SAE International

2013-01-1415
Published 04/08/2013

doi:10.4271/2013-01-1415
saepcelec.saejournals.org

Threat Analysis and Risk Assessment in Automotive Cyber Security

David Ward, Ireri Ibarra and Alastair Ruddle
MIRA Ltd

ABSTRACT

The process of hazard analysis and risk assessment (H&R or HARA) is well-established in standards and methods for functional safety, such as the automotive functional safety standard ISO 26262. Considering the parallel discipline of cyber security, it is necessary to establish an analogous process of threat analysis and risk assessment (T&R) in order to identify potential security attacks and the risk associated with these attacks if they were successful.

While functional safety H&R processes could be used for threat analysis, these methods need extension and adaptation to the cyber security domain. This paper describes how such a method has been developed based on the approach described in ISO 26262 and the related MISRA Safety Analysis Guidelines. In particular key differences are described in the understanding of the severity of a security attack, and the factors that contribute to the probability of a successful attack. However it also acknowledges that some threats may contribute to a safety-relevant hazard.

The paper will also explore some potential future directions, such as how the T&R can be used to support an assurance case for cyber security.

CITATION: Ward, D., Ibarra, I. and Ruddle, A., "Threat Analysis and Risk Assessment in Automotive Cyber Security," *SAE Int. J. Passeng. Cars – Electron. Electr. Syst.* 6(2):2013, doi:10.4271/2013-01-1415.

INTRODUCTION

Functional safety is defined in very general terms as the part of the overall safety of a system that depends on it operating correctly in response to its inputs. More specifically, the automotive standard for functional safety, ISO 26262 [1], is concerned with preventing hazards that may result from malfunctions of electronic systems. In ISO 26262, a "hazard" is defined as a potential source of harm, and the definition of "harm" is restricted to physical injury or damage to the health of a person.

In contrast in IEC 61508 [2] (the generic standard for functional safety which ISO 26262 claims to be derived from), harm is more widely defined and can include environmental or economic effects. This reflects the origins of IEC 61508 in the industrial process control sector, but is a reminder that in more general terms the definition of "harm" can be wider than just personal injury.

An area of increasing importance for the automotive domain is "cyber security". Electronic control systems in vehicles now rely heavily on networked communications between individual electronic controllers. While historically an individual vehicle has operated in isolation, the possibility of communications with the in-vehicle network from "outside" has become a reality. The legitimate motivations for such communications include

• "End of line" programming, where the software for a specific vehicle configuration is loaded (or "flashed") into its electronic controllers at the end of the vehicle's construction;

• Service actions, such as reading diagnostic data through the on-board diagnostic (OBD) port and "reflashing" of software to apply updates in the field;

• The use of consumer devices (also known as "nomadic" devices) which typically interface with the vehicle's information and entertainment ("infotainment") systems through a standardized wired (USB) or wireless (Bluetooth) connection;

• Vehicle-to-X (V2X) communications, where vehicles communicate with each other and with the transport infrastructure through a mobile *ad hoc* network.

Inevitably the existence of these external communications interfaces also creates the possibility for non-legitimate use, whether accidentally or by persons with nefarious motivations. This means it is necessary to secure the networks against unintended intrusion and use. Note that "security" requirements for road vehicles already exist but are

traditionally concerned with anti-theft provisions, e.g. [3]. Consequently, and also reflecting the wider association with IT security, this paper uses the term "cyber security" to refer to the security of vehicle networks and communications.

From a functional safety perspective, standards such as ISO 26262 describe how to design an electrical or electronic (E/E) system to provide adequate assurance that hazards will not be caused by failures in the system. A central tenet of systems safety engineering in this context is that it is not possible to completely eliminate all possible causes of hazards; instead system safety engineering seeks to determine that sufficient measures have been taken to reduce the risks associated with these hazards to an acceptable level (called "freedom from unacceptable risk" in ISO 26262). Risk is a function of both the probability of harm occurring and the severity associated with that harm. It therefore follows that hazards with higher associated potential harm will require more stringent controls for reducing the probability that the hazard occurs. In terms of E/E systems this is commonly addressed through safety integrity, and standards often have discrete levels of safety integrity such as SIL (IEC 61508) or ASIL (ISO 26262) in order to set targets on the systems. Both SIL and ASIL are associated with graded levels of increasing rigor in the specification, development and verification of safety-related E/E systems, with increased rigor applied to systems where there is a greater need for risk reduction through preventing the failures of the system that can lead to the hazard.

