Wie Automotive SPICE von ISO 26262 profitiert:

Upside down

Automotive SPICE wirkt als Prozessbewertung auf Projekt- und Organisationsebene; ISO 26262 gewährleistet die funktionale Sicherheit eines E/E-Systems im Auto. Wie können nun beide Standards voneinander profitieren? Der Artikel klärt, ob eine Prozessverbesserung nach ISO 26262 helfen kann, die Anforderungen von SPICE nachhaltig umzusetzen.

Von Timo Karasch

(Bild: Shersor – Fotolia)

Um nach dem aktuellen Stand von Wissenschaft und Technik zu entwickeln, werden auch in der Automobilindustrie Prozesse gestaltet und laufend überarbeitet. Lange Zeit konzentrierte sich die Industrie darauf, Prozesse zu etablieren, die den Anforderungen unterschiedlicher Reifegradmodelle wie SPICE genügen. Ziel sollte es sein, Transparenz in der Entwicklung zu schaffen und somit nachvollziehbare und qualitativ bessere Ergebnisse zu erzielen. Nicht selten stand dabei die Frage im Raum, inwiefern diese Standards bei der Qualitätssteigerung oder gar bei der Kostensenkung helfen können. Dennoch, betrachtet man die Ergebnisse einiger SPICE-Assessments aus den letzten Monaten, lässt die Nachhaltigkeit der initiierten Prozessverbesserung deutlich zu wünschen übrig.

Gerade jetzt gewinnt ein weiterer Standard an Bedeutung, dessen Intention deutlich schärfer formuliert ist und zudem auf den Ergebnissen der bisherigen Bemühungen aufbauen soll: ISO 26262. Um die funktionale Sicherheit bei der Entwicklung von elektrischen und elektronischen Systemen zu gewährleisten, werden hierin Anforderungen gestellt und Methoden beschrieben, die auf etablierten Entwicklungsprozessen im Unternehmen aufbauen sollen.

Viele Veröffentlichungen befassen sich mit der offensichtlichen Tatsache, dass SPICE eine gute Basis für die Etablierung von ISO 26262 darstellt. Doch kann eine Prozessverbesserung gemäß ISO 26262 auch dabei helfen, die Anforderungen von SPICE nachhaltig im Unternehmen zu verankern?

Ergebnisse aus SPICE-Assessments

Prozessverbesserungen gemäß SPICE werden nicht nachhaltig umgesetzt. Warum ist das so? Welche Probleme gibt es bei der Umsetzung der SPICE-Anforderungen?

Die Ergebnisse einiger SPICE-Assessments geben einen Einblick. In diesen Assessments wurden Indikatoren, die sogenannten „Base Practices“ und „Generic Practices“, nach einem definierten Schema bewertet. In die Analyse flossen alle Indikatoren ein, die als unzureichend (P – partially achieved) oder als gar nicht erfüllt (N – not achieved) eingestuft wurden. Das folgende Histogramm (**Bild 1**) beschränkt sich auf die 13 Indikatoren, die zu 80 Prozent der Abweichungen geführt haben.

Kategorisierung der Ergebnisse

Welche Maßnahmen wurden formuliert, um diese Abweichungen abzustellen? Offensichtlich hat man sich dabei wenig Mühe gegeben. Ein Beispiel hierzu zeigt **Tabelle 1**. Die Maßnahme passt zwar genau zur festgestellten Abweichung, jedoch ist sie gleichermaßen trivial wie nutzlos. Dabei kann schon eine ganz simple Methodik, wie eine „5-Why“ (**Tabelle 2**), helfen. Wenige Schritte genügen also, um zu erkennen, dass unklare oder fehlende Verantwortlichkeiten zu dieser Abweichung geführt haben. Die Ursachen für diese und für die anderen zwölf Abweichungen lassen sich auf drei Kernaussagen reduzieren:

Kernaussage 1: Den Projektteilnehmern sind die Verantwortlichkeiten im Projekt unklar.

Kernaussage 2: Sie wissen nicht genau, wie die Aktivitäten im Projekt umgesetzt werden können.

Kernaussage 3: Die Projektteilnehmer sehen nicht, inwiefern ihnen diese Aktivitäten helfen.

