ON THE RELATIONSHIP OF HAZARDS AND THREATS IN RAILWAY SIGNALING

J. Braband, M. Seemann

Siemens AG, Braunschweig, Germany, {jens.braband|markus.seemann}@siemens.com

Keywords: hazard, threat, safety, security, railway signaling

Abstract

This paper discusses the relationship of hazards and threats in railway-related safety and security standards. It points out similarities but also gaps and proposes improvements. It is shown that, in particular, the approaches to risk analyses and the definition of safety and security differ substantially so that these processes should be treated separately. The general goal should be the separation of safety and security concerns as far as possible, which might help in the integration and maintainability of safety and security certificates. A particular goal could be to use certified COTS security components also in the railway signaling domain, instead of creating a new certification framework.

1 Introduction

Some recent incidents indicate that possibly the vulnerability of IT systems in railway automation has been underestimated. Fortunately, so far, almost only denial-of-service attacks have been successful, but, due to several trends such as the use of commercial IT and communication systems or privatization, threat potential could increase in the near future. However, up to now, no harmonized IT security requirements for railway automation exist, but security issues have already been recognized as an issue in railway signaling standards, such as EN 50129 [9] and EN 50159 [8].

The purely safety aspects of electronic hardware are covered by EN 50129. However, security issues are taken into account by EN 50129 only as far as they affect safety issues, but, for example, denial-of-service attacks often do not fall into this category. In particular, the safety case from EN 50129 contains a chapter concerning the prevention of unauthorized access and EN 50159 deals with security issues in communications.

In safety standards, a hazard is often defined as “a condition that could lead to an accident” and traditionally safety only deals with unintentional causes such as hardware failure or software faults. Although the definition of a threat in many security standards is like “a potential cause of an unwanted incident, which may result in harm to a system or organization”, it is clear that security mainly focuses on intentional causes, e.g. attacks.

The first version of EN 50159 was elaborated in 2001. It has proved quite successful and is also used in other application areas, e.g. industry automation. This standard considers intentional as well as accidental threats and countermeasures to ensure safe communications in railway systems. So, this standard has, at an early stage, established methods to build a safe tunnel through an insecure environment. However, the threats considered in EN 50159 arise mainly from technical sources or the environment rather than from human beings. The methods described in the standard are partially able to protect the railway system also from threats arising from intentional attacks, but not completely. Until now, additional organizational and technical measures have been implemented in railway systems as, for example, separate networks, etc., to achieve a sufficient level of protection.

It is only recently that activities have been started in railway signaling to apply IT security approaches such as the Common Criteria (CC) [3,4,5] or IEC 62443/ISA99 [6,10], e.g. to derive railway-specific protection profiles [13]. From these standards, it can be learnt that for information security not only technical aspects of specific technical systems need to be taken into account, but also circumstances, organization, humans, etc. Certainly, not all elements mentioned in the general IT security standards can and need to be applied to railway systems.

The typical process as defined in the CC to derive security functions is very similar to the EN 50129 process for the derivation of safety requirements. In a first step, assumptions, threats and information about the organizational security policy have to be derived. This leads to a list of resulting security objectives which are the basis for setting security requirements.

This paper discusses the relationship between hazards from railway signaling standards and threats from IT security standards including typical assumptions in the railway domain and compares the threats to security-related hazards which have been identified in the safety standards. An approach is proposed to integrate the hazards and threats identified in both approaches.

In addition, the approaches towards risk analysis in security and safety are compared. Although the approaches seem similar at first glance, it is shown that the parameters and principles are quite different and are to be treated separately.

The general goal is to aim at the separation of safety and security concerns as far as possible, which might help in the integration and maintainability of safety and security certificates. A particular goal could be to use COTS security components, which can be certified according to the Common Criteria or ISA 99, also in the railway signaling domain, instead of creating a new certification framework.

2 Hazards and threats

2.1 Definition of hazards and threats

From a simplified point of view, safety addresses *protection of the system environment* against unintended (hazardous) operation of the system, whereas security addresses *protection of the system assets* against intentional or accidental violation (threat action).

