Development of functional safety standards for civil engineering

E. Nachtigall
Quantum Brandschutz GmbH, Basel, Switzerland

V. Shcherbina
WASCS Research Center, Moscow, Russia

ABSTRACT

Functional safety, as well as other topics related to safety, usually considered in each industry and also on the level of different standalone systems separately. This approach has developed traditionally, as standards are developed in groups whose interests often coincide and members of the group are often from the same industry.

For instance, developers and committees associated with automatic fire detection systems, usually for several reasons do not consider developments in functional safety approaches described in the IEC 61508 series, arguing that sufficient reliability of systems is completely ensured by their compliance with industry-specific national norms and standards. Thus, each developer of norms and systems manufacturers considering, basically, only their systems without take account adequately the relationship with other safety systems in buildings.

Current standards for safety systems in buildings also do not include a comprehensive approach to safety systems related to their interactions. Therefore a complex and comprehensive approach to functional safety of building safety-related systems is absent.

The aims of the paper are to present why functional safety methods are necessary for development of safety-related systems in civil engineering. Moreover, such methods are to develop in order to manage the increasing complexity of safety-related systems in modern buildings and to fit growing demands of tenants, building owner and other stakeholders. The paper presents recent developments in the Russian Federation and introduces ready to use, GOST R 53195 and interrelated standards, focused on functional safety of safety-related systems in buildings.

The paper shows clear and global trends and needs for safety in civil engineering. Furthermore the need to handle the growing complexity in civil engineering, and the need for new approaches to handle safety and complexity in this area are identified.

With presented and discussed current and interesting developments and ready to use standards a way to deal with growing complexity in civil engineering by implement and use special functional safety developments and standards is shown. First positive experiences of application of presented approaches and standards in modern and complex buildings are available.

The discussed functional safety approach can be understood as the beginning of a new era of functional safety in civil engineering. Furthermore, the conclusion can be drawn that it is necessary to consider systems theory approach in functional safety to address the complexity in modern buildings.

Further development of standards will show whether the functional safety approach can solve the presented challenges of modern civil engineering industry. In addition, the development of standards will show whether they can give a new fresh impetus to the improvement of safety and security in civil engineering.

REFERENCES

[1] J. Börcsök., 2007. Functional Safety - Basic Principles of Safety-related Systems. Hüthig, Heidelberg.

[2] GOST R 53195, 2008 – 2011. Functional safety of building/erection safety-related systems, parts 1-5.

[3] ISO/IEC 14762, 2009. Information technology – Functional safety requirements for Home and Building Electronic Systems (HBES).

[4] IEC 61508, 2010. Functional safety of electrical/electronic/ programmable electronic safety-related systems, all parts.

[5] E. Nachtigall., 2013. Systems Analysis Methods for Consideration of Fire Safety. Science and Safety, 1 (6).

[6] E. Nachtigall., 2013. Functional Safety in Civil Engineering: On the example of the GOST R 53195 Functional safety of building/erection safety- related systems. Standards and Quality.

[7] V. I. Shcherbina, E. I. Puzyrevskaya, M. M. Lubimov, and V. P. Matveev., 2011. Functional safety of the safety-related systems in construction. Technical Report 2126.

Development of functional safety standards for civil engineering

E. Nachtigall
Quantum Brandschutz GmbH, Basel, Switzerland

V. Shcherbina
WASCS Research Center, Moscow, Russia

ABSTRACT: Functional safety, as well as other topics related to safety, usually considered in each industry and also on the level of different standalone systems separately. Thus, each developer considering, basically, only their systems without take account adequately the relationship with other safety systems in buildings. Current standards for safety systems in buildings also do not include a comprehensive approach to safety systems. The aims of the paper are to present why functional safety methods are necessary for development of safety-related systems in civil engineering. Moreover, such methods are to develop in order to manage the increasing complexity of safety-related systems in modern buildings. The paper presents recent developments in the Russian Federation and describes ready to use, GOST R 53195 and interrelated standards focused on functional safety of safety-related systems in buildings.

1 INSTRODUCTION

The approach to standardization of functional safety of systems as properties of those systems to fulfill the safety functions in an environment during an interval of time with the established probability (safety integrity) appeared at the very end of the XX century (Smith & Simpson 2004 and Börcsök 2007). A milestone in this approach was the development of IEC 61508 series for functional safety of the electric/electronic/programmable electronic safety-related systems (IEC 2010). This approach began to develop rapidly.

