Rakowsky Uwe Kay
Ruhr West University of Applied Sciences, Section Safety Engineering, Germany

On the basic concepts of safety engineering

Keywords

safety, system, terminology, causality, randomness, failure, fault, hazard, standardisation, ethics

Abstract

The basic concepts of safety engineering and functional safety frameworks are presented and discussed in this paper. The scope includes safety aspects, which are deeply rooted in philosophy e.g. the principles of causality, determinability, and randomness. Moreover, concepts are presented, which are subject of standardisation, engineering association activities, and aspects, practitioners struggling with in daily business, e.g. failure and fault; architecture and structure; redundancy and channels. The paper closes with a brief glance on engineering ethics.

1. Introduction

This paper intends to summarise the basic concepts on safety engineering. Distinguishing between qualitative and quantitative, the latter are not considered. Fundamentals of probabilities and non-probabilistic reliability measures are also omitted, since they are discussed in [6] and in the assigned conference contribution of a special session during the ESREL 2005 conference in Gdansk. Moreover, risk assessment and all related issues are excluded here, as risk assessment represents a different approach to safety than this paper intents.

This paper is successively and constructively structured, beginning with system theory adaptions and terminology and then followed by the safety engineering roots in philosophy, i.e. causality and randomness. Next sections discuss practice issues, e.g. failure and fault; architecture and structure; redundancy and channels. The paper closes with a brief glance on engineering ethics.

2. System properties

2.1. Concepts from system theory adapted to safety engineering

The International Electrotechnical Vocabulary (IEV) Part 351 "Control Technology" defines a system as a

> *Set of interrelated elements considered in a defined context as a whole and separated from their environment.*

Patzak [5] describes a system more precisely by six properties:

- The definition of borders
- The specification of in- and outputs
- The definition of elements (i.e. components or modules)
- The definition of links between elements
- The interactions of the elements
- The task of the system.

A rail vehicle is used as an example to explain these properties.

System border
The border of rail vehicle is given by the outer shell, the pantograph contact point to the wire, and the wheel area contacting the rail. Communication items are embedded in the outer shell and discussed next as interfaces.

In- and Outputs
Typical in- and outputs of a rail vehicle are doors, pantograph, front window, vehicle front and rear signals (colloquially denoted as lights or lamps), train protection antenna, communication antenna, etc.

Elements
Typical elements of a rail vehicle are screws and nuts; resistors, capacitors and inductors; up to motors, gearboxes and bogies, or seats and handles.

Links between elements
The set of links or relations between elements is often denoted as structure of the system. Typical structure representations are wiring diagrams or functional block diagrams (FBD). Functional safety focusses on the specifications of links between elements.

Interaction between elements
The flow of traction energy within a rail vehicle gives a good example of interacting elements. Energy flows from overhead line to converter, motor, brake resistor or e.g. back to converter, recuperation energy storage, converter and motor again.

Task
Finally, the task or – in case that the system is a process – the objective of the system shall be defined, which is the basis for a requirement management. Obviously, the task of a rail vehicle is moving people from station to station.

2.2. System decomposition

According to IEV 192 on Dependability [1], term 192-01-01 defines an item as

A subject being considered

As the IEV states, the item may be an individual part, component, device, functional unit, equipment, subsystem, or system. The item may consist of hardware, software, people or any combination thereof. The item is often comprised of elements that may each be individually considered. This approach to safety considers systems, modules, and components as items, in which systems comprise modules and components, and modules comprise components, see *Figure 1*.

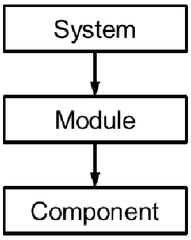

Figure 1. Typical system decomposition

A system has to be such that it can be broken down into a countable and finite number of modules or components, respectively. Sections **Błąd! Nie można odnaleźć źródła odwołania.** and **Błąd! Nie można odnaleźć źródła odwołania.** introduce critical and delicate components, respectively.

