Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P413-cd

A continuous OT cybersecurity risk analysis and mitigation process

Geir Kjetil Hanssen

SINTEF, Norway. E-mail: ghanssen@sintef.no

Christoph Alexander Thieme

SINTEF, Norway. E-mail: Christoph.Thieme@sintef.no

Andrea Vik Bjarkø

SINTEF, Norway. E-mail: andrea.vik.bjarko@sintef.no

Mary Ann Lundteigen

Norwegian University of Science and Technology (NTNU), Norway. E-mail: mary.a.lundteigen@ntnu.no

Karin Bernsmed

SINTEF, Norway. E-mail: karin.bernsmed@sintef.no

Martin Gilje Jaatun

SINTEF, Norway. E-mail: martin.g.jaatun@sintef.no

Operational Technology (OT) systems are becoming increasingly software-driven and connected. This creates new digitalization opportunities but can also increase the risk of cyber security breaches than can have severe consequences. Through a close dialogue with Norwegian actors in the oil- and gas industry and insight into the IEC 62443 standard we propose a process model for continuous risk assessment and mitigation. This paper explains the phases and details of the model and discusses its limitations and further work.

Keywords: Cyber Safety and Security, Operation Technology, Patch management, Risk Analysis.

1. Introduction

Operational technology (OT) systems, installed at offshore oil and gas (O&G) installations, must tackle extreme demands with respect to performance, availability, safety, and security. These can be highly complex systems which are well-integrated bundles of solutions and technologies from a large number of providers. OT systems includes a large number of sensors and actuators, historians, work-stations, different server solutions, firewalls, network equipment, and ultimately industrial automation and control systems (IACS), which ensure the overall supervision and operation of production, processing and drilling. Millions of lines of software code are involved in real-time operation and to produce, transfer and consume large amounts of data. The operation and maintenance of such systems need to be performed efficiently and safely with very high availability, and any downtime should be avoided for both efficiency and safety reasons.

To deal with complexity and to protect the most vulnerable parts of the total network infrastructure it is common to structure the system in levels, e.g., according to the Purdue model. The OT-parts of the system (e.g., the oil production and processing) where consequences of failures and followingly the need for protection are the highest, is separated from the IT-part of the system, which is most exposed to the internet and related vulnerabilities. The exchange of data and communication between the OT and the IT system is managed with a dedicated layer called the demilitarized zone (DMZ). Interactions between levels are restricted and controlled through separation into security zones and communications via well-controlled conduits. The mentioned layers can be split into one or more such zones (ISA/IEC 2021).

While the enterprise levels typically are based on office-grade commercial off-the-shelf (COTS) software solutions, the OT-levels are increasingly including data-intensive software solutions, such as operator support systems and predictive maintenance in addition to proprietary systems suitable for real-time operation. We see a trend of increased digitalization of oil- and gas installations and a convergence between the IT and the OT-levels (Hanssen, Onshus et al. 2021). Increased connectivity creates new opportunities but also severe cybersecurity challenges where connected software can be exploited to attack OT-systems, and hence cause severe safety implications.

As part of an ongoing Norwegian research project named Cybersecurity Barrier Management (CBM)[1], we have developed the first version of a process-model for continuous risk monitoring and mitigation of cybersecurity threats and vulnerabilities. We seek to align the process with the IEC 62443: Security for Industrial Automation and Control Systems - standard series (ISA/IEC 2021), which is getting a foothold in the Norwegian oil and gas sector. However, a lot of work is remaining to adapt and integrate it in operation.

The motivation behind defining a continuous risk process is that the current established best-practices for managing risk in these systems are too static, thereby failing to take into account that the threat landscape is continuously changing where vast amounts of information must be gathered and analysed in order to identify and carry out corrective actions. We claim that this constant change means that the understanding of the threat picture then also must be continuously updated.

The remainder of this paper will provide a brief background on relevant standards and initiatives (section 2), a layout of a continuous risk analysis and mitigation process (section 3), a discussion of the process (section 4), and finally some indications for further work (section 5).

2. Cybersecurity in industrial automation and control systems

The process model we propose in this paper is based on information that has been gathered via the CBM project over the past year and a half, through: (1) a review of the literature on threat intelligence, (2) a review of industrial standards that are relevant to IACS cybersecurity, and (3) an extensive dialogue with some of the largest operators of IACS systems on the Norwegian continental shelf. Through discussions with their cybersecurity experts, we have identified some needs that have motivated the proposed model.