Now there are about 200 standards in more than 40 sectors of standardization of ISO and IEC in this field e. g. IEC (2000, 2005, 2007, 2008, 2012). The key features of standards are: implementation of an iterative process of the analysis of dangers and risks, the general assessment of risk and taking measures to decrease the risks to an acceptable level (according to ISO/IEC Guide 51 on safety aspects), and also the possibility of ensuring management of risk by repeating regular processes at all stages of the life cycle of systems and their components (Rolle 2013a).

Many procedures of risk management have been implemented in different areas after development of ISO Guide 73, ISO 31000 and ISO 31010 ISO (2009, 2011), Hasofer & et al. (2007). Also the acceptance of risk management methods given in those standards, which are related to standards of functional safety, has increased. In IEC according to Administrative Circular AC/7/2004 and Administrative Circular AC/33/2013 steps for transition from standardization of separate units of production to standardization of systems in which separate units of production (components) are structurally and functionally interconnected to work in the common uniform system for ensuring requirement are taken.

Thus, now there are all prerequisites for standardization and sustainable development of complex sociotechnical systems with use methods and means of risk management for safety.

The international standardization in the construction branch develops more slowly, than in other branches. Perhaps it generated a certain conservatism of thinking because of centuries-old traditions in one of the most ancient and, general successful activity of the people. In civil-engineering branch standards are traditionally developed in groups, whose interests often coincide, and members of the group are often from the same industry.

For example, developers and the technical committees of developing standards of automatic fire alarm systems, as a rule, for several reasons don't consider existing functional safety approaches described in IEC 61508 or other standards, claiming that sufficient reliability of systems is completely ensured with their compliance to national norms and standards of the branch ISO/IEC (2009), Rausand & Hoyland (2004).

Thus, each developer of standards and the producer of systems consider, generally only their systems without adequately taking into account the relation with other safety-related systems in buildings. We know from the general theory of systems, that the properties of system cannot be completely defined by the sum of properties of its components (Ropohl 2012). Therefore there is no possibility to evaluate the level of functional safety or life and fire

safety in the building without considering multiple interconnections of the fire alarm system with other systems, such as a fire extinguishing system, smoke extraction systems, security systems etc. (Nachtigall 2013b).

2 COMPLEX APPROACHTOFUNCTIONAL SAFETY IN CIVIL ENGINEERING

Systematic, comprehensive approach to functional safety, systems safety and security of buildings and structures can be seen in a series of national Russian basic standard GOST R 53195 "Functional safety of building/erection safety-related systems" (Shcherbina, Puzyrevskaya, Lubimov, & Matveev 2011, Nachtigall 2013a). The series consists of seven parts, five of which are already in place, and two additional parts are planned for development. Below the seven interrelated parts of the standard are listed.

- Part 1: General
- Part 2: General requirements
- Part 3: Requirements for systems
- Part 4: Software requirements
- Part 5: Techniques and measures on risk reduction, estimation methods
- Part 6: External resources for risk reduction, monitoring systems
- Part 7: Application requirements, sample calculations

In parts 1 and 2, both first developed in 2008 general definitions and requirements of the standard are given. Parts 3 and 4 define requirements for hard- and software of safety-related systems used in buildings and constructions. In part 5 techniques and measures on risk reduction for those systems are presented. Parts 6 and 7 are in development. The focus of those parts is on methods for risk reduction and monitoring of systems as well as on application requirements and sample calculations.

The basis of GOST R 53195 laid down the basic definitions, philosophy, approaches and methods in accordance to IEC 61508 series, the requirements for quality assurance according to ISO 9000, safety aspects according to ISO Guide/IEC 51 (ISO 1999), with respect to the specificity and demands of civil engineering. During development of GOST R 53195 since the year 2008, current standards as e. g. ISO/IEC 14762 (ISO/IEC 2009) as well as experiences of applications from standards IEC (2000, 2005, 2007, 2008, 2012) were taken into account in the development process.

