PLATAINE®
people-smart automation

WHITEPAPER

How To Manage Data Security for Discrete Manufacturers in the Age of Industrial IoT

Avner Ben-Bassat, President & CEO, Plataine Technologies

Introduction

The industrial internet of things (IIoT), Industry 4.0 and cloud computing are opening new possibilities for efficient production at manufacturing companies around the world.

Full connectivity enables better visibility across the supply chain, allowing industrial manufacturers to respond more rapidly to demand changes and disruptions. The time required to improve connectivity and data security will vary, depending largely on a company's operational setup, including the number of machines and software solutions in place.

Cyber-security is a vital factor for factories considering implementing IIoT-based technologies. This paper has been written with factory managers and decision makers in mind, to help better understand how to deliver a secured IIoT solution.

Industrial Internet of Things (IIoT) Background

The Industrial Internet of Things (IIoT) is delivering a step-change in manufacturing productivity. Increasingly, factories are using cloud-based, AI-enabled software to ensure all people, systems and machines are constantly connected. The benefits, in terms of improved efficiency are huge. Yet factories operating IIoT systems must take strong precautions to make sure they are protected against cyber-security threats.

The challenges posed by cyber-threats should not be a reason to avoid using the cloud. On the contrary, providing they work with a reliable, experienced security competent IIoT provider, manufacturers can benefit from the IIoT with confidence. Embracing the industrial internet of things is increasingly a necessity for manufacturing firms to remain viable and competitive. The challenge is to embrace it securely.

This guide is designed as an introductory walk-through, so operation managers can see exactly what needs to be taken into consideration when thinking about cyber-security and the cloud.

What you will learn

A) Cyber-security and the IIoT – open issues for discrete manufacturers
B) Myth busting – is cloud-storage less secure than on-site storage? (Hint: no)
C) The characteristics of a strong cloud IIoT solution
D) Conclusion: You need to partner with an experienced IIoT solution provider

Adopting IIoT solutions means transitioning to a system where machines and operations are fully connected; and it means depending on cloud computing for data collection, analytics, and processing power. Cloud computing holds enormous benefits; not least the ability to rapidly scale computing capabilities up or down in line with the needs of a business, as well as a significant reduction in IT costs. The issue is that connecting a factory to the cloud potentially opens its operations to the possibility of cyber-attacks. Some manufacturers are intimidated by this but - in reality - it is perfectly possible to keep your business safe, if proper precautions are taken. The first step to achieving strong data security, is to understand the potential threats.

Cyber-security and the IIoT – open issues for discrete manufacturers

Implementing an IIoT solution at a discrete manufacturing facility involves a radical increase in connectivity. In most cases, it involves networking a variety of industrial devices, machines, workstations, and workers. This requires the transmission of significant amounts of data between different portals and (in many cases) the storage and analysis of data in off-site data centers.

The sheer amount of sophisticated technology and machinery used by discrete manufacturers – usually consisting of one or more significantly sized factories – makes cyber-security a challenging task for the industrial sector. In many other business areas, for example retail stores, embracing the IoT involves connecting a relatively small number of devices to the internet – often nothing more than hand-held computing devices. But, in an industrial context, it can mean connecting hundreds or even thousands of complex components.
The industrial cyber-attacks that have gained notoriety in the media have involved programmable logic controllers (PLCs) – such as the infamous Stuxnet incident which targeted Siemens PLCs. But in a modern IIoT environment, it's more than just controllers that are connected.

Anything, from variable speed drives, to cutting machines, to static stations, to 3D printers, to the simplest of sensors, can be online and communicating with other devices. And that means that all of these devices should be protected from security threat.

Added to that, with many IIoT solutions, manufacturers have to consider the issues raised by the SaaS (Software as a Service) offerings in the IIoT space. The benefits of SaaS are clear – customers have professionally designed, economically priced, scalable, and easy to use software that is kept constantly up to date. But SaaS usually involves applications and data storage/analytics happening at off-site cloud data centers – and managing this safely does require a holistic, well thought out cyber-security policy.
IIoT systems have three areas of notable vulnerability related to cloud computing: local area networks, cloud gateways, and the processing/ storage of data in the cloud.

