World Academy of Science, Engineering and Technology
International Journal of Industrial and Manufacturing Engineering
Vol:17, No:6, 2023

Approach for a Safety Element out of Context for an Actuator Circuit Control Module

H. Noun, C. Urban-Seelmann, M. Abdelfattah, G. Zeller, G. Rajesh, I. Mozgova, R. Lachmayer

***Abstract*—**Several modules in automotive are usually modified and adapted for various project-specific applications. Due to a standardized safety concept a high reusability is accessible. A safety element out of context (SEooC) according to ISO 26262 can be a suitable approach. Based on the same safety concept and analysis, common modules can reach high reusability. For developing according to a module out of context, an appropriate and detailed development approach is required. This paper shows how to deduce this development processes for platform modules. Therefore, the detailed approach of the SEooC is derived. The aim is to create a detailed workflow for all phases of the development and integration of any kind of system modules. As an application example, an automotive project for an actuator control module is considered.

***Keywords*—**Functional Safety, Safety Element out of Context, System Engineering, Hardware Engineering.

I. Introduction

THE considerably increasing complexity of modern vehicles and equipped high number of control units lead to major challenges regarding their safety. Any malfunction that may occur in electronic control units can lead to personal injury and must be prevented as far as possible in order to ensure the functional safety of the system [1]. In general, functional safety is concerned with the ability of a system to transition to a safe state when accidental or systematic malfunctions in the system could lead to a life-threatening situation. It is therefore mandatory for automotive original equipment manufacturers (OEM) and suppliers in the automotive industry to develop systems according to international safety standards. For the development of electrical and electronic systems in motor vehicles, these safety standards must be fulfilled in order to avoid unacceptable risks to people from vehicles. The standards are used to derive new safety requirements for these systems that prevent the risks when implemented correctly.

To provide manufacturers with a common approach for determining and achieving functional safety for their systems, the first edition of the ISO 26262 standard was published in 2011 and was followed in 2018 [1] by the second edition, in which the standard was completed with further additions (ISO2626:2018). The standard consists of a set of guidelines and recommendations on how to achieve the required level of safety in the system. In the electronic control units of these systems many different circuit modules are in use. Several modules are usually modified and adapted for various project-specific applications. In order to reach a high reusability, standardization of its safety concept is needed. One approach is the concept of the Safety Element out of Context (SEooC) in the ISO 26262 standard. Due to common modules, these can be developed and reused with the same safety concept and analysis. In order to start a development for SEooC an appropriate and applicable development process is required. This shall be evaluated, derived and applied for an actuator module in order to get a validated workflow.

A. Construction of an Electronic Vehicle System

The main component of a modern vehicle system is the electronic control unit (ECU), which is comparable to a small computer and which controls the system outputs. It uses the input signals from sensors or other systems to control the necessary actuators or other outputs. For the electronic control of a vehicle system, these electrical sensor signals must be first acquired and processed by integrated software in order to control the electromechanical actuators according to the desired application. Fig. 1 shows the structure of general control electronics for any vehicle system.

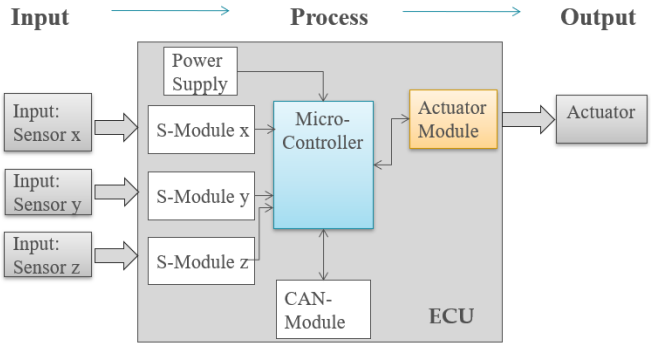

Fig. 1 Simplified construction and principle of an electronic automotive system

Based on the received information from various sensors in the vehicle, signal inputs are first prepared in the ECU and processed in the microcontroller. The processed signals in the microcontroller are transmitted to controllable elements in the system and finally used to control the coupled actuators or outputs according to the requirements of the system. The input signals as well output signals are processed due to several hardware modules.

