Bild: Stock-Fotografie_peshkov_1195639794

01 Ob bei autonom fahrenden Autos, selbstfliegenden Flugzeugen oder hochautomatisierten Techniken, die funktionalie Sicherheit stellt Produkt- und Softwareentwickler in diesen Zeiten vor eine große Herausforderung

Functional Safety dank durchgängigem Requirements Engineering

Wann eine Anforderung in elektrischen und elektronischen Systemen als sicherheitsrelevant zu definieren ist und welche prozessualen Aspekte der Entwicklung daraufhin eingehalten werden müssen, geben die Normen, wie die DIN EN 61508 oder die daraus abgeleitete Norm für Automotive ISO 26262, vor. Das sichtbare Ergebnis allein reicht für ein effizientes Safety-Konzept jedoch nicht aus (**Bild 1**). Auch der Weg dahin spielt eine wesentliche Rolle. Erfahrene Partner, wie Invenio, helfen bei der Umsetzung der Anforderungen sowie dem Erstellen der erforderlichen Traceability gemäß den einzuhaltenden Safety-Regularien, für eine effiziente Fertigung des sicherheitskritischen Produkts sowie die Minimierung der Gefahren für Personen und Anlage.

Autor: Nadine Samulski

Die sogenannte Safety – also die Sicherheit von Personen und Anlagen – erhält stetig mehr Relevanz. Zeitgleich kommt immer häufiger die Frage auf, wie diese sicherheitskritischen Aspekte eines Produkts am besten umzusetzen sind, sodass im Fall eines Fehlers oder Systemausfalls keine Menschen verletzt werden. In ihrer täglichen Arbeit erleben die Experten für Systems Engineering des Technologieunternehmens Invenio [1] jedoch häufig, dass nur sicherheits-

gerecht entwickelt wird, um die Assessments zu befriedigen. Invenio-Geschäftsführer Dipl.-Ing. (BA) Ingo Paech (**Bild 2**) erklärt, warum das nicht zielführend ist: „Dadurch schafft man nicht den Mehrwert, den es bedarf. Das Ziel sollte also nicht sein, die Normen einfach nur zu erfüllen, sondern auf effizientem Weg die beste Qualität und das sicherste Produkt zu erhalten. Erzeugt man den Mehrwert bereits auf dem Weg dahin, ist das Ergebnis automatisch richtig. Es sollte von Beginn an darauf geachtet werden, welche Normen, Standards oder Kundenanforderungen überhaupt eingehalten werden müssen. Ist dies nicht der Fall, kann es zu einer deutlichen Mehrarbeit und hohen Folgekosten führen."

02 Dipl.-Ing. (BA) Ingo Paech ist Geschäftsführer der Invenio Systems Engineering GmbH in Mannheim

Safety geht nicht ohne Requirements Engineering

Bereits jetzt wird deutlich, dass bei der Safety eines Produkts immer wieder die Anforderungen im Fokus stehen. Die Antwort auf die Eingangsfrage, wie sichere Produkte gewährleistet werden können, gibt daher das Requirements Engineering (**Bild 3**). Denn die Normen beinhalten zum einen Anforderungen an das Requirements Engineering an sich – vor allem im Bereich der Traceability, also der Nachverfolgbarkeit. Zum anderen sind die Normen selbst aber auch als Anforderungen zu sehen und müssen in die Traceability mit einbezogen werden.

Geht man nun chronologisch den Produktentwicklungsprozess durch, trifft man bereits zu Beginn auf das Anforderungsmanagement. Denn unabhängig der agierenden Branche werden zunächst die Sicherheitsziele eines Systems definiert. Daraus werden die Anforderungen abgeleitet und in sicherheitsrelevante und nicht sicherheitsrelevante Anforderungen unterschieden. Die sicherheitsrelevanten Anforderungen werden schließlich eindeutig gekennzeichnet. Für ein Projekt aus dem Automotive-Bereich gilt dabei ASIL, von QM über Stufe A mit den niedrigsten bis Stufe D zu den höchsten Integritätsanforderungen an das Produkt. Analog gilt für die Industrie- und Bahntechnik SIL in den Leveln 0 (QM) bis 4. Das QM steht dabei für „Quality managed" und bedeutet, dass auch nicht als sicherheitsrelevant eingestufte Anforderungen sauber gemanaged werden müssen, es aber weniger Pflichtaktivitäten gibt als bei sicherheitsrelevanten Anforderungen.

