Herausforderungen und Erfahrungen eines OEM bei der Gestaltung sicherheitsgerechter Prozesse

Dr. Axel Dold[1], Dr. Mario Trapp[2]

axel.dold@daimlerchrysler.com
mario.trapp@iese.fraunhofer.de

Abstract: In diesem Beitrag werden die Herausforderung erörtert, die sich aus dem neuen Sicherheitsstandard (ISO/WD 26262) für die Automobilindustrie ergeben und ein praktikables Vorgehen vorgestellt, wie die Anforderungen der Norm effizient umzusetzen sind.

1 Motivation und Ausgangssituation

Der Anteil eingebetteter Softwaresysteme im Automobil ist innerhalb weniger Jahrzehnte rasant gestiegen. Heute sind nahezu alle Funktionen im Automobil mehr oder weniger direkt durch Software kontrolliert oder bestimmt. Studien prognostizieren, dass 70-90% aller zukünftigen Innovationen im Automobilbereich erst durch eingebettete Software ermöglicht werden [Et05], [Me03]. Eingebettete Software ist die Schlüsselfunktion zur Automatisierung mechatronischer und eingebetteter Systeme geworden und gleichzeitig eine kritische Komponente des Produkterfolgs. Allerdings nimmt mit der Zunahme des SW-Anteils im Fahrzeug auch die Anzahl der Software-Fehler in Steuergeräten zu, die zu Ausfällen der Automobilelektronik führen. Mehr als 50% aller Fahrzeugausfälle basieren mittlerweile auf Elektronik- und Softwarefehlern.

Viele Funktionen im Fahrzeug sind sicherheitsbezogen bzw. sicherheitskritisch wie etwa elektronisch geregelte Bremssysteme, Fahrer-Assistenzsysteme (z.B. Abstandsregelautomat) oder auch aktive und passive Sicherheitssysteme. Das Thema Produktsicherheit gewinnt damit an Brisanz. Die Anwendung von Sicherheitsnomen wie z.B. IEC 61508 [IEC] bei der System- bzw. Funktionsentwicklung wird zum Stand der Technik und ist somit für OEM's und Zulieferer bindend und zudem im Sinne der Produkt- bzw. Produzentenhaftung auch aus Beweislastgründen eminent [AF04]. Die Beweislast im Schadensfall obliegt dem Hersteller. Ein Schadensfall kann neben einem Imageschaden vor allem auch juristische Konsequenzen nach sich ziehen.

[1]DaimlerChrysler AG, Group Research & Advanced Engineering, G012 (W50) - GR/ESP, 71059 Sindelfingen
[2] Department "Component Engineering", Fraunhofer IESE, Fraunhofer-Platz 1, 67663 Kaiserslautern

Da es sich bei der IEC 61508 um einen generischen Standard handelt, ist beim Verband der Automobilindustrie (VDA) ein Arbeitskreis (FAKRA) eingerichtet worden, der die Aufgabe hat, ihn auf die spezifischen Rahmenbedingungen und Bedürfnisse der Autoindustrie zuzuschneiden, so wie dies in anderen Industrien wie z.B. bei der Bahnindustrie bereits geschehen ist. Dieser Standard liegt derzeit in Form eines Working Drafts (ISO/WD 26262) vor [ISO] und wird damit zukünftig (voraussichtlich ab 2011) zum relevanten Standard für die Automobilindustrie. Aus Sicht der OEM's und der Zulieferer müssen die Handlungsbedarfe, die der neue Standard nach sich zieht, identifiziert und effizient umgesetzt werden.

In diesem Beitrag werden die Herausforderungen diskutiert, die sich aus dem neuen Sicherheitsstandard für die Automobilindustrie ergeben. Des Weiteren wird ein Vorgehen skizziert, wie ein Norm-konformer Entwicklungsprozess in der Praxis zu implementieren ist. Zielsetzung ist hierbei eine auf der existierenden Prozesslandschaft möglichst effiziente Umsetzung der Anforderungen. Kapitel 2 dokumentiert die Herausforderungen und gibt Antworten auf die wesentlichen Fragestellungen auf Basis des aktuellen Stands in der Praxis. Im Kapitel 3 wird ein konkretes Vorgehen bei DaimlerChrysler skizziert.

