Assurance cases to argue system resilience properties for road vehicles

Ireri Ibarra*, David Ward

*MIRA Ltd, Watling Street, Nuneaton CV10 0TU, England

Abstract

This work aims at using a safety case as a starting point to build an assurance case, in order to explore both the functional safety and cyber-security requirements of a system as an aid to system resilience.

The emphasis of the argument is placed on the shared assurance processes for functional safety and cyber security; more particularly on the relationship between cyber-security threats and functional safety hazards.

An overview of how an assurance case is presented for a given phase in the system lifecycle

Keywords: Type your keywords here, separated by semicolons ;

1. Introduction

In the past, vehicle controllers used to be standalone systems performing a specific function. With demands for increased functionality controllers then started to interact through an in-vehicle communication network; they were however still considered to be closed systems. Reliability and availability were probably the most important attributes given the relatively simple functions they performed; in addition, the supply chain was well-known and highly traceable.

At present, vehicle systems are connected via multiple networks, where controllers perform more sophisticated and complex tasks. Fault tolerance and timeliness are paramount to their operation and the focus is on safety-relevant risks due to system failure which could lead to accidents. Current vehicle systems can be used for remote unlocking, diagnostics, etc. where such a connection is on demand; operating in principle, under a controlled access policy. However, there are commercially available tools for diagnostic purposes that can be purchased off-the-shelf.

Future vehicle systems include: In-vehicle information systems (IVIS), where merging and presentation of information from several sources is typical; Advanced driver assistance systems (ADAS) utilising advanced sensor systems by increasing “perception” by vehicle systems and intervention in driver’s control; as well as further drive-by-wire. Future technologies open the vehicle for real–time, continuous communications, for example with other vehicles and the road infrastructure.

As an example of a truly distributed control system used for infrastructure communications with increasing safety-related functionality, consider “active traffic management” as initially deployed on the M42 motorway in the UK, where the use of hard shoulder is made available as a regular lane, in relation to the volume of vehicles circulating over various stretches running on the motorway.

These new technologies can potentially bring a wealth of benefits to drivers and road users; but they can also be subject to nefarious use, exploiting vulnerabilities in the system. It is therefore important to understand what such vulnerabilities can be and how they can be addressed from system design to deployment.

This is especially important for networked vehicles, since the operating environment is known to include hackers and criminals who are already actively engaged in security 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 security threats.

Several standards and guidelines have been published separately in the domains of safety and cyber-security [1] to [9]. However, there is no equivalent guidance for considering more than one of these critical system properties.

Additionally, while several EU funded projects [11] to [15] have addressed concerns about the safety, security and intelligent communications of road vehicles, consideration of more than a single critical property simultaneously has rarely been considered.

The recommended approach for establishing the safety of complex electronic control systems, based on experience in safety-related applications found in the aerospace, defence, nuclear, rail and off-shore oil industries, is to create a safety argument to show that the system is acceptably safe for the intended application and for the intended operating environment.

The important points in a safety argument are that complete safety is recognized as unachievable, although mitigation measures must be implemented as necessary to ensure that any residual risks are deemed to be acceptable, and that 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, the authors believe that a generic assurance argument can be widened and contain claims to address risks associated with cyber-security threats.

The Goal Structuring Notation (GSN) has been chosen as the preferred method to build and present the argument; the notation presented throughout the paper is consistent with that in the recently published GSN standard [16].

This paper assumes that the following two principles apply:

1. No threat shall become the cause of a hazard, and
2. In case of conflicting requirements; safety concerns take precedence over cyber security concerns.

The remaining of this paper presents a discussion on how safety cases can be extended to assurance cases and what shape the architecture of the case may have. A few examples of cases for the identification, assessment and management of risks are also presented.

2. Discussion

2.1. Assurance case vs. safety case

The term safety case has been widely defined as: A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment.

