A GSN Approach to SEooC for an Automotive Hall Sensor

Xabier Larrucea[1], Silvana Mergen[2], Alastair Walker[3]

[1]TECNALIA, Bizkaia, Spain. xabier.larrucea@tecnalia.com
[2] TDK-EPC AG & Co. KG, Stahnsdorf, Germany. silvana.mergen@epcos.com
[3]LORIT CONSULTANCY, Edinburgh, Scotland. alastair.walker@lorit-consultancy.com

Abstract

One of the key challenges for manufacturers of automotive systems, hardware components and software products is not only the process of defining explicit and implicit requirements but also the ability to satisfy safety requirements such as those specified in ISO 26262. From an element point of view, the Safety Element out of Context (SEooC) defined in ISO26262 is becoming a reference for developing systems, elements and components in the automotive sector. Integration teams have limited prior knowledge of how these third party devices have been defined, the assumed requirements used during the validation and verification phases. Goal Structuring Notation (GSN) can be used to define and document the assumed SEooC requirements in a graphical manner. However, development teams are facing several challenges for example how different requirements are implemented in SEooC, or how far GSN is able to represent SEooC definitions. This paper provides a GSN based approach to represent SEooC requirements in a practical example of an automotive hall sensor.

Keywords

Argument, assurance case, claim, Safety Element out of Context

1 Introduction

Hall sensors are used in the automotive sector in a variety of applications[1], including control systems [2], and control of position/velocity[3]. These devices must operate reliably in both wide-ranging and harsh environment conditions[4]. A hall sensor provides a useful industry implementation, integrating hardware and software components[7]. Hall sensors are becoming increasingly more complex elements [6]. In fact, vehicles are becoming increasingly more complex and the demands placed upon elements such as halls sensors equally so. Since 2011 with the emergence of the ISO26262 standard[7] this type of element is typically developed using the SEooC process. Examples of how to implement a SEooC process are documented in part 10 of ISO26262[8]. SEooC development is based upon assumed requirements. One of the key exercises for a team that has to integrate the SEooC element into an item, is to check the validity of the assumptions. This requires not only clearly defined and documented assumptions, but also clearly documented solutions.

Goal Structuring Notation (GSN)[9] allows a clear graphical representation of the assumptions, strategies, justifications and solutions. This notation allows both teams – developers of the SEooC element and the integrators of it - to review, discuss and challenge the assumptions[10]. GSN has been used as a notation for justifying sufficient confidence in software safety arguments[11]. In the automotive sector, requirements engineering is a central discipline[12]. Assumed requirements can be easily listed using a requirements capture tool such as DOORS. However, the process of capturing the justification of these assumed requirements is far more difficult. Ultimately the team integrating the SEooC element must clearly understand the reasoning behind the assumptions made by the development team. This paper reports an industrial case study using GSN as an indicative tool for defining ISO26262 requirements and also the process used in deriving the assumed requirements. The key component of this approach is the intuitive representation of the assumptions. GSN allows the strategies, assumptions and justifications to be clearly represented and understood. The addition of context descriptions provides additional supporting information.

This context implies, at least, the following set of research questions:

- How are the hall sensors requirements (hardware and software) defined in a GSN notation?
- What coverage does GSN provide in the context of ISO26262 SEooC activities?

This paper is structured as follows. First the background description, followed by the method of defining the SEooC hall sensor requirements using GSN. Subsequently the integration process for the SEooC into the item and finally, the conclusion of the process and recommendations.

2 Background

2.1 The SEooC Challenge

In accordance with ISO 26262-10[8] SEooC follows the process illustrated in Figure 1. Two parties are involved in the SEooC implementation, the developers who define the assumed requirements and the integrators who implement the SEooC element in the item.

