Europe, Sept 2015

Safety Extensions of AUTOSAR Models

AUTOSAR R4.2.1 Safety Extension

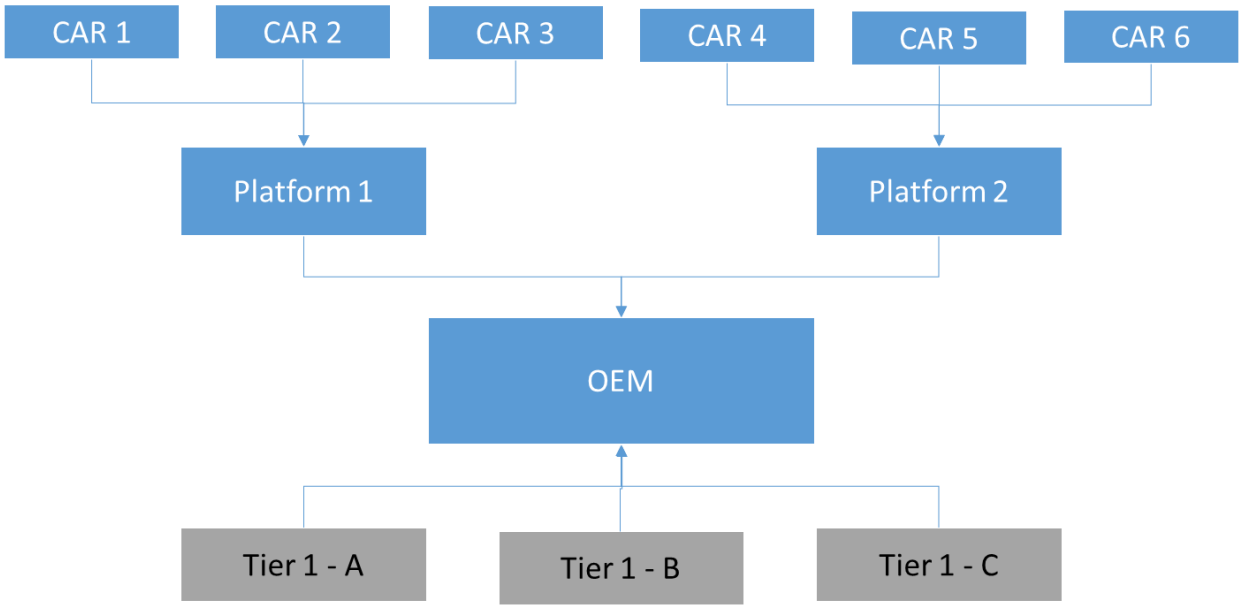
Functional safety is an increasingly important topic in automotive organizations including OEMs, Tier 1 and Tier n. In this article we describe a solution for common problems faced by automotive organization when safety information need to be exchanged along the organizations in the supply chain.

Functional safety activities do concern the whole lifecycle of the system (item) under development and are a cooperative effort of all participating stakeholders. Thus safety related work products have to be exchanged between (all) the organizations involved. Details as roles, responsibilities and work products shall - according to ISO 26262 - be specified in a Development Interface Agreement (DIA). However, it is not prescribed by ISO 26262 how such information should be exchanged (in terms of content, formats etc.) In current practice this leads typically to inefficient manual document centric processes with information duplication on both the consumer and the supplier side in the supply chain. It may also happen, that important information is missing at the time when certain activities (like the provision/configuration of safety mechanisms of basic software) are finally executed. Results are inconsistencies, limited traceability and difficulties when demonstrating the overall safety case.

On the other side, the AUTOSAR Architecture together with the AUTOSAR methodology and supporting tools already work between organizations in the supply chain by providing standard exchange formats and a common methodology. Using these formats, relevant software system and ECU implementation information can be easily exchanged. In the following, we want to explore how a standard like AUTOSAR could solve the functional safety problem in an elegant way.

Let us take an example of an OEM functional safety deployment for a vehicle platform.

Figure 1 Vehicle Platform



In the development process, there could be following general phases related to functional safety activities and work products:

OEM design & definition:

The OEM provides the general concepts for the items (systems) of the same platform. The functional safety concept work is typically started at the item level(s) of a vehicle platform leading to safety goals and requirements for the different items, systems and sub-systems of the platform.