The IEC 62443 series of standards describes procedures, management processes, technical measures and requirements for IACS (in this paper referred to as OT) with respect to cyber security. IEC 62443-2-1:2010 identifies management activities and associated requirements for OT cybersecurity management. Risk analysis, understanding and continuous evaluation is a pre-requisite for successful cybersecurity management in the standard. During operation, changes need to be risk assessed (from the safety and security perspectives), and mitigating actions must be made if the system is not secure enough.

[1] https://app.cristin.no/projects/show.jsf?id=2553016 (Accessed 2023 April 26).

To identify the need for changes, threats need to be monitored on a continuous basis to correctly understand the current risk picture. According to the recent *ISA/IEC 62443 Ontologies* (ISA/IEC 2022), a security threat is the result of a human threat or a technical threat. A threat exploits a vulnerability, a "*flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy"* (IEC TS 62443-1-1:2009). Threats are constantly changing; threat actors are looking for new vulnerabilities and means to achieve their goals. The successful exploitation of a vulnerability will lead to (negative) consequences for the system.

IEC 62443 defines Security Levels (SLs) (1-4) for IACS, based on the degree of risk reduction performed in the system, from low-risk reduction (SL1) to very high-risk reduction (SL4). An alternative view suggested by (Gordon 2021) takes an attacker-centric point of view as follows:

SL1 – offers protection against unintentional/accidental misuse

SL2 – offers protection against intentional threat actors with few resources, general skill, and low motivation

SL3 – offers protection against sophisticated intentional threat actors with moderate resources, IACS specific knowledge, and reasonable motivation

SL4 – offers protection against sophisticated intentional threat actors with extensive resources, IACS-specific knowledge and high motivation.

IEC TR 62443-2-3:2015 (ISA/IEC 2021) defines requirements for establishing a patch management system for IACS. Patch management is an important activity to remove or mitigate vulnerabilities from a system. Information from suppliers, computer emergency response teams (CERTs), cybersecurity threat intelligence suppliers or internal information sources is used to assess the criticality of vulnerabilities and accordingly to prioritize patching.

Risk assessment of the expected impact of patching OT needs to be carried out. Patches need to be tested before they are implemented. Only if the risk assessment and the patch testing provide evidence that the patch process will not disturb the OT operation, the patch can be installed. This may imply, contrary to IT systems, that the whole installation must be shut down with operational downtime and lost revenue as consequences. Thus, if patching is deemed infeasible or too costly, other measures may need to be taken (temporarily) until the system can be upgraded to remove the vulnerability. Examples of alternative measures are:

- Product reconfiguration
- Configuration and updating of firewall rules
- Intrusion detection system
- System hardening
- Physical security measures
- Segregation of the OT from the IT system.

IEC 62443 is not the only framework available that offer guidelines and concepts that can be useful. For example, the NIST Cybersecurity Framework (National Institute of Standards and Technology (NIST) 2018) has been created to help organisations understand and manage threats and risks related to critical infrastructure systems. The core part of the framework consists of a set of security controls, focussing on five different areas: Identify, to develop the organisation's understanding to identify and manage relevant risks; Protect, to develop and implement appropriate safeguards for protecting the systems; Detect, to identify and monitor security threats; Respond, to take action when cyber security incidents occur; Recover, to maintain and restore services and systems affected by such events. The framework is intended to be used in a systematic process for identifying, assessing, and managing cyber security risks and it is applicable throughout the whole lifecycle of a critical infrastructure system. The framework also includes four implementation "tiers", which describe an organisation's ambitions in terms of its risk management activities. The selected tier is intended to be used as a part of an organisation's roadmap, in which the organisation describes its approach and ambition to reduce cyber security related risks.

3. A continuous process

Based on the fact that the threat situation is in constant development we have drafted a process model that enables constant updating of the collective information, internal and external, on the threat situation. Cybersecurity is in many ways a race between the adversary and the owner of the asset (system or facility) that is being protected, and it is therefore important to manage information at a constant pace and to react properly and timely in cases where risks can lead to threats that can compromise the asset.

The model (Fig. 1) maps to the operations and maintenance phase of the IEC 62443 IACS lifecycle. It is a continuous process of (1) information gathering, to maintain an overview of (2) threats and vulnerabilities of assets under protection, (3) a risk analysis using the updated threat information, and (4) relevant mitigating actions.