1. Local area networks (LANs) connect up all the components and machines in an IIoT-enabled factory. LANs collect and process data locally as far as possible before passing it to the cloud. It is at the LAN level where ultimately – if the proper cyber-security measures are not taken – a malicious actor can cause equipment damage.

2. Cloud gateways are the point at which data is collected and transmitted to the cloud. This is a place of particular vulnerability, where a lack of security can allow systems to be easily compromised. Cloud gateways with advanced cyber-security protection, such as our own PlatraineEdge software, can easily eliminate this threat.

3. The processing and storage of data in the cloud is not necessarily insecure. But it is a big step for many companies as they must relinquish on-site data storage – which they can control – and entrust it to a third party. The misconception is that, when cloud providers come under cyber-attack, they will be more vulnerable than on-site servers. This worry is overblown (see "Myth busting" below). An additional issue – recently highlighted by the National Security Agency in the USA – is "misconfigurations"[1], meaning self-inflicted human error from poorly trained or negligent staff.

[1] Sussman (2020), 'Top 4 types of security vulnerabilitiein the cloud' in SecureWorld. Portland Or.: Securo Group. Available at: https://www.secureworldexpo.com/industry-news/4-types-cloud-security-vulnerability-mitigation

Myth busting – is cloud-storage less secure than on-site storage? (Hint:no)

It's clear that cyber-security poses a threat. What is less clear is whether using cloud storage as part of an IIoT system is necessarily a big part of this risk factor. At Plataine, we understand that discrete manufacturers have particular concerns about off-site, cloud-based information collection and storage. Yet, unless on-site servers are totally isolated from the external internet (a highly unlikely prospect), then there is little reason to believe they are any more secure than cloud storage. In fact, in many cases, on-site servers are less secure than their cloud-based counterparts.

> ***"In many cases, on-site servers are less secure than their cloud-based counterparts."***

This may sound counterintuitive but consider this: the back-end technology behind most cloud storage solutions is, in almost all cases, provided and managed by one of a very small number of global tech firms such as Google Cloud, Microsoft Azure or Amazon Web Services. These companies employ large and specialist cyber-security teams – with skill sets well beyond the reach of most manufacturing companies. Ultimately, it comes down to reputation. Cloud providers' reputations are staked on data security. If they are seen to allow a major data breach, they'll lose all their business overnight. Furthermore, today almost all business types – even the most sensitive ones – are already using and put their trust in cloud-based systems with their highly sensitive data. Take Salesforce for example, which holds and handles a critical business data of their clients, and the same hold true for banking and financial systems. The point is, that this is where the world is going and in order to avoid lagging behind, you must find the right way for you to embrace that too.

The characteristics of a strong cloud IIoT solution

The best and most secured cloud based IIoT solutions have 10 key characteristics:

- ## Multi-tenant architecture

A multi-tenant solution allows multiple customers to use the same software and runtime environment. Multi-tenancy is a core benefit of SaaS because it reduces costs by sharing core infrastructure, yet at the same time is highly configurable to the needs of individual customers. Total data security is guaranteed because all files are stored in industry-leading protected environments (such as a dedicated AWS S3 bucket). Meanwhile, IIoT providers are able to efficiently offer ongoing updates, in a way that would be impossible for completely bespoke software.

- ## Communication on secured channels

All API communication should be conducted over a secured HTTPS channel, which uses an encryption protocol to encrypt standard HTTP communications.

- ## Authentication & authorization

Secure authentication and authorization procedures mean more than just having a username and password. Industry leading IIoT systems hold multiple levels of information about individual users so that they can enforce tight rules on access at the individual level.

"Secure authentication and authorization procedures are much more than just having a username and password."

- ## Password cryptographic hashing

The most secure way to store passwords is to use cryptographic hashing, which means the passwords themselves are not stored – instead, only the password's digest is stored. Therefore, even if the database which contains the digests is broken into, the data is useless.

