

Prozesssicherheit Safety-Assessment Prozess

Als Hersteller von Produkten ist man gut beraten rechtzeitig einen Safety- und Reliability-Prozess zu etablieren, der die Frage beantwortet: *„Unter welchen Bedingungen und Anforderungen soll ein Produkt innerhalb seines Produktlebenszyklus einwandfrei funktionieren und welche Wartungsintervalle sind dafür notwendig.“*

Sicher ist der wirtschaftliche Aufwand zur Herstellung eines hochwertigen Produktes vordergründig erst einmal teurer, als die Kosten für ein weniger zuverlässiges. Aber der Imageverlustes basierend auf schlechter Verfügbarkeit eines Produktes oder hohe Wartungs- und Haftungskosten sind im Markt kein guter Leumund. Deshalb bedeutet ein Produkt mit hoher Zuverlässigkeit prinzipiell einen Wettbewerbsvorteil. Doch hohe Zuverlässigkeit setzt eine systematische Planung inklusive Berücksichtigung aller Lebenszykluskosten voraus. Neben klaren technischen Anforderungen müssen darüber hinaus wirtschaftliche und organisatorische Anforderungen berücksichtig werden. Ebenso sind frühzeitig Prozess-Methodik sowie hinreichende Quality-Gates zur Sicherstellung der Produkt-Zuverlässigkeit im Entwicklungsprozess zu integrieren. Im Ansatz wird Zuverlässigkeit nicht in ein Produkt hineingeprüft, sondern muss in das Produkt hineinentwickelt und entsprechend qualitativ gefertigt werden.

Leider sieht das in der Praxis vielfach anders aus. Der integrale Safety- und Reliability-Prozess wird oft unterschätzt und erst zu einem sehr späten Zeitpunkt in die Designfindung eingebunden. Dabei muss bei komplexen Systemen die Ausfallsicherheit zur Gewährleistung der Betriebssicherheit unter allen Umständen durch die gesamten Entwicklungsphasen wie Planung, Design, Integration, Verifikation & Validation sowie In-Service verfolgt werden. Ein in das Team integrierte externer Interim Manager, mit sehr guten Prozess-Kenntnissen, kann dort frühzeitig grundlegende Impulse setzen und somit viel Lehrgeld ersparen.

Safety Management und Part 21

Beim Part 21 mit den Vorgaben aus der ARP4754 und ARP4761 handelt es sich um die strukturierte Vorgehensweise, sicherheitsrelevante Risiken in luftfahrttechnischen Betrieben proaktiv zu minimieren. Safety Management wird von der Grundidee getragen, Sicherheit als Führungsaufgabe zu verstehen, die gesamtbetrieblich verankert ist und nicht nur auf einige Personen verteilt wird. Das diese Philosophie kurzfristigen Rentabilitätsprognosen geopfert wird, kann selbst große Firmen zum straucheln bringen. Vom Reputationsverlust gar nicht zu reden.

Zwangsläufig muss Safety Management gleichberechtigt neben dem Qualitätsmanagementsystem stehen. Dabei ist ein integraler Prozess mit guten Prozessvorgaben entscheidend, um einen effizienten und tauglichen Produktentwicklungsprozess zu etablieren. Dabei weist die EASA ausdrücklich darauf

hin, dass das Safety Management System mit den anderen betrieblichen Managementsystemen wie Qualitäts-, Arbeitsschutz- und Umweltmanagementsysteme zusammengefügt werden darf.

Product Life Cycle (ARP4754/ARP4761)

Basierend auf der Forderung nach Betriebssicherheit und Lebensdauer, darf durch das Systemdesign keine Gefahr für Leben, Gesundheit oder Eigentum ausgehen. Daraus folgend, muss das Produkt die gesetzlichen und vertraglichen Safety-Anforderungen über den gesamten Lebenszyklus gewährleisten. Ebenso sollten alle sicherheitsrelevanten Ereignisse und Verfügbarkeitszahlen, die aus dem Betrieb und der In-Service Phase resultieren, wieder in den Designprozess fließen, um eine stetige Produktqualitätssteigerung gewährleisten zu können.