A safety argument may not be sufficient in providing a case for other critical properties of the system, which need to be considered in order to build a degree of resilience into it. Amongst these critical properties are safety, cyber-security, availability, integrity, adaptability, reliability and maintainability.

System resilience is used in this paper as the capacity of a system to cope with disruptions; amongst such disruptions are have functional safety hazards and cyber-security threats. An assurance argument can be used to show how disruptions can be identified and managed to a degree such that confidence in the system is maintained.

This paper explores expanding the concept of safety argument to an assurance argument, in order to cater for other types of risks, such as those originating from malicious intentional threats in the context of road vehicles. More importantly, the assurance argument should be able to provide reasoning as to how the different critical properties of the system are related and what measures have been taken in order to cater for cascading effects in terms of disruptions.

Similarly, an assurance case may be defined as: a structured body of evidence, in the form of an argument for the intended operation and application of the system, which provides assurance over critical properties of the system.

An argument is typically based on a series of goals, strategies and solutions. The goals, strategies and solutions are usually structured in a hierarchical fashion, where each goal is supported by one or more arguments.

In general, arguments are substantiated either by solutions, or evidence collected from different sources, such as the development process or measurable characteristics and behaviour of the system itself, or by further sub goals which in turn have one or more arguments and the associated evidence supporting them.

2.2. Case architecture

The overall architecture of an assurance case can be broken down using a regular risk management model, where risks are identified, evaluated and managed, as pointed out in Figure 1. It is conducive at early stages of the analysis to abstract at this level those critical properties to be evaluated in the system; hence both safety hazards and cyber security risks are identified in this first stage in the model.

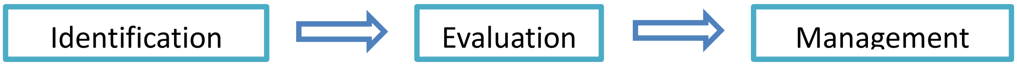

Figure 1 Risk management model

This approach starts by providing an argument per stage in this risk management model. Additionally and in order to integrate risk management activities throughout the system lifecycle, arguments to support typical concept, development, and validation activities can be incorporated., A high level view is shown in Figure 2. This high level view intends to only illustrate that several GSN modules can be used to address details of different lifecycle phases; this also intends to make the assurance case more manageable, as the information will be broken down and detailed into these different modules

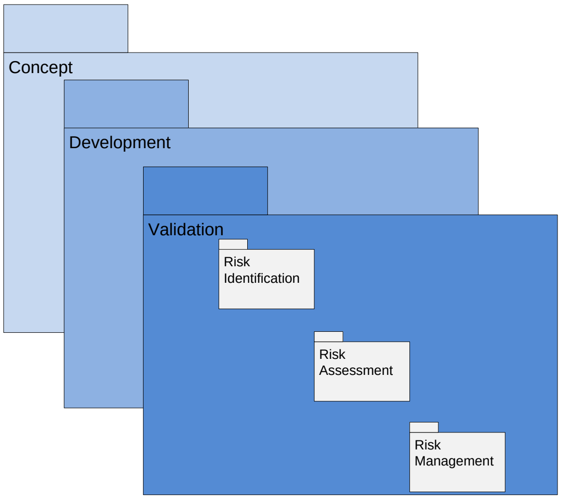

Figure 2 Arguments to cover the system lifecycle

The identification and assessment stages are likely to be revisited as the lifecycle of the system progresses; this naturally happens as a consequence of design reviews and implementation decisions; where a change in the architecture or a component results in the critical properties and requirements of the systems to be altered.

Hence it is important that the argument itself it version controlled and updates managed through a change management process; this should normally be part of the actual company’s internal processes and procedures for developing a vehicle system.

2.3. Risk identification argument

Overall the assurance argument, for example in the concept phase, can initially be constructed to address two main goals: the identification of hazards leading to safety risk; and the identification of threats leading to cyber-security risk, as seen in Figure 3. Risk ought to be identified, in order to then assess it and be able to gauge the level of effort required in the system development and design implementation.

