ACX GmbH

DO-254

Eine Einführung

Inhalt

Was ist die DO-254?

DO-254 ist der formale Sicherheitsstandard für die Entwicklung komplexer Hardware, wie beispielsweise ASICs, FPGAs und CPLDs. Eine Hardware wird laut Spezifikation als „komplex“ bezeichnet, wenn eine umfassende Kombination von deterministischen Tests und Analysen die korrekte Funktionstüchtigkeit unter allen vorhersehbaren Betriebsbedingungen nicht gewährleisten kann. Für komplexe Geräte tritt an Stelle von ausgiebigen Tests ein strenger, strukturierter Design- und Verifizierungsprozess. Der Nachweis, dass die Entwicklung und Verifikation komplexer Hardware diesem Prozess entspricht, ist Ziel der DO-245.

Ein DO-254-konformes Design wird mit einer Reihe von formalen Anforderungen festgelegt. Im Rahmen des Zertifizierungsprozesses muss nachgewiesen werden, dass die konkrete Umsetzung all diese Anforderungen erfüllt. Das wird typischerweise durch die formale Verifikation, die die Einhaltung der formalen Anforderungen nachweisen muss erreicht. Eine grafische Darstellung des typischen Prozessablaufes ist in nachfolgender Abbildung dargestellt.

