

Funktionale Sicherheit: Fallstudien

Kontext

Die Sicherheit von Maschinen, Anlagen und Systemen ist branchenübergreifend in zunehmendem Masse von einer risikofreien Funktion elektronischer Steuerungen abhängig. Die grundlegende Herausforderung der funktionalen Sicherheit besteht darin, komplexe programmierbare Systeme so zu entwerfen und zu realisieren, dass keine Systemfehler oder Ausfälle zu Schäden an Personen oder der Systemumwelt führen.

Die Kunden

Durch die steigende Anzahl sicherheitsrelevanter E/E-Systeme im Automobil gewinnt das Thema Funktionale Sicherheit für Automobilhersteller und deren Zulieferbetriebe zunehmend an Bedeutung. Im Folgenden wird dargestellt, wie SynSpace diesen Unternehmen geholfen hat.

IT-Management-Beratung

Abhängig von der Grösse des jeweiligen Unternehmens und des Stellenwertes sicherheitskritischer Produkte sind unterschiedliche Strategien für die Einführung von Entwicklungsprozessen zu wählen. SynSpace hat sowohl OEMs markenübergreifend, als auch kleine und grosse Zulieferer bei der Auswahl der richtigen Einführungsstrategie beraten. So wurde für das jeweilige Umfeld sichergestellt, dass schlanke, pragmatische, aber trotzdem den Anforderungen der ISO 26262 entsprechende Prozesse erfolgreich eingeführt werden konnten.

Je nach vorhandenem Know-How und Prozesserfahrung bzgl. der ISO 26262 wurde mit einem Awareness-Workshop für das Management zur Vermittlung der Anforderungen der Norm und deren Auswirkungen auf die Organisation begonnen oder bereits vorhandene Einführungsstrategien überprüft.

Bestehende Standardprozessbeschreibungen für die E/E-Entwicklung, z. B. aus vorausgegangenen Automotive SPICE® -Prozessverbesserungsprojekten wurden dabei in die Planung einbezogen.

Prozessgestaltung

Entsprechend der Einführungsstrategie erstellten wir Prozessspezifikationen gemäss ISO 26262 oder ergänzten vorhandene Spezifikationen um

Anforderungen aus der Norm. Hierbei ging es neben der rein fachlichen Tätigkeit auch darum, zwischen den betroffenen Abteilungen aus Entwicklung und Qualitätssicherung zu vermitteln und die eigenen Aktivitäten mit anderen Prozessverbesserungsprojekten (z.B. nach SPICE) abzustimmen.

Bereits geltende Verfahrensvorschriften und Prozessstandards wurden durch SynSpace auf Lücken, Inkonsistenzen, Angaben zur Überdeckung und Traceability zur ISO WD 26262 überprüft. Notwendige Modifikationen wurden eingearbeitet und die einheitliche Darstellung in Verfahrensvorschriften und referenzierenden Dokumenten (z. B. Schulungsmaterial) sichergestellt.

Im Falle eines grossen OEMs hat SynSpace auch einen Vergleich der vorhandenen Prozessstandards für Funktionale Sicherheit bei zwei Marken des Konzerns für die technische Entwicklung vorgenommen. Verglichen wurden inhaltlicher Umfang, inhaltliche Abweichung sowie der Detaillierungsgrad. Als Resultat wurde ein Katalog empfohlener Massnahmen zur Harmonisierung der beiden Standards erarbeitet und präsentiert. In der Folge war SynSpace massgeblich daran beteiligt, alle Aktivitäten und Arbeitsmittel, die abteilungs- und bereichsübergreifend genutzt werden, zu synchronisieren, und damit die Effizienz zu steigern.

Die abgestimmten und in Prototyp-Projekten erprobten Ergebnisse wurden anschliessend flächendeckend gemäss der jeweiligen Strategie ins Unternehmen ausgerollt. Von der zweckmässigen Bereitstellung der Arbeitsmittel im Intranet oder Projektverzeichnissen, über Schulung und Coaching, bis hin zu operativer Begleitung im Entwicklungsprojekt reichte hierbei das Spektrum.