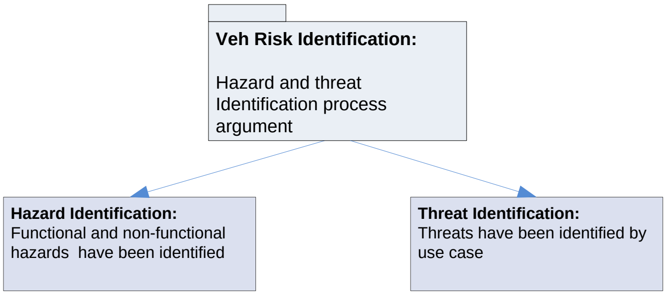
Veh Risk Identification:
Hazard and threat Identification process argument
Hazard Identification:
Functional and non-functional hazards have been identified
Threat Identification:
Threats have been identified by use case

Figure 3 Hazard and threat identification

The hazard identification goal is supported by strategies to identify functional hazards, i.e. those that result from faults in the system; and to non-functional hazards that are inherent in the design of the system, e.g. exposure to toxic substances due to the materials used in battery systems.

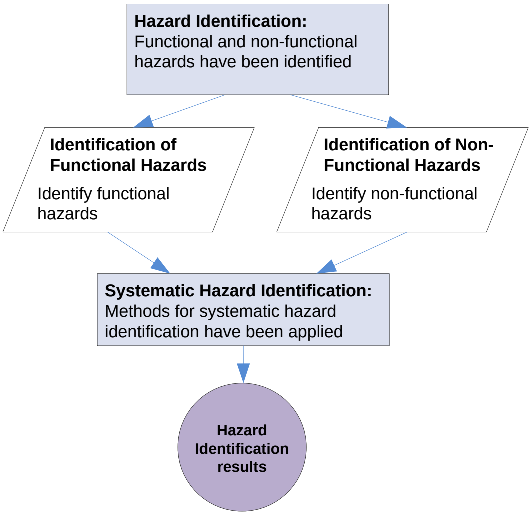
Hazard Identification:
Functional and non-functional hazards have been identified
Identification of Functional Hazards
Identify functional hazards
Identification of Non-Functional Hazards
Identify non-functional hazards
Systematic Hazard Identification:
Methods for systematic hazard identification have been applied
Hazard Identification results

Figure 4 Hazard identification

The threat identification goal is perhaps more challenging than hazard identification; while hazard identification has long been established in the safety domain and there are a variety of techniques available for this purpose, this is not the case for threats. It is important to note however, that both the identification of threats and hazards needs to be supported by a systematic approach, in order for results to be consistent and reproducible.

The identification of threats has to be constrained to those threats that have been identified in the context of the use cases of the system, in this case the vehicle. The main reason for this is that threats exploit vulnerabilities in the system and their effects are related to the context in which the vehicle is being used. Furthermore, threats tend to be malicious and intentional, which means that strategies to cope with known vehicle behaviour in the presence of faults are not applicable, as the nature of the threats and the vulnerabilities exploited is more variable.

It is however, costly and almost impossible to be able to identify every single threat; hence threats are further bound by the channels that such threats can use to exploit system vulnerabilities.