2.3. Reality and abstraction

Following Leveson [3], a system is a model. *Figure 2* distinguishes between reality and abstraction. The object which is under development is engineered by applying representations. Generally, in engineering wiring diagrams, constructional drawings, or function block diagrams are typical representations of a given system. Safety and reliability analyses are based on a model of a system, see *Figure 1*. For example, reliability block diagrams, fault trees, event trees, or Petri Nets are models of systems, which can be analysed concerning their reliability. More precisely:

- A safety model (e.g. fault tree) is a model of a model (e.g. wiring diagram).
- Safety analysis analyses the safety of a model – not of a real object.

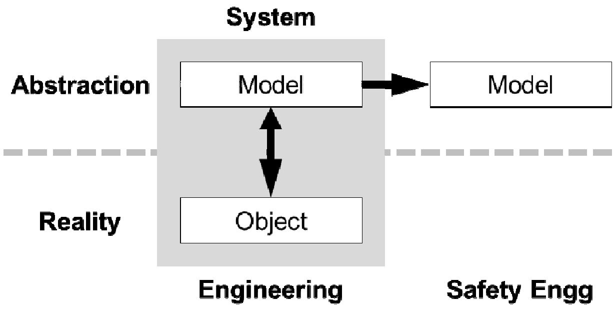

Figure 2. Reality and abstraction in engineering and especially in safety engineering

3. Terminology and engineering communication

Terminology is a discipline that systematically studies the labelling or designating of concepts particular to one or more subject fields [10]. Dictionaries, glossaries, and vocabularies are outputs of terminology. A dictionary is collection of words in one or more specific languages, often listed alphabetically, with usage of information, definitions, etymologies, phonetics, pronunciations, translation, and other information; or a book of words in one language with their equivalents in another, also known as a lexicon [12]. A glossary, also known as a vocabulary, is an alphabetical list of terms in a particular domain of knowledge with the definitions for those terms [7]. Safety and reliability vocabularies given by

- IEC 61508 Part 4:2010 – Definitions and Abbreviations,
- International Electrotechnical Vocabulary (IEV) published as IEC 60050 standard,

especially

- Part 192 “Dependability” of the IEV [1] replacing the former IEV 191,
- Part 903 “Risk Assessment” of the IEV.

The objective of applying vocabularies is supporting an unambiguous and precise communication within a team and between teams working in the field of engineering, e.g. development team, safety team, quality assurance team, consultants, assessors, or public authorities. Unambiguous communication means that a term and its definition describe exactly one fact, see *Figure 3*.

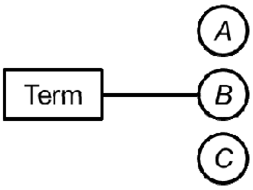

Figure 3. Unambiguous assignment of a term to one fact of the set {*A*, *B*, *C*}

Precision in communication means that a term and its definition describe a fact precisely. There is a sharp line between what is meant by the fact and what is not meant.

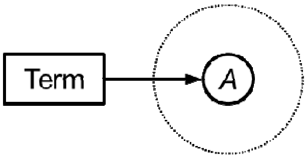

Figure 4. The sharp line around *A* indicates what is meant, the field between the sharp and the grey line indicates what is not meant by the term

A typical example for an issue in communication is the application of failure and fault, see Section 5. An unambiguous and precise communication is the basis

- for no misunderstandings in communication while designing safety-relevant systems
- and for an efficient engineering without loss of time in communication.

Applying a technical vocabulary in compliance with IEC, ISO, and specific standards is an appropriate measure achieving both objectives.

4. Causality

The objective of this section is providing an approach to causality or causation, respectively, for modelling reality, especially the interaction of elements within a system. Therefore, the following definitions just scratch the extensive philosophy work on this topic.