OEM to Tier 1 transfer:

The functional safety concepts of the OEM are then shared to Tier 1 for their specific items, system or sub system.

Tier 1 design and definition:

The Tier 1 could already have developed a (sub-) system specific safety concept using the safety element out of context method before or in parallel the OEM specific safety goals and requirements are available to them. This approach allows a safety implementation to exist based on an assumed system.

Tier 1 redesign and redefinition:

Once a Tier 1 receives the functional safety concept of the OEM, it needs to match safety requirements which are already met using the existing safety concept and potentially design or redesign the safety concept to meet the OEM's requirements.

Tier 1 implementation

To meet the safety requirements and safety goals there would be many safety measure or mechanisms taken in the sub system, this would result in specific safety mechanism being implemented and validated at sub system or system level by the Tier 1.

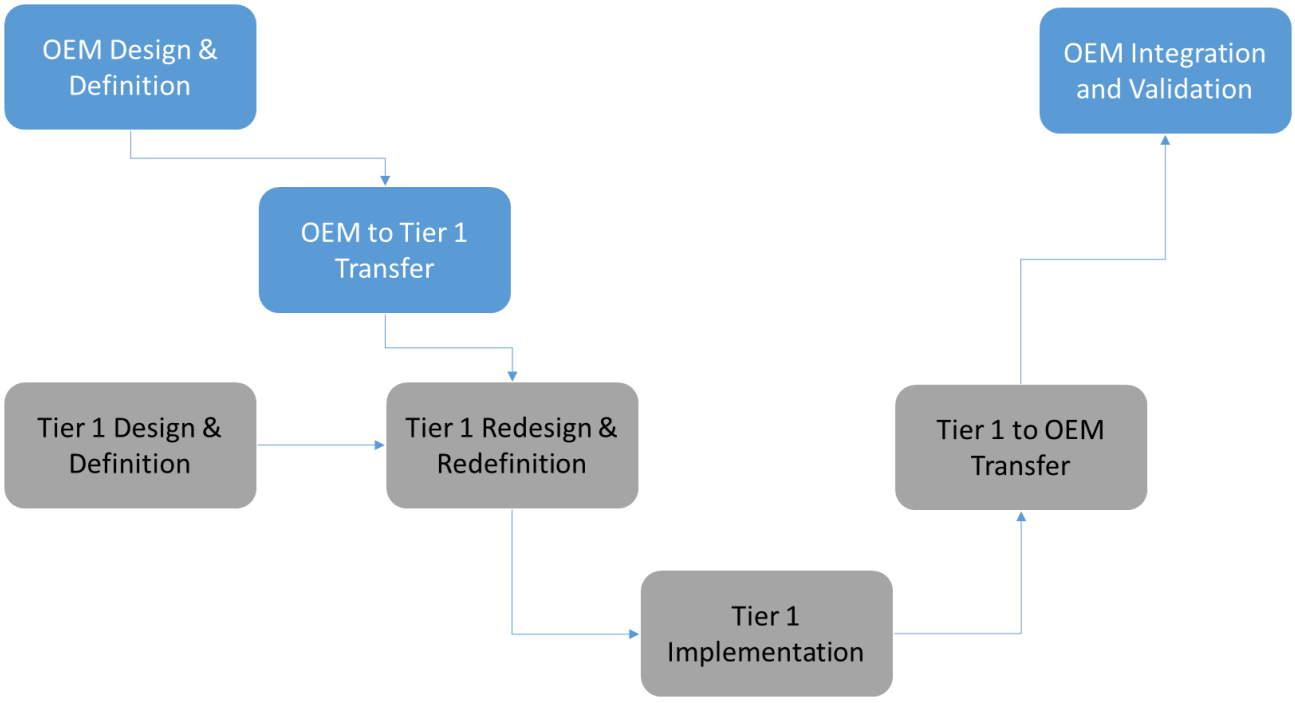
Tier 1 to OEM transfer

The Tier 1 would transfer its implementation back to the OEM, together with information on safety measures or safety mechanisms that have been implemented in order to fulfill the OEM's safety requirements.

OEM Integration and Validation

The OEM would collect various implementation for integration of the safety concepts into their system and perform validation of the system on a vehicle platform level. This could be an iterative process.