More precisely, in safety standards (e.g. [8,9]), a *hazard* is defined as "a condition that can lead to an accident". Being a potential cause of an accident, a hazard can always be described as an unintended system output to the system environment. Within a safety risk analysis of the operational environment according to EN 50129, hazards are identified for each system function and a tolerable hazard rate (THR) and a safety integrity level (SIL) is assigned. Hazards, THRs, and SILs depend on the technical functions and the operational environment only.

For the evidence that a given system fulfils the required THRs and SILs, often unintentional causes such as hardware failure, software faults or human errors are analyzed, only. Intentional causes such as unauthorized access are sometimes excluded by operational or organizational application rules.

In security standards (e.g. [6,7,12]), a *threat* is mainly defined as "potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm". Since harm is the violation of an asset, a threat can be seen as potential for an intentional or accidental violation of an asset.

This definition of a threat complies with the definition according to EN 50159, i.e. "potential violation of safety". Since the scope of EN 50159 covers the effects of threats regarding the asset *safety* in communication links, this definition of threats fits into the above-mentioned security standards.

2.2 Identification process for threats

At the beginning of any security analysis, there is a need for identification of the system under consideration and its interfaces to the environment, of its assets which are to be protected, and of all the possible threats which have the potential to harm these assets. Identification of the assets is highly subjective depending on the objectives of the stakeholders of the considered system. Almost anything could be an asset. For the identification of threats, often only brainstorming and / or proprietary checklists are used.

In most security analysis processes, it is presumed that these identifications have already been done. In [11], some structuring hints are given regarding these topics. Figure 1 cites part of the general model used in [11] regarding the identification of assets and threats.

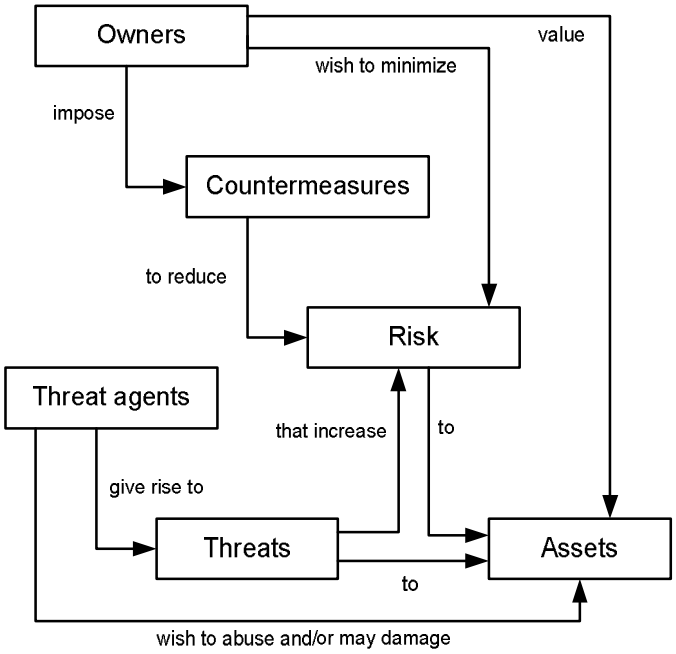

Figure 1: Security concepts and relationships [11]

Based on the identified assets and threats as input, [11] describes a detailed process to derive and tailor suitable security requirements to be implemented by the system and / or by the system environment. This process can be used to generate sets of security requirements for the intended application, either implementation-independent for groups of products (i.e. protection profiles and packages) or implementation-specific for certain products (i.e. security targets). Note that the process contains a number of plausibility checks ensuring the coverage of threats and security objectives.

2.3 Comparison of threats between EN 50159 / EN 50129 and Common Criteria

In railway signaling, the starting point is EN 50129 where the safety case explicitly demands addressing the aspect of unauthorized access (physical and / or non-physical), which is a security aspect on a very technical level. In general, threats could be described on a higher system level, but many security threats that have a safety impact could be addressed under this safety hazard. Questions like intrusion protection are only covered by one requirement in Table E.10 (protection against sabotage). Nevertheless, EN 50129 provides a structure for a safety case which explicitly includes

a subchapter on protection against unauthorized access (both physical and informational). Other security objectives could also be described in that structure.

Unfortunately, all threats related to denial-of-service type attacks are missing in EN 50129 as the CENELEC standards strictly distinguish between RAM and safety and the only standard dealing with both is EN 50126. Unfortunately, EN 50126 explicitly does not address security issues and so at least threats leading to denial of service are not covered well by the CENELEC standards.

