The need for Cybersecurity in Industrial Applications

Cybersecurity is a critical issue not only for Information Technology infrastructure but also for Operation Technology and Embedded Systems

Whitepaper

Christian Bergdahl, Leif Malmberg, Joakim Wilberg,
Thierry Bieber and Kurt van Buul

www.hms-networks.com

The need for Cybersecurity in Industrial Applications

About the Authors

Christian Bergdahl is Product Marketing Manager at HMS Networks 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 Networks 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 Networks Business Unit Anybus in Halmstad, Sweden. He has been working with industrial communication and industrial networking since the 1990s.

Thierry Bieber is Industry Segment Manager at HMS Networks Market Unit Central Europe. He has a specific focus on the industrial automation market - understanding requirements from customers and the market and to support them in adapting our value proposition to their current and future challenges

Kurt van Buul is OEM Project manager at HMS Networks Market Unit North. He is responsible for embedded and OEM projects in the Benelux region and has over 30 years involvement in embedded industrial networks.

The need for Cybersecurity in Industrial Applications

Contents

The need for Cybersecurity in Industrial Applications

1.0 Introduction

Cybersecurity is a critical issue not only for financial operations and businesses in general with Information Technology (IT) infrastructure, but also for Operation Technology (OT).

The first IT viruses were developed in the early 1970s and in those days were spread via Floppy Disks and (later) USB sticks. They were originally created by programmers to show off their skills and used to gain reputation within their social groups. With the expansion of the Internet, viruses shifted towards cyber threads. The malware tools of today are developed, sold (malware-as-a-service) and used by criminal organisations specialising in direct theft of information or data, blackmail, data hostage and other criminal cyber acts.

Meanwhile, OT was quite an innocent environment where PLCs, controllers and nodes simply worked together for a certain task and where the term security pointed to ‘secure operation and safety’ only. This changed drastically in 2010 with the discovery of the virus Stuxnet. This was a complex worm, active on PLCs to send false commands to connected slaves and at the same reporting false feedback to indicate normal operation. Suddenly it became clear that OT could be at risk too!

Traditionally, OT was an “air-gapped” environment, meaning that it was not connected to external networks or other IT infrastructure. With the growth of the Industrial Internet of Thing (IIoT) or “Industry 4.0” the gap has been closed, and OT networks are widely connected to IT systems and to the cloud. 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 are in place will need to become important questions.

Though IT Incidents are much more frequent, OT Incidents are more destructive. IT incidents often cause loss of data, information or value, unfortunately involving increasing amounts and consequences for victims, but they are recoverable. 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. The power outages in Ukraine (December 2016), and failed attempts to adjust chemical levels in the water systems in Israel (June 2020) or Florida (February 2021) make clear what the threat towards larger groups, populations or even nations could be.

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.

Bridging the gap technology wise, doesn’t imply the gap has been closed from an organisation or human point of view. OT has fundamentally different functionality compared to general IT systems because it controls physical processes rather than controlling the flow of information. While everyone is now aware of IT, the Internet and smartphones, OT is still generally only known by specialists involved in their industrial applications. Historically, the focus is different; while IT prioritizes confidentiality, OT focuses on safety.

When IT security engineers, most often the specialists with final responsibility for complete systems, look to OT they see an unknown world as some black box. The components used are often screenless (machinery, PLCs), they communicate over industrial protocols never seen on IT networks (e.g., PROFINET, Ethernet/IP, EtherCAT), they lack security tools (firewalls, antivirus), are rarely patched, and they are even programmed or maintained differently.

On the other side, OT is not aware that they have become part of an IT environment. They see protocols like MQTT or OPC UA as simply connectors to some server location and are not directly aware that they have opened their infrastructure to the world.

2.0 The growth of IIoT

The Internet of Things has become popular among consumers due to the new futures it makes possible. Suddenly a doorbell can be answered from any smartphone, the thermostat can be controlled when driving home, and smart speakers can order anything you want.