Die Experten-Teams von Invenio begleiten ihre Kunden bereits in dieser frühen Phase der Anforderungserhebung. „Wir unterstützen den Kunden, seine Anforderungen vollständig und korrekt zu verarbeiten und brechen mit ihm gemeinsam die Anforderungen in die jeweiligen Disziplinen, wie elektronische Hardware, Software und Mechanik, herunter. Darüber hinaus gehen wir je nach Komplexität auch weiter in die Tiefe. So stellen wir im Verlauf sicher, dass die Umsetzung aller Anforderungen vollständig und umfassend erfolgt und alle definierten Sicherheitsziele berücksichtigt sind sowie später auch erfüllt werden. So entsprechen wir den branchenüblichen Regularien für die Safety. Sicherheit ist ohne ein gutes Anforderungsmanagement schlichtweg nicht existent", so I. Paech.

Use-Cases zur Gefahren-Bewertung

Das Wesentliche bei der Betrachtung der funktionalen Sicherheit ist das Erkennen der Gefahr. Mittels der im Anforderungsmanagement üblichen Use-Cases werden diverse, möglicherweise auftretende Situationen durchgespielt. Manche Gefahren sind dabei trivial. Beim autonomen Fahren ist beispielsweise klar, dass das Auto allen möglichen Unfallsituationen aus dem Weg gehen muss. Es kann jedoch sein, dass die eigentliche Gefahr nicht direkt sichtbar ist: Es ist bei vielen Geräten auf Temperaturen zu achten, sodass Verbrennungen ausgeschlossen sind. Aber auch Stromstöße sind unangenehm und nicht gewollt.

In einigen Situationen für die Safety ist jedoch ein Weiterdenken erforderlich. Soll ein defekter Zug in einen sogenannten sicheren Zustand kommen, ist die Problematik folgende: Wenn der Zug brennt, ist ein Not-Halt sinnvoll. Wenn der Zug jedoch in einem Tunnel zu brennen beginnt, so ist es gegebenenfalls ein tragischer Fehler, wenn sich das Fahrzeug nicht doch aus dem Tunnel herausfahren lässt. Wenn Sicherheitsmaßnahmen greifen, ist es also von Vorteil, dass sie vom Menschen unter gewissen Umständen noch überschrieben werden dürfen.

Bei den Gefahren werden zudem aktive von passiven Gefährdungen unterschieden, wie I. Paech anhand eines weiteren Beispiels erläutert: „Bei einem elektrischen Straßenpoller, der gewisse Straßenabschnitte oder Parkplätze absperrt, ist eine aktive Gefahr, dass ein Fahrzeug darübersteht, während der Poller hochfährt. Eine passive Gefahr kann hingegen vorliegen, wenn der Poller aus einem nicht gut sichtbaren Material besteht oder er nicht so weit herausfährt wie ein herkömmlicher Straßenpoller. Es muss also aus Sicherheitsgründen eine Mindesthöhe geben und durch Tests geprüft werden, dass der Poller aus jedem Blickwinkel gut sichtbar ist oder entsprechend mit Reflektoren gekennzeichnet werden. Dafür müssen schließlich Abnahmekriterien entwickelt werden."

Die Traceability – das Kernelement der Safety

Wie bereits erläutert, ist bei der Safety – sowie beim Requirements Engineering – das sichtbare Ergebnis allein nicht ausreichend, sondern auch der Weg dahin ist von großer Bedeutung. Insbesondere bei der Nachverfolgbarkeit ist es daher nicht zielführend, wenn diese Informationen im Nachhinein erst hinzugenommen werden. Die Auflagen der Normen werden zwar dadurch erfüllt, aber es wird keine

wachsende Qualität geschaffen, auf die Verlass ist. Bei sicherheitsrelevanten Anforderungen ist die Traceability daher wesentlich wichtiger als bei nicht sicherheitsrelevanten Anforderungen. Zusätzlich wird mithilfe der Traceability ein sehr stringentes Änderungsmanagement, Fehlermanagement und Konfigurationsmanagement umgesetzt. Doch wie funktioniert die Traceability genau, damit die Safety des Produkts gesichert ist?

