Railway Safety and Security –
Two Sides of the Same Coin ? !

L. Schnieder; E. Schnieder; T. Ständer

*Technische Universität Braunschweig, Institute for Traffic Safety and Automation Engineering,
Langer Kamp 8, 38106 Braunschweig, Germany
e.mail: {l.schnieder /schnieder /staender}@iva.ing.tu-bs.de*

Abstract: In many different standards the subject matter of dependability, including reliability, availability, maintainability and safety/security, RAMS(S) for short, is defined by various concepts. Their unambiguous definition can lead to a clear interpretation which facilitates communication of all persons involved in the development of safety-critical railway applications. By means of concise communication during specification, subsequent implementation as well as the preparation of operating and maintenance manuals negative legal and financial impacts can be avoided. This paper introduces a method for terminological disambiguation and applies it to the terms “safety” and “security”. In the future this helps to improve communication in the railway domain.

Keywords: risk management, standardization, terminology, communication

1. INTRODUCTION

Railway safety is an interdisciplinary research discipline. For this reason a clear understanding of the terminology is indispensable. Often interdisciplinary projects call for a cooperation of experts from different disciplines. Domain-specific terminologies are referred to as a "double-edged sword". On the one hand side terminologies specific to a particular specialist area make it possible for the experts to effectively communicate with other members of their domain. On the other hand side cross-domain collaboration brings about some unique challenges – often misunderstandings over concepts and terminologies emerge and become obstacles for interdisciplinary collaboration (Gooch 2005). This clash of different domain-specific technical terminologies is often referred to by the proverbial Babylonian confusion. In interdisciplinary collaboration understanding is often hampered by the following aspects:

- *ambiguity:* often standards introduce one term which refers to a variety of different concepts as mental representations (so called homonymy). One example of a homonym associated with the railway domain is the word "switch" which has an identical spelling and pronounciation but can refer to either a kind of junction between multiple railroad tracks or refer to a computer device that connects network segments in computer technology. Especially in the design of electronic interlockings this usage of homonyms can cause confusion. Sometimes there are several words in a language for a thing or action (synonym). It is the aim of a controlled vocabulary to state which one of the existing terms should be preferred. In the aviation industry for example the verb "start" is used instead of the synonymous verbs "begin", "commence", "initiate" or "originate" (ASD STE 100). The readability of the document can be increased significantly if during document creation the use of synonyms is reduced.

- *inconsistency:* often different standards (sometimes even within one standard) contain definitions which state the opposite. Those opposites can not coexist at the same time. One example is the different point of view of the term "fault" expressed in IEC 61508-4 and IEC 60050(191). In the case of IEC 60050(191) a fault is referred to as the result of a failure whereas in the case of IEC 61508 a fault is an abnormal condition that may cause a failure.

- *semantic vagueness:* Practice clearly demonstrates that for the comparability of the results of risk analyses vagueness may cause a methodical problem. Even though other examples can be found, it is a commonly accepted practice to classify measures of damage on an ordinal scale ranging in ascending order from "minor injury" and "major injury" to "fatality". Despite this consensus on the classification the definition of the characteristics which constitute the difference in meaning remains fuzzy. In the first place there is no agreement on which characteristics should be used to delimit a specific class. Is the duration of clinical treatment (in hours) the delimiting characteristic as proposed by Eurostat (see CLC/TR 50126-2), or is it the time of convalescence (in weeks), the reversibility of the injury (boolean) or the regain of full capacity to work (boolean) as suggested in DIN-Fachbericht 144? Even if there was a consensus on the delimiting characteristics of the classes the definitions remain vague due to the missing harmonization of the scaling. In the example of measures of damage semantic vagueness can be overcome by unambiguous definition of harmonized risk measures and metrics.

- *context dependence:* The meaning of a term depends on the context it is used in. In linguistics it is a commonly recognized fact that linguistic symbols are arbitrary (de Saussure 2006). This means they are merely an agreed-upon convention to represent a certain thing by users of that language. For interdisciplinary collaboration this has the consequence that terms coined by one specific domain might denote something different in other domains. In electrical engineering the term "signal" refers to a physical quantity that can carry information whereas in railway engineering it refers to a mechanical or electrical device beside the railway line to transmit information relating to the state of the line ahead to the train driver. This possible source of ambiguity (homonymy) for communication across borders of one specific technical terminology can be overcome. In lexicography the meaning is disambiguated by means of annotations. Classification systems (e.g. the International Classification for Standardization of the International Organization for Standardization) might be used as an ordering principle to cope with the complexity of natural language semantics in an increasingly interdisciplinary context.

In order to disentangle from the currently existing Babylonian confusion a fundamentally new approach to terminology management is required (Schnieder/Schnieder 2009). For this reason this paper

- presents a methodical approach which can help overcome the problems currently associated with terminology standardization which solely relies on natural language (chapter 2). ISO/TR 24156:2008 which gives guidelines for using a subset of the Unified Modeling Language (UML) to represent the results of terminological concept analysis is amended by Petri-nets to support the analysis of causal concept relations.
- formalizes the term *risk* which is the common denominator of safety and security engineering (chapter 3). Using a UML-based notation the terminological relations between risk and its associated concepts are explained.
- formalizes the safety-terminology stipulated in ISO-Guide 51 using the Petri-net notation previously introduced (chapter 4). This means of description reveals the existing relations between the concepts. Previously isolated concepts are arranged as a chain of causation.

- formalizes the security-terminology recently introduced in ISO: SMB/3971/DC using the approach previously applied to safety-terminology (chapter 5). It becomes obvious that two chains of causation reveal an isomorphic structure.
- formalizes the framework for risk management which covers both safety and security aspects (chapter 6).

