Implications of OT and IT Integration for Cyber Security

HSD

securitydelta.nl

Implications of OT and IT Integration for Cyber Security

HSD
securitydelta.nl

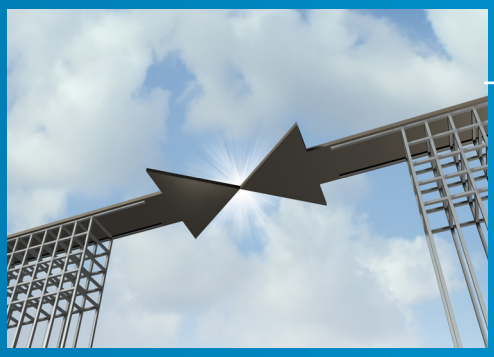


Table of Contents

Management Summary

In this report, first, awareness is raised about OT security. Second, challenges of OT-IT Integration are identified and third, opportunities for collaboration and innovation in the OT-IT domain are presented. Awareness, challenges and opportunities are not solitary in nature. It is therefore important to advance an holistic approach concerning agendasetting, best-practices and an advisory knowledge center.

OT is prevalent in the critical infrastructure and the industrial sector. With the raise of technologies such as Big Data, Data Analytics and the Internet of Things, more and more organisations have increasing business needs to integrate OT with IT networks. Numerous challenges on the general as well as the technical level threaten secure operations due to increasing cyber risk. Responsibilities are unclear, awareness is still lacking, and communication is suboptimal. All this makes that OT is left with cyber security difficulties.

The OT working field agrees on what the ideal situation should be: learning from each other by (voluntary) exchanging incidents and approaches. This could take the shape of operational and strategic information exchange within a network of organisations (Community of Practice). The potential of this information exchange finds itself in the merging of established knowledge, knowledge circulation and innovative ideas and products, leading to even more secure and safe OT environments.

Join forces and form consortia is the advised doctrine to establish this ideal situation of knowledge sharing and knowledge circulation. This is demonstrated in Smart Industry initiatives such as joint research programs with universities and businesses, an automated security operations lab and a cyber security resilience initiative that provides a safe place to share cyber security knowledge and lessons learned.

Besides exchanging knowledge and experiences, it's imperative that concrete steps are taken to improve the digital resilience of OT in companies. Segmentation of the OT network, a clear insight in legislation and security standards are of great importance.


y
x

1 – Introduction

There is a wide range of reliance on operational technology (OT) systems ranging from purely manual to highly automated processes. OT is hardware and software that monitors or controls industrial equipment, assets, processes and events. This OT reliance threatens secure operations due to increasing cyber risk.
The objective of this report is threefold:

- Raise awareness regarding OT security;
- Identify challenges of OT-IT integration;
- Present opportunities for collaboration and innovation in the OT-IT domain.

OT is prevalent in two broad-scaled sectors, (critical) infrastructure[1] and the industrial sector. OT for both sectors includes waste management, water treatment and monitoring of public works such as roads, tunnels, bridges, waterways, rail and aviation. It also entails medical equipment in the healthcare sector, electronic locks in prisons and robotics in horticulture. From distillation units, dams, logistic centers, prisons, hospitals, factories, to airports and railway stations, the push for digitalisation is driving the need for greater cyber protection across the (critical) infrastructure and industrial sector value chain.

The vulnerability of OT systems to cyber exploitation can vary dramatically from asset to asset, depending on (1) how the asset's OT and information technology (IT) networks are architected; (2) the extent to which they are integrated; and (3) the hardware, software, firmware and protocols used within the networks. There are numerous real-world examples of how OT systems were exploited.

Safety systems disrupted through a ‘zero day’

In August 2017, the Saudi Arabië firm Petro Rabigh experienced a cyberattack on its Safety systems. Two emergency shutdown systems were brought offline in a last-gasp effort to prevent a gas release and deadly explosion. But as the safety devices took extraordinary steps, control room engineers working the weekend shift spotted nothing out of the ordinary, either on their computer screens or out on the plant floor. A poorly configured firewall gave remote attackers a foothold inside corporate computers, where they were able to pivot to operational technology, the OT networks that housed Schneider Electric's safety systems. At least six Triconex controllers had been compromised by the malware, which was built to replace operating code and co-opt the safety equipment during an emergency. The hackers were taking advantage of a previously unknown vulnerability or "zero day" in the device. The incident was caused by the very sophisticated Triton malware, most likely developed by a Nation State actor. The shutdown at Petro Rabigh in august 2017 stands as the most recent known example of a cyber disruption to a major industrial safety and control system.

Nuclear enrichment facility brought to halt

In 2010 the Stuxnet malware was used for a succesful attack on Iran’s nuclear enrichment facility at Natanz. With Stuxnet it was possible to bring the nuclear plant to a halt. The Stuxnet worm was engineered to damage motors commonly used in uranium-enrichment centrifuges by destabalising them through continuously varying the spinning frequency. The result was that more than 1000 centrifuges were temporarily disabled.

Hundreds of thousands of people endured an hour long power outage

In December 2015, Ukraine experienced a large cyberattack on its electricity grid. Hackers managed to infiltrate three energy companies and shut down power generation temporarily in three regions of Ukraine. Attackers made use of the BlackEnergy 3 malware to shut down the three substations. The malware was hidden in fake Microsoft Office attachments, spread and delivered in spear phishing emails. The attack led to widespread power outages and it left nearly a quarter of a million people without electricity for up to six hours in the middle of winter.