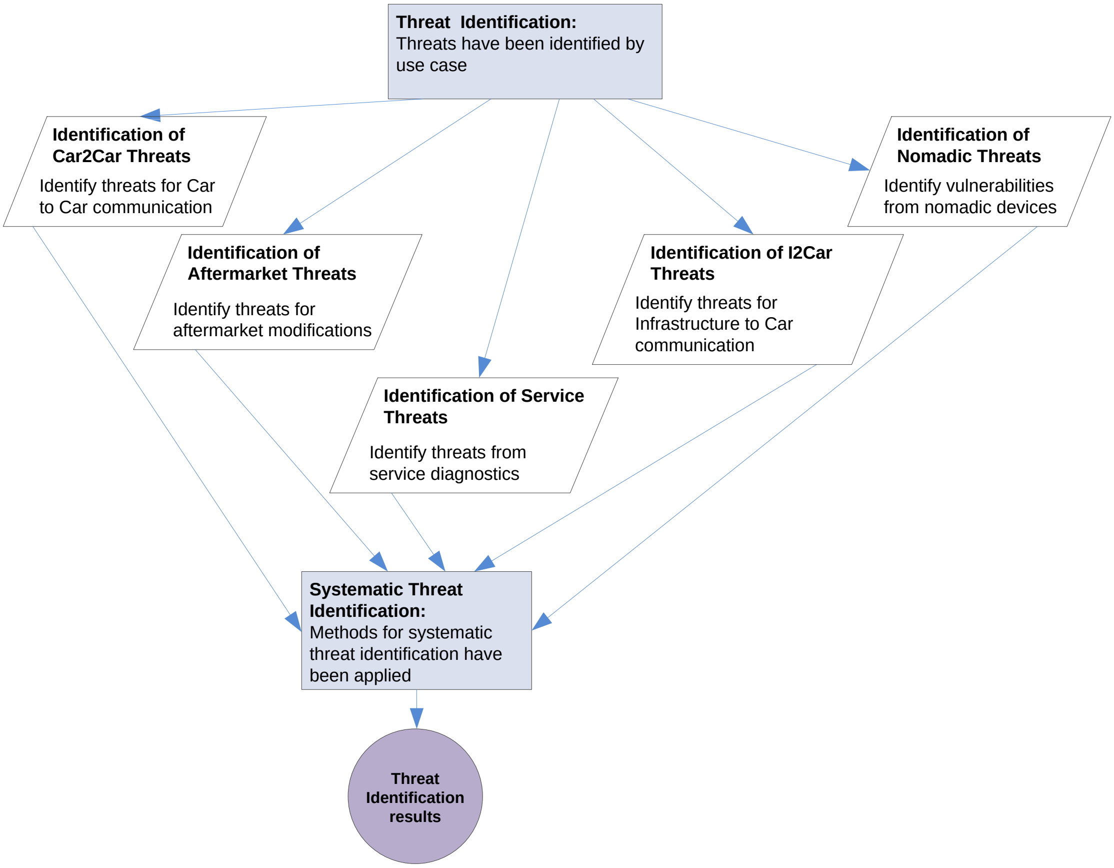
Threat Identification:
Threats have been identified by use case
Identification of Car2Car Threats
Identify threats for Car to Car communication
Identification of Nomadic Threats
Identify vulnerabilities from nomadic devices
Identification of Aftermarket Threats
Identify threats for aftermarket modifications
Identification of I2Car Threats
Identify threats for Infrastructure to Car communication
Identification of Service Threats
Identify threats from service diagnostics
Systematic Threat Identification:
Methods for systematic threat identification have been applied
Threat Identification results

Figure 5 Threat identification

Once hazards and threats have been identified, the next step is to classify them, to understand the criticality of the risk posed by them. This leads to the risk assessment goal, as shown in Figure 6.

