Cyber Security and the Industrial Internet of Things

What discrete manufacturers need to know

Avner Ben-Bassat, President & CEO, Plataine Technologies

PLATAINE®
people-smart automation

Your Intelligent Automation Partner, Delivering the Factory of the Future.
465 Waverley Oaks Rd, Suite 420, Waltham, MA, 02452 | 1-866-500-5902 | www.plataine.com

Executive summary

The Industrial Internet of Things (IIoT) and Industry 4.0 (I4.0) are transforming discrete manufacturing. Early adopters have already made extensive use of IIoT technology to radically improve factory efficiency and product quality. This has unleashed new competitive pressures for manufacturers across all sectors. Ultimately, no factory can afford to be left behind.

Cyber security is a big consideration for discrete manufacturers when implementing IIoT. Many companies are delaying investments due to cyber security concerns. Meanwhile, many others are enthusiastically adopting digital manufacturing technology without taking appropriate security precautions.

Both approaches are problematic: failing to invest in IIoT threatens the future competitiveness of discrete manufacturers; and failing to invest in cyber security precautions is risky because industry is a key target for hackers.

This whitepaper, published by Plataine, an IIoT specialist, outlines the specific cyber threats that discrete manufacturers face, and explains how they can be mitigated.

Definition: Internet of Things

The Internet of Things is a vision of a fully connected economy where physical objects are constantly communicating with the cloud. In an industrial context, it means that factories and industrial facilities share all their data in real-time, ensuring that managers can constantly track, optimize and improve their operations.

Introduction: the digital factory revolution

The Industrial Internet of Things is transforming the economics of the manufacturing industry.

As factories across the world go digital and become fully connected to the cloud, manufacturing managers are able to use a flow of real-time data to optimize production, cut losses and minimize waste. The result has been major improvements to efficiency and product quality in factories across a range of sectors, from food to automotive to aerospace to fabrics.

Early adopters have long embraced the potential of IIoT and are reaping the benefits today. The competitive pressures this has unleashed are now compelling a new wave of factories to go digital in order to remain competitive.

Yet IIoT brings problems as well as solutions. One particularly notable problem is cyber security. Many manufacturing firms are putting off IIoT investments due to the concern that, if they connect all the machines in their factories to the cloud, they will become vulnerable to hackers and other cyber security-related risks. Still others are jumping in headfirst without taking appropriate security precautions. Both approaches are flawed.

IIoT is here to stay and few manufacturers can hope to survive without adopting it. On the flip side, the cyber security risks to industry are real and growing. Discrete manufacturers across all sectors are targets for cyber criminals. Companies that adopt IIoT without taking security precautions are asking for trouble.

Cyber security: the threat to discrete manufacturers

Although the benefits of the latest manufacturing technologies are strong, discrete manufacturers find that upgrading to IIoT-level capabilities also brings a significantly higher vulnerability to cyber security threats[1]. This is because IIoT depends on smart, connected industrial machines. And being connected to the cloud means that a machine is suddenly potentially susceptible to cyber-attacks from anywhere.

Gartner, a global research and advisory firm, has released a survey showing that, over the last three years, nearly 20% of businesses were targeted by one or more IoT-based cyber-attacks. Gartner predicts that spending on IoT security will hit $1.5bn in 2018, rising to $3.1bn in 2021.

In a recent study into IIoT security, Trend Micro, a cyber security company, hacked into a series of industrial robots from different vendors[2]. The study found that the software running on industrial robots often uses outdated operating systems, that authentication systems are weak, and that tens of thousands of industrial devices around the world reside on public IP addresses.

The purpose of the study was to encourage IIoT component and system vendors to improve cyber security measures. Trend Micro argue that there are a series of reasons why a hacker might attack a manufacturing firm including:

- The theft of intellectual property
- Ransomware-style schemes where a cyber criminal damages products during production then demands ransom from the manufacturer to reveal which products were impacted
- Malicious product sabotage such as the introduction of invisible defects into drone rotors during the production process which later causes drones to crash
- Injuring or killing workers by disabling safety devices

Cyber criminals may use a variety of methods to attack industrial firms. One example is Havex – a remote access trojan that was specifically designed to attack industrial operations by collecting data from ICSs (industrial control systems) and SCADA (supervisory control and data acquisition) systems. F-Secure, an antivirus firm, has reported that Havex is used by cyber criminals to target European manufacturers of IIoT-related applications and machines for the purpose of industrial espionage. Havex criminals use 'watering hole' tactics where victims visiting legitimate websites commonly used by industry and business leaders are redirected to servers containing Havex-infected software.

