White paper

Functional safety and IT security in automation: where do we stand?

Authors:

Dr Lutz Jänicke
CTO
Innominate Security Technologies
ljaenicke@innominate.com

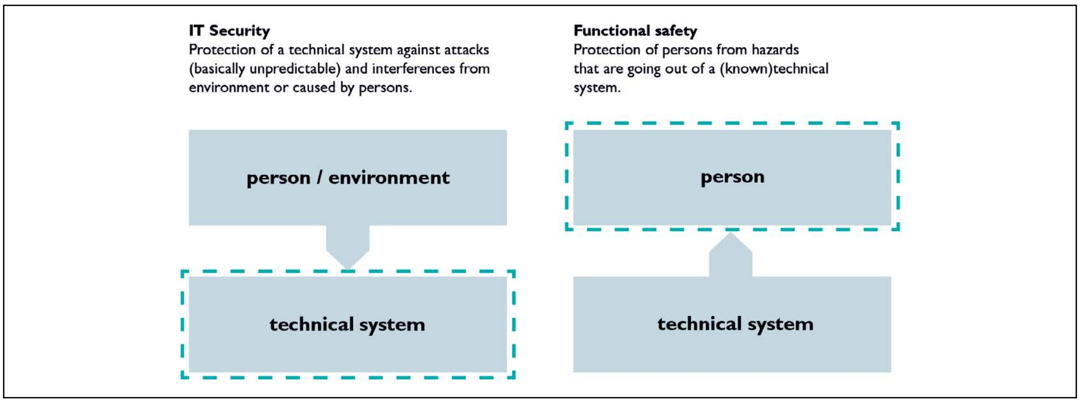
Torsten Gast
Head of Competence Center Safety
Phoenix Contact Electronics
tgast@phoenixcontact.com

Table of contents

Introduction

Safety is a key element of automation. There are two essential aspects to consider: functional safety, which involves protecting people from a technical system, and IT security, which concerns the protection of a technical system.

This document is intended for decision makers in the company and aims to outline the current and future challenges and solutions in a clear and accessible manner.



IT Security
Protection of a technical system against attacks (basically unpredictable) and interferences from environment or caused by persons.
Functional safety
Protection of persons from hazards that are going out of a (known)technical system.
person / environment
technical system
person
technical system

Figure: *IT security vs. functional safety*

While it was possible in the past to consider functional safety and IT security as separate topics, the digitalization and networking of automation systems, also in view of Industrie 4.0, is giving rise to mutual dependencies.

Both topics share a common goal: safety, i.e., the absence of unacceptable risks. The evaluation of risks is therefore a central aspect of all processes that concern safety topics.

Similarities and differences

Although IT security and functional safety share many similarities, they differ in most details. In modern applications, functional safety should usually be considered at a local level, while IT security must take external factors into consideration. The trend towards making functional safety functions and components accessible by means of network communication is also opening up new ways in which these functions can be attacked.

The following scenarios are possible:

- **Direct attacks on safety-related communication:**
  Due to the typical local configuration of safety systems, this usually requires intervention on site.
- **Attacks on safety controllers:**
  The safety controllers are accessible via networks for programming or monitoring purposes.
- **Attacks on programming environments which can be used to configure and parameterize the safety systems:**
  Nowadays these environments usually run on popular office systems that do not undergo special security hardening.

The question of how IT security and functional safety should be considered jointly in this context is currently being discussed internationally by committees.

Functional safety

The protection of people from the dangers posed by machinery is an important objective of state authorities, organizations, and associations. Accordingly, in many countries there are statutory regulations in place which are mandatory for manufacturers and operators of machinery. However, depending on the country, these regulations vary with respect to the extent of the safety requirements and with regard to the target groups involved, i.e., manufacturers, system integrators, automation specialists or operators of machinery. Anyone intending to place machinery on the market in a specific country must therefore first ensure that they are well-informed on the relevant local laws.

In the European Economic Area (EEA), uniform directives exist which must be implemented in unchanged form in the respective countries (e.g., Italy, Austria, Germany). The Machinery Directive is therefore incorporated in the 9th German Product Safety Ordinance. The requirements of the directive are enshrined in the German Product Safety Act and are therefore binding.

The Machinery Directive (1) specifies safety and protection requirements for the manufacture of machinery. The requirements are firmly established in over 700 harmonized standards (see the Official Journal of the European Union at www.europa.eu). An important requirement of the Machinery Directive is that a risk assessment must be carried out for every machine during the design stage. To this end, in addition to the limits of the machinery, all hazards that may occur in the respective phases of life must also be determined and assessed. If the risk factor (severity, probability, and possibility of avoidance) for a hazard is higher than permitted, the manufacturer of the machinery must take appropriate measures to reduce risk. Restrictive measures must be adopted in this case, firstly by means of design measures, then technical measures, and (if the residual risk is still too high) indicative measures.

