STORMSHIELD

IT-OT NETWORKS

WHY CONVERGENCE IS DELICATE, YET CRUCIAL

Khobeib Benboubaker
Responsable de la Business Line Industrie, Stormshield

Emerging industries of the future are turning convergence between industrial networks (OTs) and information networks (IT) into a hot topic in the world of industry. This phenomenon highlights the specific characteristics of this infrastructure and reveals certain risks, particularly with regard to cybersecurity.

Predictive maintenance, goods and services that precisely satisfy consumer demand: there are a proliferation of promises offered by this Industry 4.0, related to information and industrial networks. However, the task of reconciling these two very different types of infrastructure is more complex than it seems.

"*The industry of the future brings the extra dimension of data, collected by machines or from users. With the convergence of IT/OT networks, this data can be used to reduce maintenance time, predict failures and reduce environmental costs,*" explains Stéphane Prévost, Product Marketing Manager at Stormshield.

TWO-SPEED DEVELOPMENT OF IT AND OT INFRASTRUCTURE

For a number of years now, industry has watched as the boundaries between IT and OT start to blur. Computer technology, which is updated at regular intervals on control workstations in workshops, rubs shoulders with a pool of machines offering greatly increased lifespans and amortisation periods. Much like the USB/RS232 converter enabling a machine speaking one language (USB for a PC) to be understood by a different one (RS232 for an industrial machine), **the challenge for OT teams was to find a way of reconciling these worlds with their different development priorities.** "*Industrial tools have their own pace and methodology for making connections between the various active components of the network: the fieldbus. This was created during the second Industrial Revolution, and made mass production methods possible. It then survived the third industrial revolution, which ushered in the age of automation... but its relationship with the information age is rather more complicated,*"Stéphane points out. Indeed, with the advent of the Internet, commands for the industrial protocols that are now ubiquitous in workshops and consoles are now conveyed via TCP/IP.

INFORMATION NETWORKS AND INDUSTRIAL NETWORKS: DIAMETRICALLY OPPOSED DESIGN CONCEPTS

The fundamental differences in how IT and OT networks are secured originate in how they are each designed.

The purpose of information networks is to transport large quantities of data. As they were created in an open environment, interaction lies at the heart of how they operate, and secure versions of their protocols are available. Conversely, industrial networks are intended to transfer commands **to ensure industrial processes are managed correctly.** As they are generally designed independently from one workshop to another, these networks have not been specifically secured, having been deemed to be isolated and thus already protected by the respective security policies of the factories that house them.

"*From the outset, information technology has made use of secure data protocols (https for web browsing, SMTPS for email exchanges, etc.), whereas for operational networks, security has been implemented at industrial site level: there seemed to be no advantage to adding a protection layer to networks developed in a confined, secure environment,*"adds Stéphane.

INDUSTRIAL NETWORKS: SINGULAR MANAGEMENT

Until recently, industries had no need to centralise the management of their OT infrastructure: these networks, operating independently of one another and having little exposure from a cybersecurity perspective, "*just somehow worked*" thanks to the ingenuity of the on-site teams!

As convergence gains speed, the risk increases, leading to greater awareness. Many industrial companies are implementing governance systems to provide a better overview of their networks. This is especially important as every industrial network is unique. "*The bespoke nature of industrial networks makes it more complex to implement a shared security policy,*" continues Stéphane.

Lastly, the main challenge regarding convergence of IT and OT networks is a human one: how can information and operational teams learn to understand one another and adapt to the other's constraints? Dialogue between IT teams, with their experience in cybersecurity, and OT teams, with their specialist skills in their own industrial network, is the real key to better security of the overall infrastructure.

Together, they can take responsibility for better identifying and analysing risks, and for facilitating the implementation of a comprehensive IT/OT security policy.

STORMSHIELD

Stormshield, a wholly-owned subsidiary of Airbus CyberSecurity, offers innovative, end-to-end security solutions for the protection of IT networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

www.stormshield.com