What's Security Level got to do with Safety Integrity Level?

Jens Braband

What's Security Level got to do with Safety Integrity Level?

Jens Braband

Siemens AG, Braunschweig, Germany
jens.braband@siemens.com

Abstract. Some recent incidents and analyses have indicated that possibly the vulnerability of IT systems in railway automation has been underestimated so far. Due to several trends, such as the use of commercial IT and communication systems or privatization, the threat potential has increased. This paper discusses the relationship of IT security and functional safety from the perspective of their integrity measures.

Keywords. Railway, IT Security, Safety, Threats, IT Security Requirements, Security Level, Safety Integrity Level.

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. Many other attacks that have been reported or have been claimed to be possible, could fortunately be shown to be unfounded or were oriented towards public relation, e. g. a hack of Nuremberg's automated metro was performed on an unprotected self-made system [2]. However, in 2014, the German Federal Agency for IT Security (BSI) reported the first successful attack on critical industrial infrastructure. As a consequence a blast furnace was damaged and had to be shut down [3].

What distinguishes railway systems from many critical infrastructures is their inherent distributed and networked nature with tens of thousands of track-kilometers for major operators, or even more. 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 lifetime of their systems and components. Current contracts usually demand support for at least 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. Some of the technical problems are not railway-specific, but are shared by a few other sectors such as Air Traffic Management.

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, while others directly pose the question "Could rail signals be hacked to cause crashes?"[4]. While in railway automation harmonized functional safety standards were elaborated more than a decade ago, up to now no harmonized international IT security requirements for railway automation exist.

This paper starts with a discussion of the normative background and then discusses the similarities and dissimilarities of IT security and functional safety, in particular from the point of view of their integrity measure Security Level (SL) and Safety Integrity Level (SIL), respectively. In particular the requirements for SL and SIL are compared, e. g. which SL can be covered by SIL.

2 Normative background

In railway automation, an established standard for safety-related communication, EN 50159 [5] exists. The first version of the standard was elaborated in 2001. It has proven quite successful and is also used in other application areas, e.g. industrial automation. This standard defines threats and countermeasures to ensure safe communication in railway systems. The methods described in the standard are partially able to also protect railway system 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 functional safety aspects of electronic hardware are covered by EN 50129 [6]. However, IT 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 a single requirement. However, EN 50129 provides a structure for a safety case which explicitly includes a subsection on protection against unauthorized access (both physical and informational), so it is already a "security-informed safety case". Other security objectives could also be described in that structure.

On the other hand, industrial standards on information security exist. ISO/IEC 15408 [7] provides evaluation criteria for IT security, the so-called Common Criteria. This standard is solely centered on information systems and has, of course, no direct relation to safety systems. IEC 62443 [8], also known as ISA 99, 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.

How can the gap between information security standards for general systems and railways be bridged? The bridge is provided by the European Commission Regulation on Common Safety Methods No. 402/2013 [9]. 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.

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

However, application of the general standards 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 IEC 62443 [8] has been selected, as this standard series seemed to provide the best fit. With this approach, a normative base has been developed by the German standardization committee DKE [10], based on IEC 62443 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 Basic concepts of IEC 62443

A total of 12 standards or technical specifications is planned in the IEC 62443 series of standards that cover the topic of IT security for automation and control systems for industrial installations entirely and independently. This series of standards adds the topic of IT security to IEC 61508 which is the generic safety standard for programmable control systems. Up to now, though, IEC 61508 and IEC 62443 have only been loosely linked.

IEC 62443 addresses four different aspects or levels of IT security:

- general aspects such as concepts, terminology and metrics: IEC 62443-1-x
- IT security management: IEC 62443-2-x
- system level: IEC 62443-3-x
- component level: IEC 62443-4-x

Today, however, the parts of IEC 62443 are still at different draft stages. Only a small number of parts such as IEC 62443-3-3 have already been issued as an International Standard (IS) or a Technical Specification (TS). Due to the novelty of the IEC 62443 series in this section, the essential concepts of IEC 62443 will be explained briefly so as to improve understanding of the adaptation and embedding of IT security in compliance with IEC 62443 into EN 50129.