This distinction between critical infrastructure and the non-critical industrial sector is important; they have different laws to adhere to. In section 3.4, is explained, that laws are in place for organisations in the critical context, such as the Wet Beveiliging Netwerk- en Informatiesystemen (Wbni), but not for parts of the industrial sector that are not defined as critical infrastructure. In addition, organisations providing critical processes are guarded by strict supervisors, this is less the case for the industrial sector. Summarizing, the first type of organisations can find support on a national level, non-vital companies reside in a more unregulated opacity.

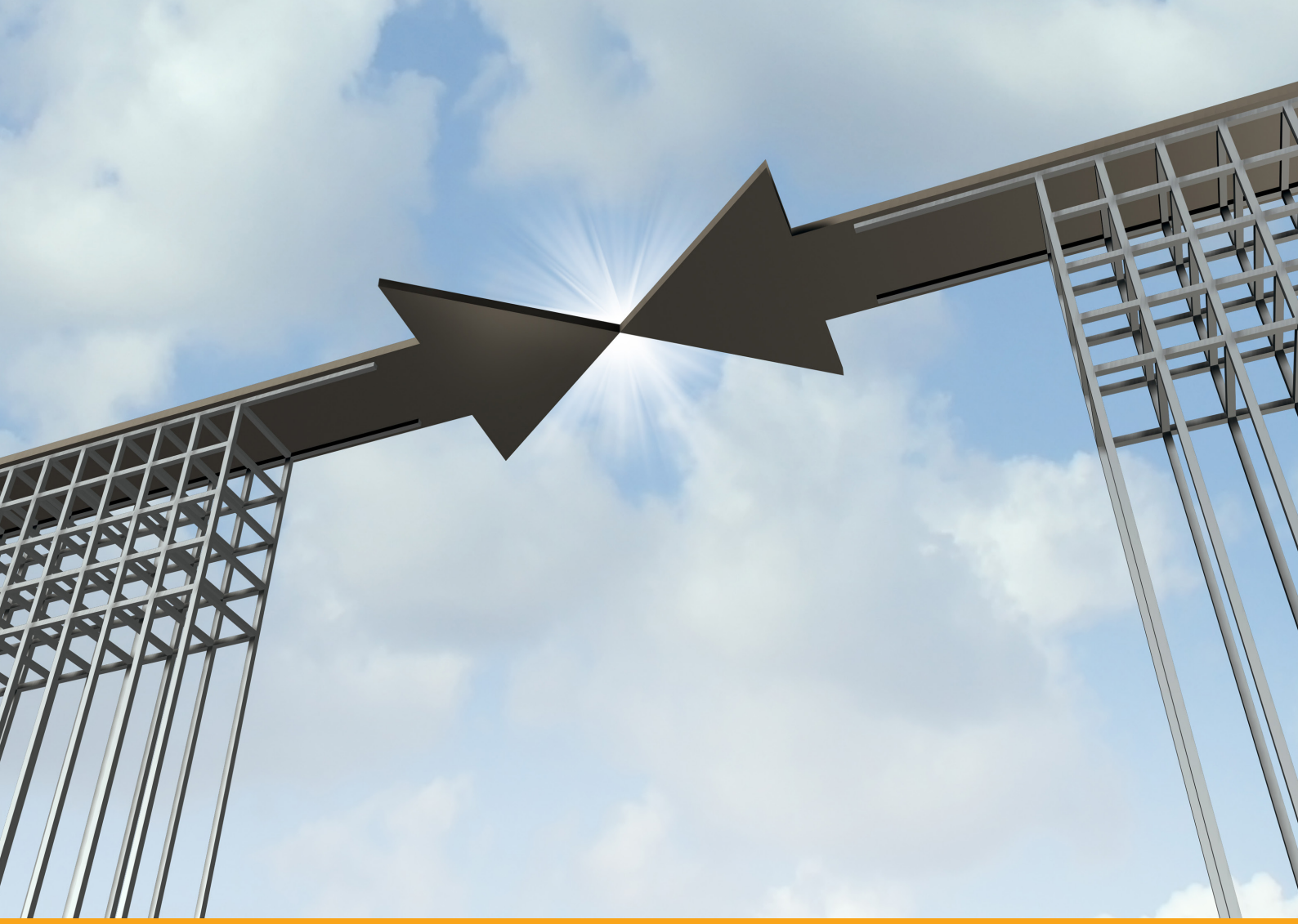
Though, by incorporating robust cyber security in Health, Safety & Environment (HSE) measures, the potential of a successful attack and its potential impact can be minimized. As part of the ongoing HSE process, a regular independent review of an OT-domain in the industrial sector, against the IEC 62443 standard combined with the current threat landscape, is recommended to become part of industrial asset management operations. This ensures cyber security policy and measures taken to mitigate the risk are up-to-date to handle current threats.

To summarise, the relevance of the OT/IT security topic is fourfold:

- Operational technology (OT) domain culturally has been more safety-aware than security-aware compared with IT, challenging effective security governance and policy in integrated IT/OT environments.
- From a security perspective, OT networks have been unmanaged for many years. They are a mix of OT protocols, unidentified assets, legacy systems and devices with unsecure communications.
- Applying a “one-size-fits-all” security controls methodology across IT and OT, as well as not fully accounting for differing security requirements, lead to decreased security efficacy from a cyber security perspective.
- Information sharing and knowledge centers about security governance and policy in integrated IT/OT environments in critical infrastructure and the industrial sector can help to boost awareness and implement best-practices.

