapp & Langill, 2018).

Missing common standard for the SIEM data integrations was mentioned already in year 2014 published Zimmerman book (Zimmerman, 2014). Zimmerman is also mentioning the resources needed for paring and transforming the data from the different type of devices into the SIEM. For the SIEM system implementations, multiple options exist when selecting the commercial SIEM technology. The SIEM vendors have different supported data integrations available.

When author is writing this thesis, the situation is still the same, there are no common standard for the SIEM data integration. In the ICS cybersecurity customer requirements (received by Valmet Automation projects) mostly seen required support is for ArcSight Common Event Format (CEF). Other industry speciation's that Zimmerman is listing in his book (Zimmerman, 2014) are

- Common Intrusion Detection Framework (CIDF)
- Incident Object Description and Exchange Format (IODEF)
- Security Device Event Exchange (SDEE)
- WebTrends Enhanced Log File (WELF)
- Common Event Infrastructure/Common Base Event (CEI/CBE)
- Common Event Expression (CEE).

Addition to above Zimmerman's list author of the thesis specification of IBM's Log Event Extended Format (LEEF) can be added. LEEF is customized for IBM SIEM system product.

Protecting and securing the centralized log management or the logs and events in the transit to the log management system is import. The logs and log management systems are critical asset and should be protected. The log management system can be target of attacks or tampering attempts of the logs. Example adversaries can try to clean or tamper theirs tracks while operating in the system or in the networks. Non existing or invalid log events makes the post forensics analysis tasks challenging if not impossible.

The logs backups and retention policies are part of the protecting the log management system, see table 5. In the audit report created in the project of Investigating Security Issues Associated with U.S. Digital-Security Standards for NERC CIP 007-6, reported following issue:

> *We recommend mandating that organizations ship logs to a data warehouse for long-term storage and investigation support if needed* (Stevens, et al., 2020).

The above recommendation was given for concerning the event log retention requirement, where CIP 007-6 defines this requirement to be 90 consecutive calendar days during three-year period. Defined 3 years of retention time was identified to be high-risk with explanation that the rolling requirement is relative short time for investigations of advanced persistent threats (APT), APT adversary group can operate within networks for years (Stevens, et al., 2020).

The log storage and retention policies, and nonrepudiation protection from tampering attempts is common requirement and part of the guidelines for the security monitoring event log storages and protection capabilities. Nonrepudiation protection can be implemented in multiple ways, example using digital signing of the log files or checksum calculation during the log collections, there are also available products to be used as file integrity monitoring (FIM) systems. The FIM system is detecting the change and alter operations within the log management system (Knapp & Langill, 2018).

Table 5 presents the log retention requirements regulated by the authorities. Table is the “Cheat Sheet” by Michael Petrov from the Digital Edge released article Log Management Laws and Regulations (Petrov, 2016).

Table 5. Log retention requirements, cheat sheet (Petrov, 2016)

Regulation	Retention Requirement
Health Insurance Portability and Accountability Act	7 years
Payment Card Industry Data Security Standards	1 year
Sarbanes-Oxley Act	7 years
International Organization for Standardization (ISO) 27001	3 years
Federal Information Security Management Act	3 years
Good Practice Guide 13	3+ months
NERC CIP	3 years
Gramm-Leach-Bliley Act	6 years
Department of Defense Instruction	5 years
NIST	3 years

3.8 Security Operations Center and ICS

The people, processes, and technology are forming the SOC organization resources to search and identify anomalies or threats form the enterprise infrastructure. Enterprises in the process or manufacturing industries can have the SOC operations and services for the IT infrastructure and communication. Same SOC capabilities can be utilized for the OT or the ICS infrastructure as well; however, customization is needed for the ICS SOC operations best practices and processes when taking into use

for the ICS (Dragos Inc, 2017). The ICS specific customization is needed in the same way as when the enterprise IT security control and protection policies would be taken in to use for the ICS environment. Same IT processes and technologies does not necessarily work or are not supported in the ICS environment (Searle, 2018).

Building the SOC capabilities in the organization can be big investment in time and financial terms. Many cases organizations are relaying to technology and not to capabilities of people-oriented decisions when implementing the SOC. Christopher Crowley is discussing capabilities and technology considerations in his 2020 published whitepaper (Crowley, 2020). In this paper Crowley is using also his 2020 SOC survey questionnaire that was executed for the different models' organizations are using for defining capabilities in to their SOC (Crowley, 2020). In the whitepaper Cowley is summarizing following six models or appearance for SOC building capabilities.

- MITRE ATT&CK
- NIST-CSF
- SOC-CMM
- SOC Class
- Gartner Visibility Triad
- CrowdStrike-Splunk-Vectra Triad.

From these models the MITRE ATT&CK and NIST-CSF (NIST Cyber Security Framework) are not models to be used for SOC specifically. These models or frameworks are targeted for cybersecurity programs within the organizations. The NIST-CSF model for SOC focus on collecting the data from the organization assets risk management and then prioritize the SOC capabilities for the critical assets. Where MITRE ATT&CK model used for SOC capabilities focuses on the like hoods of attacks trees targeted to the organization and assets. Both models provide free long-term sources for SOC implementation projects, NIST CSF is practically endless commitment from U.S Government Department Commerce and MITRE-ATT&CK provides community-based threat intelligence (Crowley, 2020).

SOC-CMM (SOC Capability Maturity Model) and SOC-Class are models specifically for SOC implementation projects. SOC-CMM model is using tool for self-assessment process and SOC implementation requirements for five elements: Business, People,

Process, Technology and Services. Where SOC-Class model is suggesting eights elements: Steering Committee, Command Center, SOC Operations, Monitoring, Threat Intelligence, Incident Response Forensics and Self-assignment. With the eight elements, SOC Class is trying to link three components: staff, process, and technology for the SOC capabilities (Crowley, 2020). These models' SOC capability implementation period may be long for organizations building a SOC. Long projects for mitigating risk of the enterprises may not be the best option when more urgent steps are needed.

SOC-CMM tool for self-assessment was created in the Rob Van Os master thesis (Van Os, 2016) In his research work Rob Va Os focusing on the SOC maturity determination and there for maybe works better if some SOC capabilities exists in the enterprise.

In the Crowley paper (Crowley, 2020) CrowdStrike-Splunk-Vectra Triad is also presented even if this is not in the 2020-SOC-Survey (Crowley, 2020); however, the technology tools for SOC that are been used in large customer base provides experienced framework for building capabilities for SOC. In this model, three different strong vendors of cybersecurity technologies and services are recommended to be used for building the SOC capabilities in the organization.

CrowdStrike-Splunk-Vectra Triad model follows Gartner research results from article *Applying Network-Centric Approaches for Threat Detection and Response,* focus on network threat detection capabilities. The CrowdStrike-Splunk-Vectra Triad proposed to use tools and services in this Gartner triad model with implementation (Crowley, 2020).

- CrowdStrike Falcon platform for endpoint protection, vulnerability management and threat hunting
- Splunk's platform for log management and data aggregation for SIEM platform
- Vectra's AI (Artificial Intelligence) *to empower the enterprise SOC to automate threat discovery, prioritization, hunting and response* (Crowley, 2020).

In the Christopher's 2020-SOC survey, four most popular frameworks used for the SOC capabilities listed in the order of most used models first (Crowley, 2020).

1. 60% were using among others MITTRE ATT&CK
2. 43% were using among others NIST-CSF
3. 31% were using among others SOC-CMM
4. 7% were using among others SOC Class.

List of above statistics comes from 2020 survey (Crowley, 2020) analyzed by Crowley. Survey report identified 97 responders answering all the questions of the survey. Industries represented by the responders in the report were divided to Banking and Financial, Education, Government, Technology and Utilities (Crowley, 2020). Author of this theses was not able of identify the "Model to determine capabilities" - question from the survey report published.

Dragos *Insights into Building an Industrial Control System Security Operations Center* whitepaper (Dragos Inc, 2017) model for building SOC ICS capabilities focuses also on people, processes, and technology. Summarized capabilities are in the below list.

- People in terms of the skills and roles. Capabilities for working between the SOC IT skilled staff and ICS engineering skilled staff. IT skills are small part of equation and people need also understand how to safely response to the incident in the ICS process environment
- Processes in terms of doing the incident handling and analysis phase, considering the business continuity demands with minimum downtime. Communication processes in large facilities with the multivendor environment using interconnections between the systems and remote support services.
- Technology in terms of doing the log collection from multivendor ICS environment with embedded or vendor supported devices and hosts. Identifying and centrally collecting ICS logs and forwarding them up to the IT side SOC is mostly approved safe way of collection.