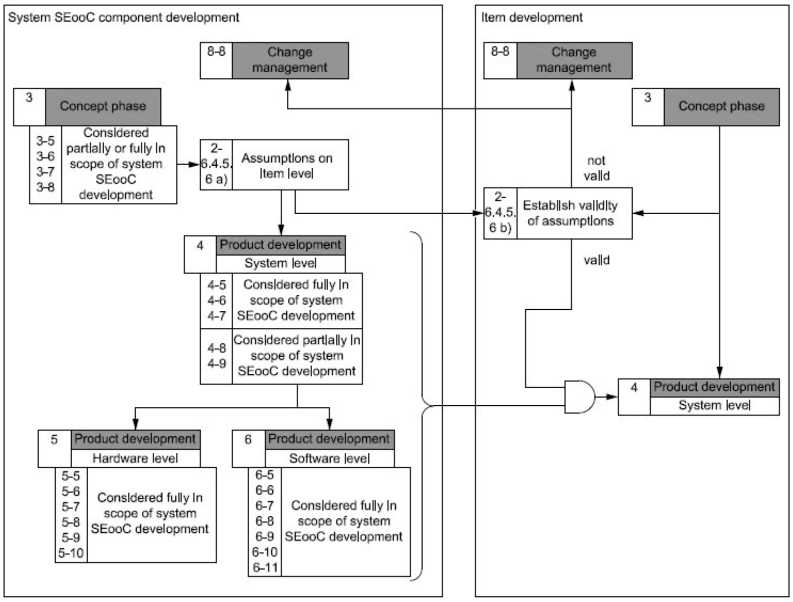
System SEooC component development
8-8
Change management
3
Concept phase
3-5
3-6
3-7
3-8
Considered partially or fully in scope of system SEooC development
2-6.4.5.6 a)
Assumptions on item level
4
Product development
System level
4-5
4-6
4-7
Considered fully in scope of system SEooC development
4-8
4-9
Considered partially in scope of system SEooC development
5
Product development
Hardware level
5-5
5-6
5-7
5-8
5-9
5-10
Considered fully in scope of system SEooC development
6
Product development
Software level
6-5
6-6
6-7
6-8
6-9
6-10
6-11
Considered fully in scope of system SEooC development
Item development
8-8
Change management
3
Concept phase
not valid
2-6.4.5.6 b)
Establish validity of assumptions
valid
4
Product development
System level

Figure 1 Assumed requirement relationship component and item development[8]

The SEooC process then has two distinct phases, the development phase and the integration phase. The development phase consists of two different assumption processes, as indicated in Table 1. As many different products can be developed according to the SEooC process, a system, an array of systems, a subsystem, a software component, a hardware component or a part, then System SEooC element development can be a complex and multifaceted process.

Table 1 SEooC Development and Item Integration Processes

SEooC Phase	Process	Activities
System SEooC component development	Assumptions on the functional safety requirements allocated to the SEooC	Manufacturer defines the safety assumptions on the component
	Assumptions on the context of the SEooC	The manufacturer lists the assumptions that will impact safety when the component is integrated in the item
Item development	Match the functional safety requirements of the item with the functional safety requirements assumed for the SEooC to establish the validity	The integrator validates the assumed requirements see Figure 1
	In the case of an SEooC assumption mismatch, a change management activity beginning with an impact analysis	The integrator initiates a change in either the item or the component based on the nature of the mismatch

2.2 GSN Overview

The object of the GSN exercise is to build up an Assurance Case that clearly indicates the assumed requirements of the SEooC element. The definition of the Assurance Case is:
A reasoned and compelling argument, supported by a body of evidence that a system, service or organisation will operate as intended for a defined application in a defined environment [13].
In order that Assurance Cases can be developed, discussed, challenged, presented and reviewed amongst the stakeholders and maintained throughout the product lifecycle, it is necessary for them to

be documented concisely. The documented argument of the Assurance Case should be structured to be comprehensible to all safety-case stakeholders. It should also be clear how the evidence is being asserted to support this argument. By appealing to core concepts of argumentation, GSN helps address these objectives.
The principle elements of GSN are as follows; however for further information refer to [9]

- Goals – the claims of an argument
- Solutions – items of evidence
- Strategies - document how claims are said to be supported by sub-claims
- Contexts – document goal or strategy context in which the claim or reasoning step should be interpreted
- Assumptions - some claims and argument strategies rely on assumptions to hold valid
- Justifications – provide a claim or argument strategy, with some explanation as to why it is acceptable

GSN provides two types of linkage between elements:

- SupportedBy relationships – represented by lines with solid arrowheads – indicate inferential or evidential relationships between elements.
- InContextOf relationships – represented as lines with hollow arrowheads – declare contextual relationships.

