Human Factors in Cybersecurity, Vol. 168, 2025, 40–46
https://doi.org/10.54941/ahfe1006141

Towards Scalable Solutions of Operational Technology Cybersecurity in Smart Energy Networks

Reijo M. Savola

University of Jyväskylä, Jyväskylä, Finland

ABSTRACT

During the last years, OT (Operational Technology) cybersecurity threat landscape has become wider, due to the increase of digitalization, more sophisticated cyberattacks and increase of ransomware. Dependence on energy and information networking and operational technology inevitably exposes smart energy networks to potential vulnerabilities associated with networking systems. This increases the risk of compromising reliable and secure use of them. Network intrusion by adversaries may lead to a variety of severe consequences from customer information leakage to a cascade of failures, such as massive blackout and destruction of critical infrastructures. Cybersecurity should be considered as core business enabler for smart energy networks. We introduce a cybersecurity governance model to cover the common cybersecurity solutions, processes and architecture for operational technology environments. The model will enable establishment of common and standardized capabilities towards creation of competitive advantage in the global business in securing industrial automation. The model covers common architecture, interoperation, processes, tools and requirements, including the essential information for OT cybersecurity improvement, and SOC service up-scaling.

Keywords: Operational technology, Cybersecurity, Security operations centers, Supply chain security

INTRODUCTION

Digitalization has created the need for industrial companies to take more actions in cybersecurity protection. However, as they do not have enough background in it, coping with more and more sophisticated attacks has become an issue. Cybersecurity of OT (Operational Technology), also commonly referred to as industrial control and automation systems, has been brought into the spotlight. Recent examples of attacks with dramatic consequences include those suffered by Maersk (Churchill, 2017), Norsk Hydro (Briggs, 2019), SolarWinds (Danish Centre for Cyber Security, 2021).

Information Technology (IT) and OT have both their own legacy approaches in cybersecurity management. OT includes hardware and software systems that monitor and control physical equipment and processes. Typically, OT is used in production environments. OT has been like an isolated island from connectivity perspective, where the stakeholders have not been so knowledgeable of how cybersecurity should be managed in their system. Currently, there are growing needs to increase the effectiveness, efficiency and scalability of cybersecurity of OT, leading to adaptation of capabilities of IT cybersecurity, and integration of IT and OT. Today's rapid escalation of cybersecurity threats has given rise to operations centres dedicated to handling them, the SOC – Security Operations Centre. SOCs are generally considered to be best provided as a service especially for those wishing to concentrate on their actual business rather than mastering the multifaceted attributes of cybersecurity. Because OT environments do not allow similar types of updates as IT environments, they need to be tested in other ways to not interfere with the actual production operations.

This paper discusses OT cybersecurity threats and building blocks for enhanced and scalable cybersecurity governance through data gathering, threat intelligence, SOCs (Security Operations Centers), and related governance model.

SMART ENERGY NETWORKS

With the help of information and communication technologies, it becomes possible to increase the performance of energy systems with intelligent energy management. These new energy systems begin to depend heavily on an associated cybernetic system, acting as a control mechanism to efficiently use distributed resources, generating savings for the final consumer, and promoting sustainability in the energy sector (Siluk et al., 2024).

Cybersecurity should be considered as core business enabler for smart energy networks. In energy solutions, sector integration means integrating various energy sectors to electricity transfer networks. This increases overall complexity of the electricity networks, but it also enables to balance out each other's peaks in consumption and generation, with benefits towards carbon-neutral and flexible energy system. Cyber secure digital platforms will be the key to manage this increasing complexity driving a sustainable energy transition.

OPERATIONAL TECHNOLOGY CYBERSECURITY THREATS

In the following, we discuss briefly example cybersecurity threats in OT environments. Cyber threat actors can use online and offline threat activities targeted towards the organization with OT environment directly, or indirect activities, utilizing second or third parties in the OT supply chain. The motivation to attack varies from financial goals to politics, and even to terrorism and hybrid warfare.