3.1 IT security management

An IT security management system (ISMS) shall be established for operation of the system. The aim of an ISMS is to continuously control, monitor, maintain and, wherever necessary, improve IT security. In the case of the ISMS, IEC 62443 is based on the general stipulations of the ISO/IEC 17799 and ISO/IEC 27000 series. It details these general standards by adding specific aspects for safety-related control systems. If an ISMS is already established, it may remain in use. However, the essential principles of the ISMS according to IEC 62443 should be introduced or integrated. In the event of integration into an existing ISMS, the special technical aspects of a safety-related railway system shall be observed. Due to the specific framework, unreflected adoption of the stipulations from IT security does not make sense and in most cases can only be implemented with difficulty. The DKE standard [10] offers a comparison of IT security elements from common standards, and is intended to assist integration.

One key task of ISMS is risk management. This includes the consideration of all functional components of the system together with those that are specific to IT security.

3.2 System definition

The system and its architecture are divided into zones and conduits. The same IT security requirements apply within each zone. Every object, e.g. hardware, software or operator (e.g. administrator) shall be assigned to precisely one zone and all connections of a zone shall be identified. A zone can be defined both logically and physically. This approach matches the previous approach for railway signalling systems very well, as has been used as the basis in numerous applications [11]. Figure 1 shows a simple application of the concept, the connection of two safety zones by a virtual private network (VPN) connection as the conduit.

The conduit would consist of the gateways at its borders and the connection in between whatever the actual network would look like. Strictly speaking management would itself be a zone with conduits connecting it with the gateways.

This example may serve as a blueprint for the connection of zones with similar IT security requirements. If zones with different IT security requirements shall be connected, different types of conduits, e. g. one-way connections or filters have to be applied.

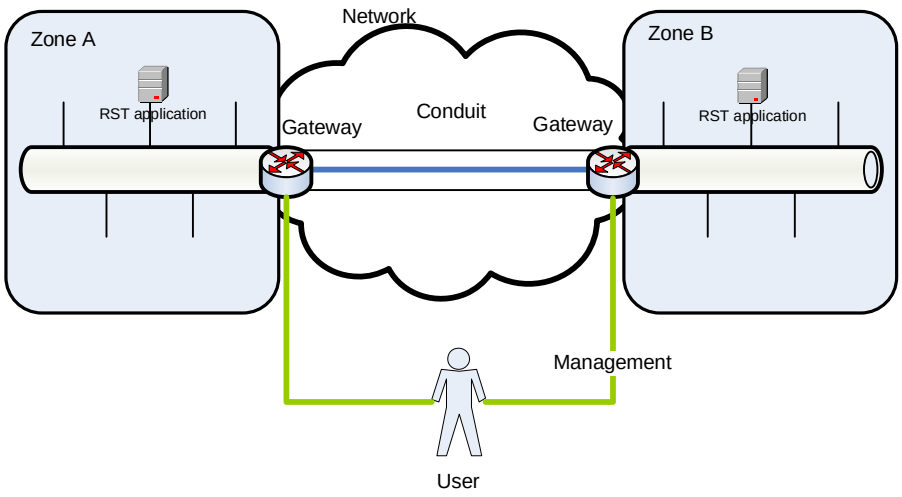

Figure 1: Zone and conduit architecture example

3.3 IT security requirements

In IEC 62443, the IT security requirements are grouped into 7 fundamental requirements:

1. identification and authentication control (IAC)
2. use control (UC)
3. system integrity (SI)
4. data confidentiality (DC)
5. restricted data flow (RDF)
6. timely response to events (TRE)
7. resource availability (RA)

Normally, only the issues of integrity, availability and data confidentiality are considered in IT security. However, the fundamental requirements IAC, UC, SI and TRE can be mapped to integrity, RA to availability and DC and RDF to confidentiality. Instead of defining a seven level Evaluation Assurance Level (EAL) as in the Common Criteria, which is to be applied with regard to the IT security requirements, a four stage IT security requirement level is defined. A possible explanation might be that also most safety standards define four levels. But it would lead to quite demanding and sometimes unnecessary requirements if the level would be the same for each of the foundational requirements. For example confidentiality often plays a minor role for safety systems and encryption of all data might lead to complications in testing or maintenance of safety systems. So different levels may be assigned for each of the seven foundational requirements. The SL values for all seven basic areas are then combined in a vector, called the SL vector. Note that this leads theoretically to 16384 possible different SL.

The SL are defined generically in relation to the attacker type against whom they are to offer protection:

SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means with few resources, generic skills and a low degree of motivation
SL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills and a moderate degree of motivation
SL 4	Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills and a high degree of motivation

Sometimes a SL 0 (No protection) is also defined, but as we argue below, at least for safety-related systems this is not an option and so we do not discuss SL 0 further in this paper.