(1) Information gathering: Multiple sources are in use to continuously maintain a threat overview in relation to the OT assets that are under protection. These can be CERTs such as KraftCERT/ InfraCERT. Other sources may be Norwegian National Security Authority (NSM), Norwegian Police Security Service (PST), National Cyber Security Centre (NCSC), etc. Security operation centres may also provide threat reports, as well as suppliers (potentially followed by a patch notification). Other third parties, such as Dragos, McAfee, or other specially hired threat intelligence firms may also provide information.

Asset owners are monitoring their own systems, using security information and event management (SIEM) systems, such as the Splunk platform (Splunk) and similar tools and technologies. Suppliers are also providing vulnerability information to the asset owners and issue security notifications and patch information.

One identified concern is the potentially overwhelming amount of unstructured information that is available and followingly the challenge of building an overview and interpreting this information in an effective, precise, and timely manner.

(2) Threat-Asset-Vulnerability: The information is used to constantly maintain an understanding of how threat actors (previously known and new) may pose a threat by exploiting vulnerabilities (previously known and new), and, ultimately, how these may compromise assets that are under protection.

(3) Two levels of risk analysis: This unified overview of threats and vulnerabilities drives a continuous risk analysis, both at the system and the component levels. It is however yet not defined what ‘continuous’ really means in this context. Probably, this will be a trade-off that balances the information that has to be analysed, which can be both voluminous and incomplete, and the need for a timely response. Furthermore, the need for a timely response will depend on whether the system has been sufficiently isolated or not. For sufficiently severe threats, corrective actions (potentially prepared upfront) may be initiated without any preceding (time consuming) risk analysis. The most important topic to address urgently when a vulnerability is discovered in an OT system, is to assess how or if it may be exploited, and if exploited, how it may affect production, safety etc. of the total system, and how severe the consequence may be. Newer methods like consequence-driven cyber-informed engineering (CCE) (Idaho National Laboratory 2020) may be used to identify where to direct the focus.

The ISA/IEC 62443 series does not have much details to offer regarding how to perform the risk analysis. ISA/IEC 62443, part 3-2 (Security risk assessment for system design) provide guidelines for the development phase, but no guidelines on how to carry out assessments in operations. We therefore see a need to establish practical guidelines and supportive tools. We however think that some of the results from carrying out the processes described in part 3-2 are useful, such as the grouping of assets in zones and conduits (ref. guidelines *ZCR 2.1: Perform initial cyber security risk assessment*, or the use of risk matrixes and consequence and severity scales (ref. Annex B). Furthermore, part 3-2 also mention several risk assessment methodologies that can be used as a basis, such as ISO 31000 (International Organization for Standardization 2018), NIST SP 800-39 (National Institute of Standards and Technology (NIST) 2011) and ISO/IEC 27005 (ISO/IEC 2018).

(4) Relevant actions: Depending on the severity of a risk, possibly in relation to the security level (SL) of the asset, actions may be needed on the short term (possibly a temporary fix) and/or on the long term (permanent). There is not yet a complete overview of relevant types of actions, but some of these may be:

- Restrict operation, e.g., shutdown, or restrict or remove access to the asset.
- Intensified internal monitoring and enhanced awareness for specific threats that have been identified as a short-term action before permanent protective measures have been put in place. Identified threats can for example be relevant threat actors that are (1) using specific tactics, techniques, and procedures that are used to conduct a cyber-attack. (Tactics describe why an adversary performs an action, and techniques describe how they do it (Lee 2019)), or (2) actors that are known to exploit certain vulnerabilities.
- Compensating measures. Typical examples include physical access control (locked doors and cabinets) to protect access to systems where authentication is infeasible and using firewalls to protect vulnerable systems that cannot be patched.
- Update existing cybersecurity barriers
- In cases where established barriers are not relevant: establish *new* barriers
- Implement patches (from suppliers)

In addition to these four steps of the process, there is also a need for supporting elements:

Asset management: In order to run a continuous risk analysis there is a need to keep track of assets under protection, and how these relate to threats and vulnerabilities. Part 2-3 of IEC 62443 describes how patch management should be managed (one of several relevant types of mitigations), and states: *"Asset owners shall maintain an inventory of devices that is appropriate and complete, covering the devices based on the risk acceptance of the system".* Part 3-2 (on security risk assessment) explains how to identify the devices that should be included in the list. Furthermore, part 2-3 states that: *"Asset owners of IACS at or above SLT-2 shall list of all devices that can be updated by modification of their functionality, configuration, operation, software, firmware, operating code etc., referring to them as updateable devices."* Furthermore, there are also requirements for protection against unauthorized access and modification of this information.

