Cyber security in production sets new demands for manufacturing

Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of physical devices, processes, and events in manufacturing. It may include IIoT (Industrial Internet of Things), robotics, process, and production control, for example. IoT networks, in turn, connect a wide range of devices and sensors that collect and exchange data.

Increasing information technology content in these traditionally isolated areas is calling for new emphasis on cybersecurity design in new production units as well as maintenance in existing facilities. Proper design and maintenance principles will ensure business continuity and keep valuable information safe. Customers require better third-party security wherever data concerning them is handled and compliance with regulations, such as NIS2 (Network and Information Security) and CER (Critical Entities Resilience) drive for improvements too.

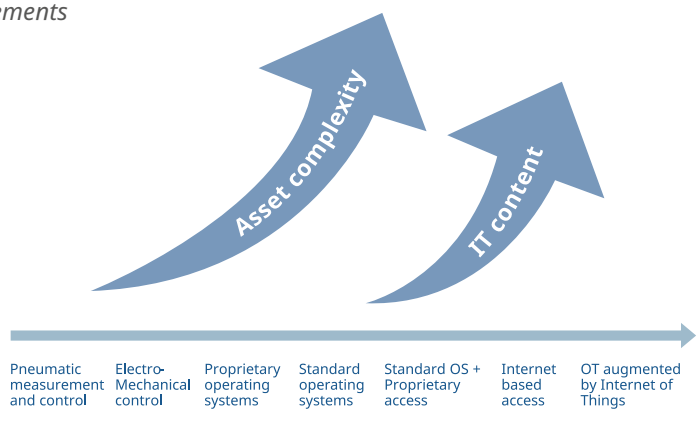
OT typically focuses on running a mill's main processes according to their design. In older mills, and if the basic process has remained stable over time, OT solutions – be it MES, DCS, Scada, programmable controllers, or others – may be perfectly capable of running their core tasks for a long time after the initial investment. These systems have traditionally been physically fully isolated from the outside world, and the need for cyber security has been very low. Over time, an increasing amount of IT has been added to the same landscape, potentially opening access to it and therefore, substantially elevating the requirements for cyber security.

This Midagon Point of View focuses on cyber security development in the manufacturing environment. These improvements are necessary as integral parts of all efficiency development initiatives but also becoming mandatory due to changes in the external environment.

Read also: Midagon Point of View on production efficiency improvements

Legacy systems and low standardisation levels are the enemy

Manufacturing machinery and OT systems are traditionally highly customised and dedicated to manufacturing specific products or a range of products. Quite often, only one OT vendor provides maintenance parts and services for one machine or manufacturing department. Standards and platforms may be missing. This is much like the corporate IT situation some 20 years ago, before IT departments got the mandate to standardize and hence save costs.



Picture 1. As efficiency improvements drive both asset complexity and information technology scope, security design becomes more and more paramount

IT has an increasing role in facilitating business growth through new businesses and more efficient processes. At the same time, the level of outsourcing has increased. Along with additional cost pressures, this means there is less money for the traditional activities, namely keeping IT up to date. This, in turn, results in older systems not being replaced very actively.

Therefore, installed base is not only a business continuity risk itself but also contributes to the ever-increasing cyber security threat. When outdated, systems are easy targets for cyber-attacks. Some inherent features of the installed base may limit their use in a modern solution landscape. These may be related to a lack of patch management capability, insufficient systems resources for running the security features or simply the visibility of the devices in the network yet providing an access point to the whole.

It is worth noticing that the skills needed for maintaining and developing older-generation OT solutions are normally not widely available due to the bespoke features of the solutions and the facilities they monitor and control. Old systems are supported by aging personnel who, in many cases, do not know the whole landscape. Support may be outsourced to OT vendors who only know their machinery. Whether working with internal or external payroll, the older generation is not willing or capable of learning new solutions, and the younger can't see the benefit of learning about almost obsolete technologies. Running factories remotely has become an option. In fact, some service providers base their services on the capability to provide them remotely – with increasing risk, obviously.

Operations development may lead to additional challenges

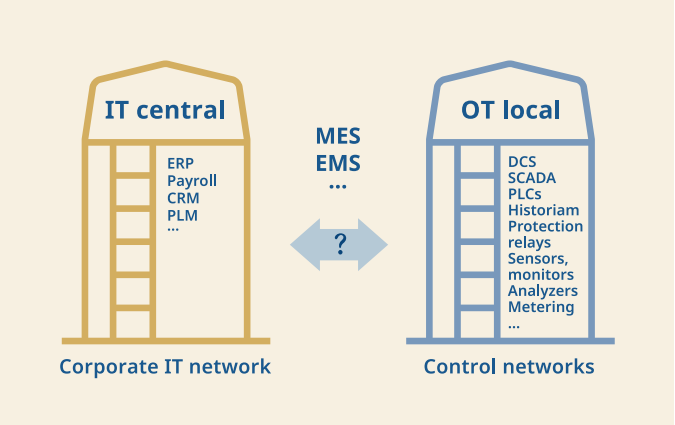
One of the most urgent business drivers for system changes is gathering more data from manufacturing devices and systems for efficiency. Compliance requirements may be another reason for data collection. The ongoing ERP upgrades across corporations will likely introduce new business processes and application functionalities that will put pressure on manufacturing systems in turn.

The need for OT systems to be connected and accessed by IT systems is increasing. This increases network capacity and security set-up requirements. Incidents in IT lead to loss of information, while incidents in OT may lead to loss of life.