> *Cause is a premise, reason, or starting for anything following.*
> *Consequence or effect is a result of a cause.*

In safety engineering, cause and consequence are events or states depending on the particular modelling context, i.e. system or scenario properties. Generally, a cause is predating a consequence; and consequently, a consequence is postdating a cause. Avoiding discussions on incompatibilism, compatibilism, and existentialism, it is not required that every event or state lead to a consequence or an effect. In terms of safety engineering, cause is an event or state leading to a consequence or effect. If there is no consequence or effect, an event or state is simply denoted as what they are: an event or a state. Reversely, every consequence has a cause. If a cause is not known, that does not necessarily imply that a cause does not exist. Mackie [4] defines

> *Causality is the relation between an event (the cause) and a second event (the effect), where the second event is understood as a physical consequence of the first.*

Reduced and tailored to the needs of safety engineering, following definition is proposed:

> *Causality is the sequence of related event(s) and state(s).*

With that,

> *Causal chain is a temporal sequence of cause-consequence elements.*

The starting of a causal chain is denoted as *root cause* (see *Figure 5*), in terms of failure and fault (refer to Section 6) modelling as *root cause failure*.

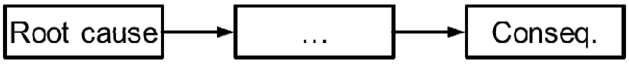

Figure 5. Causal chain starting with a root cause; the middle box can be either considered as consequence of the root cause or as cause of the succeeding consequence.

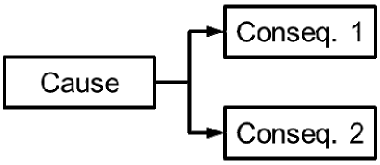

Figure 6. Example of mono-causality

Mono-causality means that every consequence is related to only one cause, see *Figure 6*. *Multi-causality* means that every consequence is related to two or more causes, see *Figure 7*.

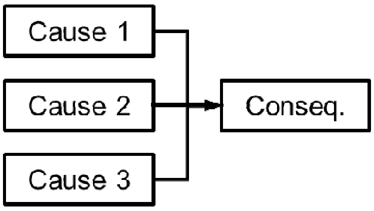

Figure 7. Example of multi-causality

As causal chain represents events and states only in a time context, scenario extents the modelling to a space-time context.

> *A scenario is a sequence of events and states in a given space-time context.*

Safety engineering requires causality in system behaviour within a given scenario. Again, if a system operates seemingly "incausally" or illogically, parts of causal chains or scenario are not known.

5. Randomness

IEC 61508-4:2010 distinguishes between random and systematic events (refer to Section 3.6.5). On the one hand,

> *Random [events] can be predicted [and] quantified with reasonable accuracy.*

On the other hand,

> *Systematic [events], by their very nature, cannot be accurately predicted. [Therefore, systematic events cannot be] accurately statistically quantified.*

Randomness is defined here as a property measured by its predictability and with that by its quantifiability. This concept may be pragmatic; however, it has not been shown, if the IEC classification of randomness fits to philosophical concepts. These concepts can be categorised by four classes as given in [8]

> *1) An event happens objectively without cause.*
> *2) An event happens without a cause would be recognizable.*
> *3) An event happens with an unpredictable result, which means that although the factors are known; however, they cannot be measured or controlled. (Empirical-pragmatic randomness)*
> *4) Two events are in no (known) causal relationship.*

Category 1 has not been observed in the macroscopic world and should not be detectable in principle. In quantum physics, the existence of objective chance is discussed in the context of their various interpretations. Category 2 implies that the causal chain or the influencing factors are not completely proven; however, their presence is suspected. Category 3 refers chaos theory and is observed in systems whose behaviour is very sensitive to small variations in initial conditions, e.g. roulette ball or dice [9]. Finally, category 4 is an attempt to bring independent things in connection. Examples are duplicity (not as rare in safety engineering as often assumed), triplicity (rarely in safety engineering), and multiplicity (typical in quantum physics). Tailored to safety engineering, randomness can be described by three properties:

> *1) For the same cause, it may be several different consequences.*
> *2) There is no apparent cause for the occurrence of a particular consequence.*
> *3) In repetitions of the same initial situation other end situations can occur.*

As IEC 61508-4:2010 states that randomness is linked to predictability and quantifiability, reliability engineering considers mean values as an appropriate countermeasure against random events. Prognostic health management (PHM) offers an even stronger confinement of random failures than classical reliability engineering does. The objective is approaching determinacy of the failure date by refined diagnosis and prognosis methods. Moreover, modern approaches discuss mathematically more elegant modelling beyond Boolean algebra and statistics theory, e.g. uncertainty modelling in probability or Dempster-Shafer theory.