Die Traceability gewährleistet die vollständige Umsetzung der Anforderungen. Sie stellt bei korrekter Anwendung sicher, dass die sicherheitsrelevanten Anforderungen auf der Systemebene und auf den darunterliegenden Ebenen ebenfalls als sicherheitsrelevant sichtbar sind – zudem wird die Konsistenz sichergestellt. Dabei werden Informationen miteinander in eine Beziehung gebracht. Eine Systemanforderung wird durch die Beziehung zu einer oder mehreren Softwareanforderungen verfeinert. Die Anforderungen selbst werden durch die Beziehung mit Testfällen verifiziert. So lässt sich also prüfen, ob alle Systemanforderungen, die softwarerelevant sind, auch auf der Softwareebene verfeinert worden sind und ob alle diese Anforderungen mindestens einen Testfall beinhalten. Bei der Konsistenzprüfung geht es dann darum, dass beispielsweise im System steht, eine Lampe soll zehn Sekunden leuchten; dann sollten diese zehn Sekunden auch in den Softwareanforderungen zu finden sein.

Bild: Stock-Fotografie_Blue Planet Studio_ 1172642339

03 Modellbasiertes Systems Engineering (MBSE) hilft Ingenieuren dabei, komplexe Systeme im Ganzen zu überblicken und eine optimale Lösung für die Anforderungen aller Stakeholder zu entwickeln. Im Gegensatz zum dokumentenbasierten Systems Engineering integriert MBSE die Systeminformationen in zentralen digitalen Systemmodellen und verknüpft diese miteinander

Mithilfe von Anforderungsmanagement-Tools, wie Polarion ALM, können die Verlinkungen vorgenommen und die Nachverfolgbarkeit gewährleistet werden. Hinzu kommt noch, dass beide Aspekte jederzeit ausgewertet und auf unterschiedliche Weise grafisch dargestellt werden können. Auch das Managen der schrittweise abgearbeiteten Anforderungen kann durch Polarion ALM – sowohl klassisch im V- oder Wasserfallmodell als auch agil – gesteuert werden.

Polarion ALM ist ein Tool für das Anforderungsmanagement, in dem das Verwalten von Erfordernissen für Produktentwicklungsprojekte vereinfacht visualisiert wird. Die zu 100 % browserbasierte Application-Lifecycle-Management-Lösung dient dem Definieren, Testen und Verwalten komplexer Systeme. Als eines der führenden Unterstützungsinstrumente für erfolgreiche Produktentwicklungen haben Anwender mit dem Tool – ob in kleinen Teams oder mit mehreren tausend Anwendern – einen permanenten Einblick auf den jeweils aktuellen Entwicklungsfortschritt. Dank Polarion ALM kann die Zusammenarbeit sowohl klassisch mit Wasserfall- oder V-Modellen als auch agil gesteuert werden: Das Tool ist flexibel und individuell einsetzbar, um sie gezielt bei ihren Prozessen zu unterstützen und überzeugt durch seine Nachverfolgbarkeit (Traceability).

Systems Engineering erfolgreich implementieren

„Häufig wird im Requirements Engineering nur Mehrarbeit neben dem eigentlichen Projekt gesehen. Wenn man allerdings in Betracht zieht, dass dadurch alle Anforderungen während des gesamten Produktentstehungsprozesses korrekt verfolgt und erfüllt werden, ist es eher so zu sehen, dass eine sehr zeit- und kostenaufwendige Nacharbeit durch das Anforderungsmanagement reduziert wird. Selbstverständlich ist das Anforderungsmanagement nur ein Teilbereich der funktionalen Sicherheit eines Produkts. Es werden viele zusätzliche Methoden verwendet, wie beispielsweise FMEA oder FMEDA, FTA und andere Analysemethoden, mit denen ein Fehlverhalten identifiziert und eingeordnet werden kann. Aber um von Beginn an auf dem richtigen Weg zu sein und alle Anforderungen zu berücksichtigen, ist das Requirements Engineering unerlässlich. Wir bei Invenio wollen, dass Projekte gar nicht erst kritisch eingestuft werden. Deshalb bringen wir unsere Erfahrung bei unseren Kunden mit ein und können so häufig auftretende Probleme bereits in den frühen Entwicklungsphasen vermeiden“, erläutert I. Paech. (no)

Literatur

[1] Invenio Systems Engineering GmbH, Mannheim: www.invenio.net

Autorin

Nadine Samulski ist Referentin Business Communication bei der Invenio GmbH Engineering Services in Rüsselsheim.
marketing@invenio.net