If technical measures have to be implemented, then these are functional safety measures. The requirements regarding functional safety are incorporated in the harmonized technical standards, e.g., EN ISO 13849-1 (2), EN 62061 (3) or EN 61511 (4). These standards describe the requirement for achieving functional safety for machine building and for process engineering systems. This is then expressed by means of the safety level or the safety integrity level. Depending on the standard, this is then defined as a performance level (EN ISO 13849-1) or SIL (EN 62061). EN 61511, which is supplemented by VDI/VDE 2180 (5), can be applied for process engineering systems.

Finally, the manufacturer of the machinery confirms conformity with the Machinery Directive by providing a declaration of conformity and affixing the CE mark; the machinery can then be placed on the European market. This declaration certifies that all the specifications of the Machinery Directive have been observed and implemented. There are also further directives which must be observed (EMC Directive, ATEX Directive, etc.).

To ensure that the use of machinery complies with directives, there are further requirements which must be met by the operator regarding occupational safety that apply for the respective country. In Germany, this is the German Occupational Health and Safety Act with the requirements implemented in the Ordinance on Industrial Safety and Health.

Manufacturers of safe switching devices, safe components, as well as safe controllers must also meet the requirements of the Machinery Directive (CE mark on the relevant devices). In order to additionally satisfy international requirements, IEC 61508 (6) is applied by many manufacturers. This standard is specifically intended for manufacturers of electrical, electronic, and programmable electronic (E/E/PE) systems that perform a safety function. The standard sets out comprehensive requirements, starting with Functional Safety Management through to calculating the probability of failure for individual components. The standard also includes requirements regarding hardware development as well as those for safe firmware and the software interface.

Manufacturers of safety devices provide their technical documentation, but also proof of safety, in accordance with application standards EN ISO 13849-1, EN 62061 or EN 61511 in order to make it easier for machine or system integrators to use their components and systems in the complete machine. This means that the product in question can be directly included in the proof of safety for the respective safety chain.

IT security

As a rule, the implementation of IT security measures in automation is not regulated by law. While the protection of people and the environment can be derived from fundamental social objectives and thus warrants legal intervention, security measures primarily serve economic objectives and are therefore subject to the economic freedom of commercial decisions. The interests of society are affected if, for example, security of supply is jeopardized and regulation becomes necessary with the aim of ensuring public services. The first step in this direction is the German IT Security Act (7), which sets out requirements for specific industries that are derived from the national strategy for critical infrastructure protection. The protection objectives of availability, integrity, authenticity, and confidentiality must be met for the critical infrastructures in operation. However, these requirements have not yet been implemented in specific, verifiable standards. A corresponding ordinance cited in the Act has not yet been published. It is to be assumed that the ordinance will be aimed at setting up and implementing an information security management system in accordance with ISO 27000 (8). The individual industry associations have the opportunity to propose industry-specific safety standards that represent the state of the art. In this respect, concrete requirements in the field of automation still need to be drawn up. At European level, a corresponding directive on network and information security (9) should be expected in the near future for this topic.

Procedure

Likewise in the field of IT security, the first step in examining the situation is to perform a risk and threat analysis. However in this case, the threats come from people or organizations whose motivation and capabilities make a quantitative assessment much more difficult. The various standards approach this issue by dividing motivation and capabilities into classes. The protection needs that are determined based on this list of criteria therefore leave a lot of room for interpretation.

In the case of functional safety, the standard function and the safety function are often implemented completely separately in order to minimize as far as possible any potential impact of defective standard functions on the integrity of the safety function. This is not possible in the case of IT security, since relevant attacks can also occur at this point. An appropriately sophisticated development process, such as on the basis of Common Criteria, can therefore only be used in very few applications in practice.

Another feature of IT security is the question of how a safe state should be defined in the event of an error. To meet the protection objectives of confidentiality and integrity, it is conceivable that operation should be shut down in the event of an error; however, this immediately causes conflict with the protection objective of availability. Availability is an important protection objective, especially in automation.

The way in which vulnerabilities are handled presents a particular challenge. For all non-trivial systems, it is to be assumed that errors exist in implementations or protocols. Intruders continuously use new methods to actively identify corresponding vulnerabilities which would be considered systematic errors in the field of functional safety. In IT security, it is therefore to be assumed that when a vulnerability comes to light in a system, where this vulnerability has long been present as a systematic error, the system in question will suddenly appear insecure and countermeasures must be taken. IT security is essentially a moving target in this respect and requires constant re-evaluation of the threat level.

It can generally be assumed that the probability of an IT security incident occurring in the various application scenarios is likely to be much higher than the failure of equipment for functional safety. Detection capabilities and responsiveness are therefore included in IT emergency planning as standard.