The forensic operations are one capability that may be required from the SOC team. Digital forensic in the ICS networks is introduced by Lee, Ropert M. and Luallen Matthew E. in the article (Lee & Luallen, 2014). In this article Rob and Matthew are comparing the digital forensic in the ICS process to investigation of normal problem when process data is not updating from the process controller components to the operator views, can this be because there is malicious activity in the ICS network?

Staring point and key step for successful forensic is to understand and knowing the network and asset. In IT SOC the asset understanding may require limited knowledge of the IT standard applications, services and operating systems or networks they are

running. In the multivendor ICS network, SOC would need to know also non-IT standard process applications and embedded devices (Lee & Luallen, 2014).

Above the required SOC key steps for forensic tasks can be supported and managed by the ICS environment operators, the ICS maintenance engineers and the ICS vendor support organizations.

The shared SOC services for the ICS was studied in the research work of (Dimitrov & Syarova, 2019). In the study Dimitrov and Syarova analyzed the known ICS incidents and identified Shared ICS SOC positive capabilities like the investment savings with the shared security knowledge staff resources equipped with capable to identify modern ICS threats by using latest technologies (Dimitrov & Syarova, 2019). Advantages in shared ICS SOC resources is also the capability of gathered intelligence information for ICS operating in specific industry sector (like oil and gas) or in geopolitical location.

Shared SOC studies also identified the lacking capabilities and challenges for collecting the data from the ICS and the embedded devices in the field. Secure connectivity to the multivendor environments from the external shared SOC services is also capability what is challenging to achieve. When adding connectivity to the interfaces or the device data, you also are expanding the attach surface of slowly security updated and the long-life cycled ICS environment (Dimitrov & Syarova, 2019);(Dragos Inc, 2017).

3.9 Incident response and ICS

The SOC capabilities and functions provided by the team are relating to the detection and incident response processes. In the book of *Ten Strategies of a World-Class Cybersecurity Operations Center* (Zimmerman, 2014) Zimmerman express the SOC and computer network as follows

> *The practice of defense against unauthorized activity within computer networks, including monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.* (Zimmerman, 2014)

The book (Zimmerman, 2014) is describing the incident analysis and the response capabilities in six different topics (Incident Analysis, Tradecraft Analysis, Incident Response Coordination, Countermeasure implementation, On-site Incident Response, Remote Incident Response) and four last are presented in table 6. Response and recovery steps for the ICS environment are critical activities because there are the ICS specific network assets, people and contractors working with the systems to keep processes available and stable (Dragos Inc, 2017). Table 6 is descripting the Zimmerman response capabilities and combines ICS specific notes.

Table 6. Incident response capabilities, quoted from (Zimmerman, 2014) and ICS specific notes

Capability	Description (Zimmerman, 2014)	ICS specific notes
Incident Response Coordination	*Work with affected constituents to gather further information about an incident, understand its significance, and assess mission impact. More important, this function includes coordinating response actions and incident reporting. This service does not involve the SOC directly implementing countermeasures*	In multivendor ICS network, organizations (internal and externals for example services) responsible for the ICS assets and production continuity must become part of coordination plans
Countermeasure Implementation	*Actual implementation of response actions to an incident to deter, block, or cut off adversary presence or damage. Possible countermeasures include*	ICS network communication termination is critical especially for large industry processes and may cause more damage than benefit, especially if the facility

	logical or physical isolation of involved systems, firewall blocks, DNS black holes, IP blocks, patch deployment, and account deactivation	process consequences are not properly understood
On-site Incident Response	*Work with constituents to respond and recover from an incident on-site. This will usually require SOC members who are already located at, or who travel to, the constituent location to apply hands-on expertise in analyzing damage, eradicating changes left by an adversary, and recovering systems to a known good state. This work is done in partnership with system owners and sysadmins.*	ICS engineering and operation staff may be lacking IT skills. Process systems may be located apart from cities. And ICS facilities may require special admittance approval for physically access into the facility area buildings and server rooms. ICS vendors support may be available only via remote connect support service
Remote Incident Response	*Work with constituents to recover from an incident remotely. This involves the same work as on-site incident response. However, SOC members have comparatively less hands-on involvement in gathering artifacts or recovering systems. Remote support will usually be done via phone*	Critical infrastructure's or specially categorized ICS environment or components may be physically isolated and remote connectivity is not possible. ICS countermeasures for active incidents or attacks in the factory IT networks (like office) may contain steps for air gap -isolation of production or ICS environment from the IT

	and email or, in rarer cases, remote terminal or administrative interfaces such as Microsoft Terminal Services or Secure Shell (SSH)	networks and remote connectivity becomes unavailable

Incident detection, Response and System Recovery defined in the NIST Special Publication 800-82r2

> *Incidents are inevitable and incident detection, response, and system recovery plans are essential. Major characteristics of a good security program are how soon after an incident has occurred that the incident can be detected and how quickly a system can be recovered after an incident has been detected. Incident response in ICS is closely aligned to disaster recovery, specifically to address the stringent uptime requirements of ICS. Incident Responders must be trained for ICS-specific scenarios, as normal methods of recovering IT systems may not apply to ICS.* (National Institute of Standard and Technology, 2015)

In this thesis author left the system recovery topic out of the scope purposely. It is important part of the response capabilities in the ICS network with special HW assets and possible with limitations for backup or spare part capacity. For the ICS SOC, recovery process capability is one that requires the ICS specification, because the ICS environment recovery process may be more depended on other OT assets and processes interconnected in the factory OT networks.

SOC incident response is usually executed in tiering hierarchy where Tier 1 is first group of people or team who will answer to the incident triggered or reported by the SOC tools or personnel operating the monitored environment. Tier 2 is group who can do more deeply analysis for the incident escalated by the Tier 1 people. Tier 2 requires more data and information from the incident and the environment. The processing flow could be executed in 3 tier hierarchy. Figure 3 illustrates SOC, incident response tiers, roles and flow illustrated in the book of (Zimmerman, 2014). In the figure 3 there is also SOC staff people who are doing threat update and SOC

tool tuning using the collected information and threat intel information from the external sources.

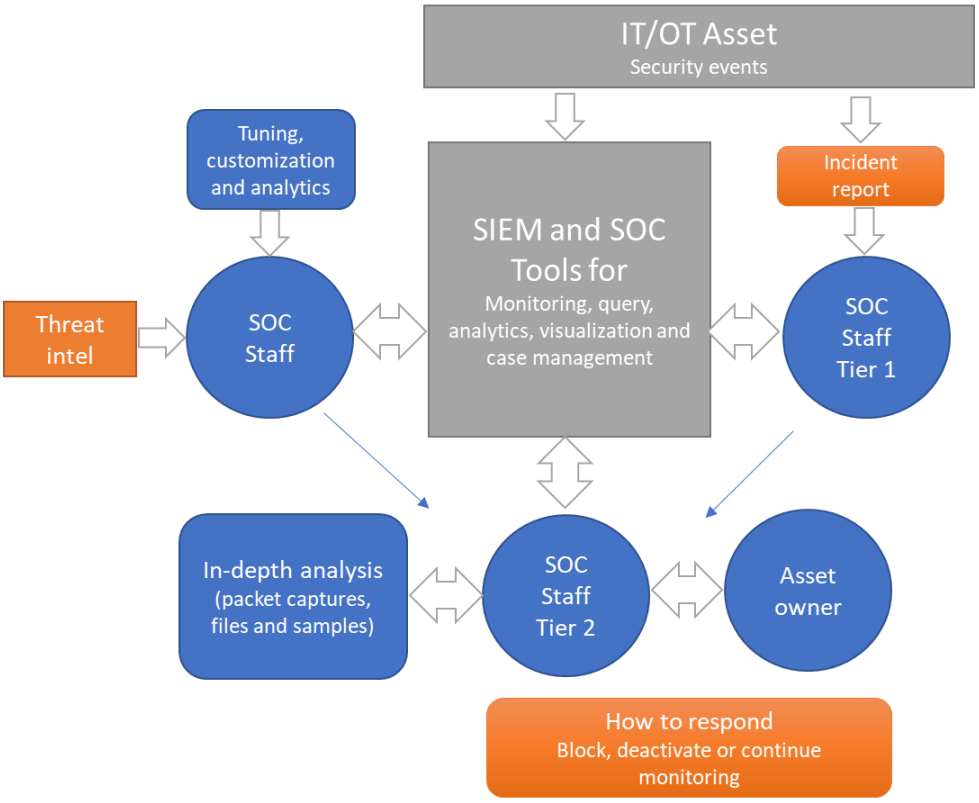


Figure 4. SOC and incident response (Zimmerman, 2014)

When OT environment processes and roles are adapted to the figure 4 the ICS information that could be described in the incident response flow are example:

- Tier 1, Incident could be triggered by the ICS vendor remote work activities, or remotely working ICS vendor person could identify and create the incident to Tier 1 group
- Tier 2, deep analyze and environment details support could be coming from the ICS vendor or organization who is maintaining the OT systems or networks
- Asset owner group working with Tier 2 could be the ICS vendors support organizations and response actions could be decided together with OT maintenance or ICS vendor organizations.

