Sicherheitserweiterungen für AUTOSAR-Modelle

Funktionale Sicherheit wird zunehmend zu einem bedeutenden Aspekt bei der Entwicklung von softwarebasierten Systemen in der Automobilindustrie, sowohl bei OEMs als auch bei Tier-1 und Tier-n Lieferanten. In diesem Beitrag wird die Lösung für ein allgemeines Problem beschrieben, wenn der Bedarf besteht, zwischen den Organisationen entlang der Lieferkette Sicherheitsinformationen auszutauschen.

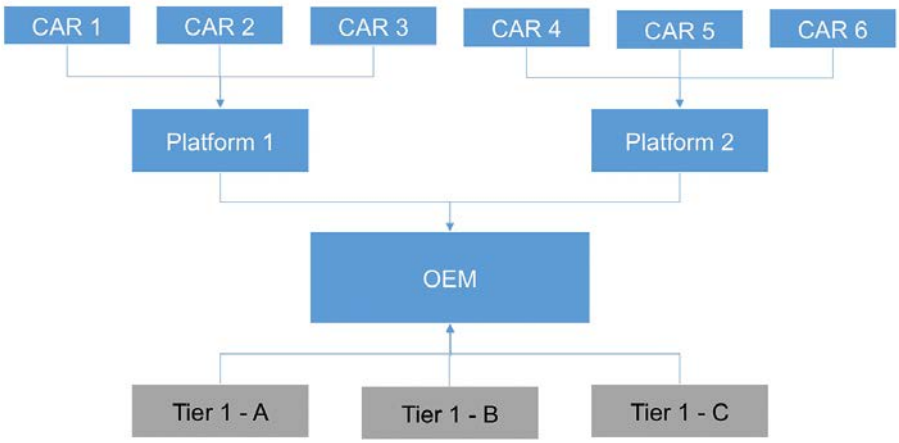

Bild 1: Fahrzeugplattform.

Maßnahmen für funktionale Sicherheit betreffen den gesamten Lebenszyklus des zu entwickelnden Systems (bzw. der zu entwickelnden Komponente) und werden von allen Beteiligten entsprechend ihren jeweiligen Zuständigkeiten durchgeführt. Daher müssen die Arbeitsergebnisse dieser sicherheitsrelevanten Aktivitäten zwischen allen beteiligten Unternehmen ausgetauscht werden. Die Details wie Aufgaben, Zuständigkeiten und Ergebnisse müssen gemäß ISO-Norm 26262 in einem Development Interface Agreement (DIA) festgelegt werden. Die ISO-Norm 26262 schreibt jedoch nicht vor, auf welche Weise diese Informationen ausgetauscht werden sollen (bezüglich der Inhalte, Formate usw.). In der gängigen Praxis führt dies oftmals zu ineffizienten, auf manueller Dokumentationserstellung beruhenden Verfahren und innerhalb der Lieferkette zu duplizierten Informationen sowohl auf Integratoren- als auch Lieferantenseite. Ebenso kann es geschehen, dass wichtige Informationen fehlen, wenn bestimmte Tätigkeiten (wie die Bereitstellung oder Konfiguration von Sicherheitsmechanismen der Basissoftware) ausgeführt werden. Das Ergebnis sind Unstimmigkeiten, unzureichende Rückverfolgbarkeit und Probleme bei der Zusammenstellung der allgemeinen Sicherheitsnachweise.

Andererseits gewährleistet die Verwendung der AUTOSAR-Architektur in Kombination mit der AUTOSAR-Methode und Support-Tools bereits die Nutzung von Standardformaten für den Austausch von Entwicklungsinformationen für alle Unternehmen in der Lieferkette. Unter Verwendung dieser Formate können für die Implementierung von Softwaresystemen und ECUs relevante Informationen auf komfortable Weise ausgetauscht werden. Nachstehend wird aufgezeigt, wie mit den seit Version 4.2.1. im AUTOSAR-Standard enthaltenen Erweiterungen das Problem des Austausches von Informationen zur funktionalen Sicherheit auf elegante Weise gelöst werden kann. Als Beispiel dient die Methode, wie ein OEM die funktionale Sicherheit für eine Fahrzeugplattform unterstützt (Bild 1). Der Prozess könnte sich im Hinblick auf die Tätigkeiten und Arbeitsprodukte für die funktionale Sicherheit aus folgenden, allgemeinen Phasen zusammensetzen:

- **Entwurf und Definition durch den OEM**
  Der OEM erstellt die übergreifenden Konzepte für die Komponenten (Systeme) einer Plattform. Die Ausarbeitung des Konzepts für die funktionale Sicherheit beginnt in der Regel auf der/den Komponentenebene/n einer Fahrzeugplattform, beginnend mit der Definition der Sicherheitsziele sowie der Anforderungen für die verschiedenen Komponenten, Systeme und Subsysteme der Plattform.

