IT/OT Cyber Security   whitepaper

How to make IT and OT more cyber resilient

MAY 2021
Operational technology is of vital importance

It is not only used to produce our foods, but it is also essential for the quality and supply of energy and drinking water, among other things. The key is basically to deliver a predictable (high) quality and the desired volumes at a minimum cost price.

Security is crucial here. It offers many opportunities to optimize production processes with the aid of IT applications. In order to achieve this, many companies have enthusiastically embarked on far-reaching automation and digitalization. Innovation and predictive maintenance are needed to ensure a better quality, higher volumes and a lower cost price. However, companies that want to seize these opportunities, will also have to consider the risks. This white paper will explore the security trends in operational technology, the future of the field, the business case and how monitoring in an OT environment actually works.
(Security) Trends within Production Environments

This chapter will explore the trends that are relevant for the predictability of the production process, sales increase and lowering costs in more detail.

One of the key trends at production companies is making factories more intelligent through ongoing digitalization and automation using technology. Aiming at optimizing processes faster, shortening lead times and making work overall more efficient. Innovation is an important topic within production environments as well. It needs to be more sustainable, better and, more in particular, faster. The race for the lowest cost price, the most sustainable product, the highest predictability and the best quality is happening head-on. This without in any way compromising safety.

Even more Links

In order to innovate and automate, machines are increasingly geared with new forms of controls, such as apps. This introduces technology in an environment in which continuity and stability are vital. Our National Security Monitor shows that 85 percent of organizations in the chemical and production process sectors at some point in their production process deploy Internet of Things (IoT) solutions, such as sensors that are connected to the Internet for read-outs of machine status. Connections from IT to OT, such as an interface to Enterprise Resource Planning, or ERP systems, are not new. Moreover, the development of Programmable Logic Controllers (PLCs) is increasingly more advanced, which blurs the line between computers and PLC. This not only adds value, but it may also involve risks since traditionally the OT side is not protected by design. And there was no need to; the systems were not connected to the outside world. The National Security Monitor also shows that 83 percent of tech decision makers in production companies themselves believe that insufficient knowledge is available as yet about the correlation between OT and IT and the security that this entails.
Journey to the Cloud

Currently, crucial production systems are still mainly located on site. At the same time, the need for information from production is increasing in many companies. The corresponding software is increasingly moved to the cloud. This renders the journey to the cloud, already made by IT, visible within OT as well. This trend and the growing links with the cloud ensure that the OT environment converges even faster with the IT environment. These innovations follow each other in rapid succession and bugs are to be avoided. Maintaining the balance between innovation on the one hand and predictability in product environments on the other, poses a challenge to many companies.

Employing Detection & Response as Innovation Enabler

The increasing number of links with IT and IoT, the development of PLCs and the journey to the cloud not only represent an opportunity to optimize processes, but also to implement security more efficiently. Developments in this field are advancing as well. Previously the focus was on prevention, protection against hacks. Today it is shifting towards detection and response. No security solution is completely waterproof. In addition, ease of use of security solutions is becoming increasingly important. The provisioning of security measures should not complicate work but ideally rather make it easier. Measures that are too restrictive may lead to no-go practices. Think ‘saving’ complicated passwords on post-its stuck to the monitor or the use of flash drives to update and quick fix defects. It is therefore important to emphasize measures that will not compromise ease of use. Accept that danger may invade and thus aiming at early detection in order to subsequently respond in an effective fashion. Not only to limit or prevent damage, but also to restore to a higher level. This is called defensibility. It has already been largely employed in IT. In OT environments specialized detection and response is very beneficial as well, as often unpredictable and continuously evolving threats are timely detected enabling the corresponding response.