For one zone, for example, (4, 2, 3, 1, 2, 3, 2) could be defined as an SL vector. Once its vector is defined, IEC 62443-3-3 calls for a complete catalogue of standardised IT security requirements for the object under consideration, e.g. for a zone.

It is necessary to take into account the fact that IEC 62443 defines different types of SL vectors:

- The target SL (SL-T) is the SL vector that results as a requirement from the IT security risk analysis.
- Achieved SL (SL-A) is the SL vector which is actually achieved in the implementation when all the framework conditions in the specific system are taken into account.
- SL capability (SL-C) is the SL vector that the components or the system can reach if configured or integrated correctly, independent of the framework conditions in the specific system.

4 Relationship of SL and SIL

First, we should recall that, like IEC 61508, EN 50129 defines only four different Safety Integrity Levels (SIL). A SIL “indicates the required degree of confidence that a system will meet its specified safety functions with respect to systematic failures”[6]. Other target measures are defined with regard to random failures, but for IT security we are only concerned with systematic failure [12].

A first look at EN 50129 reveals that safety systems also have to deal with human errors and foreseeable misuse, which corresponds well to SL 1. For this reason SL 0 is not acceptable for safety-related systems. So we can conclude that for any safety system, even if IT security threats can be effectively ruled out, the basic IT security requirements SL 1=(1,1,1,1,1,1,1) should be fulfilled. So it is an interesting exercise to discuss the SL 1 requirements and evaluate whether these are normally fulfilled by safety systems developed according to EN 50129.

In a first step we take a more general look at the Foundational Requirements (FR). Due to functional safety criteria, not all requirement groups of IEC 62443 in applications for railway signalling systems have the same significance. Only the following requirement groups have direct relevance in the sense of functional safety:

1 unauthorised physical or logical access (IAC)
2 unauthorised use (UC)
3 manipulation of the system (SI)
6 response to events that is not timely (TRE)

For example, safety-related applications generally do not impose any requirements on the confidentiality of operational data. Therefore, apart from exceptions such as key management, further requirements for confidentiality can be discarded.

So in order to come up with a manageable number of SL vectors, we may as a first simplification and short hand notation set SL 1 as the default for all FR that are not directly safety-related. And we might work under the assumption that in a first approach all other FR may have the same importance. This would lead to four generic SL profiles: (1,1,1,1,1,1,1), (2,2,2,1,1,2,1), (3,3,3,1,1,3,1) and (4,4,4,1,1,4,1). It is admitted that additional SL profiles are necessary for particular zones or conduits. For example a zone containing a key management centre will deserve more demanding confidentiality requirements leading to another profile. But the idea would be to be able to cope with 5 to 10 profiles instead of 16384 possible combinations.

In a next step, we have discussed all 43 requirements from IEC 62443-3-3 in detail in order to find out, which are covered by EN 50129. According to the analysis in the annex many IT security requirements for SL1 are already adequately covered by railway safety standards or are not relevant to safety. These results are summarised in Table 1. They no longer need to be verified in each individual case for railway signalling applications.

Reference	Title	Assessment
SR 1.6	Management of wireless access processes	This requirement is not relevant for SL1.
SR 1.13	Access through untrustworthy networks	This requirement is not relevant for SL1.
SR 2.2	Use control in the case of radio connections	This requirement is not relevant for SL1.
SR 3.1	Communication integrity	This requirement is fulfilled by application of EN 50159.
SR 3.3	Verification of IT security functionality	This requirement is fulfilled by application of EN 50128.
SR 3.4	Software and information integrity	This requirement is fulfilled by application of EN 50128.
SR 3.5	Input validation	This requirement is fulfilled by application of EN 50129 and EN 50128.
SR 3.6	Deterministic output	This requirement is fulfilled by application of EN 50129 and EN 50128.
SR 4.1	Confidentiality of information	This requirement is not relevant for railway applications with SL1.
SR 4.3	Use encryption	This requirement is not relevant for railway applications with SL1.
SR 5.1	Network segmentation	This requirement is fulfilled by application of EN 50159.
SR 5.2	Protection of the zone boundary	This requirement is not relevant for SL1.
SR 5.3	Restriction of general communication between persons	Generally, voice communication is not part of the safety system. However, this requirement shall be exported to the operator.
SR 7.1	Protection against DoS attacks	This requirement is normally not contained in safety standards because it cannot be fulfilled by safety-related systems alone. The rule shall be exported to the operator.
SR 7.2	Resource management	This requirement is normally not contained in safety standards because it cannot be fulfilled by safety-related systems alone. The rule shall be exported to the operator.
SR 7.3	Backups of the automation system	This requirement is normally not contained in safety standards because it cannot be fulfilled by safety-related systems alone. The rule shall be exported.
SR 7.4	Restart and recovery of the automation system	This requirement is fulfilled by application of EN 50129.
SR 7.5	Emergency power supply	This requirement is normally not contained in safety standards because it cannot be fulfilled by safety-related systems alone. The rule shall be exported to the operator.
SR 7.6	Network and security settings	This requirement is fulfilled by application of EN 50128 and EN 50129.