Functional safety standards have a process for evaluating the risk associated with a system and specifying the requirements to reduce that risk to an acceptable level. In outline the process is typically as shown in Figure 1 below.

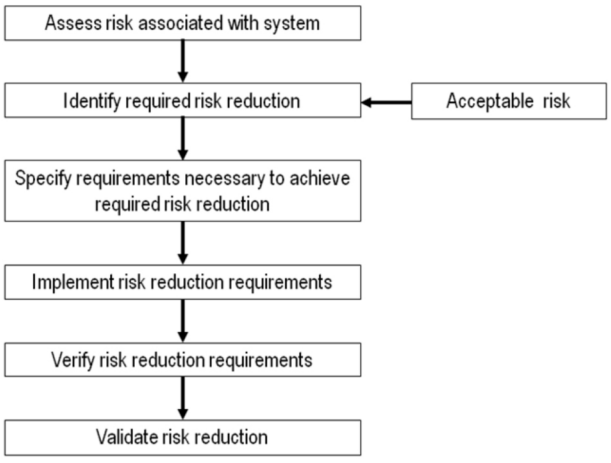

Figure 1. Typical functional safety process

The process of performing a hazard analysis and risk assessment (sometimes referred to as an H&R, or a HARA) is concerned with the first three steps of this process. It is well-established in standards and guidelines for functional safety such as IEC 61508 [2], ISO 26262 [1] and the MISRA Safety Analysis guidelines [4].

The standard IEC 15408 [5] is concerned with security evaluation for IT products, but does not explicitly address the possible safety implications of security breaches for safety-related control systems. A further limitation is that it does not provide a framework for risk analysis. Methods for evaluating the probability of a successful attack (described as "attack potential") are described in IEC 18045 [6], but the severity of the impact is not evaluated to allow risk to be assessed. Risk analysis in an IT security context is outlined in [7] and described in more detail elsewhere (e.g. [8], [9]).

In IEC 15408 the concept of "evaluation assurance levels" (EAL) has a similar role for security considerations to the SIL and ASIL categories used in the functional safety context. The EALs are similarly associated with graded levels of increasing development rigor.

EXPANDING H&R TO T&R

In the second edition of IEC 61508 [2] published in 2010, there is reference to consideration of cyber security issues with regards to their potential impact on functional safety. However, cyber security threats that are not safety-related, such as those affecting privacy or financial transactions, are beyond the scope of IEC 61508.

In the European collaborative research project EVITA [10], a unified approach to risk analysis specifically for cyber security and security-related functional safety threats to in-vehicle networks was developed. The overall aim of the project was to prototype a toolkit of techniques and components to ensure the security of in-vehicle systems, including security hardware, software, and analysis methods, as well as an evaluation of the associated legal aspects. The EVITA project was focused on in-vehicle networks, as other projects have addressed issues relating to the security of V2X communications. However the scope of cyber security threats in EVITA considered those wider issues noted above that are outside the scope of IEC 61508 Edition 2.

The MISRA "Development Guidelines for Vehicle Based Software" [11] identified the need to protect vehicle software from unauthorized access that could compromise the performance of safety-related systems, as well as to provide detection of such tampering. As an historical observation, the concept of (safety) integrity levels introduced in this document was in part inspired by earlier work on security evaluation assurance levels.

The similarities between the EAL and SIL/ASIL concepts suggested the potential for developing a unified approach for automotive functional safety and cyber security [12]. Similar observations have also been made with regard to security and safety analysis in other fields, such as mobile *ad-hoc* networks [13] and defense applications [14].

