A Business Model for selling components with safety certificates

Carl Bergenhem[1], Daniel Skarin, Fabian Wenger, Qamcom Research & Technology, Gothenburg, Sweden.

1 Abstract

This paper [2]outlines a business model for selling safety-related components. The goal is protection of the suppliers' intellectual property whilst providing confidence, to the customer, that the component is safe. The ideas in this paper are based on the Safety Element out of Context – concept as given in ISO 26262. To this we add ideas from IEC 61508 – (a safety manual), and also describe a procedure to establish a safety certificate resulting from a third-party assessment. The ideal business model is contrasted with a fictitious inferior model that is based on experience in the industry.

2 Introduction

This paper outlines a business model for selling safety-related components. The goal is protection of the suppliers' intellectual property whilst providing confidence to the customer that the component is safe. The actors, e.g. supplier, customer etc., and their roles in the business model are described and explained. The business model is described in an ideal scenario. Commentary is given where ideal assumptions differ from reality e.g. as found from experience. As this is an ideal model, it may require effort (and expense) to use in a real scenario. However, it allows deficiencies in current practices to be highlighted and at least discussed. The business model assumes the use of a safety manual, in the interface to the customer; in the scope of components that are developed according to ISO 26262. Although this concept is not new (it is found in IEC 61508), it is not currently specified in ISO 26262. The ideal business model is contrasted with a fictitious inferior model that is based on experience in the industry.

The background is the following: A supplier develops and offers a safety component. The offer is found by a potential customer through marketing, and negotiations leading to a purchase are initiated. The material used for marketing the component is based on properties from the development of the component. The customer requests a specification of the component (beyond initial marketing material), e.g. it's interface, properties, and evidence of conformance, e.g. to applicable safety standards. Since much of this data (specification sand evidence of conformance) is found in supplier documentation that also contains other information that the supplier should not expose, a challenge in this relationship is to control the exposure of the supplier's intellectual property to the customer. In the proposed business model this exposure is avoided by using a clear interface definition (a safety manual) and third-party certification, of product conformance and safety, to gain the customer's confidence without compromising the supplier intellectual property.

Traditionally, system safety analysis started with the complete systems in scope, i.e. not components. Functional safety standards (a subset of system safety) originated from this complete systems approach. For example, in aerospace, process and nuclear industry there is a long-standing tradition to estimate system reliability, to analyse faults and to mitigate failures by system engineering. In the wake of several catastrophic incidents like the Seveso disaster in 1976 and the Bhopal disaster in 1984 (Seveso disaster, Bhopal disaster), the need for an industrial standard to assess functional safety became priority.

In 1998 the IEC 61508, the first international functional safety standard, was published and helped raise awareness of functional safety in the industry. Its lifecycle approach to functional safety (design, installation, operation and maintenance, human factors) has been the basis to standardization efforts in other fields, see (Foord 2011). The second edition of IEC 61508 was released in 2010. To allow for a component-

[1] Corresponding author: carl.bergenhem@qamcom.se

[2] This article is available at arxiv.org

oriented approach, e.g. ISO 26262 proposes the concept of SEooC - Safety Element out of Scope. A similar concept is available for IEC 61505:2010: Pre-existing software element - (e.g. Route 1S: “development compliant to 61508”). See Part 3 - 7.4.2.12. The concepts in this paper, the business model and thoughts on the safety certificate, were also presented in (Johansson 2014).

3 Problem definition and Proposal

3.1 Old and inferior business model

An automotive supplier would like to develop and sell a component. Since the requirements and context for the component is not actually known before a customer is known and involved, the development life cycle can, strictly speaking, not be initiated. When a customer appears, discussions can start and requirements for the component can be given; and development starts. When development is complete, the component is associated with all work products as mandated by ISO 26262, including a safety case for the component. The development process and component are subjected to audit (fulfilment of process) and assessment (defensible technical claim that the component is safety). Most of these work products contain sensitive Intellectual Property (IP) of the component; which arguably should not be shown or passed to a customer. IP could include details about the design of the component. A typical unsatisfactory business model could be as is illustrated as Figure 1.