Darüber hinaus hat SynSpace in vielen Fällen auch die Aktivitäten der Functional Safety-Initiativen geplant und vorangetrieben. Begleitende Tätigkeiten wie die Erstellung und Präsentation von Statusberichten und Entscheidungsvorlagen vor entsprechenden Gremien rundeten das Gesamtpaket ab.

Funktionale Sicherheit: Fallstudien

Engineering Support

Bei vielen unserer Kunden ist das Thema Funktionale Sicherheit und die Erfüllung der Anforderungen der entsprechenden Normen Neuland. Die Umsetzung der Anforderungen in Prozessbeschreibungen, Arbeitsmitteln und Verfahrensanweisungen ist ein wichtiger Schritt, aber der Transfer in die Praxis von Entwicklungsprojekten stellt eine weitere, grosse Herausforderung dar.

SynSpace hat sowohl Entwicklern in kleinen Entwicklungsprojekten, als auch in grossen Projektorganisationen den Safety-Lifecycle im Rahmen von Workshops erklärt und den Umgang mit den Prozessvorgaben eingeführt. Oft wurde im Vorfeld ein von SynSpace in Kooperation mit dem Vienna Institute for Safety & Systems Engineering (VISSE) der FH Campus Wien entwickelter Safety Quick Check durchgeführt, um die Ausgangsbasis und damit die vorhandenen Lücken zu identifizieren. Dies ermöglicht eine sehr schlanke aber trotzdem zielgerichtete Vorgehensweise.

Beispielsweise wurde dadurch erkannt, dass in einem Projekt die Definition des Items zu weit gefasst war, was zu erheblichen Mehraufwänden im gesamten Entwicklungsprozess geführt hätte. Nach der Neudefinition des Items wurde die vorhandene Gefahren- und Risikoanalyse überprüft und an die neue Item-Definition angepasst. Mit dem Projektteam wurde anschliessend die weitere Vorgehensweise zur Erreichung der Safety-Forderungen der ISO 26262 abgestimmt. Das Projekt wird nun gelegentlich durch einen Experten für Funktionale Sicherheit von SynSpace begleitet, um die Konformität der Entwicklung zur ISO 26262 sicherzustellen.

In einem anderen Fall wurde im Safety Quick Check zusätzlich auf die Vorgaben von Automotive SPiCE[®] geachtet. Eine hohe Prozessreife gem. Automotive SPiCE[®] stellt eine sehr gute Ausgangsbasis für die Entwicklung sicherheitskritischer Systeme nach den Anforderungen der ISO 26262 dar. Typische Herausforderungen wie

- ❌ bidirektionale Traceability
- ❌ das konzeptionelle Trennen von Anforderungen und Lösungen
- ❌ die inhaltliche Qualitätssicherung von zu dokumentierenden Arbeitsprodukten
- ❌ das richtige Reagieren auf Abweichungen
- ❌ das Ziehen von Konfigurationen und Baselines über alle physikalischen Bestandteile, Informationen und Dokumentationen

konnten mit der Unterstützung von SPiCE-Experten schnell gemeistert werden. Die darüber hinausgehenden Aufgaben, wie

- ❌ Ermittlung von Gefahrensituationen („Hazards“) und deren Risiken
- ❌ Erstellung von Sicherheitskonzepten und Sicherheitsanalysen
- ❌ Verifikation und Validierung der Sicherheitsmassnahmen
- ❌ Erstellung eines Safety Case

konnten auf der stabilisierten Basis, unterstützt durch einen Safety Experten von SynSpace, ebenfalls gut gemeistert werden. Eine wesentliche Grundlage ist hierfür jedoch immer die korrekte Bestimmung des ASIL und das entsprechende Tailoring der Standardprozesse.

**Beratung und Optimierung über die gesamte Wertschöpfungskette.
Wir sind gerne für Sie da. Sprechen Sie uns an.**

Ihr Ansprechpartner:

Michael Landwehr

Director Sales & Marketing

phone +49 761 476 45 65

e-mail: michael.landwehr@synspace.com