Generally, the threats can be categorized into threats which are to be taken care of by the target of evaluation (the technical system) and threats which have to be dealt with by the safety system or the environment. Subsequently, also security requirements are derived for the technical systems and the environment. Requirements related to the environment could be communicated through safety-related application rules (SAR) which is a well established concept in the CENELEC standards to ensure that such requirements are enforced in applications.

Some threats regarding communication issues can be taken from EN 50159 which explores in detail security issues inherent to communication networks. In EN 50159, the threats are also divided into accidental (1.-6.) and intentional (7.) ones, i.e.:

1. repetition
2. deletion
3. insertion
4. re-sequencing
5. corruption
6. delay
7. masquerade

All threats relate to messages. With respect to accidental threats, detailed countermeasures and evidence procedures are given. Again, the security issues have been isolated mainly into one threat, masquerade. Unfortunately, this term does not seem to be very common in security standards, so that misinterpretations may occur. Also, in EN 50129, threats related to denial-of-service type attacks are almost neglected.

For a particular application, similar to virtual private networks (VPN), a protection profile (PP) according to the CC has already been drafted [13]. This provides a good opportunity to compare the threats from the protection profile to the threats identified in the CENELEC standards. On the top level of the PP, the following threats related to the technical system providing the VPN tunnel have been identified:

- t.availability: Authorized users cannot obtain access to their data and resources.
- t.entry: Persons who should not have access to the system may enter the system. The initiator of such a threat could be an attacker who masks himself / herself as an authorized user.
- t.access: Authorized users gain access to resources which they are not entitled to according to the IT security policy. The initiator is an authorized user. The system is manipulated by negligence or operating errors.
- t.error: An error in part of the system leads to vulnerability in the IT security policy. An error can also be the result of a failure. The initiator of such a threat can be an attacker.
- t.crash: After a crash, the IT system is no longer able to correctly apply the IT security policy.
- t.repudiation: Incidents which are IT security-related are not documented or cannot be attributed to an authorized user.
- t.manipulation: An IT security-related measure is changed or bypassed. This might be initiated by an attacker.
- t.diagnosis: IT security-related incidents are not diagnosed. The initiator of such a threat can be hardware failures, software errors and the action taken by an attacker.

The major differences seem to be t.availability, which also target denial-of-service attacks, and t.repudiation, which has not been directly considered in the CENELEC standards. t.enty and t.access are covered by the unauthorized access issue in EN 50129 and also t.error, t.crash or t.diagnosis would be considered in a safety context. t.diagnosis is closely related to a requirement from EN 50159 demanding that any failure of security functionality must be detected. t.manipulation may be considered to be a particular threat leading to unauthorized access and is very similar to the masquerade threat from EN 50159. More details can be found in [1,13].

As already mentioned in Section 2.1, unintentional causes such as hardware failure, software faults or human errors which are all sufficiently addressed by the safety standards [8,9] can be seen as accidental threats to the asset *safety* according to the security standards (like the CC). The obviously safety-related threats are covered quite well, but the indirectly safety-related threats are not explicitly covered.

How can this gap be bridged? The bridge is provided by Commission Regulation No. 352/2009 on common safety methods [2]. This Commission Regulation mentions three different methods to demonstrate that a railway system is sufficiently safe:

a) by following existing rules and standards (application of codes of practice)
b) by similarity analysis, i.e. showing that the given (railway) system is equivalent to an existing and used one
c) by explicit risk analysis, where risk is assessed explicitly and shown to be acceptable.

Using the approach under a), for example the Common Criteria [3,4,5] can be used in railway systems. By this

approach, a code of practice that is approved in other areas of technology and provides a sufficient level of security there is then adapted to railways. This ensures a sufficient level of safety.

However, application of the general standard [11] requires tailoring it to the specific needs of a railway system. This is necessary to cover the specific threats associated with railway systems and possible accidents and to take into account specific other risk-reducing measures already present in railway systems, e.g. the use of specifically trained personnel.