The start of IIoT or Industry 4.0 began much slower due to the initial lack of proper business cases. The technology was available but industrial customers were not willing to pay the additional costs. But slowly, mainly as a result of the success of cloud-based enterprise applications, IIoT started to take off too.

Some examples:

A refuse collector is already used to over-the-air route administration and guidance of their trucks on the road. They now want to add the physical weight and volume they collect from a customer to predict when the truck has to return to base.

A beer brewery group already has dashboards showing the production volume, production up-time and other ERP-based key-performance indexes. They now want to add production quality items like the clarity of beer, CO2 and alcohol content.

A machine builder already has remote access to their installed machines, they now want to add sensor information to predict wear and schedule predictive maintenance during production downtime.

In all of these examples the businesses drove the solution.

Although those examples show the potential of IIoT, that doesn't make it a commonly used technology yet. It raises the question; *how widely will individual machines or the complete 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 need to 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.

The likely outcome of this is 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.

3.0 Need for (self) regulation

Due to some security incidents as described before, initial steps toward regulation have been taken in most countries, focusing on protecting critical infrastructure applications. This security is mainly applied to the protection of critical information - like user information - and production aspects are currently mainly protected by disconnecting them from the external world.

Nevertheless, with the push of new environmental or resource optimization requirements, these production units are being forced more and more to become interconnected. At HMS Networks we are starting to see demands for solutions like IIoT or edge gateways for end devices like energy meters where security is the key requirement.

Other regulation has been initiated by the California IoT Security Law forcing all manufacturers of devices that connect directly or indirectly to the internet to implement a basic set of security measures – such as no default password. This law may have some impact on the consumer market, but we have seen limited impact on industrial devices.

Because government measures take time and often depend on a political priority schedule, general regulations will still be delayed. This means that demands for better security must be pushed for and will come from larger end customers or will be driven by innovative manufacturers who pursue security as a competitive advantage. Suppliers in the chain must prepare for this.

4.0 Cybersecurity needs your attention

To improve IT security requirements for industrial communication standards and development, processes must be carefully considered now to make sure that they are protected, today and in the future. 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 feel it is worthwhile to begin by sharing some key facts we have learned about these issues with manufacturers of devices and products intended for, or sold to, industrial plants, system integrators, and also end users.

We believe this will be helpful to you in creating your own roadmap for cybersecurity in industrial communication networks. For this part 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.

4.1 - 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, a system 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:

- An external maintenance person from your supplier connects their laptop to your machine for diagnostic purposes. Via this connection you are exposed to risks and threats – such as viruses or access to internal confidential documents and data.
- A PC being connected to an unused network port on an industrial Ethernet network, where only machine communication is allowed.
- Incorrect firmware being downloaded to a machine.
- An employee making unintentional configuration changes, through tools, web or other environments not requiring authentication.
- Someone, either an 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 short list illustrating some threats. The consequences though, if any of them would occur, can vary widely from downtime and system failure to risk of viruses or malware getting into your system, causing unpredicted behavior, huge loss of revenue, quality issues and even potential harm to people. On the other hand, the increasing complexity of production machines is already pushing the local team to frequently 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.

4.2 - Who will be responsible for the security of an installation?

Everyone will eventually have to consider security aspects in both new and old installations, and then build systems at 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 or installations using older networks. In addition to the question asked, 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 to 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 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 protect the network, and the products on this network, inside the factory.

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

This will be the key question for a team 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 (consider a nuclear plant vs a chair factory), the level of restricted access inside the factory (who can get close to the machines), IT and Internet network connections, and type of data on the network, to give some examples.

As mentioned previously, 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 Networks 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 our customers' 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. 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 a 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. These types of product have been developed in order to differentiate themselves on the market and to make their users' jobs easier when they need to implement specific security measures.

4.4 - 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 manufacturer'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 security in-depth, which is itself built on several lines of defence, going down to the component level. But, as a manufacturer, you have no control over the specific security policies within a factory. Therefore, strengthening a 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 already have a strong focus on security management. For example, a factory demands that its webpages shall be accessible on the network, but only products with HTTPS (secure web protocol) can be accepted. This, in turn, means the device manufacturer needs to support this secure functionality in their product, or otherwise risk losing the order and future business.

