How to Implement Efficient Safety Management in Product Development

by Wolfgang Reinelt and Michel Bonnet

Executive summary

A critical aspect of product development is to demonstrate that a given product, solution or service is adequately safe before it gets released. How product safety considerations are managed greatly affects project efficiency, scheduling, and cost. This paper proposes a logical management approach for product development safety. Methods for organizing safety-related evidence and arguments are discussed. An example is provided for how to present a safety case utilizing Goal Structure Notation (GSN).

998-2095-06-16-15AR0

Schneider Electric

Introduction

How do manufacturers within the train, automobile, airplane industries demonstrate that a given product, part, solution or service is adequately safe? A safety “case” needs to be built around evidence so that regulators and / or certifiers are convinced of the validity of any safety claims. Also this evidence needs to stand up not only on paper, but needs to be applicable to real-life situations.

Certification is an important milestone to achieve for any manufacturer that hopes to eventually release a product to the marketplace. Failure on the part of either manufacturers or certifiers to ensure product safety can result in loss of life and loss of revenues (through legal actions and through loss of customer confidence).

In the realm of safety management, evaluation through independent assessment is one of the central requirements of sound functional safety practice. In order to assist in preparing stakeholders for proper safety management, this paper describes a methodology called Goal Structure Notation (GSN) and also looks to articulate safety guidelines as highlighted within IEC 61508 specifications.

When applying IEC 61508 standards, manufacturers need to show that risk has been assessed, that safety requirements have been defined and met, and that safety management activities have planned and executed. These tasks will need to have been performed by people with the proper competence and experience. Evidence needs to be presented to the independent assessor during the course of a product’s development in order to assure the assessor that the product or system being developed will be acceptably safe. At the end of the project, when any and all points raised by the assessor have been addressed, a report is issued by the assessor to present the results of the independent assessment.

The building of this “safety case” is progressive as the product development moves through different project phases, by providing proof at each stage that safety risks are reduced to an acceptable level. The safety case gathers momentum by presenting evidence of the qualitative and quantitative aspects of the functional safety. This approach focuses not only on the technology aspects of the product in question, but also on processes, methods and compliance practices surrounding the offering (see **Figure 1**).

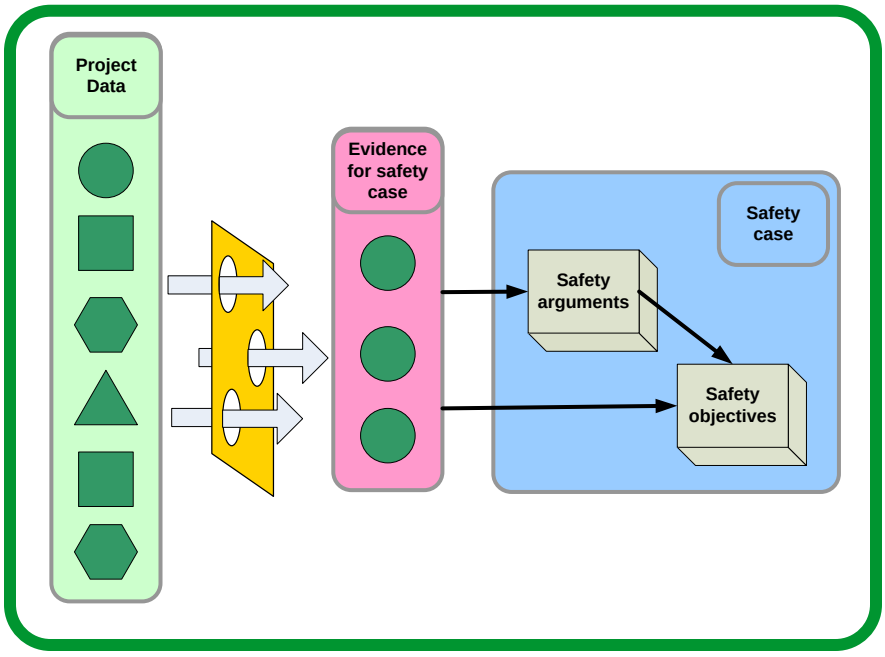

Figure 1
The body of evidence for a safety case is issued from project data.