A separate category of risk comes from a company's own employees. IIoT systems that don't use authentication or encryption are common. Such systems are vulnerable to abuse from disgruntled workers. A related issue is human error and/ or negligence which is responsible for a huge

proportion of cyber security breaches. For example, a 2017 IIoT risk report from Cyber X, a cyber security company, highlighted that 60% of industrial organizations allow passwords to access operational technology networks unencrypted, while 50% do not even use anti-virus software[3].

Threat mitigation: what can manufacturers do to secure IIoT systems?

[1] Waslo *et al* (2017), *Industry 4.0 and cybersecurity*. London: Deloitte University Press. Available at https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf
[2] Quarta *et al* (2017), *Rogue robots: testing the limits of an industrial robot's security.* Tokyo: Trend Labs. Available at https://documents.trendmicro.com/assets/wp/wp-industrial-robot-security.pdf
[3] Cyber X (2017), *Global ICS & IIoT risk report.* Framingham, Massachusetts: Cyber X. Available at https://cyberx-labs.com/en/blog/announcing-cyberx-global-ics-iiot-risk-report/

Strong cyber security arrangements can virtually eliminate the risks. Before implementing an IIoT solution, discrete manufacturers need a fully thought through cyber security strategy.

Ruggero Contu, research director at Gartner, a global research and advisory firm, says that most firms using IIoT systems do not have a common architecture or a consistent security strategy, and that the selection of vendor products and services tends to be *ad hoc*, and is often "based upon the device provider's alliances with partners".

Ideally, rather than relying on device providers for advice, the first step for a discrete manufacturer adopting IIoT should be to find an IIoT partner, and then to work with them to design a complete IIoT strategy from the ground up.

Risks and possible solutions

1. **A security fence between sensors and cloud**

IOT means connecting sensors, machines and devices to the Internet and that can be useful for numerous purposes.
However, when it comes to security, it can jeopardize your network.
Imagine that a sensor that reads vital metrics, such as location of parts and mobile tools at the factory, will send its data to the Internet and this data "leaks" into the wrong hands: a competitive company, or worse to an un-friendly organization.
It could be used to harm operations by manipulating the data and use it against the organization.
This is one case of many others that require the sensors and machines not to be directly connected to the Internet, so how do I do that?
Luckily, there is a solution – you need to create a buffer between the sensor layer and the Internet, by adding encryption algorithms inside your factory floor environment to manipulate all the data coming from the sensors to a secured and encrypted data repository that only you can understand.
Of Couse, these algorithms must be protected as well on a secured server, (location and data wise) and send it through secured channels, like SSL to the internet, where on the other side will be the second part of your servers receiving the data and make the magic. This way, even if it leaks, it won't make sense to anyone who gets it.

BTW, this mechanism can be used for another important reason – reduce traffic volume from the sensors to the cloud that will drive costs down.
In our example, much of the traffic between the sensors reporting an item's location is massive and redundant. Sensors rive around 100 times per second the location of an asset. Most of the times you don't need all this information, unless you're monitoring Superman 😊, the right way to handle it is to filter our all the redundant reads and transfer to the cloud only the events that indicate a change of the asset location or one indication per a reasonable period of time based on the use case.

2. **Multi-tenant environment.**

Building a multi-tenant environment is very common among cloud solutions for the following reasons:

- A single environment for all customers that is easy to maintain and support;
- Deployment is done only once, so all customers are upgraded at the same time;
- One code to manage, test and maintain;
- Business intelligence and insights can be computed from a larger data set that is vital for some machine learning algorithms and ensure more accurate predictions.

But it has its challenges, and the most important one, to my opinion, is the complete separation between customers' data.

We secure our customer data in multiple levels:

- In our database, we are attaching any data to its customer ID, so no query to the database could be performed without using a customer ID. In that situation, it's possible to hold one database for our customers and keep the data completely separated.
- To prevent hacking, we generate this customer ID from a session created after the user logged in and was authenticated.
- Additional hacking prevention is done when we do NOT use that customer ID from our UI (user interface), but only from within the server using authenticated data of the user.
- Customer's files are kept separately from each other, using different AWS S3 Buckets, one per customer, that is secured by AWS temporary security credentials that are created on-the-fly in real-time. That means that only after a user is logged in the system, we create temporary credentials in order to identify him and give him access only to his files within the bucket.