5.0 Security Standardisation

As suggested before, while there is no legislation in place (yet), the best way to achieve security is to commit towards international standards. The standardization aspect of the cybersecurity is a bit more advanced with some established standards like ISO27001 and IEC 62443.

ISO27001 is a standard focusing on protecting the IT management systems. It is a mature standard, driven and accepted by IT people, proven in use with highly available technology like TLS encryption, VPN connectivity, X.509 Certificates and so on. In industrial applications, this standard is mainly relevant for those systems connected to IT-environments like IIoT and cloud-based communications, where information exchange is key and where IT security is the common standard required.

IEC 62443 is an emerging standard for industrial control applications – focusing on the robustness and security of a manufacturing application where the determinism of the communication is key for the reliability.

Security for industrial control is a new concept in a market impacting the control loop of applications where dedicated industrial communication protocols like PROFINET are used. These would require additional security mechanisms and currently there is no strong security culture or processes.

The emphasis is on the total application, according to the “defence in depth” philosophy. This includes the coordinated use of security measures to ensure the integrity of information assets in a network. This is done systematically, based on a clear separation of networks into main functions with a subdivision into zones and local functions. Safeguards are installed around and between these network segments. All of this is continuously monitored and adjusted where necessary.

Secondly, the IEC 62443 standard includes so-called security levels. The specification defines a set of requirements designed to classify system security into four levels based on the strength and motivation of criminals to attack a system. These four levels have the following definitions:

SL1 - Coincidental event

This level covers coincidental incidents and accidental circumstances as a result of individual or unintentional failures. An external maintenance person, for example, connects an infected laptop to a machine for diagnostic purposes and infects the customer’s network.

The need for Cybersecurity in Industrial Applications

SL2 - Cybercrime

This concerns a single hacker who intervenes with the help of general means and knowledge, often aimed at a coincidental target. For example, a 'script kiddie' (unskilled hacker) is using software to scan server ports and finds an open port in some system of some company.

SL3 - Hacker Groups / Terrorists

From this level and above, attacks are highly motivated and targeted. At this level, a group of criminals deliberately selects the target, has planned and prepared for the attack and tries to strike with advanced tools. For example, a group targets a company to ransom their systems. They plan access to the company's IT/OT-systems by sending specific phishing mails, starting - after success - to access and analyse systems step-by-step and finally attack.