Provisioning Cyber Defence is the answer to these trends. In the next chapter we will explore how this works in more detail.
The Business Case

The race for more sales and sustainability hinges largely on quality, efficiency or cost price. For higher quality, sustainable products and a lower cost price, innovations are necessary. For example, process automation provides efficiency, a higher degree of predictability of quality and volume, less waste and less dangerous work thanks to the use of robots. Business innovation is therefore high on the agenda. Virtually any form of innovation requires more links with the OT environment. For example, better products require data about sales, volumes and quality. In order to maintain minimum stock, perfect alignment with the production capacity is key. Linking IT and OT, (large) sales are directly communicated to the factory so that production can be scaled up. In addition, in order to boost the bottom line, automation is needed to achieve efficiency and larger volumes.

Knowledge of the OT Environment

OT environments are focused on commissioning machines as fast as possible. The installation of new machines and maintenance are often carried out pragmatically. Besides, there often is much legacy, machine lifecycles are prolonged through maintenance. As a result, companies are frequently in the dark as to what versions of protocols and software are used. As a consequence, the vulnerabilities of the infrastructure are not clear. For example, many production environments use SolarWinds products without being aware of it. Charting the entire infrastructure and only using secure protocols is complex. Legacy machines are often not tuned to this and companies therefore resort to legacy protocols. Monitoring ensures understanding of the vulnerabilities in order to mitigate them. An example is the number of external devices that have access to the OT environment. Monitoring renders transparent how many there are, allowing this number - and with it the risks - to be reduced. These risks can be calculated more easily, so that informed decisions can be taken as to which devices may be allowed.
Information Technology (IT)
The data and flow of digital information that is seen all around us. It deals with information for user applications, storage, management and many more.

Operational Technology (OT)
The use of hardware and software to monitor and control all the automation assets specific for the production process.

Digital Dilemma
Digital innovation creates value, and leads to more connections, hence cyber risks; more connections also allow for better monitoring and increased resilience.

IT/OT SOC
More connections! Let’s hack!

IT/OT 24/7 SOC
- Protect your assets and data
- Detect attacks quickly in a SOC (Threat hunting)
- Respond appropriately to prevent/mitigate damage
- Recover to a higher level of resilience
- Exercise! Preferably in a simulated environment (Cyber range)

HEADQUARTERS
“Great Innovation! Let’s do this!”

DISTRIBUTED SYSTEMS OPERATIONS
“Great Innovation? How do I implement it safely?”
Cybersecurity as Enabler

Innovation requires (data) integration. Currently, this concept is not yet fully embraced since integrations and technological innovations are considered a potential risk to day to day operations. Not all innovations can be fully tested beforehand, while many interlinked system dependencies exist that make things more complex. This is why advanced technologies, such as the Industrial Internet of Things (IIoT) supporting predictive maintenance, are applied cautiously; they enhance the attack area and with it the vulnerability to external attacks. Deploying detection and response offers the solution to reduce these risks.

Within IT, it is customary to purchase 24/7 monitoring of the entire environment as a service from a Security Operations Centre (SOC). The simple reason is that individual companies can hardly afford to have such expertise in house 24/7. Let alone maintaining a response team that can take immediate action if something suspicious occurs. As mentioned above, innovations are being implemented. On the one hand, this means that the number of connections grows and with it the risks as well. On the other hand, thanks to the many connections, monitoring is improved rendering the organization more able to ward off external attacks. OT environments are often static with predictable network behaviour, which means that continuous monitoring can provide upfront analysis of internal dependencies.

