Secure Manufacturing on Cloud, Edge, and 5G

Valuable threat intelligence to help navigate the latest changes
Digital manufacturing: Convergence of IT, OT, and CT

Global producers need to digitalize manufacturing and transform their business into a digital enterprise. Examples of digitalization at factory sites include predictive maintenance using information collected by cameras and sensors on the shop floor, digital twins of production lines and products, work support using virtual reality (VR), augmented reality (AR), autonomous driving of automated guided vehicles (AGVs), and free layout by wireless controlled robots.

These systems are made possible by the fusion of IT (information technology), OT (operational technology), and CT (communication technology), which all have originated from different backgrounds. Digital manufacturing is not something we need to look to the future to envision, with 60% of factories already using the cloud (87% including those being implemented) and 26% with Private 5G already implemented (67% including those being implemented). In addition, 61% of factories have experienced cyber incidents and are rushing to take security measures. This has presented challenges as many organizations have not updated their cybersecurity strategy sufficiently.

Traditional ICS (industrial control systems)/OT have not been integrated with cybersecurity. Systems using new technologies such as the cloud, edge computing, and 5G are often secure by design and also have the advantage of integrated management of assets. Cloud and 5G are not recognized as high security risk as a whole, but vulnerabilities can lay within siloed areas.

The purpose of this e-book is to utilize threat intelligence in order to understand the cybersecurity risks facing factories equipped with cloud and 5G technology.

The first step towards cybersecurity: Identify

Traditional factories have been designed on the assumption that security incidents will not occur. Whereas the basic tenant of cybersecurity is based on the premise that all organizations are subject to cyberattacks. Cybersecurity, in its purest form, is meant to identify possible risks and reduce the frequency and impact of the most harmful risks.

NIST CSF, one of the most popular cybersecurity frameworks, recognizes the first job of cybersecurity is to identify. This means understanding the context in which the organization requires protection, its critical functions, and the risks involved. This requires asset management, business environment governance, risk assessment, risk management strategies, and supply chain risk management. Organizations must also recognize that risks not only target technology, but also people and process. When manufacturing integrates cloud and 5G into their environment, it’s necessary to consider the laws and regulations in each country it services in order to remain compliant, update corporate policy, and instill governance.

The reason “identify” is presented as the first step is that threats often stem from asset and process vulnerabilities that have not been identified. Since it has not been identified, the security level is not defined, and when incidents occur, it becomes difficult to investigate, fully contain and respond to the threat.

This document identifies system changes based on factory production processes and explains the changes that the cloud and 5G bring to factories. This document also maps the attack scenario in order to highlight the kind of risk that lies in the entire system. This will shine a light on any overlooked best practices needed to build a resilient security strategy.

The diagram shows the NIST Cybersecurity Framework, which includes:
- Identify: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Protect: Develop and implement appropriate safeguards to ensure delivery of critical services.
- Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- Respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

NIST Cybersecurity Framework
https://www.nist.gov/cyberframework
Stakeholder roles in ICS

IEC 62443, known as a series of ICS security standards, specifies four types of stakeholders; asset owner, maintenance operator, integrator, and supplier.

The supplier develops, manufactures, and supports software and devices.

The integrator incorporates the product into the design and construction of the system.

The maintenance operator looks after and controls the system.

The asset owner is responsible for all responsibilities and operations, including policies and procedures.

When using the cloud or public network, the cloud or network service provider becomes a supplier, an integrator, and a maintenance operator. Commercial products, public cloud services, and network services don’t just make sense economically, but also have the advantage in that they share common infrastructure security. On the other hand, we cannot deny that management complexity will occur by using multiple services in combination with physical and virtual at various layers.

Asset owners need to know where, who, and how much responsibility they have throughout the system.

What does and doesn’t change when cloud and 5G is implemented

Supply chain risk management
The supply chain includes cloud and network services, and the providers work as suppliers, integrators, and maintenance operators. Identify what is required when making a request to a third party, as well as what you need to handle on your own end, based on the shared responsibility model in these services.
System structures and boundaries that change when introducing the cloud

The Purdue (ISA95) model has long been referred to as ICS architecture. It has a layered structure for each function in order to connect and automate information. This was also a useful model for creating separate security zones.

However, as apps, data, and processing move to the cloud and edges, the boundary segments between layers will no longer work together. In the cloud, the shared responsibility model is generally defined and lays out how to recognize where your own responsibility begins and ends for each cloud service.