2 Herausforderungen und Stand der Praxis in der Automobilindustrie

Der neue automobilspezifische Standard zur Funktionssicherheit (ISO/WD 26262) beinhaltet im Wesentlichen organisatorische und technische Anforderungen. Organisatorische Anforderungen umfassen hierbei (1) Anforderungen an den Entwicklungsprozess (System- und Softwareebene), (2) Anforderungen an das Management und die Beurteilung der funktionalen Sicherheit und (3) Anforderungen an unterstützende und begleitende Prozesse. Technische Anforderungen fokussieren auf die Sicherheitsintegrität der Hardware. Für den Bereich der Softwareentwicklung macht der Standard Vorschläge zur Anwendung von Techniken und Methoden während der Entwicklung und Qualitätssicherung in Abhängigkeit des Sicherheitsintegritätslevels.

Bei der Analyse der organisatorischen Anforderungen in der neuen Norm ergeben sich teilweise große Übereinstimmung mit Anforderungen aus gängigen Prozessreifegrad-modellen wie CMMI [CMMI] oder SPICE [SPICE]. Vor dem Hintergrund derzeitiger Prozessreifungsinitiativen bei vielen Automobilfirmen, die darauf zielen in systematischer Weise die internen Prozesse schrittweise auf einen angemessenen Reifegrad zu bringen, stellt sich hierbei die Frage, welchen Zusammenhang es zwischen Prozessreifegrad und den Anforderungen aus der Sicherheitsnorm gibt.

Obgleich die Norm für die Automotive Domäne definiert wurde, lässt sie viele Freiräume und Interpretationsmöglichkeiten in der Auswahl der Techniken und Methoden. Das größte Problem besteht dabei darin, die Abhängigkeiten zwischen den

unterschiedlichen Anforderungen zu erfassen. Diese Abhängigkeiten entstehen zum einen aus Vorgaben der Norm, die sich allerdings häufig nur in Bemerkungen äußern. Zum anderen gibt es aber vor allem auch fachliche Abhängigkeiten. Beispielsweise erfordert eine formale Verifikation, dass eine formale Modellierung bzw. Spezifikation vorliegt. Zudem sind viele Methoden auch nicht im jeweiligen Projektumfeld bewährt und machen aufgrund der spezifischen Randbedingungen keinen Sinn. Eine große Herausforderung besteht also darin, innerhalb des von der Norm gegebenen Spielraums eine auf den Unternehmens- und den Projektkontext zugeschnittene Lösung zu erarbeiten. Es ist also eine geeignete Auswahl von Kombinationen der Techniken und eine Anpassung an den jeweiligen Projektkontext vonnöten.

Zusammenfassend ergeben sich die folgenden Herausforderungen aus der Praxis an Entwicklungsprozesse für sicherheitsbezogene Systeme: (1) Welche Änderungen sind für die Umsetzung eines IEC 61508 bzw. ISO/WD 26262 konformen Prozesses erforderlich? (2) Welche Beziehungen bestehen zwischen dem Prozessreifegrad (nach SPICE oder CMMI) und Entwicklungsprozessen für sicherheitsbezogene Systeme? (3) Wie sieht in der Praxis ein Norm-konformer Prozess konkret aus, d.h. wie leitet man einen konkreten Prozess aus den Anforderungen der Norm ab und welche Techniken/Methoden sollen in den jeweiligen Phasen angewendet werden? Welche Artefakte (Dokumente, Modelle, Code etc.) müssen erzeugt werden?

Grundvoraussetzung für einen ISO 26262-konformen Entwicklungsprozess sind Entwicklungs- und unterstützende Prozesse mindestens auf CMMI bzw. SPICE-Level 2. Diese Aussage wird durch mehrere Publikationen gestützt. In [AFE04] werden drei Schritte zu Erreichung eines Norm-konformen Standardprozesses vorgeschlagen. Erstens soll der Reifegrad der (gelebten) Prozesse bestimmt werden. Zweitens sollen diese ggf. verbessert werden um zumindest einen Reifegrad vergleichbar zu CMMI 2 zu erreichen. Drittens sollen die speziellen Sicherheitsaktivitäten wie beispielsweise die Gefahren- und Risikoanalyse in den Prozess integriert werden. Prozesse mit mindestens der Reifegradstufe 2 stellen eine gute Grundlage für einen Norm-konformen Prozess dar. Allerdings ist dies eine notwendige aber nicht hinreichende Bedingung für die Erreichung eines SIL bzw. ASIL's [Ja04] [Am05] [AFE04].