There are two distinct approaches to devising a goal structure top-down or bottom-up. As bottom-up tends to lend itself to construction of a goal structure when evidence already exists, it is not the subject of this paper. The 6 steps for a top down approach [13] are listed below:

- Step 1: Identify goals – identify top goal(s) and principle claim
- Step 2: Definition of the basis on which goals are stated - ensure adequate and correct understanding of the context surrounding the claim
- Step 3: Identification of strategy – how the claim can be substantiated
- Step 4: Definition of the basis on which the strategy is stated
- Step 5: Elaborate strategy
- Step 6: Identify solutions – claims are at a sufficient level they can be supported by evidence

2.3 Hall Sensor Architectural Overview

As stated previously hall sensors fulfil different applications[1] in the automotive sector, including control systems[2], and control of position/velocity[3]. For example, hall sensors are usually utilised in anti-locked brake, throttle control and valve position applications.

A typical architecture could be as indicated in Figure 2. The reading from the actual hall sensor interface along with the temperature is digitised and processed in the microcontroller (MCU). The MCU transmits the hall sensor reading digitally via a Single Edge Nibble Transition (SENT) interface. Configuration of the unit is possible using an external control interface CNRTx. To provide the redundancy in the design the hall sensor has two channels and each has a separate power supply Vccx. Calibration settings are stored in non-volatile memory.

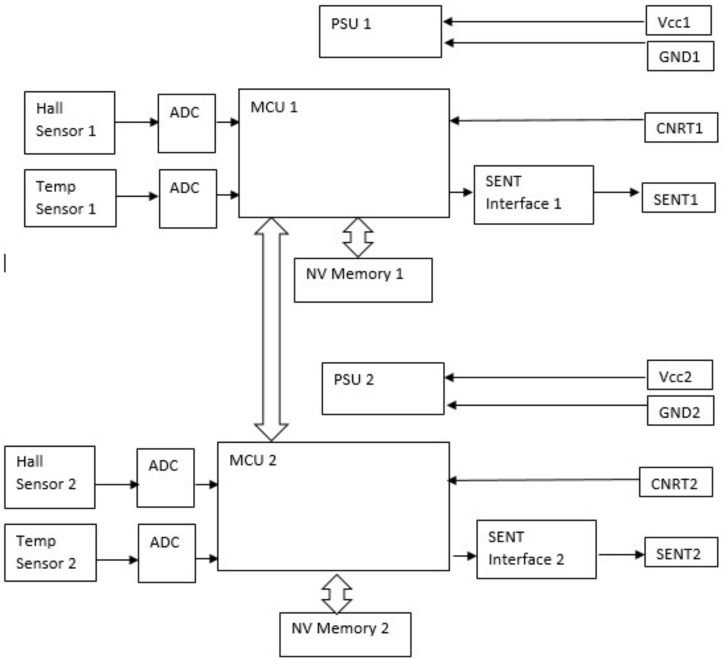

Figure 2 Hall Sensor Block Diagram

3 SEooC Hall Sensor Requirement Capture Utilising GSN

This paper only refers to the functional safety requirements of the hall sensor as defined in ISO 26262, other requirements are not the focus of this paper.

3.1 Hall Sensor Functional Safety Requirement Assumptions

Typical functional safety requirements that would be relevant to a hall sensor may include:

- ASIL requirement to ASIL D
- Maximum magnetic field strength ±250mT
- Sensitivity shall be minimum of 10 LSB/mT
- Non-linearity ±0.1% of the maximum magnetic field strength
- Magnetic drift shall be a maximum of ±5µT
- On board diagnostics to ensure single fault and latent faults detected within the allocated time
- Calibration to ensure the sensor remains accurate over time stored in non-volatile memory
- Diversity of the design to minimise common cause failures
- The non-volatile memory shall be single fault tolerant
- Redundant design prevents a single point failure from rendering the component inoperable
- Lifetime – ensure that the product remains safe and operational for the specified duration

3.2 Hall Sensor Context Assumptions

In addition to the activity of defining assumed functional safety requirements, in order to achieve the assumed safety goals, specific assumptions on the context must also be defined.

In the case of the hall sensor, these may include:

- the external source will ensure there is adequate diversity and freedom from interference between the two power supplies to the hall sensor
- in the case that the hall sensor has detected an internal error and communicated this to the external source, the external source shall take the necessary actions to switch the item to the safe state within the defined fault reaction time
- the external source will ensure that mechanical limits of the magnet position are met
- the external source will maintain the recommended operating conditions.
- the external source will meet the latency requirements for the hall sensor such that the ISO 26262 fault tolerant time interval (FTTI) requirements are met

Certain applications may require such sensors to meet ASIL D requirements, hence making the process of requirements assumption even more critical.

