Towards an IT Security Protection Profile for Safety-Related Communication in Railway Automation

Hans-Hermann Bock[1], Jens Braband[2], Birgit Milius[3], and Hendrik Schäbe[4]

[1] Deutsche Bahn AG, Berlin, Germany
Hans-Hermann.Bock@deutschebahn.com
[2] Siemens AG, Braunschweig, Germany
jens.braband@siemens.com
[3] TU Braunschweig, Braunschweig, Germany
b.milius@tu-braunschweig.de
[4] TÜV Rheinland, Köln, Germany
schaebe@de.tuv.com

Abstract. Some recent incidents have shown that possibly the vulnerability of IT systems in railway automation has been underestimated so far. 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, the threat potential could increase in the near future. However, up to now, no harmonized IT security requirements for railway automation exist. This paper defines a reference communication architecture which aims to separate IT security and safety requirements as well as certification processes as far as possible, and discusses the threats and IT security objectives including typical assumptions in the railway domain. Finally examples of IT security requirements are stated and discussed based on the approach advocated in the Common Criteria, in the form of a protection profile.

Keywords: Railway, IT Security, Safety, Threats, IT Security Requirements, Protection Profile.

1 Introduction

Recently, reports on IT security incidents related to railways have increased as well as public awareness. For example, it was reported that on December 1, 2011, “hackers, possibly from abroad, executed an attack on a Northwest rail company's computers that disrupted railway signals for two days” [1]. Although the details of the attack and also its consequences remain unclear, this episode clearly shows the threats to which railways are exposed when they rely on modern commercial-off-the-shelf (COTS) communication and computing technology. However, in most cases, the attacks are denial of service attacks leading to service interruptions, but so far not to safety-critical incidents. But also other services, such as satellite positioning systems, have been shown to be susceptible to IT security attacks, leading to a recommendation that

F. Ortmeier and P. Daniel (Eds.): SAFECOMP 2012, LNCS 7612, pp. 137–148, 2012.

GNSS services should not be used as standalone positioning services for safety-related applications [4].

What distinguishes railway systems from many other systems is their inherent distributed and networked nature with tens of thousands of kilometer track length for large operators. Thus, it is not economical to completely protect against physical access to this infrastructure and, as a consequence, railways are very vulnerable to physical denial of service attacks leading to service interruptions.

Another distinguishing feature of railways from other systems is the long lifespan of their systems and components. Current contracts usually demand support for over 25 years and history has shown that many systems, e.g. mechanical or relay interlockings, last much longer. IT security analyses have to take into account such long lifespans. Nevertheless, it should also be noted that at least some of the technical problems are not railway-specific, but are shared by other sectors such as Air Traffic Management [5].

Publications and presentations related to IT security in the railway domain are increasing. Some are particularly targeted at the use of public networks such as Ethernet or GSM for railway purposes [2], while others, at least rhetorically, pose the question "Can trains be hacked?"[3]. As mentioned above, some publications give detailed security-related recommendations [4]. While in railway automation harmonized safety standards were elaborated more than a decade ago, up to now no harmonized IT security requirements for railway automation exist.

This paper starts with a discussion of the normative background, then defines a reference communication architecture which aims to separate IT security and safety requirements as well as certification processes as far as possible, and discusses the threats and IT security objectives including typical assumptions in the railway domain. Finally, examples of IT security requirements are stated and discussed based on the approach advocated in the Common Criteria, in the form of a protection profile.

2 Normative Background

In railway automation, there exists an established standard for safety-related communication, EN 50159 [6]. The first version of the standard was elaborated in 2001. It has proved quite successful and is also used in other application areas, e.g. industry automation. This standard defines threats and countermeasures to ensure safe communication in railway systems. So, at an early stage, the standard established methods to build a safe channel (in security called tunnel) through an unsafe environment. However, the threats considered in EN 50159 arise 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 intentional attacks, but not completely. Until now, additional organizational and technical measures have been implemented in railway systems, such as separated networks, etc., to achieve a sufficient level of protection.