Bilder: KPIT Technologies

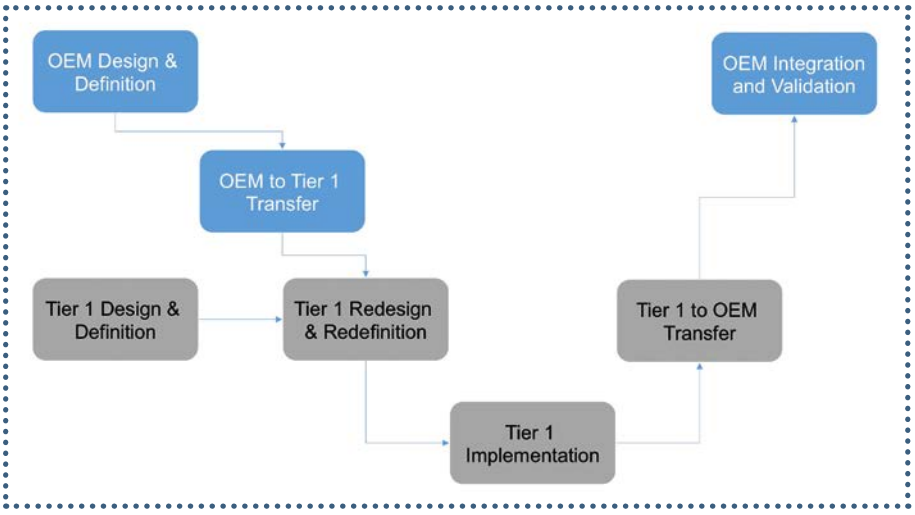

Bild 2: Sicherheitsphase.

- **Transfer vom OEM an Tier-1**
  Die Konzepte für funktionale Sicherheit des OEM werden an Tier-1, bezogen auf dessen spezifische Komponenten, Systeme oder Subsysteme, übermittelt.
- **Entwurf und Definition durch Tier-1**
  Tier-1 könnte vor der Bereitstellung der Sicherheitsziele und Anforderungen durch den OEM oder zeitgleich nach der SEooC-Methode („Safety Element out of Context") bereits selbst ein für sein (Sub-)System spezifisches Sicherheitskonzept erarbeitet haben. Dieser Ansatz ermöglicht eine Sicherheitsimplementierung auf der Grundlage eines hypothetischen Systems.
- **Neuentwurf und Neudefinition durch Tier-1**
  Wenn ein Tier-1 das Konzept für funktionale Sicherheit des OEM erhält, muss es den Sicherheitsanforderungen angepasst werden, denen mit dem bestehenden Sicherheitskonzept bereits entsprochen wurde, und möglicherweise neu entworfen oder umgestaltet werden, um den Anforderungen des OEM zu entsprechen.
- **Implementierung durch Tier-1**
  Um den Sicherheitsanforderungen und Sicherheitszielen zu entsprechen, werden verschiedene Maßnahmen ergriffen bzw. Mechanismen am Subsystem vorgesehen. Auf diese Weise werden die spezifischen Sicherheitsmechanismen auf Subsystem- oder Systemebene durch Tier-1 implementiert und validiert.
- **Transfer von Tier-1 zum OEM**
  Tier-1 übermittelt seine Implementierung nun wieder zurück an den OEM, gemeinsam mit Informationen über die Sicherheitsmaßnahmen oder Sicherheitsmechanismen, die vorgesehen wurden, um den Sicherheitsanforderungen des OEM gerecht zu werden.
- **Integration und Validierung durch den OEM**
  Der OEM sammelt mehrere Implementierungen zur Einbindung der Sicherheitskonzepte in seinem System und validiert das System auf der Ebene der Fahrzeugplattform. Dies kann als schrittweiser Prozess erfolgen.

Ein ähnliches Verfahren gilt für Unternehmen auf niedrigeren Ebenen der Lieferkette, die zur Arbeit von Tier-1 beitragen. Die oben beschriebenen Probleme mit dem Transfer sicherheitsrelevanter Informationen treten hauptsächlich in zwei Phasen auf, in denen diese Informationen zwischen Unternehmen ausgetauscht werden (Bild 2):

- **Transfer vom OEM zu Tier-1**: Die zu übertragenden Informationen beinhalten die relevanten Teile des Konzepts für funktionale Sicherheit, also die Sicherheitsziele und -anforderungen, Sicherheitsmaßnahmen für die Architektur sowie Informationen über die Zuordnung der Sicherheitsanforderungen zu bestimmten Architekturelementen.
- **Transfer von Tier-1 zum OEM:** Hier sind die Informationen über die implementierten Sicherheitsmechanismen und -maßnahmen sowie die Zuordnungen zwischen den Sicherheitsanforderungen und diesen Mechanismen von Bedeutung.