6. Failure and fault

According to IEV 192 [1], a failure is an event and a fault is a state. IEV 192-03-01 defines a failure as

> *Loss of ability to perform as required*

The definition focusses on the item functionality only and does not distinguish between electric, electronic, mechanic, pneumatic, hydraulic or software applications. Term IEV 192-04-01 defines a fault as

> *Inability to perform as required, due to an internal state*

Comparing both definition "Loss of ability" and "Inability" needs some explanations. The first describes a transient from one state to another by an event; the second is a description of a state. With that, IEV 192 states:

> *A failure of an item is an event that results in a fault of that item. A fault of an item results*

> *from a failure, either of the item itself, or from a deficiency in an earlier stage of the life cycle, such as specification, design, manufacture or maintenance.*

Figure 8 illustrates both an adds functioning and faulty.

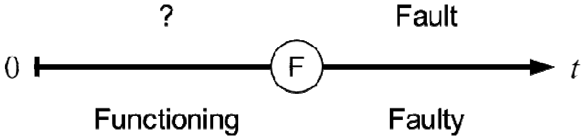

Figure 8. Failure (F) as an event shown on a time axis and fault as a state succeeding a failure

Failure and fault are sometimes confused with error which is according to IEV 192-03-02 a

> *Discrepancy between a computed, observed or measured value or condition, and the true, specified or theoretically correct value or condition*

Additionally, human error has a complete different nature specified by IEV 192-03-14 as

> *Discrepancy between the human action taken or omitted, and that intended or required*

For example, performing an incorrect action, omitting a required action, miscalculation, or misreading a value is a human error. Other disciplines have different definitions conflicting with IEV 192, e.g. information technology definition on failure and fault. Therefore, it is highly recommended that safety-related documents apply vocabulary as given in IEC 61508-4:2010 or IEV 192.

6.1. Systematic, random, and determinable failure

Functional safety approaches distinguish between systematic or reproducible failures on the one hand and random failures on the other hand. Systematic or reproducible failure is defined by IEV 192-03-10 and IEC 61508-4:2010, 3.6.6 as a

> *Failure that consistently occurs under particular conditions of handling, storage or use*

The cause of a systematic failure originates in the specification, design, manufacture, installation, operation, or maintenance of the item. A systematic failure can be reproduced by deliberately applying the same conditions; although, not all reproducible failures are systematic. The cause(s) of a systematic failure can be cleared after their discovery. Typical counteractive measures are installing a framework of quality assurance and safety assurance processes including e.g. verification, validation measures.

Random failure is not explicitly defined in the IEV 192. The IEC 61508-4:2010, 3.6.5 definition

> *Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware*

is neither precise nor helpful in application. The supplemented note gives hint on randomness as discussed in Section 5:

> *A major distinguishing feature between random hardware failures and systematic failures is that system failure rates (or other appropriate measures), arising from random hardware failures, can be predicted with reasonable accuracy but systematic failures, by their very nature, cannot be accurately predicted. That is, system failure rates arising from random hardware failures can be quantified with reasonable accuracy but those arising from systematic failures cannot be accurately statistically quantified because the events leading to them cannot easily be predicted.*

In one sentence: If randomness is assigned to predictability and quantifiability, then the intrinsic failure rate – as applied in reliability engineering – represents random failure.