The purely safety aspects of electronic hardware are covered by EN 50129 [7]. 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. Questions such as intrusion protection are only covered by one requirement in Table E.10 (exist protection against sabotage). However, EN 50129 provides a structure for a safety case which explicitly includes a subsection on protection against unauthorized access (both physical and informational). Other security objectives could also be described in that structure.

On the other hand, industrial standards on information security exist. Here we can specify the following standards:

- ISO/IEC 15408 [8] provides evaluation criteria for IT security, the so-called Common Criteria [13 to15]. This standard is solely centered on information systems and has, of course, no direct relation to safety systems.
- ISA 99 [9] is a set of 12 standards currently elaborated by the Industrial Automation and Control System Security Committee of the International Society for Automation (ISA). This standard is not railway-specific and focuses on industrial control systems. It is dedicated to different hierarchical levels, starting from concepts and going down to components of control systems.

A more comprehensive overview on existing information security standards is presented in [10]. From these standards, it can be learnt, that for information security, not only technical aspects of concrete technical systems need to be taken into account, but also circumstances, organization, humans, etc. Certainly, not all elements mentioned in the general information security standards can and need to be used for a railway system.

How is the gap between information security standards for general systems and railways to be bridged? The bridge is provided by the European Commission Regulation on common safety methods No. 352/2009 [11]. 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) similarity analysis, i.e. showing that the given (railway) system is equivalent to an existing and used one,
c) explicit risk analysis, where risk is assessed explicitly and shown to be acceptable.

We assume that, from the process point of view, security can be treated just like safety, meaning that threats would be treated as particular hazards. Using the approach under a), Common Criteria [8] or ISA 99 [9] may be used in railway systems, but a particular tailoring would have to be performed due to different safety requirements and application conditions. By this approach, a code of practice that is approved in other areas of technology and provides a sufficient level of security, can be adapted to railways. This ensures a sufficient level of safety.

However, application of the general standards [8] or [9] requires tailoring them 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, such as the use of specifically trained personnel.

As a basis of our work, the Common Criteria [8] have been selected, as ISA99 was not finalized in spring 2011, when this work started. The use of Common Criteria may enable the reuse of systems for railway applications that have already been assessed and certified for other areas of application. This is especially relevant as an increasing number of commercial-off-the-shelf (COTS) products are being used and certified against the Common Criteria. With this approach, a normative base has been developed by the German standardization committee DKE [17], 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. 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 governmental organizations Federal German Railways Office (Eisenbahn-Bundesamt, EBA) for railway aspects and Federal German Office for Security in Information Technology (Bundesamt für Sicherheit in der Informationstechnik, BSI) for IT security aspects.

3 Reference Architecture

The selected reference architecture refers to the proposed architecture B0 in CENELEC standard EN 50159, which aims at the separation of safety and security concerns. This concept can be illustrated by the onion skin model, where a security shell is placed between the Railway Signaling Technology (RST) application and network layers. It is similar to a layer-of-protection approach. This security shell is the Security Target of Evaluation (TOE) according to the Common Criteria (see Figure 1).

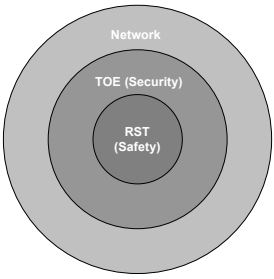

Fig. 1. The onion skin model

Based on this onion skin model a reference model for communication (see Figure 2) has been chosen, in which the RST applications are in a zone A or B. It is assumed that, if communication between the zones were through a simple wire (as a model for a simple and proprietary communication means), then all safety requirements of EN

50159 would be fulfilled. Communication between the two zones will be through a tunnel or conduit in an open network. This is similar to the zone and conduit model in ISA 99 [9], so that in the future this profile may also be used jointly with ISA99.

In order to implement the conduit, additional security components have to be provided which are the physical implementations of the TOE. In Figure 2 the user is a generic representative of security management, which could have many different physical implementations, ranging from manual on-site to automated centralized management.