Figure 1: Inferior business model

The roles in the figure are:

- The **Supplier** develops the component and assigns a safety specialist (the "Good guy") to be part of the product development team. The supplier also assigns an independent third party (the "Bad guy") to performs audit and assessment.
- The “**Good guy”** (GG) is assigned by the supplier to perform development work of the component; such as functional Safety management or safety engineering. The Good guy can also do pre-assessment, gap analysis and reviews, but will not be independent. Process development and training can also be performed. The Good Guy role could be fulfilled by a safety specialist consulting firm.
- The “**Bad guy”** (BG) is assigned by the supplier (in some cases by the customer) to perform third-party assessment and audit of the component. The bad guy is strictly independent to the supplier and the good guy, e.g. has not taken part in any development activity. This role could be fulfilled by the same type of form as for a GG, but provided that there has been no participation in development work.
- The **Customer**, typically an OEM, accepts the component based on acceptance of work products from the development. These are reviewed at joint meetings between the supplier and customer. In this review, the customer is given access to any requested work products, i.e. potentially secret IP.

With current practice, a customer for the component is found based on a RFI/RFQ procedure. In this, the supplier shows enough technical details and capability so that the customer trusts the technical capabilities and adequacy of the component. Technical details include e.g. safety case, but also other technology centred documents such technical safety concept (TSC[1]), requirement specifications and detailed system designs. The problem here is that of exposing IP to the customer. The customer could argue that refusal to do so could compromise the business deal. The supplier is in a weak position here.

The concept of good guy and bad guy can be illustrated as follows: The goal of the GG is to assist the supplier in developing the component. This includes both identifying gaps and also solving them. Conversely, the goal of the BG is to always offer an independent opinion. This implies that gaps can be identified, but the BG cannot aid in solving them; as this would compromise independence. In ISO 26262, confirmations measures (confirmation review[2], functional safety assessment and functional safety audit) require independence according to the ASIL level of the function. This implies that a GG (and also roles within the supplier development team) may be excluded from performing some of these tasks, as independence is not achieved.

3.2 A New and improved business model

We propose a business model where the supplier interfaces to the customer with a certificate of safety and a safety manual. The certificate is signed and issued by an accredited independent 3rd party (e.g. certification body) that has reviewed details of the component. The certification process is in addition to functional safety assessment and audit, because the subsequent report may expose IP. The safety manual defines the usage, interface, restrictions, and prerequisites of the component, and exposes no IP. Central to the business model is also the use of and trust in accredited parties and safety certificates. In the proposed business model, these are needed to claim independence between key parties. To understand the details of the business model, we first discuss the relationship between the actors, and the generated work products, see Figure 2. The supplier performs a tailored life cycle that is applicable for the SEooC, e.g. only the software phase. The remain life cycle are covered by the assumed context and assumed requirements.

- The **Safety Assessor** (SA) is an accredited Bad Guy (e.g. independent inspection body). This implies that the party is accredited according to e.g. ISO/IEC 17020 to perform independent assessment according to a specific standard. ISO/IEC 17020 gives "General criteria for the operation of various types of bodies performing inspection"; basically an extension to an existing quality management system. Accreditation implies that a certification or inspection body (in this case the safety assessor) has been assessed to demonstrate their competence, impartiality, and capability. In this setting, inspection (assessment) is done according to ISO 26262, e.g. this is what the SA is accredited for. The SA performs the assessment of the component being developed and issues a functional safety assessment (FSA) Report (an ISO 26262 work product). This role could be fulfilled by an accredited company.
- An **accredited FSA report** implies that the technical merits of the component to fulfil safety has been assessed. In the case of an SEooC, it is assessed based on the assumed usage and context. "Accredited" implies that the party performing the assessment has a quality management system that ensures correct procedure and handling of the assessment assignment, e.g. maintain quality of the assessment service. Note that the report still may contain sensitive IP, hence distribution should still be controlled.
- A **Certification Body** (CB) is an organisation accredited by a recognised accreditation body for its competence to perform assessment and issues a **safety certification**. Here the CB[3] is an organisation with the business focused on certification, i.e. technical competence to assess a

[1] This is a system level view of safety requirements allocated to system elements in a system design (technical architecture). It is a mandated view in ISO 26262.
[2] This activity aims to ensure adherence to requirements of the standard (e.g. ISO 26262) in a number of core core products.
[3] Examples of certification bodies are: RISE-SP in Sweden or DNV GL internationally.

particular product is not in the scope of business. The role of the CB is motivated through added independence and trust vis-á-vis the SA – who does have technical competence. The CB can oversee and "accredit" the assessment work of another party, such as the SA. Alternatively, the certificate could also be issued directly by a SA; but with no gain in independence and trust. A notified body is a special case of certification body that is applicable to, e.g. the machinery directive.