The execution of a safety case methodology presents multiple advantages:

- Argumentation and documentation is organized and structured; information can be accessed quickly and easily by the stakeholder. Such a structure also facilitates review and challenge from others
- The process encourages arguments and clarifies assumptions
- Focus is broadened beyond just the technology by introducing an analysis of process, methods and compliance.
- Formalizes the company approval and/or independent assessment processes
- Serves as a basis for any change management.

Safety case vs. certification

Within the domain of products, **certification** is the process of attestation whereby specified requirements are met by a product.[1] Certification is performed by third party individuals or bodies who are neither supplying nor consuming the product. A certificate is the deliverable (or outcome) of this process. Certification is often performed in three stages:

1. A review report containing safety evidence compiled is issued by the product's provider and is submitted to the certifier.
2. A technical report detailing requirements fulfilled by the product which addresses the questions of how and why these requirements are fulfilled is also submitted.
3. The issuance of a certificate that is made available to potential customers / consumers of the product. A certificate often consists of a single page stating listing the requirements that have been met as per international standards.

Table 1
Elements presented in a typical safety case document

Elements of a safety case	
Executive summary	Emergency and contingency arrangements
System definition and description summary	Operational information**
Assumptions	Independent safety assessment report
Progress against designated safety program	Conclusions and recommendations
Conformance to safety requirements*	References

* Consists of safety requirements, targets and objectives; summary of argument and evidence showing how requirements have been / will be met; any requirements that are unlikely to be met, with remedial actions; outstanding risk management actions; residual risk; regulatory approval and associated restrictions; feedback arrangements for defects and shortfalls; interface issues with other systems

** Operational envelope; limitations on operational capability; main areas of risk

Functional safety assessments are different from certifications in that they place much more emphasis on safety integrity levels and consequences. Like a certification, they also seek out a different person, department or organization perform the assessment. However, this "different organization" is not necessarily a third party in the same sense as certification, since the functional safety assessment only decrees that the evaluator be "separate and distinct, by management and other resources" (IEC 61508-4, 3.8.13). For example, in the

[1] As defined by the IEC within the International Electrotechnical Vocabulary (IEV) at http://www.electropedia.org/

case of a functional safety assessment, a customer may be assessing a supplier. Although the assessment activity might be the same, it does not qualify as a certification.

A **safety case** (see **Table 1**) is more of 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 environment. A safety case report is a deliverable that summarizes a safety case at a particular instant in time. The safety case report highlights areas of safety-related project risk requiring management attention and provides stakeholders with safety case visibility and status.

Safety cases are most often produced by contractors or by the provider of the product and they often use the wording of certification. However, since they are not interpreted by a true third party, they cannot be a certification, but they can facilitate certification by providing the argument needed to attain certification. A safety case can serve as the basis for company approval and/or independent assessment. Note that an independent (functional) safety assessment report, as defined above, is a subset of the safety case report (see **Figure 2**)