Test Coverage

Bei wachsender Komplexität und damit einhergehenden Kosten eines aus mehreren Komponenten zusammengesetzten Systems, kann eine Prüfung der Zuverlässigkeit des Gesamtsystems weder als 100% Prüfung, noch als Stichprobenprüfung in der notwendigen Signifikanz (Test Coverage) vorgenommen werden. Da Aussagen über voraussichtliche Ausfälle von Funktionen und deren Wahrscheinlichkeit benötigt werden, muss mithilfe von Statistik und real erworbenen Daten aus der Lebensdauer-Prüfung/Feldausfällen, eine quantitative Aussage über das sicherheitsrelevante Verhalten des gesamten Systems ermittelt werden.

Ermittlung von Schwachstellen und Bewertung von Systementwürfen

Der Einsatz von Design-Mitteln wie Redundanz, Monitoring, Partitionierung oder implementiertes Fail-Safe-Verhalten erhöht die Zuverlässigkeit eines Systems. Aber zur Absicherung und Ermittlung von Schwachstellen, können analytische Verfahren, Simulation, Stresstests oder organisatorischen Methoden angewendet werden. Mittels probabilistischer Aussage für Funktion, Architektur oder Bauteil, können Systemschwachstellen bereits zu einem sehr frühen Zeitpunkt des Entwicklungsprozess ermittelt und Gegebenenfalls durch kostengünstigere Verbesserungsmaßnahmen ersetzt werden. Um den Begriff Sicherheit als Wahrscheinlichkeit quantitativ zu erfassen und daraus entsprechende Kenngrößen ableiten zu können, wird Sicherheit als *Wahrscheinlichkeit definiert, in der für einen bestimmten Zeitraum von der Komponente keine Gefährdung ausgeht*. Die Durchführung einheitlicher Analysen, auf Basis der Zuverlässigkeit, ermöglicht eine quantitative und vergleichende Aussage über die innere Zuverlässigkeit von Systemen. Das ist dann möglich, wenn für die einzelnen Bauelemente der verschiedenen Geräte Gleichartigkeit vorausgesetzt wird.

Auf dieser Basis ist frühzeitig ein Kriterium für die zuverlässigkeitstechnische Beurteilung gegeben. Der uneingeschränkte Wert oder die quantitative Aussage einer derartigen Berechnung ist aufgrund der fehlenden absoluten Datensicherheit zwar häufig strittig. Der Wert der vergleichenden Analyse zweier Systeme ist jedoch unstrittig und liefert somit die Grundlage für eine systematische Einstufung der relativen Zuverlässigkeit.

Safety Assessment Luftfahrt

Die Safety Aktivitäten über den gesamten Entwicklungs- bzw. Produktlebenszyklus sowie die dabei zu erfüllenden Aufgaben, zeigt exemplarisch die Abbildung 1 Safety Assessment Prozess.