More importantly, it is required to identify which asset and services are responsible for what function across the entire system, and how to set the security level for each function. You need to identify the users and assets to access, the required permissions, and the flow of data.

In addition, it is important to recognize where the data and resources are geographically located. Also known as data sovereignty, you should know which country governs the service providers and data centers involved.

What does and doesn’t change when cloud and 5G is implemented

Basic security rules that can be overlooked when operating within a closed on-premises environment becomes critical when moving to the cloud. This includes,
- Authentication, authorization, and secure configuration
- Managing users and data by ensuring asset owners follow and recognize the shared responsibility model
Changes to the field network when introducing Private LTE/5G

With advancement of automation, communications throughout the field network is shifting from the fieldbus to industrial Ethernet, although the real-time communications and reliability that fieldbus brings remains unchanged. While the use of wireless is rising, the ratio remains small. There are high expectations for the use of cellular networks as a means of providing wireless that satisfies the low latency and reliability required in the field.

Unlike wi-fi and Bluetooth, cellular networks are highly reliable because they are based on a mechanism that monitors communication status and stabilizes connections. LTE/5G separates control and user plane (C/U separation), enabling data communication according to the application while maintaining a high level of connectivity and mobility.

Asset owners need to consider the cost savings and level of security when using a cellular network in a factory. Public cellular network connectivity could be affected by use of other users, whereas private networks bring higher costs. 5G gives organizations the option of choosing a hybrid deployment method.

A popular deployment option would be to share the control plane and RAN (radio access network) for public use and place the user plane in private. UPF (User Plane Function) may seem to work similar as routers, but they are a part of the cellular core network, as devices communicate through both physically separated public control planes and private user planes. The cellular network should be regarded as a part of the factory infrastructure.

In addition, the use of cellular networks, whether public or private, requires considerable investment, so it is limited to 5G related use cases. In the future, if 5G and Wi-Fi6 are integrated as new standards, field wireless network will become more versatile.

What does and doesn’t change when cloud and 5G is implemented
If you switch from wired to private 5G, asset owners should review the following, - Vulnerability of connected devices - Encryption (supported protocol), port forwarding - Filter traffic and detect threats on the network It is important to be aware of core separation in 5G based on merging of public control and private data communications.
Map attack scenarios on process and systems

We have mapped threats of the production process supported by systems comprised of on-premises assets, cloud, and 5G.

The attack scenario is based on the Trend Micro Research report on potential threats in smart factories and all affect manufacturing production.

These scenarios include ransomware intrusion from IT, compromises to the MES database and industrial cloud, attacks from a cellular core network, the rewriting of command at the protocol gateway, and vulnerabilities in the programming language of robots.2

---

2 Trend Micro Research refer to the list on P.8
### Understanding risks of the threats revealed by these experiments

Trend Micro’s recent research shows that not only the ICS—which directly controls factory production activities—but IT, cloud, and cellular network connections can be entry points and routes for attacks.

It is important to identify the risks associated with attack scenarios holistically, not as a standalone asset or service.