- ## Separate accounts for production and development personnel

Different levels of user access ensure IIoT system users can only access the data they need to perform their own specific roles.

- ## Data encryption

IIoT solutions rely on encryption for security because data and applications are stored in the cloud – outside company firewalls. According to recent research[2], most companies prefer to manage their own security keys, ensuring only they control access to their cloud-based information. The best IIoT solution providers always invest heavily in the latest encryption technology.

- ## Most accessibility restricted to a VPN

Highly secure IIoT systems restrict entrance for APIs to a single API gateway. All other components can be restricted so that access is only possible via virtual private network (VPN) – creating a totally secure channel between the user and the cloud.

- ## SSH connectivity

Secure shell (SSH) technology can be used to allow a secure connection over unsecured networks through use of a shared agreement between two computers on how to communicate. This means that, if required, an individual's access can easily be blocked.

- ## Virtual private clouds

Many cloud infrastructure providers, such as Amazon Web Services, offer a virtual private cloud (VPC): a secure, isolated section of cloud dedicated to a single organization, but hosted within a public cloud.

- ## Using security groups to restrict internal communication

A security group is a "virtual firewall" which controls incoming and outgoing traffic in order to restrict access between system components.

[2] Cracknell et al (2019), 'Securing software as a service'. New York: McKinsey.
Available at: https://www.mckinsey.com/business-functions/risk/our-insights/securing-software-as-a-service

Conclusion: You can't do this on your own

Choosing the right IIoT partner

Most discrete manufacturers focus on their core business of manufacturing, and not on IT capabilities. Yet most up to date IIoT solutions in a discrete manufacturing setting will involve moving large amounts of data at high speed. Furthermore, this is a fast-moving sector and the technology is evolving rapidly. So, it's not enough just to bring in an IIoT system and forget about it. It needs to be constantly maintained[3]. Many manufacturers don't have the time or inclination to develop the necessary IT and IIoT capabilities in house, so finding an appropriate external IIoT partner is often the most efficient and cost-effective way to ensure you have access to the top-level cyber-security expertise that will mean you can sleep well at night.

> ***"Finding an appropriate external IIoT partner is often the most efficient and cost-effective way to ensure you have access to the top-level cyber-security expertise that will mean you can sleep well at night."***

[3] Lall (2019), Select the best IoT platform: 6 criteria. Rockville, Maryland: IoT for all. Available at:https://www.iotforall.com/6-criteria-selecting-best-iot-platform-partner/

The question is what to look for in an IIoT partner?
Manufacturers are adopting Industrial IIoT for the competitive advantages and security it can provide. The market-leaders have been at it for some time; the laggards will soon be forced into it by competitive pressures.

So, it stands to reason that most companies will be considering the immediate, quantifiable efficiency or economic benefits that prospective IIoT partners can bring to their factory. Yet cyber-security is equally important – arguably more so – for discrete manufacturers, because the consequences of part of a production line going down in a large factory can be serious.

So, consider the credentials of any prospective IIoT solution provider carefully:
Do they specialize in Industrial IoT or are they a generalist IoT company?
Generalist IoT companies may not take security seriously enough for your needs: things can be more lax in consumer IoT where the consequences of a breach are often far less severe
Look for a proven track record and a strong case history – have they worked with big names in discrete manufacturing, and did this lead to quantifiable improvements?
Find out about their cyber-security set-up. Do they have a dedicated security team? What are their processes for keeping their capabilities up to date?
Are they ISO 27001 certificated? Do they constantly work to maintain the highest quality standards?

Time to take the next step

At Plataine, we provide IIoT solutions to some of the world's largest OEMs, Tier 1 & 2 discrete manufacturers, including General Electric, Siemens, Airbus and Renault F1 manufacturing team.

To learn more about how we can drive your factory's efficiency – bringing you the benefits of the 4th industrial revolution – continue the conversation directly with one of our Digital Transformation Specialists here.