Applications Brief

ELATEC
RFID Systems

MACHINE AUTHENTICATION: ENDPOINT SECURITY IN THE SMART FACTORY

A GUIDE TO BEST PRACTICES IN CYBERSECURITY FOR PRODUCTION MACHINERY

Smart, connected production machinery has transformed manufacturing, leading to tremendous productivity, safety and product quality gains. However, the Industrial Internet of Things (IIoT) has also created new security risks. Connected machines represent a cybersecurity endpoint in the Smart Factory that can put facilities and data at risk. Strong endpoint security practices—including machine user authentication—are needed to protect valuable intellectual property (IP), prevent production delays, and ensure the safety of people and facilities.

PRODUCTION MACHINERY AS A CYBERSECURITY ENDPOINT

Cyberattacks on manufacturers[1] are rising, with an average cost of $4.47 million per incident in 2022. Many of these are traditional attacks on IT infrastructure (e.g., phishing attacks, ransomware, malware attacks on websites or networks, etc.). However, as the manufacturing industry ramps up using IIoT and Operational Technology (OT) devices, production machinery has become a tempting target for hackers and bad actors. Attacks on production machinery or safety instrumented systems[2] (SIS) can cause considerable operational disruption.

IIoT and OT devices are cyber-physical systems that act as endpoint devices for the factory network. In addition to risks presented by

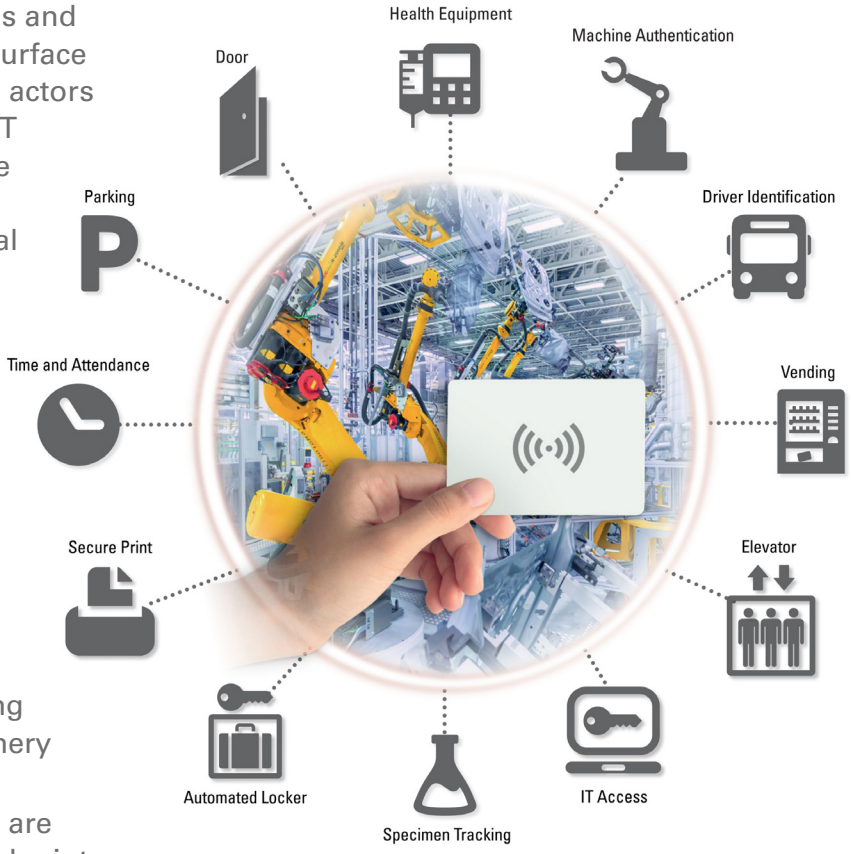
unauthorized access to machine controls and software, they also increase the attack surface for the factory as a whole, allowing bad actors to use them as a pivot point into other IT systems. Unprotected IIoT devices leave factories vulnerable to data breaches, malware and ransomware attacks, denial of service attacks, and other potential harms.

Cyberattacks on production machinery can cause severe damage, including:

+ Unexpected production shutdowns due to malicious capture of machinery controls.
+ Loss or theft of valuable company or client IP stored on or transmitted to connected machines.
+ Safety or product quality issues arising from unauthorized changes to machinery controls and settings.

In many factories, production machines are among the most vulnerable network endpoints. This is partly because IT and OT tend to exist in silos, with IT handling traditional endpoint devices (laptops, printers, servers, etc.) while the operations department handles machinery on the factory floor. The 2019 Deloitte and MAPI Smart Factory Study[3] suggests that IT and OT are seriously misaligned in many factories, leading to significant vulnerabilities on the factory floor. Other factors that increase cyber risk include:

+ Weak authentication methods that are easily compromised by hackers or inside actors.
+ Poor physical security on the factory floor.
+ Lack of proper encryption to protect stored data or data in transit.
+ Lack of security updates or outdated operating systems and software.
+ Legacy equipment that lacks modern security features.
+ Minimal endpoint and network security features (e.g., firewalls, intrusion or anomaly detection, antivirus software, etc.).