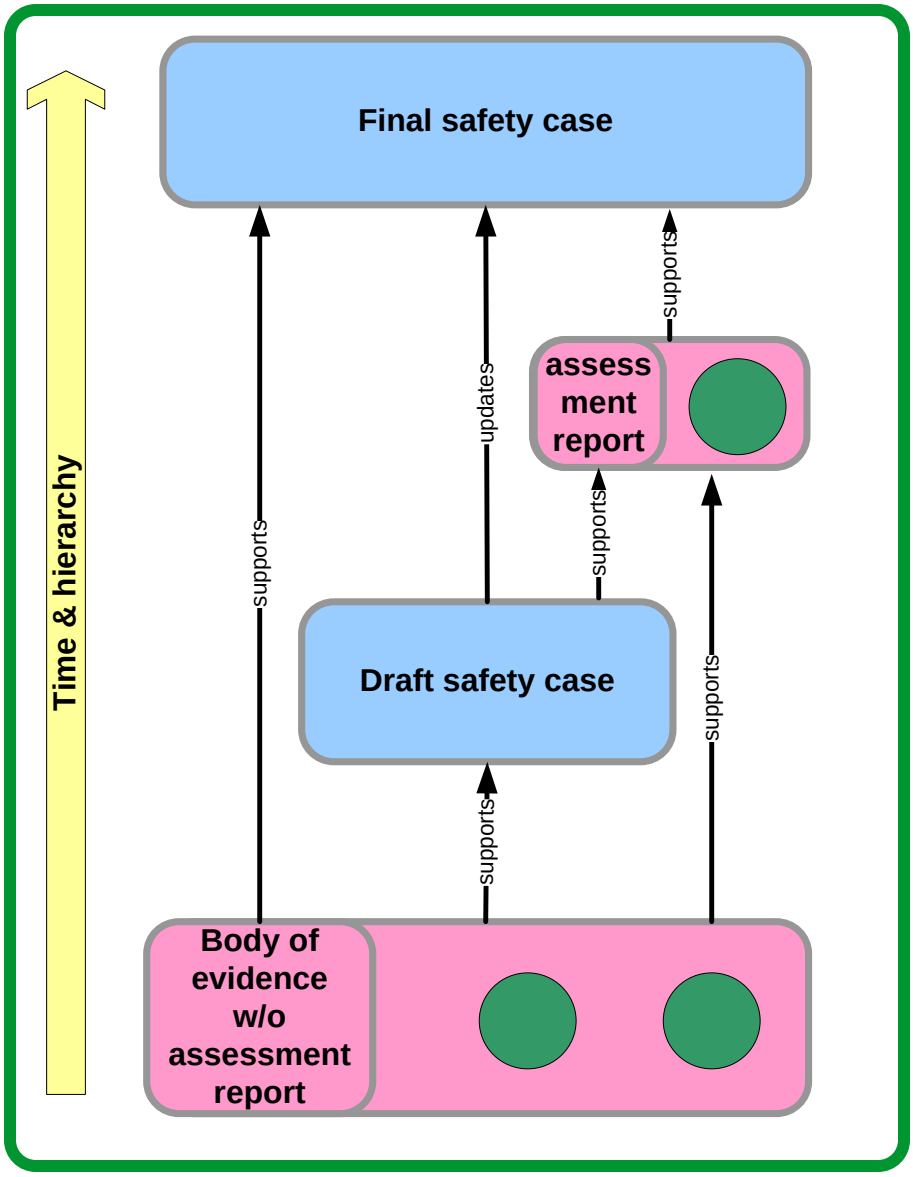

Figure 2
Integration stages of safety case and assessment report outputs

Building the safety case

The work involved in piecing together a safety case consists of selecting and collecting the proper safety evidences that will prove that all safety requirements have been fulfilled. Those safety requirements can be classified into the following two categories:

- **Technical requirements** - Even if the IEC 61508 standard requires forward and backward traceability, the safety evidences will be provided by the project development lifecycle deliverables including specifications, design and test results.
- **Process requirements** - The IEC 61508 standard provides several tables that can be used to select the appropriate measures for the targeted safety integrity level. Once selected the set of techniques and methods must be executed during the project lifecycle phases. The quality assurance of the project and the project deliverables will then help to show that all planned measures have been successfully applied.

Depending on the project size, complexity or novelty, the safety evidences may be collected from different contributors, and may vary in format and quantity. As a result, safety arguments and assumptions are discussed between the different contributors and the functional safety assessment team or the certification team (if a manufacturer or supplier is at the stage of seeking required certification from a third party).

A good safety case report is organized and structured in the way it presents assumptions, arguments, and evidence. A good report clearly answers the question “why is your product adequately safe?” By involving stakeholders such as product designers in the safety case process, the designers are forced, by default, to learn how and why their product is acceptably safe (or unsafe). This will encourage them to take more care about safety in their current and future designs. Management will also gain a clear understanding of the risks and responsibilities involved in bringing a product to market.

“A good report clearly answers the question ‘why is your product adequately safe?’.”

The more structured the documentation and argumentation, the easier it is to manage changes (such as safety standards evolution, design changes, or product operations updates) and perform rapid safety impact analysis.