2. METHODICAL FOUNDATION

Misunderstandings can be resolved or even prevented if a concept system is established which has been empirically tested and checked for logical consistency (Jansen and Schnieder, 2001). This contains in particular an unambiguous terminology which is characterized by a proper identification of concept relations within a concept system.

The suggested formalization of the concept model as well as the concepts defined following this model are a further step towards consistent concepts. The concept system with its terms and concept relations developed based upon the theoretical foundation outlined in the following sections can then be applied to disambiguate the currently ambiguous, inconsistent, vague and context-specific terminology of safety and security in the railway domain.

2.1 Formulation of the concept (meta-)model

Complex technical systems are often developed based on concepts expressed in natural language which can (and often will) be interpreted differently by different persons with different backgrounds. In linguistics, words can be described as linguistic signs as they represent the word in a symbolic, rather than a literal way, and that understanding these symbolic relationships is what distinguishes speakers from non-speakers of a language. The influential Swiss linguist Ferdinand de Saussure states that a word comprises two elements: a sound image, that is, a pronunciation form, or *signifier*, and a meaning, termed the *signified* (de Saussure 2006; Finch 2000). The signified, thus the meaning corresponds to the *concept* of ISO 1087. The initial two-sided model of Saussure was meant to be context-independent. In order to allow for clear differentiation of domain specific conceptualization an amendment is required. Thus a sign’s pragmatic context can be modeled (see figure 1) with the *variety*. The constituents of the metamodel of a linguistic sign stipulated in this paper are as follows:

- A *designation (signifier),* that means either a verbal representation (so called term or appellation) or a representation by a symbol.
- A *subject field (domain),* which describes a special field of knowledge. In terms of sociolinguistics this form of domain-specific language variation is also referred to as a *linguistic variety*.
- A *concept (signified),* which is defined as „a unit of thought which is determined by reasons of common properties by means of abstraction“. According to ISO 1087 a concept comprises the following constituents:
    - A *relation* to other concepts which is based on the properties and characteristics of the objects or sets of objects. Relations allow to distinguish between different objects. This in turn requires the perception of their essential characteristics (Lorenzen 1987 and van Schrick 2002) which is referred to underneath as a concept's intension.
    - An *extension,* which characterizes the totality of objects to which a concept corresponds.
    - An *intension* as the set of characteristics which makes up the concept. As already mentioned above the set of characteristics is crucial to delimit a concept and finally constitutes semantic relations.

- A *definition*, which is based on a concepts intension (so called intensional definition), extension (so called extensional definition) or concept relations.

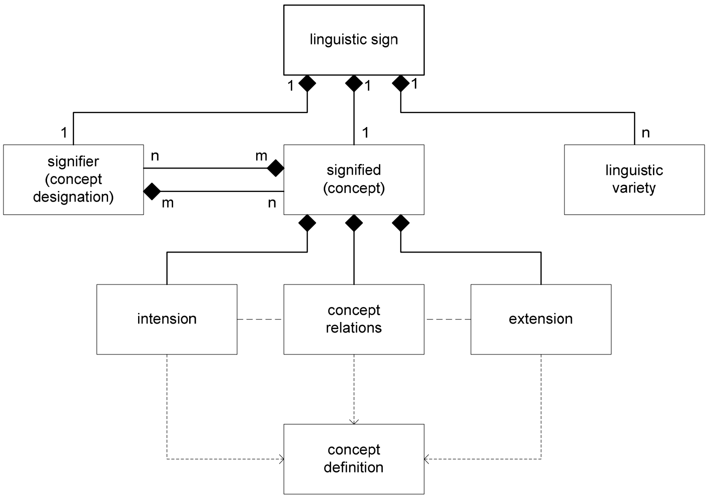

Fig. 1: Metamodel of a linguistic sign

Terms do not exist isolated. Their relational contexts constitute them. There are a variety of different lexical and semantical relations between concepts which span the concept system. According to the basic standards of terminology work (ISO 704, ISO 860, ISO 1087) relations can be differentiated as follows:

- *Hierarchical relations*, which fall into generic relations (taxonomies, e.g. the term "signal" is the superordinate system for the term "mechanical signal") and partitive relations (e.g. a color light signal consists of a fresnel lense, a light bulb as well as a hood and shield to shade the signal lamp from sunlight).
- *Non-hierarchical relations*, which fall into sequential relations (i.e. a successor and predecessor relationship in terms of a causal and/or temporal relation) as well as pragmatic relations such as antonymies (e.g. the differentiation between open block and the fixed block in railway signaling) or the relation of complementarity.

Figure 2 provides an overview of the different relations within a concept system.

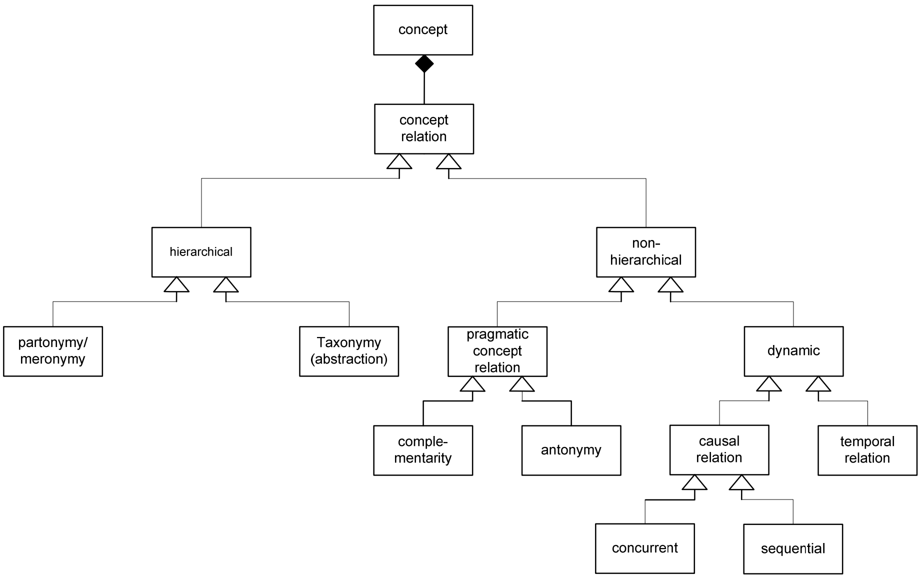

Fig. 2: Relations within a concept system

The *intension* of a concept can be refined and rendered more precise by using abstraction. This leads to a distinction of different hierarchical attributes at different levels of abstraction. This is done in accordance with Carnap's "classical" steps of concept formation (Carnap 1999):