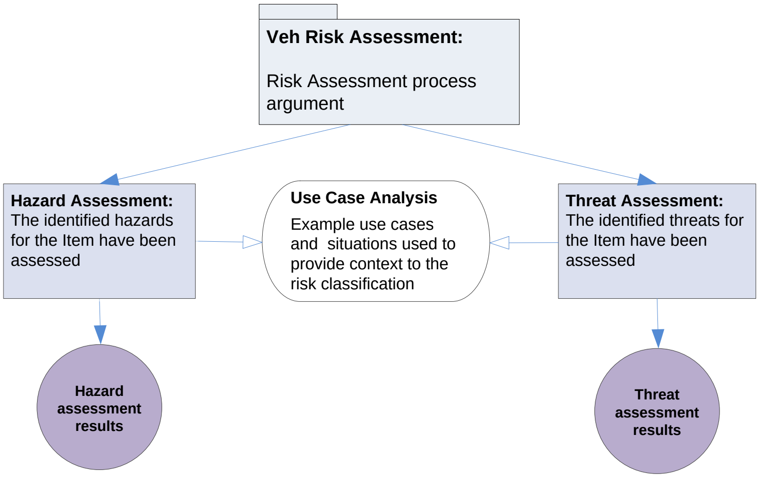
Veh Risk Assessment:
Risk Assessment process argument
Hazard Assessment:
The identified hazards for the Item have been assessed
Use Case Analysis
Example use cases and situations used to provide context to the risk classification
Threat Assessment:
The identified threats for the Item have been assessed
Hazard assessment results
Threat assessment results

Figure 6 Risk assessment

At this point, once a basic set of hazards and threats has been identified, it may be necessary to investigate further on the relationship between threats and hazards; this is in order to address the fact that in some cases, threats may further develop onto hazard sources.

2.4. Risk management argument

The risk management argument is organized in two parts: the first provides an argument over the measures for risk reduction and how these can address the causes of the identified hazards and threats, or if this is not possible, then establish mitigation measures that aim at dealing with the effects of the fault or threat. The second argues over the assurance management arrangements, such as planning and independent assessment of the risk identification, assessment and reduction phases.

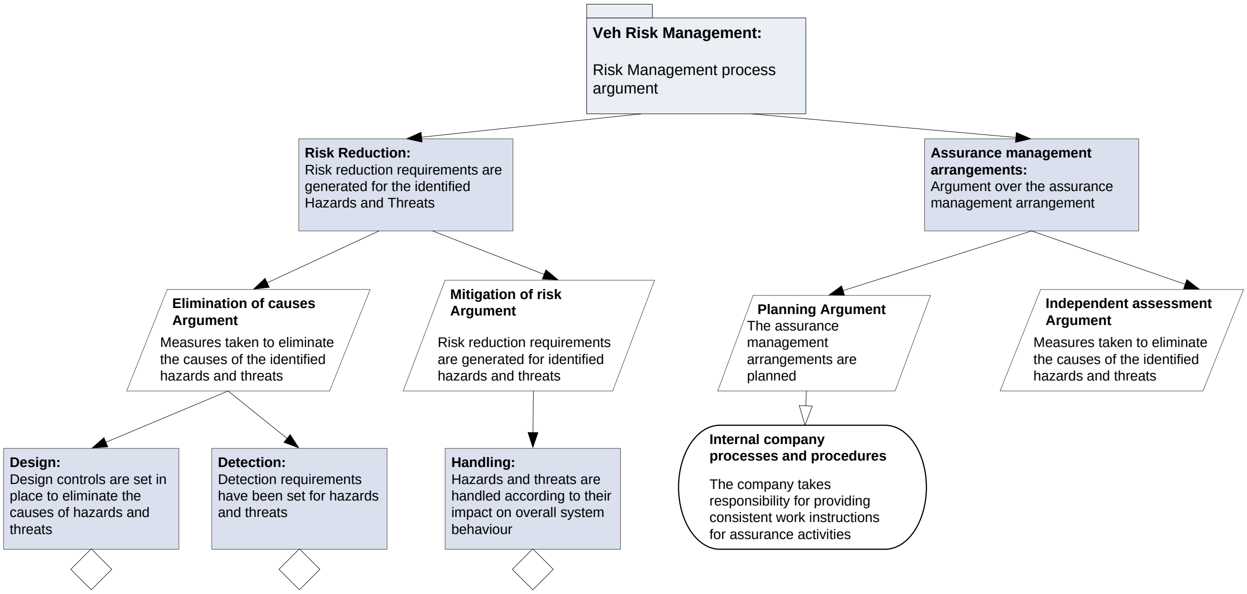
Veh Risk Management:
Risk Management process argument
Risk Reduction:
Risk reduction requirements are generated for the identified Hazards and Threats
Assurance management arrangements:
Argument over the assurance management arrangement
Elimination of causes Argument
Measures taken to eliminate the causes of the identified hazards and threats
Mitigation of risk Argument
Risk reduction requirements are generated for identified hazards and threats
Planning Argument
The assurance management arrangements are planned
Independent assessment Argument
Measures taken to eliminate the causes of the identified hazards and threats
Design:
Design controls are set in place to eliminate the causes of hazards and threats
Detection:
Detection requirements have been set for hazards and threats
Handling:
Hazards and threats are handled according to their impact on overall system behaviour
Internal company processes and procedures
The company takes responsibility for providing consistent work instructions for assurance activities

