TÜVRheinland®
Risktec

RISKworld / The Newsletter of Risktec Solutions / Autumn 2018 p4-5

# Cyber-security meets functional safety

The cyber-threat to industrial control systems is very real, as demonstrated by high profile attacks in recent years. That said, many defensive measures put in place to assure functional safety will also protect against cyber-attacks. But is that enough? What else needs to be done?

The control systems that operate physical processes in an industrial plant work within a so-called Operating Technology (OT) environment. OT systems' priorities are reliability, availability and maintainability. Whilst corrupted data in standard Information Technology (IT) systems can be disruptive to a business, it is not life threatening. However, when transmitted to thousands of sensors in an industrial plant, for example, it can cause major business interruption and, potentially, a major accident with a catastrophic impact on people, assets, environment and reputation.

Stuxnet, Industroyer and Triton are just a few examples of malware attacks in recent years on digital systems that control critical infrastructure (see below). Other plausible cyber-threats include the possibility of gaining unauthorised control of systems remotely or locally, or seeding systems with unauthorised data (via USB ports for example). With the frequency of cyber-attacks growing rapidly, clearly industry needs to focus on protecting automation and control systems against what must be assumed to be an inevitable attack.

### EFFECTIVE CYBER-SECURITY

Effective cyber-security for OT systems is delivered by a blend of:

- Cyber-security defensive measures covering the system lifecycle, from design to operations and the subsequent decommissioning of the systems and individual components.
- Cyber-risk assessments of the systems to establish any additional security measures required to protect them from cyber-threats (e.g. following security standard IEC 62443 or NIST 800-82).
- The integration of cyber-security alongside physical and procedural

### STUXNET

In January 2010, Stuxnet became the first discovered malware known to spy on and subvert industrial control systems. Stuxnet targets SCADA and PLC systems and is believed to be responsible for causing substantial damage to Iran's nuclear programme by causing the fast-spinning centrifuges at the Natanz uranium enrichment facility to tear themselves apart. Although unconfirmed, the worm is believed to be a jointly built American/Israeli cyber-weapon. Stuxnet was uploaded by an infected USB flash drive.

### INDUSTROYER

One fifth of Ukraine's capital, Kiev, lost electrical power for one hour in December 2016, the result of an attack by the Industroyer malware, specifically designed to disrupt the working processes of industrial control systems used in electrical substations. A similar attack had been experienced precisely one year earlier.

### TRITON

In December 2017, the safety systems of an unidentified power station, believed to be in Saudi Arabia, were compromised when the industrial safety technology was targeted by Triton malware. This exploited a vulnerability in computers running the Microsoft Windows operating system and is believed to have been a state-sponsored attack. The plant shut down and no harm was done.

security measures within the context of overall security.
- Cyber-security vulnerability assessment and penetration testing of the installed systems.

## ALIGNMENT WITH FUNCTIONAL SAFETY

The development of functional safety requirements and their delivery are well-established and both generic (IEC 61508) and industry-specific (e.g. IEC 61511 for process industry and IEC 61513 for nuclear industry). These standards address the software, hardware and management aspects associated with a system's lifecycle, all of which are potentially vulnerable to a cyber-attack.

As it turns out, defensive cyber-security measures are often closely aligned with measures introduced during the project lifecycle to deliver functional safety. Where true, this alignment presents an opportunity for cyber-security assessment to take credit for safety measures that are necessarily put in place to deliver functional safety in existing systems, since many of the means of achieving systematic safety integrity are similar to those required to defend software, hardware and procedures from cyber-attack. Resources can then focus on plugging any cyber-security holes.

## INTEGRATING CYBER-SECURITY AND FUNCTIONAL SAFETY

However, to deliver a truly cost-effective control system, which is optimised for both cyber-security and functional safety, requires an integrated approach. The earlier the integration of cyber-security and functional safety, the greater the benefits that can be reaped.

For effective integration, the vulnerability to a cyber-attack needs to be considered during each phase of the functional safety lifecycle. Ideally, safety hazard and cyber-threat identification would occur at the same time, so that optioneering can consider solutions that eliminate or reduce the risks from both sources.

Achieving adequate cyber-security could include ruling out remote terminals and data ports, relocating equipment to a manned central control room, avoiding programmable systems in remote areas and introducing air gaps where data transfer requirements are minimal, especially between control and protection systems. Other provisions include limiting access both physically and by password protection. Importantly, considering such options at an early stage not only reduces downstream time, trouble and cost, but it also allows decisions to be weighed equally against the needs of operational effectiveness and functional safety.

The outcome would be an integrated set of functional requirements that embrace both safety and cyber-security requirements, and ultimately a compliant design and effective supporting management system.

This approach is not without its pitfalls, however. Take the setting of Safety Integrity Levels (SIL) as an example. SIL targets for safety systems quantify the level of safety integrity required for each safety function in order to meet overall risk targets. Four levels are designated in IEC 61508 with SIL4 denoting the highest integrity requirement. These are very precisely defined. The corresponding Security Levels (SL) in IEC 62443 are much more subjective, both in terms of their selection and definition, which reflects the subjective nature of the threat. As such, the early integration of cyber-security and functional safety requires a pragmatic approach as well as holistic security thinking, since over-specifying SL targets to meet a hypothetical cyber-threat could potentially lead to an overly designed and costly solution.

**Contact:** Mel Davies
mel.davies@risktec.tuv.com

## CONCLUSION

The integration of cyber-security, functional safety assessment and design makes sense for delivering cost-effective and optimised industrial automation and control systems, but requires care to avoid over-specifying and over-designing to address a subjective cyber-risk.