Table 1 – IT security requirements that are already covered or are irrelevant

This means that for new safety-related systems it would be an advantage to implement all SL1 requirements from IEC 62443 (independent from the SIL) as most of them are already covered by safety standards (and some might not be relevant). In this case also an additional IT security certification for SL1 might be avoided as the requirements could adequately be included in the safety certification.

However a more detailed analysis (see the appendix) shows that starting with SL2 requirements there is no similar relationship with SIL anymore. The reason is that by definition the higher SL levels deal with intentional attacks which have only partially be covered by safety standards such as EN 50159 for communication. So also simple rules like “If you have a SIL x safety system then you must require at least SL x” cannot be justified as the allocation of SL depends also on the overall security architecture, e. g. physical protection, and not on the technical solution alone.

5 Summary

This paper has discussed the relation between SL from IEC 62443 and SIL from EN 50129 for safety systems. The major new results are:

- SL and SIL are completely different concepts, e. g. SL is a seven dimensional vector in contrast to the scalar SIL
- There is no simple relationship between SL and SIL
- SL 0 for safety-related systems is not acceptable. For safety systems, it is recommended to always take the requirements of SL 1 into account
- A preliminary proposal for SL profiles has been made in order to master the complexity of potentially 16384 SL vectors

Table 1 gives a summary of which requirements for SL 1 are already covered or not relevant from a safety perspective. The annex gives a more detailed discussion including a comparison with SL2 requirements.

The results should also hold for other related safety standards such as IEC 61508 as they build upon similar general principles, however the details would have to be checked and might differ.

6 References

1. Hackers manipulated railway computers, TSA memo says, http://www.nextgov.com/nextgov/ng_20120123_3491.php?oref=topstory, accessed on February, 7, 2012
2. Keine Hacker-Angriffe auf Nürnberger-U-Bahn, http://www.merkur.de/bayern/vag-gegen-vorwuerfe-keine-sicherheitsluecken-nuernberger-u-bahn-4654909.html, accessed on May, 25, 2015
3. Die Lage der IT-Sicherheit in Deutschland 2014, Bundesamt für Sicherheit in der Informationstechnik, 2015
4. BBC: Rail signal upgrade 'could be hacked to cause crashes', April, 24, 2015, http://www.bbc.com/news/technology-32402481, last accessed on May 20th, 2015
5. EN 50159 Railway applications, Communication, signaling and processing systems –Safety related communication in transmission systems, September 2010
6. EN 50129 Railway applications, Communication, signaling and processing systems – Safety-related electronic systems for signaling, February 2003
7. ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security, 2009
8. IEC 62443: Industrial communication networks - IT security for networks and systems, series of 12 standards (planned), see http://en.wikipedia.org/wiki/Cyber_security_standards
9. Commission Regulation (EC) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No. 352/2009, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0402&from=DE, last accessed on April, 14th, 2014
10. DIN V VDE V 0831-104: Electric signaling systems for railways – Part 104: IT Security Guideline based on IEC 62443 (in German), 2015
11. Braband, J., Bock, H., Milius, B. und Schäbe, H.: Towards an IT Security Protection Profile for Safety-related Communication in Railway Automation, in: Ortmeier, F., Daniel, P. (eds.) Computer Safety, Reliability and Security, Proc. SAFECOMP2012, Springer, LNCS 7612, 2012, 137-148
12. Braband, J., Schäbe, H.: Probability and Security – Pitfalls and Chances (mit Schäbe, H.): in Proc. Advances in Risk and Reliability Technology Symposium 2015, Loughborough, 2015

7 Appendix: Relationship between SL 1 and Functional Safety

This annex reports in detail the result of a comparison between the SL 1 requirements (Security Requirements (SR) in compliance with IEC 62443-3-3 and those of EN 50129, EN 50128 and EN 50159. As SL 1 is only intended to offer protection against unintentional or random attacks, it may be presumed that safety-related systems that have to offer protection against foreseeable misuse and operating errors already fulfil a large proportion of the requirements. For example, EN 50129 also already protects against random errors and unintentional disruptions, similar to EN 50159 for Category 1 and Category 2 against corresponding transmission errors. Further measures are only necessary where unauthorised access cannot be ruled out (Category 3).