Unifying the engineering processes for functional safety and cyber security may offer potential benefits in terms of reduced development costs through:

• Re-use of risk analysis for those applications where cyber security may also have possible functional safety implications;

• Deployment of common solutions to achieve both safety integrity and security integrity;

• Sharing of evidence in an assurance case.

While alignment is needed over all aspects of the lifecycle, the work in EVITA specifically concentrated on a unified approach to threat analysis and risk assessment [15]. The term "threat" is used generically to cover both functional safety hazards (which may result in physical harm), and cyber security breaches that result in other types of quantifiable losses.

In developing such a unified process it is necessary to consider what "risk" means in the context of cyber security, and specifically how to interpret the severity and probability factors associated with a threat.

Severity

The starting point for the severity classification is the categories given in ISO 26262. This defines three classes of severity (S1, S2 and S3), which are defined in terms of the estimated personal injury that could result from the hazard. A fourth class (S0) is reserved for hazards that could result in some physical damage but no significant personal injury. In practical use, the severity classes are often calibrated with respect to a defined scale such as the Abbreviated Injury Scale (AIS).

An important restriction of scope of ISO 26262 is that any technical failure resulting in a hazard can only affect a single vehicle. In contrast, a cyber security threat that has a potential functional safety consequence may affect multiple vehicles. It was therefore necessary to extend the definitions of the severity classes to include the potential consequences for multiple vehicles, and to include a fourth class, S4, for threats that have the potential to cause the most severe consequences in multiple vehicles. It should be noted that such a higher classification of severity already exists in the MISRA Safety Analysis guidelines and is reserved for cases involving multiple vehicles.

As well as considering functional safety related consequences of cyber security threats, it was also necessary to extend the definition of "severity" to cover non-safety consequences.

Breaches in the security of vehicle information or functions could lead to possible issues for stakeholders in four main areas:

• Privacy - unwanted or unauthorized acquisition of data relating to vehicle/driver activity, vehicle/driver identity data, or vehicle/sub-system design and implementation.

• Financial - unwanted or unauthorized commercial transactions.

• Operational - unwanted or unauthorized interference with on-board vehicle systems or V2X communications that may impact on the operational performance of vehicles and/or intelligent transportation systems (ITS) (without affecting physical safety).

• Safety - unwanted or unauthorized interference with onboard vehicle systems or V2X communications that may impact on the safe operation of vehicles and/or ITS.

An important consequence of considering these four aspects collectively is that the severity of an attack, which is a measure of the impact of the harm for the stakeholders, becomes a "severity vector" with four components relating to safety, privacy, financial and operational threats. Each of these components may have different ratings, rather than a single severity parameter for all aspects. For example, it is possible that an attack has little or no impact on safety, but presents significant risks in terms of compromised driver privacy or loss of reputation for vehicle manufacturers. Thus, the individual components may translate to quite different relative risk levels, depending on the probability measures that are applied to assess the associated risk level.

Table 1 shows how the safety-related component of severity is classified. Entries in *italics* are extensions to the definitions of ISO 26262.

Table 1. Safety-related component of severity

Class	Safety-related severity
S0	No injuries
S1	Light or moderate injuries
S2	Severe and life-threatening injuries (survival probable) *Light or moderate injuries for multiple vehicles*
S3	Life threatening (survival uncertain) or fatal injuries *Severe injuries for multiple vehicles*
S4	*Life threatening or fatal injuries for multiple vehicles*

Tables 2, 3, 4 show how the non-safety-related components of severity are classified.

Table 2. Privacy-related component of severity

Class	Privacy-related severity
S0	No unauthorized access to data.
S1	Anonymous data only (neither specific driver nor vehicle data)
S2	Identification of vehicle or driver Anonymous data for multiple vehicles
S3	Driver or vehicle tracking Identification of driver or vehicle, for multiple vehicles
S4	Driver or vehicle tracking for multiple vehicles

Table 3. Financial-related component of severity

Class	Financial-related severity
S0	No financial loss
S1	Low-level loss (~$10)
S2	Moderate loss (~$100) Low losses for multiple vehicles
S3	Heavy loss (~$1,000) Moderate losses for multiple vehicles
S4	Heavy losses for multiple vehicles