3.10 Situation awareness

SOC organization is creating situation awareness (SA) using the SIEM tools and threat intelligence data. As discussed, earlier the SOC room team and the ICS/SCADA control room team are monitoring systems to form SA of security (done in SOC) or stability (done in ICS/SCADA). Cybersecurity SA is usually requiring more information from the external systems or is targeted for higher number of assets. Where control rooms must focus on smaller number of assets for example specific process or manufacturing. Managing the risk or losing production systems CIA, SA about threats towards the critical infrastructures' ICS is important in national level and for any other organization level where the ICS is important asset for the business continuity.

SA process is usually described using originally military developed theory OODA (Observe, Orient, Decide, Act) Loop (Martin & Miroslav, 2017). In this theory SA of the environment is constantly Observed and targeted for new Actions that must be performed. Before Action is decided there is Decision done based on the environment observations and Orientation to the environment status (Svenson & Axelsson, 2020).

SOC to be effective it must understand the environment it operates and executes protection; this understanding is referred as SA (Zimmerman, 2014). Industrial environment infrastructure's protection is managed with up-to-date SA information (ics-isac, 2016). In the study of Architecture for the Cybersecurity Situational Awareness System (Tero, 2016), Cybersecurity SA capabilities are summarized to below list.

- Collecting events from multiple sensors like IDS or Intrusion Prevention Systems (IPS) and other implemented security controls
- Assets status information like change management and integrity monitoring information
- Analyzed information like identified threats or Indications Of Compromise (IOC)
- Information sharing between communities and organizations using standards like Structured Threat Information eXpression (STIX) or Trusted Automated eXchange of Indicator Information (TAXII) (OASIS Open)

National and organizations cybersecurity SA management require information sharing and threat detection capabilities. In Finland Traficom aka. National Cyber Security Center of Finland (NCSC-FI) is hosting communities/groups, Information Sharing and Analysis Centre (ISAC) groups that have common interests for cybersecurity. ISAC groups are divided to industry specific groups. These groups are sharing information to support national cybersecurity situation awareness. ISAC groups' personnel are forming nationwide network for information sharing. Groups also have role in decision making processes during the disturbance situations (Traficom ISAC). From the below list of ISAC groups first 4 industries are dealing with ICS systems in OT networks.

- Elintarvike-ISAC for food production and logistic industry
- E-ISAC for energy industry
- Water supply ISAC for water treatment
- KEMIA-ISAC for chemical industry
- FINANSSI-ISAC for financial industry
- ISP-ISAC for internet service provider industry
- L-ISAC for logistics and transportations
- MEDIA-ISAC for media industry
- SOTE-ISAC for social and healthcare industry
- ISAC for government organizations
- HAVARO-service users.

Traficom's HAVARO-service is national situation awareness intel information provider, HAVARO-users are from ISAC groups and its members. HAVARO-service's technology sensors provide threat intel and detection of possible organization targeted cyberattacks (Traficom HAVARO)

4 Research

4.1 Research work sources and target

OT and critical infrastructures have more connectivity to the enterprise external systems and more IT or cloud edge technologies are added to OT's ICS networks. These and global world with different level of ICS cyberattacks and threats for cybersecurity indents have increased the risk and like hood for OT environment's process controls system adversaries' attack to shutdown systems, maliciously control or lock down system using ransomware software.

Enterprise organizations risk management and business continuity requires that risks and like hoods of the attacks or incidents must be mitigated. New OT specific cybersecurity technologies and services are increasing in the industry markets. Cybersecurity companies are targeting their control and monitoring products for the OT network asset and for asset owners' risk management requirements. These targets are driving common understanding of adding more visibility to the OT network assets deployed by the ICS vendors.

This thesis was doing research work by using new OT security monitoring and logging requirements and the results of studies from OT/ICS security monitoring technologies and services offered for detection and response activities. Primary scope and sources used for the research was focusing on the event logging, log management and security response services like SOC. Research was answering to the thesis assigner's product development, project, and service organizations requirements to implement log management system into the customer ICS environment. The log management system maintenance and adaption require support services and interfaces for the customer assets – and security owners to gain more visibility to the ICS's they are using for production. The results will help Valmet Automation DCS product adaption to customer enterprise OT scoped risk management policies and mitigation targets.

Research process in the scope of ICS log management and security monitoring topics was collecting and analyzing information of the cybersecurity requirements enterprise organizations are defining for the ICS vendor products and services. This

information was available from the thesis assigner organization's ICS projects for different industry sectors.

Research was also analyzing the information collected from the ICS specific cybersecurity standards and guidelines recommended for the industrial sectors. Standards and guidelines were specified partly in the customer requirements for ICS vendors. Or this information was available from the thesis assigner's products, processes and roadmaps targeting to cybersecurity products and services improvements.

Information collection process was also using details of the commercial SIEM products and SOC services provided and studied by the OT cybersecurity companies or universities. Studies and whitepapers were available from the JAMK information libraries and author's previous gained access for the ICS cybersecurity SANS institute lectures and courses.

The thesis research was concentrating to identify security events logging and monitoring methods required for the ICS environment. Important aspect for the research work was to understand how the ICS log management system must provide the log information to the OT or the IT SIEM systems and how the ICS logs must be protected when the logs are collected and stored inside the ICS network.

Research sources used in the thesis work was also providing information about the SOC organization processes and roles used for threat hunting. Important aspect was also the capabilities required for OT incident response, in means of protecting and responding to the anomalies detected from the ICS vendor specific networks and devices.

When the ICS vendor is implementing monitoring – and detection capabilities with log collection system, the OT asset security monitoring, response - and auditing capabilities can be improved. The ICS environment and maintenance services are primarily designed for the industry's physical processes highly reliable automation (monitoring and controlling). Adding new security control and measure technologies cannot weaken the resilience of reliable process automation computer systems.

The thesis project was doing research and development of the centralized management system to be integrated into the Valmet Automation DCS system. The log management system was collecting the DCS network endpoint log events and storing them to the central location with possibilities to audit the events over time. Sources of the logs were endpoint operating systems and the applications executed on them. Implemented log management system is required to protect the events and to be able to forward the events to the external syslog server or SIEM system. The thesis focus was also to research the skills and services the log management's maintenance and SOC type of incident response would require from the thesis assigner organizations.

4.2 Research work methodology and methods

Research methodology selected for the thesis was the constructive approach. This approach was selected because it fits well to the thesis assigner's organization exiting product development and maintenance service processes. The thesis assigner's technology and services are used in the large field of customer installation base. Global service organizations are deploying the products and technologies to various OT networks and there for constructive approaches' innovative field study-based problem-solving model was excellent fit for the thesis project.

Figure 5 describes the key elements and the content for the thesis research's constructive methodology. Key elements for the construction: problem and solution meaning, solution in practical use, linking previous theories and research work theoretical contribution (Lukka, 2014).

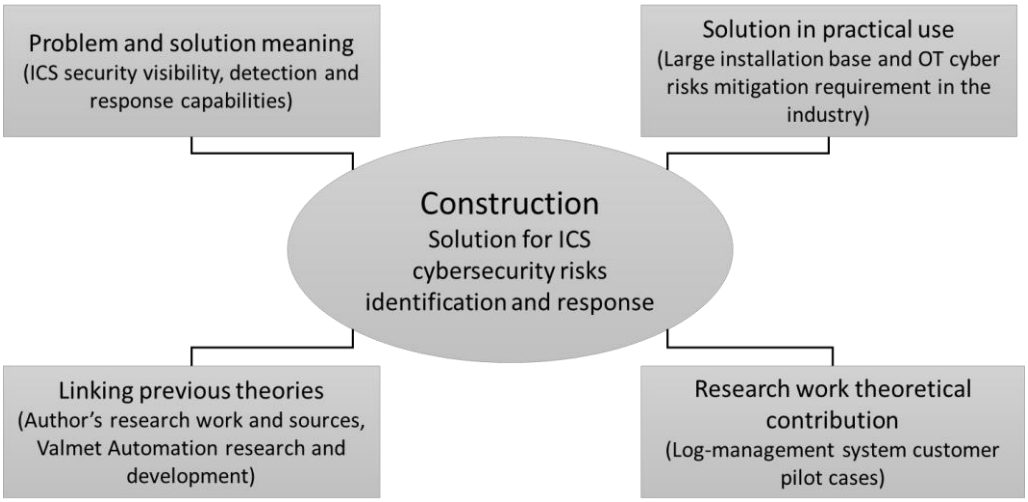


Figure 5. ICS Log management construction's key elements (Lukka, 2014)

Log management improvement and development research work were utilizing the benchmarking matrix, table structure visible in the Appendix 1. PDCA iterations was used for the requirements implementation management. Benchmarking table includes links to the log-management project's Jira board, backlog of issues and implementation requirements. Benchmarking table items were the results of the thesis.