B. Actuator Circuits in Automotive Systems

In a vehicle, different actuators are used to operate a function.

Hassan Noun is with Leibniz University Hannover, Germany (phone: +49 511922-2042; e-mail: hassan.noun@zf.com).

An actuator can be a door lock solenoid valve, a fuel injection, a relay, or an ignition coil. Other final effectors can be stepper motors, headlights or a high torque motor [2]. In the electronic itself complex transistor circuits are used for this purpose. A typical application for a transistor is to turn one of these devices on and off. These transistors thus act as electronic switches. In this regard, there are two specific configurations for a transistor switch: namely, a high-side and a low-side. When the actuator has to be controlled by connecting it to the positive battery power source, then a high-side driver is needed. If the load is controlled by connecting to the negative pole of the battery (ground), a low-side driver is required. Both drivers are designed as electronic switches and will be referred to as high-side switch (HSS) and low-side switch (LSS) in the following sections. An example circuit is shown in Fig. 2, in which two individual actuators are controlled independently by an HSS and an LSS. Both actuators are only energized if the respective switch is closed (low impedance). For actuator B, the LSS switches the current path to ground. The load here is between the positive battery current source and the transistor. With the actuator A, the transistor is between the battery and the device itself. The HSS switches between battery voltage and actuator.

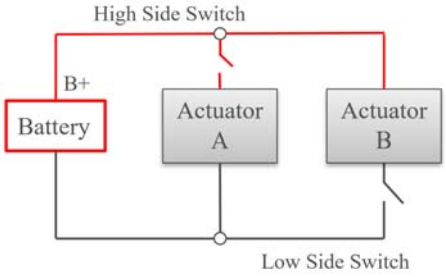

Fig. 2 Two separate loads can be controlled by using a switch [3]

The transistor switches are controlled by a digital microcontroller and all switching operations are performed by a software process. The type of transistor can be chosen arbitrarily (bipolar transistor (BJT), field effect transistor) [3].

C. Safety Element out of Context

In the automotive industry, generic components or elements are developed for different applications and different customers. Here, assumptions are already made with regard to requirements and design. An element can be a system or subsystem, as well as a hardware or software component. Requirements according to functional safety are also planned for such elements. They are often developed in such a way that they can be used as SEooC. An SEooC is a safety-related element that has been developed not only for a specific application or in the context of a specific vehicle, but for which no item exists yet during development. They can be integrated into many different but similar systems [1]. Examples of SEooC are ECUs, controllers, microcontrollers or various software components for implementing communication protocols. The development of a SEooC is based on assumptions according to ISO26262 which are made for intended functions and uses and include interfaces. When developing an SEooC, assumptions are therefore made about the requirements. This can be, for example, a software component that must be developed according to ISO 26262. Fig. 3 shows the relationship between the assumptions and the SEooC development. Here, the development of an SEooC can start at a certain hierarchical level of requirements and design. The requirements are derived from the assumptions related to the design. Proper implementation of the requirements is verified during the development of the SEooC. Validation of these requirements and assumptions then occurs only during the development of the contextual target item. Based on assumptions regarding the requirements, developers define the purpose, functions, and external interfaces with other items. Initial assumptions may be, for example, that the system should be designed for vehicles of a certain weight and drive type. After this, the assumptions become more precise. Furthermore, functional requirements are derived from the assumptions. These are then such that the system should activate and deactivate the function when the driver wants it to. In addition to the functional requirements, there are also the safety requirements. In the development of a SEooC, assumptions are made about the item definition, its safety goals and its safety objectives. From this, the corresponding functional safety requirements (FSR) can be defined in terms of the functionality of the SEooC, from which the technical safety requirements (TSR) can then be derived [4]-[5]. In the standard, the development process (process flow) of a SEooC (sub-) system is described as shown in Fig. 3. For a new design, the concept phase is performed first, and then item-level assumptions are derived.

If a previously developed SEooC is reused, the results from the concept phase only need to be updated. The adopted FSRs then form the input for the design at system level (ISO 262626-4), at hardware level (ISO 262626-5) and/or at software level (ISO 262626-6). If the SEooC is then used in the development of an item, the FSRs of the item are compared with the FSRs assumed for the SEooC. In case of a mismatch, a change management process must be initiated that includes an impact analysis. The adopted safety requirements are validated during the development of the item, not during the SEooC development process.