In practice, the different phases of safety analysis are often executed by different teams. Each team works out how to improve safety within its own domain and complies with targeted safety levels. The safety case document serves as a catalyst that connects all the parts and argues how each practice or activity contributes to compliance of safety objectives. Safety case generation can act as a tool to manage complexity. Disparate tasks such as requirements engineering, development of software and hardware, and testing, for instance, can be harmonized from a safety perspective. The safety case aids in connecting all parts and to focus all of them to the same degree. During the documentation exercise, weaknesses become visible and can be addressed for the current project and can be compensated for ahead of time for future projects.

The ultimate goal, however, is to produce a complete safety case that is summarized by a safety case report. The information in the report is supported by safety evidences that meet regulatory requirements and demonstrate that a product is acceptably safe and ready to release to the market.

Risk abatement

Those who pursue a safety case approach should guard against a couple of factors. First, not all safety case report templates are standardized. Some departments within organizations may have built their own template which may include inconsistent specifications. Second, safety case report templates can sometimes mask a culture of "paper safety" which comes at the expense of "real safety".

Incremental safety case

Another important aspect to consider when building a safety case is the timing. Historically safety case development was left until the end of the product development cycle. As a result, opportunities to detect safety issues early on were lost and, in certain cases, this has lead to costly redesign to meet safety objectives.

To mitigate such project risks, a safety project management plan, that includes early stage conceptualization and a test verification and validation strategy should be built early on in the product development lifecycle. This enables the execution of a preliminary assessment in order to gain confidence that the product is on its way to meeting safety objectives. The most evolved organizations look to implement a full safety case lifecycle which is inclusive of incremental safety case audits that are conducted throughout several stages of the product development project (see **Figure 3**).

