ISO 26262 SAFETY CASES: COMPLIANCE AND ASSURANCE

***Rob Palin*[1], *David Ward*[2], *Ibrahim Habli*[3], *Roger Rivett*[4]**

[1] MIRA Ltd, UK *(rob.palin@mira.co.uk)*;
[2] MIRA Ltd, UK *(david.ward@mira.co.uk)*;
[3]The University of York, UK *(Ibrahim.Habli@cs.york.ac.uk)*;
[4]Jaguar Land Rover, UK *(rrivett@jaguarlandrover.com*)

Keywords: Safety Cases, Assurance, Automotive Functional Safety, ISO 26262, Goal Structuring Notation.

Abstract

In the automotive domain, there is currently no formal requirement to produce an explicit safety case. Instead the implicit safety case for a vehicle is comprised of compliance with extensive national and international regulation and standards. With the imminent introduction of the automotive functional safety standard ISO 26262, the production of a functional safety case is now a requirement for compliance with the standard. This presents both opportunities and challenges to safety practitioners and researchers within that industry. This paper sets out what form an ISO 26262 safety case might take and how this fits within the existing hierarchy of automotive safety, based on the experiences of the authors who are actively engaged in the development and delivery of real automotive projects. Using the pattern and modular extensions of the Goal Structuring Notation (GSN) a number of reusable safety arguments are proposed covering all parts of ISO 26262 and the issues of compliance and assurance. The patterns proposed are not instantiated for confidentiality reasons but are provided to give guidance and shared learning for others within the automotive functional safety community.

1 Introduction

In many non-automotive industries there have been legislative or regulatory requirements for the production of a safety case before the engineered artefact can be introduced into service. Arguably the oldest example of a safety case resulted from the worst nuclear accident in Great Britain's history, the Windscale fire 1957 [1]. As a consequence, the Nuclear Installations Act 1965 was introduced and as a part of this Act the Nuclear Inspections Incorporate (NII) was founded with the authority to issue operating licenses providing a set of reports was produced justifying the safety of the design, construction and operation of the plant. Although the term 'Safety Case' was not used explicitly, this regulatory action in essence captured what is now known as the production of a Safety Case.

In contrast, although road vehicles have been in production for over a hundred years, automotive safety has been managed through compliance with extensive national and international regulation and standards; for example, the United Nations Economic Commission for European (UN-ECE) regulations [2] and the Federal Motor Vehicle Safety Standards (FMVSS) [3].

In essence, these technical regulations and standards provide the regulatory framework for the automotive industry. In Europe EU Directives implement the UN-ECE regulations. For example, EU Regulation 407/2011 lists all the UN-ECE Regulations that apply for the Type Approval of a vehicle. The UN-ECE regulations have also been adopted by other jurisdictions, for example in the Asia-Pacific region. Type Approval is used within Europe for automotive manufacturers to demonstrate compliance with the technical regulations to an independent government-appointed authority. In the UK this role is fulfilled by the Vehicle Certification Agency (VCA) [4]. Once compliance has been demonstrated to one of the government authorities, the product is approved for sale in all European countries. In contrast, the United States operates a system of self-certification, administered by National Highway Traffic Safety Administration (NHTSA) against the FMVSS.

Whilst concerned with safety, these regulations and standards are however primarily related to mechanical features and their performance, which is to be expected given that automotive engineering is historically based on mechanical engineering principles. However, with the rapid increase in vehicle functionality many of these features are now delivered with programmable electrical/electronic (E/E) systems.

1.1 Safety Cases and ISO 26262

The automotive industry has until recently mainly adopted IEC 61508 (the generic international standard for electrical and electronic systems) [5] or design instructions such as the MISRA *Guidelines for Safety Analysis of Vehicle Based Programmable Systems* [6] as examples of best practice for the development, operation and maintenance of embedded E/E systems.

The MISRA *Guidelines for Safety Analysis of Vehicle Based Programmable Systems* [6] identified the safety case as a potential way of collecting evidence in response to the fulfilment of safety requirements, and the role of the safety argument which links the requirements and evidence together. With the introduction of ISO 26262[1][18] there will be an explicit requirement for a safety case, this is captured in requirement 6.4.6.2 within Part 2 ~ Management of Functional Safety [18]:

> ***6.4.6.2*** *The safety case should progressively compile the 'work products[2]' that are generated during the safety lifecycle.*

As formulated this explicit requirement implies that the ISO 26262 Safety Case is simply the set of work products produced by the activities of the standard. This could therefore encourage a 'box ticking' mentality in compliance with the standard; namely, that an organisation may claim it has a safety case in accordance with the standard simply because it can demonstrate that the required work products exist.