- *Properties* relate to the perceivable qualities of an object. Following Carnap's logical empiricism all knowable relates to sensory experience.
- A *characteristic* is an abstraction of a property of an object. A characteristic is seen as quantifiable which means it can be counted (in case of a topological measurement scale) or measured (in case of a cardinal measurement scale). Measurement is the assignment of numbers to objects or events in a systematic fashion. There is a relationship between the level of measurement (nominal, ordinal, interval, ratio or absolute) and the appropriateness of various statistical procedures.
- A *physical quantity* is a characteristic, which can be quantified. This means it can be measured and calculated and expressed in numbers. According to Carnap this quantitative method of description has essential advantages over purely qualitative methods. On the one hand it permits a more exact description of the separate facts. On the other hand it allows the elaboration of decidedly more effective general laws expressing connections between the values of various quantitative concepts with the help of mathematical functions.
- A *numerical value* is the output of a measurement. This quantity that is being determined by a measurement is also referred to as measurand.

2.2 Mapping the concept model to Petri-nets

It is the intention of this paper to use Petri-nets as a means of (process) description to formalize concepts because some important properties of Petri-nets match the dynamic relations of the concept model best.

Causal relations within a concept system can be explained by the syntactic combination of the notation elements places (can be interpreted as conditions, prerequisites or states within a concept system), transitions (can be interpreted as events, activities, rules or functions within a concept system) and arcs (which represent the causal relation between places and transitions).

Temporal relations can be modeled by means of the token flow. Tokens are created, move around and disappear in a Petri-net. By the token flow the behavior of a system is depicted with the restrictions determined in the structure. Since places, transitions and arcs can be attributed with temporal restrictions temporal aspects can be depicted with this means of description.

Petri-nets can express the semantic *relation of partonymy/meronymy*. The *compositionality* of Petri-nets means that modular sub-nets can be combined to form a complex Petri-net. The idea behind this is to allow the construction of a large model by using a number of small Petri-nets which are related to each other in a well defined way. Of course it has to be taken into consideration that only temporal or causal aspects of a concept system can be further decomposed. Petri-nets also allow for *abstraction* and *refinement*. Transitions can be further refined until a sufficient level of detail has been achieved. This property of Petri-nets allows to deal with a higher degree of complexity.

3. THE RISK CONCEPT AND RELATED TERMS

Before differentiating the terms safety and security their common characteristics shall be highlighted. This will facilitate the latter discussion of the concepts' delimiting characteristics. Since both concepts are related to adverse events which are to be avoided they share the risk concept as a common characteristic. By means of risk the adverse effects can be quantified and become subject of the management discipline of risk management.

In order to understand the idea of risk it is necessary to discuss the concepts which constitute this complex term. These concepts generically defined in ISO/IEC Guide 51 are applicable for all domains. Because risk is a complex term the explanation of this term follows a systematical order. For this reason a bottom-up approach has been chosen starting with the basic terms and ending with the abstract top terms. Nevertheless, the complete taxonomy results in a complex concept system with several relations (Schnieder and Drewes 2008). This can be better expressed graphically by a UML-based visualization in a class diagram (see figure 3).

- *damage:* harm to people, environmental harm or financial detriment to an enterprise or a combination of these which may rise from accidents.
  - *human harm:* is a casualty resulting in fatalities, major/serious injuries or minor injuries to passengers, employees or other members of the public. Currently there is no common definition about what constitutes a fatality, a minor injury or a major injury (see CLC/TR 50126-2).
  - *environmental harm:* This term describes the severity of the extent of contamination and/or destruction of the natural habitat which may arise from an accident. This refers to damage to neighboring property, spread of toxic or other harmful agents into the environment, fire, etc. (c.f. CLC/TR 50126-2).
  - *commercial harm/financial detriment:* This term describes the severity of financial loss which may be associated with an accident or undesirable event. This refers to damage to property (assets belonging to the stakeholders or damage to the reputation/ridership of the operation (see CLC/TR 50126-2 and DIN-Fachbericht 144).
- *Frequency of occurrence:* empirically measured frequency or predicted probability of an (adverse) event.
- *risk:* multiplicative combination of the empirically measured frequency or predicted probability of harm and the severity of that harm. The risk concept is shown in figure 3.
  - *tolerable risk:* risk, which is accepted in a given context based on the current values of society
  - *initial risk:* the risk existing for the specified hazardous events – no designated safety protective features are considered in the determination of this risk (IEC 61508-5)
  - *necessary risk reduction* refers to the reduction in risk that has to be achieved to meet the tolerable risk for a specific situation (IEC 61508-5)
  - *residual risk:* risk remaining after protective measures have been implemented (ISO Guide 51)
  - *actual risk reduction* refers to the reduction of risk achieved by all safety-related systems and external risk reduction facilities (IEC 61508-5).
- *safety:* freedom from any unacceptable risk of harm