A new German security standard [13] is elaborated within the scope of safety-related communications. This will enable systems to be re-used for railway applications that have already been assessed and certified for other areas of applications. This is especially relevant as an increasing number of COTS products is used and certified against the Common Criteria. With this approach, a normative base can be developed, based on the Common Criteria and a specific protection profile tailored for railways, considering railway-specific threats and scenarios and yielding a set of IT security requirements. The assessment and certification of such a system can be carried out by independent expert organizations. Safety approval in Germany could then be achieved via the Federal German Railways Office (EBA) for railway aspects and Federal German Office for Security in Information Technology (BSI) for IT security aspects.

3 Approaches to risk analysis

At first glance, risk is defined in safety and security as quite similar in terms of expected loss, technically evaluated as a combination of the frequency and severity of the occurrence of an unwanted event. In both domains, risk is often evaluated by a risk matrix for these parameters.

Whereas, for safety applications, failure rates can be estimated quite well as considerable operational experience and data are often available, the situation is quite different in the security field. The first difference is that, in the safety field, the environment is quite stable and field data from the past can be used to predict future failure behavior. Major technological innovations which may change the situation often take decades, in particular in the railway field. In the security field, the situation sometimes changes quite rapidly after accidents or incidents, e.g. after the 9/11 incident in civil aviation or after the occurrence of new viruses or malware. Just imagine that a new approach towards cryptanalysis might be discovered. Secondly, at least some of the effects that affect safety, e.g. hardware failure and also software failure to some extent, originate from physical phenomena and can be predicted by reliability theory. In security, we deal with intentional attacks which are much harder to predict and do not follow known physical laws.

In our opinion, it is thus very questionable that the same means for risk estimation are used in both fields. Last but not least, we predominantly counteract criminal behavior in the security domain, while in the safety domain we deal with unintended human errors and technical failures. This problem is fully acknowledged only by a few security standards, e.g. ISA99: “Threat Risk Assessment (TRA), in particular with respect to electronic attack on computer systems connected to unsecured or untrusted networks, are at this time not amenable to mathematical-statistical analysis, i.e., malicious human attacks are purposeful and do not have the statistical property of random failure events. Thus extrapolating from historical data (as generally possible with random failures) cannot predict the future probability of human attack. For this reason, the likelihood of security-related occurrences may elude a purely statistical approach forever. While there are many TRA models available, none has been widely accepted. Quantitative methods are misleading.”

In order to come up with a new approach towards the evaluation of security risk, we first take a qualitative look at the parameters influencing this risk, see Figure 2. In a first step, we simply describe whether factors have a negative or positive impact on each other, leaving out the obvious links.