Risk-mitigation tracking: There is a need to keep track of all risks that are identified (including new ones), and how these develop over time. Correspondingly, there is a need to keep track on respective mitigations and corrective actions as well as to document which risks are accepted (and un-mitigated). The concept of a continuous process, based on information gathering, risk analysis, and corrective actions will have to be defined according to a set of domain (O&G IACS) specific restrictions that protect operation that (normally) cannot be disturbed:

- Monitoring of OT-assets cannot disturb operations
- Monitoring cannot create new cybersecurity vulnerabilities
- Corrective actions cannot disturb operation
- Updates or new barriers cannot disturb operation

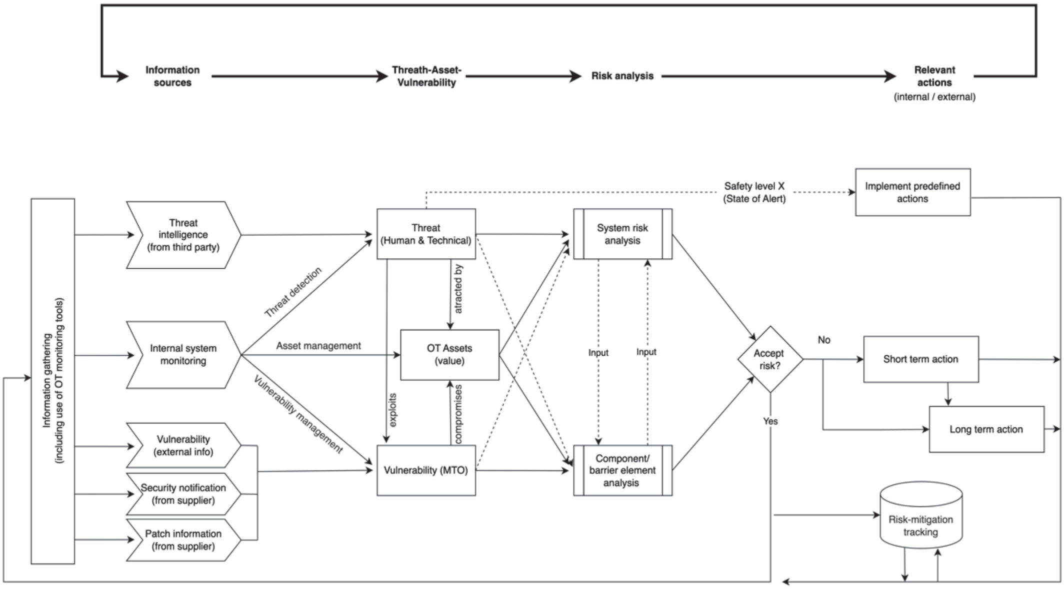

Fig. 1 A continuous risk analysis and mitigation process

4. Discussion

The process model is indented to complement the IEC 62443 standard series by addressing how to manage cybersecurity threats in the operations phase as this is yet superficially covered in the standard. From our industry partners we see that the main challenge is not having access to relevant data (on threats and vulnerabilities), but rather having the necessary capacity to process and use such information in a timely manner. Hence, there is a clear need to automate information management and potentially also analysis. Following this, there are also ongoing discussions on whether to visualize the cybersecurity status. This is inspired by safety barrier panels that some operators are using to maintain an updated overview, typically as a map of the facility showing status on various components. It is however challenging to visualize cybersecurity status of ICT-systems, which are more abstract or logical, than physical.

To develop the process model further there is also a need to better understand restricting factors and how to mitigate these. Monitoring of production-near equipment must for example not hamper stability, and new monitoring solutions should off course not open new vulnerabilities.

We claim that the analysis and mitigation of risks must be a continuous process to implement corrective actions “in a timely manner”. It is however not yet clear what would be the required turn-around time of such a process. If segregation and isolation of vulnerable components work, it means that they are not exposed to cyber-attacks, at least not from external threat actors. However, we believe that the development of connected cyber-physical systems does challenge these well-proven principles, and that segregation over time becomes less of a guarantee for cyber security.