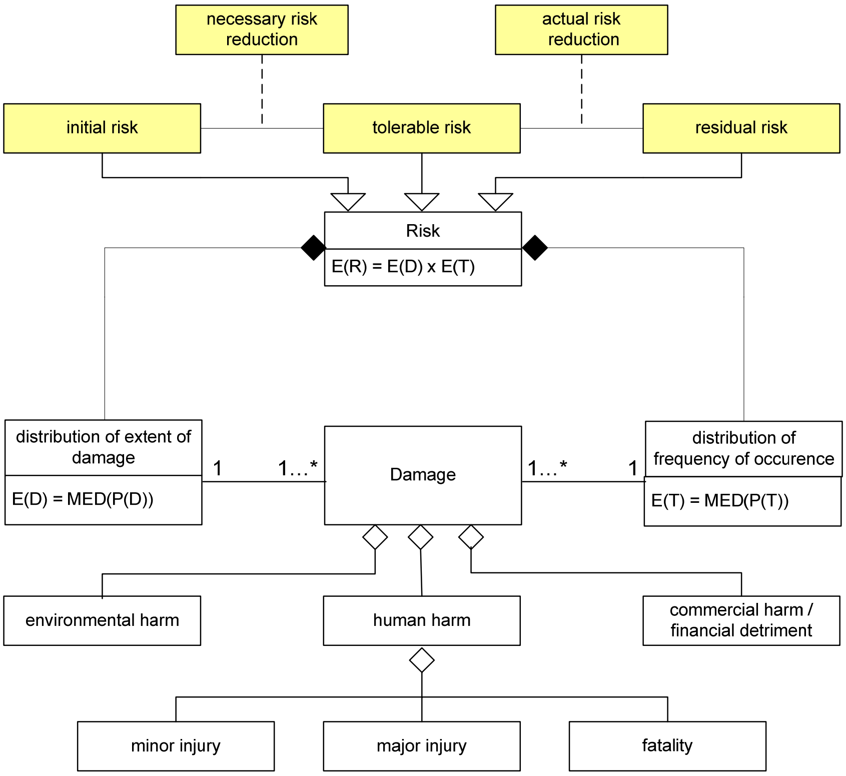

Fig. 3: Risk as a concept system

4. THE SAFETY CONCEPT

ISO/IEC Guide 51 contains a generic chain of causation. In order to understand this, the following concepts are introduced:

- *Hazardous event:* event that can cause harm (EN 1050). The failure of safety-related electronic system for signaling can be considered as a hazardous event. A signal passed at danger (SPAD) can be seen as such a precursor safety occurrence - an event which could, under specific circumstances, lead to an accident such as a collision between trains. The frequency of occurrence may be referred to with the term "hazard rate" which is defined as "rate of occurrence of a hazard" in CLC/TR 50126-2
- *Hazard:* potential source of harm
- *Hazardous situation:* circumstance in which people, property, or the environment are exposed to one or more hazards. This definition already implies the coincidence of a prevalent hazard and the presence of unimpaired assets.
- *Harmful event:* occurrence in which a hazardous situation results in harm. The harmful event can be attributed with its probability of occurrence, which can be either predicted or empirically tested. This rate is required to quantify the *risk* associated with railway operations. The probability that the unimpaired asset is impaired depends on the hazard duration and the exposure time of the individual to the hazards. This probability reflects the possibility that the hazard already exists when the individual enters the system as well as the possibility that the hazard occurs while the individual is exposed (Mokkapati 2004). In the case of a SPAD it becomes obvious that the actual *risk* of collision following the SPAD depends on many factors including whether the train travelled into another section of track and whether that section was occupied.

- *Harm:* physical injury or damage to the health of people, or damage to property or the environment. The harm can be further attributed with its severity. This attribute besides *probability of occurrence* is required to quantify the *risk* associated with railway operations.
- *Risk:* combination of the probability of occurrence of harm and the severity of that harm. As a random variable the loss frequency can be described by its probability distribution which assigns probabilities to events of different frequencies. The same applies to loss severity, which also can be described by its probability distribution. In this case probabilities are assigned to events of different severities.

Nota bene: The term "hazardous event" is used but not defined in the European standards for safety-related electronic systems for railway signalling. The lack of this definition contributes to the inconsistent use of this term throughout this standard series: "in most cases, the term has been used in the standard to mean an 'accident' and should be interpreted as such" (see CLC/TR 50126-2). This has the consequence that currently the standards do not make a sufficiently clear distinction between the fundamental terms "hazard rate" and "risk". This is deemed inacceptable as this leaves unclear which metric serves as a reference value for the process of risk assessment and risk reduction described in section 6.

Figure 4 provides an overview of the safety concept system introduced in ISO/IEC Guide 51. In this figure the terms used in ISO Guide 51 are arranged according to their causal relation by using the Petri-net notation previously introduced. Since each place and each transition of the Petri-net are concepts themselves they can be further described with their intension. For this reason figure 4 refines the concepts with their properties and (physical) quantities.