ISO 26262 does contain a part dedicated to guidance on applying the standard (Part 10) that gives further explanation on the characteristics of a safety case, including the recommendation for an argument to demonstrate why the specific work products permit a claim to be made for the safety of a product. The emphasis here is on product *assurance* rather than *compliance* with the standard. This is an important point since ultimately it is a *product* that is bought and operated by consumers. However, Part 10 of ISO 26262 is 'informative' (i.e. does not contain requirements) and therefore there is no obligation, if claiming compliance with the standard, to adopt these recommendations.

It could be argued that since ISO 26262 requires an independent functional safety assessment, the assessor would ensure that the safety case contains an assurance argument. However, while a safety case is required for an 'item[3]' that has at least one safety goal assigned ASIL B or higher, independent functional safety assessment is only a requirement for ASIL C or ASIL D, and the full level of independence (i.e. complete separation in terms of managerial, financial and release authority) is only a requirement for ASIL D. Thus, there is the potential for a significant gap in terms of 'safety cases' in accordance with the standard being produced that are simply a checklist of deliverables.

In this sense, the ISO 26262 requirement for a safety case may be seen as a requirement for a *process* safety argument. In this paper, we argue that a product safety argument is also required and should form the core of the safety case. The process safety argument is also important, particularly in providing confidence in the evidence used to support the product safety argument. To this end, this paper focuses on two questions:

1. How does the ISO 26262 safety case fit within the existing implicit product safety case? The term implicit is used since in the experience of the authors the safety of a product is often not captured explicitly within a safety case. This is perhaps not an obvious question but is frequently asked by those attempting to apply ISO 26262 for the first time.
2. How best to characterise the different work products that ISO 26262 stipulates must be produced since they have different objectives?

In order to answer the two questions posed, this paper is structured in two main parts. The first, section 2, examines the issues surrounding the dependencies and context for the production of an automotive safety case which could be applicable to any automotive product whether it is a vehicle, an 'item'or a system. The second, section 3, aims to provide a safety case architecture which outlines how ISO 26262 fits within the existing framework of arguing product safety and how reusable arguments can be created. Section 4 draws some conclusions.

1.2 Contribution

Several papers [7], [8], [9] and [10] have been published regarding the development of a framework for automotive safety cases and the use of modules, patterns and models. This paper builds on this work and presents guidance for those actively involved in the development of automotive systems in compliance with ISO 26262. Furthermore it is intended to be of interest to automotive managers, and to safety engineers who are not actively involved in the automotive industry.

2 Automotive Safety Case Dependencies and Context

The validity of a safety case for an automotive product rests on a number of dependencies as shown in Figure. 1. At its core is the conceptual model 'Dependencies between elements of the Safety Case' diagram developed by Kelly [11] that illustrates the inter-dependent relationship between the four main elements of a safety case, namely:

- **Requirements** the safety objectives that must be addressed to assure safety;
- **Evidence** information from study, analysis and test of the system in question;
- **Argument** showing how the evidence indicates compliance with the requirements;
- **Context** identifying the basis for the argument presented.

[1] ISO 26262 is an adaption of IEC 61508 for the application of E/E systems within road vehicles. Adoption of ISO 26262 is purely voluntary and is not part of the current automotive regulatory framework.

[2] ISO 26262 defines a work product to '*result of one or more associated requirements of ISO 26262'*.

[3] ISO 26262 defines an item to be '*a system or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied'*.