At the same time, the difference between SL 1 and SL 2 should be pointed out. Additional requirements that are added for SL2 are printed in italics.

This comparison does not mean that all requirements for SL 1 are already covered in EN 50129. At least the requirements that are normally not fulfilled by safety systems should be adopted as requirements in future. Table 1 gives a list of the requirements which are either covered by the safety standards or are not relevant from a safety point of view.

Ref.	Title	Requirement for SL 1	Fulfilment by safety standards
SR 1.1	Identification and authentication of persons	The automation system must have the ability to identify and authenticate all human users (persons). The automation system with its corresponding capabilities must assert the identification and authentication at all interfaces of persons who want to achieve access to the automation system, that would allow them to separate obligations and restrictive assignment of authorisations, in accordance with the applicable IT security guidelines and processes. *RE1 The automation system must have the ability to uniquely identify and authenticate all human users.*	This is required by EN 50129 B.4.6. This standard in particular requires that protective measures have to be taken with regard to – oversights by authorised personnel, and – intentional changes by unauthorised personnel. NB The requirements need not necessarily be technically implemented, but can also be fulfilled by corresponding organisational measures.
SR 1.2	*Identification and authentication of software processes and devices*	*The automation system must have the ability to identify and authenticate all software processes and devices and function units. The automation system with its corresponding capabilities must assert the identification and authentication at all interfaces of software processes and devices that want to achieve access to the automation system, that would allow them to restrictively assign authorisations, in accordance with the applicable IT security guidelines and processes.*	Generally, access protection is understood in a wide sense in EN 50129, just like in EN 50159.
SR 1.3	User account management	The automation system must have the ability to manage and administer all user accounts of authorised users, which includes opening new accounts and activating, modifying, blocking and deleting accounts.	This is not required explicitly, but is an implicit conclusion from EN 50129 B.4.6.
SR 1.4	Identifier management	The automation system must have the ability to manage identifiers and IDs of different kinds and conditions according to users, groups, roles or different interface types of the automation system.	This is not required explicitly, but is an implicit conclusion from EN 50129 B.4.6.
SR 1.5	Authenticator management	The automation system must possess the following capabilities and must implement them: a) initialising the authenticator's content, i.e. the means of confirming a user's identity; b) changing all default authenticators after installation of the automation system; c) changing or renewing all authenticators; and d) protecting all authenticators from an unauthorised disclosure and modification during storage or transmission.	This is not required explicitly, but is an implicit conclusion from EN 50129 B.4.6.
SR 1.6	Management of wireless access processes	The automation system must have the ability to identify and authenticate all users communicating by wireless means (persons, software processes and devices). *RE 1 The automation system must have the ability to uniquely identify and authenticate all users communicating by wireless means (persons, software processes and devices).*	For SL1, this requirement is contrary to EN 50159 B.1. A radio transmission system would generally be assigned to Category 3 and would need cryptographic protection, i.e. more than SL1. Therefore, this requirement is not relevant for SL1.
SR 1.7	Security of authentication by passwords	Automation systems that use passwords for authentication must have the ability to enable configuration of password security by means of password length (with a given minimum length) and diversity of characters.	This is not required explicitly, but is an implicit conclusion from EN 50129 B.4.6.
SR1.8	*PKI certificates*	*If a public key infrastructure (PKI) is used, the automation system must have the ability to operate such a public key infrastructure in accordance with common conventions or it must be able to obtain public key certificates from an existing public key infrastructure.*	Covered in EN 50159 for Category 3 if asymmetrical methods are used.
SR 1.9	*Security of asymmetrical crypto systems*	*In automation systems that use asymmetrical crypto systems (public key crypto systems) for authentication, the automation system must have the following capabilities:* *a) The ability to validate certificates by checking the validity of a given certificate's signature* *b) The ability to validate certificates by building up a certification path to a recognised certification agency (CA) or, in the case of a self-signed certificate, by issuing mutual confirmations to all hosts that communicate with the key holder for whom the certificate was issued* *c) Checking certificates to determine whether they are on a certificate blacklist (or a revocation list)* *d) Bringing about secure storage and monitoring of the associated private key by the user (person, software process or device)* *e) The ability to map the authenticated identity to a user (person, software process or device)*	Addresses in EN 50159 for Category 3 if asymmetrical methods are used, but not in relation to all details.
SR 1.10	Feedback from the authenticator	The automation system must have the ability to suppress (blacken) feedback messages generated by the authenticator during the authentication process.	This is not explicitly required, but is easy to realise.