Office applications and automation

In general, security measures are much more well-established in computer centers and office environments. However, for a variety of reasons, it is difficult to transfer most of these measures to automation. Many of these measures are aimed at human-operated systems where a temporary failure is tolerable. In addition, corresponding systems are under the control of the IT organization and are regularly updated or replaced. Even brief failures are not acceptable in automation. The service life of installations depends on the technical service life of the physical system, which is much longer than the typical innovation cycle of the IT industry. In addition, the operator does not have control over the IT systems in the automation components, but is dependent on the automation provider. The background to this is that the provider must test updates prior to their release to ensure there is no impact on the automation function.

Standards

The ISO 2700x series of standards (8) describes an information security management system which follows the general concepts of a management system such as ISO 9000 for quality management or ISO 31000 for risk management. It is therefore aimed at organizations and processes. Versions exist for specific industries, such as energy supply in accordance with ISO/IEC TR 27019:2013 (10). Details of the technical implementation are then covered in other standards, such as IEC 62351 (11),

Various approaches have emerged in industrial automation technology. In Germany, VDI/VDE 2182 (12) was drafted, which among other aspects describes the coordinated approach between providers, integrators, and operators. At international level, based on US initiative ISA 99, work was started on preparing IEC 62443 (13), which has now reached an advanced stage. IEC 62443 comprises four parts, which in turn are aimed at operators, integrators, and providers. With respect to the operator level, an information security management system will be introduced, which is not coordinated with the ISO 2700x series in current versions, but the transition to ISO 2700x is in progress. For products, IEC 62443 uses Security Levels (SL-1 to SL-4), which together with the maturity of the operator, should provide an assessable Protection Level (PL). However, these aspects are still being discussed. In general, IEC 62443 currently appears to have found great acceptance among those parties involved, from operators to providers.

The recently published NAMUR recommendation NE 153 (14) has a special role to play; its aim is to identify concise and concrete requirements for future automation solutions with particular focus on the process industry, without covering the comprehensive concepts of a standard such as IEC 62443.

The publications of the German Federal Office for Information Security (BSI) (15) (16) also provide a good overview of the topic of security in automation.

The Common Criteria according to ISO/IEC 15408 (17) are specifically aimed at security products. Protection objectives are defined in the methodology of the Common Criteria; compliance with these objectives is validated based on an Evaluation Assurance Level (EAL-1 to EAL-7). The protection objectives complement each other, ensuring that topics are covered in a meaningful way. The necessary Evaluation Assurance Level must be derived from the intruder's capabilities and, depending on the level, ranges from inspecting the user documentation and performing design reviews to demonstrating correctness – if at all possible. It should be noted here that only the combination of protection objectives and the Evaluation Assurance Level, i.e., the protection profile, is significant. Existing protection profiles are aimed at products such as smart cards, health insurance cards, and the German Smart Meter Gateway. Protection profiles exist for firewalls and VPN gateways, but are only used by a small number of products. In general it can be seen that the Common Criteria along with the associated costs and limitations are only used in regulated environments. Another fundamental problem is the degree of inflexibility, as complex and especially time-consuming recertification is necessary in the event of any change to the product, which conflicts with the need to respond quickly to changing security challenges.

Industrie 4.0 requirements

Digitalization and networking open up new possibilities some of which are impossible to predict. However, there is also a growing threat from the point of view of IT security. Increasing the level of security is therefore a fundamental part of the efforts being made in relevant international initiatives, such as the Industrie 4.0 platform. The implementation strategy (18) has a specific section devoted to the topic of security.

Achieving the type of company-wide networking that is desired comes with various challenges:

- In Industrie 4.0, many partners work together in real time: manufacturers and users, suppliers, services providers, and operators. The boundary between the different communication domains of the partners involved becomes blurred, which means that relationships of trust must be built between partners. Data and information is to be exchanged between these partners, which is why common security levels must be agreed. At present, there are still no models to show what assessment procedures for security levels might look like.
- When people and machines from different parties work together, access methods and rights must be coordinated. In order to enable mutual authentication and authorization, the communication partners must use suitable, secure identities. Models are also needed here for company-wide, secure identification and roles.
- Data is exchanged beyond the bounds of a company and beyond national borders. A legal framework is therefore required that addresses the ownership of data, for example. There are also major differences internationally in the statutory regulations governing encrypted communication which is necessary for secure data exchange. The inclusion of German policy is ensured through the Industrie 4.0 platform.
- Intelligent production has made the production-related rapid conversion, retrofitting or adaptation of machinery a necessity. These undertakings must not conflict with functional safety. Systems and models which support this, including with respect to checking functional safety, must be defined and described.