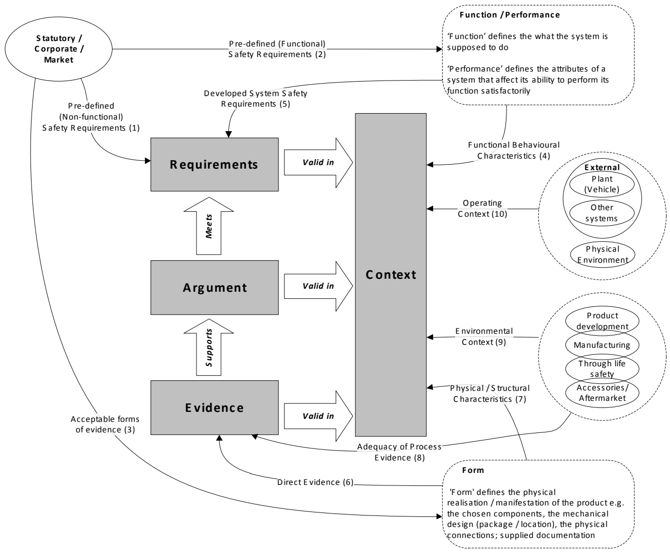
Function / Performance
'Function' defines the what the system is supposed to do
'Performance' defines the attributes of a system that affect its ability to perform its function satisfactorily
Statutory / Corporate / Market
Pre-defined (Functional) Safety Requirements (2)
Developed System Safety Requirements (5)
Pre-defined (Non-functional) Safety Requirements (1)
Requirements
Valid in
Meets
Argument
Valid in
Supports
Evidence
Valid in
Context
Functional Behavioural Characteristics (4)
External
Plant (Vehicle)
Other systems
Physical Environment
Operating Context (10)
Environmental Context (9)
Product development
Manufacturing
Through life safety
Accessories/ Aftermarket
Physical / Structural Characteristics (7)
Acceptable forms of evidence (3)
Adequacy of Process Evidence (8)
Direct Evidence (6)
Form
'Form' defines the physical realisation / manifestation of the product e.g. the chosen components, the mechanical design (package / location), the physical connections; supplied documentation

Figure 1 ~ Safety Case Dependencies

As previously stated, since it is a product that is bought and operated by consumers this product will have engineered *Form* and *Function* in order to achieve a specified set of attributes or level of performance in order to create brand differentiation. It is not claimed that the dependencies shown in figure 1, numbered from **(1)** to **(10)** represent a complete set; rather they represent the major considerations that should be made.

2.1 Requirements

There are essentially 3 different types of automotive safety requirements. On the one hand, there are predefined safety requirements (**1**) that include the statutory regulations and standards that must be met, as a minimum, in order to sell vehicles (e.g. UN-ECE, FMVSS). On the other hand, there are developed safety requirements (**5**)*,* typically generated from analysis, which specify the implementation of risk reduction measures. These developed requirements may also incorporate performance based predefined functional safety requirements (**2**). In the context of ISO 26262, examples of the developed requirements would be the 'item' safety goals or functional safety requirements.

2.2 Evidence

In view of the fact that the predefined safety requirements are explicit in what is required, some regulations and standards are also explicit in how these requirements can be satisfied (**3**). As a result, compliance with these requirements leads to the production of direct evidence taken from the testing or analysis of the product (**6**). In addition to the evidence that is directly related to the product, the adequacy and quality of the process (**8**) used to generate that evidence should also be considered. In the context of ISO 26262, an example of this could be a confirmation review.

2.3 Context

For any safety case the context of the safety case needs to be accurately defined. This is essential since '*a safety case cannot argue the safety of a system in any context*' [12]. For example, with reference to Figure 1, if an argument is being made about the functional characteristics of a product, such as its response time, then the operating, environmental and structural characteristic would all typically become declared context. Figure 1 includes four context categories for an automotive safety case:

- The functional characteristics and modes (**4**) which contextualise the safety argument based on the product's functions, performance and configuration;
- The operating context (**10**) which contextualises the safety argument based on how the product is operated, and the physical environment;
- The environmental context (**9**) which contextualises the safety argument based on the stage of the product through its life and the engineering lifecycle;
- The structural characteristics and modes (**7**) which contextualise the safety argument based on how the product has been physically implemented.

2.4 Argument

In automotive engineering the role of the safety argument is often neglected even though requirements and evidence may have been generated. This leads to a potential deficiency in the safety case as described by [11], "*Evidence without argument is unexplained – it can be unclear how the safety objectives have been satisfied*."

3 An Approach to Creating Automotive Safety Cases

In this paper, the Goal Structuring Notation (GSN) is used to represent the safety case arguments. These arguments are notation independent and as such can be represented in textual [19] or tabular formats [20].

3.1 The Goal Structuring Notation

In brief, (GSN) is a graphical notation for the representation of arguments in terms of basic elements such as goals (requirements), solutions (evidence) and strategies (argument). Arguments are created in GSN by linking these elements using two main relationships, '*supported by*' and '*in context of*' to form a goal structure.