Field based research work from the customer environment and OT cybersecurity requirements were also used in PDCA planning phase when the log managements systems were taking into use at customer facilities and log forwarding to external system was enabled. Figure 6 describes the process flow of using PDCA, benchmarking and Jira management tasks. Jira backlog of issues used for PDCA iterations was coming from benchmarking table and the field based research work when the log management system pilot was implemented.

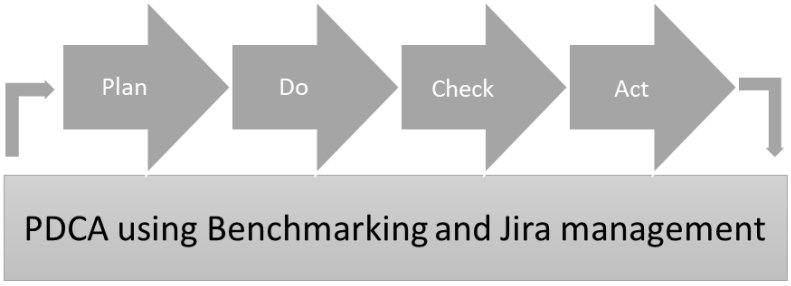


Figure 6. log management PDCA iteration cycle

Benchmarking table capability main categories are listed in the below and are not in any kind of prioritized order. The thesis log-management development project was focusing mainly on the log management category capabilities, field-based research issues and some SIEM category capabilities. The SOC category is included to provide more references and capabilities provided by commercial solutions and industry cybersecurity service. The benchmarking table was not used for resources skills development and contains Jira issue management only for technical and documentation requirements of a log management project. Benchmarking table's categories and elements are listed below.

- Log Management
    - Sources
    - Storage
    - Protection
    - Analysis/Audit
    - Security event detection
    - Log forward integrations
- SIEM
    - Dashboard and visualizations
    - Reporting
    - Alerting and notifications
- SOC and SOAR
    - Incident management process / ticketing
    - Automatic response / orchestration
    - Threat intelligence
    - AI and Machine learning

Sources for research project were easily identified and many of the sources are publicly available. Industry specific customer requirements and the thesis assigner's organization intellectual properties were available for the thesis author and are not publicly available.

4.3 Previous research

The thesis research project was done from ICS vendor point of view. How to adapt to new OT cybersecurity risk management requirements. Assigner organization should manage the changes that these OT requirements will have to the exiting installation

base of products. The assigner's service organizations maintaining these customer environments should also be preparing the need for OT security visibility in the IT SOC.

Doctor Anton Chuvakin has author of books and variety of papers for the log management, the SIEM and other security publications, these are available in the chuvakin.org (Chuvakin A.). SANS university and many OT cyber protection specialized companies are providing multiple resources and publications for the OT/ICS security risk management.

Previous research reports exist for many known ICS cybersecurity incident. How the ICS has been compromised and what are the possible advisory groups behind these attacks. There are cybersecurity companies and other organizations that are specialized to the ICS/OT cybersecurity topics. These companies' reports and researchers' studies are used as resources in the thesis's chapter 3. Same chapter also contains resources for SOC, SA and log management studies. SOC operations centers connected into the OT environment have not been used that much yet. There were few studies where ICS SOC was considered or how SOC should or can be implemented into the ICS, example Analysis of the Functionalities of a Shared ICS Security Operations Center (Dimitrov & Syarova, 2019).

Many of the research are focusing to the technology-based asset visibility or threat identification capabilities, done with passive network traffic monitoring. Simple log management or the SIEM system implementation to the ICS vendor environments don't have public research. All major global ICS vendor companies do have the SIEM and log management system supported by help of selected technology vendor. Author of the thesis was not able to identify studies of process industry environment vendors' cybersecurity services target example for SOC.

The result of the thesis will provide understanding for the ICS vendor provided asset visibility services and log management/SIEM capabilities. Enterprise OT asset owners also have possibility to use the ICS vendor's skills and technologies part of managing production business continuity risks. Asset visibility and security awareness building and especially SOC incident response processes can be integrated to the ICS vendor provided skills and processes.

5 Results

5.1 Research results

Research target was to get knowledge of the ICS/OT security monitoring log management, processes, and skills. That are used for detecting and responding to the ICS incidents or to the security risks identified example by the SOC. Cybersecurity responsible people or the SOC team skills in many cases are not equipped with the OT specific or even ICS vendor specific skills. People who maintain or provide the maintenance services for the OT/ICS environments are usually the first point of contact when there are any problems detected in the ICS software, computers, or networks.

The research results were used to implement log management system into ICS network, centrally collect DCS endpoint security information events and forward them to the OT syslog server or SIEM system. Log forwarding capability is implemented to add more visibility to the ICS asset security events. Installing log collectors and collecting security information from the DCS endpoints without losing system vendor guarantees or compromising the ICS network device communications can be challenging. With ICS vendor supported event collectors these challenges can be mitigated. Central log management maintenance and SIEM/SOC service descriptions and customer presentations were created part of the thesis results. Internal and customer presentation and meetings have been already kept with help of these results. First feedback from the customers have been good. Especially in cases where customer IT organization have been present. When the ICS vendor is prepared to support OT SOC connections with technology solution and services, it makes IT SOC adaptation to OT environment more simple process.

Research question: Can ICS vendor implement and maintain log management system used as source for OT SIEM and SOC capabilities?

Yes, ICS vendor implemented and supported log collector(s) with capabilities of forwarding and normalizing messages for the external security events and threat intel correlation system provides good option for ICS security monitoring and risk identification. Productizing ICS vendor specific log management system improves

thesis assigner's organizations' security detection skills. This can be achieved by learning the selected technology solution capabilities and maintenance task. ICS vendor supported log management improves the ICS vendor's HW and SW monitoring capabilities and capabilities for commercial SIEM integrations.

Main research question was also divided to following sub-questions. These questions are answered also in the later chapters:

- What interfaces and protection features log management must provide?
    - Figure 7 illustrates interfaces for log management ICS environment log sources, ICS maintenance management service (Tier 2-3) and interface for external SIEM system. SOC operator interaction with ICS maintenance service organization is also visible in the figure
    - Appendix 1 table lists requirements of log management's source and forwarding interfaces and features. Appendix table also illustrates the protection requirements for events collected and stored
    - Appendix 3 Service blueprint describes log management delivery phase 1 and monitoring incident response phase 2
- What skills are needed implement log management used for SOC operations in ICS?
    - Table 7 lists created service description documentations and planned trainings for service organizations. Service description of Consultancy SOC/SIEM connection describes the roles and responsibilities when SOC is using log-management as source for risk detection
    - Figure 7 illustrates ICS maintenance and SOC operator interaction service tiers 2-3
- What services ICS vendor can provide to support SOC capabilities for threat - and risk detection and incident response in the ICS environment?
    - Table 7 lists created service description documentations and planned trainings for service and sales organizations. Table also lists presentation that are been used in customer meeting to support IT SIEM/SOC topics and IT - OT synergies
    - Appendix 3 service blueprint describes log management delivery phase 1 and monitoring incident response phase 2

As the research results Valmet Automation DNA Central Log Management system development process was improved and the log-management system was delivered to the customer enterprise factory OT environment using the DNA central log management virtual machine template image and build in container services.

In the customer OT environment, they are using two segregated and segmented DNA DCS systems. For this reason, two separated central log management systems were implemented in to the DCS networks. The log-management systems were used to

centrally collect DNA network endpoints log events and forward them to the external syslog server that is operated by customer organization personnel.

The thesis results also provide possibilities for Valmet automation organization to continue the log management system development processes. This continuous improvement process includes log-management planning, development, and implementation of the new technical or functional capabilities. List of these capabilities are presented in the thesis result benchmarking table Appendix 1. And in the log-management Jira project backlog (not published in the report).

As part of research targets it was important to understand roles and services Valmet Automation customer service organizations would need to gain for the cases where there are requirements of Valmet automation systems' security events visibility. How these events are collected, normalized, and categorized for the external SIEM system used and provided by external SOC team personnel, who is responsible analyzing and detecting OT assets risks.

Service and project organizations have excellent expertise for different type industry process automation designing, building and maintenance. Cybersecurity or IT skills to understand example the SIEM, SOC and security monitoring terminology is something that must be also gained by these organizations. These skills are needed when working with the ICS security risk management for new and existing customer projects.