Chapter 2 introduces the convergence of OT and IT Security by describing stakeholders and its opposite system priorities, confidentiality, integrity and availability (CIA, AIC). Chapter 3 looks specifically at Cybersecurity and OT and IT integration. Cyber security challenges in OT are addressed and general and technical challenges are partly matched with cyber security solutions.

Overall, the report uses recent literature on the subject in light of contextual examples, together with input from stakeholders, and presents conclusions and recommendations for stakeholders seeking to understand how to navigate emerging OT and IT integration and mitigating cyber security risk. Furthermore, it provides stakeholders with opportunities to fill in knowledge gaps by providing information and best practice to help advance the journey to operational excellence and fine-tune solutions to support safer, more reliable assets and operations.



2 – Convergence of OT and IT Security

2.1. Introduction

This chapter introduces the convergence of OT and IT security by describing stakeholders and its opposite system priorities. Although IT (information technology) and OT have commonalities, they are not the same. As the name illustrates, IT is about information. It comprises technologies[2] for information processing, often a combination of software, hardware, and communication technologies. Illustrative IT components are end-devices, networks, databases, applications, and systems. An IT environment could easily contain thousands of hosts, and hundreds of applications. The focus of OT is not information, but physical manufacturing processes. OT environments often contain a limited number of hosts. These differences result in different cyber security risks for IT and OT, which requires a distinct approach. Table 1 briefly depicts the cyber security differences regarding OT and IT. Chapter 3 dives deeper into differences related to OT and IT integration.

OT started as an isolated technology domain with separate standards, protocols, and governance models. In the early stages OT systems were so called 'monolithic', which means they were independent, standalone. Networking, let alone the internet, did not exist and real interconnection of systems was not possible. If there was a connection, it was via a Wide Area Network (WAN) between the master system and each of the Remote Terminal Units (RTU). A second generation OT was "distributed": the development of local area networks (LAN) enabled the connection of multiple stations, including real-time communication and data exchange. Still, the communication remained within the local network. The third "networked" generation allowed geographically dispersed systems to be interconnected which each other. Starting from the early 2000s, OT has entered the current "web-based" architecture. These industrial systems that were once inaccessible for the outside world, are now sometimes even reachable via the internet – for example via laptops, tablets, and smartphones.

	OT	IT
Anti-virus	Often difficult or impossible to use in (legacy) systems	Is used everywhere
Vulnerability scanning	Passive scan as an advice, an active scan could disrupt the operational production	Active scan
Network an asset scanning	Passive scan	Active scan
Patching	Slowly, or not possible (anymore), and requires supplier approval	Frequently, even daily
Reliability	Failure is unacceptable	Incidental failure is accepted
Availability	24 / 7 / 365	Planned downtime is OK
Security testing	Only after very careful considerations and after identifying risks	Is widely used
Performance	Large delay is a serious problem	Large delay and instability are acceptable
Security	Information system network is isolated from plant network	Little separation between networks at the same location
Security and awareness	Bad	Reasonable to good

Table 1 **OT versus IT security**

The interconnectivity mainly shows through the OT systems being connected to the office network. The legacy systems tied to the IT network brings technical challenges and risks, especially when looking at cyber security.

The interconnectivity mainly shows through the OT systems being connected to the office network. The legacy systems tied to the IT network brings technical challenges and risks, especially when looking at cyber security.

2.2. Stakeholders

OT-IT security encompasses and affects different types of parties. To identify those stakeholders, the OT-IT chain including stakeholder interdependencies should be considered. The chain starts at the supplier of industrial components and materials, and ends at the customer. The process is orbited by boundary conditions, such as standards and laws. Therefore, certification organisations, and supervisors are considered stakeholders as well.

Suppliers, or vendors, provide for the components and materials that build up an OT environment. Think of hardware manufacturers of SCADA systems, PLC or DCS controllers, sensors, motors, cables, pipes, and other industrial machine elements. But also software vendors can be OT suppliers: examples are providers of machine control systems, software for monitoring and analysing production data.

System integrators bring different subcomponents or subsystems together into a complete system, based on the needs of the customer. Sometimes these subcomponents could come from one and the same supplier, but it is feasible that components from different vendors are put together by the system integrator. In order to reach an operational system, system integrators have to combat compatibility challenges regarding hardware, software, and interfaces of different products.

Customers (end-users) are organisations that use OT in their production environments. Often, these organisations 'make' something, be it a product or a service. An oil and gas company is a customer in the OT supply chain, so is a manufacturer of microchips, and so is a vegetable grower. Customers work together with system integrators to build up their infrastructure. Within these customer organisations, both **IT employees** and **operational employees** are involved in OT-IT integration.

IT employees receive management information from the OT environment, while operational employees are working on the plants. This described stakeholder interdependency is in contemporary times preferred, however not the status quo.

Further described in section 3.4., organisations in OT have to abide by several laws and regulations. In addition, there are some standards that provide organisations with best-practices and guidelines. **Inspectors** or **supervisors** are parties that assess whether organisations comply to the laws and regulations that are applicable and mandatory for them. Next to laws and regulations, the technology domain has various standards to which companies can certify themselves, such as the IEC 62443. **Standardisation**

organisations are the parties that establish these standards. Those organisations usually work together with organisations that develop and provide training in using these standards.