Standards focus on specifications providing improvements of safety to people and properties. They provide methods for analysis of hazards, risks and quantifying the safety of technical means to ensure the safety of buildings and erection or structures in order to achieve an acceptable level of safety, and provide a systematic approach to the facilities in civil engineering. Technical and safety related subsystems used in facilities of civil engineering are considered as systems of system. Also a holistic view of the entire system is given in Shcherbina, Lubimov, Puzyrevskaya & Matveev (2012).

3 TWO TYPES OF APPROACHES TO SAFETY AND RISK REDUCTION AS APPLICATION OF GOST R 53195

Production as a result of activity differs in industrial and construction branches. In Figure 1 the lifecycle of production of industrial manufacturing is shown.

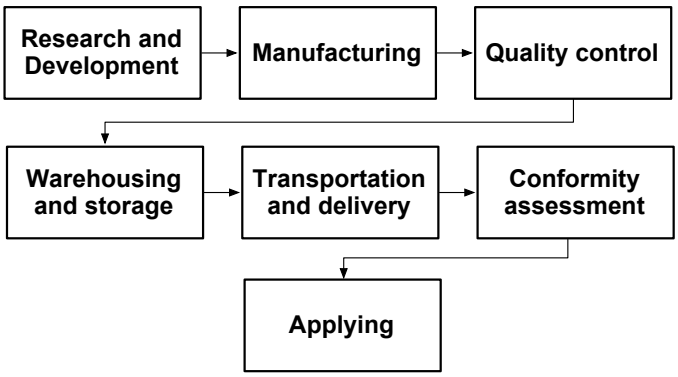

Figure 1. Life cycle of production of industrial manufacturing (after Ryan & Faulconbridge 2014).

Goods of industrial production are usually created in the design office and made at the factory. Those goods can be tested for compliance to be used in any situation and places according to its specifications.

Such goods, usually of mass production, can be stored in a warehouse, transported and delivered to the consumer, including with crossing of customs borders (Meyna & Pauli 2010).

In contrast to the life cycle of goods of industrial production in civil engineering the lifecycle of goods differs. In Figure 2 a simplified lifecycle of production in civil engineering is shown.

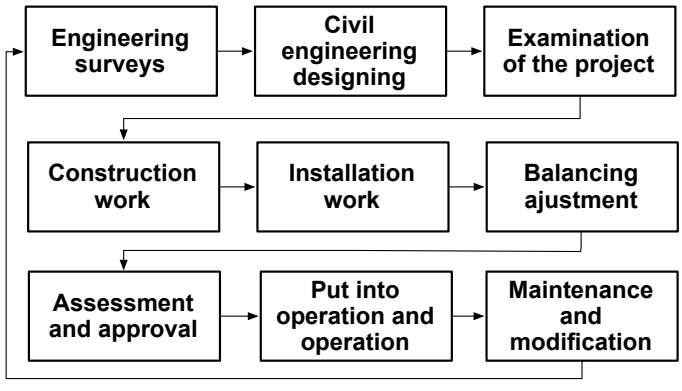

Figure 2. Life cycle of production in civil engineering (compare Mumovic & Santamouris 2009).

Typically, the lifecycle in civil engineering for most stakeholders begins with some engineering surveys followed by the process of design. After the examination of the project the construction work follows. At the end of this phase installation of technical systems is performed. This is followed by phases of adjustment, assessment and approval. Finally phases of put into operation, operation, maintenance and modifications start.

Due to different life cycles in industrial manufacturing and in civil engineering the approach to functional safety and risk reduction should take into account these differences.

In Figure 3 the general approach to decrease risk is shown.

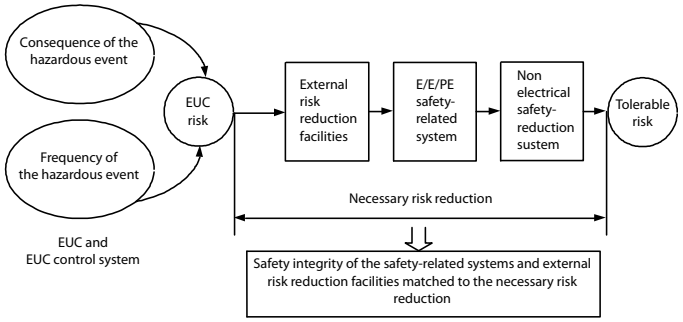

Figure 3. General approach to decrease risk (after DIN 1994, Börcsök 2007).