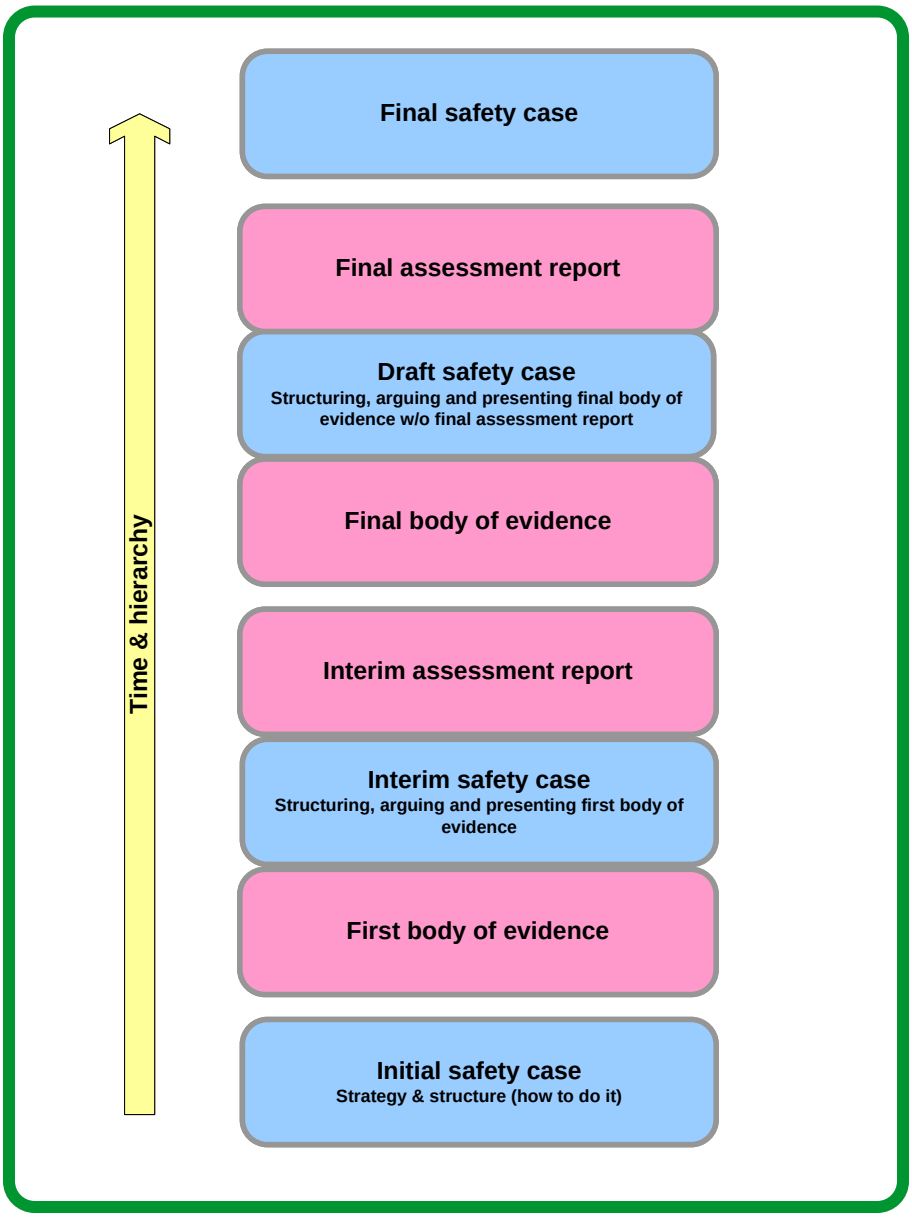

Figure 3
Example of a safety case that is developed throughout the entire project life-cycle

Goal Structure Notation

To this point, this paper has reviewed the concept of the safety case and presented its advantages and limitations. The safety case report has been described as a document summarizing the events that have taken place in order to assure product safety. Since the safety case is defined as a "structured argument", the next logical step is to further formalize both: "structure" and "argument" parts of the process. A method called Goal Structure Notation (GSN) has been created to support this effort. GSN is defined as follows:

"Graphical argumentation notation can be used to document explicitly the individual elements of any argument (claims, evidence and contextual information) and, perhaps more significantly, the relationships that exist between these elements (i.e. how claims are supported by other claims, and ultimately by evidence, and the context that is defined for the argument). Arguments documented using GSN can help provide assurance of critical properties of systems, services and organizations (such as safety or security properties)."[2]

Figure 4 illustrates an example of how Goal Structure Notation portrays the elements of an argument.