3. Internal employee damage control

Customer relying on your company and its employees not to harm or steal their data. They also rely on your company's employees not to damage their infrastructure.

To make sure none of the above happens, by error or deliberately, you should manage the employees' access to the data and infrastructure.

To make it manageable you should follow a few basic rules:

- Create a personal user for each employee, so no general password or key should be shared among users.
  In case an employee is leaving the company or switching roles, you can remove its user from the system without affecting other users.

- Give the minimal access needed to each user.
- Password change should be done every several months to ensure that each user changes his or her password, lowering the risk for hacking.

As for administrators:

- Some users will have full access to the data and infrastructure. This list should be short! but should include more than one user (in case of alien obduction 😊), probably the DevOps manager and the R&D Manager.
- Those users should use as much security as possible to prevent access to their accounts, using services like MFA, encrypting their laptops, not keeping passwords on a plain text file, etc.

As for developers:

- Access to logs so they can help in case of malfunction. But instead of giving them SSH access directly to all production servers, you can use one of many services, online or local, to aggregate all logs into one place that can give access to much more intuitive and cross servers logs, such as ELK.
- Database – my suggestion is to give developers read-only access to the DB as it's part of the data they should see during customer support events. When the customer has confidential data, it could be done by obfuscating sensitive data using some services.

As for customer support users:

- Those users should be giving tools to get data from customers, in case of such data exists only in the customer environment, such as access to log files, so those users will not need to access the production data or infrastructure to minimize risks.
- Access to logs should be done the same way as described in previous section (for developers) – using an external tool

4. External access to hardware

The infrastructure should be planed and build in such way that minimal components in the system should have access to the outside world, thus the Internet.

To do so, you should plan that only the necessary components should have an external IP and connected through ~~to~~ an Internet gateway.
All other components that can be accessed only from within the system, should be kept apart from the external network and can have access only from within the server to the outside world using a NAT gateway.
That separation eliminates the potential risk of direct access to your servers, services and databases from the outside world.

For employees who need access to the servers or for services that cannot be accessed from the outside world, you should create a secured VPN service and grant access only to specific employees that need that kind of access.

Choosing the right IIoT partner

Most manufacturers do not possess strong in-house IIoT capabilities, and so the first step on the IIoT journey is usually to choose a partner who can provide an IIoT software system and platform. IIoT platforms are the support software that connects the software in an IIoT system to the hardware and user interfaces. Strong IIoT platforms are crucial for cyber security, and for providing authentication for devices and users.

IIoT is a growth industry, and consequently there are a lot of companies out there purporting to offer a full IIoT solution. This means there's a lot to think about when choosing a partner. Cyber security should be among the top considerations.

Different industry verticals face very different cyber security threats, and thus have unique requirements. For discrete industrial manufacturers, a cyber security failure can be a huge problem. For example, if a production line in a high-volume factory goes down, it can result in millions of dollars of lost profits per hour. This contrasts with consumer IoT security requirements, where a breach may be nothing more than a slight inconvenience.

It is therefore crucial that, when choosing an IIoT partner, discrete manufacturers avoid consumer IoT firms. Instead, look for a specialist Industrial IoT partner. First, consider their past case history and ensure the provider can demonstrate a strong track record of providing secure IIoT systems to discrete manufacturers.

Next, set a meeting or call with the prospective provider to discuss security. It is important to ensure that IIoT software has security built into every element of the system. The solution provider should be able to quantify the impact of cyber security breaches in diverse areas, from legal responsibility

to revenue loss to data leakage. And their business model should be structured to allow them to deal with cyber security issues in real-time. See Fig. 1 below for a list of the top ten cyber security issues to discuss with a prospective IIoT partner:

1. Device-to-cloud network security and user app-to-wireless network security
2. Cloud security
3. Device and application security (including authentication, authorization and certification)
4. System architecture resiliency
5. Advanced threat detection and threat intelligence
6. How cyber security breach alerts are distributed
7. Access control precautions
8. The use of data encryption including full data protection at rest, in transit and in the cloud
9. Secure session initiation
10. Full training for company employees

Fig. 1 Cyber security checklist to discuss with potential IIoT partners

Finally, ensure that IIoT software providers have definite plans for updating their security features over time. This is vital because cyber security threats evolve with dizzying speed. It is particularly important to ensure IIoT partners can offer over-the-air communications so that regular patches can be easily installed.