Reliability engineering distinguishes between *intrinsic* and *extrinsic* (or more widespread used *external*) failure causes. Intrinsic failure causes are mostly related to unknown failure physics. Failure causes can be amplified and failure rates increased by external influences as load (especially electric power), temperature, vibration, or radiation (especially in space applications)

Generally, the time to failure can neither be predicted exactly for systematic or reproducible nor for random failures. This is in contrast to the impression that the IEC 61508-4:2010 gives on random failure in Section 3.6.5. Actually, the standard refers to the mean time to failure, which is computable by probabilistic or statistic methods. Consequently *determinable failures* are

> *Failures, occurring at a predictable time*

Typical examples are cracks in aircraft wings or railway vehicle wheel sets, where point, depth, and length determine the so-called remaining useful lifetime. Safety-related measure is a scheduled maintenance (IEV 192-06-12) specifying maximum operating time between two inspections.

6.2. A priori and a posteriori

Many case studies in safety engineering focus on the knowledge of involved persons *before* (*a priori*) an event occurs and *after* (a posteriori) an event occurred, see *Figure 9*. The same holds for Bayesian and other approaches in reliability engineering.

A priori predictions and quantifications (e.g. probabilities) are based on assumptions considering random failures. A posteriori quantifications apply frequencies and resulting estimated probabilities on the basis of experience of the past and observations. A posteriori, every random failure is determinable if detection means enable an analysis of failure physics.

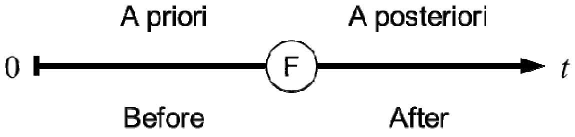

Figure 9. A priori and a posteriori in context of a failure with system commissioning at $t = 0$

6.3. Critical component

As defined in Section 2.2, a component is an element of the system considered. A failure or fault, respectively,

> *Which is assessed as likely to result in injury to persons, significant material damage or other unacceptable consequences*

is defined by former IEV 191-04-02 as *critical failure* or *critical fault* (IEV 191-05-02), respectively. The term critical state is defined in analogy (IEC 191-06-10). A component, whose failure or fault is critical, is denoted as critical component. The same holds for critical module or system. Critical components can be identified by a variety of importance measures, c.f. Birnbaum, Fussell, Armstrong, Levitin & Lisnianski, and others.

6.4. Stress and strain

Stress and *strain* are terms applied in safety engineering beyond mechanical context

> *Stress represents effects on an item from the outside*
>
> *Strain is the reaction on the stress of the item*

A typical example from human reliability is sport (stress) and pulse rate (strain).

6.5. Delicate components in terms of PHM approaches

The IEC definition on criticality tends rather to safety than to reliability-related issues. Unacceptable consequences in terms of operating in a prognostic health management (PHM) context are all effects, which have a relevant influence on system behaviour concerning reliability, availability, maintainability, or lifecycle costs.

PHM approaches consider properties of well-selected components. Here, a delicate component is a critical component where system dynamics are known for having an influence on the component reliability characteristics. For example, the voltage at a capacitor has an influence on the failure rate of the capacitor; the same holds for current on relay contacts, or temperature (among others) on semiconductors. It is required that the context between system dynamics and the reliability of a delicate component

- is sufficiently known by cause-consequence chains,
- and it can be quantified.

The overall number of components only limits the number of delicate components; however, in view of the calculation efforts needed, their number should be kept to just a few.

7. Damage and hazard

Definitions of safety (refer to Section 8) presume an understanding of *damage* and *harm.*

> *Damage or harm is an unrequested change of the system or its environment, which is caused by the system.*

IEC Guide 51 and IEV 351-57-02 tend to a different definition of *damage* and *harm*

> *Physical injury or damage to the health of people or damage to property or the environment*

Thereby, damage is defined by damage. The first definition on damage and harm requires a criterion of what is requested and what is unrequested. This points to a definition of acceptance of injuries or damage; however, defining acceptance level depends on the legal framework of the country where the system is operating. For example, in Germany only a judge is permitted to decide on what is acceptable and what is not.

A general example of acceptance and aversion are airbags as mounted in cars: Injuries and damages caused by airbag expansions are accepted because they are less severe than accidental injuries or damage on vehicles without installed airbag.