Following chapters are describing the research results more detailed and answers 1. What interfaces and protection features log management must provide? 2. What skills are needed implement log management used for SOC operations in ICS? 3.What services ICS vendor can provide to support SOC capabilities for threat - and risk detection and incident response in the ICS environment?

5.1.1 Log management implementation

Research implementation phase was continuing Valmet DNA Log management system development and proof of concept (POC) results. Earlier POC results for log-management project was introducing the technologies and high-level system

architecture. The thesis project was following POC results and target was to utilize and improve the containerized services for the log-management capabilities.

As for the research results, DCS system's key functionalities for centrally collect, protect, and forward important logs were developed or improved. The thesis work was utilizing already existing Valmet Automation development operations and processes for creating new versions and releases of the log-management project. Release of the log-management project was used for pilot delivery of central log management system into the customer OT environment.

One example of developed important interface feature for log-management system was the support for Common Event Format (CEF). CEF is the normalized message format integration for the commercial SIEM technologies. Log forwarding integrations are also visible in the Appendix 1 table. CEF implementation was done with the help of results collected from the log management pilot project and the thesis resources.

Central log management system was implemented to the thesis assigner, Valmet Automation's Security server concept. Security server concepts helps example patch and vulnerability management processes implementation work in the existing industrial control system. For this purpose, Central log management virtual machine template and development and deployment documentations were created. Security server's central log management add-on enables the DNA security events collection, visibility, and detection capabilities.

Documentation and guidelines for updating central log management system template image and services from new continuous developed versions was also provided during the research project. This will help to maintain and upgrade new versions and features of log-management system to the on-premises installed virtual machines. Appendix 2. gives high level description of security server concept's development and deployments when this server is equipped with central log management capabilities. Figure 7 describes ICS log management system and OT services interacting for better ICS asset security visibility, detection, and risks management processes.

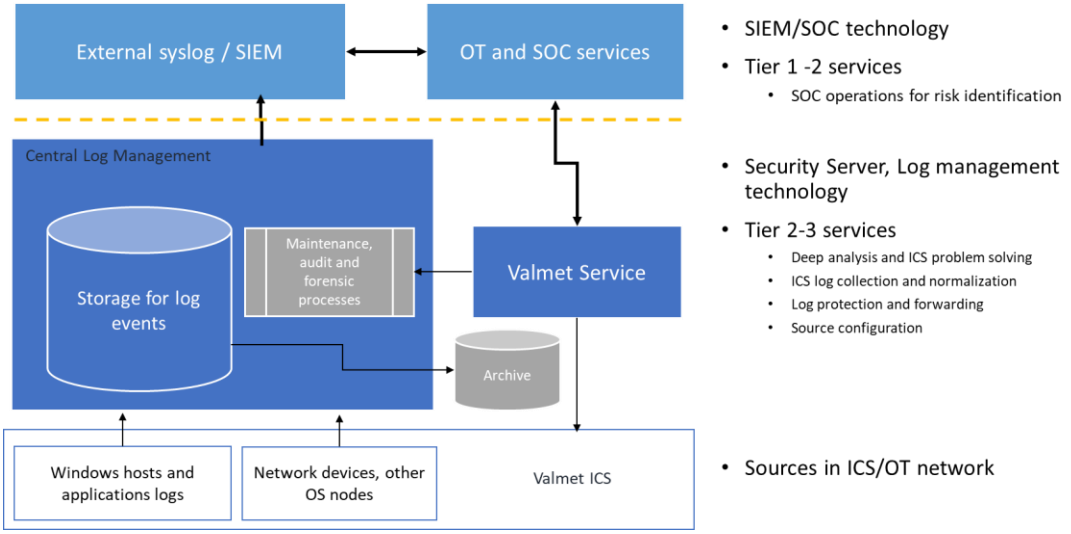


Figure 7. ICS log management and OT-SOC service tiers

5.1.2 Security logs monitoring and service skills

Log management trainings are planned and designed for sales, project, and service organizations to gain basic understating of central log management. Trainings target is to educate participants about the industry and the customer ICS security monitoring visibility and detection requirements. Training will also describe how the new security server central log management delivery adapts to these requirements.

For sales phase or other customer discussions forum, it is important to understand what are the SIEM and SOC support and service capabilities from Valmet organizations. Specify what capabilities and skills will be available from the Valmet automation provided products and resources. Terminologies and processes used between the cybersecurity professionals and the ICS vendor or industry process professionals might lead to misunderstandings. Target with Valmet internal trainings is to mitigate the like hood of this.

More specific service engineering level maintenance trainings are planned. This will provide required skills for the event source and SIEM forwarding integrations, especially when new event normalization actions are required by the SIEM operators or it is new interface/feature from the SIEM technology vendor.

Service organization documentations for deployment and maintenance services were created. Table 6 describes documentation, trainings and service descriptions created and the final status of the thesis project implementation. Appendix 3. Blueprint's phase 1, describes on high level the involved processes and responsible organizations when the central log management is deployed to the customer OT environment. Phase 2 in the blueprint, illustrates the CLM service processes for the incident response or for the situation awareness capabilities.

Documentation for the project installation process was created. Log management security events mapping document was created to describe security events in syslog message format. This document is used for service organizations when the SIEM normalization is required. Documentation help implementing the log management system to the existing Valmet automation system.

Project implementation document describes and gives guidelines of how to configure project settings for the central log management server when it is deployed from the developed virtual machine template or when new features are updated using offline docker image exports and deployment process. Similarly, the security event mapping document helps in the customer project implementation work. Document describes details how the Valmet automation system security event fields and values are mapped to the syslog messages. Syslog messages are used when the event is forwarded to the external syslog server. Mapping document helps on planning discussions of how the Valmet Automation DCS events are normalized for the SIEM technology or SOC personnel analysis purpose.

Service description attachments were created for service managers usage when customer discussions are in process. Service descriptions attachments describes and summarizes the services provided with the ICS implemented central log management system. Service descriptions roles and responsibilities in SIEM and SOC services is important for all organizations to understand what additional skills Valmet service people can provide for the threat detections and forensic investigations. And that the threat hunting and risk identification capabilities are within the SOC operator personnel, who are using the special skills and threat intelligent information for the threats that might increase risks for the customer OT environment continuity.

These research results are targeted to answer research project sub-questions: 1. What interfaces and protection features log management must provide? 2. What skills are needed implement log management used for SOC operations in ICS? 3. What services ICS vendor can provide to support SOC capabilities for threat - and risk detection and incident response in the ICS environment?

Table 7 lists documents and trainings created or planned as results of research projects. Table elements are categorized to

- Documentation, Central log management virtual machine development and project implementation guides
- Trainings, ICS Log management, SIEM/SOC principles for Valmet Automation sales, project, and service organizations
- Service descriptions, to be used in service agreement attachment for supporting scope, role and responsibilities between Valmet customer service, customer asset owners and SIEM/SOC operators

Table 7. Documentation, training, and service results and status

Type of	Purpose or object	Status
Document: Project installation guideline	For delivery and maintenance of central log management server using VM template and installation files	Implemented and tested in pilots
Document: Security event mapping to syslog message	Syslog forward integration and message field and value mapping/normalization to the external SIEM system integration	Implemented
Document: Log audit and visualization basic	Auditing the logs from log management system. Creating basic metrics and visualizations	Implementation planned not yet tested
Document: Internal and customer presentations	Internal and customer presentations of technologies and services provided with the Central Log Management	Done

Training: Service engineering level presentation	Details of the log management server implementation and maintenance for engineering personnel	Implemented and scheduled
Training: Service hands on training	Service engineers' hand on training of how to develop new events from log files and sources (Valmet DNA HW and SW events)	Requirement planned
Service description: Central log management in Remote monitoring services	Summarizes and describes central log management purposes and maintenance services	Done
Service description: Consultancy SOC/SIEM connection	Describes scope, roles and responsibilities used in customer OT environment together with asset owners, service - and SOC/SIEM provider organizations	Done

5.2 Result reliability and limitations

In the theory of the research, author has used sources where the log collection requirements and ICS security monitoring importance and best practices were discussed and studied. Real customer cases from the industry were used as resources and field-based studies, log management project implementations and requirements were coming from these customer cases.

The quality of threat detection capability depends on what are the security controls and measures implemented, these are also sources for the events. You can't get security monitoring events if the control or measure are not implemented into the ICS system. Integrity and ICS engineering modifications or possible malicious actions' information can't be detected and logged if there is no proper event generated or actions logs are not available.

Adding ICS log collection and management system itself is not enough for ICS integrity, change management or anomaly detection. Application and system logs and event generation capabilities must be also developed to be successful in ICS security monitor (What to log, what and why to add information to log (Table 4. What to do for logging). Valmet Automation DCS application log collecting, and normalizations did not start during the thesis project.