In addition to the basic elements and relationships, GSN has two extensions: *Patterns* and *Modular* extensions. The concept of safety case patterns in GSN was developed as '*a means of documenting and reusing successful safety argument structures*' [11]. In comparison, with the adoption of modular architectures and software design principles within industry, modular GSN was developed to capture the arguments associated with this decomposition. As a result modular safety cases can be viewed as a set of well-defined and scoped modules, the composition of which defines the safety case. By allowing modules to exist in a safety case two properties must be adhered to:

1. Modules must independently stand up to scrutiny.
2. The dependency on other modules must be captured.

For a detailed description of GSN and its extensions, the reader is referred to [11] and [13].

3.2 The Architecture Framework

Using the pattern and modular extensions of GSN, a framework is proposed to explicitly capture the implicit safety case for an automotive product. This is very much a safety argument at the macro level and is shown in Figure 2. The top-level argument, '*Product Safety'*, is that the product meets its safety requirements. The emphasis of this argument is on a particular product that has been or is being developed. The intended application of this argument would be to cover specific vehicles or a specific vehicle system. At this level of abstraction this argument has a context argument '*Product Line Safety*' and it is achieved by three separate arguments covering wider product safety issues such as '*Crash Protection*', '*Particular Risks*' and '*E/E Systems Safety.*'

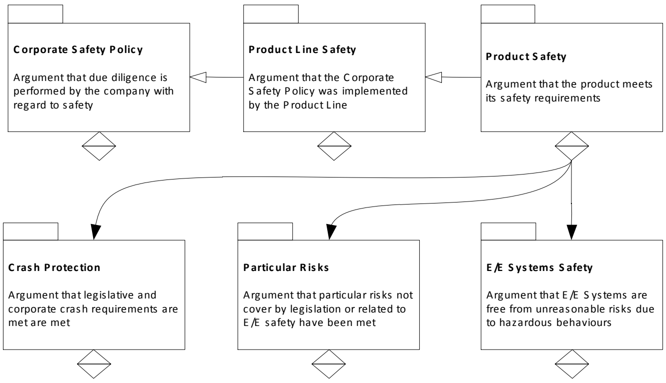
Corporate Safety Policy
Argument that due diligence is performed by the company with regard to safety
Product Line Safety
Argument that the Corporate Safety Policy was implemented by the Product Line
Product Safety
Argument that the product meets its safety requirements
Crash Protection
Argument that legislative and corporate crash requirements are met are met
Particular Risks
Argument that particular risks not cover by legislation or related to E/E safety have been met
E/E Systems Safety
Argument that E/E Systems are free from unreasonable risks due to hazardous behaviours

Figure 2 ~ Safety Case Framework for an Automotive Product

The emphasis of the argument '*Product Line Safety'* is on similar variants of the same product. This stems from the fact that economies of scales within the industry are very important and products are often modified and reused in new applications. The intended application of this argument would therefore be to cover vehicle programmes with different vehicle derivatives (e.g. saloons or coupes) or vehicle systems derivatives developed to satisfy different vehicle manufacturer's requirements. This argument itself has a context argument '*Corporate Safety Policy.'*

The '*Corporate Safety Policy*' module contains all the macro level claims for a company's products and those processes that are directly and indirectly related to safety. In the context of ISO 26262 this would cover Part 2 Clause 5 '*Overall Safety Management'* which defines the requirements for key management tasks. The intention of this module would be to capture the argument that would be put forward by senior automotive executives regarding safety within their company and could therefore be used as an indicator of the safety culture within that company.

With reference to secondary arguments which support the top-level argument:

- The '*Crash Protection*' argument is intended to cover the product safety in the context of the 3 phases of a crash {Pre-crash, Crash, Post-crash} as identified by Haddon [14] and is primarily concerned with legislative and, where deemed necessary, corporate crash requirements. As previously stated as an absolute minimum a vehicle manufacturer and supplier must meet specific market legislative requirements but in order to highlight a particular product attribute or meet multiple market legislative requirements they may develop more rigorous internal standards.
- The '*Particular Risk*' argument is intended to cover product related safety issues that are not specifically covered by crash legislation or E/E safety. In practice this typically means non-functional safety issues. For example, the management of toxic substances or more recently the management of hazardous voltage in hybrid vehicles.
- The '*E/E' Systems Safety*' argument is intended to cover product related functional safety issues related to the safety risks associated with E/E systems which is the intended scope of ISO 26262.