SR 1.11	Failed login attempts	The automation system must have the ability to assert a limit to the number of failed successive login attempts (person, software process or device) within a configurable time. The automation system must have the ability to block physical or logical access for a specified time or it must allow an administrator to lift this block again after this time had been exceeded. For system accounts on whose behalf critical services or servers are operated, the automation system must provide for the ability to forbid interactive logins.	This is not explicitly required, but is easy to realise.
SR 1.12	Reference to system use	The authentication system must have the ability to refer, even before authentication, to the rights and obligations linked with use of the system. A 'System Use Notification' is displayed for this purpose. It must be possible for authorised personnel to configure this display.	This is not explicitly required, but is easy to realise if wished by the operator.
SR 1.13	Access through untrustworthy networks	The automation system must have the ability to monitor and control all kinds of access to the automation system through untrustworthy networks. *RE1 The automation system must have the ability to deny access through unreliable networks, but the desire is approved by an instance authorised to do this.*	In SL1, only Category 1 and 2 networks come into consideration. In 1 there are only known users, i.e. the requirement is unnecessary. In Category 2, although the users are not all known, they are trustworthy.
SR 2.1	Enforcing authorisation	At all interfaces, the automation system must ensure enforcement of the authorisations assigned to all human users; as a result, these persons become authorised and are enabled to control the automation system in such a way that separation of duties and restrictive authorisation assignment can also be asserted. *RE 1 At all interfaces, the automation system must ensure enforcement of the authorisations assigned to all users (persons, software processes or devices); as a result, these users become authorised and are enabled to control the automation system in such a way that separation of duties and restrictive authorisation assignment can also be asserted.* *RE 2 The automation system must possess the ability and must make it possible for an authorised user or an authorised role to define and modify mapping of the authorisations of all human users to roles.*	This is derived from EN 50129 B.4.6.
SR 2.2	Use control and monitoring in the case of radio connections	In the case of radio (wireless) connections into the automation system, the automation system must possess the ability to authorise, monitor and also fulfil restricted use in accordance with the security conventions that are generally common in industrial practice.	This requirement is contrary to EN 50159 B.1. A radio transmission system would generally be assigned to Category 3 and would need cryptographic protection, i.e. more than SL1.
SR 2.3	Use control and monitoring in the case of portable and mobile devices	The automation system must possess the ability to automatically implement and execute configurable restrictions of use: a) Preventing use of portable and mobile devices b) Demanding a context-specific authorisation c) Restricting transmission of data and code from and to portable and mobile devices	In EN 50129, mobile devices are treated just like other devices if they perform fail-safe tasks. The specific requirements must be derived from a hazard analysis, however.
SR 2.4	Mobile code	If mobile code techniques are used, the automation system must be able to assert restricted use, taking into account the damage that can possibly be caused in the automation system. These abilities include: a) Preventing execution of mobile code b) Demanding clean authentication and authorisation of the code source c) Limiting transfer of mobile code to and from the automation system d) Monitoring the use of mobile code	Mobile code is not allowed in safety-related systems because it is not covered by validation and approval.
SR 2.5	Session blocking	The automation system must possess the ability to prevent further access to the system by blocking the session after an adjustable inactivity time or by manual intervention. The session must remain blocked until the session owner or another authorised person restores access by again initiating the identification and authentication process intended for this purpose.	This is not explicitly required, but is easy to realise.
SR 2.6	*Ending a remote session*	*The automation system must possess the ability to end a remote session either automatically after an adjustable period of inactivity or it must make it possible for the session to be ended manually by the user who initiated it.*	This is not explicitly required, but is easy to realise.
SR 2.8	Verifiable events and their recording	The automation system must possess the ability to generate audit data (data recorded during computer and network monitoring, information technology measurements) concerning the IT security achieved in the following categories and to record such data as audit records: access control, flawed queries, incidents in the operating system, incidents in the automation system, incidents during backup and recovery of data, potential reconnaissance and incidents during audit report creation. The individual audit reports must contain the following information: Time of the incident, incident source (designation of the device, equipment, software process or user account in which the incident is taking place or has taken), category, type, incident number and result.	Although data logging is a common practice, it is not required normatively because such data is generally not considered to be relevant to safety.