For analyzing and correlating multiple sources' security information in the central SIEM, it is important to normalize the data. Basic and high-level requirements are simple to follow; what happed, when where and how. Challenges are related to the needs for the information to be normalized against different SIEM technology and vendor specific integrations that are not standardized.

Same information event field name can vary between SIEM solutions or there is no clear specification for field names to be used. Normalization work or customization hours must be always considered when log management is integrated into different SIEM systems. OT asset owner's organization is providing the SIEM solutions or possible is planning to migrate to different SIEM vendor. During the theses project, commercial SIEM systems integrations with the log management system were not evaluated.

During the research there were no actual customer SOC processes implemented or tested. Even if the central log management can be integrated to the existing SIEM system this was not tested during the thesis project. Working and testing the ICS service engineer work together with SOC team will be carried out in later projects.

Network traffic captures or the events that are available from IDS devices were not implement to the central log management system. Network endpoint devices' logs are captured and same can be done also for the IDS/IPS events; however, in the thesis network traffic analyzing was not implemented to be part of central log management system features. SOC proactive threat and risk identification would need also network packet captures from the ICS environment. Missing the network packet capture capability from the central log management system can be seen a weakness. Especially if the protected and monitored system does not contain any additional IDS or other similar network flow threat detection measures.

Research project's constructive approach usually require longer time for innovate solution for the problem. During the thesis, time was limited for implementing all the required and identified capabilities for the log-management project; however, because of constructive approach supports many constructions for the solutions, implementation development can be continued after the thesis project. Implementations planning can be continued using the log-management project's Jira management board and theses research results can be used for later PDCA iterations.

Research work was also using field-based research results that were collected from the service engineers who were working with the log management pilot implementation in customer environment. By using these results, it was possible to mitigate problem of constructive approach missing the objectivity from the constructed solution. Using the service engineers in the pilot implementations also improved the documentation and template virtual machine quality. Issues identified in the documentation and virtual machine template were recorded to the Jira projects and fixes were done for pilot implementation and for the log-management master project.

Using the result Valmet Automation have excellent resources to continue improving log management product capabilities and example include new log sources from the ICS products, normalize events and severities. This would also improve the situation awareness for the customer's OT asset owners. For ICS vendor it is create advantage to be able develop log management and incident response capacities with the thesis developed results. The results will also give excellent resources for future research improve Valmet Automation organization's situation awareness and the security operation center service capabilities for the ICS enterprise customers.

6 Conclusion

Industrial 4.0 digitalization revolution and risks of OT cybersecurity incidents, known ICS attacks and their consequences are driving industrial automation systems' functional maturity model towards more security maturity models. This means that OT security solutions and processes are merging to the IT, or maybe it is vice versa, and the IT policies are merging to the OT policies and processes. ICS environment threats' proactive detection, ICS active monitoring, ICS response and recovery maturity is improving and increasing regardless of the industry sector.

OT environments' risk management starts from the information of the assets that need to be protected. Asset inventory using passive network monitoring technologies that support vide range of OT protocols is commonly the strategy how the knowledge for what to protect is built. This technology also adds visibility to the OT network and can contain detection rules for alerting anomalies.

OT networks' endpoint logging is also required for detecting events or anomalies inside the endpoint OS, applications, or security controls. Correlating all this together: network traffic and endpoint detected events give the best visibility and detection capabilities for events that requires instant response or more investigation/analysis.

Post forensic actions or deep analysis of threats or incidents require auditing capabilities for logs from longer period. Adversary actions capable of acting under radar so that instant intrusion detection mechanics are not identifying them. These advanced persistent threats actors can possibly be detected from collected logs and network captures. This capability requires a huge amount of storage. In ICS on-prem systems this is usually not practical because of limitations in storage space, especially capturing and storing all network traffic.

Threat and risk detection capabilities from known threat intelligence is clear; however, how the ICS vendor can add support for the technologies used for the detection is more challenging. Threat detections are now provided by cybersecurity companies using their commercial technology products, and IT is pushing their policies towards OT. The ICS environment specific solutions availability is improving,

business is booming, new companies and products are added to the OT cybersecurity marketspace.

ICS vendor may have challenges to add support for different technology installations that require changes to existing defense-in-depth strategies (endpoint protection, and redundancy and segmentations for networks). Network devices and firewall rules are altered, endpoint hardening policies are changed to allow 3rd party software installations and usage. Log normalization process and configuration may also need customization per technology requirements, and this customization must be done for each endpoint node in the OT network.

Response to the incidents in the OT networks requires more skills than the standard IT networks. The number of organizations involved in the OT response processes is larger than in IT world. OT probably contains the same organizations as in the IT side incidents; however, OT specific organizations (internal and external) must also be part of the response process. This way the right knowledge and skills are added to identify and understand the OT/ICS consequences for the physical processes and its machinery.

The thesis main research question was:

- Can ICS vendor implement and maintain the log management system used as source for OT SIEM and SOC capabilities?

During this research project I was working in the customer project where DCS central log management system was implemented in the customer OT environment. Answer to the main question is yes, ICS vendor can implement and support log management system for these capabilities. In this customer project there were no SOC capabilities added; however, log-management product template was successfully created, and SIEM/SOC consultancy service descriptions were created as research results.

During the customer project local service organization engineers found the central log management systems working very well for problem solving. To be able to search log events from single tool is easier than remoting to multiple endpoints for collecting the logs. In the project, the log events were also forwarded to the external syslog/SIEM server. The DCS central log management system's forwarding implementation gained more OT visibility for the customer organization. Customer

can now see the events of Valmet DNA DCS system in the same system where also other customer OT assets are providing log events and asset visibility.

In this customer log management implementation project, also improvement ideas were identified. Implementing and testing the new integrations were successfully done in the Jira's log-management project. This process gives confidence to the main research answer, the ICS vendor selected log collecting technology improves the vendor support capabilities when new features or changes are needed for better threat detection or visibility.

During the log management implementation project, there were no SOC organization involved nor incident response processes were not defined or agreed. Implemented SIEM forwarding capability did not specify field mapping or naming requirements for the DCS log management forwarding feature. How well research results will help in the SIEM specific implementations or adaptation to SOC processes and capability understanding are something that will be seen in the future when more central log management OT implementations and services are provided.

The main research question was divided into tree sub-questions:

- What interfaces and protection features the log management must provide?
- What skills are needed to implement the log management used for SOC operations in ICS?
- What services can the ICS vendor provide to support SOC capabilities for threat - and risk detection and incident response in the ICS environment?

What interfaces and protection features are required for the log management question is answered in the Appendix 1. Log management capabilities benchmarking matrix table, and in the figure 7, the ICS log management and OT-SOC service tiers, from what more specific system architecture designs were created but not published with the thesis.

Skills required question was answered during the log-management customer implementation project and project administrations documentation was created. These documents give instructions for the central log management virtual machine and containers template deployment. There are also documentation and training schedules defined for the sales and project people. Service organization's service

agreements description attachments were created for the central log management system maintenance and for SIEM/SOC connection support.

SOC threat detection and incident response process question answers are only research theory based and only implemented to the internal documentations and trainings. These OT SOC processes were not implemented during the customer project where the log management system was implemented in to the DCS system. It will be seen later how well log-management system's security events SIEM forwarding will help on SA for the OT customers or if the Valmet Automation organization SA and services will gain advantages from the implemented central log management systems.

I selected constructive approach for the research methodology. The thesis assigner's ICS projects there were not yet deliveries done with central log management using the SIEM integrations. Constructive approach was good choice to solve this problem for the existing installation base. Central log management's technology POC was already done and it was possible to use the results to continue adding security and the SIEM capabilities to this architecture. There was also requirement to understand what it would be needed from the assigner's service organizations to support and maintain OT SIEM and SOC integrations.

To implement solution from the constructive research approach, I was also using benchmarking and PDCA methods for selecting and planning the implementations of required capabilities during the log-management project. Log-management project was using Jira board for managing the tasks of the project. Using Jira and PDCA methods for development processes are well known in the thesis assigner's organization and because of this there were no need to learn or implement any tools for these methods.

The constructive approach worked well in the thesis project and with the assigner organization processes. Constructive approach's problem about lack of objectivity was mitigate with multiple industry sector customer requirements and with different type of the existing ICS installations. The thesis was not solving only problem of missing log management or SIEM system, research work was giving results for integrating log management and support services for OT asset owners in different

industries. Problem of constructive approach taking long time of creating a solution was managed with Jira planning and benchmarking. As all the thesis result were not yet completely implemented into the log-management project. It is now possible to continue the research work by using the Jira and benchmarking results to develop centralized log management products and DCS logging capabilities.