The proposed process fits very well into the risk-based approach to manage cyber security that is proposed by the NIST Cybersecurity Framework, in particular regarding the defining and implementation of the implementation "tiers". As described in Section 2, organisations that choose to adopt the framework can utilize the framework's profiles to define a roadmap for reducing cyber security risks, which includes selecting a suitable tier to describe its ambition. The highest-level tier, "Tier 4", implies that the organisation has implemented a continuous cyber security risk management process, where they monitor, respond and adapt to the changing threat and technology landscape. Tier 4 also means there is an organisational-wide approach to manage cybersecurity risks, which have become a part of the organisational culture. Further, just like in the proposed process, Tier 4 implies that the organisation receives, utilizes and shares threat intelligence, both internally and externally with its collaboration partners. The proposed process in this paper will hence aid organisations that aim to implement and maintain a mature approach to cyber security risk management, which is compliant with the NIST framework for improving critical infrastructure security.

5. Further work

Through our ongoing research we have identified a set of relevant goals to develop the process model into an approach that can be implemented in practice, and that will enable continuous management of cybersecurity in OT.

1. Identify and describe the domain-specific limitations and restrictions for such a model, where information gathering (e.g. monitoring) and implementation of mitigating actions (e.g. patches or other actions) are not allowed to disturb operation and compromise safety functions, in particular within the lower OT-levels.

2. Build a more complete overview of the information input and division of responsibility to such a continuous risk assessment process. The information input includes threat intelligence, internal system monitoring, and cybersecurity information from the supply chain, including cybersecurity patches. In sum, it is a rich and continuously updated body of information that

must be managed. As part of this more comprehensive overview, it might be relevant to add sub-models to the process model for the internal system monitoring process and the system risk analysis.

3. Detailed risk analysis principles, approaches, and techniques at the system and component levels. Such a risk analysis should ideally have some qualities such as being fast, being automated or assisting human experts, and being able to exploit a rather large amount of information. This could be done using structured methods to focus the analysis to the most critical scenarios, like e.g., CCE.

4. Suggest visualization of threats, vulnerabilities and impairments in e.g. a cyber-security barrier panel. Inspired by safety barrier panels, how could a cybersecurity barrier panel look like, and how would it support cybersecurity professionals?

5. Suggest a continuous risk analysis approach requires sufficient inventory management (protected assets). How can such an inventory be defined, maintained, and used?

6. There is also a need to maintain a CMDB (Configuration Management Database) and to keep track of identified risks and mitigations. What would be good practices and solutions for this? This overlaps with the considerations on asset inventory.

7. Industry experience shows that it is challenging to follow up on cyber security with all the suppliers and vendors. We therefore see a need to further investigate how asset owners should assess and manage cyber security risk in the supply chain, to ensure supply chain cyber resilience.

Acknowledgements

The input and feedback from partners in the Cybersecurity Barrier Management project is highly appreciated. The work presented in this paper was founded through the Norwegian Research Council's funding scheme with project grant nr. 326717. We also would like to thank Thor A. Buan for valuable contributions.

References

Gordon, J. (2021). "The Essential Guide to the IEC 62443 industrial cybersecurity standards." Retrieved April 26, 2023, from https://industrialcyber.co/features/the-essential-guide-to-the-iec-62443-industrial-cybersecurity-standards/.

Hanssen, G. K., T. Onshus, M. G. Jaatun, T. Myklebust, M. Ottermo and M. A. Lundteigen (2021). "Principles of digitalisation and IT-OT integration."

Idaho National Laboratory (2020). Consequence-driven Cyber-informed Engineering (INL-EXT-20-58089). Idaho Falls, USA.

International Organization for Standardization (2018). Risk management.

ISA/IEC (2021). IEC TR 62443 Security for industrial automation and control systems. Part 2-3: Patch management in the IACS environment.

ISA/IEC (2021). ISA/IEC 62443 series of standards on the cyber security of industrial automation and control systems, International Electrotechnical Commission.

ISA/IEC (2022). ISA/IEC 62443 Ontologies Release 1.

ISO/IEC (2018). ISO/IEC 27005 "Information technology — Security techniques — Information security risk management.

Lee, A. (2019). Cyber Security Risk Management and Risk Assessment Methodology Template.

National Institute of Standards and Technology (NIST) (2011). Managing Information Security Risk.

National Institute of Standards and Technology (NIST) (2018). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1.

Splunk. "The Key to Enterprise Resilience." Retrieved April 18, 2023, from https://www.splunk.com/