Damage or *harm* is caused by a hazard, which is defined as

> *Potential source of harm*

by IEC 61508-4:2010 Section 3.1.2 and ISO/IEC Guide 51:1999. A *hazardous event* is consequently an

> *Event that may result in harm*

refer to IEC 61508-4:2010, 3.1.4. Next, a *harmful event* is an

> *Occurrence in which a hazardous situation or hazardous event results in harm*

As defined in IEC 61508-4:2010 Section 3.1.5. These three definitions demand a qualitative definition of *security* without applying risk approaches. A proposal may be

> *State that prevents the transition from hazardous event to harmful event.*

8. Safety and reliability

8.1. About safety

Definitions of safety can be categorised into three classes

1) Definitions of absolute or ideal safety
2) Definitions of relative safety
3) Definitions of pragmatic safety

An example for the first class of an absolute *safety* is given in the rejected German guideline VDI/VDE 3542-4:2000

> *Safety is absence of danger.*

Leveson [3] defines safety as

> *Freedom from accidents or hazards*

Second class definition of relative safety is given by the System Safety Society

> *Freedom from exposure to the occurrence of accidents.*

Examples for third class pragmatic *safety* definitions are published by the Society for Risk Analysis

> *Relative protection from adverse consequences*

and, finally, IEC 61508-4:2010 Section 3.1.11 and ISO Guide 51:1999, 3.1 with *safety* as

> *Freedom from unacceptable risk*

8.2. About reliability

Safety and reliability have a big intersection in methods, measures, and activities. Therefore, parts of the safety engineering framework have their roots in reliability theory.

The term *reliability* is used as denotations for a discipline, a performance, and a measure. Reliability as a performance is defined by IEV 192-01-24

> *Ability to perform as required, without failure, for a given time interval, under given conditions*

Generally, the synonymous generic terms *reliability* and *dependability* include

- Availability (IEV 192-01-23)
- Recoverability (IEV 192-01-25)
- Maintainability (IEV 192-01-27)
- Maintenance support performance (IEV 192-01-29)

and in some cases

- Durability (IEV 192-01-21)
- Safety
- Security

8.3. Links between safety and reliability

Safety is a system property. There is no safety in system decomposition: No safe component or module, no safe hardware at all, no safe software.

The property *reliable* can be assigned to components, modules, software, architecture, maintenance, etc. The relation between safety and reliability is not trivial. Opposites of both exist: There are safe and reliable systems, as well as unsafe and reliable. Nevertheless, the intersection between safety and reliability exist as well.

8.4. About functional safety

IEC 6150-4:2010 Section 3.1.12 defines *functional safety* as

> *Part of the overall safety relating to the equipment under control and the equipment under control control system that depends on the correct functioning of the electrical, electronic, programmable electronic safety-related systems and other risk reduction measures*

Note, that “equipment under control control system” is no editing mistake. In practice, “other risk reduction measures” is widely interpreted. Even mechanic, hydraulic, pneumatic items are integrated in functional safety frameworks. The four main objectives of functional safety are

- Avoiding systematic errors in the development
- Detection of failures in operation
- Control of failures

– Transition to a safe state

As stated in Section 8.2, safety and reliability have a big intersection, see *Figure 10*. The same holds for functional safety, where the intersection is filled with

- Methodology for demonstrating safety
- Measures, functions, and parameters for quantifying item reliability and
- for quantifying hazard.

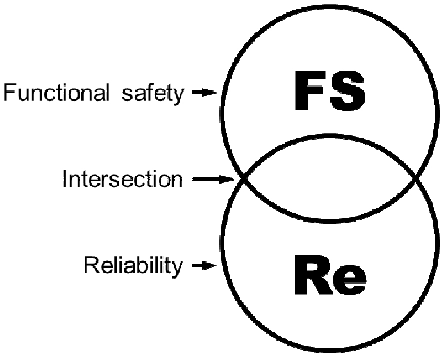

Figure 10. Relation between functional safety and reliability

8.5. Safety analysis

Safety analysis is the

> *Systematic process of decomposing a system into elements to gain a better understanding of system safety*

With that

- The system has to be structured by methodological means, e.g. Boolean algebra and its graphical representation fault tree
- The system has to be reviewed, evaluated, and assessed.
- The system properties as defined in Section **Błąd! Nie można odnaleźć źródła odwołania.** built the framework in which a safety analysis is conducted.