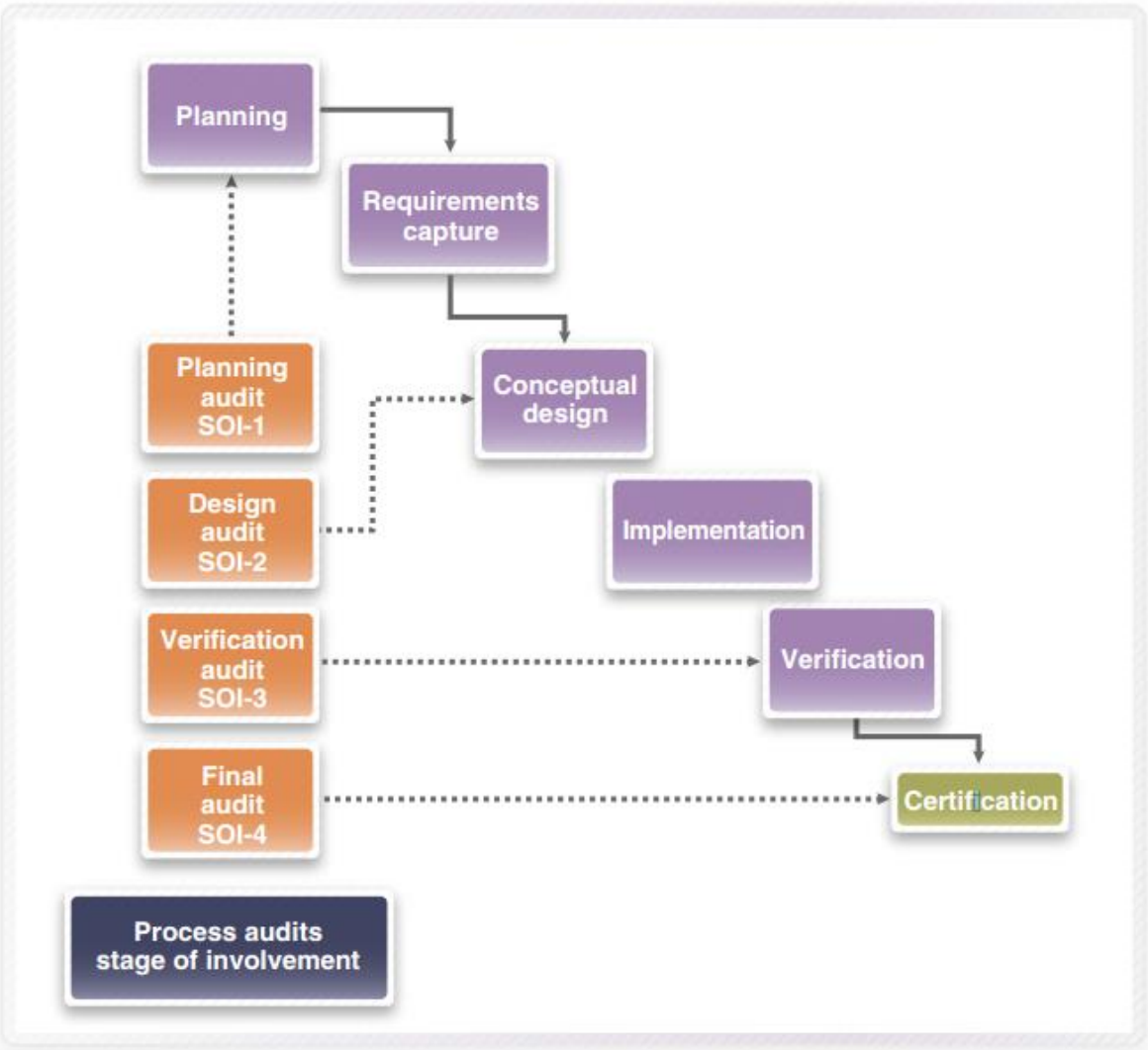

Figure 2: DO-254 process flow

Die Abbildung zeigt lediglich ein Beispiel des Prozessablaufes. Der Prozessablauf, die einzelnen Phasen und die benötigten Werkzeuge können sich von Projekt zu Projekt unterscheiden. Um die DO-254 Konformität erfolgreich zu erreichen, muss das Prinzip der „Rückverfolgbarkeit“ eingehalten werden: die Verifikationsergebnisse müssen nachvollziehbar sein und sich von den formalen Anforderungen ableiten lassen.

Die DO-254 ist in erster Linie eine Prozessspezifikation. Der Standard enthält ähnlich wie die DO-178, der Standard zur Entwicklung sicherheitskritischer Software für die Luftfahrt, keine konkrete Beschreibung der detaillierten Implementierung des Prozesses.

DO-254 SAFETY LEVELS

Die DO-254 definiert fünf Levels der Kritikalität von Level A (höchste) bis Level E (niedrigste), entsprechend den fünf Klassen von Fehlern: katastrophal, gefährlich/sehr schwer, schwer, leicht und ohne Wirkung. Abhängig von dem Grad der Schäden, die durch einen Hardwarefehler verursacht werden können, wird festgelegt, nach welchem Level die Hardware zertifiziert werden muss. Die fünf Stufen reichen von schwersten, wo ein Hardwarefehler zu einem Totalausfall des Flugzeuges führen würde, bis hin zu dem am wenigsten schweren, wo ein Hardwarefehler keine Wirkung auf die Flugzeugsicherheit zur Folge hätte. Die fünf Stufen sind:

Level A Der Ausfall der Hardware wird das sichere Weiterfliegen und Landen des Flugzeuges verhindern. Dieses Maß an Sicherheit ist erforderlich, wenn ein Ausfall einer Hardwarefunktion einen Ausfall einer Systemfunktion verursachen würde, die zu einem Totalausfall des Flugzeuges führen würde. Die Wahrscheinlichkeit eines Level A Fehlers darf nicht größer als einmal in einer Milliarde Flugstunden sein. Aus diesem Grund wird Hardware der Level A redundant ausgelegt.

Level B Der Ausfall einer Level B Hardware reduziert die Fähigkeit des Flugzeuges oder die Fähigkeit der Flugbesatzung die ungünstigen Betriebsbedingungen zu bewältigen. Die Flugbesatzung kann so beeinträchtigt werden, dass sie nicht mehr in der Lage ist ihre beruflichen Pflichten, ohne Fehler oder bis zum Abschluss durchzuführen. Ein Hardwarefehler könnte auch zu schweren oder tödlichen Verletzungen der Menschen am Bord des Flugzeuges führen. Ein Level B Fehler darf nicht öfter als einmal in zehn Millionen Flugstunden auftreten.