- Accredited parties, such as the certification body, are subject to periodic assessment of their competence and conformance to their certification by national **Accreditation Bodies**. It is mandatory for every European member-state to have a single national Accreditation Body. Examples are SWEDAC in Sweden or UKAS in the United Kingdom. Accreditation is a confirmation that a party meets requirements to work with a particular standard; such as ISO 9001 or ISO 26262

The gain for the **supplier** with this setup is stronger independence of the FSA report due to accreditation, and a new artefact, a **safety certificate.** With this artefact, the supplier can now make publicly available a statement (the certificate) that the component has been (successfully) subjected to audit and assessment by an accredited third-party, without exposing any IP before or after a business relation is entered. Hence the certificate can be seen to guarantee the conclusion on the FSA report, i.e. acceptance that the component fulfils functional safety.

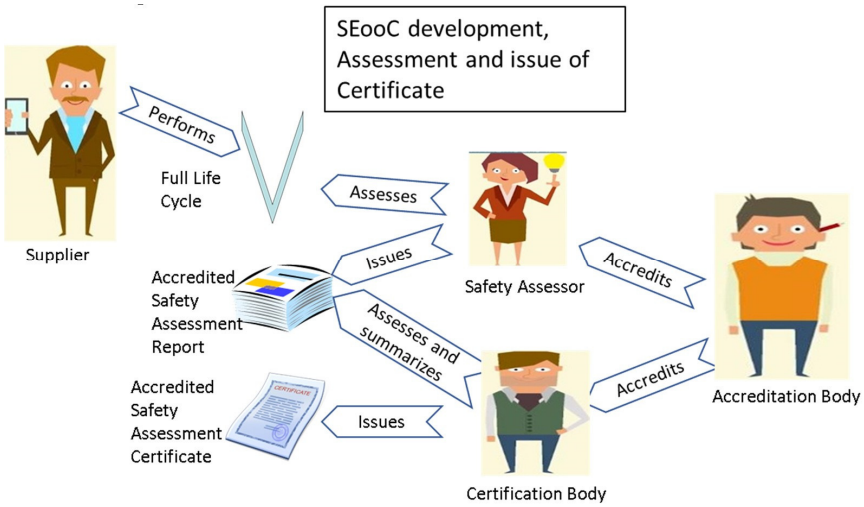

Figure 2: Relations between actors during development (as adapted from Johansson 2014)

For life-cycle based automotive functional safety the first publication of ISO 26262 dates from 2011, (26262). Development of a component according to ISO 26262 can be according to different development categories: new development, modification, or SEooC (Sivencrona, Johansson 2007). The latter, a novel functional safety concept, was introduced to cater for reusable components that are developed without a specific system or vehicle in mind but which are developed with the reuse of the component in different vehicles in mind e.g. an AUTOSAR communication stack or a microcontroller. It is described in 26262, part 10, clause 9. A supplier develops a component (subsystem) as an SEooC, and makes assumptions about the context; what is provided (guarantees) and what is needed (assumes) by the component. This implies that outcomes of the concept phase need to be made such as item definition, hazard analysis and safety goals. When a customer for the component appears, a gap analysis between the true context and the assumed context is made and addressed. This implies that a component can be (almost) ready before a final customer is identified.

In itself such a SEooC component can never be assessed as finally safe unless it is evaluated in its final system context at vehicle level, but the pre-qualification we consider here becomes much more valuable if

business practices are established which allow the assumed context leveraged by the SEooC to be evaluated within the true context of a specific item (in the vehicle).

Hence, the prequalification of the SEooC component can be expressed with:

- a **Safety Certificate** from an accredited third party which has critically assessed the complete safety case (not only the safety manual) without tight binding to a specific item, i.e. final context. The certificate could be made publicly available, e.g. on the supplier home page.
- a **Safety Manual** containing the interface of the component. This can include a **Safety Contract** (Soderberg 2013) with assumptions and guarantees of the component that shall be fulfilled for the component to give correct service when included in an item. The Safety Manual could be made available to the customer first after negotiations with a customer have been started, as it may contain sensitive details. Safety manuals are discussed in a later section.

The development of the component, according to the proposed business model, is illustrated in Figure 3. The key activities before negotiations take place with a customer are: component development, third-party assessment and issue of certificate for the component.