Wie anfangs beschrieben, kommuniziert der OEM potenziell mit mehreren Tier-1-Lieferanten und diese müssen wiederum mit mehreren Tier-n-Lieferanten kommunizieren. Ein standardisiertes Austauschformat für Sicherheitsinformationen erleichtert die Kommunikation zwischen den Unternehmen und gewährleistet, dass kostenintensive fehleranfällige Nacharbeit oder die Übersetzung sicherheitsrelevanter Informationen vermieden werden. Die AUTOSAR-Sicherheitserweiterungen für AUTOSAR-gestützte Entwicklungen, verfügbar ab Release 4.2.1, stellen ein solches Austauschformat bereit. Zusätzlich zur Bereitstellung des Austauschformats »

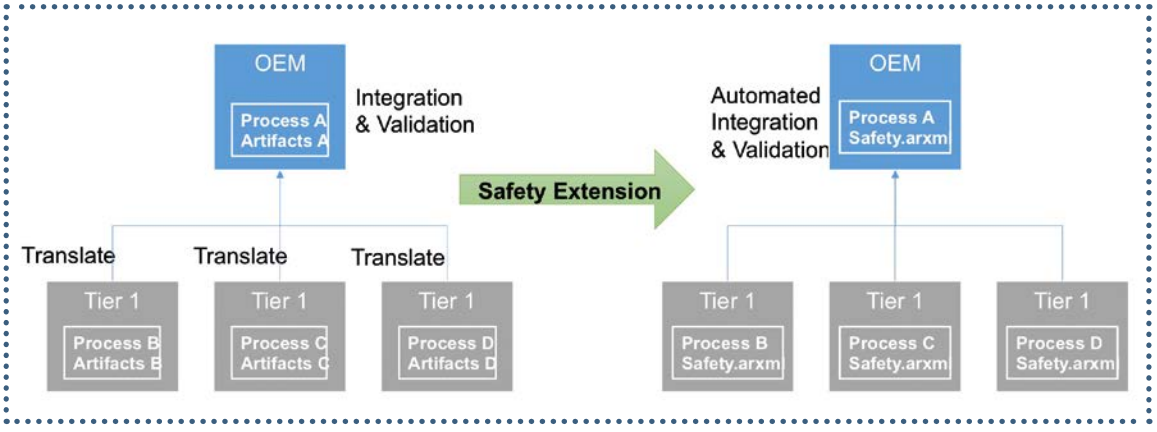

Bild 3: AUTOSAR-Sicherheitserweiterungen.

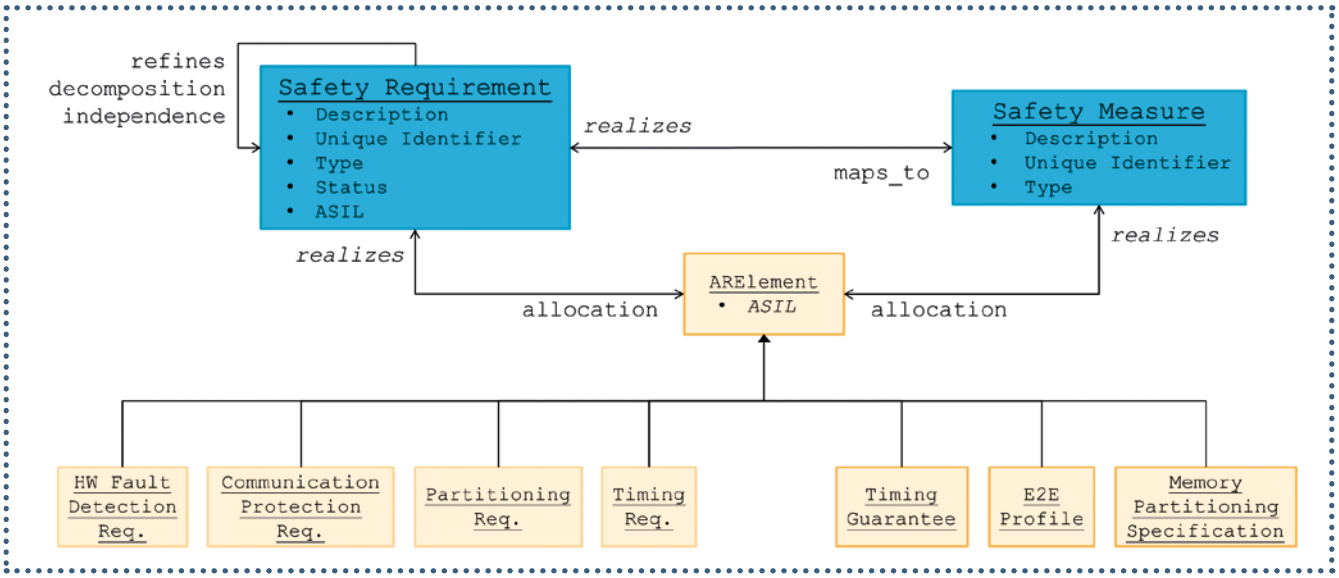

Bild 4: Hauptkonzepte der Sicherheitserweiterungen.

wurde die AUTOSAR-Methode erweitert und beinhaltet nun auch Verfahren für die Erstellung der sicherheitsrelevanten Elemente (Bild 3).

