Security for industrial devices

Five key questions about industrial cybersecurity, as IT and OT rapidly converge.

Christian Bergdahl, Leif Malmberg and Joakim Wiberg

www.hms-networks.com

Security for industrial devices

Introdcution

Cybersecurity is a critical issue not only for internet banking and general IT infrastructure. As IT and OT converge, general factory floor automation and many industrial applications need to be prepared for both today´s and tomorrow's cybersecurity threats. Where things are going and what security measures will be needed are the big questions. And often the magnitude of the potential threats is hard, if not impossible, to estimate due to the simple fact that the threat landscape is constantly evolving.

> "A security breach in an industrial or infrastructure system can lead to so much more than just financial loss

Comparing industrial applications and systems to more commercial ones presents quite different pictures and completely different outcome scenarios. A security breach in an industrial or infrastructure system can lead to so much more than just financial loss – since a more physical picture comes into play. Imagine for example a malfunction in industrial equipment like a robot, or an infrastructure system like a dam or water supply system failing. This could seriously hurt or even kill people, and on a very large scale even threaten a nation.

In an ever-developing world, more and more applications are exposed to a larger group of threat vectors, which need to be handled securely. Here we outline the current situation and discuss several key questions that are worth considering right now.

MANUFACTURING INDUSTRIES TODAY are undergoing a significant digital transformation as Information Technology (IT) and Operational Technology (OT) communication systems rapidly converge, thanks to smart industrial automation devices that are designed to provide more useful information than ever before – in many cases through use of networks like OPC UA and MQTT transferring data to IT domains, combined with existing industrial Ethernet networks, that in their turn also evolves, adding features and TSN capabilities. This means that a much larger range of data is being made available and collected from the factory floor, across local enterprise IT functions, on-site storage, and into the external cloud – to give companies new competitive advantages.

The IT/OT convergence, encompassing aspects of Industry 4.0 and the Industrial Internet of Things (IIoT), allows new interconnected communication which helps factory OT equipment create greater value out of data shared with local IT applications or via a manufacturer's IoT Platforms. This cross-shared data can offer many benefits in terms of enhanced levels of production, quality and profits. It will also provide industrial processes with much better possibilities to enable predictive maintenance and analysis.

Security for industrial devices

Cybersecurity needs your attention

At the same time, however, these advances make industrial communication networks and manufacturing processes vulnerable to intrusion and attacks. Although large-scale IT hacking cases like Stuxnet and the Ukraine power grid cyberattack a number of years ago are more famous, attacks and intrusions are happening at industrial plants at an increasing rate. Quite recently, in February 2020, several paper mills in Canada were shut down by computer hackers, creating chaos and making headlines around the world.

To improve security, IT security requirements for industrial communication standards and development processes must now be carefully considered – to make sure that they are protected, today and tomorrow.

Thought Leadership from HMS, to help build your cybersecurity roadmap

In this paper, we wish to present HMS's views on factory floor network security and to discuss some basic aspects that you may want to consider in helping you achieve a state of safety. It is important to note that this is a very dynamic field and it may therefore be somewhat difficult to predict exactly how, when and to what level these issues will develop. We do, however, want to stimulate the discussion on these subjects of growing importance and get the market thinking about logical solutions in the rapidly evolving area of cybersecurity in industrial plants.

We will also follow this up by demonstrating our take on how to solve many of the challenges at hand.

HMS has over 30 years of experience in the field of industrial communication, giving us an excellent foundation and valuable insight from which to start. Using this as a base, we have in recent years committed significant R&D resources to map the security landscape and start implementing solutions within our products. Although it will clearly be a long journey, we have now made several of the important first steps – and the progress so far has even gained the attention of several major industrial automation device manufacturers.

At this point, via this paper we feel it is worthwhile to begin sharing some of our key knowledge and learnings about these issues with manufacturers of devices/products intended for, or sold to industrial plants, system integrators, and also end users. We believe this can be helpful in creating your own roadmap for cybersecurity in industrial communication networks. We are using a Q&A format for some crucial questions, and we are of course also very happy to talk with you directly about these topics as well.

Security for industrial devices

1 How widely will the factory floor of the future be connected to higher level systems?

Extracting information from devices, machines and production lines, and passing it on to other IT systems, is a process that has been going on for quite a while. A common way of achieving this is to only use selected points of entry at certain places in a plant/factory. However, the trend and evolution is clearly going in a direction where these will open up more and more.

Without question, some factories or installations will continue to be tightly closed. But considering the advantages interconnectivity can bring – and driven by initiatives like Industry 4.0 – the market is striving to connect industrial machines to the IT level to enhance maintenance, analysis and production effectiveness.

This likely means that a fast-growing number of industrial machines will no longer be completely isolated from the outside world. Going forward, a factory needs to consider opening selected entry points on different levels. There will most certainly be a transition period as this opening up occurs; what remains to be seen is how fast and how extensive it will be.

> “The market is striving to connect industrial machines to the IT level to enhance maintenance, analysis and production effectiveness.

2 Aren’t today’s factories closed systems, meaning outside access is denied?

Not necessarily, but it depends on how we define “closed”. If there is absolutely no connection to the internet, then yes it has a higher protection from external threats. However, a factory owner needs to consider security on different levels. For example, even if it is closed to the internet, people allowed inside the factory can make security “mistakes” that need to be considered. Examples might be:

1. An external maintenance person, from your supplier, connects their laptop to your machine for diagnostic purposes. Via this connection you are exposed to unnecessary risks and threats – such as viruses or access to internal confidential documents and data
2. A PC being connected to an unused network port on an industrial Ethernet network, where only the machine communication is allowed.
3. Incorrect firmware being downloaded to a machine.
4. An employee making unintentional configuration changes, through tools, web or other environments not requiring authentication.
5. Someone, either an inside employee or outside contractor, bringing a non-secure USB memory stick containing a virus into a factory. Upon connecting to an internal computer or port, the virus itself enables its installation.