<table>
<thead>
<tr>
<th>Zone</th>
<th>Object</th>
<th>Attack</th>
<th>Damage</th>
<th>Recommendation</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise and control network</td>
<td>IT endpoint &gt; file server</td>
<td>Ransomware lateral infection and sensitive file encryption</td>
<td>Production stoppage</td>
<td>Prevent lapses and mistakes in basic settings and configurations (password, privilege, router, etc.)</td>
<td>(Article) Fake Company, Real Threats (Full report) Caught in the Act: Running a Realistic Factory Honeypot to Capture Real Threats</td>
</tr>
<tr>
<td></td>
<td>HMI</td>
<td>Control of HMI</td>
<td>Device malfunction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise, control, and field network</td>
<td>IT system &gt; MES</td>
<td>Database compromise</td>
<td>Damage to products</td>
<td>Database protection Access control Cloud security EWS protection Development policy Software supply chain visualization</td>
<td>(Article) Forward-looking security analysis of smart factories (Full report) Attacks on Smart Manufacturing Systems: A Forward-looking Security Analysis</td>
</tr>
<tr>
<td></td>
<td>Application store &gt; EWS</td>
<td>Malicious software extension</td>
<td>Malware intrusion Stolen data</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cloud library &gt; EWS</td>
<td>Trojanized libraries</td>
<td>Device malfunction Production stoppage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control and field network</td>
<td>LTE/5G core network</td>
<td>Rewriting control traffic</td>
<td>Defective products Loss of security</td>
<td>Network encryption Manage network routing</td>
<td>(Web) The Transition to 5G: Security Implications of Campus Networks (Full report) Attacks From 4G/5G Core Networks: Risks of the Industrial IoT in Compromised Campus Networks</td>
</tr>
<tr>
<td></td>
<td>Rewriting monitor traffic</td>
<td>Defective products Loss of security</td>
<td></td>
<td>Use secured - encrypted, authentication, certificated protocol</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wrong command to PLC by port forwarding</td>
<td>Production stoppage</td>
<td>Network encryption R/W protection of the PLC Support challenge-response authentication in PLC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device compromised</td>
<td>Device malfunction</td>
<td>Endpoint security for LTE/5G-based devices Development policy across IT and CT Content security in 5G network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field network</td>
<td>Protocol gateway</td>
<td>Packet rewriting via the protocol gateway</td>
<td>Field device malfunctions</td>
<td>Manage protocol gateways as important assets Select protocol gateways with a packet filtering function Introduce industrial firewalls supporting the OT protocol</td>
<td>(Article) A Blind Spot in ICS Security: The Protocol Gateway (Full report) Lost in Translation: When Industrial Protocol Translation Goes Wrong</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information theft via robots</td>
<td>Information theft Financial gain via ransomware attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Generation of targeted and self-spreading malware</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Threat intelligence based on IT, OT, and CT helps manufacturing cybersecurity

In this document, we first employed threat intelligence across IT, OT, and CT to identify the risks associated with change. We can also use this method effectively in order to protect, detect, respond, and recover.

Threat intelligence is a broad term that can be misinterpreted, but the essential elements include context and action. And the intelligence required depends on who uses it for what.

As an example, CPNI’s past report have identified four subtypes; long-term use, short-term use, high level, and low level. Strategic intelligence is used by management and business owners to formulate risk forecasting, security strategies, and policies due to changes in the environment. Operational intelligence provides the perspective on what an attack campaign is aiming to achieve. This knowledge helps security team managers allocate resources needed to combat these and similar attacks. Tactical intelligence is known as tactics, techniques, and procedures (TTP), and MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) are typical examples. Technical intelligence can be achieved by recognizing indicators of compromise (IoCs), which include vulnerabilities, IP addresses, ports, file names and hash values. The SOC is responsible for handling these.

It is important that each stakeholder involved in manufacturing cybersecurity leverages threat intelligence across IT, OT, and CT, depending on their role.

[3 - EU Protective : Proactive Risk Management](https://ec.europa.eu/research/participants/documents/downloadPublic?documentids=080166e5b2a13ee7&appId=PPGMS)
How can Trend Micro support digital manufacturing?

Trend Micro's threat intelligence helps manufacturing cybersecurity in many ways. For example, based on our Trend Micro™ Smart Protection Network cloud-based global threat intelligence, statistical data on industry-specific ransomware trends, recognizing the state of industrial endpoints and utilizing Trend Micro Research's findings are useful when presenting planning strategies to C-level executives. They also provide value to educational workshops looking to promote the cooperation between IT and OT organizations. In addition, Trend Micro Research has provided international government and law enforcement agencies, including Interpol, the United Nations, the FBI, and the US Department of Homeland Security with valuable important information of the threat environment, attacker groups, and threat campaigns across the globe.

Learn more on our Research, News, and Perspectives page.

Tactical and technical intelligence can be automated so that it feeds into in your environment through our platforms and services. Smart Protection Network data such as files, IPs, and URLs—which are collected and analyzed globally—immediately stamp out attacks before they can harm you. Through our Trend Micro™ Zero Day Initiative™ (ZDI), the world's largest vendor-agnostic bug bounty program, we are uniquely positioned to understand the latest vulnerabilities and potential exploits. This allows us to instantly protect our customers with virtual patching technology that shields applications and environments. In addition, our solutions implemented by customers become sensors. This allows the threat defense platform, Trend Micro Vision One™, to provide you with risk visibility and the ability to faster respond to attacks. This is based on indicators of attack (IoAs) and IoCs found across multiple layers and various environments including IT, OT, and CT.

Learn more about our solutions for Smart Factories, the cloud, and 5G.