SL4 - Nations / States

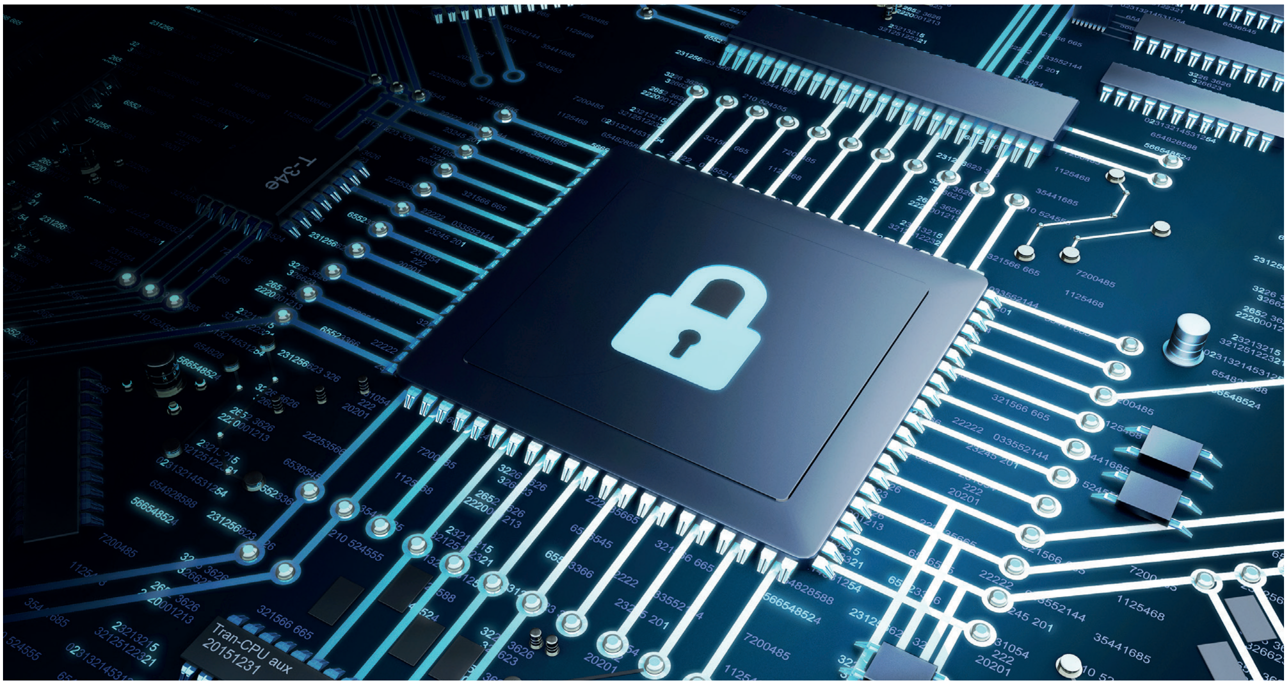
Finally, attacks can be launched by states. With a select group of specialists with the right competences, a very specific attack is launched with the most advanced tools, aimed at a very specific target and with a defined desired result. There are a lot of rumours about certain attacks, but almost no clear examples. However, Stuxnet is generally regarded as a cyber weapon developed by one nation's intelligence agency to attack a secret program of another nation.

Although security therefore has a holistic character, embedding countermeasures for a combination of people, processes, systems and components, it's still important to note that these individual parts of the security chain each play their own individual role to contribute to the security effort.

HMS Networks - as an independent market leader in industrial communication solutions and IIoT - focuses on an important link in the whole. As of October 2020, HMS Networks is certified according to the standard IEC 62443-4-1: 2018. The certification process was performed by TÜV Rheinland to validate a safe life-cycle process for product development within industrial automation and control systems.

6.0 Embedded applications

Security in an embedded application has its own challenges. After all, security affects the entire life cycle of the product, starting with definition, followed by design, development, testing and the production environment. But at the same time, the security of the product is somewhat dynamic, requiring devices already installed in the field to be kept up to date during operation. So, security must be viewed in the longer term and it affects the whole life-cycle management of the product.



An additional challenge is related to the scope of the security implementation within the device. As shown, IEC 62443 sets security levels from 1 to 4, depending on the size and motivation of cyber criminals regarding a specific application. The required level thus defines the robustness that an industrial device must have and thus also the security measures that must be implemented.

The challenge is that these security levels are quite diverse in practice and are highly application and user specific. Thus, device manufacturers must strike the right balance between the level of security and the implementation complexity / average cost.

For complete protection in accordance with IEC 62443, the following requirements would apply to the device itself:

Secure boot: A security chain verifies and guarantees the authenticity of the individual elements, from hardware to firmware to configuration, where each element is individually signed. Certificates are used for this authentication and for secure communication these must be managed and delivered to the device. User and role management is also needed.

All confidential information on the device, such as the private keys, must be protected from any possible extraction, supported by a secure storage of these keys. The communication interfaces to the outside must also be set up securely.

Certificates are a major component in secure communication. They are used to identify the owner of the certificate as a trusted partner in communication. A node will trust a certificate (and therefore the owner) if it trusts the Certificate Authority (CA) that has issued the certificate.

A device should have sufficient resources to withstand attacks, as well as the additional processing capacity required by the security mechanism. All possible but unused interfaces must be closed, such as ports, JTAG-interfaces and so on.

In summary, by closing the gap between IT and OT, OT is increasingly becoming part of a system chain that can be hacked. Industrial environments will have to be fully secured for this. This security includes all people, processes, systems and components involved.