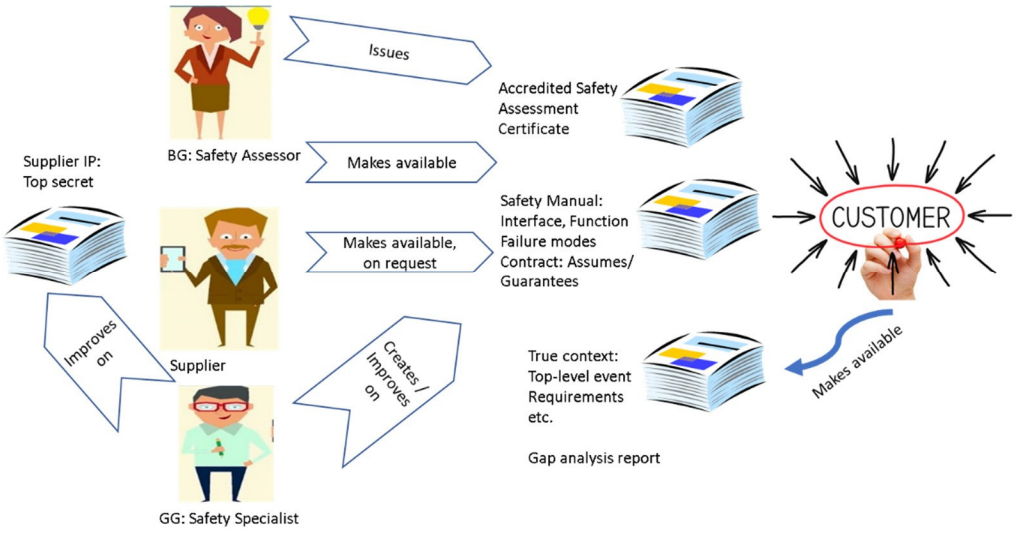

Figure 3: Roles in the improved business model

The roles in the figure of the proposed business model are:

- The Good Guy participates in the development of the component. This includes developing the **safety contract** for the component and **safety manual**.
- The Bad Guy is accredited and performs an independent functional safety assessment of the component and work products including the safety contract and safety manual. The BG issues the corresponding **FSA Report**, that will be part of the supplier´s top secret IP. The BG also issues a **safety certificate** as discussed above.
- The interface to the **Customer** is hence: the safety contract, safety manual and the safety certificate.
- The **true context,** e.g. requirements and context, is now known and a gap analysis can be performed. The supplier addresses and corrects the gaps.

When the component later is included in an item development there is a second step in which the component is assessed in an item-specific safety case which relies on the publicly available safety manual and safety certificate. For a review an assessor can still review any of the internal safety documentation (such as the TSC etc.) but the safety requirements shall be readily evaluated and validated by the means documented in the safety manual.

4 How hard can it be?

What are the obstacles to accepting this model? For example, there may be conflicting goals, e.g. accidents can happen because what is fail-safe at the lower level (e.g. stopping the car) may become unsafe under certain conditions (e.g. another vehicle that rapidly approaching from behind). To gain confidence, the OEM therefore needs to be able to see at review how a function is implemented, i.e. known specific technical details. Also, to check the maturity of safety practices at the supplier and technical capability (e.g. how tasks are scheduled to guarantee latency etc.). Even if probabilities are quoted and tested (e.g. detection or false alarm), the context in which these are tested are important, i.e. what assumptions have been made.

At Joint Review (JR) between the customer and supplier, detailed work products, e.g. the Safety Case, TSC, requirements, are normally available eyes-only. I.e. IP is partially protected. The level of protection, however, becomes less if e.g. the review is conducted via teleconference or the participants in the meeting are not well-known to each other.

Potentially all these obstacles could be addressed by more details in a safety manual and including these issues in the third-party assessment. However, there will always arise questions and issues which could be answered by the OEM simply being allowed to “take a look behind the scene”. In the end, it is a question of trust. It is not certain that an OEM would trust the third party.

The SEooC concept states that assumptions can be made on the context so that development of the (system) component can take place. However, often there is are actual customers in mind, although the problem is only partially known. This leads to an SEooC that is less generic and has assumptions that ties it too closely to a particular customer. Further, since the problem is only partially known, the SEooC-development still needs to make assumptions. There will probably always be changes to the component e.g. for different OEMs. We expect that this implies recertification; which thus adds cost. A general comment on current practices is that it is difficult to know before-hand, when making assumptions on an SEooC, which requirements that will be present in the final context. It is a risk that any assumptions that are made, by a component, will not be possible to meet; either due to sensor limitations or final system architecture. The latter two are not known at the time that the SEooC is designed.