II. Determination of Working Steps

The ISO suggests activities to be carried out for the development of the SEooC. These are divided into four major steps and are illustrated in Fig. 4. The development of the SEooC and its implementation are divided into two separated activities. The SEooC supplier develops the element and the integrator develops the item and integrates the element into its context. In the first step, the assumptions for the safety requirements of the SEooC are created by the supplier. The second step is the development of the SEooC according to the safety lifecycle of ISO 26262. The consistency of the requirements from the assumptions and the corresponding implementations must be checked during the SEooC development phase [6], [7]. In the third step, the work products and documents are provided to the item integrator during the SEooC development, which will be used in the item

development.

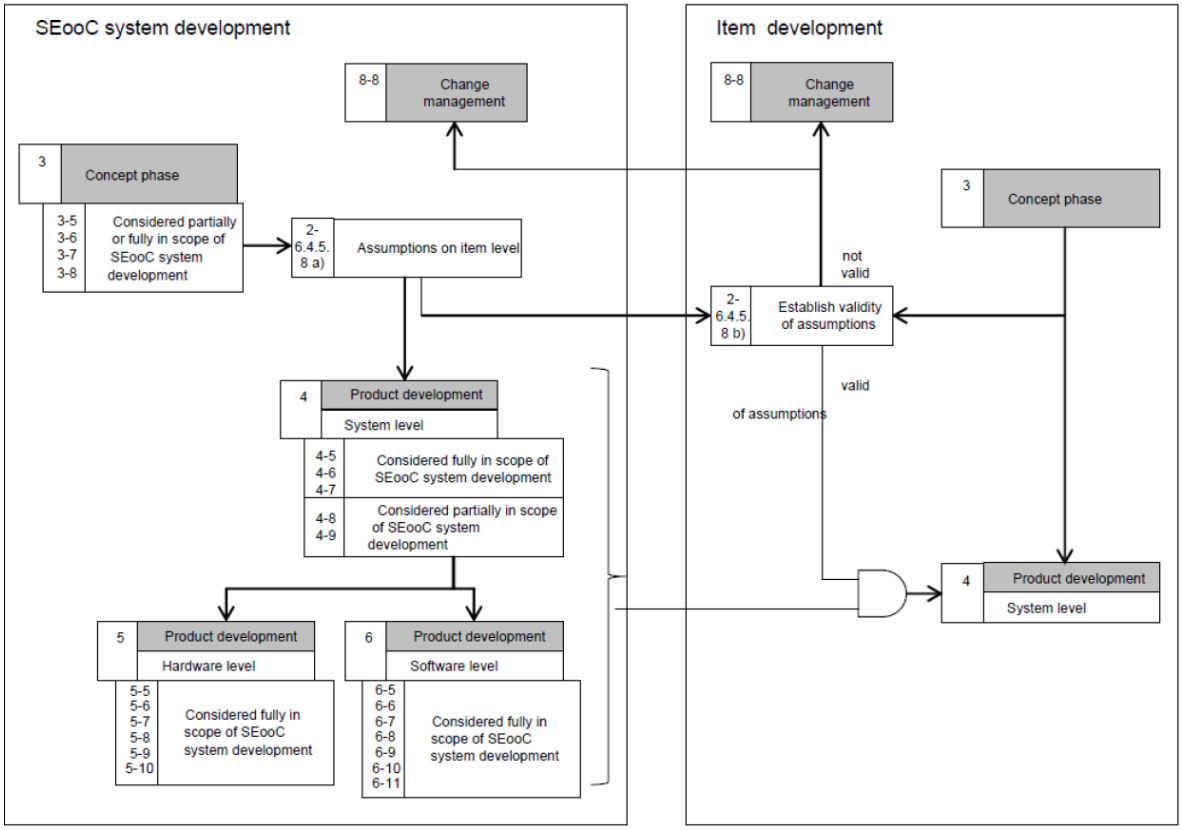

Fig. 3 Process flow of a SEooC development [1]

The integrator takes the documents of the assumptions and safety analyses and compares the safety requirements. The fourth step is the integration of the SEooC into the item [8], [9].