In general, the risk is the result of a combination of consequence of the hazardous event and the probability of occurrence of these hazardous events. This combination influences the equipment under control risk. If this risk is higher than the tolerable risk, than necessary risk reduction measures are to apply to reach the tolerable risk level. To reach the tolerable risk level external risk reduction measures, the implementation of safety-related systems and the application of non electrical safety reduction systems are to be considered.

With a combination of measures and systems the risk level achieved is usually even lesser than the tolerable risk. In Figure 4 the relationships of risk and safety integrity are shown.

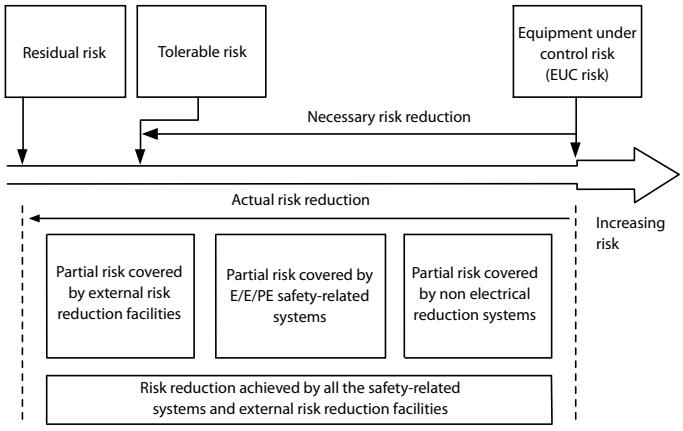

Figure 4. Risk and safety integrity (compare Börcsök 2007).

The actual risk reduction should usually be greater than the necessary. By judicious selection of shown modules the risk reduction achieved by all the safety-related systems and external risk reduction facilities can be optimized especially for the needs of civil engineering.

During the process of evaluation of different risks not only the safety-related systems are to be considered. This is because in modern buildings many very complex and interrelated systems are usually used (Novak 2008). Therefore for different scenarios different initially non-safety or security-related systems can become crucial for safety or security. This results from the complexity of modern high performance systems in civil engineering. To take this into account GOST R 53195 provides methods and show examples of interrelated systems to consider different safety- and security-related scenarios and systems.

First practical applications of standard show positive experiences in modern and complex buildings. It is reported by the practical users that the use of standards real-world problems can be solved. Furthermore, it is reported that using the standards the safety can be significantly improved as a whole. Since the standards are new and still largely unknown, so far the application was limited to large objects that have an outstanding importance for national safety in Russia.

4 FURTHER DEVELOPMENT OF STANDARDIZATION

Along with independent application of the GOST R 53195 this standards created a basis for development of new standards for functional safety for special buildings and constructions.

Within National association of builders of Russia (NOSTROY), which itself is part of 270 self-regulating organizations uniting over 100.000 enterprises of the construction branch of Russia, the STONOSTROY 2.35.73-2012 "Engineering networks of high-rise buildings. Systems of complex safety of high-rise buildings and constructions." was developed and approved (NOSTROY 2014). Both authors of the presented paper are involved in the development and implementation of GOST R 53195 and STONOSTROY 2.35.73-2012 in Russia and abroad. One of the authors is the coordinator of GOST R 53195.

The STONOSTROY 2.35.73-2012 standard is applicable on safety-and security-related and other systems installed in high-rise buildings or constructions. Because of the importance of this type of buildings the engineering networks and other boundary conditions play a very important role to ensure the safety needs.

As features and factors influencing safety especially in high-rise buildings following examples can be listed:

- Difficult infrastructure of the building or construction and high saturation power-intensive engineering systems which may contain large volumes of harmful substances
- Large number vertically and horizontally directed supply channels which can be ways of fire propagation
- Vertical layout and natural updraft of air
- Large number of people in the high-rise building
- Limited possibility of safe evacuation of people from the building in emergency situations
- Lack of the effective technical means, allowing to organize rescue of people from high-rise buildings
- Attractiveness to carry out terrorist acts and actions of a criminal nature
- Possible considerable weight of consequences at realization of events doing harm.