3.3 E/E System Safety Product and Process Safety Arguments

Habli and Kelly in [15], [16] and [17] discuss the importance of both product and process arguments within a safety case. As stated in the introduction, product-based arguments address safety assurance by arguing over the acceptable safe behaviours of the product. These claims are typically substantiated by direct evidence generated from product testing, analysis, simulation and in-service 'proven in use' history. However, confidence in this evidence may be undermined by uncertainties about the provenance of this product evidence. The trustworthiness of the product evidence therefore relies, in part, on the quality of the engineering process.

3.3.1 E/E Product Safety Arguments

Figure 3 shows a possible product argument structure for expanding the E/E Systems Safety argument from Figure 2. To be valid, an argument using this structure needs to be supported by evidence. Evidence in compliance with ISO 26262 comes in the form of the aforementioned work products and there are over 100 work products that are required to be produced. The key work products that are believed to be directly related to the safety of the product are shown in Figure 3. It should be noted that the work products listed in Figure 3 cover concept and product development phases and have been taken from Parts 3, 4, 5 and 6 of ISO 26262.

3.3.2 E/E Process Safety Arguments

As stated in the introduction to this section, for the product argument to be credible it is not enough that it be supported by evidence, the evidence itself must be trustworthy, and this is the role of the process argument. Figure 4 shows a possible argument structure for connecting the process arguments within ISO 26262 to the product arguments.

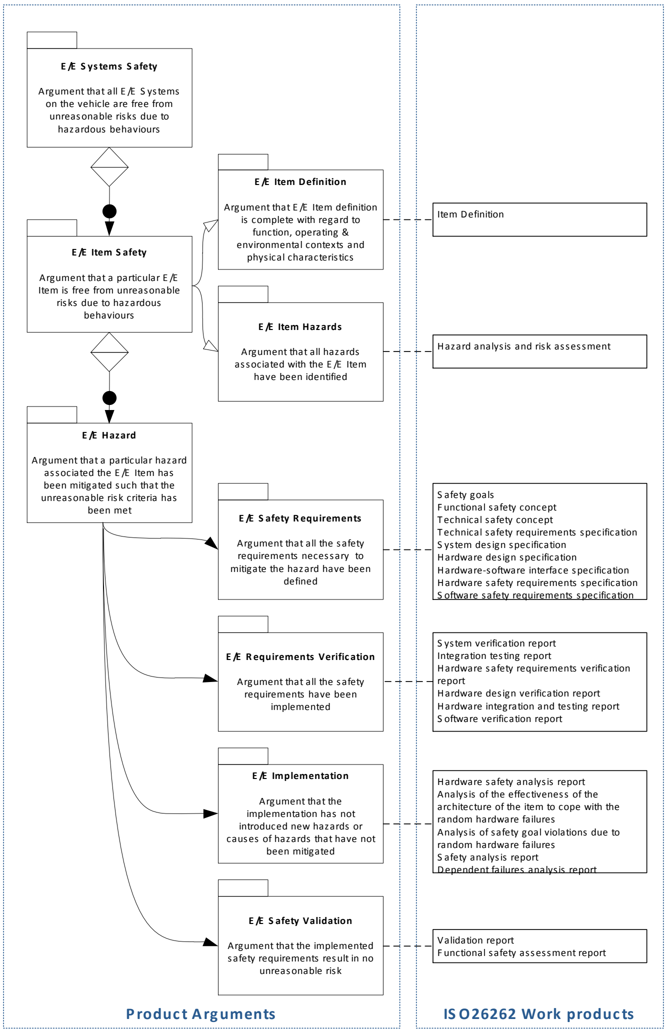
E/E Systems Safety
Argument that all E/E Systems on the vehicle are free from unreasonable risks due to hazardous behaviours
E/E Item Safety
Argument that a particular E/E Item is free from unreasonable risks due to hazardous behaviours
E/E Hazard
Argument that a particular hazard associated the E/E Item has been mitigated such that the unreasonable risk criteria has been met
E/E Item Definition
Argument that E/E Item definition is complete with regard to function, operating & environmental contexts and physical characteristics
E/E Item Hazards
Argument that all hazards associated with the E/E Item have been identified
E/E Safety Requirements
Argument that all the safety requirements necessary to mitigate the hazard have been defined
E/E Requirements Verification
Argument that all the safety requirements have been implemented
E/E Implementation
Argument that the implementation has not introduced new hazards or causes of hazards that have not been mitigated
E/E Safety Validation
Argument that the implemented safety requirements result in no unreasonable risk
Item Definition
Hazard analysis and risk assessment
Safety goals
Functional safety concept
Technical safety concept
Technical safety requirements specification
System design specification
Hardware design specification
Hardware-software interface specification
Hardware safety requirements specification
Software safety requirements specification
System verification report
Integration testing report
Hardware safety requirements verification report
Hardware design verification report
Hardware integration and testing report
Software verification report
Hardware safety analysis report
Analysis of the effectiveness of the architecture of the item to cope with the random hardware failures
Analysis of safety goal violations due to random hardware failures
Safety analysis report
Dependent failures analysis report
Validation report
Functional safety assessment report
Product Arguments
ISO26262 Work products