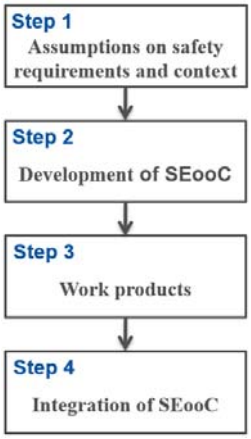

Fig. 4 Simplified workflow of a SEooC

A. Workflow of the SEooC

Based on the derived major steps further activities need to be decomposed. In order to define a process flow from the ISO 26262 activities for the development, an extension and interpretation of the SEooC approach is presented in following. This is illustrated in Fig. 5 and shows the development of the SEooC as well as the development of the item and how these are linked. In the SEooC Development the supplier activities are organized. In the Item Development, the item integrator develops the item and performs the integration of SEooC into it. In Step 2, the corresponding safety analyses are performed in all three levels. They differ in the method and are required by ISO 26262 depending on the Automotive Safety Integrity Level (ASIL). Deductive analyses include the Fault Tree Analysis (FTA) and the FMEA is an inductive analysis. In the hardware level, in addition to the FMEA of the design, the determination of the safety metrics is done by calculating the Failure Mode Effect and Diagnostic Analysis (FMEDA) of the hardware design. On the right side of the V-model, the metrics determined from the safety analyses are tested and verified. It is the task of the SEooC developer to verify the derived safety requirements from the assumptions [9]. For this purpose, safety related test cases are specified for the defined TSR and safety mechanisms and then tested in all three levels. They should prove that the requirements are implemented properly. When all safety mechanisms have been successfully tested and the required metrics have been achieved, the verification is complete.