3.3 GSN SEooC Development Implementation

Figure 3 shows the system level development of the hall sensor assurance case starting from the top goal, the hall sensor meets the ASIL D requirements. The subsequent Figures 4 to 6 illustrate the modules that expand the detail of specific areas of the Assurance Case in Figure 3.

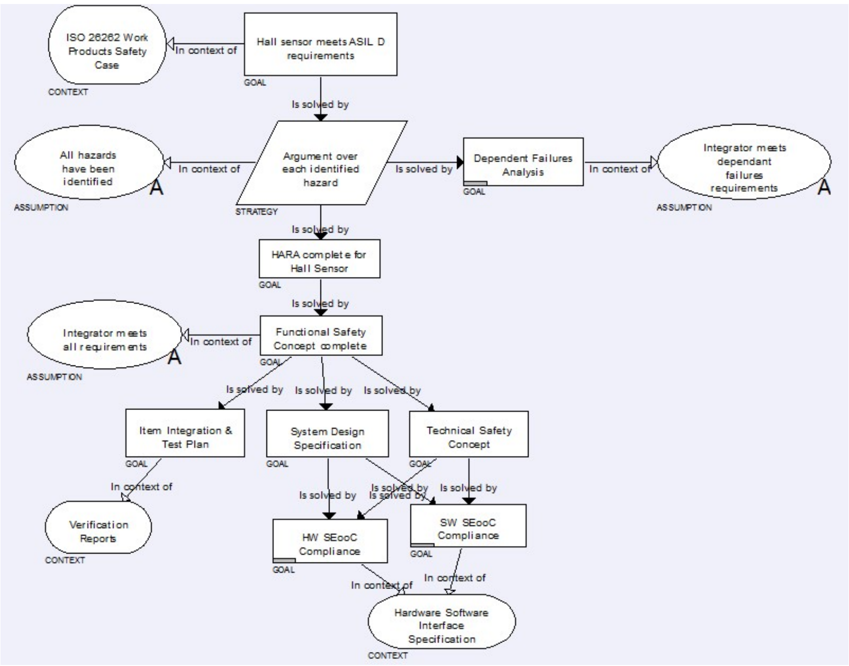
ISO 26262 Work Products Safety Case
CONTEXT
In context of
Hall sensor meets ASIL D requirements
GOAL
Is solved by
All hazards have been identified
A
ASSUMPTION
In context of
Argument over each identified hazard
STRATEGY
Is solved by
Dependent Failures Analysis
GOAL
In context of
Integrator meets dependant failures requirements
A
ASSUMPTION
Is solved by
HARA complete for Hall Sensor
GOAL
Is solved by
Integrator meets all requirements
A
ASSUMPTION
In context of
Functional Safety Concept complete
GOAL
Is solved by
Is solved by
Is solved by
Item Integration & Test Plan
GOAL
System Design Specification
GOAL
Technical Safety Concept
GOAL
In context of
Verification Reports
CONTEXT
Is solved by
Is solved by
Is solved by
Is solved by
HW SEooC Compliance
GOAL
SW SEooC Compliance
GOAL
In context of
In context of
Hardware Software Interface Specification
CONTEXT

Figure 3 GSN Hall Sensor System Level Assurance Case

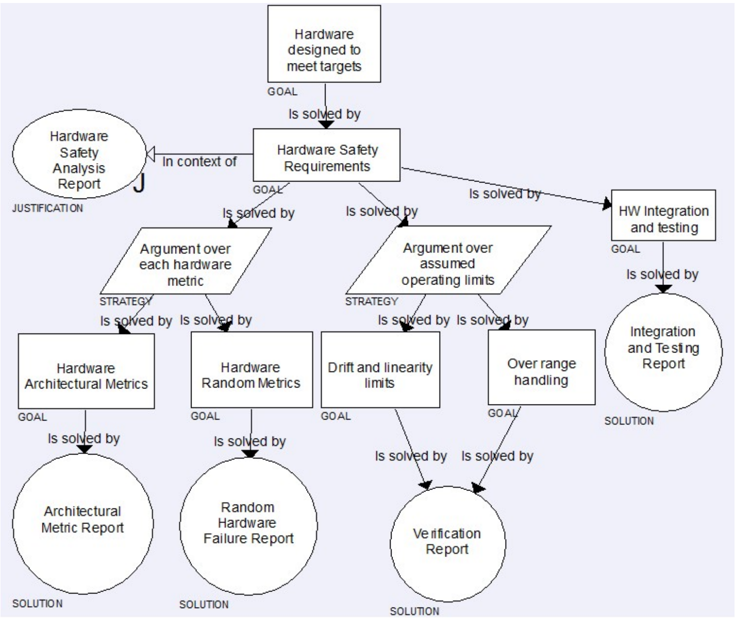
Hardware designed to meet targets
GOAL
Is solved by
Hardware Safety Analysis Report
J
JUSTIFICATION
In context of
Hardware Safety Requirements
GOAL
Is solved by
HW Integration and testing
GOAL
Is solved by
Is solved by
Argument over each hardware metric
STRATEGY
Argument over assumed operating limits
STRATEGY
Is solved by
Is solved by
Is solved by
Is solved by
Hardware Architectural Metrics
GOAL
Hardware Random Metrics
GOAL
Drift and linearity limits
GOAL
Over range handling
GOAL
Integration and Testing Report
SOLUTION
Is solved by
Is solved by
Is solved by
Is solved by
Architectural Metric Report
SOLUTION
Random Hardware Failure Report
SOLUTION
Verification Report
SOLUTION

