Safety meets Security

Common strategy required

The importance of the safety technology installed in machines and systems steadily increases over the entire life cycle of the application. However, as networking of automation systems with the IT world is becoming more and more commonplace, scenarios are likely to arise where a different approach is required, especially for safety applications (lead image).

Lead Image –Figure 1

As production and IT become more and more inextricably linked in the Internet of Things within the framework of the future project Industry 4.0, the security challenges are also growing. The network interfaces between office IT systems and production networks represent a significant gateway for hackers. Examples of threats that industrial control systems are currently facing are:

- Infection with malware via the Internet and Intranet
- Introduction of malware via removable media and external hardware
- Social engineering, i.e. influencing of people in order to bring about certain modes of behaviour
- Human error and sabotage
- Unauthorised access to the system via remote maintenance solutions
- Control components coupled to the Internet via the IP protocol
- Technical errors and force majeure
- Compromising of smartphones in the production environment, as well as extranet and cloud components.

A study by the software company Kaspersky conducted in 2017 revealed that nearly every third cyber attack on computers for industrial control systems was directed against manufacturing companies. Experts fear that the number of malware attacks is set to increase in 2018, with the focus being on industrial systems. The worlds of "Safety" and "Security" meet when automated solutions for implementing functional safety become the target of

hackers. A common strategy must therefore be developed in future. The "Triton" malware in combination with a cyber attack against a so-called "Safety Instrumented System (SIS)" is a current case which demonstrates that this is a far from hypothetical scenario.

Indirect effect on the end product

The aspect of functional safety refers to the safety component of a system that relies on the correct function of the safety-related (control) system and other risk-reducing measures. In this case, the controller performs the task of initiating the safe state when a critical error occurs. The requirements for the quality of safety-relevant control components are described in the B-standard EN ISO 13849 and the IEC series 61508/61511/62061. Depending on the degree of risk, corresponding risk-reducing measures are classified into to different safety levels – Performance Level (PL) or Safety Integrity Level (SIL).

In contrast to functional safety, security protects goods from detrimental impairment as a result of intentional or inadvertent attacks on the availability, integrity and confidentiality of their data. This involves the use of preventative or reactive technical and/or organisational measures. If security aspects in the area of safety are disregarded, this can not only have direct effects on production facilities, it can also indirectly affect the production process and therefore the end product. In the context of pharmaceutical products and safety-relevant components for the automotive industry, it is easy to see how the effects on consumers could be significant. The IEC 61511-1 therefore requires an IT risk assessment to be carried out for safety equipment in the process industry. If operators of PCE (process control engineering) safety equipment perform the IT risk assessment as specified in the attached NAMUR NA worksheets and implement the measures identified, it is likely they will have assessed their PCE safety equipment in accordance with the latest technical standards and will therefore have fulfilled their duty-of-care obligations.

Active search for weak points

When considering the aspects of functional safety and access security the potential risk must initially be considered based on a risk assessment or IT threat analysis. Here, a considerable difference in approaches is already evident: While the risks that design engineers need to consider within the scope of the risk assessment in accordance with the Machinery Directive – mechanical or electrical hazards for example – tend to remain the same, the environment in which IT security experts find themselves is constantly changing. In the latter case,

attackers are always actively looking for ways to exploit vulnerabilities which would be considered systematic errors in the area of functional safety.

Another important aspect to consider is the "human factor": The expression "foreseeable misuse" is used in the field of machine safety, for example, to describe situations where safety equipment – such as door switches – are tampered with by operating personnel. With large-scale cyber attacks on industrial systems, on the other hand, it must be assumed that a high degree of criminal energy is exerted in these cases.

Initial approach in a NAMUR worksheet

To safeguard the product life cycle of safety-oriented systems or components, manufacturers, system integrators and operators are required within the scope of "Functional Safety Management" to adopt an approach to quality management that reflects the requirements of the situation in accordance with IEC 61508. A comparable solution for this exists in the security world in the form of "Information Security Management" in accordance with ISO 27000. Since there is so much common ground, it should now be possible to interlink the two spheres of activity Safety and Security in practice.

The worksheet published by NAMUR entitled "IT risk assessment of PCE safety equipment" adopts an initial pragmatic approach which leads in this direction. It describes an IT risk assessment method which uses the IEC 62443 security standard as its starting point to provide a basis for increasing the capability of the PCE safety equipment of averting IT threats. To this end, the three steps in phase 1 were performed once as an example for one system, which reflects the systems typically found in the NAMUR member companies. This allows the user to gauge the usefulness of the method for the PCE safety equipment to be assessed. The fourth step – monitoring implementation of the measures and documenting the IT security requirements and general conditions – must be carried out individually for all items of PCE safety equipment to be evaluated and constitutes phase II (figure 2).