Das Ziel der Sicherheitserweiterungen besteht darin, die AUTOSAR-XML-Darstellung (.arxml) als das Standardformat zu etablieren, in dem Sicherheitsinformationen präsentiert und ausgetauscht werden. In der aktuellen Version, die Teil von AUTOSAR 4.2.1 ist, wurde ein Ansatz verwendet, der das bestehende AUTOSAR-Metamodell nicht verändert. Der neue Standard definiert aber, wie die Informationen nur unter Einsatz bestehender, allgemeiner Konzepte des AUTOSAR-Metamodells durch Verwendung spezifischer, standardisierter Tags und Inhalte bereitgestellt werden. Die Idee besteht darin, dass zusätzlich zu den herkömmlichen AUTOSAR-Modellen, die zwischen Unternehmen innerhalb der Lieferkette ausgetauscht werden, Sicherheitserweiterungen bereitgestellt werden, die das Modell um neue Elemente erweitern und sich gleichzeitig auf bestehende Elemente beziehen. Die Sicherheitserweiterungen können daher als reine Ergänzungen genutzt werden, das bedeutet, sie wirken sich auf bestehende AUTOSAR-Modelle nicht aus.

Sicherheitsanforderungen und Sicherheitsmaßnahmen

Gemäß dem vorstehend genannten Entwicklungsprozess sind die Hauptkonzepte der Sicherheitserweiterungen die Sicherheitsanforderungen und Sicherheitsmaßnahmen, gemeinsam mit deren ASIL-Attributen (Bild 4).

- **Sicherheitsanforderungen:** In AUTOSAR R4.2.1 können klar unterscheidbare Sicherheitsanforderungen im AUTOSAR-Metamodell definiert werden, sodass die Vorgaben gemäß ISO 26262 Teil 4 und 8 (Abschnitt 4) erfüllt werden. Sicherheitsanforderungen können Attribute und Relationen haben, die verwendet werden, um sie gemäß ISO 26262 zu spezifizieren, wie z. B. Dekomposition oder Verfeinerung. Mit AUTOSAR-Trace können außerdem die Rückverfolgbarkeit und die Allokation von Sicherheitsanforderungen und Sicherheitsmaßnahmen gemäß ISO 26262 Teil 4, 6 und 8 (Abschnitt 6) beschrieben werden.
- **Sicherheitsmaßnahmen:** Sicherheitsmaßnahmen setzen sich aus einer Beschreibung in Textform, einer eindeutigen ID und einer Typangabe zusammen, die definiert, ob es sich um einen Sicherheitsmechanismus (z. B. Teil der AUTOSAR-Implementierung) oder eine externe Maßnahme handelt (z. B. einen Review). Außerdem können ASIL-Attribute gemäß ISO 26262 festgelegt werden.
- **ASIL-Attributwerte:** In AUTOSAR R4.2.1 können jedem AUTOSAR-Element Sicherheits-Integritätslevels / ASIL zugewiesen werden, einschließlich Sicherheitsanforderungen und Sicherheitsmaßnahmen.

Fazit

Die Nutzung der AUTOSAR-Sicherheitserweiterungen in Kombination mit angemessener Tool-Unterstützung bietet diverse Vorzüge. Die Notwendigkeit, Informationen in beliebigen Formaten (in der Regel Word und Excel) auszutauschen, wird reduziert, ebenso wie die Notwendigkeit, diese Daten zu konvertieren, wenn sie unternehmensübergreifend transferiert werden. Folglich können die Arbeitsabläufe wesentlich effizienter organisiert werden als zum aktuellen Zeitpunkt. Neben den Vorteilen im Prozess wird auch die Qualität der Sicherheitsinformationen gesteigert, da ihre Rückverfolgbarkeit optimiert ist, beispielsweise für die Argumentation zur Erlangung von Sicherheitsnachweisen. Außerdem ermöglicht diese explizite Rückverfolgbarkeit innerhalb der Modelle die Durchführung von Konsistenzprüfungen. ■ (oe)

» www.kpit.com

Sugandar Swetharanyam ist AUTOSAR-Experte bei der KPIT Technologies GmbH.

Dr. Marc Born ist Chief Technology Officer bei KPIT medini Technologies, einer Tochterfirma der KPIT Technologies GmbH.