Gashi, I., Bloomfield, R., Bloomfield, R. E. & Stroud, R. (2012). How secure is ERTMS?. Paper presented at the Workshop on Dependable and Secure Computing for Large-scale Complex Critical Infrastructures (DESEC4LCCI), 25 September 2012, Herrenkrug, Germany.

CITY UNIVERSITY LONDON

City Research Online

How secure is ERTMS?

Richard Bloomfield[1], Robin Bloomfield[2,3], Ilir Gashi[2], Robert Stroud[3]

[1]Independent Consultant, UK
richardbloomfield52@yahoo.co.uk
[2]Centre for Software Reliability, City University London, London, UK
{reb, i.gashi}@csr.city.ac.uk
[3]Adelard LLP, London, UK
rjs@adelard.com

Abstract. This paper reports on the results of a security analysis of the European Railway Traffic Management System (ERTMS) specifications. ERTMS is designed to be fail-safe and the general philosophy of 'if in doubt, stop the train' makes it difficult to engineer a train accident. However, it is possible to exploit the fail-safe behaviour of ERTMS and create a situation that causes a train to halt. Thus, denial of service attacks are possible, and could be launched at a time and place of the attacker's choosing, perhaps designed to cause maximum disruption or passenger discomfort. Causing an accident is more difficult but not impossible.

Keywords. Security assessment, safety-critical systems, ERTMS, railway signaling systems, safety and security interactions.

1 Introduction

This paper reports on the results of a security analysis of the European Railway Traffic Management System (ERTMS) specifications that was commissioned on behalf of key UK railway stakeholders and UK government. ERTMS is a major industrial project that aims at replacing the many different national train control and command systems in Europe with a standardised system. In the UK, Network Rail are preparing to introduce ERTMS as part of the upgrade of the signalling and communications systems running on Britain's rail infrastructure. This upgrade has the potential to increase the risk of an electronic attack on the rail infrastructure, as it brings more systems under centralised control. Consequently, the railway industry and government identified a need to understand the security implications of the new technology, and we were asked to conduct a security audit of ERTMS to identify potential vulnerabilities and suggest mitigations.

In this paper, we discuss the ERTMS/ETCS specifications from a security perspective and identify areas where there are potential vulnerabilities. We also explain our methodology of using attack scenarios to assess the impact of these vulnerabilities and present our overall assessment of the scenarios we analysed. However, because

the results of our analysis are sensitive, we do not provide details of specific vulnerabilities or attack scenarios, which can be found in our detailed reports [1,2]. Although these reports are currently not publicly available, copies can be made available on request, subject to the approval of the key stakeholders.

The rest of the paper is organised as follows: section 2 gives an overview of ERTMS; section 3 explains the scope of our analysis; section 4 discusses our threat model; section 5 describes our methodology; section 6 discusses the trust relationships between the components of the ERTMS architecture; section 7 presents a summary of the weaknesses and vulnerabilities that we found in each part of the ERTMS specifications; section 8 explains our use of attack scenarios to assess the impact of these vulnerabilities and our scenario analysis technique; section 9 discusses related work on ERTMS security; and finally section 10 provides a discussion, conclusions and areas for further work.

2 Overview of ERTMS

ERTMS consists of two major components:

- **ETCS** is the European Train Control System, an automatic train protection system that is intended to replace existing legacy train protection systems;
- **GSM-R** is a radio system for providing voice and data communication between the track and the train. It is based on GSM technology but uses a different frequency range and has some special features for railway applications.

ERTMS is implemented using a number of trackside and on-board sub-systems, and the ERTMS/ETCS specifications describe the interfaces by which these various sub-systems interact. The ERTMS/ETCS System Requirements Specification (SRS) [3] provides a technical specification of the overall system, and details of specific protocols can be found in related standards. However, it is important to understand that ERTMS is an interoperability standard, and only deals with the interaction between trains and trackside devices. The interfaces that are used by each national railway to control and manage its own infrastructure are outside the scope of the standard.