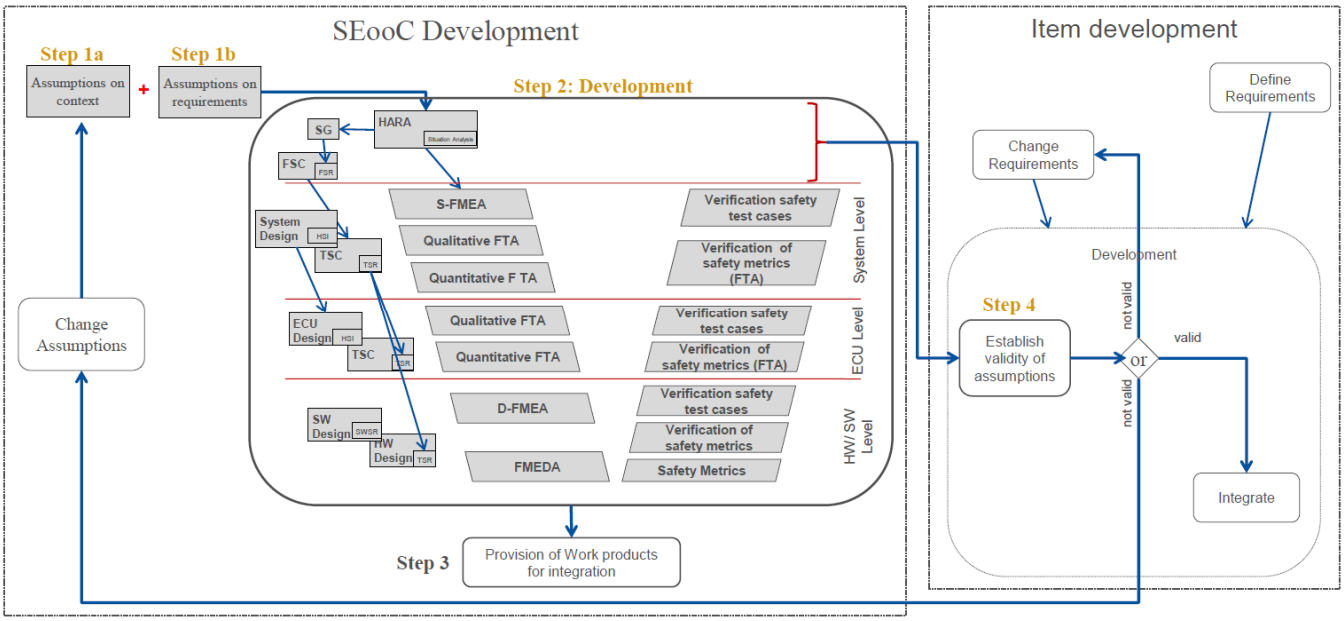

Fig. 5 Derived SEooC development process

III. Development of the SEooC

In the second step, the SEooC is developed based on the assumptions made in accordance with the complete safety life cycle. In Fig. 5, the second step of the SEooC development includes the development processes, which are based on the V-model and are consistent with the development of the ISO 26262 standard. Here, the company's internal safety process for development and safety analysis related to ISO 26262 is incorporated into the development of the SEooC. Based on the assumptions in the vehicle level, the safety objectives as well as the safety concept are determined and broken down to the lower levels. The activities for the functional and technical safety concepts are carried out in accordance with the safety objectives defined by ISO 26262. The further safety process is divided into three levels and is described according to the V-model. Here, the ECU level corresponds to the system level in the standard. In the next level, the ECU is integrated into the vehicle system. At the top level, Hazard and Risk Assessment (HARA) is performed at the vehicle level, in which the actual safety objectives for the assumed context of the SEooC are determined and the highest safety requirements are subsequently derived. From this, all product development safety analysis activities are broken down to the lower levels. As part of a SEooC development the following safety related artefacts can be summarized:

- Item Definition
- TSR
- TSA (Technical Safety Architecture)
- HSI (Hardware-Software Interface)
- Block Diagram
- Design/Schematic
- FTA
- FMEDA
- Fault Injection Test Report
- Product Specification
- Safety Manual
- Safety Case Report

A. Example of SEooC for an Actuator Control Circuit

In the item definition, the SEooC should be now defined in order to obtain a comprehensive understanding of the item so that the subsequent steps, such as the determination of the safety objectives and safety requirements, can be performed. This requires a detailed description of the item, its functionality, and its dependencies and interactions with other items. The functional requirements can be derived from the assumptions of the various contexts into which the element has to be integrated. In this example the item is a (sub-)system which is controlling an external actuator. The element is an actuator circuit, which shall be developed as a reusable module. The purpose is to integrate this module in various possible vehicle systems with the same or lower ASIL rated functions. Fig. 6 gives an overall view of the integrated circuitry within a vehicle system and its interfaces with subsystems. The circuit is controlled by application software in the microcontroller, which processes the input data and controls the output stages due to control signals. The output stages of the circuit activate the load.

The actuator can alternatively be controlled by a single switch in the low-side variation. This circuit variation has advantages and disadvantages due to its simplicity. However, it would not meet any required safety in the event of a switch malfunction. If there were a short to ground on the low voltage side of the actuator (LSS), then this would cause the unintended activation of the actuator. Thus, a safety objective is violated here. In order to be able to deactivate the load when a short to ground occurs on the low voltage side of the actuator, the low-side MOSFET will be supplemented by a high-side MOSFET that can turn off the battery voltage of the actuator. Therefore, the configuration of an additional HSS serves as a safety

mechanism for the circuit, which, in conjunction with diagnostic software, increases the diagnostic coverage of critical faults.