In OT environments, safety and uptime (availability) objectives are dominating in cybersecurity management, compared to the situation in IT, where availability is not that much emphasized. Security needs in OT are more and more emphasized, because cyberattacks can cause severe financial loss in production and energy environments and even impact the public safety and security.

Persistent Ransomware Attacks

Persistent ransomware threat actors dominate the threat landscape in OT environments. There has been an 87 percent in ransomware attacks against industrial organizations in year 2024, with a 60 percent rise in ransomware groups affecting OT (Ribeiro, 2025).

Malware Targeted to OT Processes

The goal of OT malware can range from modifying how an industrial process operates, resulting to availability issues, through to more destructive cyber-physical attacks. Examples of OT malware include Stuxnet, Havex, BlackEnergy2, Industroyer or CrashOverride and Triton (U.K. National Cyber Security Centre, 2021).

Data Destruction

Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt the availability of systems, services, and network resources. Data destruction will likely render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives (MITRE, 2024).

Manipulation of Control

Adversaries may also manipulate physical process control within the OT environment. Control manipulation methods can include changes to set point values, tags, or other parameters. Adversaries may manipulate control systems devices or possibly leverage their own to communicate with and command physical control processes. The duration of manipulation may be temporary or longer sustained, depending on operator detection (MITRE, 2024).

OT Supply Chain Attacks

Cyber threat actors target the OT supply chain for two general direct purposes: to obtain commercially valuable intellectual property and information about the OT in use. Moreover, supply chain attacks are an indirect route to access an OT network. In addition, high-sophistication cyber threat actors target the OT supply chain to obtain sensitive information about clients' OT assets that they can use to develop cyber sabotage capabilities (Canadian Centre for Cyber Security, 2021).

ENHANCED AND SCALABLE CYBERSECURITY GOVERNANCE

To answer the challenges of OT cybersecurity, we suggest a novel OT cybersecurity governance model, with building blocks of enhanced data gathering, threat intelligence and SOC functions.

It is obvious that a novel cybersecurity governance model for OT is required, driven by knowledge of risks, vulnerabilities, threats, assets, potential attack impacts, and the motives and targets of potential adversaries. Traditional reactive approach to cybersecurity strategy is no longer effective, nor is it defensible. The focus will be in best secure and resilient governance practices in sector integration, maintenance and processes, handling of security requirements, risks, objects and measures and management of multiparty operations.

The OT cybersecurity governance model aims at considerable cost savings, as well as cybersecurity effectiveness and efficiency and scalability.

Two Pillar Research Approach: Testbed and Governance Model

The research approach consists of two pillars. Firstly, we have a testbed environment to test electrical equipment such as relays and software representing critical network elements in an OT environment, with relevant use cases. The software that we use comprises two main categories. Open-Source-based SOC software will monitor the operations and transfer relevant information. Another software class belongs to industrial equipment. The built environment will reflect the real-life SOC environment.

Secondly, a governance model, integrated to the testbed is introduced. The model is based on the results of use cases and inner and outer level-specific requirements that are considered. The use case inputs from testbed work in a simultaneous environment and analysis of threat assessment-based risk scenarios will create outputs for the governance model (Simola et al., 2023).

The security infrastructure may include unnecessary or multiple actions, or it may be configured inefficiently. The aim of is to find out more effective configuration. This includes removal of legacy software and devices, consolidating external connections to internal network, grouping assets, defining allowed actions, listing allowed applications, and simplifying processes to decrease false positive alarms.

Testbed Environment

Technical scalability and enhancements of OT environment can be probed in a testbed environment, a crucial part of the overall solution. The testbed has a core function as in validation of the actual solutions. As a part of this research, a testbed environment was developed by the University of Jyväskylä, Finland. It is a unique platform for testing various OT vulnerabilities and threat scenarios. The environment consists of a process plant with its OT devices and the control and monitoring network, reflecting a smart energy use case. An energy production system needs to fill the requirements with validated functionalities, such as cybersecurity and operation controls.