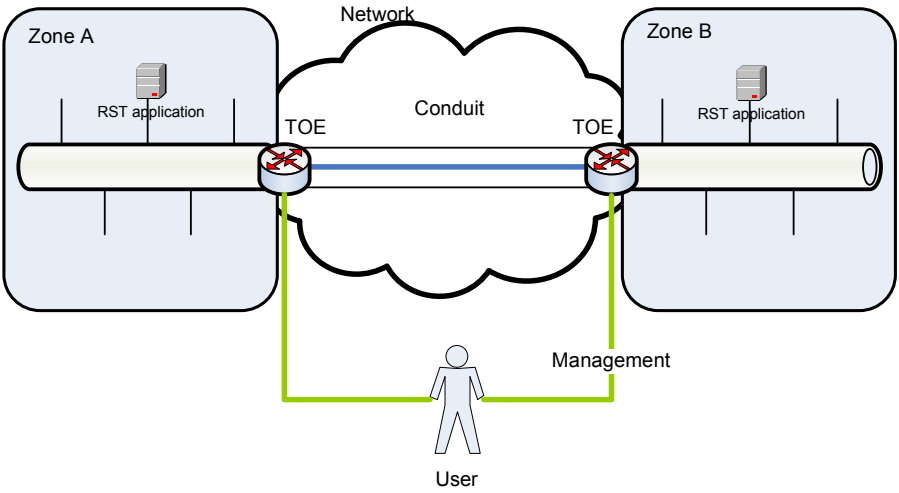

Fig. 2. Zone and conduit reference architecture

As an example, implementations of this reference architecture, Deutsche Bahn AG have long-standing operational experience with security gateway solutions from Siemens [15], where the zones are the centralized traffic control centers and the local interlockings. As a future general solution for a secure communication infrastructure for all safety-critical applications, a pilot project designated KISA [15] is conducted by Deutsche Bahn AG. The protection profile of the TOE provides the basis for evaluating a product solution and the necessary safety approval for use.

4 Assumptions, Threats and Security Functions

4.1 General Process

The typical process as defined in the Common Criteria [12 to14] to derive functional IT security requirements is shown in Figure 3. 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. Note that the process contains a number of plausibility checks ensuring the coverage of threats and security objectives. The process is very similar to the process for the derivation of safety requirements in the CENELEC standards [7].