Figure 4 Module HW SEooC Compliance

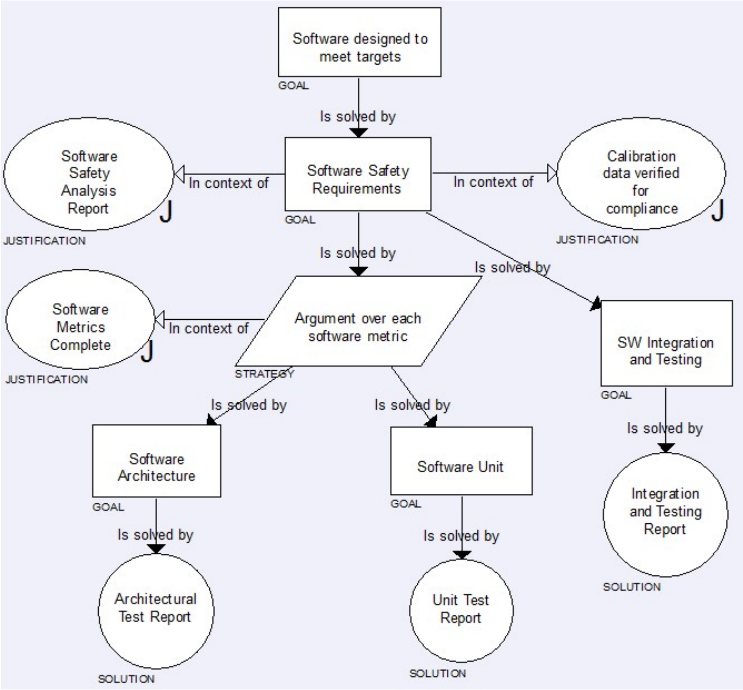

Figure 5 Module SW SEooC Compliance

Figures 3 to 5 start to build the Assurance Case for the hall sensor architecture indicated in Figure 2. The duplicated hall sensor circuit is being defined to provide adequate redundancy to meet the ASIL D requirement. The detailed definition of diverse software design is beyond the scope of this paper, but the use of two microcontrollers (MCUs) enables the freedom from interference requirements to be met. The fault handling capabilities of the architecture are indicated in a simplistic manner in Figure 4 i.e. the +/-250mT range being exceeded represented by the goal ‘Over range handling’. In practice this would be expanded to fully represent each relevant assumed safety requirement.

