KNOW-HOW IN
SAFETY
by GIT SICHERHEIT &
PHOENIX CONTACT

Focus Topic

Safety meets Security

Carsten Gregorius, Senior Specialist Safety

The importance of the safety technology installed in machines and systems steadily increases over the entire life cycle of the application. 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. The network interfaces between office IT systems and production networks represent a significant gateway for hackers. 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.

Cyber security vs. Functional Safety

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, e.g., a short circuit. 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 different safety levels: Performance Level (PL) or Safety Integrity Level (SIL). In contrast to functional safety, cyber security protects goods from detrimental impairment as a result of intentional or inadvertent attacks on the availability, integrity and confidentiality of the data. This involves the use of preventative, technical, and organizational measures.

Pragmatic Approach in acc. with 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.

The worksheet published by NAMUR (User Association of Automation Technology in Process Industries) entitled "Security Risk Assessment of SIS" (Safety Instrumented Systems) adopts an initial pragmatic approach to interlinking safety and cyber security in process control engineering (PCE). 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, a process was developed in the first phase as a one-off example of processes typically found in the chemical industry. This allows the users to gauge the usefulness of the method for their PCE safety equipment to be assessed. The second phase monitors implementation of the measures and documents the IT security requirements. This step must be carried out individually for all items of PCE safety equipment to be evaluated.

Would you like more detailed knowledge, insider information and infographics on this topic? Then find out more on:

**http://www.phoenixcontact.net/
webcode/#2312**

Author:
Dipl.-Ing. (FH)
C. Gregorius,
Senior Specialist Safety,
Phoenix Contact
Electronics GmbH,
Bad Pyrmont

CONTACT
Phoenix Contact GmbH & Co.KG
Blomberg, Germany
cgregorius@phoenixcontact.com
www.phoenixcontact.com