SOC implementation results like the service descriptions are only theory based. In the thesis log management implementation project, there were no SOC operator or service processes implemented. This means that incident response capabilities between and together with different asset owner organizations was not yet evaluated. My conclusions of the industry enterprise organization's SOC capability requirement is that these should be focusing more on the complete enterprise OT asset, not only to requirements for one vendor specific scope. In multi-vendor OT systems, SOC capabilities should focus more on the specific enterprise critical assets, including organizations' processes and risk management to protecting the business continuity.

Although it is not yet seen, but it could be in the future that the ICS security detection devices, services and SIEM systems would utilize the same process data for anomaly detection as the control room operators and mill personnel are using for mill and process operations. Vendor specific components such as historians, process controllers, engineering and human machine interfaces would need to support this capability and categorize security or anomaly identified information. Before the ICS environments are ready for these capabilities, OT environment is focusing on passive monitoring, logging and asset inventory solutions to identify cybersecurity risks from the processes controlling and monitoring computer system.

Enterprise organizations responsible for managing cybersecurity risks are inquiring services and technologies from the 3rd party companies and not from the ICS vendors. Technologies and service providers for service like SOC might be changing over time. This may be a problem for the ICS network asset owners and vendors. New SOC service provider might require different log collections and normalization of security monitoring information. Asset owners and vendors responsible for production and ICS availability must also be prepared to adapt and support these changes when new technologies and capabilities are selected for implementation.

For future, the central log management system development would be good if DCS endpoints and software executed in them logging is improved. When the ICS vendor adds more visibility and security events to the logs. It will also add more threat detection capabilities for the SOC teams. If the ICS logs would have capabilities to provide security categorized events from the process management or engineering tasks, it would extremely be useful to SIEM or SOC to visualize or detect anomalies from the ICS operations. Anomalies could be possible identified from the malicious control room operators and OT engineers' task when industry process is under control and monitoring by human.

In the thesis project the central log management system was not capable of monitor network traffic or analyze example .pcap files from the network traffic. These capabilities are currently targeted to be in the IDS/IPS systems. For future it should be determined if IDS/IPS events would be also collected to the same central log management system for forwarding purposes. Or would it be more useful if theses logs would stay in the IDS systems itself and maybe to be forwarded directly to external SIEM system and not forwarding events to central log management system.

The DCS central place for visibility of asset security events or security awareness would not be realized if two separated systems would be in use (log management and IDS). This would be the case when there is one log management system for endpoint and application logs storage, and another system (log storage) would be inside the IDS/IPS technology. Asset visibility, risk identification and threat hunting decidedly requires network traffic monitoring with IDS/IPS technology. Having log management and security events from known endpoint will create visibility for known asset/endpoints; however, you do not see unknown rogue endpoints that creates the critical risk in your OT environment.

The problem of missing one central place for SA and visibility, could possible be avoided when there is a SIEM technology used for central point. During my thesis project, commercial SIEM systems were not fully integrated to the log management system. And the SIEM system capabilities were not development into the log-management project; however, the capabilities like threat hunting and reporting were presented in the benchmarking matrix table. Future research work and implementations would be needed to create the ICS SIEM product and capabilities.

Maybe the commercial SIEM technologies should studied and integrated with the ICS vendor products and log management.

When I was starting the thesis project, I was hoping to get more practical experiences of the SIEM integrations and SOC team process when example incident response actions are required and planned. Unfortunately, this did not yet happen, and we need to wait until there are opportunities to Valmet service organizations to be part of implementing these incident management processes. Large ICS network events collection and threat detection can be challenging; however, this can be now achieved. We don't yet know what will happened or how are the incident response processes working in multi organization environment.

SOC discussions have already been taken, especially with energy and other critical infrastructure Valmet Automation customers. It is huge help when the ICS vendor product and services are prepared for SOC capabilities. In many cases the SOC operators and incident response teams are missing the OT/ICS skills to take any actions in production computer environment. This would normally slow down IT organization capabilities to deploy SOC services into their critical OT environment; however, when they get the support from Valmet Automation organization and products, they have been pleased to see the ICS vendor preparedness also for SIEM/SOC connections. There are not many ICS vendors who built physical process lines with computer automation, provides maintenance and readiness of state-of-the-art security services under the same house.

References

ALLEA - All European Academies. Accessed April 2021. The European Code of Conduct for Research Integrity. ALLEA - All European Academies.

Behrens, D. (2021). *Industrial Traffic.* SANS institute.

Chuvakin, A. (2021). *Chuvakin*. Retrieved from http://www.chuvakin.org/

Chuvakin, A., & Peterson, G. (2010). How to Do Application Logging Right. IEEE Security & Privacy.

Chuvakin, D. A. (2010). *Whitepaper The Complete Guide to Log and Event Management.* Retrieved from https://www.novell.com/: https://www.novell.com/docrep/documents/9x1wixnqhd/Log_Event_Mgmt_WP_DrAntonChuvakin_March2010_Single_en.pdf

Crowley, C. (2020). *20/20 Vision for Implementing a.* Retrieved from SANS Reading room: https://www.sans.org/reading-room/whitepapers/soc

Crowley, C. (2020). *2020 soc survey*. Retrieved from 2020 SOC-Survey A Tale of Two SOCs: https://soc-survey.com/

Dimitrov, W., & Syarova, S. (2019). *Analysis of the Functionalities of a Shared ICS Security Operations Center.* Sofia, Bulgaria: University of Librarian Studies and Information Technologies.

Dragos Inc. (2017). *Insights into Building an Industrial Control System Security Operations Center.* Retrieved from Dragos.com: https://www.dragos.com/wp-content/uploads/Dragos-Insights-into-Building-an-ICS-Security-Operations-Center-1.pdf

ENISA. (2017). *Matching of baseline security measures with sectors.* European Union Agency for Network and Information Security.

Finnish Advisory Board on Research Integrity. (2012). Responsible conduct of research and procedures for handling allegations of misconduct in Finland. Finnish Advisory Board on Research Integrity.

Hao, X., Zhou, X., & Chen, X. (2016). Analysis on security standards for industrial control system and enlightenment on relevant Chinese standards. Hefei: IEEE 11th Conference on Industrial Electronics and Applications (ICIEA).

Harp, D. R., & Gregory-Brown, B. (2016). *Industrial control Systems SANS.* Retrieved from ICS Library Whitepapers: https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf

ics-isac. (2016). *The Industrial Control System Information Sharing and Analysis Center (ICS-ISAC)*. Retrieved from ics-isac: http://ics-isac.org/blog/sara/

JAMK. (2017). *Pedagogical and Ethical Principles.* Retrieved from Studyguide: https://studyguide.jamk.fi/en/study-guide-masters-degrees/information-about-jamk/pedagogical-and-ethical-principles/

Johnson, B., Caban, D., Krotofil, M., Scali, D., Brubaker, N., & Glyer, C. (2017). *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure.* Retrieved from Fireeye Threat Research: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Kang, D., Kim, B., & Na. (2014). Cyber threats and defence approaches in SCADA systems. Pyeongchang, South Korea: 16th International Conference on Advanced Communication Technology.

Knapp, E. D., & Langill, J. T. (2018). *Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems Second Edition.* Syngress.

Knapp, E. D., & Samani, R. (2013). *Applied Cyber Security and the Smart Grid.* Syngress.

Kotofil, M., & Kopeytsev, V. (2019). *IT vs. OT: We are Much More Similar than We are Different. Comparing Process Control Room and SOC operations*. Sweden: Slideshare.net / CS3STHLM ICS/SCADA Conference 2019.

Laine, E. (2007). *Benchmarking-menetelmän hyödyntäminen yrityksen energianhallinnan työkalun toteutuksen suunnittelussa.* LAB University of Applied Sciences.

Lee, R. M., & Alperovitch, D. (2019). *Bridging the IT and OT Cybersecurity divide.* Retrieved from Dragos: https://www.dragos.com/resource/bridging-the-it-and-ot-cybersecurity-divide/

Lee, R. M., & Luallen, M. E. (2014). Making digital forensics a critical part of your cyber security defenses. *Control Engineer*.

Li, Y., Niu, W., Li, P., Ma, J., & Shen, Y. (2014). *Secure Networking Protocol with Identity Protection for Cooperation of Unmanned Platforms.* Tenth International Conference on Computational Intelligence and Security.

Lukka, K. (2000). The Key Issues of Applying the Constructive Approach to Field Research. https://www.researchgate.net/publication/281549256_The_key_issues_of_applying_the_constructive_approach_to_field_research.

Lukka, K. (2014). *Metodix Oy Article: Konstruktiivinen tutkimusote.* Retrieved from https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/

M. Geiger, J. B. (2020). An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems. *25th IEEE International Conference on Emerging Technologies and Factory Automation*. Vienna, Austria.