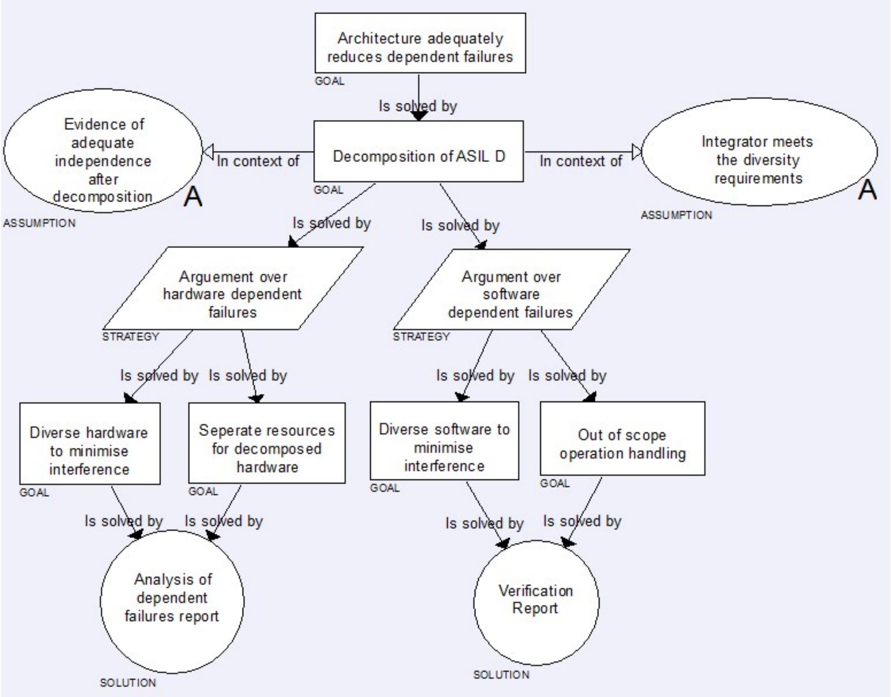
Architecture adequately reduces dependent failures
GOAL
Is solved by
Evidence of adequate independence after decomposition
A
ASSUMPTION
In context of
Decomposition of ASIL D
GOAL
In context of
Integrator meets the diversity requirements
A
ASSUMPTION
Is solved by
Is solved by
Arguement over hardware dependent failures
STRATEGY
Argument over software dependent failures
STRATEGY
Is solved by
Is solved by
Is solved by
Is solved by
Diverse hardware to minimise interference
GOAL
Seperate resources for decomposed hardware
GOAL
Diverse software to minimise interference
GOAL
Out of scope operation handling
GOAL
Is solved by
Is solved by
Is solved by
Is solved by
Analysis of dependent failures report
SOLUTION
Verification Report
SOLUTION

Figure 6 Module Dependant Failure Analysis

Figure 6 expands the assumptions on the dependent failures as the ASIL D requirement is decomposed to lower ASIL ratings. Again, many assumptions are dependent on how the integration team utilise the hall sensor in the Item.

4 *Item Development SEooC Integration*

Referring to the right-hand side of Figure 1, the activities applied during the integration of the SEooC into an Item may have an impact on the assumed requirements defined during the element development phase.

4.1 Assumption Validity

One major advantage of generating the assumed requirements using GSN is that the Assurance Case can be supplied to the integrators and they can use this model during the assumption validation phase (right-hand side of Figure 1). At each stage of the integration the team will validate not only the assumptions, but also the requirements for the item integration. Figure 7 indicates a typical amendment of the system level Assurance Case where certain assumptions indicated in Figure 3 are converted to justifications in Figure 7. During the activity illustrated in Figure 7 the integration team would justify assumptions such as a diversity between the power supplies interfacing with Vcc1 and Vcc2. A software based assumption justified at this point might be that the Item meets the diagnostic error detection requirements of the context based assumptions defined in section 3.2