Figure 3 ~ E/E System Product Based Argument

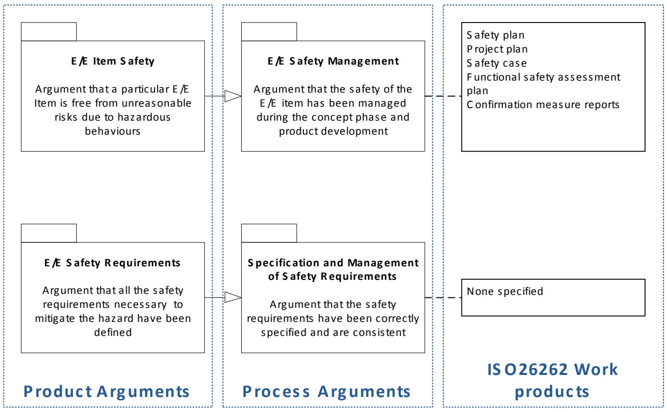
E/E Item Safety
Argument that a particular E/E Item is free from unreasonable risks due to hazardous behaviours
E/E Safety Requirements
Argument that all the safety requirements necessary to mitigate the hazard have been defined
E/E Safety Management
Argument that the safety of the E/E item has been managed during the concept phase and product development
Specification and Management of Safety Requirements
Argument that the safety requirements have been correctly specified and are consistent
Safety plan
Project plan
Safety case
Functional safety assessment plan
Confirmation measure reports
None specified
Product Arguments
Process Arguments
ISO26262 Work products

Figure 4 ~ E/E System Product Based Argument

With reference to Figure 4 it can be seen that the argument '*E/E Item Safety'* is made with the context process argument '*E/E Safety Management.*' The scope of the argument '*E/E Safety Management*' is intended to cover Part 2 Clause 6 of ISO 26262 and therefore has the specified work products: safety plan, project plan, safety case and confirmation measure reports. Although safety plans, project plans and confirmation measure reports are important in the development of the product they are not directly related to the safety of the product and are therefore considered to be process related. In this way the ISO 26262 standard can be used to support a product argument.

3.3.3 The Product and Process Challenge

Given that there are over 100 work products required by ISO 26262 to infer from this large quantity of diverse material that a top-level claim such as '*the E/E Item is free from unreasonable risks due to hazardous behaviours*' [18] is a challenging task. This is true even for the 24 work products directly related to the product that are shown in Figure 3.

The construction of both product and process arguments allows the information to be structured and organised into more manageable modules. However it is the explicit representation of the product argument that helps guide the reader into understanding what all the material implies, or otherwise, the intended conclusion. This is an important point since as previously stated it is a *product* that is bought and operated by consumers. This proposed approach would therefore seem to be much more in the spirit of the standard's definition of a 'safety case[4]' than merely compiling a list of work products as per the requirement 6.4.6.2 within Part 2. The good news is that due to the way ISO 26262 is structured, identification of the product and process argument is not as onerous as it might first appear.

4 Conclusions

Experience and theory developed over the last 50 years regarding safety cases can be usefully applied to automotive products. Although the concept of a safety case was considered in earlier automotive safety guidelines, the international standard ISO 26262 has significantly increased interest within the automotive safety industry in how safety arguments and evidence should be generated, documented, reviewed and maintained for automotive systems. Currently, there is not a consensus on the real value of an automotive safety case, particularly when a safety process is compliant with ISO 26262. On the one hand, some are treating the safety case as a repository of the work products generated from the safety lifecycle phases. On the other hand, others are emphasising the role of the argument in showing how and why the work products (i.e. evidence) support the overarching claim that residual risks are acceptable.