Table 4. Operational-related component of severity

Class	Operational-related severity
S0	No impact on operational performance
S1	Impact not discernible to driver
S2	Driver aware of performance degradation Indiscernible impacts for multiple vehicles
S3	Significant impact on performance Noticeable impact for multiple vehicles
S4	Significant impact for multiple vehicles

Probability

The concept of "attack potential" is used in security evaluation techniques for IT systems [16] for both the attacker and the system under investigation. If the attack potential of the attacker exceeds the attack potential that the system is able to withstand then the attack will be successful.

The attack potential for an attack is a measure of the effort required to create and carry out a successful attack against a system. Some attackers may be willing to exert greater efforts in mounting an attack if they have the necessary resources and the benefits justify the effort required. There are multiple methods of representing and quantifying the influencing factors. The following factors should be considered in assessing the attack potential [6]:

• Elapsed time - total time taken by an attacker to identify that a particular potential vulnerability may exist, to develop a method to exploit this vulnerability, and to sustain the effort required to mount the attack.

• Specialist expertise - the required level of general knowledge of the underlying principles, product types or attack methods.

• System knowledge - specific knowledge and expertise relating to the system under attack.

• Window of opportunity - the time needed to identify and exploit a vulnerability may require prolonged access to a system that may increase the likelihood of detection. Some attack methods may require considerable effort offline, and only brief access to the target to exploit. Access may also need to be continuous or over a number of sessions.

• Equipment - hardware, software or other equipment that may be required to identify and/or exploit the vulnerability.

These factors are often not independent, but may be substituted for each other. For instance, expertise or equipment may be a substitute for time.

Attack potential has been suggested as a probability measure for security risk analysis [16]. In the risk analysis context, however, the term "attack potential" is effectively describing the difficulty of mounting a successful attack, while for risk analysis purposes a measure of probability is required. A high probability of successful attack is assumed to correspond to the "basic" attack potential, since many possible attackers will have the necessary attack potential. Conversely, a "high" attack potential suggests a lower probability of successful attacks, since the number of attackers with the necessary attack potential is expected to be comparatively small. Consequently, a scale was proposed (see Table 5) that reflects the relative probability of success associated with the attack potential in a more intuitive manner. The numerical ranking (*P*) for "attack probability" is higher for easier attacks that are associated with lower attack potentials, and lower for more difficult attacks that are associated with higher attack potentials.

Table 5. Mapping of attack potential to attack probability

Attack potential (effort required to mount successful attack)		Attack probability (relative likelihood of successful attack)	
Value	Description	Ranking (*P*)	Description
0 – 9	Basic	5	Likely
10 – 13	Enhanced basic	4	Possible
14 – 19	Moderate	3	Unlikely
20 – 24	High	2	Remote
≥ 25	Beyond high	1	Very remote

In functional safety risk analysis, the probability is evaluated by considering two qualitative parameters, exposure and controllability. "Exposure" refers to the probability that the vehicle is in a particular driving situation or environmental condition where the hazard will develop into a hazardous event. In this sense the "attack probability" and "exposure" are loosely analogous. "Controllability" refers to the possibility that the driver or other persons at risk can take some action to avoid the hazard or mitigate its risk. For cyber security threats where the potential severity includes a safety component, the risk assessment should therefore also include controllability. In ISO 26262 there are three classes of controllability (C1 to C3); the MISRA Safety Analysis guidelines include a further class C4 for genuinely uncontrollable situations that are associated with multiple vehicle applications.

Risk Classification

In common with ISO 26262, the MISRA Safety Analysis guidelines and other functional safety standards, the risk is

classified by combining the severity and probability classes using a "risk graph". Each combination of severity and probability is mapped to a security risk level R0 … R7. R0 represents the situation that no significant risk is identified and R1 to R7 represent increasing levels of security-related risk. A further class R7+ exists that signifies a risk beyond normally-acceptable levels.