3 Vorgehen bei der Umsetzung der Norm-Anforderungen

Vor dem Hintergrund der Zielsetzung, Engineering- und Supportprozesse zu etablieren, die sowohl den Anforderungen der ISO/WD 26262 als auch den individuellen Rahmenbedingungen in den Baureihenprojekten entsprechen, ist ein Entwicklungs-leitfaden ausgestaltet und in Pilotprojekten evaluiert worden.

Im ersten Schritt wurde der betrachtete Entwicklungskontext bei DaimlerChrysler erfasst. Dazu wurde anhand eines aktuellen Engineering-Prozesses für die Entwicklung einer bestimmten Fahrzeugbaureihe untersucht und überprüft, welche Methoden, Techniken und Werkzeuge zurzeit im Rahmen des Entwicklungskontextes genutzt werden oder in Zukunft eingeführt werden können. Dies lieferte eine erste Auswahl an möglichen Techniken und Methoden.

Im nächsten Schritt wurde das ISO/WD-26262 Phasenmodell (Sicherheitslebenszyklus) mit dem bestehenden Engineering-Prozess abgeglichen, um eine Zuordnung der Forderungen der Norm an die einzelnen Phasen des bestehenden Engineering-Prozesses zu ermöglichen. Darauf basierend lässt sich dann festlegen, welche Techniken und Methoden in welchen Phasen des Engineering-Prozesses unter welchen Bedingungen zum Einsatz kommen müssen/sollen. Daneben wurden Zusammenhänge und Abhängigkeiten in der Norm analysiert und die erlaubten Prozessvarianten ermittelt. Des Weiteren sind die Randbedingungen der internen Entwicklung beispielsweise an das Qualitätsmanagement mit zu berücksichtigen.

Als Ergebnis entstand ein initialer Norm-konformer Prozessleitfaden, der die verpflichtenden, optionalen und variablen Phasen im Engineering-Prozess darstellt. Für jede Entwicklungsphase (Anforderungsdefinition, Design, Test etc.) wird festlegt, welche Techniken / Methoden angewendet werden sollen und welche Artefakte (Dokumente, Modelle, Code etc.) erzeugt werden müssen. Dabei ist der Leitfaden so gestaltet, dass er einen Spielraum zur Anpassung an unterschiedliche Projekte und unterschiedliche Entwicklungstiefen (von Systemlieferantenbeziehungen bis hin zur Eigenentwicklung von Code), sowie an unterschiedliche Zulieferer ermöglicht. Der Leitfaden soll zum einen die Ausgangsbasis für eine Projektunterstützung sein, die es Projektleitern ermöglicht, für ihren Projektkontext einen normkonformen Engineering-Prozess in Abhängigkeit der Sicherheitsintegritätsstufe (ASIL) zu initiieren. Zweitens soll der Leitfaden als Analysewerkzeug dienen, bestehende Engineering-Prozesse im Hinblick auf ihre Konformität zur ISO/WD 26262 zu bewerten. Drittens fungiert der Leitfaden als Instrument zur Planung und zum Controlling der sicherheitsrelevanten Aktivitäten. Anhand des Status bzw. der Ausführung der sicherheitsrelevanten Aktivitäten lässt sich der *Safety Case* als Basis für die abschließende Beurteilung der funktionalen Sicherheit erstellen.

Auf Basis dieses Leitfadens wurde bereits eine Bestandsaufnahme in mehreren Pilotprojekten hinsichtlich ihrer Norm-Konformität durchgeführt. Maßnahmen aus der Bestandsaufnahme werden derzeit umgesetzt. Detaillierte Erfahrungen sind momentan noch nicht berichtbar. Prinzipiell muss man aber bei den Ergebnissen zwischen den allgemeinen Vorgaben der Norm an die Entwicklungs- und Qualitätssicherungsprozesse einerseits und die Anforderungen an das Safety-Management andererseits unterscheiden. Viele Anforderungen der Norm an Entwicklungs- und QS-Prozesse sind heute bereits in vorhanden internen Qualitätsrichtlinien abgebildet. Die Prozesse sind entsprechend den zusätzlichen Normanforderungen anzupassen: betrachtet man beispielsweise das Änderungsmanagement, so müssen alle Änderungen zukünftig bzgl. ihrer Auswirkung auf die funktionale Sicherheit analysiert werden. Im Rahmen des Requirementsmanagements müssen Sicherheitsanforderungen explizit als solche im Lastenheft gekennzeichnet werden und Design-Guidelines für die modellbasierte Entwicklung erfordern eine Anpassung an die spezifischen Normanforderungen.