Figure 2 - The various steps in the risk assessment process in accordance with NAMUR recommendation NA 163

No adverse effects on functional integrity

From the hardware and software perspective, the system being examined can therefore be subdivided into three zones:

- The core PCE safety equipment in zone A comprises the PCE safety equipment as defined in the IEC 61511-1. This includes the logic system, the input and output modules including remote I/O, and also the actuators and sensors. Connections and, if applicable, available network components – for example cables or switches – that are used to interface with devices located in zone A are also allocated to this zone.
- Components that are not necessary for implementation of the safety function but could nonetheless influence the behaviour of the core PCE safety equipment are allocated to the extended PCE safety equipment in zone B. These could be operator/control panels, visualisation stations, the programming unit for the PCE safety equipment, and also devices for sensor/actuator configuration.
- Components and systems that do not belong either directly or indirectly in the same category as the PCE safety equipment but could be linked to the safety function belong in the zone referred to as "environment". This could be reset requirements or the visualisation of the status of the safety function (figure 3).

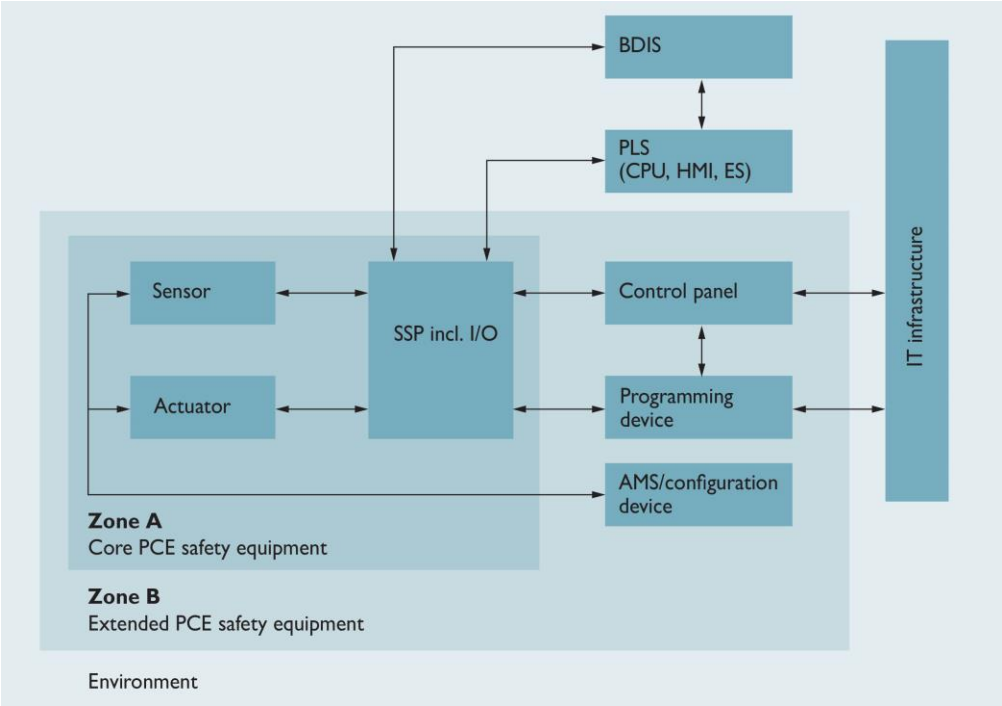

Figure 3 Subdivision of PCE safety equipment into various zones

The common objective of the zones is to ensure that the functional integrity of the safety equipment is not compromised by feedback effects from the environment.

Comprehensive training of relevant personnel

Measures must be taken to reduce the effects of compromised PCE safety equipment or to counteract threats. The "human factor" also plays a significant role in this process. This is highlighted by the fact that the blame for more than 50 percent of cyber security incidents ultimately lies with employees. It is therefore important that there is an IT security officer responsible for the security equipment. In this regard, all persons involved in the specification and design of the safety equipment should be made more aware of the subject of 'Automation Security' and trained accordingly. Furthermore, it is advisable for the end user to conclude confidentiality agreements with his contractual partners – i.e. manufacturers, suppliers and external operators – to safeguard information and knowledge in relation to the safety system.

Figure 4 - Phoenix Contact provides a wide range of services in the security environment

Components, software tools and solutions by Phoenix Contact support users by providing them with a flexible and economic combination of safety and security technology to increase their competitive edge in the international market. This, complemented by a comprehensive range of services, provides system planners and operators with a service portfolio which remains perfectly tailored to their requirements throughout the entire safety lifecycle.

More information:
www.phoenixcontact.de/safetyindercloud
www.phoenixcontact.de/security

If you are interested in publishing this article, please contact Becky Smith: marketing@phoenixcontact.co.uk or telephone 0845 881 2222.

Cloud-based provision of key safety system data

The Proficloud from Phoenix Contact provides companies with important information on optimizing production processes. Safety of machinery also remains a critical issue for plant engineers and machine operators. Although safety applications are in the first instance designed to protect users of the machine, they can also cause unplanned downtimes. The ability to access safety system data via the Internet of Things in real time and to convert this into meaningful information has enormous potential (figure 5).

With Profinet-based control solutions, status information for standard and safety functions is transmitted continuously to the Proficloud. Adopting a holistic approach to resources and machinery gives operators and designers a whole new range of options for increasing operational performance.

Figure 5 The system operator can access the safety system data in real time via the Proficloud