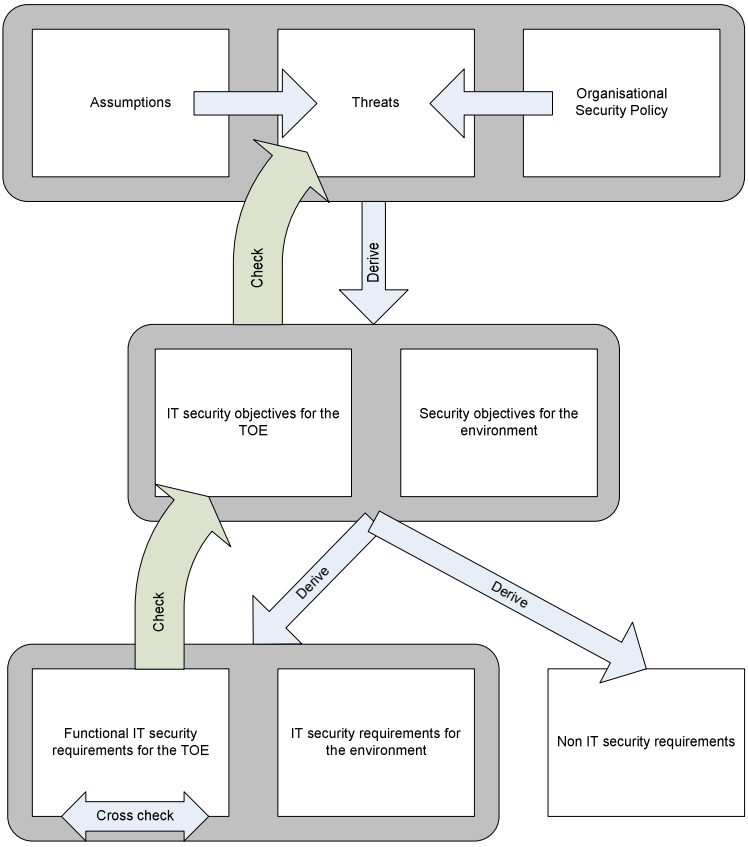

Fig. 3. Derivation of security requirements based on Common Criteria

RST in itself is safe but not necessarily secure. Often, there is a misconception in the railway world that by having safe signaling technology, security issues do not have to be taken care of. In this section, we will discuss the security threats which aim directly at signaling applications.

4.2 Threats

There is a common notion in the Common Criteria that threats are directed towards the three major IT security aspects: confidentiality, integrity and availability. One approach might be to analyze threats on this very high level. However, in our case experience has shown that only availability can be used directly as a threat; the other aspects need to be more detailed to derive security objectives.

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). In general, threats can be described on a higher system level.

The threats can be categorized into threats which are to be taken care of by the TOE and threats which have to be dealt with by the safety system or the environment. Some threats regarding communication issues can be taken from EN 50159. This standard explores in detail security issues inherent to communication networks. Threats taken from this standard are often defined on a lower level and are not discussed in this paper.

The threats have been listed using the following structure:

t.<attack>{.<initiator>.<further properties>}

t stands for threat and initiator for the initiator of the attack, typically a user, an attacker or a technical problem, such as a software error. As the security profile is generic, in most cases there has been no further detailing.

Is it is not prudent to list all threats in this paper; we will only list threats on the highest level. The lower levels give more properties e. g. regarding the particular types and means of an attack. We will name the initiators taken into account. The following threats have been used for the security profile. They deal with threats that have to be controlled by the IT system:

- 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 can not 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 following threats have to be controlled by the environment of the IT security system:

- t.installation: The IT system is installed in an insecure mode.
- t.operation: Due to errors in administration or operation, an IT security policy violation occurs.
- t.roles: Due to incorrect definition or allocation of roles and/or rights, the IT security policy is disabled.

- t.violence: Due to external violence, IT security functions are manipulated or deactivated.

It became quite obvious during the process of threat derivation that a detailed knowledge of the railway system and railway operation is necessary because otherwise no definite decision about what threats are relevant was possible.

4.3 Assumptions

The identification of threats depends on assumptions. As threats usually arise at the system boundary, the assumptions are related to the boundary and the environment. Some important assumptions are:

- a.entry: At least some parts of the system are in areas which are accessible for authorized persons only.
- a.protection: All system parts of the IT security system are protected directly against unauthorized modifications or there are (indirect) organizational measures which allow effective protection. This includes protection against elementary events.
- a.user: Users are correctly and sufficiently trained. They are considered trustworthy. This does not mean that users are expected to work error-free and their interactions with the system are logged.

4.4 Objectives

In order to protect against threats, security objectives are defined. For the sake of brevity, we can demonstrate this process only for one example in Table 1:

Table 1. Coverage of threats by security objectives (example)

Threat	Description of threat	Related security objectives	Comment
t.repudiation	Incidents which are IT security-related are not documented or cannot be attributed to an authorized user.	o. traceability, o.function, o.administration, o.storage, o.environment	All information that is necessary to hold a user accountable for his or her actions is to be saved.

As we have explained above, the threat t.repudiation summarizes all incidents where security-related incidents are not documented or cannot be attributed to an authorized user. To make sure this threat is counteracted, several security objectives have been defined:

- o.traceability: The TOE allows the indisputable traceability of all IT security-related actions. This information is stored securely. Access to this data is only possible for authorized users with appropriate rights
- o.function: The TOE offers all necessary functions for administration to the authorized user with appropriate rights.