Ein anderes Bild ergibt sich im Bereich der Anforderungen, die gezielt auf Safety ausgerichtet sind. Dies beinhaltet zum einen die unter dem Begriff Safety-Management subsumierten Aufgaben wie beispielsweise die Einführung eines Safety-Plans. Zum anderen stellt auch die Einführung durchgängiger Gefährdungsanalysen eine Herausforderung dar. Dies gilt insbesondere, da entsprechende Verfahren wie FMEA oder FTA auch für die Softwareentwicklung gefordert werden.

4 Fazit

Die neue Sicherheitsnorm für den Automobilbereich stellt derzeit eine große Herausforderung für die Automobilindustrie dar. Es gilt die Anforderungen der Norm geeignet zu interpretieren und für das eigene Umfeld handhabbar zu machen, d.h. unter Berücksichtigung der internen Gegebenheiten (ökonomisch) effizient umzusetzen. Dabei müssen u.a. zusätzliche Anforderungen an Entwicklungs- und Supportprozesse berücksichtigt werden. Grundvoraussetzung eines norm-konformen Entwicklungsprozesses sind Entwicklungs- und Supportprozesse mindestens auf CMMI bzw. SPICE-Level 2. Das Thema „Sicherheit“ muss somit integraler Bestandteil laufender Prozessverbesserungs-initiativen sein, d.h. sicherheitsbezogene Aktivitäten sind dabei geeignet in die Prozesslandschaft (Entwicklungs- und Supportprozesse) zu integrieren. Solche Aktivitäten umfassen etwa das Management der funktionalen Sicherheit, z.B. durch einen Sicherheitsmanager im Projekt, die Auswahl adäquater Techniken in jeder Entwicklungsphase in Abhängigkeit des Sicherheitsintegritätslevels, die Validierung und das Assessment der funktionalen Sicherheit.

Literaturverzeichnis

[AF04] Amsler, K-J.; Fetzer J.: Definition von Entwicklungsprozessen unter spezieller Betrachtung sicherheitskritischer Aspekte und der Produzentenhaftung. 5. Euroforum-Konferenz SW im Automobil 2004.

[AFE04] Amsler, K-J.; Fetzer J.; Erben M.F.: Sicherheitsgerechte Entwicklungsprozesse - alles neu geregelt? Tagungsband „Aktive Sicherheit durch Fahrerassistenz“, 2004.

[Am05] Amsler K-J. et.al.: Über Prozessreife zur Sicherheitsintegrität. VDI Berichte Nr. 1907, 2005.

[CMMI] Capability Maturity Model Integration (CMMI): www.sei.cmu.edu/cmmi.

[Et05] Etter, A. et.al.: Auto Electronics: Getting a grip on embedded systems. McKinsey’s embedded systems initiative, November 2005.

[IEC] IEC61508 „Functional safety of electrical/electronic/programmable electronic safety related systems”, www.iec.ch.

[ISO] ISO/WD 26262 “Road vehicles – Functional safety” (Working Draft), to appear..

[Ja04] Jacobs, M. et.al.: Electronic Architecture and System Engineering for Integrated Safety Systems – State Of The Art. EASIS-Report, Deliverable D.0.1.2. EASIS Consortium, 2004.

[Me03] Mercer Management Consulting: Automobil-Elektronik, Problemfelder, Herausforderungen und Lösungsansätze, Vorstudie, Aug. 2003.

[SZ02] Schäuffele, J.; Zurawka T.: Automotive Software Engineering: Stand der Technik, Perspektiven und Herausforderungen. Automotive Electronics I/2002, ETAS GmbH.

[SPICE] SPICE: www.isospice.com.