Figure 7 Risk Management argument

The risk reduction argument is shown in Figure 7 as an example of the type of measures that can be used to eliminate or mitigate risks; this however may also include other strategies pertinent to reduce the occurrence of hazards and threats. Unlike the identification and assessment arguments, the risk reduction argument requires more detailed information about the system under development, its interfaces and what particular context it is going to be deployed in.

High level, rather abstract requirements may be written at this stage to start defining the design criteria used for the detection and handling of faults; subsequently, and as the system development progresses, these requirements will be refined and detailed further.

The argument over the assurance management arrangements addresses the use of systematic processes and procedures to increase consistency and repeatability in the development of the system.

Both the risk reduction and assurance arrangements arguments are not fully developed in this example. It is expected that when such approach is taken to develop a commercial system, both arguments will be more detailed and populated as the project goes forward.

3. Conclusions

This paper presented an approach to combining a safety and cyber-security argument to address system assurance. A regular risk management model is taken as the basis to build the assurance argument over three distinct phases: identification, assessment and management of risks.

These different arguments are constructed with the use of the GSN to help organizing their complexity and size. Additionally, modularity in the arguments is central to this paper.

Future work will include the analysis of the requirements necessary to specify the interfaces between those different modules as well as include more strategies for risk management.

This approach is seen as a step forward to aid system resilience, in terms of allowing for considerations of different concerns to be elaborated in a combined form, where the interactions between safety and cyber-security concerns are specifically detailed.

Amongst the most challenging points for this approach are the completeness in the identification of threats; cyber-security attacks have a more unpredictable nature and will exploit vulnerabilities in the system, which may be introduced as emergent behaviour of the system.

Additionally, the specification of requirements to address the elimination of risks is well known for safety properties of the system, it is however not the case for cyber-security threats that may have an impact on safety.

Acknowledgements

The authors would like to thank the management of MIRA Ltd for their permission to publish this paper.

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, “Development Guidelines for Vehicle Based Software”, ISBN 0-9524156-0-7, MIRA, 1994.
5. MISRA “Guidelines for safety analysis of vehicle based programmable systems”, ISBN 978 0 9524156 5 7, MIRA, 2007.
6. ISO/IEC 15408, “Information technology — Security techniques – Evaluation criteria for IT security”, (3 parts).
7. ISO/IEC 18045, “Information technology — Security techniques — Methodology for IT security evaluation”.
8. ISO/IEC TR 15446:2004, “Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets”, 2004.
9. ISO/IEC 13335, “Information technology — Security Techniques — Management of information and communications technology security”.
10. 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

11. EVITA project overview, 2010 [Online]. Available at: http://www.evita-project.org
12. SeVeCom project overview, 2006 [Online]. Available at: http://www.sevecom.org/
13. PRECIOSA project overview, 2008 [Online]. Available at: http://www.preciosa-project.org/
14. OVERSEE project overview, 2010 [Online]. Available at: https://www.oversee-project.com/
15. Safespot project overview, 2006 [Online]. Available at: http://www.safespot-eu.org/
16. GSN Standard 211 [Online]. Available at: http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf