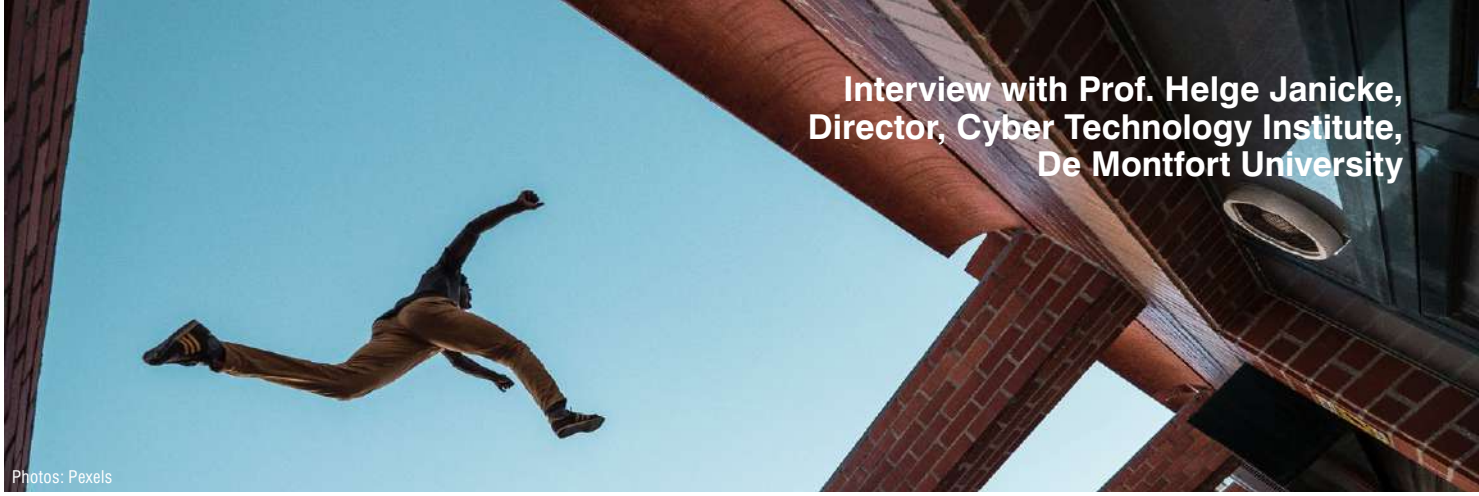

Photos: Pexels

Interview with Prof. Helge Janicke, Director, Cyber Technology Institute, De Montfort University

The need to create a culture of agile incident response in Industrial Control Systems

by **Alice Clochet**, *Content Manager, Defence IQ*

With the digitisation of networks comes the risk for Industrial Control Systems (ICS) to be cyber attacked, creating the need for all stakeholders involved to take measures and avoid any damages made on their business. Ahead of Defence IQ's ICS Cyber Security conference taking place 29 April-1 May in London, Professor Helge Janicke, Director of the Cyber Technology Institute at De Montfort University, shares his insights on agile incident response in ICS. He discusses here risk management of Supervisory Control and Data Acquisition (SCADA) systems, the effectiveness of the current ICS instant response capability, and what the key elements are to secure the digitised network connected to ICS.

ICS CYBER SECURITY

Preparing your industrial control systems for the new phase of cyber security. As the most established Industrial Control Systems (ICS) Cyber Security Event in Europe, the ICS cyber security conference brings together leading practitioners, operators, and decision makers from across Europe to share a wealth of practical experience in implementing cyber security in organisations, and best practice on defending against cyber security risk to ICS. Attend the event to understand how leading organisations are operating in the post-NIS implementation phase (the EU directive on security of network and information systems), assessing new threats to IP and data theft, and maintaining an effective secure network against cyber threats. Use the event to understand how industries are engaging with cyber risk internally and externally, and expanding their cyber security capabilities against the total cyber threatscape. For more info, please visit www.defenceiq.com/events-icscybersecurity

■ **SCADA systems are widely used by a vast array of organisations from sectors such as energy, oil and gas, power, transportation, etc. How can they best manage the risks associated with a digitised real-time data analysing system and thus avoid any malicious intrusion?**

This question is a little complex. Obviously, SCADA systems are widely deployed in almost our entire critical national infrastructure (CNI). How you best manage the risk is a very good question because we are all collectively still trying to find the answer to it.

One of the key starting points is making sure that we are actively looking at the risks because traditionally these infrastructures were disconnected from the network, and nowadays they are popping up everywhere. They are connected to business systems through the regular IT side of an enterprise, for purposes such as real-time monitoring, monitoring throughput, power production and logistics – logistics systems today are deeply integrated into the control systems that underpin them.