9. Architecture and structure

The term *architecture* is frequently used in safety, reliability, and software system safety frameworks and defined by IEC 61508-4:2010 Section 3.3.4 as

> *Specific configuration of hardware and software elements in a system*

Other interpretations say that *configuration* is an

> *Arrangement, compilation, or selection of objects*
> *Adaptation of software or hardware to the entire system*

In terms of reliability engineering, *structure* is

> *Arrangement and combination of components and modules in reliability block diagram*

Figure 11 shows a reliability block diagram with a redundancy, defined by IEV 192-10-02 as

> *Provision of more than one means for performing a function*

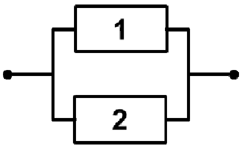

Figure 11. Redundancy of two components shown in a reliability block diagram

The definition of channel in IEC 61508-4:2010 Section 3.3.6 tends in the same direction (see *Figure 12*) with following definition

> *Element or group of elements that independently implement an element safety function*

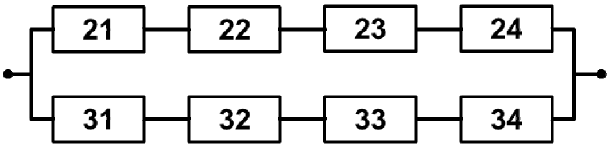

Figure 12. Channel is understood as a path in a redundancy, i.e. components 21 to 24 are forming a channel

A subset of redundancy consists of diverse components or modules. *Diversity* is defined in IEC 61508-4 Section 3.3.7 as

> *Different means of performing a required function*

Moreover, paths and cuts of a system have to be identified in many applications, see *Figure 13 Path* is a

> *Subset of serially linked functioning components and modules in reliability block diagram, which leads to the functioning state of the system*

and cut a

> *Subset of faulty components and modules in reliability block diagram, which leads to system fault*

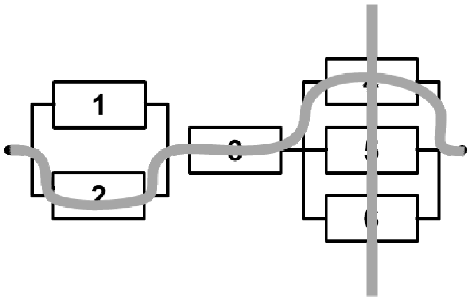

Figure 13. The grey snake indicates a path, the vertical line a cut within the given reliability block diagram

10. State of the art and standardisation

The objectives of standardisation in safety engineering are

- Avoiding damage, accidents, disasters, or catastrophes
- Avoiding errors in system development or operation
- Avoiding economic damage, e.g. loss of market share

From a legal point of view, standards are defining the state of the art. According to IEV 901-01-04 the *state of art* is a

> *Developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience.*

The state of science can be defined according [11] as the

> *Epistemological and philosophical summary of each current knowledge of a scientific discipline or of all sciences*

There is a global consensus on the content of the standards. Standards are periodically reviewed, corrected, and updated. A very large, globally distributed team is involved in maintaining standards. An IEC or ISO standard is verified by more than hundred people. This compares with textbooks, which are reviewed by about three people. Moreover, standards are compiling and providing the knowledge of past generations. Finally, clauses in commercial contracts in engineering are based on standard. The main topics of standardisation in the safety engineering framework are

- Concerning development and safety team: roles, qualifications, training, certificates
- Concerning communication: terminology, e.g. failure, fault, error, mistake
- Concerning product or process: safety requirements, testing, modelling (fault tree, reliability blo), safety and reliability measures

Most relevant organisations publishing standards on safety, functional safety, reliability, dependability, and related working fields are the *International Electrotechnical Commission* (IEC) and the *International Organisation for Standardization* (ISO), both based in Geneva. The IEC publishes international standards for all electrical, electronic, and related technologies; the ISO promotes worldwide proprietary, industrial, and commercial standards. The European counterpart of the IEC is the *European Committee for Electrotechnical Standardisation* (CENELEC) and the *European Committee for Standardisation* (CEN) for the ISO. Additionally, national engineering organisations e.g. IEEE in the US, VDI in Germany, or FSNT-NOT in Poland are publishing guidelines.