Manufacturers looking to integrate secure industrial and IIoT communication capabilities into their products face many challenges. These industrial security technologies are still young, diversified technologies for any industrial protocol and many aspects remain to be defined. Controlling the development of secure products is linked to important competencies and processes that must be established. This means a longer learning curve, a longer time-to-market and therefore significant investment.

Several options are available to meet these challenges. Modularization of the communication interface helps to separate the specific communication and security aspects from the core functionalities of the device - where the customer has their expertise. It creates the possibility to use existing and proven communication solutions that already integrate the expected functionalities.

The risk and time to market for execution can thus be significantly reduced to focus on what really matters - the functionality of your device - and quickly creates a learning curve better related to the market and expectations from the customer.

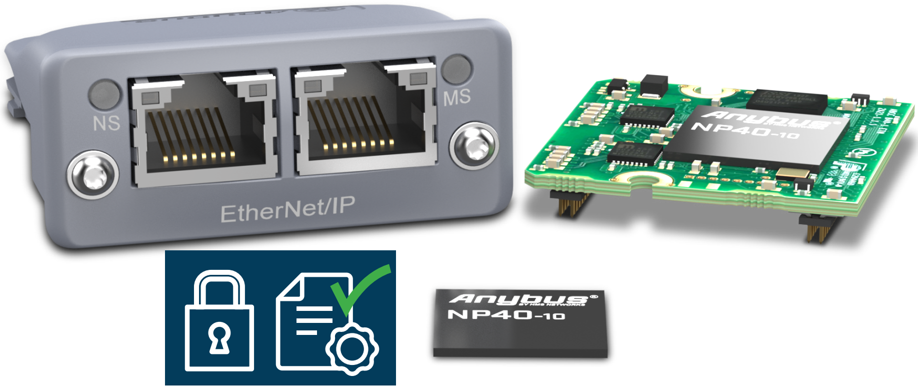
And in this choice, it is also relevant to consider a long-term relationship with a partner to ensure security throughout the product lifecycle.

7.0 Anybus CompactCom IIoT Secure

As a solid company and leading communications provider, HMS Networks has been heavily involved in all aspects of cybersecurity for many years. To support our customers on this path, our Anybus IIoT & Secure module is a ready to use interface incorporating the industrial communication technologies for fieldbuses and also the support of the new IIoT communication standards. HMS Networks is the first company to release a complete and ready-made embedded security product that enables fully secure communication from devices in the field to the cloud.

The solution is called CompactCom IIoT Secure and features powerful new security hardware, secure boot, certificate management and encryption, as well as secure OPC UA and MQTT communication. The first release focuses on CompactCom for Ethernet/IP and PROFINET IRT with OPC UA and MQTT connectivity and includes the following main new software and hardware elements.

The module incorporates both high-level security hardware features - such as secure boot, certificate management, security chip and more - and securely runs the different communications protocols. This means that almost no specific knowledge, programming or production processes are required from our customers.



It provides encryption of data sent to the cloud using secure OPC UA channels or encrypted traffic via MQTT over the transport layer system. Secure boot functionality ensures the use of HMS Networks firmware only. Authentication through advanced certificate management and secure access and file transfer over TLS using HTTPS and WebDAV adds further layers of security.

The module integration is based on our standard Anybus API. For our existing customers who want to migrate to this new version, no changes are required to bring their application up to higher security standards.

At HMS Networks, we are committed to being at the forefront within the security arena, just as we always have been within the industrial communication space. We will make certain 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.

The need for Cybersecurity in Industrial Applications

HMS Networks is active in several 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 the HMS Networks 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.

The solution is future proof, meaning the hardware and the investment of HMS Networks in future security requirements will help you to create a strong differentiation in the market with low invest.

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

Work with HMS Networks.
The number one choice for
industrial communication
and IIoT.

Anybus® BY HMS NETWORKS

Ewon® BY HMS NETWORKS

Intesis™ BY HMS NETWORKS

Ixxat® BY HMS NETWORKS

hms-networks.com