5 The safety manual in related practices

IEC 61508:2010 part 2 – Annex D gives requirements for the safety manual for a compliant component. The purpose of the safety manual is to document all the information, relating to a compliant component, which is required to enable the integration of the component into a safety-related system, or a subsystem or element, in compliance with the requirements of this standard. (Note that the terminology used in IEC 61508 may differ from ISO 26262)

Here we give examples of high-level contents of safety manuals for two types of components: hardware and software. The examples are cited from (Simpson 2010). In section "3.7 Safety Manuals" a manual for specific hardware items is given. Thus, instrumentation, PLCs and field devices will each need to be marketed with a safety manual. Contents can include (hardware):

- a detailed specification of the functions
- the hardware and/or software configuration
- failure modes of the item
- for every failure mode an estimated failure rate
- failure modes that are detected by internal diagnostics
- failure modes of the diagnostics
- the hardware fault tolerance proof test interval (if relevant).

In section "4.6 Safety Manuals" a safety manual for software is given. For specific reusable software elements, such as items of code and software packages, content can include (software):

- A description of the element and its attributes
- Its configurations and all assumptions
- The minimum degree of knowledge expected of the integrator
- Degree of reliance placed on the element
- Installation instructions

- The reason for the release of the element
- Details of whether the pre-existing element has been subject to release to clear outstanding anomalies, or inclusion of additional functionality
- Outstanding anomalies
- Backward compatibility
- Compatibility with other systems
- A pre-existing element may be dependent upon a specially developed operating system
- The build standard should also be specified incorporating compiler identification and version, tools
- Details of the pre-existing element name(s) and description(s) should be given, including the version/issue/modification state
- Change control
- The mechanism by which the integrator can initiate a change request
- Interface constraints
- Details of any specific constraints, in particular user interface requirements shall be identified • A justification of the element safety manual claims

6 Conclusion

We have discussed a business model for providing automotive safety components and focussed on how supplier IP can be protected. This is done while developing the component as an SEooC, a concept from ISO 26262, providing a safety manual, a concept from IEC 61508, and providing the component with safety certificate as issued from a third party. Roles in this setup are discussed and compared with a fictitious example of an inferior business model.

7 Acknowlegements

The research leading to these results has been performed in the SafeCOP project, that received funding from the ECSEL Joint Undertaking under grant agreement 692529, and from Vinnova Swedish national funding in project ESPLANADE.

8 References

(26262) ISO 26262:2018 FDIS, International Standardization Organization. “Road vehicles – Functional safety”. International Standard 2018.

(61508) IEC 61508:2010, Functional safety of electrical/electronic/ programmable electronic safety-related systems – Parts 1–7.

(Bhopal disaster) Bhopal disaster https://en.wikipedia.org/wiki/Bhopal_disaster, accessed 2018-03-12

(Foord 2011) Foord, A. G., Gulland, W. G., & Howard, C. E. (2011). Ten Years of IEC 61508; Has It Made Any Difference?. In IChemE Symp (No. 156, pp. 232-237).

(IBM Software Rational, 2010), IBM Software Rational. (2010). *DO-178B compliance: turn an overhead expense into a competitive advantage.* Aerospace and Defense: White paper.

(Johansson 2014) Rolf Johansson, Jonas Borg, Jeong-Taek Kong, Byung Chul Kim. (2014). Enabling Safe and Innovative Electrical/Electronic(E/E) Systems in the Automotive Domain. VOLUME 15, ISSUE No. 6 AUTO JOURNAL: Journal of the Korean Society of Automotive Engineers, 36(10), 45-51.

(Seveso disaster) Seveso disaster: https://en.wikipedia.org/wiki/Seveso_disaster, accessed 2018-03-12

(Simpson 2010) "Safety Critical Systems Handbook: A Straightforward Guide to Functional Safety, IEC

61508 (2010 Edition) and Related Standards", David J. Smith and Kenneth G.L. Simpson

(Sivencrona, Johansson 2007) http://www.mynewsdesk.com/se/news/the-idea-of-iso26262-for-functionalsafety-10227

(Soderberg 2013) Soderberg, Andreas, and Rolf Johansson. "Safety contract based design of software components." Software Reliability Engineering Workshops (ISSREW), 2013 IEEE International Symposium on. IEEE, 2013.