This is illustrated in Figure 1, which shows the relationship between ERTMS and a national railway implementation. Green arrows denote interfaces and protocols that are covered by the ERTMS specifications, whilst red arrows denote interfaces that are considered to be part of the national implementation.

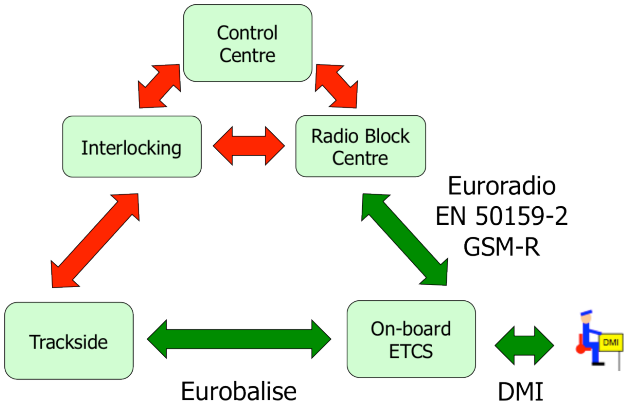

Fig. 1. Relationship between ERTMS and national railway implementation

The SRS defines four different ERTMS application levels, which cover different operational relationships between the track and the train. Our review focused on Level 2, which is the application level currently being considered for deployment in Britain. At ERTMS/ETCS Level 2, traditional trackside signals are replaced by movement authorities, which are sent to the train over the GSM-R radio link from a control centre. Movement authorities provide safety-critical information about the track conditions ahead, and how far and how fast the train can go. The train also gets location references from devices called balises that are mounted in the track. An on-board computer uses this information to give a display to the driver (via the Driver Machine Interface (DMI)) and to monitor the speed that the train is being driven at, in order to ensure that the train stays within the limits of its movement authority; if not, the on-board computer (not the DMI) applies the brakes automatically.

3 Scope of analysis

The aim of the study was to examine the ERTMS specifications for potential security vulnerabilities and identify systemic weaknesses in the ERTMS specifications. This was a paper-based study and we were concerned with conceptual problems with the specifications rather than vulnerabilities introduced by design flaws and bugs in implementations of ERTMS technology. Nor did we consider vulnerabilities that might be caused during the operation or maintenance of an ERTMS system. Such vulnerabilities are important but were outside the scope of our study.

Our analysis was holistic and considered whether a national deployment of ERTMS might introduce vulnerabilities into the national rail infrastructure. Our review focused on ERTMS Application Level 2, which made it possible to restrict attention to a number of core specifications, and ignore specifications for interacting with legacy train protection systems and trackside signalling equipment. We also considered the security of GSM-R and analysed how GSM security impacts on

GSM-R security. We were particularly interested in electronic attacks that could be launched remotely and would cause widespread disruption.

However, it is important to note that the ERTMS/ETCS specifications only deal with the interoperability requirements of a European Railway Traffic Management System, and therefore do not cover the interfaces that are used by each national railway to control and manage its own infrastructure. This limits the scope of any security or safety analysis to interactions between the various components of the ERTMS/ETCS architecture. For example, although the Radio Block Centres (RBCs) need to interact with the existing rail infrastructure, these interfaces are not required for interoperability and are typically proprietary. This is problematical from the perspective of a security review because it means that these interfaces cannot be reviewed, even though they are critical to the safety and security of the overall system.

4 Threat model

Traditionally, computer security deals with threats to confidentiality, integrity, and availability, but here we are concerned with train movements rather than information, so our primary concern is integrity, then availability, and finally confidentiality. Loss of integrity could result in accidents or collisions, whereas loss of availability would bring the railway system to a halt. Loss of confidentiality is less of an immediate threat, but might result in the leak of sensitive operational information. Reliability is also important, since an unreliable train service will result in a loss of public confidence in the railway operators.