Building a detailed security flow and project plan

Creating and structuring a methodic security and project plan is vital. To do this, it is advisable to bring in an external expert.

One option is to recruit an independent 3rd party IIoT consultant. Typically, an IIoT consultant will have significant industrial experience and will bring vast knowledge of the security problems faced by other discrete manufacturers. Another option is to use an IIoT software provider for this task.

An important part of any security plan is to set rules about how employees can access data. This should be dependent on user roles and sensitive data should be restricted to trusted employees. Defining and sticking to strict data access rules is an important part of how industrial firms can protect themselves against both employee negligence and the growing threat of industrial espionage. It is also important to set up a system for generating periodic security reports so that progress can be monitored, and weaknesses corrected where necessary.

According to a 2018 report from Cisco, most organizations are unable to see around 40% of the IoT devices on their networks and do not know what those devices are doing[4]. To ensure good cyber security, all digital assets on an IIoT production line should be mapped out so any security breach can be immediately located and dealt with. A dedicated IIoT security team is a necessary part of this process: this could be an internal team, or it could be external and managed via the IIoT partner. IIoT security gateways are a particularly important consideration. On a modern, IIoT-enabled, discrete production line, a network of devices and sensors monitors all aspects of production. These devices and sensors constantly talk to each other, to factory managers, and to external actors at both ends of the value chain – such as raw material suppliers and logistics companies. With devices in the same factory often communicating over multiple protocols, the whole process can become extremely complex. That's where IIoT gateways come in. In an IIoT ecosystem, the gateway sits between devices and the cloud, offering local processing and storage solutions (see Fig. 2).

[4] Cisco (2018), *Cisco 2018 annual cybersecurity report.* San Jose: Cisco. Available at https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

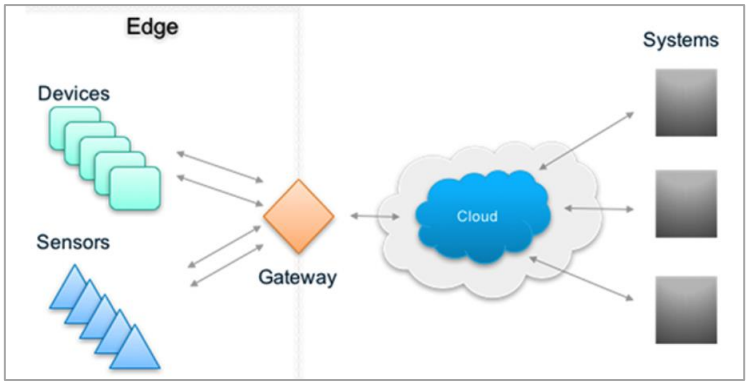

Fig. 2 – An IIoT gateway device within the wider IIoT ecosystem

Though IIoT gateways exist to improve system performance, they offer the opportunity to add a significant element of security to a manufacturing firm's operations. Communications between IIoT devices and sensors and the cloud must be secured. There are multiple ways to do this. One example is through a PKI (public key infrastructure). Under such a system, all IoT devices are assigned a digital certificate enabling the encryption of communication. The IIoT gateway is a convenient way to manage the assignment of digital certificates.

For a cyber-criminal trying to hack into an industrial system, the IIoT gateway is often the obvious point of entry. This is both because it sits between industrial operations and the cloud, and also because gateways tend to have higher processing power which can be exploited by an attacker. Therefore, for an IIoT-enabled factory, the IIoT gateway should be considered the first line of defense. An IIoT partner can provide detailed IIoT gateway security advice.

Training people

For the IIoT-enabled manufacturer, people – both employees and partners – are the most important elements of the system. Without skilled staff to keep it running, a sophisticated IIoT system is of little use. Yet people are also the biggest risk factor.

Human error or behavior is responsible for the vast majority of cyber security breaches – over 90%, according to Chief Executive magazine. And that means much of the solution to cyber security lies through better people management, rather than through solving weaknesses in technology defenses. Indeed, a huge proportion of cyber breaches are down to easily preventable instances of employee negligence – such as leaving a laptop on a train.

The best place to start is simple employee training to ensure that workers always use strong passwords and company-approved software. Thought should also be given to how and when employees are allowed to take company devices off site. Depending on the nature of the industry, it may be advisable to conduct employee background checks before allowing access to sensitive IIoT-related systems and data.

For more sophisticated IIoT security training, specialist IIoT partners will offer the best solutions. Many IIoT vendors offer a comprehensive cyber security training program, including sophisticated cyber-attack simulations (see below).