SR 2.9	Storage capacity for audit records	The automation system must provide adequate storage capacity for storing audit records in accordance with generally recognised recommendations for log management (archiving of incident logs) and system configuration. The automation system must ensure that not too much storage capacity is maintained.	See above.
SR 2.10	Response to failed audit data processing	If it should transpire that the audit data (data recorded during computer and network monitoring, measured results regarding information technology processes in IACS) is no longer processed at all or no longer correctly, the automation system must possess the ability to inform operating personnel of this and it must prevent the loss of essential services and functions. As a response to failed processing of audit data, the automation system must possess the ability to initiate suitable remedies in accordance with generally recognised industrial conventions and to support them.	See above.
SR 2.11	*Time stamp*	*The automation system must assign a time stamp to the audit records generated.*	As detailed in EN 50159, time stamps can be used, but are not required.
SR 3.1	Communication integrity	The automation system must possess the ability to preserve the integrity of information transferred.	Protecting the integrity of the message stream is a basic requirement of EN 50159.
SR 3.2	Protection against harmful code	The automation system must possess the ability to take precautions against harmful code or unauthorised software; corresponding mechanisms should detect and report such harmful code and should defuse any negative impacts. These protective mechanisms must be updated. *RE 1 The automation system must possess the ability to use processes for protection against harmful code at all entry and exit points.*	In SL1, IEC 62443 assumes untargeted attacks, the viruses, etc. are not specifically directed at the system. EN 50128 15.4.6 requires protection of software against unintentional or random modification and this suffices for SL1.
SR 3.3	Verification of IT security functionality	The automation system must possess the ability to verify the intended operation of the IT security functions and must report whenever anomalies are detected during factory acceptance testing (FAT), during site acceptance testing (SAT) and during a scheduled maintenance operation. These security functions must comprise all functions that are needed to fulfil the information technology security requirements defined in this standard.	In the case of safety systems, this requirement is covered by validation in compliance with EN 50128.
SR 3.4	Software and information integrity	The automation system must possess the ability to detect, record, report and protect against unauthorised changes to software and stored inactive or archived data.	EN 50128 13 requires protection of software against unintentional or random modification.
SR 3.5	Input validation	The automation system must validate the syntax and the contents of indirect inputs into an industrial process control system and of direct inputs with direct impacts on the automation system.	Plausibility checks are required by EN 50129 E.5.1 and also by the principle of defensive programming in EN 50128.
SR 3.6	Deterministic output	The automation system must possess the ability set outputs to a predetermined status if no normal operation can be maintained any more as a result of an attack.	In accordance with EN 50129 B3.4, a safe status must be assumed in the event of a fault, including avoidance of unsafe outputs.
SR 3.7	Error handling	The automation system must detect errors and must handle error states in such a way that an effective remedy is possible. At the same time, steps must be taken to ensure that no information is disclosed that can be used by enemies to attack the IACS unless the disclosure of this information is indispensable to remedy the problems in good time.	EN 50129 and EN 50159 do not contain any specific requirements in this respect.
SR 3.8	*Session integrity*	*The automation system must possess the ability to preserve the integrity of sessions. The automation system must reject use of invalid session identifiers (IDs).*	This is required in EN 50159.
SR 3.9	*Protection of audit information*	*The automation system must protect verified and recorded incidents (audit information) and audit tools (insofar as available) against unauthorised access, modification and deletion.*	EN 50129 and EN 50159 do not contain any specific requirements in this respect.
SR 4.1	Confidentiality of information	The automation system must possess the ability to preserve the confidentiality of information for which a read authorisation is expressly required, be it in transit or in the idle state. *RE 1 The automation system must possess the ability to preserve the confidentiality of information or data that is in the idle state and protect data that is routed through an untrustworthy network during a remote session.*	Confidentiality is not normally required for railway applications. Processes that are not safety-related may also access information.
SR 4.2	*Information constancy*	*The automation system must possess the ability to permanently delete all information on data media for which a read authorisation was expressly required and which are to be taken out of operation or shut down.*	EN 50129 and EN 50159 do not contain any specific requirements in this respect.
SR 4.3	Using encryption	If encryption is required, the automation system must use cryptographic algorithms for the size, the mechanisms of key creation and management of keys in accordance with the security conventions and recommendations generally recognised in information technology.	Generally not required in the case of Category 1 or 2 in accordance with EN 50159 Annex C.