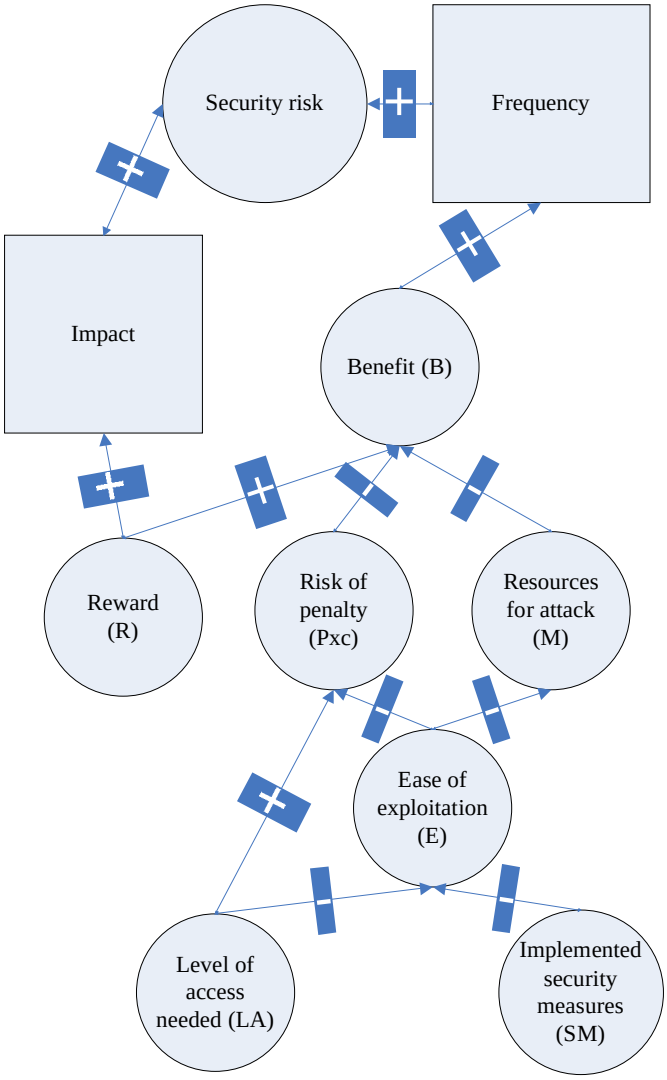

Figure 2: Qualitative interpretation of security risk

Figure 2 depicts additional relationships between the parameters: the higher the level of access needed, the higher the probability of becoming caught, or the higher the ease of exploitation, the lower the resources needed.

The impact of a security threat is more or less correlated to the reward the attacker receives from a successful attack: the higher the impact, the higher the reward, in either monetary terms or non-monetary terms, e.g. publicity. The estimated net benefit the attacker gains from a successful attack is positively correlated to the frequency of attacks. We think that the net benefit can be simply estimated by a rough cost-benefit approach

$$B = R - P \cdot c - M \,. \qquad (1)$$

where B stands for the net benefit, R for the average reward, P for the average penalty if the attacker is sentenced, c for the probability that an attacker is caught and M for the means or effort the attacker has to invest for a successful attack. If the net benefit is significantly larger than zero, we will be facing a large number of attacks, so the goal of risk analysis must be to keep the net benefit negative. On the technical side, there are two parameters that can be influenced by the implemented security measures: first to increase the effort the attacker has to invest and to increase the probability of becoming caught.

In summary, the security risk assessment results in the assignment of a kind of security level (SL), which is a quality measure for the implemented security measures that should be derived by

$$SL = f(R, E) \text{ or} \qquad (2)$$

$$SL = f(R, c, LA). \qquad (3)$$

This means that the type and strength of the security measure should be determined as a function of the average reward R and the ease of exploitation E, which could be described by sub parameters such as the probability of becoming caught c and the level of access LA needed. We have assumed that penalties cannot be changed as part of a risk assessment. It should be noted that c and LA are not independent and that the approach could possibly be simplified by the identification of common factors between the parameters. However, it does not seem reasonable to measure the risk in IT security in the same way as the risk in safety, as the quantitative assessment of IT security threats does not seem to be justified.

The big question is what is measured by SL. In safety applications, the safety integrity level (SIL) is related to the required risk reduction by the safety function in order to reach an acceptable level of residual risk. From Figure 2, we can conclude qualitatively that the effectiveness of SM should be measured in terms of the probability to catch or trace an attacker and the effort needed for a successful attack. So, SM should rather be measured in terms of effort than in risk reduction. As the security risks are much harder to quantify than safety risks, it is immediately clear that semi-quantitative or qualitative methods have to be used such as risk matrices or risk priority numbers. A simple approach could be defined by a particular risk matrix for each LA (in particular remote access) which combines R and E. This clearly underpins that safety and security need different approaches towards risk analysis and those methods from the safety field cannot simply be re-used.

For determination of the level of security, it should also be evaluated what kind of alternative attacks are possible, e.g. physical attacks, and what would be their corresponding net benefit. A reasonable attacker would not launch an IT security attack if its net benefit would be much lower than the net benefit of a physical attack.

4 Review of security levels

The most important SL today seems to be the evaluation assurance levels (EAL) from the CC and the security assurance levels (SAL) from ISA99.

The EAL provide an increasing scale from EAL1 to EAL7 “that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance”. So, EAL is rather a concept which rates the trust or confidence in correct implementation of the security measures than their effectiveness to withstand attacks. Thus, it is not sufficient in itself to define the necessary level of security as demanded as a result of the risk analysis. The strength of the solution against exploitation against an attack scenario must be part of the security requirements. This means that, in the CC, the security level is defined by the type and strength of the security functions and the trust in their implementation (only the latter aspect being expressed by the EAL).