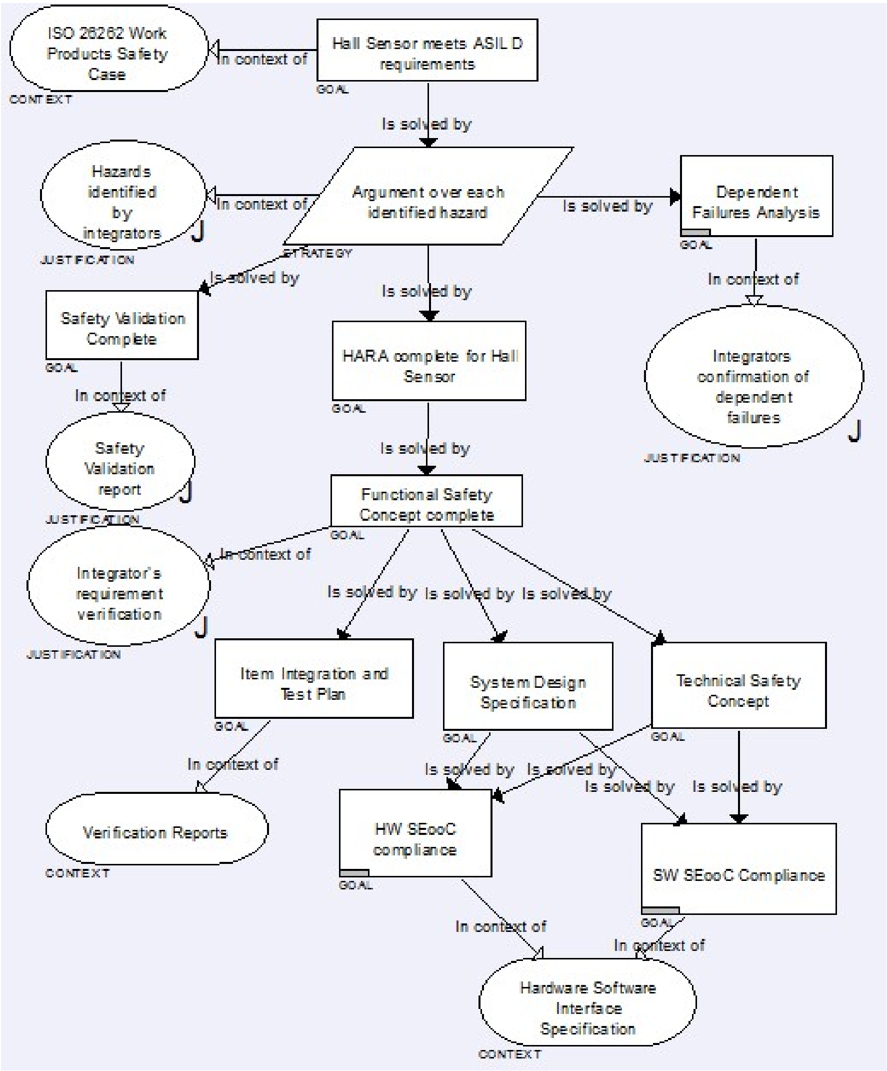

Figure 7 Integrator Validation of Assumptions

4.2 Assumption Mismatch

One of the three potential outcomes listed in ISO 26262 for an SEooC during the integration phase is that a change in the SEooC itself is required. A detected difference may not meet the Item Safety Goal(s) and hence initiate a change to the SEooC.

The result of the assumption validity exercise may not necessarily be positive and both the manufacturer of the element and the item integrator need to be prepared to initiate a change management process in the event that there is a mismatch between assumed requirements and item requirements. Again GSN is a powerful graphic tool that enables a clearly defined mismatch to be highlighted and communicated between the element developer and the item integrator. As the two parties work to resolve the conflict, the GSN assurance case can be amended and exchanged between the teams.

5 GSN and ISO 26262 Coverage

Literature reflects scarce industrial applications of GSN or completed Assurance Case supporting ISO26262 SEooC definitions. As represented by Figure 1, a system SEooC development consists of system, hardware and software assumptions. This paper presents different figures supporting the whole ISO26262 SEooC definition processes described in Table 1:

- Assumptions on the functional safety requirements allocated to the SEooC
- Assumptions on the context of the SEooC
- The validation of the functional safety requirements of the item with the functional safety requirements assumed for the SEooC
- A change management activity, beginning with an impact analysis

Many SEooC manufactures at present list the assumed requirements in accompanying documents. These can be distributed over many pages and the relationship to other assumed requirements may not be easily identified. GSN representation as indicated in Figures 3 to 6 assists in increasing the clarity of the ISO 26262 SEooC activity.

6 Conclusion

GSN, as a technique for documenting assumed requirements, lends itself very well to the process defined in ISO 26262 for SEooC. Assumptions and the rationale behind them can be documented and this documentation shared between the team developing the element and the team integrating the element into the item. A graphical representation such as GSN is both concise and clearer to understand. The granularity of the figures used in this paper are not as fine as an actual GSN representation due to the restricted space in the paper. However, the detail of justification and context in the GSN can be greatly expanded to eliminate ambiguity and support the assumptions used.

The ability to share a GSN assurance case between the teams involved in the development enables a more efficient working relationship between the two teams.

GSN cannot improve the quality of the assumed requirements, this is down to the expertise of the personnel involved, but it can assist those working on the project to reach their conclusions in a more efficient and timelier fashion.

GSN as a technique enables a concise overview of requirement assumptions. However, for a complex element such as a hall sensor the assurance case may reach a size where the comprehension is more of a challenge, due to the large number of strategies, assumptions and justifications.

GSN supports the definition of assumptions that may have been incomplete. This is another area that can benefit from a graphical representation, and in the case of sharing between the two teams, the Assurance Case can then be concluded by the Item integration team.