Level C Der Ausfall der Hardware wird die Fähigkeit der Flugbesatzung, mit den ungünstigen Betriebsbedingungen umzugehen, begrenzen. Die Flugbesatzung kann so behindert werden dass sie nicht mehr in der Lage ist ihre beruflichen Pflichten effizient durchzuführen. Ein Hardwarefehler könnte auch zu gewissen Beschwerden oder Verletzungen von Personen an Bord des Flugzeugs führen. Ein Level C Fehler ist nicht öfter als einmal in 100.000 Flugstunden zulässig.

Level D Der Ausfall einer Level D Hardware kann geringfügig die Sicherheit des Flugzeuges beeinträchtigen. Ein Fehler kann zu einer erhöhten Arbeitsbelastung der Flugbesatzung führen aber wird ihre Fähigkeiten nicht behindern. Dies kann auch zu einigen Unannehmlichkeiten für die Menschen am Bord des Flugzeuges führen. Ein Level D Fehler darf, wie ein Level C Fehler nicht häufiger als einmal in 100.000 Flugstunden auftreten.

Level E	Der Ausfall einer Level E Hardware hat keinen Einfluss auf die Leistungsfähigkeit des Flugzeuges oder die Menschen am Bord des Flugzeuges.

Diese Sicherheitseinstufung wird durchgeführt um sicherzustellen, dass sicherheitskritische Systeme an Bord eines Flugzeuges mit dem notwendigen, bezüglich der Sicherheitsbestimmungen, Aufwand entwickelt werden.

Entwicklungsprozesse

Die DO-254 beschreibt drei Hauptprozesse für den Hardware-Entwicklungsprozess:

- Planung
- Entwicklung
- Test

Für jeden dieser Prozesse müssen Zertifizierungsdokumente entsprechend der Sicherheitseinstufung des Projektes erarbeitet werden. Die folgende Liste zeigt das Grundgerüst der benötigten Dokumente:

- Plan for Hardware Aspects of Certification
- Hardware Design Plan
- Hardware Validation Plan
- Hardware Verification Plan
- Hardware Configuration Management Plan
- Hardware Process Assurance Plan
- Requirements Standards
- Hardware Design Standards
- Validation and Verification Standards
- Hardware Archive Standards
- Hardware Requirements
- Hardware Design Representation Data
- Traceability Data
- Review and Analysis Procedures
- Review and Analysis Results
- Test Procedures
- Test Results
- Hardware Acceptance Test Criteria
- Problem Reports
- Hardware Configuration Management Records
- Hardware Process Assurance Records
- Hardware Accomplishment Summary
- Der erste Schritt in jeder DO-254-Entwicklung ist der Planungsprozess. Während dieses Prozesses werden die sechs Planungsdokumente erstellt:
- Plan for Hardware Aspects of Certification (PHAC)
- Hardware Development Plan (HDP)
- Hardware Verification Plan (HVeP)

- Hardware Validation Plan (HVaP)
- Hardware Configuration Plan (HCP)
- Hardware Process Assurance Plan (HPAP)

Die Dokumente definieren die geplante Vorgehensweise der folgenden Entwicklungsphasen: Design-und Entwicklung, Validierung und Verifikation, Konfigurationsmanagement und Qualitätssicherung. Durch diese Dokumente wird die Entwicklung der Hardware der Behörde vorgestellt und abgestimmt.

Das wichtigste Dokument in dieser Phase ist der Plan for Hardware Aspects of Certification (PHAC). Die Behörde erhält als Erstes dieses Dokument. Der PHAC definiert die Prozesse, das Verfahren und die Standards, die zu verwenden sind um die DO-254-Ziele zu erreichen und die Zertifizierungszulassung für die Zertifizierung der Hardware zu erhalten. Der PHAC kann sich auch auf dem Verifikationsplan beziehen, die zu verwendete Methodik zur Ausführung der Gesamtverifikation beschreiben und den vorhandenen „Rückverfolgbarkeit"-Mechanismus erklären. Der PHAC sollten auch die im Projekt verwendet EDA-Tools spezifizieren und die Methode zur sog. „Tool Assessment" für jedes Tool vorstellen.

