Cassidian Electronics

Ottmar Bender, Head of Mission Management Software

Erkenntnisse aus der Entwicklung komplexer und sicherheitskritischer Avionikarchitekturen

OOP 2011, 25.01.2011

Abstract

An Systeme für Luftfahrzeuge werden im Allgemeinen große Anforderungen gestellt bezüglich funktionaler Sicherheit (*safety*), Performanz, Zuverlässigkeit und Robustheit. Stringente Standards wie SAE-ARP4754 und RTCA/DO-178B geben die Ziele und Anforderungen für den System- und Software-Entwicklungsprozess vor, um eine Zertifizierung des entwickelten Systems zu ermöglichen. Der Systemersteller definiert auf der Basis dieser Standards einen durchgängigen und angemessenen Entwicklungsprozess, dessen strikte Einhaltung über den gesamten Produktlebenszyklus hinweg nachgewiesen werden muss.

Ausgehend von den operationellen Anforderungen an eine komplexe Flugzeug-Cockpit-Anwendung werden in diesem Vortrag wichtige Entwicklungsprozessschritte präsentiert und erläutert, die von der Systemanalyse über Systemdesign, Subsystemdesign, Softwareanalyse bis hin zum Softwaredesign reichen. Im Entwicklungsfluss werden Erkenntnisse, die bei der Entwicklung von komplexen und sicherheitskritischen Avionikarchitekturen gewonnen wurden, dargestellt.

Inhalt

- EADS – Cassidian – Cassidian Electronics
- Standards für Systementwicklung in der Avionik
- *Development Assurance Levels*
- Systementwicklungsmethode anhand eines Beispiels
- Prozessvorgaben RTCA/DO-178B
- Erkenntnisse und *Lessons Learned*

EADS Management Structure

Bodo Uebber — *Chairman of the Board of Directors*

Louis Gallois — *Chief Executive Officer (CEO)*

Finance	Strategy & Marketing	Chief Technical Officer	EADS North America	Human Resources
Hans-Peter Ring	Marwan Lahoud	Jean J. Botti	Sean O'Keefe	Jussi Itävuori

Coordination CASSIDIAN EADS Astrium

François Auque

Airbus

Tom Enders (CEO)
Fabrice Brégier (COO)

Airbus Military
Domingo Ureña-Raso

Eurocopter

Lutz Bertling (CEO)

Cassidian

Stefan Zoller (CEO)

EADS Astrium

François Auque (CEO)

CASSIDIAN

A comprehensive portfolio to meet operational needs

Electronics / Subsystems | **Platforms / Systems** | **Lead Systems Integration**

Cassidian Electronics

- Detection
- Mission Avionics
- Services

Cassidian Air Systems

- Combat Air Systems
  - Eurofighter
- Mission Air Systems
  - Unmanned Aerial Vehicles (UAVs)
- Services
  - System Support, MRO, Upgrades
  - Aircrew, Groundcrew, Air Defence Training
  - Integrated Logistics Support (ILS)
  - Integrated Support Services (ISS)

MBDA*

- Ground Based Air Defence (GBAD)
- Air Dominance
- Maritime Superiority
- Battlefield Engagement

* 37.5% EADS shareholding Joint Venture with BAE Systems and Finmeccanica)

Cassidian Systems

- Integrated Systems
  - Intelligence
  - Air Defence
  - Land and Joint
  - Secure Information Infrastructure
  - Critical National Infrastructure.
  - Border Security
  - Naval Systems (Sofrelog & Atlas)
- Risk Management of Complex Systems (Apsys)
- Security & Communication Solutions
  - Secure Networks
  - PMR Products
  - Security Products
  - Control Rooms
- Services
  - ILS/ ISS
  - Managed services

System Design Centre

Services / Through-life product and systems support

CASSIDIAN
AN EADS COMPANY

CASSIDIAN Electronics

With highly qualified employees around the globe, Defence Electronics develops and produces high-end electronics for different platforms in order to support its customers' missions.

- **Detection**
- **Mission Avionics**
- **Test & Services**

CASSIDIAN
AN EADS COMPANY

Beispiel eines Cockpits: A380

Quelle: http://www.airbus.com/galleries/photo-gallery/

Standards für sicherheitskritische, … und komplexe Systeme in der Avionik

Für sicherheitskritische, hoch integrierte und komplexe Systeme in der Luftfahrtindustrie sind unter anderem folgende Entwicklungsstandards zu berücksichtigen:

- SAE ARP 4754 *Certification Considerations for Highly-integrated or Complex Aircraft Systems*
- SAE ARP 4761 *Guidelines and Methods for Conducting the Safety Assessment Process for Civil Airborne Systems and Equipments*
- RTCA/DO-178B *Software Considerations in Airborne Systems and Equipment Certification*
- RTCA/DO-160 *Design Assurance Guidance for Airborne Electronic Hardware*
- ARINC 653 *Avionics Application Software Standard Interface*
- ARINC 661 *Cockpit Display System Interfaces to User Systems*