7 Literature

[1] C. Chen, W. Sun, X. Zhou, and X. Feng, “Magnetic Induction Model of the Hall Sensor: Analysis and Simulation of an Automotive Shift,” *IEEE Veh. Technol. Mag.*, vol. 7, no. 1, pp. 38–43, Mar. 2012.

[2] W.-S. Ra, H.-J. Lee, J. B. Park, and T.-S. Yoon, “Practical Pinch Detection Algorithm for Smart Automotive Power Window Control Systems,” *IEEE Trans. Ind. Electron.*, vol. 55, no. 3, pp. 1376–1384, Mar. 2008.

[3] L. Romero and A. Concha, “Control of Position/Velocity in a Mobile Robot Using DC Brushless Motors,” in *Electronics, Robotics and Automotive Mechanics Conference (CERMA’06)*, 2006, vol. 2, pp. 200–205.

[4] U. Ausserlechner, M. Motz, and M. Holliber, “Drift of magnetic sensitivity of smart hall sensors due to moisture absorbed by the IC-package,” in *Proceedings of IEEE Sensors, 2004.*, pp. 455–458.

[5] D. G. Messerschmitt, “Rethinking Components: From Hardware and Software to Systems,” *Proc. IEEE*, vol. 95, no. 7, pp. 1473–1496, Jul. 2007.

[6] Wells Counter point, “Understanding hall effect sensors,” *Wells Counter point*, 1999. [Online]. Available: http://www.wellsve.com/sft503/Counterpoint3_1.pdf. [Accessed: 31-Mar-2016].

[7] International Standard Organisation, “ISO 26262-1:2011- road vehicles -- Functional safety -- Part 1: Vocabulary,” 2011.

[8] International Standard Organisation, “ISO 26262-10:2012- road vehicles -- Functional safety -- Part 10: Guideline on ISO 26262,” 2012.

[9] J. Spriggs, *GSN - The Goal Structuring Notation*. London: Springer London, 2012.

[10] S. Nair, J. L. de la Vara, M. Sabetzadeh, and L. Briand, “Classification, Structuring, and Assessment of Evidence for Safety -- A Systematic Literature Review,” *2013 IEEE Sixth Int. Conf. Softw. Testing, Verif. Valid.*, pp. 94–103, Mar. 2013.

[11] A. Ayoub, B. Kim, I. Lee, and O. Sokolsky, “A Systematic Approach to Justifying Sufficient Confidence in Software Safety Arguments,” in *SAFECOMP 2012*, 2012, pp. 305–316.

[12] F. Fabbrini, M. Fusani, and G. Lami, “One Decade of Software Process Assessments in Automotive: A Retrospective Analysis,” *2009 Fourth Int. Multi-Conference Comput. Glob. Inf. Technol.*, pp. 92–97, 2009.

[13] Origin Consulting, “GSN COMMUNITY STANDARD VERSION 1,” *Origin Consulting*, 2011. [Online]. Available: http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf. [Accessed: 06-Apr-2016].

8 Author CVs

Xabier Larrucea
Xabier Larrucea is a senior project leader and research scientist at Tecnalia and a part-time lecturer at the University of the Basque Country. He is IEEE Software constituency ambassador for Spain and Latin America. His research focuses on areas such as safety-critical software systems, software quality assurance, software process improvement, empirical software engineering, and metamodeling technology strategy. Over the last decade, he has managed several European research projects related to information and communications technology. He has also provided consultancy activities related to software engineering. He contributed to several Object Management Group standardization initiatives, such as SPEM 2.0 and UPMS. Larrucea has received a computer engineering degree, a PhD in software engineering, an executive MBA, and Project Management Professional certification. Contact him at xabier.larrucea@tecnalia.com.

Silvana Mergen
Silvana Mergen is a development engineer at TDK-EPC and responsible for matters relevant to Functional Safety after the ISO 26262 in the Sensors Business Group. Silvana holds a materials science degree, a PhD in Piezoelectrics from Cranfield University and a TÜV-certificate in quality management. Before joining TDK-EPC she was a project leader at The HEARing CRC as well as a research fellow at the University of Melbourne working in the field of Cochlear implants. Silvana has over 10 years of research experience in sensor development and development of medical devices.

Alastair Walker
Alastair Walker is an engineer with over 25 years development experience in medical, automotive and aviation industries. He is a TÜV Rheinland Functional Safety Engineer and has extensive knowledge of developing embedded systems in safety related industries, such as ECG stress test, cryotherapy and electrical muscle stimulator systems, automotive inverters and aviation transponders.