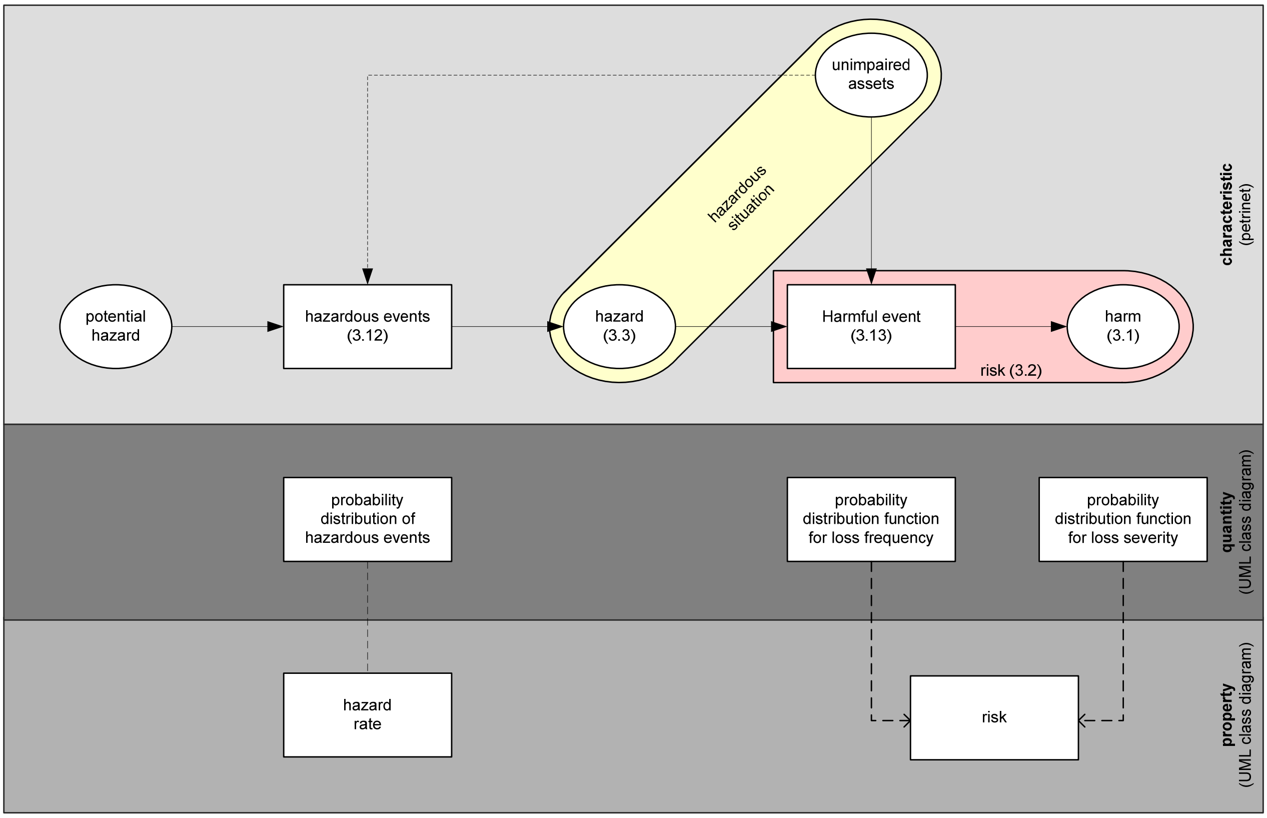
unimpaired assets
hazardous situation
characteristic (petrinet)
potential hazard
hazardous events (3.12)
hazard (3.3)
Harmful event (3.13)
harm (3.1)
risk (3.2)
probability distribution of hazardous events
probability distribution function for loss frequency
probability distribution function for loss severity
quantity (UML class diagram)
hazard rate
risk
property (UML class diagram)

Fig. 4: Formalization of the safety terminology of ISO/IEC Guide 51

Safety-related electronic systems for railway signaling include hardware and software aspects. To install integrated safety-related systems both parts within the whole life-cycle of the system have to be taken into account.

- EN 50128 provides a framework of methods which need to be used in order to provide *software* which meets the demands for safety integrity which are placed upon it. This standard identifies techniques and measures for 5 levels of software safety integrity.
- EN 50129 provides the requirements for safety-related hardware as it includes procedures relating to electronic hardware components.

5. THE "SECURITY"-CONCEPT

According to EN 50126 security, as an element that characterises the resilience of a railway system to vandalism and unreasonable human behaviour, can be considered as a further component of RAMS(S). However, consideration of security is outside the scope of that standard.

Prevention, including the avoidance, detection and deterrence of risk and threats to security of processes begins with the objective of protecting assets (human, physical or environmental) in the design processes. As already discussed in relation with the term "safety" security also is not absolute. Some risk will remain (residual risk). Therefore a product, process or service can only be relative secure. Security is achieved by reducing risk to a tolerable level (tolerable risk). Tolerable risk is achieved by the iterative process of risk assessment and risk reduction beginning in the design phase. The initial risk can be reduced by inherent incorporation of security in design (EN 50159-2 contains guidelines for defences against deliberate attempts to insert incorrect messages into safety-related railway applications). In case the risk remaining after design still is above the tolerable risk, other measures have to be taken by the user (e.g. personal protective devices). Taking into consideration the assumption that the user has a role to play in risk reduction the residual risk should finally be below the tolerable risk.

Similar to the discussion of the term "safety" in the previous section the terminology of the ISO/IEC Draft Guide for the inclusion of security aspects in standards can also be visualized in a concept system (see figure 5). In order to understand this, the following concepts are introduced:

- *threatening event (attack):* attempt to destroy, expose, alter, disable, steal or gain unauthorized access to, or make unauthorized use of anything that has value to an organization (ISO/IEC 27000). Penetrations (unauthorized act of bypassing a security mechanism of a cryptographic system) and sabotage are possible examples of an attack.
- *threat:* potential cause of an unwanted incident which can result into harm to individuals, a system or organization, the environment or the community (ISO/SMB/3971)
- *unimpaired asset:* anything that has value to an organization. There are many types of assets including information, software, physical assets, services, people and intangibles such as reputation and image (ISO 27000).