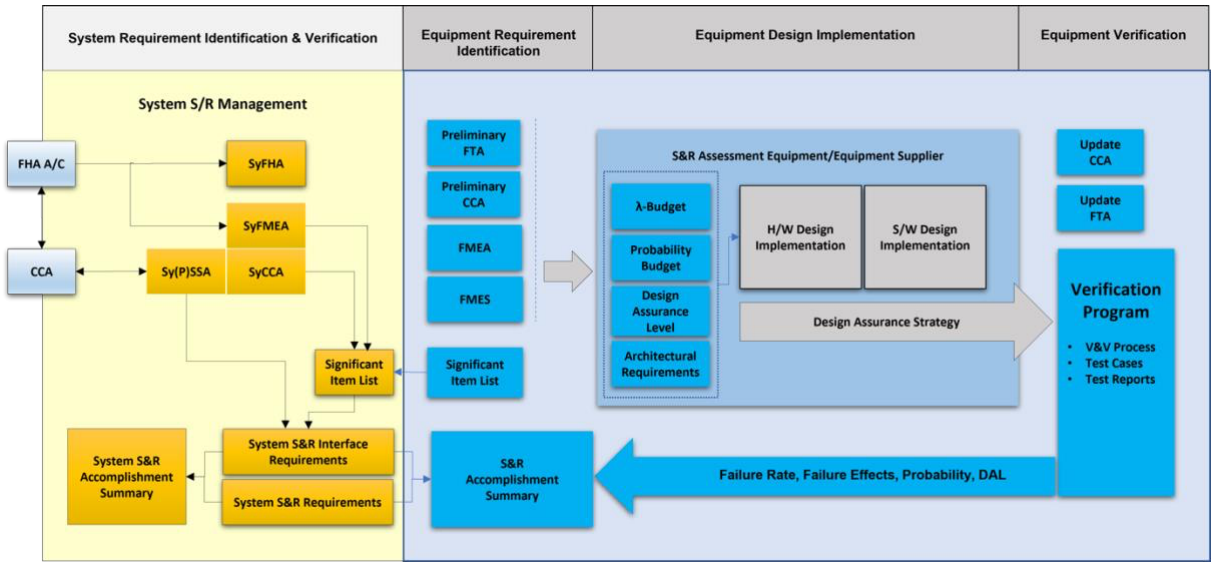

Abbildung 1 Safety Assessment Prozess /"ARP4754" und „ARP4761"/.

Basierend auf der ARP 4754A (Certification Considerations for Highly-Integrated Or Complex Aircraft Systems) und ARP 4761 (Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment), gelten die beschriebenen Artefakte für alle Safety Aktivitäten im Zusammenhang mit nachfolgenden Aufgaben:

- Definition der Methodik für Sicherheits-/Zuverlässigkeitsaktivitäten sowie der Erstellung von begleitenden Dokumenten.
- Durchführung aller erforderlichen Sicherheits-/Zuverlässigkeitsanalysen sowie der Bewertungen zur Ermittlung von Sicherheits-/Zuverlässigkeitsanforderungen.
- Zuweisung von Sicherheits-/Zuverlässigkeitsanforderungen für den Entwurf der luftfahrtspezifischen Funktionen, Systeme und Komponenten sowie der zugehörigen Ausrüstung und ihrer Installation.
- Durchführung aller erforderlichen Nachweisprozesse, um sicherzustellen, dass die ermittelten Sicherheits-/Zuverlässigkeitsanforderungen erfüllt werden (V&V Prozess).

Im Einzelnen werden die Assessment Anteile durch die jeweiligen STC-Halter, dem Unterauftragnehmer oder durch die Lieferanten verantwortet und durchgeführt.

Support im Safety Assessment Prozess

Im Safety Assessment beginnt der ganzheitliche Ansatz mit der gründlichen Analyse von Arbeitsumgebung sowie der Bewertung bestehender Prozesslandschaften. Basierend auf diesen Erkenntnissen können maßgeschneiderte Strategien zur Implementierung von effektiven Sicherheitsprozessen entwickelt werden, die auf die jeweiligen spezifischen Kunden-Bedürfnisse zugeschnitten sind. Von der Erstellung von Sicherheitsrichtlinien, nachfolgenden Audits, Reviews, oder Assessments bis zur Schulung der Mitarbeiter ist Unterstützung möglich. Als Coach oder integriert im Entwicklungsteam stehe ich Ihnen als verlässlicher Partner zur Seite.

Kontakt

Lösungen bedürfen des ersten aktiven Schritts.

Wenn Sie nach einer zuverlässigen, professionellen und kundenorientierten Dienstleistung suchen, wie Sie Ihre betriebliche Strategie zukunftssicher machen? Dann kontaktieren Sie mich für ein erstes Gespräch. Als Beratung, Work-Shop oder integriert in Ihr Team vor Ort, finden wir eine für Ihr Bedürfnis angepasste Lösung.

AvioniQ Engineering GmbH
Dipl.-Ing. Luft- und Raumfahrt
Joachim Venrath
https://www.avioniq.com