2.3. CIA and AIC Security Triads

In IT security the focus is on the CIA security triad:

1 **C**onfidentiality
2 **I**ntegrity
3 **A**vailability

These are the three pillars of security. Because IT is all about information, the **confidentiality** of the information is usually considered the most important security goal. The nature of OT on the other hand, requires the triangle to be inverted to the AIC security triad:

1 **A**vailability
2 **I**ntegrity
3 **C**onfidentiality

This inversion can be explained by the function of OT systems, and is best illustrated by an example. Think of an energy company, that supplies electricity to an entire city. After this electricity is generated at a power plant, it is distributed throughout the city via a branched network of underground electricity pipes. Now imagine an attacker that places a data tap at the point where the main pipe splits into different branches, representing different city areas. The data that could be retrieved this way, for example what amount of electricity goes to what area of the city, is probably not that classified. Now imagine the same attacker, at the same place in the pipe network, performing a different attack: drilling a hole right through the electricity pipe, damaging it such that all electricity flows away into the earth. The electricity now will not be delivered to the city areas, rendering them secluded from the power network. Availability is in the OT context intertwined with safety. When industrial systems are not available, safety of personnel and environment is in jeopardy. As can be seen, loss of **availability** here has more severe consequences than loss of confidentiality; and this is typically the case for OT environments.

2.4. Conclusion

Historically, OT systems were physically or virtually isolated from information technology (IT) networks, except the days of OT isolation are almost over. With the raise of technologies such as Big Data, Data Analytics and the Internet of Things, organisations have increasing business needs to integrate OT with IT networks via connections to the internet. This interconnectivity is mostly used for the exchange of data for the purpose of management information and to provide access for suppliers and maintenance personnel. This development introduces the IT personnel as stakeholders in the OT field. Due to the interconnectivity between IT and OT both environments are more conducive to cyber-attacks.

3 – Cyber Security and OT & IT Integration

3.1. Introduction

This chapter discusses topics regarding cyber security in relation with OT-IT integration. First, 3.2. depicts cyber security challenges in OT. These challenges are found in literature, and were mentioned various times during interviews with respondents. General challenges are found in the definition of an OT person, in addressing responsibilities, awareness, and communication of cyber incidents. Technical challenges are found on the topics of asset validation, patching, testing OT environments, root cause analysis, detection of attacks, and monitoring. Use of standards, laws, and regulations can help organisations decrease OT challenges. So second, laws, standards and regulations are discussed. 3.3. gives an introduction in the concept of HSE, towards the IEC 62443 standard, the *Wbni* law and the perceptions of organisations in the current practice.

3.2. Cyber Security Challenges in OT

3.2.1. General Challenges

What is an OT Security Person?

Multiple respondents argue that there is no clear concept of an 'OT security person'. Whereas there is a general consensus on IT roles and functions with their according tasks and responsibilities, these functions are lacking for OT. This hiatus shows for example through the scarcity of OT security job vacancies. Also, the OT counterpart of IT security study programmes is not established. Young professionals in OT (graduates in mechanical, industrial and electrical engineering) usually have a solid basic knowledge, but universities and schools embed little attention to security in their programmes.

Responsibilities

Coherent with the lack of 'OT people' is the unclarity regarding OT security responsibilities. Who is, or should be, in charge of OT security? Is it someone in the operational part of the organisation? Or an IT or HSE officer? Maybe OT is a shared responsibility, that can not be attributed to one person. Multiple interviewees described that OT security often comes down to the IT manager as a side task; but the IT manager also does not have the appropriate knowledge. This may result in a wrong approach to OT security

Awareness

Although awareness on the topic of OT security regarding HSE is rising[3], society is not there yet. Even though some stakeholders indicate higher awareness levels than others, from the interviews follows that the general awareness at boardroom level is not sufficient yet. Boardroom members usually do not have a technical background: explaining to them why OT security is important, is therefore a challenge. In the most optimal scenario, the executives have an IT background, or they have IT in their portfolio (like the chief financial officer). However, as explained in chapter 2, a background in IT does not implicitly make you an OT professional, due to 'cultural' differences between the two fields.

At the same time, organisations indicate that they are willing to learn. Internally, stakeholders see that employees at all levels are increasingly open to OT security training and awareness sessions. Also, the respondents elaborated on concrete ideas to raise OT security awaress in a practical way. Externally, various organisations see sharing of lessons learnt as a useful way of learning among organisations. In addition, external stimuli such as insurances contribute to the rising feeling of urgency. Organisations were always able to obtain insurances for 'traditional' safety incidents within their companies. An insurance covering cyber incidents could be less trivial, or at least very expensive. The same holds for cyber incidents: often things must go wrong to wake up the world.

Communicating Cyber Incidents

The general tendency in companies is to not communicate about cyber attacks that they have endured. However, respondents unanimously mention that it would be better if everyone was open about cyber attacks. Then why are cyber attacks being kept secret? One first mere cause is that companies sometimes do not even know that they are hacked. And if they do know, a feeling of embarassment often prevails: a feeling of not having protected the organisation well enough. In line with this sense of shame, organisations fear reputational damage, possibly resulting in their customers switching to a competitor. The fear of reputational damage could also explain why some communicate cyber incidents internally and with the management team, but not externally.

As one of the respondents stated: 'media attention in OT is often negative attention'. The persistent silence about cyber attacks counteracts the learning process. Severe cyber incidents must be connected with business continuity management and crisis management.

Other issues

Other issues mentioned by the respondents are the ageing of people working in OT, liability challenges and cyber security insurances. Furthermore, separation between IT and OT environments is recommended, nevertheless this is merely a transitional solution. This to mature OT security first, until integration between the two domains is possible. For example, when legacy systems are disposed and new equipment and OT systems are procured.