There are most likely numerous other examples, and this is just a shortlist illustrating some threats. The consequences though, if any of them would occur, can vary widely from downtime and system failure to risk of viruses/malware getting into your system, causing unpredicted behavior, huge loss of money, quality issues and even potential harm of people.

On the other hand, the increasing complexity of production machines is already pushing the local team to often interact with their suppliers through remote access solutions that, if not fully secured and managed, create additional entry points to the factory. This trend will clearly continue and accelerate.

Security for industrial devices

3 Who will be responsible that an installation is secure?

Everyone will eventually have to consider security aspects in both new as well as old installations, and then build systems in different levels by segmenting various parts of a factory to create a higher security level. We will also need to accommodate co-existence with older products/ installations using older networks. In addition to the question stated in the headline, another interesting question is: **Can device manufacturers rely on someone else's technology to solve the actual security part?**

Yes, it is our belief that in many cases this will be possible, and even preferred. And when industrial manufacturers are required by their customers and end users to do this, the use of communication solutions that include built-in security features will help them do it more easily and efficiently. Thus, a manufacturer of automation equipment can meet their customers' installation requirements related to security, but without the headaches and investments needed to do it by themselves.

It is worth pointing out that security is not only meant to prevent someone from outside the factory getting access to the network. It can also be intended to protect the network, and the products on this network, inside the factory.

4 Do I need to secure all my products, or can I only secure the ones considered to be at risk? And how do I know which products those are?

This will be the key question for the people specifying a new factory or installation containing industrial network communication. The level of security will probably be decided based on numerous factors. This could be the value of the product being made, the value of the information and processes inside the factory, the consequences of a security breach (eg. a nuclear plant), the level of restricted access inside the factory (who can get close to the machines), IT/ internet network connections, and type of data on the network, to give some examples.

> "It is important to note the difference between the meaning of a 'secure' product and a 'security' product

As mentioned above, it is not totally clear at this point how and at what speed IT security in industrial communication networks will develop in the future, and what routes will be taken to achieve it. However, we do know that HMS is in an ideal position to help start to make things clearer. We are actively using our deep network communication experience to undertake numerous progressive steps that will assure that our communication solutions, and the users' automation devices and systems, will be secure as IT and OT converge further in the future.

In this context, it is important to note the difference between the meaning of a 'secure' product and a 'security' product. A Secure product is any type of product, e.g. an I/O block, a proximity sensor, or a PLC – that has been developed with security in mind, and therefore certain security methods and counter measures have been implemented to add a certain level of protection for the product's intended usage.

A Security product, on the other hand, is product developed with the sole purpose of addressing specific cybersecurity functionality, e.g. a firewall, a DPI gateway, or data diode. Naturally, those products are also secure products. Those kinds of products have been developed in order to differentiate themselves on the market and to make their customers' jobs easier when they need to implement specific security measures.

Security for industrial devices

5 Is it the device manufacturer's responsibility to solve the security requirements in a factory?

The quick answer is no, it is not the device maker's sole responsibility to solve security. But, if you want to sell your devices in an international marketplace with a wide variation of use cases, you will have to meet the protection requirements of an installation, using security protocols and functions built into your product.

A secure infrastructure is based on in-depth security, which itself is built on several lines of defense – going down to the component level. But, as a manufacturer, you have no control over the specific security policies within a factory. Therefore, by strengthening the device to handle any situation helps to provide more reliable security performance regardless of the installation conditions.

Security also depends on acceptance by users that have already a strong focus on security management. For example, if a factory demands that its webpages shall be accessible on the network, only products with HTTPS (secure web protocol) can be accepted. This, in turn, means the manufacturer/device maker needs to support this secure functionality in their product, or otherwise risk losing the order and future business.

> "A secure infrastructure is based on [...] several lines of defense – going down to the component level.

Security for industrial devices

Even though the route is not entirely clear, the journey has certainly begun and is in full motion

At HMS, we are committed to being in the forefront within the security area, just as we always have been within the industrial communication space. We will make sure to do what it takes to ensure that our solutions are continuously future proof – both from a connectivity standpoint, but also from a security perspective. For any company aiming to work within industrial communication in the future, security is a requirement – not an option.

HMS is active in a number of domains when it comes to security, where we intend to display our capabilities on a deeper level. That includes items such as active participation in the development of major open industrial networks, an ongoing certification process for HMS capabilities of designing secure products (IEC62443), as well as the launch of new products including both OPC UA and MQTT capabilities together with the necessary security features.

About the authors

Christian Bergdahl
is Product Marketing Manager at HMS's Business Unit Anybus in Halmstad, Sweden. He has 20+ years of experience in industrial communication from both technical and commercial positions.

Joakim Wiberg
is Group Manager Technology & Platforms at HMS's Business Unit Anybus in Halmstad, Sweden. He is also CTO of ODVA and a frequent lecturer on security and Industrial communication.

Leif Malmberg
is Product Owner for Anybus embedded products at HMS's Business Unit Anybus in Halmstad, Sweden. He has been working with industrial communication and industrial networking since the 1990s.