Wie kann ISO 26262 an dieser Stelle helfen? Die Norm fordert: „Etabliere eine Sicherheitskultur im Unternehmen.“ Die Inhalte einer solchen Kultur

Abweichung	Maßnahme
Qualitätssicherung ist im Projekt nicht etabliert.	Qualitätssicherung im Projekt etablieren

Tabelle 1. Beispiel einer nutzlosen Maßnahme (Quelle: Method Park)

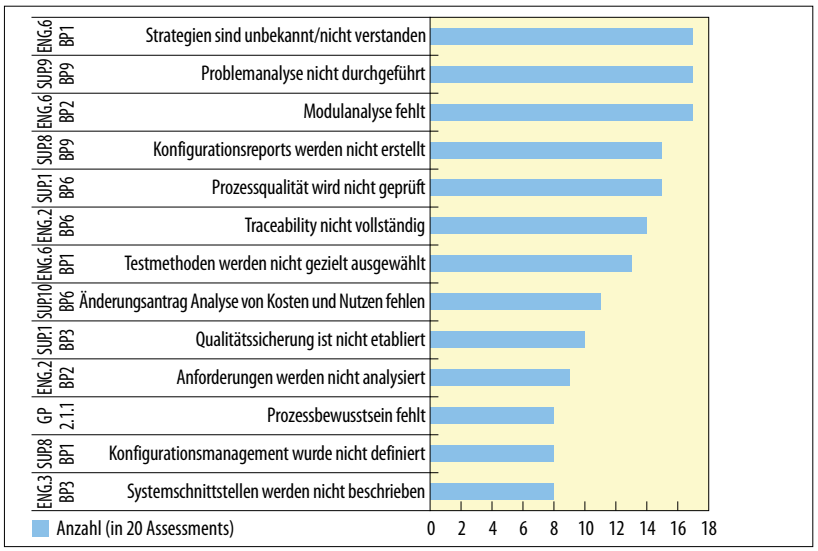

Bild 1. Das Histogramm zeigt die 13 größten Abweichungen der SPICE-Assessments. (Quelle: Method Park)

lassen sich auf drei Grundpfeiler reduzieren, nämlich Verantwortung, Kenntnis und Bewusstsein (**Bild 2**).

Lösungsidee

Startpunkt ist die Etablierung einer Sicherheitskultur im Unternehmen, wobei man sich jedoch nicht ausschließlich auf das Thema funktionale Sicherheit beschränkt, sondern diese auf eine Prozesskultur erweitert (**Tabelle 3**).

Diese Anforderungen unterstützen sowohl bei der Bearbeitung der Abweichungen als auch bei der Umsetzung der höheren Reifegradstufen in SPICE. Sie helfen vor allem dabei, festzulegen, wer (Kernaussage 1) Aktivitäten fordert und teilweise auch warum (Kernaussage 3) Aktivitäten notwendig sind.

Lösungsvorschläge

Zu den folgenden Punkten in Hinsicht auf Kernaussage 1 sollten auf Basis der Prozesskultur ausreichend Ideen gesammelt werden:

Strategien sind unbekannt oder nicht verstanden

Lösungsvorschlag: Der jeweilige Verantwortliche (PC_7) beschreibt rudimentär, welche Aktivitäten und Dokumente das jeweilige Themengebiet umfasst (PC_1, PC_2). Dabei besteht seine Arbeit unter anderem aus dem Sammeln von Informationen bei erfahrenen Mitarbeitern im Projekt. Erfahrungen aus dem Vorgängerprojekt werden bei der Überarbeitung der Strategie berücksichtigt (PC_6).

Qualitätssicherung ist nicht etabliert, Konfigurationsmanagement wurde nicht definiert

Systemschnittstellen werden nicht beschrieben

Als Nächstes folgt ein Vorschlag, wie Abweichungen zur Kernaussage 2 auf Basis der Anforderungen aus ISO 26262 angegangen werden können:

Abweichung	Qualitätssicherung (QS) ist im Projekt nicht etabliert.
Warum wurden keine QS-Aktivitäten im Projekt durchgeführt?	Weil kein Plan erstellt wurde.
Warum wurde kein Plan hierzu erstellt?	Weil man nicht wusste, welche Maßnahmen hierin beschrieben werden sollen.
Warum wusste man das nicht?	Weil es keine Beispiele für sinnvolle Maßnahmen gab.
Warum hatte man keine Beispiele?	Weil niemand diese Aufgabe bislang wahrgenommen hatte.
Warum wurde diese Aufgabe nicht wahrgenommen?	Weil hierfür kein Verantwortlicher bestimmt wurde.
Maßnahme	Ein Verantwortlicher für die Auswahl möglicher QS-Maßnahmen muss definiert werden. Auf Basis dieser Definition kann im Projekt künftig die Planung der Maßnahmen erfolgen.