The SAL of ISA99 define “a set of security controls which if implemented and determined to be effective in their application, would most cost-effectively mitigate risk while complying with the specific security requirements.” They are specified on four increasing levels which can be specified differently for the following top IT security requirements: access control, use control, data integrity, data confidentiality, restrict data flow, timely response to an event, network resource availability. So, for a given application, an SAL is a seven-dimensional vector containing numbers from 1 to 4. As a matter of fact, a family of SAL is defined: system target SAL-T, system design SAL-D, achieved SAL-A and capability SAL-C. It should be noted that this concept differs from the EAL or SIL concept, where only a single number is allocated.

SAL-T is defined by impact only, e.g. SAL-T 1 is related to “a limited adverse effect”, while SAL-T 4 relates to “a catastrophic adverse effect”. Thus, SAL-T relates to impact only. For each requirement, SAL-T is then translated into system capability SAL-C. For example, for data confidentiality, SAL-C 1 requires the protection of data

integrity “against casual or coincidental manipulation”, while SAL-C 2, 3 and 4 require the prevention of dissemination against an attacker who actively searches using “simple means”, ”sophisticated means” or ”sophisticated means with extended resources”, respectively. So, SAL-T and SAL-C could be indirectly seen as a kind of risk matrix determining the acceptable security risk as a function of impact and means of exploitation, which is very similar to the approach given by (2), see Table 1 for an extrapolation. The interpretation is that, for a given impact, it is required to cope with a particular level of exploitation E, but no more (designated “n. r.” (not required) in Table 1). The diagonal of the risk matrix gives the limits of acceptability of a SAL for the given impact and level of exploitation.

Extended resources	n. r.	n. r.	n. r.	SAL 4
Sophisticated means	n. r.	n. r.	SAL 3	
Simple means	n. r.	SAL 2		
Casual	SAL 1			
Ease of exploitation / impact	Limited	Serious	Severe	Catastro-phic

Table 1: Extrapolated security risk matrix from ISA99

In summary, the ISA99 approach seems to be closer to the approach given by Figure 2. However, in contrast to the CC, ISA99 is an application-specific standard, which means that the security requirements have already been derived related to industrial automation and control systems. For railway applications, it would be beneficial to be able to use COTS components certified against any of these standards, but, to make this feasible more, the PP according to the CC would have to be created and the suitability of risk acceptance implied by the definition of SAL would have to be checked.

5 Conclusion and outlook

This paper has shown that, while there is already a useful link and broad conceptual overlap between safety and security approaches in railway signaling, some issues need to be addressed in more detail in future, e.g. availability threats from denial-of-service attacks. It has also been argued that there is a consistent misbelief in the communities as well as in a number of standards that safety and security issues can be addressed by the same approaches in risk analysis. A new approach has been proposed which clearly emphasizes that security and safety issues should be separated as far as possible, also with respect to certification. Finally, by reviewing two popular standards, it could be shown that implicitly the new proposal can be brought into line with these standards, so that this direction seems promising for future research work.

References

[1] Bock, H., Braband, J., Milius, B. and Schäbe, H.: “Towards an IT Security Protection Profile for Safety-related Communication in Railway Automation”, to be published in *Proceedings SAFECOMP2012*

[2] Commission Regulation (EC) No. 352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of Directive 2004/49/EC of the European Parliament and of the Council

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. Part 1: Introduction and general model

[4] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. Part 2: Functional security components

[5] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. Part 3: Assurance security components

[6] IEC TS 62443-1-1 Technical Specification, Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models, Edition 1.0, July 2009

[7] IEC TS 62351-2 Technical Specification, Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms, Edition 1.0, August 2008

[8] EN 50159 Railway applications, Communication, signaling and processing systems – Safety-related communication in transmission systems, September 2010

[9] EN 50129 Railway applications, Communication, signaling and processing systems – Safety-related electronic systems for signaling, February 2003

[10] ISA 99, Standards of the Industrial Automation and Control System Security Committee of the International Society for Automation (ISA) on information security, see http://en.wikipedia.org/wiki/Cyber_security_standards

[11] ISO/IEC 15408-1 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model, Third edition, December 2009

[12] RFC 2828 – Internet Security Glossary, http://www.faqs.org/rfcs/rfc2828.html.

[13] VDE 0831-102 Electric signalling systems for railways – Part 102: Protection profile for technical functions in railway signalling, to be issued