BEST PRACTICES IN OT / IIOT CYBERSECURITY

To protect people, data, and production machinery, manufacturers need a comprehensive cybersecurity strategy. This requires adopting best practices and complying with industry standards and regulations.

1. BRING IT AND OT INTO ALIGNMENT

One of the most essential things manufacturers can do is break down the silos between OT and IT. When considering production machinery as a network endpoint, it becomes clear that OT/IIoT devices must have the same level of attention and protection as laptops, servers and other IT devices. That means adopting best practices from the IT side. These measures include:

+ Ensure timely firmware and security updates for all production machinery.

- Implement network segmentation and isolation to prevent users or hackers from using machines to pivot into the network.
- Use appropriate encryption to protect production data both at rest (in the machine memory) and in transit (during communication between the machine and other networks or systems, including cloud applications).
- Adopt a zero-trust security model for networked devices, which continuously verifies device trustworthiness rather than assuming devices are trustworthy once verified initially.
- Utilize intrusion detection, intrusion prevention and anomaly detection software to detect unusual network traffic to or from the machine and monitor machine health and behavior.

2. PROTECT PRODUCTION MACHINERY WITH STRONG USER AUTHENTICATION

Machine authentication is a cornerstone of endpoint security in the smart factory. A strong authentication solution ensures that only authorized, trained operators can access controls for production machinery and allows companies to track exactly who has accessed each machine and at what times. The right machine authentication solution can also reduce the risk of remote hacking.

Many manufacturers still rely on password or PIN systems for machine access. However, passwords and PINs are often shared or forgotten. They can also be hacked.

Radio-frequency identification (RFID) offers a more secure alternative to a password or PIN for machine authentication. Users present a physical badge or token to unlock access to the machine. This can also be accomplished via a mobile credential on a smartphone using

Near-field Communication (NFC) or Bluetooth® Low Energy (BLE). An RFID or mobile solution for machine authentication increases machine security in several ways.

+ These systems are highly secure and difficult to clone or hack when appropriate encryption is used. Physical badges, tokens or phones are also less likely to be shared than a password or PIN.
+ The user must be physically present at the machine with the badge, token or device in hand to unlock access, reducing the risk that the machine can be inappropriately accessed via remote hacking or password theft.
+ For higher security, RFID and mobile access solutions can be implemented as part of a multi-factor authentication solution using a secondary password or biometric system.
+ Loss or theft of a physical badge, token or device is likely to be noticed immediately, unlike a compromised password. IT can quickly and easily shut off authorization if a card is lost or stolen or an employee leaves the company.

3. CONSIDER PHYSICAL ACCESS AS AN ASPECT OF ENDPOINT SECURITY

Endpoint security must be considered in the context of the total security concept, including physical security. Physical access control (PAC) enhances endpoint security by limiting who can enter the production floor or have physical access to production lines and machines.

This is important because many industrial espionage cases are inside jobs. Limiting physical access to production areas and machinery prevents bad actors from tampering with or disabling access hardware (such as RFID readers), plugging unauthorized devices into a machine (such as a USB drive carrying a virus), or damaging the machine. The PAC solution should go beyond the front door to enable monitoring of employee movements through production areas. In the case of a security or cybersecurity incident arising from the inside, it can be crucial to know precisely who has been in each production area and accessed each machine and at what times.

4. ENSURE COMPLIANCE WITH CYBERSECURITY STANDARDS AND REGULATIONS

Manufacturers must ensure that cybersecurity systems and protocols comply with industry best practices and relevant regulations. The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides guidelines for improving cybersecurity risk management across all industries, including manufacturing. It offers a framework for identifying, protecting, detecting, responding to, and recovering from cybersecurity threats. NIST has also developed a set of cybersecurity resources for manufacturers[4]. In addition, the system should comply with relevant ISO standards such as:

+ **SA/IEC 62443:** A widely recognized industrial automation and control systems (IACS) cybersecurity standard. It provides a structured approach to securing industrial control systems and is especially relevant to manufacturing.
+ **ISO 27001:** A globally recognized standard for information security management systems (ISMS) that manufacturers widely use to establish and maintain comprehensive information security controls.

Manufacturers in highly regulated industries such as energy or defense may have additional cybersecurity and machine access control regulatory requirements.

SETTING UP A SECURE MACHINE AUTHENTICATION SOLUTION

A strong machine authentication solution is an integral part of an endpoint security solution for manufacturing. For an optimal solution, consider the following points.