Martin, R., & Miroslav, L. (2017). OODA loop in command & control systems. *2017 Communication and Information Technologies (KIT)*. Center for Defense Information.

More, S., Jamadar, I., & Kazi, F. (2020). Security Visualization and Active Querying for OT Network. Kharagpur,, India: 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT).

Narayanamurthy, G., & Gurumurthy, A. (2016). *Benchmarking lean practices and performance measures of a hospital.* IEEE International Conference on Industrial Engineering and Engineering Management (IEEM).

National Institute of Standard and Technology. (2006). NIST Special Publication 800-92. *Guide to Computer Security Log Management*.

National Institute of Standard and Technology. (2015). NIST Special Publication 800-82r2. *Guide to Industrial Control Systems (ICS) Security*. National Institute of Standard and Technology.

NERC. (2014). NERC CIP 007-6. *Cyber Security — System Security Management*. North American Electric Reliability Corporation.

OASIS Open. Accessed April 2021. *STIX and TAXII*. Retrieved from https://oasis-open.github.io/cti-documentation/

Peterson, D. (2013). *Insecure By Design / Secure By Design*. Retrieved from https://dale-peterson.com/2013/11/04/insecure-by-design-secure-by-design/

Petrov, M. (2016). Log Management Retention Requirements. Digital Edge. Retrieved from Digitial Edge: https://knowledge.digitaledge.net/newsletters/log-management-retention-requirements/

Searle, J. (2018). ICS410 ICS/SCADA Security Essentials. https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/.

Stevens, R., Dykstra, J., Wendy, K. E., Chapman, J., Bladow, G., Farmer, A., . . . Mazure, M. L. (2020). *Compliance Cautions: Investigating Security Issues Associated with U.S. Digital-Security Standards.* San Diego: Network and Distributed Systems Security (NDSS) Symposium 2020.

Svenson, P., & Axelsson, J. (2020). *Situation Awareness and Decision Making for Constituent Systems.* Budapest: IEEE 15th International Conference of System of Systems Engineering (SoSE).

Tero, K. (2016). Architecture for the Cyber Security Situational Awareness System. In O. Galinina, S. Balandin, & Y. Koucheryavy, *Internet of Things, Smart Spaces,*

and Next Generation Networks and Systems (pp. 294-302). Springer International Publishing.

Traficom HAVARO. (2020). *Havaro*. Retrieved from Traficom: https://www.havaro.fi/fi/ukk

Traficom ISAC. (2021). *ISAC-infomation sharing*. Retrieved from https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat

Valmet Automation. (2021). *Valmet Automation cybersecurity services*. Retrieved from https://www.valmet.com/automation/services/cybersecurity-services/

Van Os, R. (2016). SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers. *SOC-CMM*. Luleå University of Technology.

Ylönen, J. (2021). *Paraphrasing video.* Retrieved from https://panopto.jamk.fi/Panopto/Pages/Viewer.aspx?id=7dfccb22-0600-4e05-98eb-acc200d9a4e7

Zimmerman, C. (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center.* MITRE Corporate.

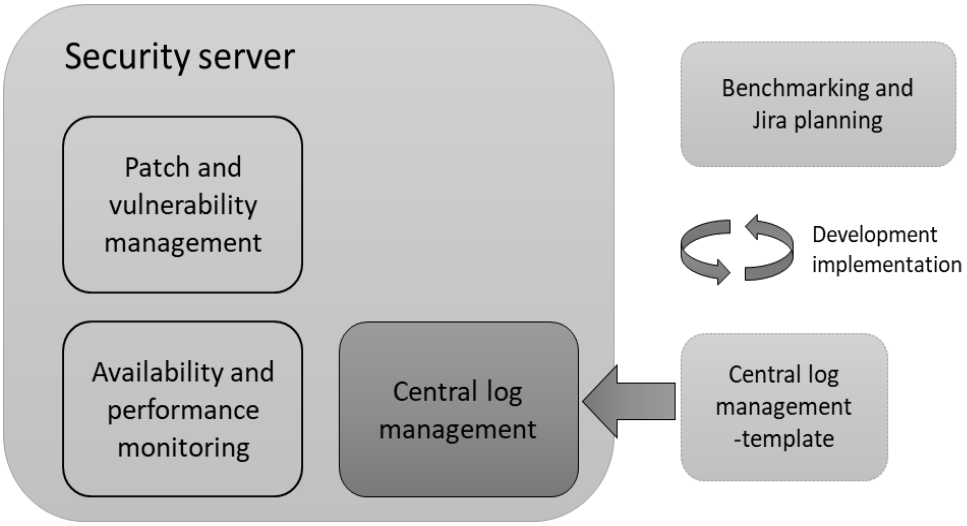
Appendices

Appendix 1. Log management capabilities benchmarking matrix table

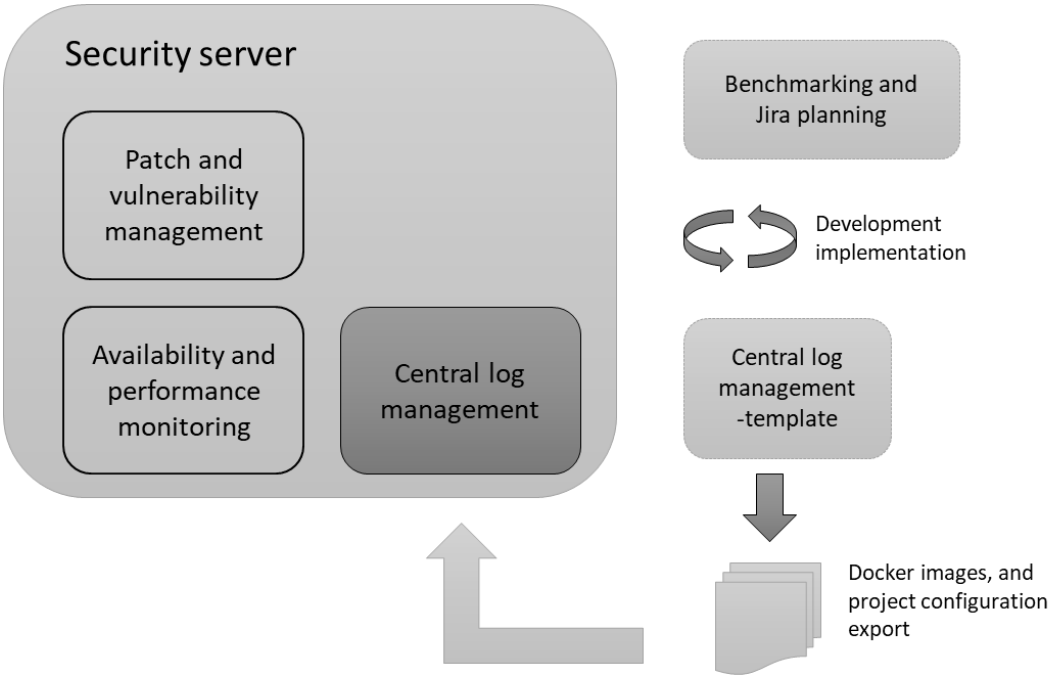
		ISO27k, NIST, IEC and NERCIP specific	DNA Central Log Management - system	log-mangement project Jira board/ticket	Technology solution (commercial SIEM/SOC)	Competitors (ICS Vendors, SIEM and log management)
Log Management						
Sources/types						
	Windows machine					
	Agent service in use					
	Agents central management					
	Application Log Files					
	DNA engineering, operation and management events					
	DNA Functional - PID block events					
	Syslog					
	PLC/PCS/IED					
	Netflow packages logs pcaps, any					
Storage						
	Storage encryption					
	Retention period / policies					
	Inludes raw logs data					
Protection						
	Encryption of logs in transit					
	Backup and restore of logs					
	External Backup					
	Backup encryption and protection					
	Identification, Authentication and Autohiyt					
Analysis / Auditing						
	Monitoring of logs					
	Searching from the logs					
	ICS/DCS/SCADA Operation logs					
Security events detection						
	Successful login					
	Failed login attempts					
	Malicious code					
	File and system integity					
Log forward / integrations						
	Syslog					
	Syslog TLS					
	CEF					
	LEEF					
SIEM						
Dashboard visualizatoin						
	Visualization Metrics and Trends					
	Centralized security dashboard					
Reporting						
	Report generation adn export					
Alerting and Notification						
	Detected malicious code					
	Detect Failure of event logging					
	File and system integrity					
SOC and SOAR						
Incident management process/ticketing						
Automatic response/orchestration						
Threat inteligence						
AI and ML algortihms						

Appendix 2. Security server and log management implementation development and deployment process.

Virtual machine template deployment



Docker image upgrade deployment



Appendix 3. Valmet DNA CLM and service deployment blueprint