Der Systementwicklungsprozess nach SAE ARP 4754

Das Dokument SAE ARP 4754 *Certification Considerations for Highly-integrated or Complex Aircraft Systems* gibt Anleitungen (Empfehlungen) zu Zertifizierungsaspekten für hoch integrierte oder komplexe Systeme, die in Flugzeuge eingebaut werden. Dabei werden das operationelle Umfeld als auch die Flugzeugfunktionen betrachtet. Das Dokument SAE ARP 4754 ist eine *Guideline* für Zertifizierer (*certification authority*) und Systemersteller.

Die beschriebenen Konzepte im SAE ARP 4754 stammen von Vertretern aus den verschiedenen Bereichen zivile Avionik, Flugzeugstruktur, Flugzeugtriebwerk und Behörden.

Die Anleitungen im SAE ARP 4754 können auf einfachere Systeme angewendet werden, dann sollten aber die formalen Prozesse der Entwicklung und deren Dokumentationsumfang signifikant reduziert werden.

Auch hier gilt das Prinzip der Angemessenheit des Entwicklungsprozesses in Bezug auf das zu entwickelnde Produkt.

SAE ARP 4754 Bezug zu anderen Standards

Für die Softwareentwicklung wird auf das Dokument RTCA/DO-178B *Software Considerations in Airborne Systems and Equipment Certification* verwiesen. Auf die Inhalte von DO-178B wird später noch eingegangen.

Für die Methoden der Sicherheitsanalysen und Prozesse wird auf das Dokument SAE ARP 4761 *Guidelines and Methods for Conducting the Safety Assessment Process for Civil Airborne Systems and Equipments* verwiesen. Der Inhalt spielt für diesen Vortrag nur eine geringe Rolle.

Für die HW-Entwicklung wird das RTCA-Dokument mit dem Arbeitstitel „*Design Assurance Guidance for Airborne Electronic Hardware*“ angegeben (heute mit der Nummer DO-160).

Wasserfallmodell vs. iterativen Prozess

Im ARP 4754 wird der Wasserfallprozess (*top-down sequence*) als ein zweckmäßiges konzeptionelles Modell für einen Systementwicklungsprozess, zur Implementierung einer Flugzeugfunktion, beschrieben. Typische iterative Systementwicklungsprozesse verwenden *top-down* und *bottom-up* Strategien.

Wegen der Komplexität der einfachsten Flugzeugsysteme ist der zugeordnete Systementwicklungsprozess eher zyklisch (iterativ) als sequenziell zu sehen.

Wie ARP 4754 wird in diesem Vortrag ein Wasserfallprozess dargestellt, da er für die gegebene kurze Zeit leichter zu erfassen ist.

ARP 4754 generische Systementwicklungsprozessschritte

Der ARP 4754 nennt die folgenden generischen Systementwicklungsprozess-schritte:

(1) Identifikation der Flugzeugfunktionen (*aircraft-level functions*), funktionalen Anforderungen und funktionalen Schnittstellen
(2) Feststellung der funktionalen Fehlerkonsequenzen und Auswirkungen
(3) Zuweisung (*allocation*) der Funktionen auf Systeme und Personen
(4) Design der Systemarchitektur und Zuweisung der Anforderungen auf (System-) Elemente
(5) Zuweisung der Systemelementanforderungen auf Hardware und Software
(6) Erstellung der Hardware und Software
(7) Integration der Hardware und Software
(8) Integration des Systems.

ARP 4754 *Development Assurance*

Development Assurance (Unterstützungsprozesse) soll sicherstellen, dass Fehler und Lücken in Anforderungen und Design entdeckt werden und soweit beseitigt werden, dass das implementierte System die geforderten Zertifizierungsanforderungen erfüllt. Der ARP 4754 nennt die folgenden generischen *Development Assurance*-Schritte:

(1) Certification Coordination
(2) Safety Assessment
(2) Requirements Validation
(3) Implementation Verification
(4) Configuration Management
(5) Process Assurance
(6) Integration der Hardware und Software
(7) Integration des Systems.

Development Assurance Levels

Systemen und Systemelementen (zum Beispiel Geräte, Software-Konfigurationseinheiten) werden *Development Assurance Levels* zugeordnet. Diese richten sich nach der Einstufung des Fehlereffekts in Bezug auf die zu implementierende Flugzeugfunktion (*aircraft level function*).

Die geforderte Strenge und Disziplin der *Development Assurance* für die Entwicklung eines Systems oder Systemelements richtet sich nach dem *Development Assurance Level* (DAL).