It is often desirable to include security in the development of innovations. This is called Secure-by-Design. It is not feasible to develop something that is entirely waterproof, and trying this is not recommendable. It is better to accept the fact that non-authorized people will be able to find a way to access the factory remotely. That new systems offer chances, but that the links in any existing OT environment may also involve risks for the systems that are already in place. And that the security of legacy systems is not compatible with new systems, leading to downtime. Detection and response therefore provide a better solution to faster innovation and lower risks. Besides, it has other benefits as well.
Criminal Inquiry

Continuous monitoring captures undesired activities. Should people with malicious intent try to harm production, they will not only be stopped quickly but also be tracked down. Data collection about infrastructure activities allows for the collection of burden of proof and the prosecution of any illegal activities. By having clear evidence of who performs what action, and to correlate this with future events, insurances will become accessible and criminal inquiries are supported. For example, picture an unmanned vehicle (Automated Guided Vehicle - AGV) that comes crashing through the factory wall due to a change in the software. You will be able to prove afterwards that the incident with the AGV can be traced back to the incident with a hacker or supplier modifying the software. Cyber damage will therefore become traceable.

Gap Analysis

Finally, continuous monitoring also supports gap analysis. This allows companies to determine where a wide range of OT security frameworks, such as IEC 62443, is adhered to or breached. This is a way to demonstrate that law and regulation are complied with, improvements are being made and reports carried out. Based on a monitoring analysis, modifications can be implemented, which can also be tested by monitoring. Safety Instrumented Systems (SIS) ensure the safety of the factory, for example the maximum temperature of a machine. Monitoring, however, enables you to discern variations that deviate from normal behaviour. This may be an indication that either the new software or the equipment fails. This type of trend analyses renders the process even more predictable. Moreover, data that are required for compliance reporting are collected automatically. This allows all sorts of periodic audits to be carried out without any additional paper work.

Deploying monitoring in the OT environment thus yields multiple benefits. They all contribute to building the correct business case. But how does monitoring exactly work? In the next chapter, we will explore this in greater detail.
Monitoring the OT Environment

Many IT environments use 24/7 monitoring and thus maintain transparency in cybersecurity. This facilitates the detection of unwanted activities. The more information is available regarding ‘normal’ behaviour, the faster abnormal behaviour can be detected. To become more agile as an organization and to be able to innovate faster, OT environment monitoring is crucial. OT and IT are inextricably connected. However, monitoring an OT environment requires different skills than an IT environment.

IT Monitoring Alone

OT environment monitoring facilitates faster innovation. For example, take IIoT solutions; they are key to generating data that enables process optimization and essential to controlling the OT environment. OT environments thus need IT, which also creates numerous links between both infrastructures. Links lead to vulnerabilities if they are not leveraged. It is therefore essential that 24/7 monitoring be extended to the OT environment. This way risks can be more easily mapped and mitigated.

Current practice shows that many companies only monitor their IT environment. This does not, however, reflect the trend that IT and OT are so emphatically interwoven. This is how the SolarWinds hack ended up in production environments through OEM (Original Equipment Manufacturers) produced software. Similarly, remote access to a robot arm does not have to be linked to the IT environment to represent a risk. Monitoring the OT environment mitigates risks and offers benefits such as faster innovations and compliance with law and regulations. The next step therefore is IT and OT monitoring as one environment. However, OT monitoring requires other skills as well; not every Security Operations Centre will be able to offer both competences.

Security Operations Centre

Monitoring of incidents is mainly done via a Security Operations Centre. At Thales in the Netherlands, data and systems are monitored 24/7. This allows for the fast detection of incidents which enables immediate action.

Detection Differences Between IT and OT

To get an idea of what OT environment monitoring entails, the differences with IT should be laid out. The greatest difference is that IT traffic is dynamic and OT traffic static. The production environment operates properly if the same repetitive activities are carried out continuously. OT monitoring therefore focuses on detecting the odd one out, thus making the environment on the whole more predictable. Detection in an OT environment is therefore easier. Deviations can be detected faster than in a dynamic IT environment. This makes it easier for systems and analysts to identify irregularities; the response is the real challenge.
Response Differences Between IT and OT

The response within an OT environment is a greater challenge. When detecting irregularities, an IT analyst is able to act immediately to minimize the impact by taking the infected computer offline. This does not affect the entire environment. The same action can not be propagated to the OT environment. An OT analyst must be aware what the impact will be of an incident on the production process and what the potential consequences may be in case of intervention. To power down a machine in the production process may have grave implications for the entire process. The best response is based on this consideration. Ideally, action is taken, serious impact avoided and no downtime caused in the production process.