5 PECULIAR PROPERTIES OF NOSTROY 2.35.73-2012

The standard establishes the main requirements to functional safety of safety- and security related systems according to GOST R 53195 and IEC 61508, and also considers the systems interrelated to engineering life support systems. Other engineering systems that are initially non-safety or security-related such as comfort maintenance systems according to the IEC 61511 series are considered, too (IEC 2003).

It contains requirements for functional safety of about 28 types of safety- and security related systems, including complex system of safety. The standard establishes requirements for actions and procedures, which have to be executed in stages of the life cycle of these systems for achievement and maintenance of their functional and complex safety and antiterrorist and ant-criminal security of the high-rise buildings as a whole. The standard enables planning a control center to manage crisis situations and of evacuation of people. It contains requirements to elevators and their controls for safe evacuation of people, including the evacuation during a fire.

In the standard as well as in GOST R 53195 a systemic process approach is used (Meyers 2009, Ropohl 2012). Lifecycle of system or building is a process, which breaks into subprocesses, etc. Each of them has an input (e. g. information, energy or materials), an output (e. g. information, energy or goods) and functionality (actions in transformation of in- to outputs). A process can have some in- and outputs. The outputs of the previous process are used as inputs of the subsequent processes. Processes can also branch and unite.

In the standard besides requirements to systems also requirements for responsible persons influencing safety at each stage of the life cycle of systems, subsystems and complex systems or safety systems, and to their actions for reduction of influence of a subjective factor are established.

On the basis of presented standards similar standards for different types of construction objects in civil-engineering branch can be developed. Currently the possibility of development of standards for safety-related systems for underground objects is discussed in NOSTROY.

6 ADVANTAGES AND DISADVANTAGES OF FUNCTIONAL SAFETY APPROACH IN CIVIL ENGINEERING

As shown in the examples of the development of functional safety in civil engineering in the Russian Federation the role of functional safety approach is becoming more important.

Below some advantages and disadvantages of the approach of functional safety in civil engineering are listed.

Advantages:

- The society's needs for safety and security can be better achieved
- Civil engineering industry can learn from other industries (compare Rolle 2013b)
- Civil engineering industry can adopt and use best practice processes from other industries (e. g. IEC 2003)
- Civil engineering industry can use certified and reliable hardware and software from other industries
- Quality of safety and safety-related systems can be improved in the civil engineering industry
- Achieved safety level can be quantified.

Disadvantages:

- The adoption of standards and processes in the civil engineering industry can take long time
- The adoption of hardware and software can, in some cases, be expensive
- Expertise is necessary
- Certificate processes are to develop.

In spite of the disadvantages the advantages of the shown approach predominate from the point of view of the authors.

7 WORLDWIDE DEVELOPMENT OF FUNCTIONAL SAFETY IN CIVIL ENGINEERING

The importance of functional safety has grown steadily in recent years. This, on the one side, is because no other adequate solution to challenges in areas of safety, security and complexity can be observed. And on the other side for fast growing complexity of safety systems e. g. as for fire protection systems a solution to this problem has to be found rapidly as shown in Nachtigall & Klingsch (2011).

In Germany the standard VDI 6010 Part 4 "Safety Technology-Application of SIL classifications in the technical building equipment" is planned. The development of this standard by the Association of German Engineers begins in 2014 and will build on existing parts of the standard VDI 6010 parts 1-3 (VDI 2005). Also other commissions in Germany e. g. in German Commission for Electrical, Electronic & Information Technologies of DIN and VDE develop new standards in functional safety for the special needs of electrical engineering in the civil engineering industry.

Besides the identified national developments and discussed Russian standards the letter are planned to launch to international standards.

8 CONCLUSIONS

The paper shows clear and global trends and needs for safety in civil engineering. Furthermore the need to handle the growing complexity in civil engineering, and the need for new approaches to handle safety and complexity in this area are identified.

With presented and discussed current and interesting developments and ready to use standards a way to deal with growing complexity in civil engineering by implement and use special functional safety developments and standards is shown. First positive experiences of application of presented approach and standards in modern and complex buildings are available.

The discussed functional safety approach can be understood as the beginning of a new era of functional safety in civil engineering. Furthermore, the conclusion can be drawn that it is necessary to consider systems theory approach in functional safety to address the complexity in modern buildings.