3.2.2. Technical challenges

Asset Management and Validation

Asset Management and Validation means that you check what assets you have and if they are secure. OT assets often contain operating software that should be checked for cyber security. According to a respondent, in OT environments, asset validation is lacking – at least on the Dutch market. The problem here is that the source code of OT assets is often not provided by the supplier. As a result, companies possibly use these assets without being able to test these components for security.

Vulnerability Management

Various international standards for security management systems mandate or recommend vulnerability management or assessment. The scope here is to map publicly known vulnerabilities to assets in an OT system (or a fleet of systems) and, based on risk assessment, identify and execute an appropriate response. Vulnerability Management depends on creating an inventory of OT assets (so it's directly linked to asset management) and gathering the sources of vulnerability information and remediation plans that can be instantiated to address identified vulnerabilities. Vulnerability Management activities include:

- Creating and maintaining an inventory of relevant OT assets;
- Identifying sources for vulnerability information and regularly obtaining updated disclosures;
- Mapping known vulnerabilities to assets – identifying which vulnerabilities affect products in an OT asset inventory;
- Analyzing the risk associated with vulnerabilities and identifying and executing mitigations to address them.

Patching

Patching, the installation of software updates, is a challenge in OT environments. A patch can result in unforeseen incompatibility with connected systems, thereby disturbing the production process. This is even more of a challenge because organisations cannot simply put their systems on hold for a couple of hours. To illustrate this, respondents mentioned patching frequencies of once per quarter to once a year. To prevent compatibility issues, organisations usually wait for vendor approval for a patch. Dependent on the vendor, it can take some time before a patch can be installed, possibly leaving the system vulnerable in the meantime. Closely linked to the problem with patching is the challenge of testing OT environments.

Hardening

Security hardening is the process of resolving risks and vulnerabilities on OT assets and networks to ensure secure and reliable cyber-physical operations. Key elements of OT security hardening, include:

- Patching of software and firmware
- Secure configuration, use security functionality available in assets (security level)
- User and account access limitation
- Ensuring network connectivity security
- Limit network communication protocols and communication paths
- Removal of unnecessary software
- Removal or disablement of unnecessary hardware components
- Ensuring proper back-ups

Testing OT Environments

Testing within OT environments is not as trivial as testing within IT environments, argue multiple organisations. Test environments are used to test functionality and compatibility of patches or other new pieces of software. Testing on the production environment can cause undesired, or severe, disruptions in the production process. Because, whereas the simulation of IT environments can be done relatively easily and cost effective by cloning the IT environment on a separate network or to the cloud, you cannot 'copy-paste' an OT environment with its the physical components. Regarding the latter, the development of OT simulation software is evolving; this software enables so-called digital twins.

Lack of Root Cause Analysis

A lack of, or unjust, root cause analysis was mentioned as a problem in OT environments. When a defect or

an unplanned disruption in the system happens, it is sometimes classified as a maintenance issue such as 'component is defect – must be replaced', while the actual cause could be a hack. In this case, there is a wrongly diagnosed root cause and a solution that will not solve the problem.

Difficulty in the Detection of Attacks

OT systems are usually protected by safety systems, that detect whether the operations of the system are still showing common behaviour. Through manipulating safety systems first, hackers can attack the operational system without the organisation being able to detect this at first hand. While the hackers can go on disrupting the operations, the safety system keeps communicating normal values, like happened in the 2010 Stuxnet attack.

In addition to the challenges that exist for detecting attacks, there are several overall challenges for OT monitoring. One stakeholder explained that monitoring can have an impact on the system operation, which can harm the safety of the system. Another stakeholder explained that monitoring is often outsourced to external organisations, as the organisations with the OT environments usually don't have the required expertise or an own security operations center (SOC). Furthermore, due to the differences in IT and OT network traffic, OT asks for other technical monitoring approaches than IT.

3.3. Standards and Regulations

3.3.1. Health, Safety and Environment and OT Cyber Security

HSE stands for Health, Safety, and Environment. HSE is a discipline that looks into the environmental protection and safety at work. Processes in critical infrastructure and the industrial sector, may have severe impacts on safety, health, and environment. Therefore, adhering to HSE best-practices is important in order to protect employees and others. In the past decade, cyber security has shown itself more and more intertwined in issues in HSE. For example, in 2010 the Stuxnet attacked impacted Iran's national nuclear plant, and in 2017 the Saudi Arabia firm Petro Rabigh experienced a cyber-attack on its safety systems. In both attacks, safety systems were manipulated and bypassed by hackers.

Standards, laws, and regulations can provide organisations guidance in implementing cyber security measures and thereby improving operations towards HSE. For OT environments, the IEC 624432 standard and the *Wbni* are currently applicable. Below, a short introduction on both documents is given.

3.3.2. IEC 62443 standard

The IEC 62443 “Cyber Security for Industrial Automation and Control Systems” (IACS) is a series of standards providing a flexible framework towards managing cyber security for OT systems in a structured way.[4] Adhering to the IEC 62443 standard can help organisations in reducing the risk of a major (cyber) incident by the application of organizational and technical measures to protect the process control and safety systems. Business and IT cyber security solutions can be used here as part of a holistic approach that incorporates people, processes, procedures and technology. This holistic approach is included in the IEC 62443.

As indicated by the interviewed companies, IEC 62443 is regularly used as a requirement in the selection of suppliers. Individuals can follow training on the IEC 62443, which provides them with knowledge and skills to help manage cyber security within their organisation.[5] Implementing measures from the standard helps organisations in complying to national and European law, as described in 3.4.3.

