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

Joakim Wiberg, Leif Malmberg,
Thierry Bieber and Kurt van Buul
© 2020 HMS Industrial Networks AB. All rights reserved.
www.hms-networks.com

The need for Cybersecurity in Industrial Applications

About the Authors

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.

All rights reserved.

The need for Cybersecurity in Industrial Applications

Contents

1.0	**Introduction**	**3 - 4**
2.0	**The growth of IIoT**	**4 - 5**
3.0	**Need for (self) regulation**	**5**
4.0	**Cybersecurity needs your attention**	**6 - 9**
4.1	Aren't today's factories closed systems, meaning outside access is denied?	6 - 7
4.2	Who will be responsible for the security of an installation?	7
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?	8
4.4	Is the device manufacturer's responsibility to solve the security requirements in a factory?	8 - 9
5.0	**Security standardisation**	**9 - 10**
6.0	**Embedded applications**	**11 - 12**
7.0	**Anybus CompactCom IIoT Secure**	**13 - 14**

All rights reserved.

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.

All rights reserved.

The need for Cybersecurity in Industrial Applications

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.

All rights reserved.

The need for Cybersecurity in Industrial Applications

Pages 4-14 are not included in this sample. If you would like to read the full whitepaper, please fill out our form at the QR code below:

Link to whitepaper: hms-networks.com/technologies/iot-security/whitepaper-security-for-industrial-devices?

All rights reserved.

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