Tabelle 2. Analyse von Abweichungen mit der 5-Why-Methode (Quelle: Method Park)

Nummer	Anforderung	auf Basis von ISO 26262-2
PC_1	Die Organisation soll eine Prozesskultur erstellen, pflegen und etablieren, die eine effektive und effiziente Erreichung der Prozess Ergebnisse ermöglicht.	5.4.2.1
PC_2	Die Organisation soll organisationsspezifische Regeln und Prozesse einführen, nutzen und aufrechterhalten, die den Anforderungen des Stands von Wissenschaft und Technik genügen.	5.4.2.2
PC_3	Die Organisation soll einen Prozess einführen, nutzen und aufrechterhalten, der es den Projekten ermöglicht, Abweichungen in der Qualität frühzeitig zu entdecken und dies an alle erforderliche Personen zu berichten.	5.4.2.3
PC_4	Während des Projekt- bzw. Produkt-Lebenszyklus soll die Organisation sicherstellen, dass alle erforderlichen Prozessaktivitäten (inkl. Management und Support) sowie alle erforderlichen Arbeitsergebnisse geplant und ausgeführt werden.	5.4.2.5
PC_5	Die Organisation soll ausreichende Ressourcen (personell und materiell) bereitstellen, um die Erreichung der Prozessergebnisse sicherzustellen.	5.4.2.6
PC_6	Die Organisation soll einen Prozess zur ständigen Verbesserung einführen, nutzen und aufrechterhalten, der auf der folgenden Grundlage arbeitet: – Erfahrung aus der Durchführung der Projektaktivitäten werden genutzt. – Ergebnisse aus SPICE-Assessments werden herangezogen und analysiert.	5.4.2.7
PC_7	Die Organisation stellt sicher, dass Verantwortlichkeiten definiert und diese Personen mit genügend Kenntnis und Autorität ausgestattet sind, um ihre Aufgaben wahrzunehmen.	5.4.2.8

Tabelle 3. Anforderungen an eine Prozesskultur (Quelle: Method Park)

Modulanalyse fehlt

In SPICE wird die Analyse, anschließend die Kategorisierung und Priorisierung der erzeugten Units oder Module erwartet. Eine Begründung oder nützliche Beispiele hierfür werden jedoch nicht gegeben.

ISO 26262 lässt sich entnehmen, dass Erstellung, Analyse der Funktion und Test durch mehrere Methoden möglich sind. Dafür werden die entsprechenden Tabellen bereitgestellt. Mit dem ASIL steigen auch Anforderungen und Aufwand für diese Tätigkeiten. Daher ist eine Kategorisierung zur Festlegung der erforderlichen Methoden für Erstellung, Analyse der Funktion und Test sinnvoll.

Mögliche Analyseergebnisse können somit sein: ASIL-Einstufung, besitzt Schnittstellen zu sicherheitskritischen Modulen (Fehleranalyse), Fehleranfälligkeit, Neuheitsgrad etc.

Ähnlich lässt sich mit den anderen Aussagen dieser Kategorie verfahren.

Zuletzt bleiben noch Abweichungen zur Kernaussage 3, die sich nicht direkt auf Anforderungen beziehen lassen. Eine Begründung, warum eine Aktivität oder ein Arbeitsergebnis erforderlich oder gar hilfreich sein könnte, lässt sich in einer Prozessbeschreibung ohnehin nicht ausreichend darlegen. Vielmehr sind hier geeignete Schulungen zum Prozess und den damit verbundenen Aktivitäten sowie eine Betreuung bei der erstmaligen Umsetzung im Projekt erforderlich. Weil es jedoch auch um die Frage geht, welche Probleme der Mitarbeiter hierdurch eventuell gelöst werden können, lassen sich Erfahrungen und Risiken aus ISO 26262 nutzen.

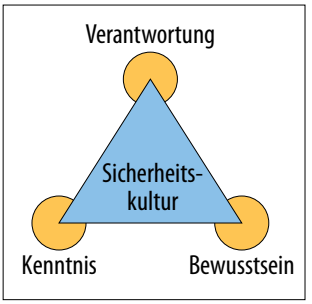

Bild 2. Die Grundpfeiler der Safety Culture bilden die Grundlage für eine neue Lösungsidee. (Quelle: Method Park)

Prozessqualität wird nicht geprüft (Lösungsvorschlag zur Kategorie 3)

Eine Prüfung der Durchführung aller Prozessaktivitäten und ein kritisches Hinterfragen der Eignung dieser ermöglicht es, Abweichungen in der Transparenz und Rückverfolgbarkeit der Ergebnisse frühzeitig sicherzustellen. Sie ist also weniger als Kontrolle, sondern vielmehr als Hilfestellung für die Entwickler zu verstehen.