Unlike functional safety risk graphs, there is not a single mapping of severity and probability to risk since:

• Severity is a 4-component vector, therefore the risk also has 4 components related to potentially different severities for different attack objectives;

• For security threats that also have a potential outcome related to functional safety, controllability also has to be considered.

An incomplete section of such a risk graph is shown in Table 6, in which the severity parameters denoted "S_S" represent the safety component of the 4-component severity vector, and the "combined attack probability" is evaluated by logical combination of the individual probabilities of success for the steps needed to mount the attack [15].

Table 6. Risk graph fragment for safety-related security threats

Controll-ability	Severity	Combined attack probability				
		A1	A2	A3	A4	A5
C1	S_S1	R0	R1	R2	R3	R4
	S_S2	R1	R2	R3	R4	R5
	S_S3	R2	R3	R4	R5	R6
	S_S4	R3	R4	R5	R6	R7

COMPARISON WITH THE ISO 26262 APPROACH TO H&R

Since the ISO 26262 approach for hazard analysis and risk assessment is being widely applied, it may be questioned why a modified approach is proposed for cyber security threat analysis.

Definition of Hazard

In ISO 26262, a hazard is defined as resulting from a malfunction of a system. An H&R can be conducted by considering only consequences of failure, although if information on potential causes is available this can also be useful in ensuring completeness of hazard identification. Nevertheless functional safety H&R is usually a high-level and top-down process.

In contrast, for cyber security threats the consequences may result from intentional actions, not only malfunctions. The use of attack trees [17] to identify the consequences of the so-called "asset attacks" developed in EVITA [15] represents a related but different approach to threat identification.

Definition of Severity

In ISO 26262 the definition of severity is only concerned with physical harm to people. Since cyber security threats can have significant consequences that do not involve injury, a wider definition of severity is needed. Consequently, "severity" in the context of cyber security is a vector quantity.

Furthermore, the extent of harm in ISO 26262 is limited to the effects on a single road user. Cyber security threats have the potential for consequences for multiple road users simultaneously. Therefore an additional severity class is needed to cater for these situations, leading to the "S4" class in the approach described in this paper.

Risk Analysis Process

A hazard analysis and risk assessment process can be generally described as the following three steps [18]:

• Hazard identification: identifying the potential consequences of system failure;

• Hazard classification: assigning values to specified parameters (such as severity, exposure and controllability) in order to identify the risk associated with each hazard;

• Risk analysis: identifying the required risk mitigation strategies to reduce the risk associated with each hazard to an acceptable level.

In ISO 26262, the second two stages are effectively combined since an ASIL value is both a hazard classification and a risk mitigation target associated with a safety goal. This is a direct consequence of the definition of hazards being due to malfunctions. However, since the severity associated with cyber security threats is multi-dimensional, it is useful to have an intermediate measure of risk that can be subject to further manipulation before targets are assigned to safety goals and security goals to prevent or mitigate the threats.

SAFETY REQUIREMENTS

In general safety requirements (compare IEC 61508) are divided into:

• Safety functional requirements: requirements for functionality required to be implemented in the system to implement a safety function (IEC 61508) or transition to and/or maintain a "safe state" (ISO 26262)

• Safety integrity requirements: requirements for reliability of safety functions (IEC 61508) or robustness of the system (ISO 26262) to control the probability of a hazard occurring during to a system failure.

Safety Functional Requirements

In ISO 26262 there is a well-defined hierarchy of safety requirements as follows:

• Safety goals (high level safety requirements to help prevent hazards or mitigate their risks);

• Functional safety requirements[1] (a design-independent strategy to fulfill the safety goals);

• Technical safety requirements (system level strategy to implement the functional safety requirements);

• Hardware and software safety requirements (which will be specifically implemented in the detailed design).

Note that specifying safety goals is an integral part of the H&R process in ISO 26262. Therefore, the principle of safety requirements can be extended to security requirements in a similar manner, starting with security goals and developing security functional requirements.