Maintain constant vigilance

Cyber security threats evolve fast. Therefore, industrial IoT security measures must evolve faster. Discrete manufacturers using IIoT should constantly monitor their own security status as well as keeping abreast of developments in the wider cyber security world.

Specific industries or technologies tend to have specific cyber security weaknesses. Trend Micro's study on industrial robots found that criminals could tailor their attacks to specific industrial robot brands[5]. The report name-checked the ABB Yumi cobot and several others. This implies that users of sophisticated IIoT-enabled machines would be well advised to keep up to date with news of attacks on their specific brand and model of machinery. Another recent example came from computer science academics Belikovetsky *et al* who co-authored a paper in which they demonstrated a specific hacking technique that could be used against drone manufacturers using 3D printers[6]. The technique allowed the introduction of virtually invisible defects into drone rotor blades during the 3D printing process. The result was that the drones crashed out of the sky when flying was attempted.

It's important for discrete manufacturers to be aware of the particular cyber threats they face. And the best IIoT software partners will make a point of keeping their customers up to date with industry-specific developments in the world of IIoT-related cyber security threats.

Prepare a response plan

Don't sit back and wait for a cyber-attack: be sure to make plans in advance.

Governments and regulators around the world are increasingly recommending that planning in advance for a cyber-attack is a requirement of basic corporate risk management. And failure to appropriately manage the aftermath of a cyber-attack can be more damaging than the attack itself. According to a recent report from Ernst & Young, a professional services firm, "It's no longer a question of if your organization will be breached, or even when, it's likely to have happened already. The real question is do you know and are you prepared to react?"[7].

Appropriate crisis planning is essential because companies that are unprepared for an attack will struggle to contain it when it happens and are likely to be impacted to a far greater extent. IIoT-enabled discrete manufacturers first need to set up a pre-planned attack response process. This should extend well beyond initial incident identification to include investigation of the incident, measures to contain it, and procedures such as data restoration that can ensure damage is quickly rectified.

But setting up a response plan is not enough on its own. The plan needs to be tested and the best way to do this is via regular simulations. Simulations ensure that everybody in an organization who will be involved in the response to a cyber-attack is fully aware of their roles and responsibilities. Good simulations teach staff of the importance of reacting immediately and of coping in a pressurized environment where decisions must be taken fast, and only limited information is available.
Simulations also ensure staff develop invaluable understanding of the technical aspects of a cyber-attack. Other benefits of simulations include exposing employees to the motivations of cyber

[5] Quarta *et al* (2017), *Rogue robots: testing the limits of an industrial robot's security.* Tokyo: Trend Labs. Available at https://documents.trendmicro.com/assets/wp/wp-industrial-robot-security.pdf
[6] Belikovetsky *et al* (2016), *DrOwned – cyber-physical attack with additive manufacturing.* ARXIV: September 2016. Available at https://arxiv.org/ftp/arxiv/papers/1609/1609.00133.pdf
[7] Kessel *et al* (2017), *Cybersecurity incident simulation exercises.* London: Ernst & Young. Available at https://www.ey.com/Publication/vwLUAssets/EY_-_Cybersecurity_Incident_Simulation_Exercises/$FILE/EY-cybersecurity-incident-simulation-exercises-scored.pdf

criminals and developing awareness of the direct impact that a cyber-attack is likely to have on customers. Additionally, simulations can ensure non-technical aspects of cyber-attack responses are also rehearsed, such as external communications strategies which, depending on the severity of the breach, may be vital to maintain the confidence of concerned customers.

Conclusion – use external expertise, and don't be put off: the IIoT is here to stay

When the security project plan is complete, it should be checked by an external expert who suffers from no preconceptions about the business and who can ensure nothing critical was missed out. A 3rd party consultant or IIoT software provider will be able to do this.

While the cyber security threats that come with adopting IIoT may seem daunting, they must be balanced against the competitive challenges that discrete manufacturers will face if they fail to adopt the latest manufacturing technologies. Those manufacturing companies that delay adopting IIoT will ultimately be forced into it by market pressures. Similarly, those firms that adopt IIoT but fail to take security seriously will soon find themselves to be the victims of cyber security problems.

The most efficient way to adopt IIoT while ensuring cyber security is to find a specialist industrial IoT partner with deep knowledge of the needs of discrete manufacturers and strong expertise at cyber security issues.