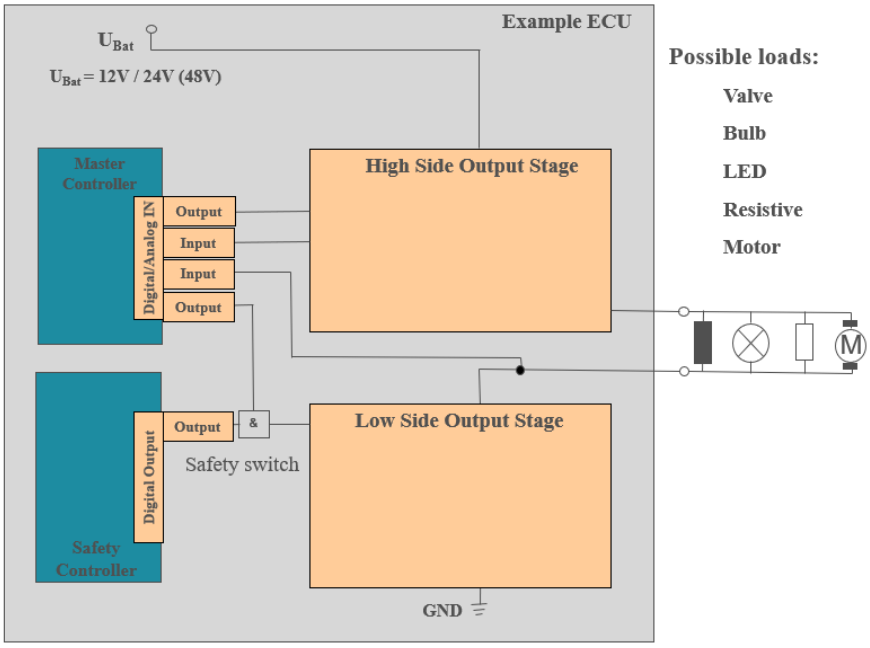

Fig. 6 Simplified circuit architecture of an actuator module. Due to a high side and a low side switch several actuators can be controlled

B. Assumptions of the Context

The development process starts with the safety assumptions. Further the rating will be assumed. Since the entire process is highly dependent on these assumptions, it is important that they are reliable and consistent. The safety standard does not limit the number of contexts [9]. Here the developer of the SEooC can foresee several use cases in different types of items without having a concrete or specific item in mind. As part of this example the item is controlling an actuator as SEooC, which activates or deactivates the actuator on demand. This results in an element for several target applications with any wired actuator. This can be integrated into a variety of potential vehicle systems. Examples may include the following applications:

- Electric braking - ASIL D
- Steering control - ASIL D
- Anti-lock braking - ASIL D
- Motor control management - ASIL D
- Electronic suspension control: ASIL D
- Gear shift control: ASIL D

The ASIL rating for the target item obtains ASIL D in order to cover the highest criticality. Regardless of whether the SEooC being developed is a system or subsystem, or a hardware or software element, the assumptions are made at the system level. Assumptions about contexts as well as requirements are made at the system level and result in sets of requirements, which serve the development of the element. At this level the actuator incidents can be summarized to the following two critical top events:

1. Unintended activation of the load.
2. Unintended deactivation of the load.

These two top events are covering all possible critical failures independent of the electrical, pneumatic and hydraulic logic of the system peripherals. For these reasons, the safety objectives are accordingly defined in such a way that these main hazards must be prevented. In this case the safe state is the deactivation of the actuator with a further warning operation. This shall transit the system into a controllable situation, even if in case of a loss of the entire control unit. The target system must take over this as a constraint. In conclusion the safety goals including the safe state can be summarized as in Table I.

TABLE I
TABULAR LIST OF SAFETY GOALS, THE SAFE STATES AND THE ALLOCATED ASIL RATING

ID	Safety Goal Description	Safe State	ASIL
SG 1	The item shall prevent unintended activation of the load. FTT = tbd ms.	The item shall disable the corresponding high and low side switches in case of any detected failure.	D
SG 2	The item shall prevent unintended deactivation of the load. FTT = tbd ms.	The item shall disable the corresponding high and low side switches in case of any detected failure.	D

C. Requirements and Documents Structure of the SEooC

The top events are allocated to the system level and need to be decomposed into more detailed TSR on a subsystem level. Further these are inputs for electronic specifications which satisfying the upper level. For this purpose, an architecture document is available, which also contains the hardware design. The software requirements document contains the software design and the software safety requirements. These two documents are verified by the test specifications documented in

the test specification document. Fig. 7 presents the requirements structure of SEooC example.