The framework contains recommendations divided over four main blocks: General, Policies and Procedures, System, and Component. The table below contains an overview of these four main blocks and the subtopics they address.

General	**62443-1-1** Concepts and models	**62443-1-2** Master glossary of terms and abbreviations	**62443-1-3** System security conformance metrics	**62443-1-4** IACS security life-cycle and use-cases	
Policies & procedures	**62443-2-1** Security program requirements for IACS asset owners	**62443-2-2** Security protection rating	**62443-2-3** Patch management in the IACS environment	**62443-2-4** Requirements for IACS service providers	**62443-2-5** Implementation guidance for IACS asset owners
System	**62443-3-1** Security technologies for IACS	**62443-3-2** Security risk assessment and system design	**62443-3-3** System security requirements and security levels		
Component	**62443-4-1** Secure product development lifecycle requirements	**62443-4-2** Technical security requirements for IACS components			

3.3.3. Dutch Law: "Wet beveiliging netwerk- en informatiesystemen (Wbni)"

As described above, adhering to an OT standard can help organisations towards compliance to law. The *Wet beveiliging netwerk- en informatiesystemen (Wbni)* is the Dutch implementation of the European Union guideline on network and information security.[6]

Organisations to which the law applies, have a twofold duty:

1 The duty to report *(meldplicht)* means that they must report incidents immediately to the Dutch Telecom Agency and the respective Computer Emergency Response Team (CERT).
2 The duty of care *(zorgplicht)* means that an organisation must take appropriate organisational and technical measures to manage the security risks if their ICT systems and to reduce the impact of incidents.

The *Wbni* is applicable for the following types of organisations: providers of critical infrastructure, digital service providers and the *Rijksoverheid.*[7] *This implies that the Wbni* is enforced on OT organisations in critical infrastructure, but **not** on (non critical) OT organisations in the industrial sector. This dichotomy in OT can lead to differences in a sense of security urgency, or to unclarity in cases when it is not clear whether an organisation classifies as critical or not.

3.3.4. Laws, standards and regulations in Practice

Multiple respondents mentioned the scope of the *Wbni* as an issue for OT. The duty to report and the duty of care are seen as major incentives for organisations to take (cyber) security measures within their organisations. Though, as the law is merely applicable to critical infrastructure providers, the industrial part of OT does not have to comply to this law. As a result, it is difficult to reach security harmonisation in the OT field.
Furthermore, the respondents were asked about the use of standards, and whether they possess certifications. The answers varied, all supported by different argumentations. Not all organisations have a certification themselves. Or, some organisational parts have a certification, while others do not. For the latter case, it was indicated that the need for a certification depends on the focus of the organisational part. When the focus is external, certifications are more important than when the focus is internal. For internal projects, certification tends to be less crucial. This perspective is in line with others indicating that a certification is often set as a requirement when selecting suppliers.

3.4. Conclusion

This chapter discussed general and technical challenges in OT security. It explained how the implementation of the IEC 62443 standard can help reducing these challenges, and at the same time can help in being compliant to the OT law *Wbni*. Organisations use the standard to assess their suppliers, and to be more cyber secure themselves, for example by training employees and taking the measures instigated by the standard. Whereas the standard is applicable to all types of OT organisations, the scope of the *Wbni* is limited to critical infrastructure organisations.

4 – Conclusions and Recommendations

4.1. Introduction

Based on the analysis and conclusions in this paper, three main objectives are envisioned:

1 Incorporate Cyber Security Awareness in OT by Agenda-Setting
2 Magnify OT Cyber Security Knowledge by expanding Cyber Resilience initiatives
3 Create an OT Best-Practice Portfolio

These three objectives are outlined below.

4.2. Agenda-Setting to Incorporate Cyber Security Awareness

Employ agenda-setting to incorporate cyber security awareness in OT and address OT-IT convergence themes by:

1 This underlying report about 'Implications of OT and IT Integration for Cyber Security'
2 Knowledge sharing and circulation by organising knowledge sessions on OT-IT use cases and general applications in a wider perspective
3 COSO[8] and CISO Intervision Meetings to:
   a Combine OT and IT expertise to tackle for example OT cyber monitoring adequacy
   b Engage in conversation about (critical) assets a vulnerable system components
   c Build a best-practice portfolio

Writing articles about topics emerging from the CISO and COSO intervision meetings. These articles aim to improve OT cyber security with a holistic approach incorporating people at all levels, processes, procedures and technology. The articles are circulated among the HSD community: companies, knowledge institutions and government, with the aim to fill in knowledge gaps, blind-spots and creating a reciprocal understanding of OT and IT interaction due to cross-pollination.

4.3. Magnify OT-IT Cyber Knowledge by expanding Cyber Resilience initiatives

Driven by the objective of broadening and deepening collaboration between different parties, a visible and operational knowledge center should be established based on experiences of the Cyber Resilience Center Brainport. HSD could support setting up such a knowledge center, Cyber Resilience Initiative (CRI) that focuses on Smart Industry (paragraph 4.4.8.)

An OT best-practice portfolio is showcased in this Cyber Resilience Initiative and will be enabled with and via partners in an open ecosystem. This OT best-practice portfolio, provided by input from different organisations, consists of knowledge about OT-IT cybersecurity and its derived products and services, that accumulates and enhances over time. The potential of the CRC finds itself in the merging of established knowledge, knowledge circulation and innovative ideas and products, leading to even more secure and safe OT environments. In the next paragraph some possible future best-practices for the portfolio are mentioned.