1. USE THE RIGHT ACCESS CONTROL TECHNOLOGY.

As explained above, RFID or mobile credentials using BLE or NFC are more secure, reliable and convenient than password or PIN systems for machine authentication. An RFID badge or token is usually the preferred choice in a factory environment. Smartphones may be a safety or security risk on the factory floor and can be damaged in dusty, hot or humid factory environments. Since most manufacturers issue a corporate ID card for building access and security, it makes sense to leverage the same card for machine access.

2. CHOOSE TRANSPONDER TECHNOLOGIES AND ENCRYPTION SUITABLE FOR THE APPLICATION.

Communication between the RFID tag and the reader should be encrypted to prevent eavesdropping and credential cloning. In general, high-frequency (HF) RFID technologies, which operate at 13.56 MHz, allow for more advanced encryption and longer encryption keys than low-frequency (LF) RFID technologies, which operate in the 125 kHz range. Well-known transponder technologies such as MIFARE, LEGIC and HID Prox or iClass offer a range of security features and encryption options. For machine authentication, look for a reader that supports at least 128-bit encryption (e.g., AES-128). Some readers now support advanced Elliptic Curve Cryptography (ECC) for an even higher level of security.

NFC is usually preferred over BLE for facilities that support smartphone use for user authentication. NFC credentialling mimics an HF RFID signal on the same 13.56 MHz band. Compared to BLE, NFC has a much shorter read range (a few centimeters vs. up to 100 meters), which ensures users are in close proximity to the machine or device they are unlocking. The short read range prevents others from piggybacking on

the proximity of users who are in the vicinity but not actively using the machine. It also reduces signal eavesdropping risks. NFC supports strong encryption, just like HF RFID. A universal reader, such as those available from ELATEC, enables manufacturers to support smartphone credentialing, LF or HF RFID, and even newer interoperable and open standard credentials such as LEAF or those based on public key infrastructure (PKI), providing maximum flexibility.

For even higher security, consider adding two-factor authentication. This can be accomplished, for example, by requiring both a password and an RFID token to log into the machine. Smartphone credentialling allows for an additional layer of security through the device itself; biometrics (facial or fingerprint recognition) can be turned on for the phone, ensuring that only the phone owner can open the credentialing app.

3. DIFFERENTIATE ACCESS LEVELS BY USER.

The access solution should allow for differentiation of access levels by user or role. Make sure the system allows a unique identification for each user so that it is possible to identify precisely who is operating each machine and when. Then, consider the type and level of access appropriate for their role and responsibilities.

Having different access levels for different roles (e.g., machine operators, line supervisors, process engineers, IT, and maintenance) is usually desirable. For example, line operators may only need basic access to a few machine functions to carry out production activities, while supervisors and IT may need to be able to access advanced machine parameters and configurations. For maximum security, users should only have the minimum access required to perform their jobs.

4. INTEGRATE PHYSICAL AND CYBERSECURITY.

With RFID, the same access control technology can be used for physical access control (including building entry and "beyond the door" locations), machine authentication, and digital access to systems and networks. A unified access system simplifies security for both IT and OT. It's also easier for employees, since the same credential can be used for everything they need to access at work.

An integrated system enhances endpoint security by limiting both physical access to machines and access to machine controls. This protects the machine from physical tampering and sabotage as well as unauthorized access to the human-machine interface (HMI).

Physical security also includes the integration of the reader into the production machinery. A reader fully integrated into the machine or HMI is more tamper-resistant than one simply plugged into the machine with a USB cord, for example.

Endpoint security is a critical consideration in the Smart Factory. Implementing a secure and reliable machine authentication system will help manufacturers protect sensitive data and IP, ensure facility and employee safety, and minimize the risk of operational disruptions.

1 Arctic Wolf. (2023, March 30). *Biggest Manufacturing Industry Cyber attacks.* https://arcticwolf.com/resources/blog/top-8-manufacturing-industry cyberattacks/

2 Higgins, K. J. (2018, January 25). *Industrial Safety Systems in the Bullseye.* Dark Reading. https://www.darkreading.com/operations/industrial-safety-systems-in-the-bullseye

3 Wellener, P., Shepley, S., Dollar, B., Laaper, S., Ashton Manolian, H., & Beckoff, D. (2019). 2019 Deloitte and MAPI Smart Factory Study. Deloitte Insights Research Center for Energy and Industrials Group.

4 NIST (2022). Cybersecurity Resources for Manufacturers | NIST. https://www.nist.gov/mep/cybersecurity-resources

For more information contact our Application Specialists at the locations below:

elatec.com

EMEA
Puchheim, Germany
+49 89 552 9961 0
sales-rfid@elatec.com

AMERICAS
Palm City, Florida, USA
+1 772 210 2263
americas-info@elatec.com

ASIA
Shenzhen, China
+86 755 2394 6014
apac-info@elatec.com

JAPAN
Tokyo, Japan
+81 355 799 276
japan-info@elatec.com