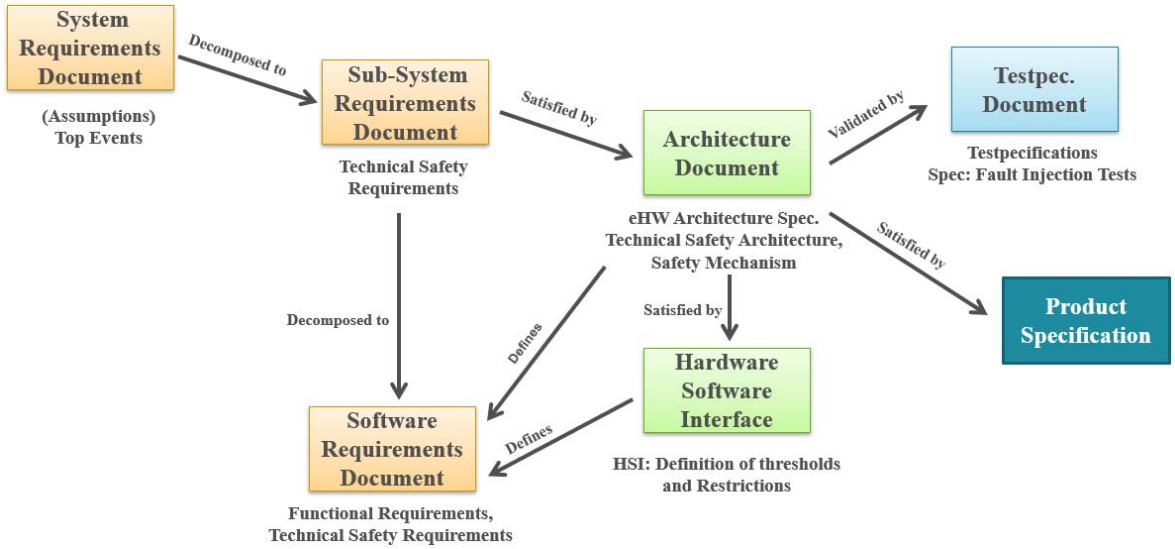

Fig. 7 Simplified requirements document structure of the SEooC example

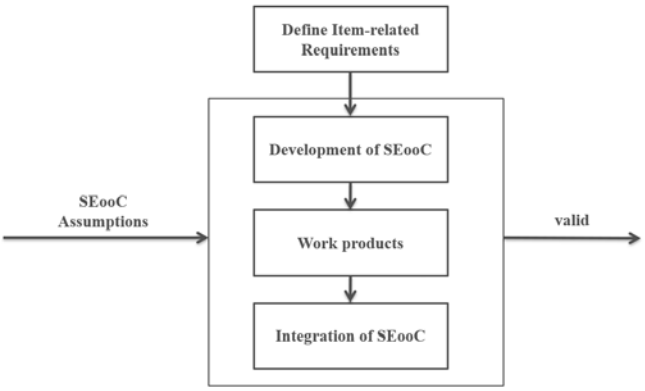

Fig. 8 Simplified illustration of the validation of the assumptions for the target system

IV. Integration of the Element

In the last step it is necessary to integrate the element into the target item. In this phase, the assumptions of the SEooC development need to be considered by the item integrator. It must compare the validity of the assumptions and adapt the requirements to the item. The item integrator must ensure that the SEooC is integrated properly into the context and is matching the safety requirements of that item and does not violate any of its safety objectives. From the perspective of the item, it must be verified that the assumptions are valid. This is only feasible if the supplier has considered all necessary safety related requirements during development of the SEooC without knowing the actual requirements of the item. The concept phase of the item development results in top events and the ASIL rating. In the following the safety objectives are determined and further refined into FSR, which are assigned to the architectural elements in the next step. These are the actual safety requirements of the item. Once the SEooC is used in a contextual system, the assumed requirements are compared and matched with the actual safety requirements assigned to the module. This step, which is identified as Step 4 in Fig. 5, is to determine the validity of the assumptions in the SEooC development. Here, the assumptions about the safety requirements of the SEooC are compared with the determined requirements of the item. For this, the validity check of the assumptions has been extended and interpreted in more detail. In case of a validity of the safety objective the refined FSRs also need to be compared. In the next step it is necessary to check the validity of the existing safety analysis.