4.4. Create an OT Best-Practice Portfolio

This paragraph describes examples of potential activities that generate best-practices and together form a best-practice portfolio that can be showcased at the Cyber Resilience Initiative.

4.4.1. Human Capital and Lifelong Learning

Access to talent is a crucial prerequisite for the creation of innovative OT security solutions and the growth of the OT security sector. Dedicated OT security study programmes are not established. As working professionals in the OT field are perceived to have a solid basic knowledge, Lifelong Learning programmes can be set up especially for OT security skills to fill this specific cyber security knowledge gap. The knowledge gaps that are identified by the COSO-CISO Intervision Meetings from paragraph 4.2 can serve as input to help shape these Lifelong Learning programmes and serve as input for the best-practice portfolio.

4.4.2. Table Top Exercises

Security is a shared responsibility between users, administrators, and technical professionals.[9] Table-top exercises will help cybersecurity teams develop tactical strategies for securing their systems. They are meant to help organizations consider different risk scenarios and prepare for potential cyber threats. Each scenario will list:

– tested processes,
– identified threat actors,
– impacted critical infrastructure and industrial assets.

The Cyber Resilience initiative can provide for the perfect environment for these table top exercises. Discussion

questions and use-cases that are the input for the table top exercises are derived from the earlier mentioned COSO and CISO intervision meetings.

Meaningful learning points derived from the exercises are bundled and serve as input for the best-practice portfolio that is designated to be showcased in the Cyber Resilience initiative.

4.4.3. Innovative OT Testing Solutions

As mentioned in 3.2.2., testing within OT environments is not as trivial as testing within IT environments. We should look towards sound testing possibilities for OT, for example by developing a digital twin of the OT environment in which patches and new software components can be tested in a safe and secure way. One working initiative in technical simulation is already on the market, making use of gaming techniques to simulate environments in 3D.[10] Accessibility to these techniques for the widespread range of organisations using OT can help in decreasing deployment time and minimizing risks.

4.4.4. Join Forces and Form Consortia

While we see that the practice is different, the OT working field agrees on what the ideal situation should be: a (voluntary) exchange of incidents and approaches, and learning from each other. This could take the shape of operational and strategic information exchange within a network of organisations. Strategic and operational collaboration can occur at Information Sharing and Analysis Centres (ISACs) as initiated by the NCSC.[11] In an ISAC, organisations exchange sensitive and confidential information about incidents, vulnerabilities, threat (intelligence), and countermeasures. Another way to join forces is chain collaboration, such as the Smart Industry Initiatives as described in 4.4.8. Openness and honesty leads to lessons learnt, which companies can use to improve their OT security.

HSD, as a neutral, connected organisation, could help provide insights in ongoing initiatives. In addition, it provides a fertile ground to jump-start initiatives that have the aim to improve OT security and aim to conduct a more holistic approach for OT security. Example can be taken from the Cyber Resilience Center Brainport; ways to cooperate should be explored.

Lessons learnt about consortia-building and its outcomes can serve as best practices and become part of the best-practice portfolio that can be showcased at the Cyber Resilience Initiative.

4.4.5. Establish an OT Governance Body

To bring together the dispersed knowledge and responsibilities regarding OT, it is advised to establish one single OT governance body that has oversight over OT security and its integration with IT security.[12] In order to reach an optimally aligned scenario, in this body OT and IT expertise's should be combined. This means that employees from both the OT and IT domains must be represented in this group. OT people will then bring their knowledge about the critical assets of the operational (or safety) systems. Possible tasks for this OT body include, but are not limited to: providing an overview of the OT-IT security environment, attributing responsibilities, and developing a policy for integrated OT-IT security.

COSO-CISO intervision meetings organized by HSD as part of the Cyber Resilience initiative activities, serve as a recruiting ground for representation in OT-IT expert groups that provide input for the establishment of an OT governance body. The role of the Security Delta is facilitating the OT companies/OT branche organisations in developing such an OT governance body.

4.4.6. One-Way Information Flows using Data Diode Technology

The convergence of OT and IT inhabits network communication between the office IT environment and the operational environment. Operations data generated in the operational environment is sent to the office IT environment. This data, transmitted by OT systems, helps the control center to monitor the operations. However, sending back data across the same connection might affect the operations: intentionally by an attacker, or unintentionally by an employee. Therefore, one-way communication paths in OT-IT integrated environments can help reducing risks. A data-diode is a technology that enables one-way communications.

A data diode[13] is a hardware-based electronic device designed with two separate circuits, that physically constrain the transfer of data to one direction only. In other words, a data diode enforces communication to be transmit-only, or receive-only. For OT-to-IT data streams, transmit-only would be an appropriate solution. A challenge in the deployment of data diodes is the fact that many network protocols require a two-way connection by their fundamental nature. Use of software components and/or proxies can help solve these challenges. Taken as a whole, data diode technology is something COSOs and CISOs should consider to help reduce cyber risks.

4.4.7. Compliance Monitoring

Where OT environments have to be compliant to law and legislation, it's important for organisations to have an insight in their compliance levels. Organisations may use standards like the IEC 62443 to ensure compliancy to the legislation. Often, organisations find it cumbersome to manually keep track on how they perform against the requirements of the standards and take timely action to mitigate non compliance.