An important factor in the derivation of safety functional requirements, particularly the technical safety requirements of ISO 26262, is considering causes of hazards and mitigating them. Targets for evaluating whether the adequate coverage of potential causes has been achieved are given, for example for random hardware failures the safe failure fraction (IEC 61508) or hardware metrics (ISO 26262).

The analogous process for cyber security is to introduce counter-measures to help protect against asset attacks. Counter-measures that help protect against those asset attacks that are judged to have the highest attack probability (i.e. lowest attack potential) reduce the threat level for the associated attack method, and if the attack probability for this attack method dominates the risk level for the associated attack objective then the attack objective risk level will also be reduced.

An important result of mapping the risk analysis results to the system assets is that this naturally leads to a "defense in depth" approach [19].

Safety Integrity Requirements

In functional safety H&R, the resulting risk classification is used to specify the necessary countermeasures to reduce the risk associated with potential hazards to an acceptable level. In ISO 26262 this is measured by the automotive safety integrity level (ASIL). ASIL is one of four levels to specify the applicable requirements of ISO 26262 and the safety measures necessary to avoid an unreasonable residual risk.

Similarly the security risk level also needs to be used to identify both functional safety and cyber security integrity requirements that are appropriate to the security requirements that are to be implemented. In order to achieve this, Table 7 shows a possible mapping from the risk levels of Table 6 to the ASILs of ISO 26262 [1] and the EALs of IEC 15408 [5], as well as to the SILs of IEC 61508 [2].

Table 7. Mapping of cyber-security risk to EAL, SIL or ASIL

Risk level	EAL	SIL	ASIL
R0	0	N/A	QM
R1	1	1	A
R2	2	1	A
R3	3	2	B
R4	4	2	B
R5	5	3	C
R6	6	3	D
R7	7	4	N/A
R7+	Risk deemed beyond normally-acceptable levels		

ASSURANCE CASES

A common approach to documenting the safety of complex electronic control systems, based on experience in safety-relevant applications found in the aerospace, defense, nuclear, rail and off-shore oil industries, is to create a safety argument to demonstrate that the system is acceptably safe for the intended application and for the intended operating environment.

This paper proposes to extend the concept of a safety argument to an assurance argument, in order to cater for other types of risks, such as cyber security risks, which normally originate from malicious intentional threats.

An assurance case may thus be defined as a structured body of evidence, in the form of an argument for the intended operation of the system, typically based on a series of goals, strategies and solutions. The goals, strategies and solutions are structured in a hierarchical fashion, where each goal is supported by one or more arguments. The arguments are substantiated either by solutions, or evidence collected from different sources, such as the development process or measurable characteristics and behavior of the system itself, or by further sub goals which in turn have one or more arguments and the associated evidence supporting them.

The important points in a safety argument are that

• Absolute safety (i.e. zero risk) is recognized as unachievable, although mitigation measures must be implemented as necessary to ensure that any residual risks are deemed to be acceptable;

• The safety argument only applies to the intended application and operating environment.

Safety arguments have been widely used for demonstrating that a system meets its required safety objectives; translating this to the cyber security domain will result in an assurance argument, containing claims to address risks associated with both functional safety and cyber security. This is particularly relevant for networked vehicles, since the operating environment is known to include hackers and criminals who are already actively engaged in security

[1] Note that the "functional safety requirements" of ISO 26262 are a subset of the "safety functional requirements" of IEC 61508. The latter term does not appear in ISO 26262.

attacks against existing computer networks and can be expected to turn their attention to vehicles in future. Thus, an assurance case for vehicle applications should also take account of safety-related cyber security threats.

Following from Figure 1, the assurance argument can be structured around the same steps; for the first three steps, where H&R and T&R are implicitly allocated, the assurance argument can therefore initially be divided to meet two main goals: the identification of hazards to leading to functional safety risk; and the identification of threats leading to cyber security risk.