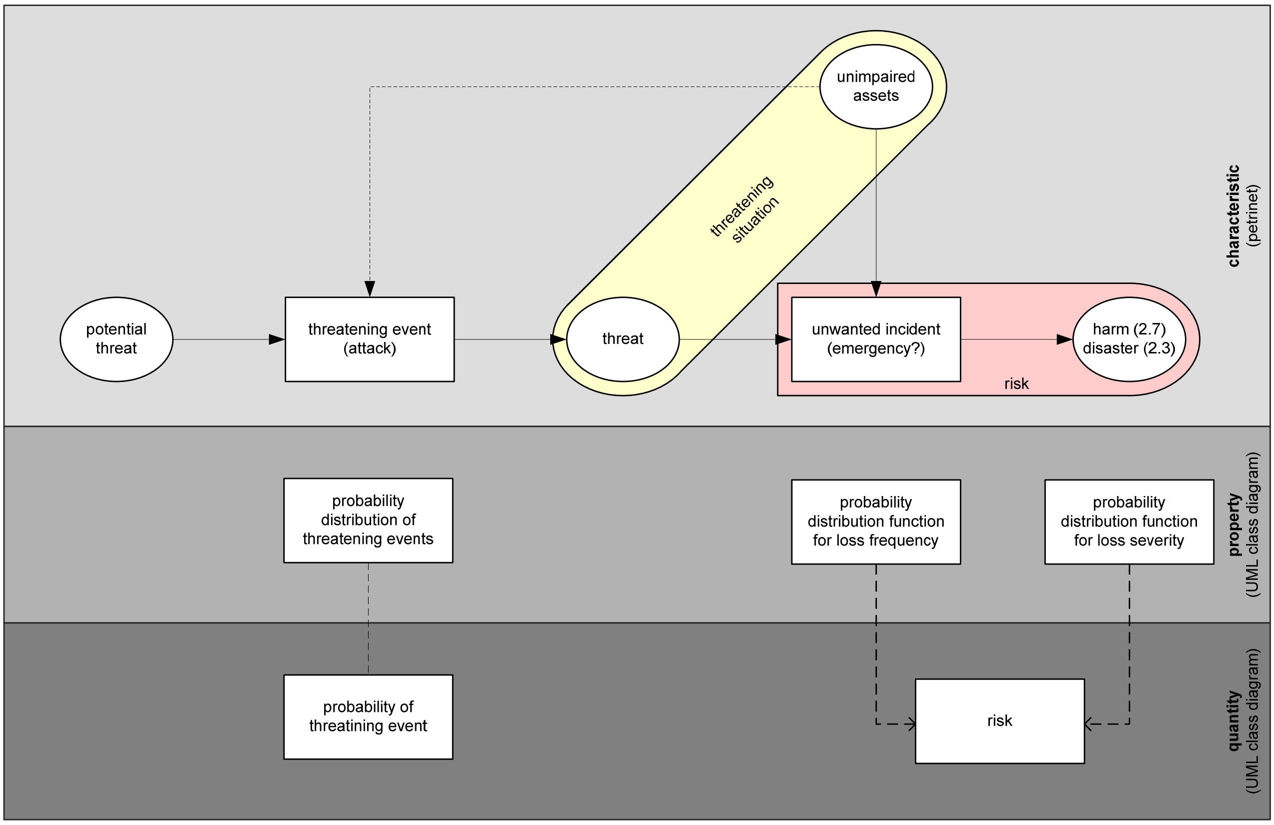
unimpaired assets
threatening situation
characteristic (petrinet)
potential threat
threatening event (attack)
threat
unwanted incident (emergency?)
harm (2.7) disaster (2.3)
risk
probability distribution of threatening events
probability distribution function for loss frequency
probability distribution function for loss severity
property (UML class diagram)
probability of threatining event
risk
quantity (UML class diagram)

Fig. 5: Formalization of the security terminology of the ISO/IEC Draft Guide

6. THE PROCESS OF RISK ASSESSMENT AND RISK REDUCTION

There is a general agreement, that absolute safety is not achievable. Despite the application of protective measures some level of risk will remain which is referred to as residual risk. A process, product or service can only be relatively safe. Safety is achieved by reducing risk to a tolerable level. The procedure applied to do this is outlined in this section (see figure 6). The Petri-net notation applied in this figure has the following advantages:

- By means of the Petri-net notation activities (transition) and their results (places) can be clearly distinguished. The use of this formal notation introduces terminological rigour and helps to avoid terminological inconsistencies.

- Besides the causal relations also hierarchical concept relations can be made explicit by using the Petri-net notation. Petri-nets are well-suited to express the compositionality of complex expressions. By means of decomposition (e.g. the complex process of risk analysis is broken down into its basic constituents) the meaning of a complex expressions can determined by the meanings of its constituent expressions and the rules used to combine them.

- The process model depicted in figure 6 links the process of risk assessment and risk reduction to the risk concept system shown in figure 3.

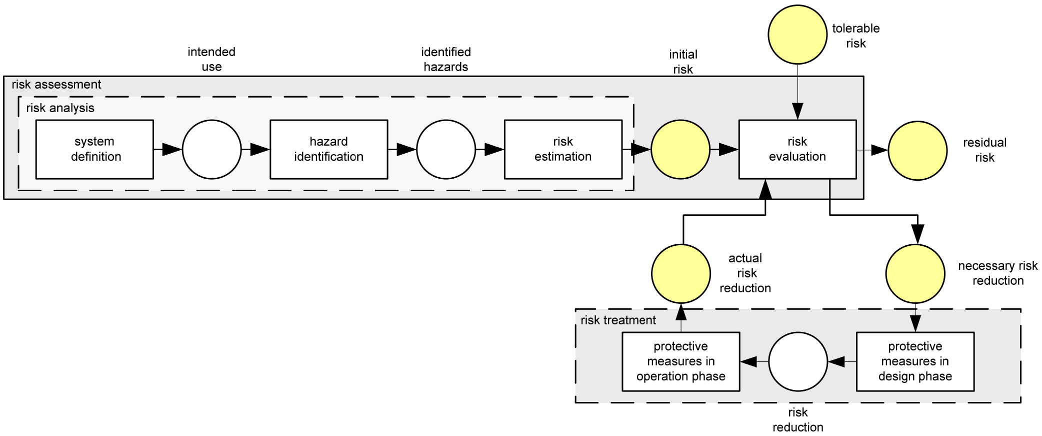

Fig. 6: Iterative process of risk assessment and risk reduction (risk control)