In ISO 26262 wird verdeutlicht, dass ein Sicherheitsaudit zur Sicherstellung der Durchführung aller Sicherheitsaktivitäten und Erstellung aller erforderlichen Dokumente regelmäßig im Projekt geschehen sollte. Ein solches „Confirmation Measure" soll dabei helfen, Abweichungen frühzeitig zu erkennen, damit diese nicht erst dann identifiziert werden, wenn die Freigabe des Produkts anliegt.

Die vorgestellten Lösungsansätze sind selbstverständlich nur Vorschläge. Um die Umsetzbarkeit in einem Unternehmen zu gewährleisten, sind Anpassungen an spezielle Bedürfnisse erforderlich. Bei der Umsetzung der Verbesserungen helfen zwei grundlegenden Vorschläge:

„Management Commitment" einholen.

Eine detailliertere Analyse der Abweichungen und eine Erweiterung der Anforderungen, beispielsweise zur Prozesskultur, ziehen einen erhöhten Aufwand nach sich.

Es kann aber gelingen, diesem Aufwand einen zumindest gleichbedeutenden Nutzen entgegenzustellen. Dieser Nutzen sollte sich sogar dann einstellen, wenn keine sicherheitskritischen Projekte bearbeitet werden. Was dennoch bleibt, ist zumindest die Erhöhung von Transparenz in der Entwicklung und somit die Schaffung nachvollziehbarer und qualitativ besserer Ergebnisse.

In den Prozessen Fokus auf SPICE und ISO 26262 legen.

Wie vor allem die Lösungsideen zu den Abweichungen der Kategorie 2 zeigten, schlägt ISO 26262 konkrete Methoden vor, die auch in nicht sicherheitskritischen Projekten von Nutzen sein können. Daher empfiehlt es sich, solche Elemente als verpflichtende Methoden und Ergebnisse im Standardprozess zu übernehmen.

Zudem sinkt in sicherheitskritischen Projekten der Aufwand bei der Erstellung der Arbeitsergebnisse aufgrund der erhöhten Erfahrungswerte; gleichermaßen steigt die Qualität.

Nachhaltige Umsetzung

Bei der nachhaltigen Umsetzung von Verbesserungsmaßnahmen in Hinsicht auf SPICE gibt es zahlreiche Probleme. Die Einteilung der Abweichungen wiederum ähnelt den Grundpfeilern der Sicherheitskultur, wie sie ISO 26262 fordert. Daher muss eine Art Prozesskultur im Unternehmen etabliert werden. Das stellt sicher, dass die Mitarbeiter

die Verantwortlichkeiten kennen und nutzen,

Informationen verfügbar haben, mit deren Hilfe sie ihre Aufgaben effektiv bearbeiten und

erkennen, warum diese Aktivitäten ihnen im Projekt helfen können.

Vorgeschlagene Methoden und Arbeitsergebnisse von ISO 26262 können helfen, die geforderten Aktivitäten gemäß SPICE zu etablieren. Begründungen aus den Erfahrungen mit ISO 26262 lassen sich nutzen, um konkrete Probleme und die dazugehörigen Lösungen zu zeigen.

Einige Forderungen von ISO 26262 sind in den Prozessen verbindlich zu etablieren. Sie geben Lösungen zu bekannten Fragen vor und steigern Effizienz und Qualität der Arbeitsergebnisse. Das erfordert aber zuvor die Unterstützung der Geschäftsleitung, weil hiermit zusätzliche Aufwände verbunden sind. Auch müssen die Vorteile einer vollständigen und etablierten Vorgehensweise aufgezeigt werden, da diese sich mit den Aufwänden messen lassen sollte.

Die Prozessverbesserung nach SPICE funktioniert selbst ein wenig wie eine sicherheitskritische Entwicklung. An vielen Stellen lauern Fehlermöglichkeiten, die die störungsfreie Einhaltung der Prozesse gefährden. Eine Sicherheitsanalyse dieser Gefährdungspotenziale zeigt, wie sich sicherheitsrelevante Maßnahmen in den Prozessen etablieren lassen. Die Sicherheitsziele könnten somit lauten:

Sicherheitsziel 1: Verantwortlichkeiten sind klar zugewiesen und kommuniziert.

Sicherheitsziel 2: Vorgehensweisen zur Bearbeitung der Projektaufgaben sind bekannt und wenn möglich standardisiert.

Sicherheitsziel 3: Der Nutzen dieser Aufgaben ist erkannt und wird regelmäßig hinterfragt. *eck*

Timo Karasch
ist für Method Park als Senior Consultant zu den Themen Automotive SPICE, funktionale Sicherheit und Projektmanagement tätig. Er ist Mitglied des intacs Advisory Board und seit 2012 Dozent an der Dualen Hochschule Baden-Württemberg in Mannheim.
Timo.Karasch@methodpark.de