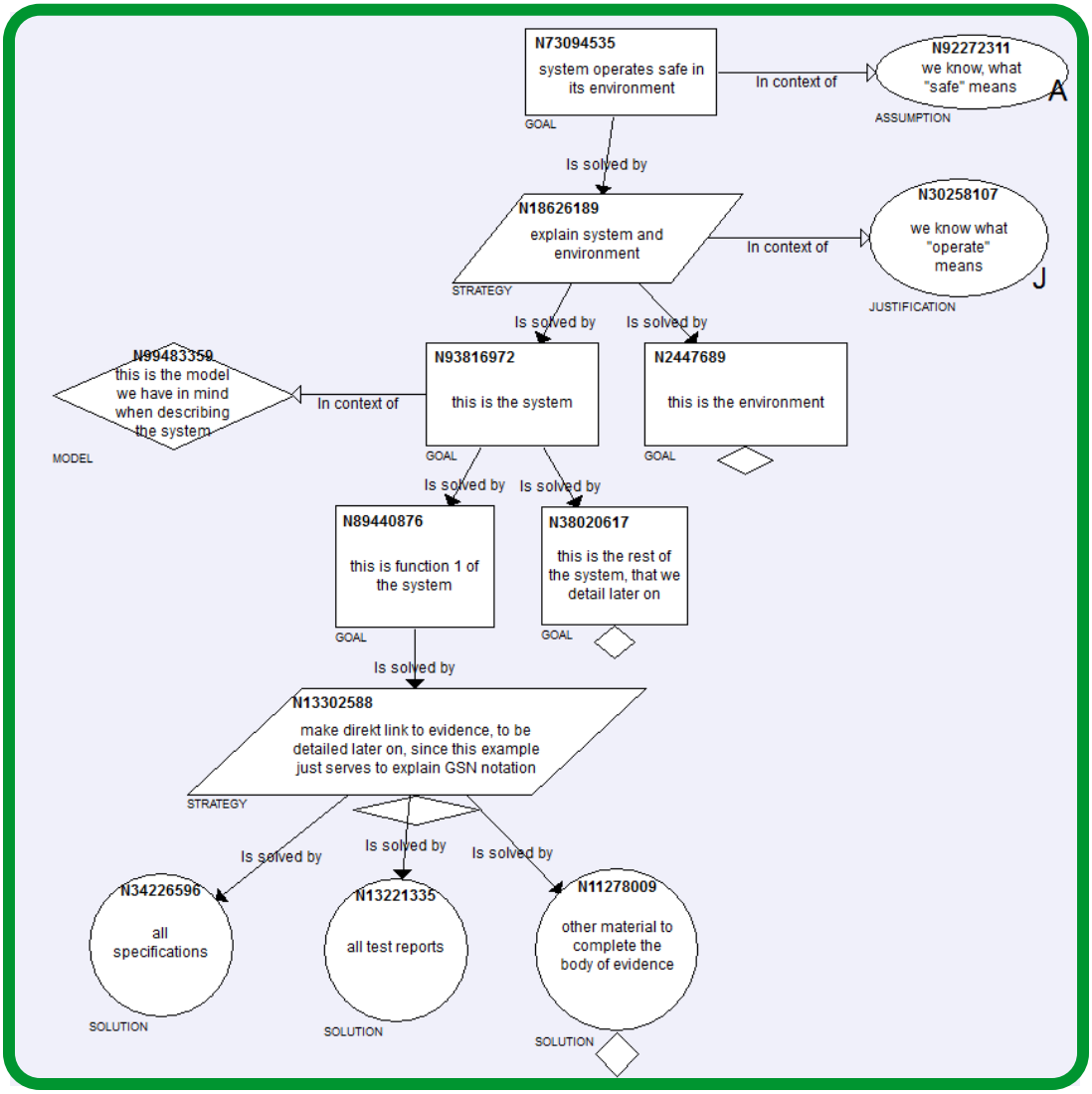

Figure 4
Example of a Goal Structure Notation

[2]Goal Structure Notation Working Group: GSN community standard version 1 (2011)

In **Figure 4**, the information flows from top to bottom. A new argument is linked to previous arguments that have already been solved. This makes it easier to understand the reasoning. Information is carefully divided into goals and sub-goals, assumptions, justifications and references to models under consideration.

Conclusion

Safety case reports provide an important catalyst for growing a "safety first" culture among organizations that manufacture parts, products and systems to important industries such as avionics, aerospace, rail and automobile. In addition to documenting arguments for the safety of any given product, safety case reports also generate the following benefits:

- **Provides an overview of modifications** – Once a product hits the market, modifications to the product, such as new features, will be added. The record provided by the initial safety case report can act as a reference that helps to catalog these new changes and modifications from a safety perspective.

- **Explains project specifics and deviations to initial safety plan** - During the course of a project, the project team might deviate from the original planning with approval of the steering committee. For example, team members could change, methods could be re-enforced to increase the level of quality, and customer requirements could change. Therefore, planning must be updated, including those aspects of planning that affect the safety plan. As such, the safety plan acts as a record of changes that have taken place.

- **Clarifies dependence on other safety cases** – A well documented safety case can serve as a springboard for launching other safety cases by leveraging a line of argumentation that has been successful in garnering approvals and release of products.

For further information, refer to conference paper "Safety Case and Certification" by Wolfgang Reinelt & Michel. Bonnet (Safe.tech 2015, Munich, Germany).

About the authors

Wolfgang Reinelt Is a Group Senior Export for Functional Safety at Schneider Electric and responsible for Functional Safety Management within the Machine Solutions department (Industry Business). He holds a Master's degree in mathematics and a PhD in Electrical Engineering both from Paderborn University, Germany. He published numerous peer reviewed conference papers and journal articles and holds patents within the area of control engineering, fault detection and safety. Prior to joining Schneider Electric in 2007, he worked in automotive industry on similar topics.

Michel Bonnet is responsible for functional safety management within Schneider Electric's energy automation department (Energy Division). Since 2008 he has driven quality assurance and functional safety management development projects in the domain of protection relays. He is an experienced application engineer and has worked on safety and substation Automation Digital Control System projects. He holds an engineering degree from ESIGELEC, in Rouen, France.