- *System definition* covers both the definition of the *intended use* and the reasonably foreseeable misuse of the product. The use of a product, process or service in accordance with the information provided by the supplier is referred to as the intended use whereas the use of a product, process or service in the way not intended by the supplier and which may result from readily predictable human behaviour is referred to as *reasonably foreseeable misuse*.
- *Hazard identification* is the process to find, list and characterize possible sources of harms. Hazard identification refers to the identification of hazardous situations and harmful events arising in all stages and conditions for the use of the product, process or service, including installation, maintenance, repair and destruction/disposal. At this stage methods include:
  - evidence based methods, examples of which are check-lists and reviews of historical data;
  - systematic team approaches where a team of experts follow a systematic process to identify risks by means of a structured set of prompts or questions;
  - inductive reasoning techniques such as HAZOP.
- *Risk estimation* is the task to quantify risk. According to ISO-Guide 73 it is the process used to assign values to the probability and consequences of a risk. This term is used but not defined in ISO-Guide 51.
- *Risk evaluation* is the process of comparing the estimated risk against a given risk acceptance criterion (tolerable risk according to ISO Guide 51) to determine the significance of the risk, thus risk evaluation is used to assist in the decision to accept or to counteract a risk. In the railway domain risk acceptability is referred to by the ALARP (as low as reasonably possible) or GAME principles (globalement au moins aussi bon). Risk evaluation uses the understanding of risk obtained during risk analysis to make decisions about future actions. Ethical, legal, financial and other considerations, including perceptions of risk, are also inputs to the decision. Decisions may include:
  - whether a risk needs treatment;
  - priorities for treatment;
  - whether an activity should be undertaken;
  - which of a number of paths should be followed.
- *Risk treatment* is the process of selection and implementation of measures to lower risk. Having completed a risk assessment, risk treatment involves selecting and agreeing to one or more relevant options for changing the probability of occurrence, the effect of risks, or both, and

implementing these options. This is followed by a cyclical process of reassessing the new level of risk, with a view to determining its tolerability against the criteria previously set, in order to decide whether further treatment is required (ISO 31010 FDIS). This term can be seen as the superordinate concept of the term risk reduction. This is shown as a transition refinement in the Petri-net notation of figure 6.

- *Risk reduction in the design phase* can be achieved by inherently safe design of the system under consideration. This activity leads to a risk remaining after design (ISO Guide 51).
- *Risk reduction in the operation phase* is based on the assumption that the user has a role to play in the risk reduction procedure. In this phase risk reduction can be achieved by personal protective equipment or organizational measures. Risk reduction in the operation phase leads to the residual risk (ISO Guide 51).

7. CONCLUSION

During reviewing different safety-related standards in the normative framework following deficits and inconveniences have been identified:

- *Incoherence:* During the last decade international standardization set out a comprehensive framework for risk management. ISO Guide 73 published in 2002 sets out a generic framework for risk management inside an organization. With respect to safety this generic framework is refined by ISO Guide 51 published in 1999. With respect to security the generic risk management framework is refined by ISO SMB/3971/DC recently published as a first draft. This clearly demonstrates that the discussion of methodical approaches for security lags behind the discussion of safety. Due to the time delays between the preparation of those guides this framework currently is incoherent. In order improve coherence the existing guidelines should be reviewed in order to strengthen the logical connections between those guides.

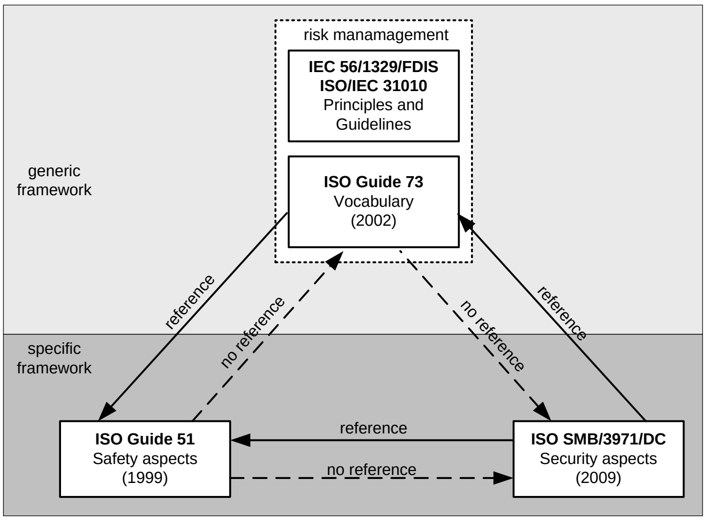

Fig. 7: Normative framework for risk management

- *Terminological deficits:* All three guidelines show terminological deficits. Firstly the terminology of all three guidelines is incomplete as core concepts are not defined (e.g. danger, asset). Secondly the terms are not explicitly related to one another. Due to this lack of a concept system there still are inconsistencies between the concepts and their definitions. Furthermore in-depth analysis reveals that the generic risk management framework has a different understanding of the key concepts of "risk assessment" and "risk analysis".

For the *legislatory framework* the following deficits have been identified:

- *Inconsistencies:* ISO Guide 73 defines a *risk management system* which is referred to as a set of elements of an organization's management system concerned with managing risk. Following ISO Guide 73 this management system contains elements like strategic planning, decision making and other processes for dealing with risk. The Safety directive 2004/49/EC defines the term *safety management system* which means the organisation and arrangements established by an infrastructure manager or a railway undertaking to ensure the safe management of its operations. It is not clear if both terms can be used synonymously. Further analysis is required with respect to the delimiting characteristics. Only an in-depth terminological analysis can reveal differences in those concepts.