The right partner on the road to Industrie 4.0

For the customer it is important to take a holistic approach to the automation task. From the point of view of the requirements involved, there are certain points at which the topics of functional safety and IT security overlap and it is these points which require customer-specific analysis and implementation in an overall concept. There is then the question of implementation and subsequent checking (verification and validation). In addition, the company's personnel need to be informed, instructed, and trained. Continuous development of expertise is essential, as new requirements and threats are constantly emerging, especially in the field of IT security.

When it comes to implementation, the right partner must possess different competencies in order to fulfill these tasks.

Industry-specific expertise

The specific requirements regarding functional safety and IT security differ depending on the industry. In this respect, long-term experience in the various industries is essential in order to be able to offer suitable products, solutions, and services. Through involvement in industry associations and standardization, state-of-the-art technology can be developed further, simultaneously ensuring the currentness of the portfolio.

Adapted product and solution portfolio

Phoenix Contact's product and solution portfolio consists of numerous specific products for functional safety and IT security. With respect to functional safety, the portfolio ranges from safety relays and configurable safety solutions to central safety controllers. For IT security, the mGuard product range provides state-of-the-art solutions for network security and secure remote maintenance.

Service portfolio

In order to provide customers with the best possible support when implementing their automation projects, a comprehensive portfolio of services that focus on specific topics is necessary:

Training programs provide an ideal introduction to the topics of functional safety and IT security. A tailored consultation is then necessary for the implementation of customer projects.

Phoenix Contact supports its customers in projects by providing specific advice. The range of services offered for functional safety has had a proven track record for many years. The services offered for IT security will be developed further.

Active further development

In the future world of Industrie 4.0, IT security, which was not an area of focus for automation users in the past, will have to be taken into consideration from the outset, essentially through security by design. For implementation, IT security features will have to represent the current state of the art in all processes, products, and solutions in future. Phoenix Contact is already leading the way with this in organizations and committees.

With a partner who not only offers suitable products and solutions, but can also demonstrate a comprehensive portfolio of services, the customer is well equipped to meet objectives for Industrie 4.0.

References

1. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC. Machinery Directive.
2. Safety of machinery – Safety-related parts of control systems. ISO 13849.
3. Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems. IEC 62061.
4. Functional safety – Safety instrumented systems for the process industry sector. IEC 61511.
5. Safeguarding of industrial process plants by means of process control engineering. VDI/VDE 2180.
6. Functional safety of electrical/electronic/programmable electronic safety-related systems. IEC 61508.
7. Legislation to improve the security of information technology systems. German IT Security Act. 2015.
8. Information technology – Security techniques – Information security management systems. ISO/IEC 27000:2014.
9. Network and Information Security Directive (at the consultation stage). NISD.
10. Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. ISO/IEC TR 27019:2013.
11. Information Security for Power System Control Operations. IEC 62351.
12. IT-security for industrial automation. VDI/VDE 2182.
13. Industrial communication networks – Network and system security. IEC 62443.
14. Automation Security 2020 – Design, Implementation and Operation of Industrial Automation Systems. NAMUR NE 153.
15. ICS Security Compendium. Bonn: BSI, 2013.
16. Recommendations for component manufacturers. Bonn: BSI, 2014.
17. Common Criteria for Information Technology Security Evaluation. ISO/IEC 15408.
18. Umsetzungsstrategie Industrie 4.0 (Industrie 4.0 implementation strategy). Berlin/Frankfurt: Industrie 4.0 Platform, 2015.

PHOENIX CONTACT

Phoenix Contact is a global market leader for components, systems, and solutions in the field of electrical engineering, electronics, and automation.

Our extensive manufacturing capability means that it is not just screws and plastic and metal parts that are produced in-house, but also highly automated assembly machines. The product range consists of components and system solutions for energy supply including wind and solar energy, device manufacturing and machine building, as well as control cabinet manufacturing.

With a wide range of terminal blocks and special terminal blocks, PCB terminal blocks and connectors, cable connection technology, and installation accessories, we offer innovative components. Electronic interfaces and power supplies, automation systems based on Ethernet and wireless, safety solutions for people, machines, and data, surge protection systems, as well as software programs and tools provide comprehensive systems for installers and operators of systems as well as device manufacturers.

Markets within the automotive industry, renewable energy, and infrastructure are supported by means of consistent solution concepts, ranging from engineering and maintenance to training services, in line with specific needs. Product innovations and specific solutions for individual customer requirements are created in the development facilities at our sites in Germany, China, and the USA. Numerous patents emphasize the fact that many developments from Phoenix Contact are unique. Working closely with universities and scientific institutes, technologies of the future such as E-Mobility and environmental technologies are researched and transformed into marketable products, systems, and solutions.

PHOENIX CONTACT GmbH & Co. KG
32825 Blomberg, Germany
Phone: + 49 52 35 3-00
Fax: + 49 52 35 3-4 12 00
phoenixcontact.com