Das Konfigurationsmanagement ist ein weiterer wichtiger Aspekt bei der Planung. Für DO-254 ist es wichtig, die Version und die Geschichte aller mit dem Projekt verbundenen Artefakte zu steuern. Das schließt alle Unterlagen, RTL und Verfahrensanweisungen, Scripts und Berichte ein. EDA-Tools sollten auch unter Revisionskontrolle sein, um die „Tool Assessment" – Anforderungen zu erfüllen. Eine Konfigurationsmanagementstrategie sollte für jeden Entwicklungsschritt definiert und in der PHAC beschrieben werden.

Während der Planung werden auch die Hardware Levels definiert.

Sobald die Planung abgeschlossen ist, beginnt der Hardware Design Prozess. Er beinhaltet folgende Schritte:

- Requirements Capture
- Conceptual Design
- Detailed Design
- Implementation
- Verification
- Transfer to production

Die DO-254 legt fest, dass das Design mit formalen Anforderungen spezifiziert werden muss. In dem ersten Entwicklungsschritt sollen diese Anforderungen erfasst werden. Anforderungen werden hierarchisch geschrieben. Das bedeutet dass eine hohe Anforderung aus mehreren einfachen Anforderungen zusammengesetzt wird. Diese werden auf drei Ebenen abverlangt:

System Level Requirements	beschreiben Funktionen und Eigenschaften der zu entwickelnden Hardware nach außen, also zum Anwender hin.
High Level Requirements	beschreiben die grundsätzlichen Anforderungen und Designentscheidungen an das System um das System Level Requirement zu erfüllen, welchem sie zugeordnet worden. (Was soll getan werden?)

Low Level Requirements	beschreiben, wie genau die beschriebene Funktionalität des High Level Requirement, welchem sie zugeordnet sind, implementiert werden soll. (Wie soll etwas getan werden?)

Dabei soll die „Rückverfolgbarkeit“ der Anforderungen gewährleistet werden. Damit wird bewiesen, dass, wenn alle untergeordneten Anforderungen einer übergeordneten Anforderung erfüllt sind, die übergeordnete Anforderung auch erfüllt ist.

Eine Ausnahme bilden die sogenannten „Derived Requirements“. Das sind Anforderungen, die sich nicht auf System- bzw. High-Level-Anforderungen beziehen oder auf diese zurückzuführen sind. Eine abgeleitete Forderung ist eine zusätzliche Anforderung, abgeleitet aus dem Hardware Entwicklungsprozess.

In der Designphase wird eine Architektur entworfen, die alle definierten Anforderungen wiederspiegelt. Nach diesem Prozess folgen der detaillierte Design-Prozess und der Implementierungsprozess.

Der Verifikationsprozess stellt sicher, dass die implementierte Hardware die vor dem Beginn des Prozesses festgelegten Anforderungen erfüllt. Dies wird normalerweise mit der Durchführung von Design-Prozess-Reviews, Leistungsanalysen und Tests erreicht. Diese sind allesamt im Hardware Verification Plan definiert. Hauptziel des Verifikationsprozesses ist der Nachweis folgender Punkte:

Die implementierte Hardware erfüllt die zum Projektbeginn festgelegten Anforderungen.

Die Beziehung zwischen der Hardware-Anforderungen, der Umsetzung der Pläne und der Tests, zusammen mit den Ergebnissen der Ausführung der Tests, ist nachvollziehbar.

Alle Fehler können zu einem konkreten Prozess zurückgeführt und als gelöst betrachtet werden.

Der Validierungsprozess gewährleistet, dass die abgeleiteten Anforderungen in Bezug auf die Systemanforderungen korrekt und vollständig sind.