With the help of the methodical framework outlined in the first part of the paper it could be demonstrated, that railway safety and security are two sides of the same coin:

- Both concepts have the ultimate goal to protect humans, physical assets, financial assets or a combination thereof. Thus they target the freedom from any unacceptable risk. The key difference is the trigger for the chain of causation which finally leads to the physical injury or damage to health of people, or damage to property, the community, or the environment. In the case of "safety" the triggering condition is regarded to come from within the system (it can be explained by the system's inherent properties of reliability and maintainability). In the case of "security" it is usually seen to penetrate the system boundary from outside. In case the threat comes from within the system it stems from intentional misuse.
- Both safety and security require a structured risk management procedure. This calls for the same coordinated activities to gain control of potential adverse effects. The generic approach of the subsequent steps of risk analysis, risk assessment and risk treatment is valid in both cases.

With the help of the methodical approach outlined in this paper the two guidelines for safety and security aspects could be compared. The method also helped to identify inconsistencies and deficits of the currently existing terminology in this area. In the future this approach could help to reach a convergence of the currently separated safety and security aspects.

REFERENCES

ASD-STE 100: Aerospace and Defence Industries Association of Europe: *ASD-STE 100 Simplified Technical English: International Specification for the preparation of maintenance documentation in a controlled language*. ASD, Brussels, 2007.

Carnap, R. (1999). *Der logische Aufbau der Welt.* Weltkreisverlag; first edition 1928, Weltkreisverlag, Berlin-Schlachtensee.

DIN-Fachbericht 144:2005-08: *Safety, precaution and avoidance in technique* (German edition). Beuth-Verlag, Berlin, 2005.

CLC/TR 50126-2: *Railway Applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Guide to the application of EN 50126-1 for safety.*

EN 1050:1997-1*: Safety of Machinery, Prinicples for risk assessment (English version of DN EN 1050).* Beuth Verlag GmbH, Berlin, 1997.

EN 50126:1999: *Railway applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS).* Beuth-Verlag, Berlin, 1999.

EN 50128:2001: *Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems*. Beuth-Verlag, Berlin, 2001.

EN 50129:2003: *Railway applications - Communications, signalling and processing systems - Safety related electronic systems for signaling.* Beuth-Verlag, Berlin, 2003.

EN 50159-2:2001: *Railway applications - Communication, signalling and processing systems - Part 2: Safety related communication in open transmission systems.* Beuth-Verlag, Berlin, 2001.

Finch, Geoffrey: *Linguistic Terms and Concepts*. Barsingstoke, Palgrave, 2000.

Gooch, John C.: *The Dynamics and Challenges of Interdisciplinary Collaboration: a Case Study of "Cortical Depth of Bench" in Group Proposal Writing.* IEEE Transactions on Professional Communication 48(2):177-190, 2005.

ISO/IEC Guide 51:1999: *Safety aspects - Guidelines for their inclusion in standards.*Beuth-Verlag, Berlin, 1999.

ISO/IEC Guide 73:2002: *Risk management – Vocabulary – Guidelines for use in standards.* Beuth Verlag, Berlin, 2002.

IEC 56/1329/FDIS ISO/IEC 31010 Ed. 1.0: *Risk Management – Risk Assessment Techniques.* International Organization for Standardization, Geneva, 2009.

IEC 61508-5:1998: *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels.* Beuth Verlag, Berlin, 1998.

ISO: SMB/3971/DC: *ISO/IEC Draft Guide: Guidelines for the inclusion of security aspects in standards.* International Standardisaton Organisation, Geneva, 2009.

ISO/TR 24156:2008: *Guidelines for using UML notation in terminology work.* Beuth Verlag GmbH, Berlin, 2008.

ISO 704:2000-11. *Terminology work – Principles and methods.* Beuth Verlag GmbH, Berlin, 2000.

ISO 860:2007-11: *Terminology work – Harmonization of concepts and terms.* Beuth Verlag GmbH, Berlin, 2007.

ISO 1087-1:2000-11: *Terminology work – Vocabulary – Theory and application.* Beuth Verlag GmbH, Berlin, 2000.

Lorenzen, P. (1987). *Lehrbuch der konstruktiven Wissenschaftstheorie.* BI Wissenschaftsverlag, Mannheim, 1987.

Mokkapati, C. (2004). *A practical risk and safety assessment methodology for safety-critical systems.* In: Proceedings of the AREMA 2004 C&S Technical Conference, Nashville (Tennessee) May 17-18, 2004; http://www.arema.org/eseries/scriptcontent/custom/e_arema/library/2004_Conference_Proceedings/00042.pdf (retrieved on August 16th 2009).

Saussure, Ferdinand de (2006): *Writings in General Linguistics*. Oxford University Press, Oxford, 2006.

Schnieder, E. and Drewes, J. (2008): *Merkmale und Kenngrößen zu Bemessung der Verkehrssicherheit.* Zeitschrift für Verkehrssicherheit 54(3):117-123, 2008.

Schnieder, E. and Jansen, L. (2001): *Begriffsmodelle der Automatisierungstechnik – Basis effizienten Engineerings*. In: Schnieder, Eckehard (Herausgeber): Engineering komplexer Automatisierungssysteme, 7. Fachtagung Entwurf komplexer Automatisierungstechnik, Pages 1-37. Braunschweig, 2001.

Schnieder, E. and Schnieder, L. (2009): *Ein formalisiertes Begriffssystem zur Zuverlässigkeit – Grundlage fehlerarmer Kommunikation.* Tagung Technische Zuverlässigkeit, Stuttgart 2009.

Van Schrick, D. (2002). *Entepetives Management – Konstrukt, Konstruktion, Konzeption – Entwurf eines Begriffssystems zum Umgang mit Fehlern, Ausfällen und anderen nicht erwünschten technischen Phänomenen.* Shaker-Verlag, Aachen.