The plant can be controlled with local and remote SCADA system. Remote control is implemented with a Long-Term Evolution (LTE) connection. Monitoring is implemented by mirroring the network traffic from the central switch and OT device log information from the central logging points of the process plant and the control center. The data transfer between the process plant and the office space is remotely monitored with a separate SOC. Furthermore, a distinct isolated network is employed for the surveillance of OT device logs, while a different network is used to directly request OT device logs from the device itself (Simola et al., 2024). The blocks in the testbed allow investigation of scalability, with the possibility to replace devices and their connections in an easy way. Scalable interfacing is a clear goal of the research.

Along with scalability goals, the aim of is to find out more effective configuration. The security infrastructure may include unnecessary or multiple actions, or it may be configured inefficiently. The aim of is to find out more effective configuration. This includes removal of legacy software and devices, consolidating external connections to internal network, grouping assets, defining allowed actions, listing allowed applications, and simplifying processes to decrease false positive alarms.

Data Gathering and Decision Support Automation

Data gathering and decision support automation consists of (i) data gathering and filtering, and (ii) decision support automation parts. By data gathering and filtering here we mean the processes of data capture (logging) and data filtering for the purposes of analysis in the OT environment. The challenge of coping with varying vendor-specific sensors and protocols in OT environment should be tackled. This includes investigation of what kind of data is needed to build up a good situational picture of cybersecurity, and what type of metadata is needed.

Core questions are which systems are monitored in detail, and which events are important. Decision support automation offers decision-making cybersecurity experts and/or software information to make effective, efficient and justified decisions. The decision points include, for example, mitigation of incidents, eradication of problems so that production is not disturbed, and how to recover from the situation when production has already been disturbed.

Monitoring a process and its data traffic in OT environments aids in creating a holistic situational awareness, in addition to process awareness, which includes elements such as steps taken, transferred data, used devices, and software versions. If a cyberattack uses specific process as an attack vector, process-based monitoring aids in forensics due to documented and monitored content. Additionally, monitoring a singular process through various data sensors aids in auditing process function events. For example, if a cyberattack manipulates data at a particular step of a process, such as during a log request or SCADA (Supervisory control and data acquisition) command, it may be analysed in forensics towards a specific section in internet infrastructure where the step would occur (Simola et al., 2024).

Threat Intelligence and Incident Communication

The importance of timely and scalable threat intelligence information is increasing, especially in the OT domain. There are some threat intelligence and incident communication environments available, such as AlienVault (AlienVault, 2016) and Malware Information Sharing Platform (MISP, 2025). However, OT environment sets specific requirements for both the types of threats and incidents, and their communication.

As Artificial Intelligence-based attacks become more and more common, the reaction time is getting shorter. It is of outmost importance to be share the OT threat information among in a trusted way the stakeholders, critical infrastructure companies, government, researchers and different actors in the supply chain.

Security Operations Centers

Governance model for OT cybersecurity enables effective service model use of SOCs for OT. The demand for SOCs has increased tremendously lately.

This is a major shift in the industry, allowing a move from in-house handling of cybersecurity to a service model, both leading to improved security and a significant amount of new type of opportunities in the enterprise market for various ecosystem players, and effectively increasing the total addressable market of the SOC providers. The current SOC business lacks standardization: the main stakeholders have their own validation models.

Functionalities are distributed to internal and external domains (on-site and SOCs). Subsystems of the smart energy network are connected to the SOC by wired or wireless connections. The SOC can use common procedures and processes for different kind of operations. This enables automation of the continuous cybersecurity monitoring, along with AI techniques, making the SOCs as correlation points for every logged event within the sector connected energy production system and overall smart energy network system.