- o.administration: The TOE will be administered by personnel who are trained accordingly. This personnel are trustworthy for this task. Administration makes sure that no connections to non-trustworthy connections will jeopardize security.
- o.storage: In the environment of the TOE, there is storage space for the data and especially the backups according to the relevant laws.
- o.environment: The TOE ensures that attackers cannot bypass the security mechanism, especially not using manipulative or erroneous software.

In general, it is possible to show that the security objectives cover the threats completely, but the argument for each threat relies on expert opinion and does not give a formal proof.

5 IT Security Requirements Based on Common Criteria

Those portions of a TOE that must be relied on for correct enforcement of the functional security requirements are collectively referred to as the TOE security functionality (TSF). The TSF consists of all hardware, software, and firmware of a TOE that is either directly or indirectly relied upon for security enforcement.

Table 2. Overview of functional classes and selected IT security functions

Class	Description	Selected IT security functions
FAU	Security Audit	FAU_GEN.1, FAU_SAA.1
FCO	Communication	FCO_NRO.1, FCO_NRR.1
FCS	Cryptographic Support	FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FCS_COP.1
FDP	User Data Protection	FDP_ACC.1, FDP_ACF.1, FDP_DAU.1, FDP_DAU.2, FDP_ITT.1, FDP_ITT.3, FDP_ROL.1, FDP_SDI.2
FIA	Identification and Authentication	FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.2, FIA_UAU.3, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UAU.7, FIA_UID.1, FIA_UID.2, FIA_USB.1
FMT	Security Management	FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_REV.1, FMT_SAE.1, FMT_SMF.1, FMT_SMR.1, FMT_SMR.2, FMT_SMR.3
FPR	Privacy	-
FPT	Protection of the TSF	FPT_FLS.1, FPT_ITT.1, FPT_RCV.1, FPT_STM.1, FPT_TST.1, FPT_ITA.1, FPT_ITC.1, FPT_ITI.1
FRU	Ressource Utilisation	FRU_RSA.2
FTA	TOE Access	FTA_LSA.1, FTA_MCS.1, FTA_SSL.1, FTA_SSL.2, FTA_SSL.3, FTA_SSL.4, FTA_TAH.1, FTA_TSE.1
FTP	Trusted Paths/Channels	FTP_ITC.1, FTP_TRP.1

The Common Criteria, Part 2 [13], define an extensive list of security functions and requirements in a formalized language. Thus, the next step is to try to satisfy the security objective by a subset of the security functions. As a countercheck, a walkthrough of all functions was performed. Table 2 shows an overview of the functional classes and the selected IT security functions as specified in the Common Criteria part 2.

For some classes, it is immediately clear that their functionality is not required, e. g. privacy, which would in fact contradict some of the objectives.

We give a short informal overview of the classes and the selected security requirements. Class FAU sets basic requirements related to logging and rule-based evaluation of security-related events. Classes FCO and FTP set requirements for communication integrity.

Class FCS sets requirements for the use and management of cryptographic keys over the complete lifecycle. The requirements demand the use of asymmetric key management according to standardized procedures with a minimum key length, but do not require a particular algorithm.

Class FDP is concerned with the protection and integrity of user data, while class FIA is concerned with user identification and authentication. As an example, FIA_UAU.1 deals with requirements on the timing of authentication. Generically, it states "The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated." It was decided that no security-related user actions may be performed before user authentication. Other requirements limit the number of failed authentication attempts or time-out for inactive user sessions.

Class FMT specifies a large number of generic configuration and management requirements, but leaves freedom to implement particular role schemes.

Classes FPT, FRU and FTA deal with protection of the TOE and the TSF themselves. The requirements covered include self-testing and recovery as well as preservation of a secure state which is very similar to requirements from EN 50129: "FPT_FLS.1: The TSF shall preserve a secure state when the following types of failures occur: [assignment: list of types of failures in the TSF]." It was decided to apply this generic requirement rigorously to any failure of the TSF.

Finally, as a plausibility check, coverage of the security objectives by the security requirements is evaluated (see Table 3 for an example).