OT vendors also play a critical role in designing, building, and implementing new features. If their solution remains as a component in the new architecture, their cooperation is needed. Internal IT and OT personnel and external IT and OT vendors are needed for the full picture.

Organisationally, these resources reside in different teams, and the internal participants may have different coverage with respect to their global or local coverage.

As OT uses more standard IT components, joining forces and using the whole company's purchasing power will save costs. This may also mitigate the threat of losing critical skills when the current generation retires.



Picture 2. IT is traditionally centrally organised, whilst OT is owned by the local organisation at the production site. This should not become an obstacle to synchronous security management.

> *I have an existing mill and I'm concerned about cybersecurity. What should I do?*

Understand where you are

Whilst security audits are useful for new production facility designs, they have also become common as a tool to increase top management awareness of cyber security threats. Audits provide an outside view of the company's current situation without bias. They create a clear understanding of business continuity and information security risks and give focus to the development work.

Understanding the company's systems and their lifecycle status is the starting point. Ideally, all assets are in the same inventory system, like Configuration Management DataBase, CMDB. This would collect information about manufacturing machinery and IT hardware and software, including license information, in the same place.

Define the target state and roadmap

Companies should decide on the high-level target stage of their manufacturing IT architecture. How to get there is

> *Left unchecked, technical debt will ensure that the only work that gets done is unplanned work*

in most cases a long and costly road. One Infrastructure and security set-up, including an optimised support model for the manufacturing operation, should be the ultimate target. Reaching a low risk level may be a costly exercise and be a balancing act on risk, cost, and skills as parts of the overall solution can become obsolete.

The knowledge gap of OT teams regarding IT systems and security can be solved by training the people, agreeing the roles and responsibilities between OT and IT. Let OT concentrate on running the business and IT ensuring that the systems are working.

Operate safely and provide support on issues

When something goes wrong, a speedy response with corrective actions is crucial. A well-documented architecture, understanding the dependencies between systems, and repeatedly rehearsing incident response processes will get you back to business faster.

Organisations must ensure security in many layers. Information and data are the most crucial assets for IT to protect. Cybercriminals have lately noticed that, too. Encryption backups and demanding ransomware cases are surfacing more to public knowledge. Instead of relying on old offline types of backup solutions, companies should change to modern backup solutions with immutability and backup scanning solutions for malware detection.

Sometimes, when OT & IT are not integrated on a network level, data is transferred via portable media. If either side is virus-infected, spreading them further is likely. Portable media handling should be minimised, and scanning the media before connecting is essential.

Cybercriminals are entering companies slowly. They look for weak points of the defence. Their target is often to find poorly managed user accounts with admin privileges, penetrate critical systems and data and take control of them. Once succeeded, ransom demands are on the table. Collecting log information and analysing it with security tools and the Security Operations Center help find suspicious movements from the network and other systems.

Fix the architecture, and don't forget about integrations

As the need to exchange data between manufacturing systems and corporate-level systems increases and updating all the legacy takes a long time, network segmentation helps control the data traffic securely between those systems. All systems should be separated with firewalls and security monitoring tools to control and detect unwanted network traffic. OT vendors are already supporting systems remotely. However, remote connections are often a big security risk as IT professionals do not necessarily implement them.

Fundamental ways to keep the attack vectors as small as possible for cybercriminals include:

- Ensure all devices with IP addresses and network connections are **configured with endpoint security software and unnecessary software and protocols** are **removed.**
- The needed service breaks are implemented to **install all patches** provided by the hardware and software vendors, including OT and IT vendors.

It's clear that this level of change to the current ways of working, roles and responsibilities is not easy to implement. Full support from top management is essential for success. Involving change management professionals guarantees that the needed changes are implemented fully and the change sticks to the organisation.

Finally, some parts of the OT legacy may need to be replaced. It is sometimes difficult to justify these with traditional business case elements, like operational improvements. However, risk mitigation and the value of business continuity should be considered motivating benefits in this context.

Start improving your security today

There are very clear reasons with backed up business impacts to act now.

1. Take the first step and start the discussion with your colleagues in the IT and OT organisations.
2. Agree on a joint OT/IT infra and security architecture target, including mode of operation, support model, funding model, and roles and responsibilities.
3. Document the current situation. To do this, use experts to run a Security Audit.
4. Prioritise the actions jointly between IT and OT experts and decision-makers. Establishing a Security Operations Center may be an option.
5. Define a roadmap to reach the targets.
6. Run the needed projects according to their priority.
7. Continuously develop and update the steps above.

Prepare your organisation for the fact that this is a long journey and while it's not easy, it's compulsory.

Midagon's services

Executing the cybersecurity transformation in the manufacturing context is no simple task. Due to the unique nature of production processes and facilities, it is necessary to understand the operation itself before trying to identify the vulnerabilities. Experts with many different backgrounds need to work in unison to reach the desired targets.

First class project management is the core competence of all Midagon consultants. In production and other operations domains, this is augmented with our long experience in various environments. We are well equipped to understand the context and needs of different circumstances and clients. Midagon can help facilitate the work for understanding the current state, elaborating, creating, and maintaining roadmaps and project portfolios as well as running the various projects to reach the target.

Contact for more information:

Mika Mäkinen

Senior Managing Consultant

mika.makinen@midagon.com

+358 50 486 7104

Matti Ketonen

Senior Managing Consultant,
Supply Chain and Production
Community Lead

matti.ketonen@midagon.com

+358 50 381 9348

Ilkka von Schulman

Director, Strategy and Architecture

ilkka.schulman@midagon.com

+358 40 571 0712