Despite all appreciation, there is some criticism on some standardisation activities:

- Standards are not perfect, especially issues in terminology lead to lot of disputes.
- Standards are still containing a rest of ambiguities.
- Lobbying may lead to “braking and blocking” of new upcoming standardisation activities.

However, in medium term, standardisation activities are unstoppable and developing a kind of self-healing effect.

11. Engineering ethics

Ethics is a

> *Part of the field of philosophy that deals with the conditions and criteria of rational human action. In the center of ethics is the specific moral action, in particular with regard to their justifiability and reflection.*

The objective of codes of ethics in engineering are

- Ethics provides assistance in decision making.
- Ethics provides general principles of good conduct and judgment.

However, codes of ethics are theoretical approaches that must be applied situation-specific by each individual in his/her particular situation. Codes of ethics are addressed to all disciplines of engineering. Typically, safety is prominently addressed in codes. For example, the IEEE Code of Ethics is given here as reference. As defined in the IEEE Policies [2], the members of the IEEE agree:

> *1. to accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors*

that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding of technology; its appropriate application, and potential consequences;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics.

12. Conclusions

Obviously, the further work on the basic concepts of safety engineering should focus on aspects and issues, which are not (yet) subject of standardisation or engineering association activities. Safety engineering is deeper rooted in philosophy, as some practitioners might admit while struggling in daily business. Especially, the principles of causality (refer to Section 4), determinability, and randomness (refer to Section 5) need a deeper discussion and understanding in the framework of safety engineering and reliability theory.

Abbreviation

CEN	European Committee for Standardisation
CENELEC	Committee for Electrotechnical Standardisation
IEC	International Electrotechnical Commission
IEV	International Electrotechnical Vocabulary
ISO	International Organisation for Standardization
PHM	prognostic health management

References

[1] IEC 60050-192: International Electrotechnical Vocabulary – Part 192: Dependability. (2014-04, FDIS) IEC, Geneva.

[2] IEEE Policies, Section 7 – Professional Activities (Part A, 7.8). *IEEE Code of Ethics*. Approved by the IEEE Board of Directors, June 2014.

[3] Leveson, N. (1995) *Safeware: System Safety and Computers*. Addison-Wesley, Boston.

[4] Mackie J. L. (1988) *The Cement of the Universe: A study in Causation*. Clarendon Press, Oxford.

[5] Patzak, G. (1982) *Systems Engineering – Design of complex innovative systems: principles, methods, techniques* (in German). Springer, Berlin.

[6] Rakowsky, U.K. (2005). Some Notes on Probabilities and Non-Probabilistic Reliability Measures. Kolowrocki, *K. (edt.): Advances in Safety and Reliability. Proc. of the European Conference on Safety and Reliability – ESREL* 2005, Gdynia-Sopot-Gdansk/Poland. Leiden: Balkema, 2, 1645–1654.

[7] Web page: en.wikipedia.org/wiki/Glossary, accessed 2015-02-25.

[8] Web page: de.wikipedia.org/wiki/Zufall, accessed 2015-02-23.

[9] Web page: en.wikipedia.org/wiki/Randomness, accessed 2015-02-23.

[10] Web page: en.wikipedia.org/wiki/Terminology, accessed 2015-02-25.

[11] Web page: de.wikipedia.org/wiki/ Stand_der_Wissenschaft, accessed 2015-02-28.

[12] Webster's New World College Dictionary, Fourth Edition, 2002