Figure 2 Safety Phase



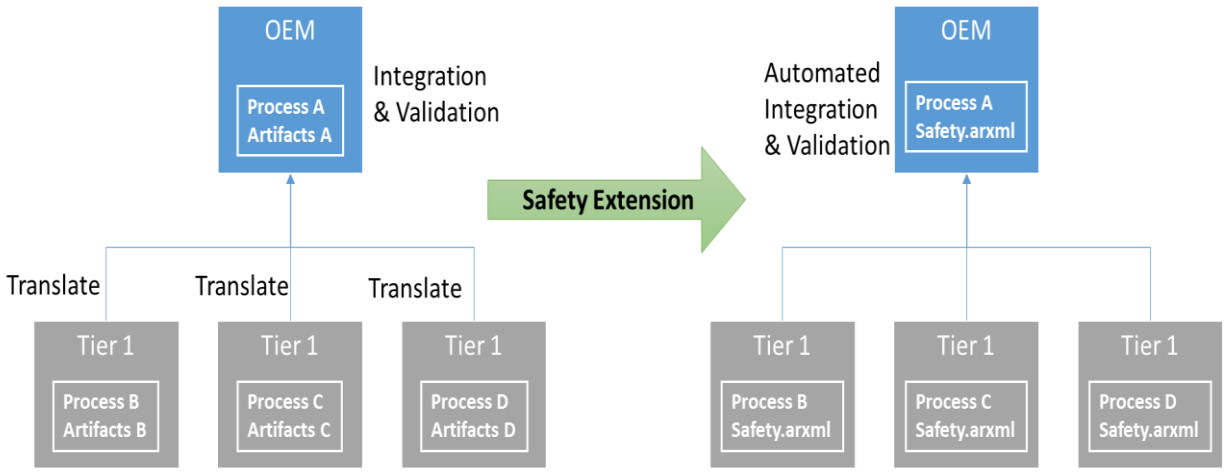
A similar process would occur for lower Tier's, which contribute to the Tier 1 work. The above described difficulties in transferring safety related information mainly exists in 2 phases when such information is exchanged between organizations:

- OEM to Tier 1 Transfer - the information to be transferred contains the relevant parts of the functional safety concept that means the safety goals and requirements, safety considerations in the architecture and allocation information of safety requirements to elements of the architecture.

- Tier 1 to OEM's Transfer – here the information on the implemented safety mechanisms and measures and the mapping between the safety requirements and such mechanisms is the important information.

-

As initially described, the OEM will potentially communicate to multiple Tier 1 suppliers and the Tier 1 suppliers usually again have to communicate to multiple Tier n suppliers. The presence of a standardized exchange format for safety information will ease the communication between organizations and avoid cost intensive and error-prone re-work or translation of safety related information.