Another consideration in a production environment in case of an incident is the question whether the safety of people will be compromised. Are workers safe despite the incident and can the quality of the product still be safeguarded? This is why the repair works differ. An example would be temporarily powering down a packaging machine in order to replace the firmware on a compromised PLC (Programmable Logic Controller). Such intervention will always require close consultation between the SOC analyst and the OT operator. Stopping or resetting a PLC will have direct consequences for the entire chain in the factory.

Integrate IT- en OT Monitoring

Technically, no distinction can be made between monitoring IT and OT environments. Due to the many links, threats will not be stopped at this separation line. Within production companies, however, this is often still organized in separate organizational units. For effective detection and response to take place, it is important not to make this distinction and to gain understanding across domains. The benefit is that irregularities in one environment may be an indication for incidents in the other. This provides better understanding and may pre-empt any potential negative consequences. Logically, when the threat is visible within OT, it is already active, which you would rather want to rule out proactively. A targeted cyber attack, or Advanced Persistent Threat (APT), includes a number of steps before it reaches its target. For example, a hacker uses a phishing email to access a work station of the server. Through combined monitoring these steps would be recognized earlier. This allows for a faster response and limits damage. One stand-alone action maybe difficult to recognize, but a chain of actions so much the better. This way, security analysts can be one step ahead of the hacker that is targeting the OT environment.

Security Operations Centre

Thales is building the Cybels Sensor, which identifies APT cyber attacks even faster and automatically. The information from the specialized IT and OT solutions is converted so that SOC analysts are able to combine the alerts from both systems. In addition, the Cybels Sensor is equipped with sector-specific threat information. This facilitates the prevention of damage even more. Currently there are no solutions that are able to do this automatically.
The Future of Defensible OT Environments

There is still a great deal to be gained in the field of production environments and for critical infrastructures. Developments happen fast. What does the future have in store?

Within OT environments, security remains the top priority. This is why cybersecurity becomes increasingly important. Because of this need, the number of machines that apply secure-by-design is growing. Subsequently, the number of secure protocols used for the exchange of messaging and data is growing as well. Due to the life of machines, it will still take a long time before all machines in the company will be able to communicate with each other through secure protocols. As laid out above, monitoring is an effective means to solve this problem.

Since security is vital, more and more cybersecurity measures will find their way to OT environments. Safeguarding security remains important here, without affecting ease of use. One method to do so is red teeming. In a red teeming drill, ethical hackers scan for vulnerabilities within the OT environment that could be exploited by cyber criminals. This drill is aimed at gaining understanding of the risks that the organization is running and subsequently implement improvements. In addition to fire drills, it is important to conduct cyber drills. Exercise in peace time so that, when required, optimal procedures are stand-by. In an OT environment, such exercise is a challenge. That is why it is important to work with test environments to simulate real practice.

Response Differences Between IT and OT

The success of detection and response hinges on the number of connections. When new connections are created and added, new services and means will be devised for their security. Take for example IoT. In the past year, the technology to monitor IoT from a SOC has matured and is still developing. Finally, the experience of Security Operations Centres specializing in OT environments is increasing. Subsequently, the number of roadmaps is growing as well. These roadmaps include the actions that lead to irregularities within OT environments. The growing knowledge ensures that attacks can be stopped even sooner. Moreover, the development of algorithms to stay ahead of hackers is gaining in importance. Here at Thales, we also continue to build a future we all can trust. The defensibility of critical OT environments is an important part of this!
Contact us
For more information about how to leverage connections and deploying monitoring or other security measures, please contact Eric ten Bos, OT expert at Thales via eric.tenbos@nl.thalesgroup.com

> thalesgroup.com <