Special OT Monitoring solutions[14] is can keep track of not only anomalies in the expected behavior of an OT network, but also provide clear insight in the actual compliance levels towards the used standards. Not only can organisations at any given time see whether they are working in compliance with the standard, they also gain insight in any non compliances, as soon as they occur. This helps organisations to stay compliant to both standards and law and legislation.

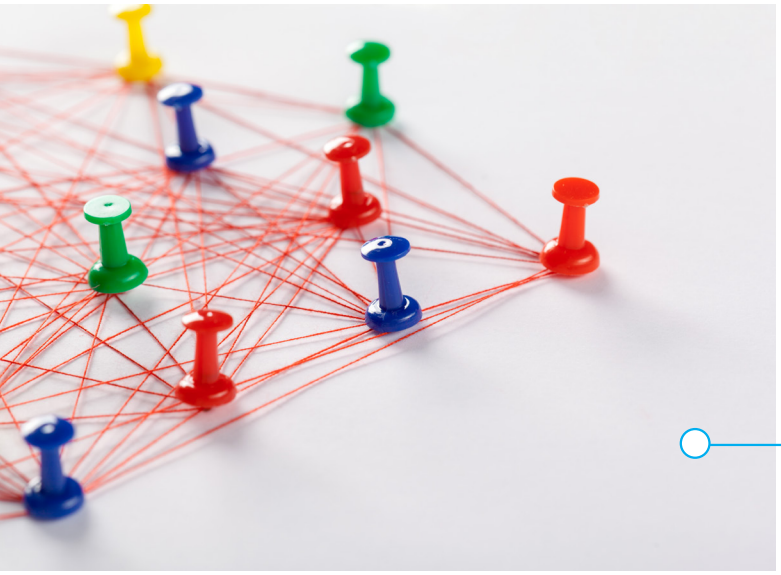
4.4.8. Connect to Smart Industry Initiatives

The world is in anticipation of a fourth industrial revolution. This revolution is driven by giant leaps in ICT innovation and promises to radically alter the face of industry in the coming decades. Automated production systems using advanced robotics increasingly communicate with each other on detailed aspects of production, joining up previously fragmented manufacturing processes. By linking all steps in the value chain, a world of possibilities opens for companies, old and new. This digital transition will lead to a significant transformation regarding industrial internet solutions. It is recommended that COSOs and CISOs connect to Smart Industry Initiatives (Industry 4.0).

4.4.9. Establish a COSO Community of Practice

The last recommendation is to establish a COSO Community of Practice (CoP). This is a group of COSOs that share a concern or a passion for something they do, and learn how to do it better as they interact regularly. This definition reflects the fundamentally social nature of human learning. Communities of Practice can be organized at a central location, for example at HSD, and can take form in fieldtrips to organisations of interest. It is in line with the proposed CISO-COSO intervision meetings, however a Community of Practice has a broader scope. Examples of activities:

- Reverse Monitoring, where the older generation learns from the young or vice versa;
- Sharing Best-Practices;
- After Action Review, where CoP members review each others projects.



Annex

Annex 1

List of respondents

- ASML
- Autoriteit Nucleaire Veiligheid en Stralingsbescherming
- Batenburg N.V.
- Hudson Cybertec
- One DYAS
- VolkerWessels

Furthermore, during a round table session hosted by HSD, input was gathered from the following organisations:

- Vialis (a VolkerWessels organization)
- Deloitte
- Thales Group
- P-X Systems
- Hoogheemraadschap Rijnland
- NIXU
- TNO

Reference List

1 https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen
2 https://www.gartner.com/it-glossary/it-information-technology
3 https://www.tno.nl/nl/over-tno/nieuws/2019/11/operationele-technologie-security-rapport/
4 https://www.isa.org/intech/201810standards/
5 https://www.nen.nl/Trainingen/Elektrotechniek-overzicht/IEC-62443-Cyber-security-for-Industrial-Automation-and-Control-Systems.htm
6 https://wetten.overheid.nl/BWBR0041515/2019-01-01
7 https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/voor-wie-geldt-de-wbni
8 https://www.cybersecurityalliantie.nl/alliantieprojecten/documenten/publicaties/2019/09/30/cybersecurity-woordenboek
9 https://cisecurity.org Table Top Exercises: Six Scenarios to help prepare your cybersecurity team. Centre for Internet Security, accessed January 16th, 2020
10 https://www.batenburg.nl/research-development/
11 https://www.ncsc.nl/aan-de-slag/samenwerken/start-zelf-samenwerking/samenwerking-sector
12 https://www.gartner.com/en/documents/3873972/2018-strategic-roadmap-for-integrated-it-and-ot-security
13 Open Source Data Diode: https://www.thehaguesecuritydelta.com/images/Factsheet_Data_Diode.pdf
Fox DataDiode: https://www.fox-it.com/en/technology/datadiode/
Compumatica MagiCtwin: https://www.compumatica.com/products/products/magictwin/?type=
14 https://www.hudsoncybertec.com/nl/ot-insight/

Publication information
Implications of OT and IT Integration for Cyber Security

A publication from
Security Delta (HSD)
Wilhelmina van Pruijsenweg 104
2595 AN Den Haag
T + 31 (0)70 204 5180
Info@securitydelta.nl
www.securitydelta.nl
@HSD_NL

Authors
Aniek den Teuling
Stef Liethoff
Emmy Koning

Editors 2021 version
Marcel Jutte
Bert Feskens
Stef Liethoff

Design
Studio Maartje de Sonnaville by the design
of Studio Koelewijn Brügenwirth

Print
Drukkerij Edauw + Johanissen

Together we Secure the Future

www.securitydelta.nl