Further development of standards will show whether the functional safety approach can solve the presented challenges of modern civil engineering industry. In addition, the development of standards will show whether they can give a new fresh impetus to the improvement of safety and security in civil engineering.

REFERENCES

Börcsök, J. (2007). Functional Safety evacuation Basic Principles of Safety-related Systems. Heidelberg, Germany: Hüthig.

DIN (1994) DIN V 19250:1994-05 Leittechnik – Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben, Änderung 1:1994-10.

Hasofer, A. M. & et al. (2007). Risk Analysis in Building Fire Safety Engineering. Amsterdam, Netherlands: Elsevier.

IEC (2000). IEC 60204-1 Safety of machinery – Electrical equipement of machines – Part 1: General requirements, Edition 4.1 2000-05.

IEC (2003). IEC 61511 Functional safety – Safety instrumented systems for the process industry sector, All parts.

IEC (2005). IEC 62061 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems, Edition 1.0 2005-01.

IEC (2007). IEC 61131-2 Programmable controllers – Part 2: Equipment requirements and tests, Edition 3.0 2007-07.

IEC (2008) IEC/TS 61000-1-2 Electronic compatibility (EMC) – Part 1+2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena, Edition 2.0 2008-11.

IEC (2010). IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, All parts.

IEC (2012). Programmable controllers – Part 6: Functional safety, Edition 1.0 2012-10.

ISO (1999). ISO Guide 51 Safety aspects – Guidelines for their inclusion in standards.

ISO (2009). ISO Guide 73 Risk management. Vocabulary.

ISO/IEC (2009) ISO/IEC 14762 Information technology – Functional safety requirements for Home and Building Electronic Systems (HBES).

ISO (Entwurf, 2011.). DIN ISO 31000 Risikomanagement. Grundsätze und Leitlinie.

Meyers, R. A. (Ed.) (2009). Encyclopedia of Complexety and Systems Science. Springer.

Meyna, A. & B. Pauli (2010). Zuverlässigkeitstechnik – Quantitative Bewertungsverfahren. Hanser.

Mumovic, D. & M. Santamouris (2009). A Handbook of Sustainable Building Design and Engineering, Earthscan.

Nachtigall, E. (2013a). Functional Safety in Civil Engineering: On the example of the GOST R 53195 Functional safety of building/erection safety-related systems. *Standards and Quality*. *February 2013*

Nachtigall, E. (2013b). Systems Analysis Methods

for Consideration of Fire Safety. *Science and Safety 1 (6)*.
Nachtigall, E. & W. Klingsch (2011). Perspektiven anlagentechnischer Komponenten im ganzheitlichen Brandschutz. *sicher ist sicher - Arbeitsschutz aktuell 04, 160-163.*
NOSTROY (2014). STONOSTROY 2.35.73-2012 Engineering networks of high-rise buildings; Systems of complex safety of high-rise buildings and constructions.
Novak, T. (2008). Functional Safety and Systems Security in Building Automation and Control Systems - A Common Approach, PhD-Thesis, Vienna.
Rausand, M. & A. Hoyland (2004). System Reliability Theory Models, Statistical Methods and Applications. Hoboken: John Wiley.
Rolle, I. (2013a). Die Sicherheit eingebetteter Systeme. *Elektronik 3*.
Rolle, I. (2013b). Modelle der funktionalen Sicherheit. *Elektronik 3*.
Ropohl, G. (2012). Allgemeine Systemtheorie Einführung in transdisziplinares Denken. Germany: edition sigma.
Ryan, M. J. & R. I. Faulconbridge (2014). Systems Engineering Practice. ArgosPress.
Shcherbina, V. I., M. M. Lubimov, E. I. Puzyrevskaya, & V. P. Matveev (2012). Functional safety of the safety-related systems in construction. *Globalnaya bezopasnost, Yubileyny vypusk.*
Shcherbina,V. I., E. I. Puzyrevskaya, M. M. Lubimov, & V. P. Matveev (2011). Functional safety of the safety-related systems in construction. Technical Report 2126.
Smith, D. J. & K. G. L. Simpson (2004). Functional Safety. A straightforward guide to applying IEC 61508 and related standards. Elsevier Butterworth-Heinemann.
VDI (2005). VDI 6010Technical safety installations Systems overlapping functions, All parts.