Due to a perceived effort overhead, many will initially regard the development of a safety case as a documentation exercise

[4] ISO 26262 defines a safety case to be '*argument that the safety requirements for an item are complete and satisfied by evidence complied from work products of the safety activities during development'.*

needed merely for compliance. However, clear and practical industry guidance, supported by example safety arguments and evidence, should help in paving the way for a smooth introduction of the safety case concept in a way that ensures a consistent understanding of this concept. To this end, the Motor Industry Software Reliability Association (MISRA) in the UK has launched an initiative to create a guidance document on automotive safety cases. The guidance aims to provide supporting information on the structure and contents of the argument as well as worked examples of arguments and sample means for generating evidence.

Acknowledgements

The authors would like to thank their respective organisations for giving them the time to collaborate in the writing of this paper. They would also like to thank the MISRA Safety Case working group especially Fredrik Torner (Volvo Car Corporation) and David Higham (Delphi) for their contribution.

References

[1] L.Arnold, Windscale 1957. 'Anatomy of a Nuclear Accident' London, Macmillan, 1992.

[2] UN-ECE Website Accessed 1st July 2011. http://live.unece.org/trans/main/welcwp29.html

[3] Federal Motor Vehicle Safety Standards and Regulations Website Accessed 1st July 2011. http://www.nhtsa.gov/cars/rules/import/fmvss/index.html

[4] Vehicle Certification Agency Website Accessed 21st July 2011. http://www.vca.gov.uk/vca/index.asp

[5] International Electrotechnical Commission (IEC), 'IEC 61508: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems', 2010-04-30, 2010.

[6] MISRA. 'Guidelines for Safety Analysis of Vehicle Based Programmable Systems' November 2007

[7] F.Torner, P .Ohman. 'Paper G ~ A Framework for Automotive Safety Cases' Chalmers University of Technology, Goteborg. December 2008.

[8] S.Wagner et al. 'A Case Study on Safety Cases in the Automotive Domain: Modules, patterns and Models' ISSRE'10', p 269-278, 2010.

[9] I.Habli et al. 'Model-Based Assurance for Justifying Automotive Functional Safety' Proceedings of the 2010 SAE World Congress, Detroit, Michigan, USA, April 2010.

[10] R.Palin, I.Habli. 'Assurance of Automotive Safety: A Safety Case Approach' Proceedings of the 29th International Conference on Computer Safety, Reliability and Security (SAFECOMP), Vienna, Austria, September 2010.

[11] T.Kelly. 'Arguing Safety – A Systematic Approach to Safety Case Management DPhil Thesis' Department of Computer Science, University of York, UK. 1998.

[12] T.Kelly. 'A Systematic Approach to Safety Case Management' Proceedings of SAE 2004 World Congress, Detroit, March 2004.

[13] I.Bate, T.Kelly 'Architecture Consideration in the Certification of Modular Systems' Reliability Engineering and System Safety, vol. 81, Issue 3, pp 303--324, Elsevier 2003.

[14] W.Haddon Jr 'The changing approach to the epidemiology, prevention, and amelioration of trauma: the transition to approaches etiologically rather than descriptively based.' Am J Public Health 58: 1431-1438, 1968.

[15] I.Habli, T.Kelly. 'Achieving Integrated Process and Product Safety Arguments' Proceedings of the 15th Safety Critical Systems Symposium (SSS'07), Bristol, United Kingdom, February 2007.

[16] I.Habli, T.Kelly. 'Process and Product Certification Arguments - Getting the Balance Right' Achieving Integrated Process and Product Safety Arguments' in the Proceedings of 12th IEEE Real-Time and Embedded Technology and Applications Symposium, San Jose, California, USA, April 2006.

[17] I.Habli, T.Kelly. 'A Model-Driven Approach to Assuring Process Reliability', in the proceedings of the 19th IEEE International Symposium on Software Reliability Engineering (ISSRE), Seattle, USA, November 2008.

[18] ISO. 'ISO 26262: Road vehicles -- Functional safety' International Standard ISO/FDIS 26262, 2011.

[19] M. Holloway. 'Safety Case Notations: Alternatives for the Non-Graphically Inclined? IET 3rd System Safety International Conference 2008.

[20] P.G.Bishop, R.E. Bloomfield 'The SHIP Safety Case Approach' SafeComp95, Belgirate, Italy 11-13 pp 437-451, published by Springer October 1995.