Thus, the hazards or potential failures or undesirable outcomes to be avoided are:

- a collision involving multiple trains;
- an accident such as derailment involving a single train;
- widespread disruption of train service over a large area;
- disruption to individual trains, or trains within a local area;
- creation of a situation that leads to panic and potential loss of life (e.g., an emergency stop and uncontrolled evacuation onto the track);
- creation of a situation that leads to passenger discomfort and dissatisfaction, (e.g., stopping a train indefinitely in a tunnel);
- loss of public confidence in the railway system due to intermittent low-level problems affecting the reliability of the service;
- leak of sensitive information (e.g., movements of hazardous cargoes or VIPs).

The ERTMS safety analysis considers the effect of potentially catastrophic events on the integrity of the system. Faults that could result in an accident need to be considered in both a safety and security analysis, regardless of the underlying cause of the fault (accidental, deliberate or malicious).

A security analysis also needs to consider the capabilities of the attacker. It is usual to make a distinction between an insider and an outsider. An insider is someone with legitimate access to a system that abuses their position and privileges, either willingly or under duress, whereas an outsider is someone outside the system with limited ac-

cess, who seeks to break into the system out of curiosity, malice, or for personal gain. Historically, railway systems have relied on highly specialised, proprietary technology, and there has been a relatively small community with the necessary knowledge to exploit vulnerabilities. However, the widespread adoption of open standards like ERTMS that are designed to promote interoperability and the commoditisation of technology could result in both the necessary knowledge and the necessary tools becoming more readily available to potential attackers who are sufficiently motivated to gain the necessary skills.

5 Methodology

We started by considering the trust relationships between the various components of the overall architecture and analysing the consequence of a breach of trust. This enabled us to identify a set of potential weaknesses and vulnerabilities in the specifications. We then developed scenarios that showed how these weaknesses could be exploited by an attacker. These scenarios were refined and validated in discussion with railway stakeholders, and proved to be a very effective way of communicating the risks of an ERTMS implementation being compromised.

6 Trust relationships

ERTMS is implemented using a number of trackside and on-board sub-systems, and the ERTMS/ETCS specifications describe the interfaces by which these various sub-systems interact to ensure that trains move safely without exceeding their movement authority. Our approach to the security analysis was to consider the trust relationships between the various components of the overall system and analyse the consequences of a breach of trust.

Messages are transmitted between the ERTMS/ETCS sub-systems over various channels, so a security analysis needs to consider:

- whether there are safeguards built into the system that protect against messages being corrupted or deleted in transmission by the input channel;
- whether these safeguards protect against all possible threats to the input channel (for example, deliberate attacks on the channel, as opposed to random failures);
- whether the source of the input is trustworthy, or whether it is possible for the input source to have been compromised;
- whether there is adequate protection at the application level to guard against malicious messages generated by an attacker who controls the input source.

With this approach in mind, we performed a systematic analysis of the ERTMS/ETCS specifications from a security perspective by examining the on-board ETCS application, and considering its interfaces and trust relationships with other components of the ERTMS/ETCS system, both trackside and on-board the train.

7 Weaknesses and vulnerabilities

Based on our analysis of the trust relationships, we identified a set of potential weaknesses and vulnerabilities in the ERTMS interoperability specifications, which we outline here. The details can be found in our full report [1].

7.1 General observations

Safety is always paramount in railway systems, and ERTMS/ETCS is designed to be a safe system. Thus, the general philosophy is 'if in doubt, stop the train', which means that it is very difficult for an attacker to engineer a train accident. However, it is possible for an attacker to exploit the 'fail-safe' behaviour of ERTMS, and create a situation that causes a train to halt. Thus, denial of service attacks are possible, and could be launched at a time and place of the attacker's choosing, perhaps designed to cause maximum disruption or passenger discomfort, for example, by arranging for a train to halt in a tunnel.

Nevertheless, most attacks exploiting ERTMS/ETCS would require the attacker to have physical access to the railway line and are therefore localised in their impact; attacks that cause disruption over a wide area depend on compromising the GSM-R network. The threats and vulnerabilities posed by GSM-R depend very much on the national implementation of GSM-R and its supporting telecommunications network.

Moreover, some of the most critical elements of the ERTMS/ETCS system, for example, the interfaces between the control centres and the RBCs, are outside the scope of the ERTMS/ETCS specifications, which are only concerned with interoperability and do not address implementation issues within a single ERTMS/ETCS system. However, it is important to ensure that these interfaces remain logically separate and secure during the migration of existing control systems towards ERTMS, because this process will involve the integration of installations that are currently separate, and the use of multi-purpose transmission networks that carry messages for different applications with varying degrees of criticality.

One of the major vulnerabilities of ERTMS/ETCS is that it is a data-driven system, and therefore any compromise to the data held by the RBCs could cause a serious accident. However, the procedures for managing and updating this data fall outside the scope of the ERTMS/ETCS specifications.

Similarly, the security of the Euroradio protocol [4] used to safely transmit movement authorities depends on the security of the key management and key distribution process. There is a specification for off-line key management between key management domains [5], but the procedures for key management within a key management domain are a matter for the national or local implementation.

Nevertheless, the specification for off-line key management [5] defines a set of security requirements that must be met by the operational key management systems in each key management domain. These requirements, together with compliance with the off-line key management specification, provide a basis for secure key management between key management domains.

Ideally, the ERTMS/ETCS specifications would impose a similar set of requirements on other parts of the system that are managed by national authorities, for example, the interface between control centres and RBCs.

7.2 Specific observations

The on-board ETCS system needs to interact with a number of other systems, and it is therefore possible to draw conclusions about the security of ERTMS/ETCS with respect to each of these interfaces.

Driver/Train. The driver and train interfaces are only specified at a functional level, but the interfaces to these systems are fairly narrow and limited. However, clearly both the driver and the train itself are trusted components of the system: the driver because he could override the entire ERTMS/ETCS system, and the train because it could have been sabotaged in other ways, such as compromising the braking system. In the present specifications, there is no authentication on the communication channels that are used for these interfaces. This is only acceptable as long as these driver and train interfaces remain part of a closed network that is only connected to the on-board ETCS system. If the ETCS system were ever to be connected to an on-board network that also carried non-critical messages, for example, passenger access to the Internet, then there would be a very real possibility of ETCS being compromised by a virus or deliberate intervention.

Balises. Messages from balises are protected against accidental transmission errors and interference from outside the immediate area of the track. However, the interface does not address the possibility that an attacker might have subverted existing balises, or placed a new balise on the track at a strategic location. Although various levels of data consistency checks are built into the ERTMS/ETCS, balises provide no authentication guarantees, which opens up the possibility of malicious attacks via the balise interface, since the data received from a balise is effectively trusted by the system.

In particular, the ERTMS specifications make a distinction between linked and unlinked balises. Trains are informed about the locations of linked balises in advance as part of their movement authorities, which are transmitted by radio over a secure channel; failure to encounter a linked balise in the expected location will cause the train to halt. However, trains must also be prepared to react to unlinked balises, which can be encountered anywhere. Although trains will only accept a limited number of commands from an unlinked balise, an attacker can exploit almost all of these commands to a greater or lesser extent. Most of these attacks would result in some form of denial of service, but some commands can be used to create a hazardous situation.

Euroradio. The Euroradio protocol [4] uses a shared secret key to establish a secure communications channel. The protocol guarantees authenticity and integrity of messages, but does not guarantee confidentiality. Thus, if the underlying GSM-R network

were to be compromised, it would be possible for an attacker to eavesdrop on ERTMS messages and perhaps learn sensitive information. In particular, the ability to eavesdrop on messages also makes it easier for an attacker to intercept communications using a 'man in the middle' attack.

Otherwise, the Euroradio protocol appears to be sound from a security perspective, although we are not aware of it ever having been subjected to a formal cryptographic analysis. However, the specification prescribes the use of Triple DES (Data Encryption Standard) as the underlying cryptographic algorithm rather than a more modern algorithm such as AES (Advanced Encryption Standard). Triple DES is no longer recommended for use in new cryptographic systems and the Euroradio specification should be upgraded accordingly, but for ERTMS, a bigger problem is managing key distribution on the scale of an international railway network.

The ERTMS/ETCS interoperability specifications only deal with secure key management between different key management domains [5], leaving key distribution within a key management domain to the national implementation. A new specification has recently been published that deals with the distribution of keys to ETCS entities (trains and trackside devices) within a key management domain [6], but the current standards mandate an off-line key management solution, which is not practical, particularly if there is a requirement to refresh or revoke keys. For example, in the UK, depending on the key allocation policy, there could be as many as 400,000 keys to manage.

Voice. GSM-R extends the basic GSM network services with some special services that are required for railway operations. Standardised numbers are used to address onboard functions, and an attacker with access to the GSM-R network and an authorized SIM (Subscriber Identity Module) card could cause considerable disruption.

GSM-R. GSM-R is built on top of GSM, which is known to be fundamentally insecure [7]. In particular, GSM uses weak encryption algorithms and does not provide any form of network authentication, which means that GSM networks are vulnerable to a 'man in the middle' attack. Also, an attack on the GSM-R network could bring down the ERTMS/ETCS system over a large area, creating a wide area denial of service attack. The engineering of the GSM-R network is critical to addressing these risks.

8 Scenario analysis

Having identified some potential vulnerabilities in the ERTMS specifications, we devised attack scenarios to explore the ways in which an attacker could exploit these potential weaknesses and vulnerabilities to achieve one of the undesirable outcomes listed in section 4. In this section, we explain our methodology for constructing these scenarios and summarise our overall assessment. Full details can be found in our report [2].

We devised seven attack scenarios and then analysed each scenario in detail by considering the following questions:

- **How** is the attack performed?
- **What** vulnerabilities does the attack exploit?
- **Where** can the attack be launched from?
- **What** are the possible mitigations?

We then graded each attack according to a range of criteria:

- The **type of access** required to exploit a vulnerability;
- The **level of technical sophistication** required to exploit a vulnerability;
- The **type of failure** caused by a successful attack;
- The **scale of effect** for a successful attack;
- The **scalability of the attack** from the attacker's perspective;
- The **type of impact** caused by a successful attack;
- The **types of mitigation strategy** that are possible;
- The **level of difficulty** for implementing each mitigation.

Our analysis and grading methodology was partially based on a technique for scenario analysis that was devised by a NATO Research Task Group for a study on the Dual Use of High Assurance Technologies [8].

We considered several different categorisations but chose these particular categories because we thought they were the most informative and provided a good summary of the issues raised by each scenario. We deliberately did not attempt to rank the various attack scenarios using a weighted average of the category scores because we believe that such a ranking would be too simplistic – the relative weighting of the various categories and the ranking of the scenarios is a matter for government and industry stakeholders. Similarly, we did not attempt to estimate the likelihood of attacks being successful because this would depend on the national implementation of ERTMS and is therefore best left to the domain experts. Instead, we used colour coding (HIGH, MEDIUM, Low) to highlight the issues, as shown in Table 1.

Minimum access required	*Technical sophistication*	*Type of failure*	*Scale of effect*	*Scalability of the attack*	*Type of impact*	*Mitigation strategies*	*Ease of mitigation*
REMOTE ACCESS ACCESS TO INFRASTRUCTURE, BUT NOT THE TRACK SUPPLY CHAIN ACCESS Physical access to the track	LOW MEDIUM High	LOSS OF LIFE DENIAL OF SERVICE	GLOBAL NATIONAL REGIONAL Local	HIGH MEDIUM Low	SAFETY-CRITICAL ECONOMIC POLITICAL Psychological	REACTIVE Preventive	HARD MEDIUM Easy

Table 1. Grading of the issues

Using this colour coding, we summarise our grading of each attack scenario in Table 2 to enable the scenarios to be easily compared.

Broadly speaking, attacks that can be launched remotely do not require a high level of sophistication and are highly scalable – however, such attacks are relatively easy to mitigate. Conversely, attacks that require local access are less scalable but also more difficult to mitigate. Hence important trade-offs need to be made by the relevant decision makers and risk managers. The advantage of the analysis and grading approach presented here is that it identifies these trade-offs and helps decision makers to make more informed decisions.

	Minimum access required	*Technical sophistication*	*Type of failure observed*	*Scale of effect*	*Scalability of the attack*	*Type of impact*	*Mitigation strategies*	*Ease of mitigation*
Scenario 1	REMOTE ACCESS	LOW	DENIAL OF SERVICE AND LOSS OF LIFE.	LOCAL/ GLOBAL	HIGH	SAFETY-CRITICAL AND/OR PSYCHOLOGICAL	Preventive and reactive	Easy
Scenario 2	REMOTE ACCESS	LOW	DENIAL OF SERVICE	LOCAL/ GLOBAL	HIGH	ECONOMIC, POLITICAL	Preventive and reactive	Easy
Scenario 3	REMOTE ACCESS	LOW	DENIAL OF SERVICE	LOCAL/ GLOBAL	HIGH	ECONOMIC, POLITICAL	Preventive and reactive	Easy
Scenario 4	REQUIRES ACCESS TO WIRELESS CELL.	High	DENIAL OF SERVICE	Local	MEDIUM	ECONOMIC, POLITICAL	REACTIVE	MEDIUM
Scenario 5	REQUIRES ACCESS TO WIRELESS CELL.	High	DENIAL OF SERVICE AND LOSS OF LIFE	Local	Low	SAFETY-CRITICAL AND/OR PSYCHOLOGICAL	Preventive and reactive	MEDIUM
Scenario 6	Physical access to track	LOW	DENIAL OF SERVICE AND LOSS OF LIFE	Local	Low	SAFETY-CRITICAL AND/OR PSYCHOLOGICAL	REACTIVE	HARD
Scenario 7	Physical access to track	MEDIUM	DENIAL OF SERVICE AND LOSS OF LIFE	Local	Low	SAFETY-CRITICAL AND/OR PSYCHOLOGICAL	REACTIVE	MEDIUM

Table 2. Grading of the issues

9 Related work

We are aware of some related work, but to the best of our knowledge, this is the first holistic study that analyses the security of ERTMS at the level of a national infrastructure and considers the potential impact of an ERTMS implementation being compromised. In a paper published around the time of the development of the Euroradio protocol, one of the authors of the specification discusses the safety and security requirements for the technology [9]. More recently, ERTMS has attracted the atten-

tion of security researchers and we are aware of two presentations in German [10,11] that touch on some of the issues identified in our more detailed and extensive study, which pre-dates this German work. One of these presentations was to the Chaos Communication Congress in Berlin and attracted a lot of media attention [12], although the media reports were rather confused and made little sense to rail engineers familiar with the technology [13].

10 Discussion and Conclusions

Safety and security are both forms of dependability and use similar techniques to assess the impact of possible failures on the overall behaviour of a system. In general, a safety assessment assumes that failures have accidental causes rather than deliberate causes. In contrast, a security analysis tends to assume a worse case scenario in which all failures are possible.

Nevertheless, safe systems need to be secure – if they are not secure, then they are not safe. A safety analysis that does not consider hazards that could be caused by underlying security vulnerabilities is deficient.

In practice there may be conflicts between security requirements and safety requirements. For example, in an emergency situation, a timely response may be more important than a secure response. Moreover, safety concerns are rather different from security concerns: confidentiality is not usually a safety concern, and in fail-safe systems such as ERTMS, availability is considered to be a reliability issue rather than a safety issue. In contrast, security is traditionally concerned with confidentiality, integrity and availability. A failure of confidentiality would not be considered a safety concern, but would definitely be a security concern. Similarly, fail-safe behaviour is important from a safety perspective but conflicts with the security requirement to maintain availability.

In this paper we presented the results of a security audit of the ERTMS interoperability specifications. ERTMS is designed to be a safe system and the general philosophy is ‘if in doubt, stop the train’. This ‘fail-safe’ behaviour makes it relatively easy for an attacker to bring trains to a halt. Causing an accident is more difficult but not impossible – it is important to remember that ERTMS does not drive the train and it is the driver who is ultimately responsible for the safety of the train. However, as the speed and number of trains increases, the ability of the driver to react to critical issues in a timely fashion may become limited, forcing the system to become more dependent on automated control.

Some of the vulnerabilities we identified depend very much on the specific details of the national implementation of ERTMS and GSM-R. Moreover, some of the most critical parts of an ERTMS implementation (e.g., the interface between the control centre and the RBCs) are outside the scope of the ERTMS/ETCS specifications, which are only concerned with interoperability and do not address implementation issues within a national implementation. Thus, a complete security analysis would need to consider the whole of the national railway infrastructure.

More generally, our work has highlighted the need to ensure that security issues are taken into account when preparing safety cases [14], and we plan to do more work on "security-informed" safety cases, particularly in the context of the Artemis-JU project on Security and Safety Modelling for Embedded Systems (SESAMO) [15].

11 Acknowledgments

Our original research was commissioned on behalf of the UK railway industry and UK government and we are grateful to our sponsors who commissioned the research and facilitated discussions with key railway stakeholders that were invaluable to us in developing our scenarios and validating our work. Our current research is partially funded by Artemis-JU as part of SESAMO (project number 295354).

References

1. Bloomfield, R., Stroud, R., Gashi, I., Bloomfield R., Information Security Audit of ERTMS, Technical Report, 2010.
2. Stroud, R., Gashi, I., Bloomfield, R., Bloomfield, R., ERTMS Specification Security Audit – Analysis of Attack Scenarios, Technical Report, 2011.
3. UNISIG SUBSET-026, System Requirement Specification, Version 2.3.0, http://www.era.europa.eu/Document-Register/Pages/UNISIGSUBSET-026.aspx
4. UNISIG SUBSET-037, Euroradio FIS, Version 2.3.0, http://www.era.europa.eu/Document-Register/Pages/UNISIGSUBSET-037.aspx
5. UNISIG SUBSET-038, Offline Key management FIS, Version 2.3.0, http://www.era.europa.eu/Document-Register/Pages/UNISIGSUBSET-038.aspx
6. UNISIG SUBSET-114, KMC-ETCS Entity Off-line KM FIS, Version 1.0.0, http://www.era.europa.eu/Document-Register/Pages/UNISIGSUBSET-114.aspx
7. Quirke, J., Security in the GSM system, 2004.
8. Bloomfield, R., Craigen, D., Miller, A., Dual Use of High Assurance Technologies, Technical Report, 2009. http://www.rto.nato.int/Pubs/rdp.asp?RDP=RTO-TR-IST-048
9. Braband, J., Safety and Security Requirements for an Advanced Train Control System, Proc. 16th International Conference on Computer Safety, Reliability and Security (Safecomp'97), York, Springer, 1997.
10. Stump, F., Datenübertragung über öffentliche Netze im Bahnverkehr – Fluch oder Segen?!, Safetronic 2010.
11. Katzenbeisser, S, Can trains be hacked? Die Technik der Eisenbahnsicherungsanlagen, 28th Chaos Communication Congress, Behind Enemy Lines, December 2011.
12. BBC News, Train-switching technology 'poses hacking threat', December 2011. http://www.bbc.co.uk/news/technology-16347248
13. RailUK Forum, BBC News: Hackers could delay trains, December 2011. http://www.railforums.co.uk/showthread.php?t=57565
14. Bloomfield, R.E., Guerra, S., Miller, A., Masera, M., Weinstock, C.B: International Working Group on Assurance Cases (for Security), IEEE Security and Privacy, Vol. 4 (3), pp. 66-68, 2006.
15. SESAMO – Security and Safety Modelling, ARTEMIS Embedded Computing Systems Initiative 2011, Project Number 295354, May 2012.