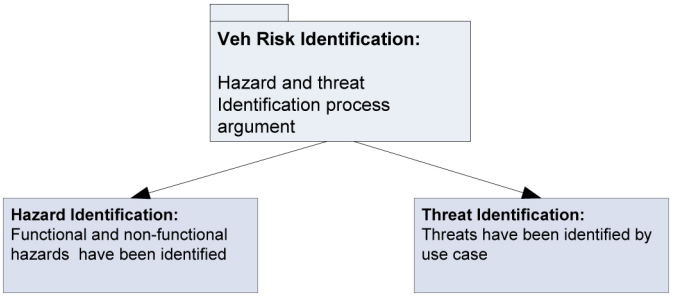

Figure 2. Hazard and threat identification

CONCLUSIONS

This paper has demonstrated how a parallel process to functional safety hazard analysis may be developed for threat analysis in cyber security. This method is an extension to existing functional safety approaches, such as the ISO 26262 H&R method. However, the ISO 26262 method for H&R cannot be applied directly since the definition of "hazard" in ISO 26262 is narrower than the scope of cyber security threats, and different models are needed to identify threats. Furthermore threats can affect multiple vehicles simultaneously.

Future extensions to the work described will consider how to develop parallel processes for engineering of security requirements versus safety requirements, how to measure the effectiveness of cyber security countermeasures, and arguing for an adequate level of confidence in a system through an assurance case.

REFERENCES

1. ISO 26262, "Road vehicles - Functional safety", 2011.
2. IEC 61508, "Functional safety of electrical, electronic and programmable electronic safety-related systems", Edition 2, 2010.
3. Federal Motor Vehicle Safety Standard (FMVSS) number 114 "Theft protection".
4. MISRA "Guidelines for safety analysis of vehicle based programmable systems", ISBN 978 0 9524156 5 7, MIRA, 2007.
5. ISO/IEC 15408, "Information technology - Security techniques - Evaluation criteria for IT security", (3 parts).
6. ISO/IEC 18045, "Information technology - Security techniques - Methodology for IT security evaluation".
7. ISO/IEC TR 15446:2004, "Information technology - Security techniques - Guide for the production of Protection Profiles and Security Targets", 2004.
8. ISO/IEC 13335, "Information technology - Security Techniques - Management of information and communications technology security".
9. NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook". October 1995 [Online]. Available at: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
10. EVITA project overview, 2010 [Online]. Available at: http://www.evita-project.org
11. MISRA, "Development Guidelines for Vehicle Based Software", ISBN 0-9524156-0-7, MIRA, 1994.
12. Jesty, P.H. and Ward, D.D., "Towards a unified approach to safety and security", Proc. 15th Safety-Critical Systems Symp., Bristol, UK, February 2007, Springer, ISBN 978-1-84628-805-0
13. Clark, A., Chivers, H.R., Murdoch, J. and McDermid, J.A., "Unifying MANET safety and security", International Technology Alliance in Network-Centric Systems, Report ITA/TR/2007/02 V. 1.0, 06/11/2007 [Online]. Available at: http://www.usukita.org/papers/3155/ITA-TR-2007-02-v1.0_0.pdf
14. Lautieri, S., Cooper, D. and Jackson, D., "SafSec: commonalities between safety and security assurance", Proc. 13th Safety Critical Systems Symp., Southampton, UK, February 2005, Springer, ISBN 1-85233-952-7.
15. Ruddle, A.R, Ward, D.D. et al., "Security requirements for automotive on-board networks based on dark-side scenarios", EVITA Deliverable D2.3, 30th November 2009 [Online]. Available at: http://www.evita-project.org
16. Scheibel, M. and Wolf, M., "Security risk analysis for vehicular IT systems - a business model for IT security measures", Proc. 7th Embedded Security in Cars Workshop (escar 2009), Düsseldorf, Germany, 24th-25th November, 2009
17. Schneier, B., "Secrets and Lies - Digital Security in a Networked World", Wiley, New York, 2000, Chapter 21.
18. Ward, D., Rivett, R., and Jesty, P., "A Generic Approach to Hazard Analysis for Programmable Automotive Systems," SAE Technical Paper 2007-01-1620, 2007, doi: 10.4271/2007-01-1620.
19. Anderson R., "Security Engineering: A Guide to Building Dependable Distributed Systems", Wiley Computer Publishing, 2001, p.296.