CYBERSECURITY NOW ENCOMPASSES A COMPLETE PROCESS, AS SEEN AT PANASONIC INDUSTRY

‘IF YOU LEAVE THE DOOR OPEN, SECURITY IS USELESS’

No industrial company can ignore cybersecurity anymore. The Cyber Resilience Act (CRA), which comes into force this autumn requires companies to strengthen the cybersecurity of connected devices and software within the EU. At Panasonic Industry focus on security is therefore necessary especially as more and more companies move further into the Industrial Internet of Things (IIoT). In that digital network, how do customers securely make every connection? ‘People in every company need to be trained for it.’

BY JAN BROEKS

Asked about the future of the industrial production environment, Thomas Rottler does not have to think for long. Indeed, if there is something it is increasingly about, it can be summed up in one word: connectivity. ‘Data goes via machine and PLC to the cloud. And there, in the cloud, a lot of things are going on. Features are constantly increasing; the number of AI applications is growing extremely fast. How to interpret all that data efficiently? Everything hinges on the right connections.’

Bin Zhou, who, like Rottler, works at Panasonic Industry's European headquarters in southern Germany, concurs with his colleague. ‘The fear of storing production data in the cloud has all but disappeared. More and more companies are taking the next step, by now wanting to analyse that collected data.’

CONNECTED TO THE CLOUD

Zhou works at Panasonic Industry as an embedded software developer, Rottler is a system developer. To say that their field of work is changing rapidly is an understatement.

- **‘Data goes through the machine and PLC to the cloud. And there, in that cloud, all sorts of things happen.’**
- **‘The fear of storing production data in the cloud has all but disappeared.’**
- **‘You simply have to conform to the rules, for which you must make agreements with both your customer and cloud provider.’**
- **‘It is up to the customer to secure the entire machine.’**

At the European headquarters of Panasonic Industry in Southern Germany, Thomas Rottler and Bin Zhou notice how quickly their field of work is changing. 'With the demand for more data analysis, the need for further data collection also grows.' Photo: Panasonic Industry

According to Zhou, just take the pace at which more and more devices and machines are becoming remotely controllable. ‘Companies want to connect them directly to the cloud, and with the demand for more data analysis, the need for further data collection is also growing.’

All these developments have their impact on the Industrial Internet of Things (IIoT), in which systems and machines are connected online and exchange production data among themselves. This creates the basis for monitoring and analysis, for predictive maintenance, for example. There is, therefore, no shortage of potential, Rottler believes. ‘At the same time, a term like IIoT is very broad and open to multiple interpretations. Customers want their data, but which exactly should it be and what infrastructure is needed for that? That view is usually lacking.’

DON'T JUST STORE DATA

For Rottler and Zhou to help companies get started with it; to explain to them how to transfer and collect data, and what are the critical points besides the benefits as well. After all, to what extent is a move into IIoT cost-effective? Zhou: ‘If you know what data you are going to send, then you also know how much data you need to store. That knowledge is crucial, because too much data storage is of no use to you. In that respect, IIoT is also a cost consideration.’

Furthermore, apart from the information the data provides: how do you store it securely? Good management of cloud solutions is indispensable, notes Rottler, not to mention the production floor. ‘Behind cloud services are big vendors which provide automatic security updates, but also consider, for example, that PLC in your own production environment. Only with timely updates do you exclude security risks as much as possible.’

AREA OF TENSION BETWEEN OT AND IT

Precisely the latter is challenging, continues Rottler. 'The hardware within OT (operational technology, ed.) lasts much longer than the latest software update on the IT side. And that distance between the two sides is getting bigger and bigger; more and more changes are taking place in terms of IT technology during a PLC's, say, 20-year lifespan.' It is up to Panasonic Industry to respond to this, with the FP-I4C, for example. The controller provides an update of a machine’s communication environment, forming a bridge between OT and IT (see box ‘Developed within Europe’). Still, Zhou stresses, the FP-I4C is middleware – and not a final product. ‘It is up to the customer to secure the entire machine.’

CRA MAKES IMPORTANCE ALL THE GREATER

So, you see the importance of having the right mindset for cybersecurity. ‘People in every company need to be trained for it,’ says Rottler. ‘They need to know the rules of cybersecurity, know what potentially the problem is and how to solve it. How do you store data securely, but also: for how long? You now must conform to the rules, for which you must make the right agreements with both your customer and cloud provider. Cybersecurity now requires a complete process, and with the Cyber Resilience Act, its importance is only increasing.’

Security is also high on the agenda within Panasonic Industry, according to Rottler. ‘That already starts with product development. We are also trained for this, so that once the product is on the market, it meets the required standards and regulations. We also support companies with a security guide in several languages. Think of that document as a checklist, for passwords, connections and firewalls, among other things.’ So, the customer is supported through multiple avenues, Zhou explains. ‘But ultimately, a company itself must strengthen the knowledge of, for instance, developers and programmers. You can secure a device as well as you can, but if you leave the door open and give everyone access, that security is useless.’

‘ONLY WITH TIMELY UPDATES DO YOU ELIMINATE SECURITY RISKS AS MUCH AS POSSIBLE’

- **www.industry.panasonic.eu**

DEVELOPED WITHIN EUROPE

Panasonic Industry provides products and services worldwide, headquartered in Japan. Much of its new proprietary hardware comes from there, but not the FP-I4C. It was developed by the group in Europe, which, according to embedded software developer Bin Zhou, is a very conscious choice. ‘If we need specific functionality, we can decide within our European division whether to implement it. That shortens the time-to-market and makes us much more flexible, also to customise the product if necessary.’ The FP-I4C works with protocols such as MQTT and OPC UA, provides access to the IIoT and, according to Zhou, includes security by design, which means that necessary updates will be made available in a timely manner. ‘Also, the controller offers an open platform and integration with cloud services such as Amazon Web Services, Microsoft Azure and Google Cloud. So, the product works plug-and-play; the connectivity has been tested by us.’