Table 3. Coverage of security objectives by security requirements (example)

Security objective	Security requirements	Explanation
o.error	FIA_AFL.1 FIA_SOS.1 FMT_MSA.2 FMT_SAE.1 FTA_SSL.1 FTP_ITC.1 FTP_TRP.1 EAL4	FIA_AFL.1 addresses the handling of authentication failures. FIA_SOS.1 makes sure that no weak passwords, etc., are used. FMT_MSA.2 inhibits insecure configuration. FMT_SAE.1 reduces the effect of compromised secrets. FTA_SSL.1 locks a session in the absence of a user. FPT_ITC.1 and FTP_TRP.1 protect data during communication. The evaluation assurance level (EAL) 4 ensures that implementation of the functions is sufficiently trustworthy.

A very important point is the selection of the evaluation assurance level according to the Common Criteria, which is a measure for how trustworthy implementation of the TSF is. In the particular railway environment, EAL 4 is proposed, because a sufficiently high level of security has to be guaranteed but, on the other hand, economic aspects must also be taken into account. A high EAL may even be counterproductive and, considering the railway environment, may also not be necessary, but on the other hand, a low EAL may not be appropriate for safety-related applications. Currently, EAL 4 is selected, which means that the TSF must be methodologically designed, tested and reviewed. According to the Common Criteria [14], "EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices …. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line."

6 Summary

This paper has defined a reference communication architecture, which aims to separate IT security and safety requirements as far as possible, and discussed the threats and IT security objectives including typical assumptions in the railway domain. Examples of IT security requirements have been stated and discussed based on the approach advocated in the Common Criteria, in the form of a protection profile [17]. The goal is to use COTS security components which can be certified according to the Common Criteria, also in the railway signaling domain, instead of creating a new certification framework. The work presented is still ongoing (the public consultation ends September 2012), in particular with respect to approval of the protection profile and practical experience.

References

1. http://www.nextgov.com/nextgov/ng_20120123_3491.php?oref=topstory (accessed on February 7, 2012)
2. Stumpf, F.: Datenübertragung über öffentliche Netze im Bahnverkehr – Fluch oder Segen? In: Proc. Safetronic 2010, Hanser, München (2010)
3. Katzenbeisser, S.: Can trains be hacked? In: 28th Chaos Communication Congress, Hamburg (2011)
4. Thomas, M.: Accidental Systems, Hidden Assumptions and Safety Assurance. In: Dale, C., Anderson, T. (eds.) Achieving System Safety, Proc. 20th Safety-Critical Systems Symposium. Springer (2012)
5. Johnson, C.: CyberSafety: CyberSecurity and Safety-Critical Software Engineering. In: Dale, C., Anderson, T. (eds.) Achieving System Safety, Proc. 20th Safety-Critical Systems Symposium. Springer (2012)
6. EN 50159 Railway applications, Communication, signaling and processing systems – Safety related communication in transmission systems (September 2010)
7. EN 50129 Railway applications, Communication, signaling and processing systems – Safety-related electronic systems for signaling (February 2003)

8. ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security (2009)
9. ISA 99, Standards of the Industrial Automation and Control System Security Committee of the International Society for Automation (ISA) on information security, http://en.wikipedia.org/wiki/Cyber_security_standards
10. BITKOM / DIN Kompass der IT-Sicherheitsstandards Leitfaden und Nachschlagewerk 4. Auflage (2009)
11. 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
12. Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 3, Part 1: Introduction and general model (July 2009)
13. Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 3, Part 2: Functional security components (July 2009)
14. Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 3, Part 3: Assurance security components (July 2009)
15. Wickinger, T.: Modern Security Management Systems. Signal & Draht, (4) (2001) (in German)
16. DB AG: European Patent Application EP2 088 052 A2 (2000)
17. DIN V VDE V 0831-102: Electric signaling systems for railways – Part 102: Protection profile for technical functions in railway signaling, Draft (2012) (in German)