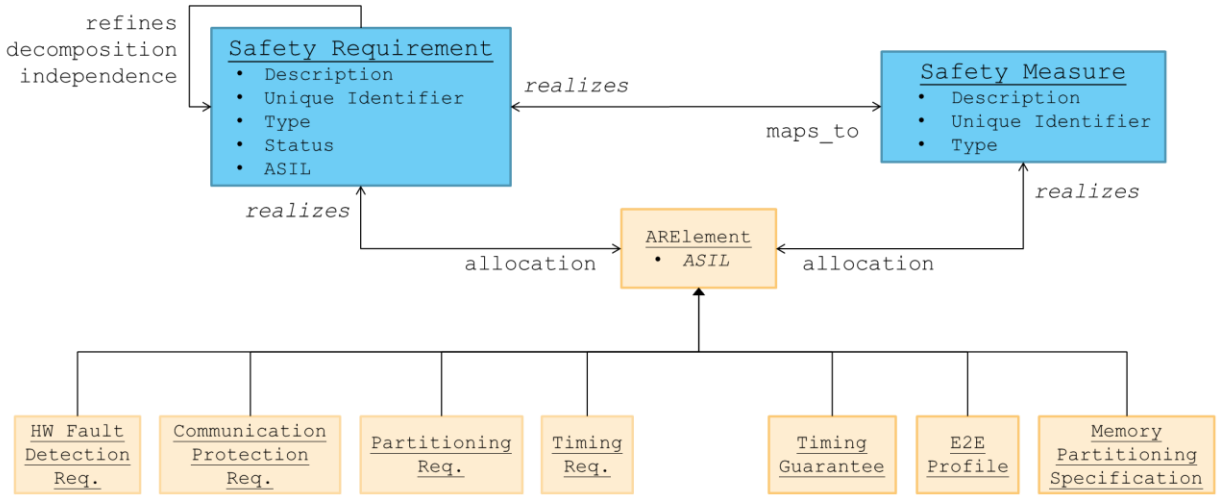


In AUTOSAR based developments, the AUTOSAR Safety Extensions introduced in release 4.2.1 provide such a standardized exchange format. In addition to the introduction of the pure exchange format, the AUTOSAR Methodology has been extended and now contains activities in which the safety related artifacts are produced.

The idea of the Safety Extensions is to facilitate the AUTOSAR XML (.arxml) representation as the format in which safety information is represented and exchanged. In the current release as part of

AUTOSAR 4.2.1 an approach is used which does not impact the existing AUTOSAR metamodel. The new standard defines how the information has to be provided using only existing generic concepts of the AUTOSAR metamodel by applying specific standardized tags and contents. The idea is, that in addition to the usual AUTOSAR models that are exchanged among organizations in the supply chain, the safety extensions are provided which add new elements to the model and refer to existing elements. The safety extensions can be applied as extension only that means, they do not affect exiting AUTOSAR models.

According to the above described development process, the main concepts of the safety extension are Safety Requirements and Safety Measures together with their ASIL attributes.



- Safety Requirements - In AUTOSAR R4.2.1 clearly distinguishable safety requirements can be defined in AUTOSAR metamodel, thus fulfilling the needs as specified by ISO 26262 parts 4 and 8 (section 4). Safety Requirements may have attributes and relations that are used to specify them in accordance with ISO 26262, like decomposition and refinement. Also by using AUTOSAR Trace, Traceability and allocation of safety requirements and safety measures according to ISO 26262 parts 4, 6 and 8 (section 6) can be described.
- Safety Measures - Safety Measures have a textual description, a unique ID and a type which declares whether it is a safety mechanism (i.e. part of the AUTOSAR implementation) or an external measure (e.g. a review). Furthermore, ASIL attributes according to ISO 26262 can be specified.
- ASIL Attribute Values - In AUTOSAR R4.2.1 safety integrity levels /ASIL can be assigned for each AUTOSAR element including safety requirements and safety measures.

The provision and processing of AUTOSAR models with safety extensions is subject of appropriate tool support. Tools supporting the safety process according to ISO 26262 could be used to provide the safety requirements and the required ASIL attributes. AUTOSAR tools like configuration tools could read these information and add further information like the traces to the safety mechanisms and measures that are part of the final configuration. As the safety extensions are standardized, arbitrary AUTOSAR complaint tools can be used here.

The application of AUTSOAR safety extensions together with appropriate tool support provides several benefits. The need for information exchange in arbitrary formats (mostly with Word and Excel) is reduced and also the time necessary for transformation of this information if it flows across an organization border. Hence the workflow can be organized much more efficient then today. Besides the advantages in the process, there is also an increase in the quality of the safety information, as the traceability is much better to provide, for example for a safety case argumentation. In addition, this explicit traceability in the models offer possibilities for consistency checks.

Authors

Sugandar Swetharanyam

AUTOSAR Expert,
KPIT Technologies GmbH

Dr. Marc Born
Chief Technology Officer
KPIT medini Technologies AG,
Subsidiary of KPIT Technologies GmbH

About KPIT

KPIT Technologies (BSE: 532400, NSE: KPIT), is a fast growing global product engineering and IT consulting partner focused on co-innovating domain intensive technology solutions for automotive & transportation, manufacturing and energy & utilities corporations. KPIT is at the forefront of automotive engineering globally with solutions in the areas of AUTOSAR & in-Vehicle Networks, Body Electronics, Chassis, Safety & Driver Assistance, Functional Safety, Vehicle Diagnostics, Infotainment and Powertrain.

Press Contact:
Stefanie Köhler**,** Tel: +49 89 322 99 66 140, stefanie.koehler@kpit.com, www.kpit.com