A. Mismatch of the Requirements

According to the safety standard as well according to other quality standards a proper change management is necessary in case of mismatches between the development and the requirements. In case of a discrepancy of the safety requirements, a change management process must be initiated. This process includes the change request and an impact analysis of the change of the system. The changes may have potential impacts on safety-related functions or properties and thus on the functional safety of the system. For each required change, an impact analysis must be performed for the element and its interfaces. After this, the functional safety processes must be performed again and verified. Thus, the process ensures the implementation of required changes while maintaining the relevant functions and properties of the item throughout the entire safety life cycle. Among the possible results of a change management process in the event of a nonconformance of safety requirements, the three scenarios shown in Fig. 9 are conceivable.

If the change requirement does not result in an impact on the implementation of the safety target under consideration, no further action is required. If there is an influence, a change in the item definition or the functional safety concept of the item is necessary. Here, the item developer adjusts the requirements

accordingly so that the item with the integrated element meets them. An example of this can be a defined fault tolerance time interval (FTTI) of the item developer, which the SEooC does not achieve. According to this, the item developer can adjust this requirement, if necessary and if this does not result in a safety goal violation.

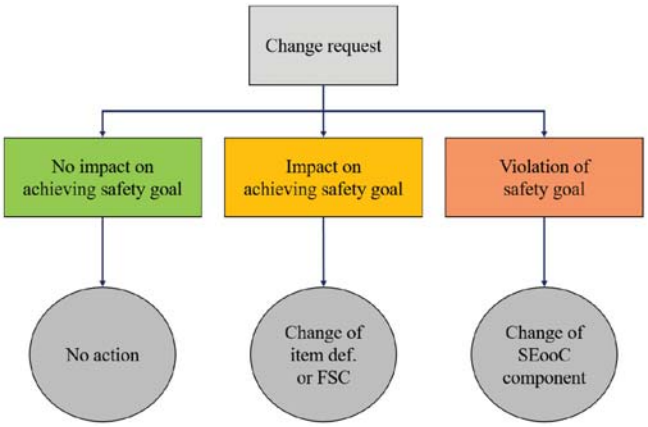

Fig. 9 Simplified illustration of the impact due to changes at item level

V. Summary and Conclusion

For the development of safety critical modules in automotive, additional development steps and work products are necessary. The creation and establishment of these processes are complex. By evaluating, deriving and applying of a standardized module according to the SEooC approach the relevant process structure can be presented. This detailed workflow has been worked out. The linked processes provide a guideline for process development from the identification of work steps and work products to their creation and application. In the next step this approach has been applied in an automotive platform development project for a standard module. As part of this an industry practice shows how to apply this approach for an actuator control module. In future automotive projects this worked out approach can be applied for new systems, subsystems or circuit modules. Further as part of new safety related projects, the reusability of these processes can be validated in separate domains as system, hardware and software development. Furthermore, other best practices can be gathered for item integrations or change management. This can be evaluated and considered by ASPICE and other quality management processes.

References

[1] ISO26262:2018, International Standard Organization
[2] K. Reif, “Automobilelektronik”, Springer, 2009.
[3] N. Zaman, “Automotive electronics design fundamentals”, Springer, 2015.
[4] N. Adler, “Modelbasierte Entwicklung funktional sicherer Hardware nach ISO26262”, Karlsruhe, KIT Scientific Publishing Verlag, 2015.
[5] V. Gebhardt, “Funktionale Sicherheit nach ISO 26262: Ein Leitfaden zur Umsetzung”, Heidelberg, dpunkt.verlag, 2013.
[6] M. Hillenbrand, “Funktionale Sicherheit in der Konzeptphase der Entwicklung von Elektrik/Elektronik Architekturen von Fahrzeugen”, Karlsruhe, KIT Scientific Publishing, 2015.
[7] P. Löw, “Funktionale Sicherheit in der Praxis: Anwendung von DIN EN 61508 und ISO/DIS 26262 bei der Entwicklung von Serienprodukten”, Heidelberg: dpunkt.verlag, 2011.
[8] R. Nörenber, “Effizienter Regressionstest von E/E-Systemen nach ISO 26262”, Karlsruhe: KIT Scientific Publishing, 2012.
[9] H. Ross, “Funktionale Sicherheit im Automobil ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährter Managementsysteme”, München, Hanser, 2013.