In terms of risk management, understanding what the links are and

having architect solutions that pay attention to cyber risk is crucial, especially when we build new installations. Segregating the data flows in there is also important, to make sure that not a single component is accessible from everywhere, and used by an attacker to pivot through the system. I think controlled flows and the use of data diodes for example, to ensure that the flow of information is unidirectional to some parts of the system through that network, are very good practices to manage and deal with some of the risks.

However, many of the risks come from widely different fronts. If you look at the supply chain surrounding the building of these SCADA systems, you can find there are a lot of suppliers working in concert in a production plant. This creates issues because the integration of all of these at the interface level might not go as smoothly as it should.

Any system is only as secure as its weakest link, so there is a reliance on the security of your supply chain. If we look at the European NIS directive (on the security of network and information systems), it is important for operators of essential services to focus on their supply chain because they have, at least in the UK, the responsibility to ensure that adequate protection of their supply chain is being implemented and that suppliers are applying the same rigorous levels of security and risk management.

■ **Operators of essential services are responsible for making sure their suppliers are secure, but are they currently doing this? Are they aware of their need to do this?**

That depends on the sector you are talking about, as some sectors are significantly better in managing their supply chains than others. In the energy sector, there is a detailed logging of the supply chain, what is being used and what is being implemented; aircraft manufacturers have a very detailed trace of where the parts come from and when there were manufactured.

■ **On a range of one to ten, how would you rate the current ICS instant response capability?**

Again, this depends a lot on the sector. The more critical the sector is, the higher the number would be; the broad stroke, however, is possibly somewhere around two or three on this scale.

There is a lot of work to do, especially when it comes to small manufacturing plants that have sometimes zero cyber security and no awareness of cyber security. Machines can be 20 years old and in this type of setting there is very little response capability on the cyber part, even though they are effective in the incident response mechanisms on the safety part. I believe that the operation technology (OT) side needs a lot of development; we come much further with IT incident response, where the issues are much better understood than in the operations technology side.

■ **Is there a push from CNI organisations to work with industry in order to build agility in incident management solutions? If not, where does the push to become more agile come from?**

This question links very nicely to the current project we are running, about agile incident response and industrial control systems. So far the push really comes from the realisation that incident response is taking place quite often in isolation of A) the business, and B) the ICS context, with the engineers and the operators of these technologies. You often find that the security operations centre and the incident response management teams are IT-focused and do not understand or cannot operate OT.

While there are things that these stakeholders can afford to lose, others are absolutely critical and must be maintained. Bringing teams together to know which ones are which and to share this knowledge is particularly relevant in case of a response to an incident, as it will enable them to make the right decision quickly in a stressful situation; it is less relevant in the preparation and post-incident phases, as it is all about limiting damages. The real trick in ICS is not to make matters worse when responding to an incident.

■ **What do you believe to be key in securing the digitised network connected to ICS? What about in ensuring an effective incident response?**

The key in securing the digitised network is the attitude towards ICS because often these are built for a single purpose and a production line is being set up for them. Currently, we find it very difficult to patch ICS; we can patch them, but the process invalidates some of the safety certification that these plants have undergone, so this is a big additional cost that we don't manage effectively at this point. Changing a software configuration in the digitised network might invalidate the safety case established in a plant. Making any changes requires a complete recertification of the plant and there are very few people who can do that. That loss of regularity is financially not viable to run, so we need to look at some different ways to maintain and secure the systems that have the benefits of being connected, but not falling foul of the operating nature of these control systems.

I very strongly believe that an effective incident response is only possible if you understand your systems and know what assets you have deployed, what configurations are running, what kind of patch levels have already been applied throughout the system, to be effective in managing it; it is not necessarily the case in all incidents at the moment.

Moreover, you need to have the right stakeholders on board and the management buy-in, to deal with an incident effectively and quickly move and respond. You also need to get access to the right people such as engineers and business people, and bring them together in a value-focused approach to responding to an incident. I believe this is the key for the future.

■ **Do you believe there is enough management buy-in now, in order to achieve this?**

Currently, there is significant awareness among managers that cyber security is an issue and the question is to make it an internal business case. To a large extent and in the finance sector for example, because it is too expensive to proactively put controls into place, people just accept the risks associated with having less controls. There are some protections, but there is also the ability for them to pay up for any mistakes that are happening. The key element here is to have management buy-in to change the organisational culture effectively, all the way down to the employees who are operating these systems. This can happen through rigorous security awareness programmes and putting the right architectural solutions and infrastructure in place when the plants are built or refurbished; this will help to anticipate incidents and be able to segregate attacked networks or production lines, to avoid the spread of an attack.