Governance Model

Traditional reactive approach to cybersecurity strategy is no longer effective, nor is it defensible. The focus will be in best secure and resilient governance practices in smart energy sector integration, maintenance and processes, handling of security requirements, risks, objects and measures and management of multiparty operations.

From the cybersecurity perspective, ENISA's governance framework for developing national cybersecurity strategies (ENISA, 2023) is used as a basis for OT governance model. This governance model has been divided into four levels: political, strategic, operational, and technical levels. The term governance, or governance model, can be understood in many ways. However, the primary function of a governance model is to organise cybersecurity functionalities based on regulations, policies, guidelines, standards, and protocols. The technical level of administration aims to link the implementation strategy so that technical and technological development takes place simultaneously, which is essential in cyberspace, a rapidly developing field where new threats and challenges arise simultaneously as new technological opportunities and solutions. The operational and technical levels are crucial for the formation of situational awareness. The cybersecurity governance model must consider the workplace culture, financial factors, risk and threat management, other security plans, and reporting processes that already exist in a company so that the board receives all the information it needs to put the goal of governance into practice.

CONCLUSION

Use of information technology solutions in OT environments like smart energy networks has created the need to take more actions in cybersecurity protection, in an effective, efficient and scalable way. We have discussed the building blocks for effective, efficient and scalable cybersecurity governance for OT environments, with smart energy networks as an example. The building blocks include a testbed environment, related data gathering and threat intelligence functions, SOC service up-scaling, and a supporting governance model, addressing the cybersecurity from regulations, policies, guidelines, standards, and protocols perspective. The exact solution can be validated in a testbed environment with enough flexibility. Arrangement of data gathering and management is a core cybersecurity and resilience process, supported by threat intelligence work and information sharing.

ACKNOWLEDGMENT

The work has been carried out in CSG (Cybersecurity Governance of Operational Technology in the Smart Energy) and CISSAN (Collective Intelligence Supported by Security Aware Nodes) projects, co-funded by Business Finland and University of Jyväskylä.

REFERENCES

AlienVault (2016). “AlienVault Unified Security Management Solution – Support reference guide, Version 5.1”, 2016.

Briggs, B. (2019). “Hackers hit Norsk Hydro with ransomware. The company responded with transparency”, Microsoft News.

Canadian Centre for Cyber Security (2021). “The cyber threat to operational technology”, Cyber threat bulletin.

Churchill, J. (2017). “When the screens went black”, Maersk Post Sept-Oct, 2017.

Danish Centre for Cyber Security (2021). “SolarWinds: State-sponsored global software supply chain attack”, Investigation report, Nov. 2021.

ENISA (2023) “Building effective governance frameworks for the implementation of national cybersecurity strategies”, European Union Agency for Cybersecurity, Feb. 2023.

MISP (2025) “MISP Threat Sharing”, Website: https://misp-project.org/.

MITRE (2024) “ATT&CK for Industrial Control Systems”, MITRE Corporation.

Mairesse Siluk, J. C., Sauer Oliveira, H. L., Donaduzzi Rigo, P., da Silva Sidrim, A. S., Schaefer, J. L. (2023) “Collaborative drivers’ networks for the development of Smart Energy environments”, Sustainable Energy Technologies and Assessments, Vol. 65, May 2024.

Ribeiro, A. (2025) “Dragos finds ransomware attacks on industrial sector surge 87%, manufacturing hit hardest as OT targeting rises”, Industrial Cyber, Feb. 25, 2025.

Simola, J., Savola, R., Frantti, T., Takala, A., Lehkonen, R. (2023) “Developing cybersecurity in an industrial environment by using a testbed environment”, Proc. of the 22nd European Conference on Cyber Warfare and Security, pp. 429–438.

Simola, J., Takala, A., Lehkonen, R., Frantti, T., Savola, R. (2024) “Validation of sensor data integrity in OT environments through multisource data sensors”, Proc. of the 23rd European Conference on Cyber Warfare and Security, pp. 487–495.