SR 5.1	Network segmentation	The automation system must possess the ability to logically separate automation systems from non-automation systems and to logically separate critical automation systems from other automation systems. *RE 1*: The automation system must possess the ability to physically separate automation systems from non-automation systems and to physically separate critical automation systems from other automation systems.	This is a basic requirement of EN 50159 7.3.7.2 and is generally warranted by the safety protocol.
SR 5.2	Protection of the zone boundary	The automation system must possess the ability to monitor communications at zone boundaries and to intervene, if necessary, to be able to execute the departments defined in the risk-based zone and conduit model. *RE 1 The automation system must possess the ability to always reject network traffic and to permit it only in exceptional cases.*	Only Category 1 and Category 2 networks may be used for SL1. These form a single zone with uniform IT security requirements and so no splitting is necessary and this requirement does not make sense for SL1.
SR 5.3	Restriction of general communication between persons	The automation system must possess the ability to prevent exchange of messages between persons that are sent by users or systems outside the control system and are received by persons inside the control system.	Generally, voice communication is not part of the safety system. However, this requirement should be exported to the operator.
SR 5.4	Partitioning applications	The automation system must possess the ability to partition data, applications and services depending on the complexity of the zone model to be realised.	This is a requirement of EN 50129 E.2.1.
SR 6.1	*Access to audit logs*	The automation system must possess the ability to grant read access to stored audit logs to authorised persons and tools.	Although data logging is a common practice, it is not required normatively because such data is generally not considered to be relevant to safety.
SR 6.2	*Continuous monitoring*	*The automation system must possess the ability to continuously monitor the performance and behaviour of all IT security mechanisms and, to this end, to use the security conventions and recommendations that are generally recognised in information technology, thus being able to detect and report on any security violations early on.*	This is explicitly required in EN 50159 if the IT security functionality has not been developed in accordance with EN 50129, i.e. in particular in the case of commercial components.
SR 7.1	Protection against DoS attacks	The automation system must possess the ability to continue working in a restricted mode of operation during a DoS attack. *RE* 1 The automation system must possess the ability to control the traffic load (for example by limiting the data transfer rate) so that the impact of a provoked inundation with data leading to triggering of a reduced availability can be mitigated.	This requirement is normally not contained in safety standards. In railway, however, there is normally a fallback level after failure of technology. In future, IT security aspects may have to be considered in the design of the fallback level.
SR 7.2	Resource management	The automation system must possess the ability to counteract exhaustion of resources; to this end, security functions would possibly have to be granted fewer resources.	This requirement is normally not contained in safety standards.
SR 7.3	Backups of the automation system	The automation system must be capable of storing and archiving backup copies (backup) of critical files and data from the user and the system levels (including information about system status) in a secure location without detrimentally influencing ongoing operation of the system. *RE* 1 The automation system must possess the ability to check the operability (reliability) of backup mechanisms.	This requirement is normally not contained in safety standards.
SR 7.4	Restart and recovery of the automation system	The automation system must possess the ability to restart after an interruption or a failure and to return to a known secure state.	This is required in EN 50129 B5.2.
SR 7.5	Emergency power supply	The automation system must possess the ability to switch to an emergency power source, or to return to a normal supply source from it, without exerting any detrimental impact on the existing security state or a documented restricted mode of the IACS.	This requirement is normally not contained in safety standards.
SR 7.6	Network and security settings	The automation system must possess the ability to be configured as provided for in the instructions included by the supplier of the automation system; this applies in particular to recommended network and security settings. The automation system must provide an interface to the current network and security settings.	EN 50129 or EN 50128 requires configuration management as part of quality management. The requirements for configuration are part of the safety application conditions.
SR 7.7	Restrictive functionality assignment	The automation system must possess the ability to specifically suppress the application and use of unnecessary functions, ports, protocols or services or at least to restrict these applications.	EN 50128 requires complete tests. Railway software may only contain (activated) functions that are required in accordance with the specification. EN 50128, Section 7.3.4.7 can be referenced with regard to pre-existing software. Nevertheless, the result in certain circumstances for COTS components such as a switch is that certain functions are deactivated.
SR 7.8	*List of the automation system's components*	*The automation system must possess the ability to issue a list of all currently installed components of the automation system with the relevant characteristics and features.*	This requirement is normally not contained in safety standards.