Failure Condition/Effect (Hazard) Classification	**DAL**	**Safety Objective Requirement[1]**
Catastrophic	A	$P< 10^{-9}$
Hazardous/Severe Major	B	$P< 10^{-7}$
Major	C	$P< 10^{-5}$
Minor	D	None
No safety effect	E	None

Wird festgelegt durch die Systemarchitektur und dem *Preliminary Safety Assessment* (PSSA).

[1] pro Flugstunde

Anforderungsgetriebener Entwicklungsprozess

Motivation:

Von einem Avioniksystem wird verlangt, dass es nur die beabsichtigten Funktionen ausführt (funktionale Anforderungen) und die definierten Eigenschaften (Qualitätsanforderungen) erfüllt und nur diese.

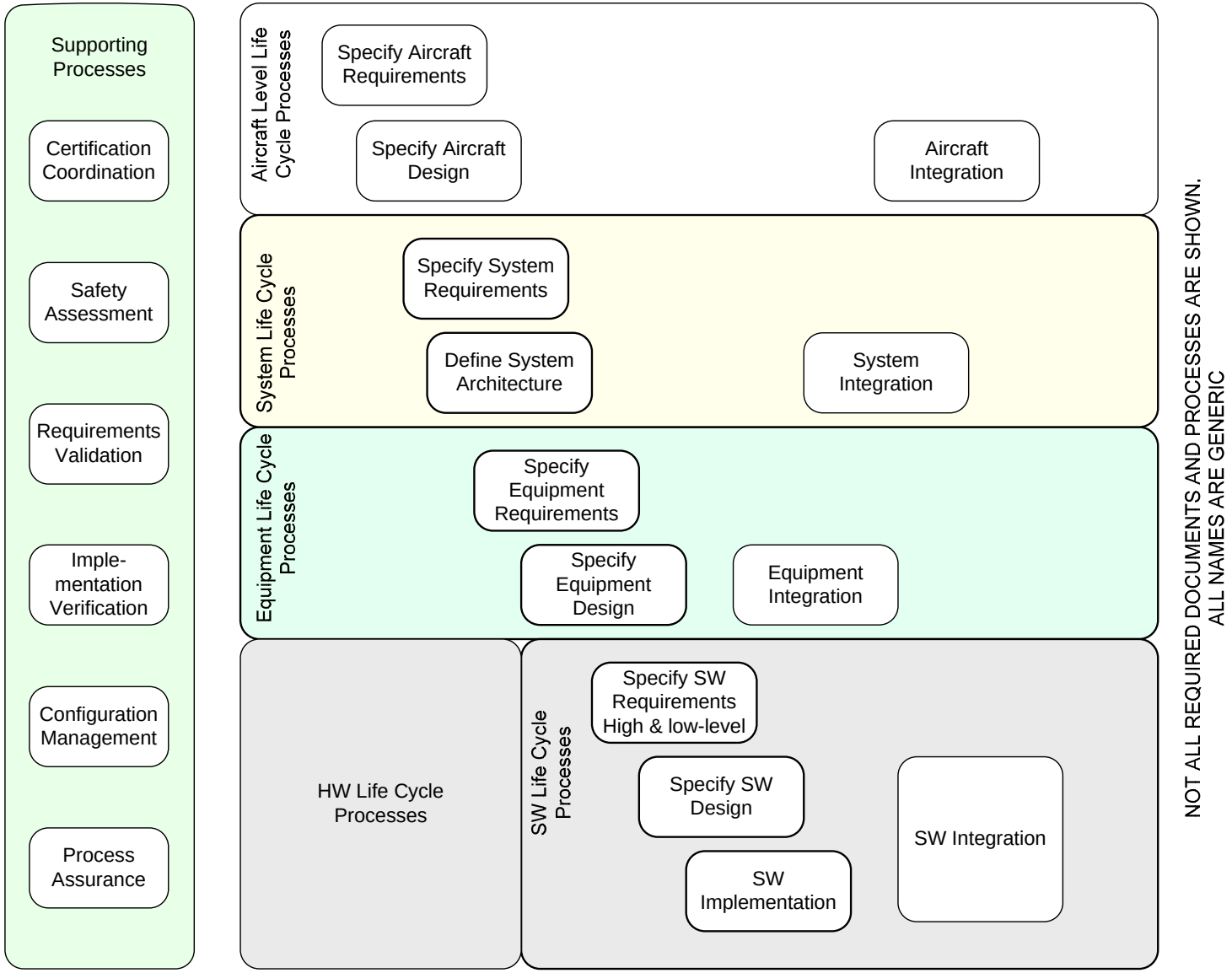
Darüber hinaus müssen in der Architektur und Implementierung Vorkehrungen für das Unerwartete getroffen werden.

Nur so ist Verhalten von Avioniksystemen verstehbar und damit vorhersagbar.

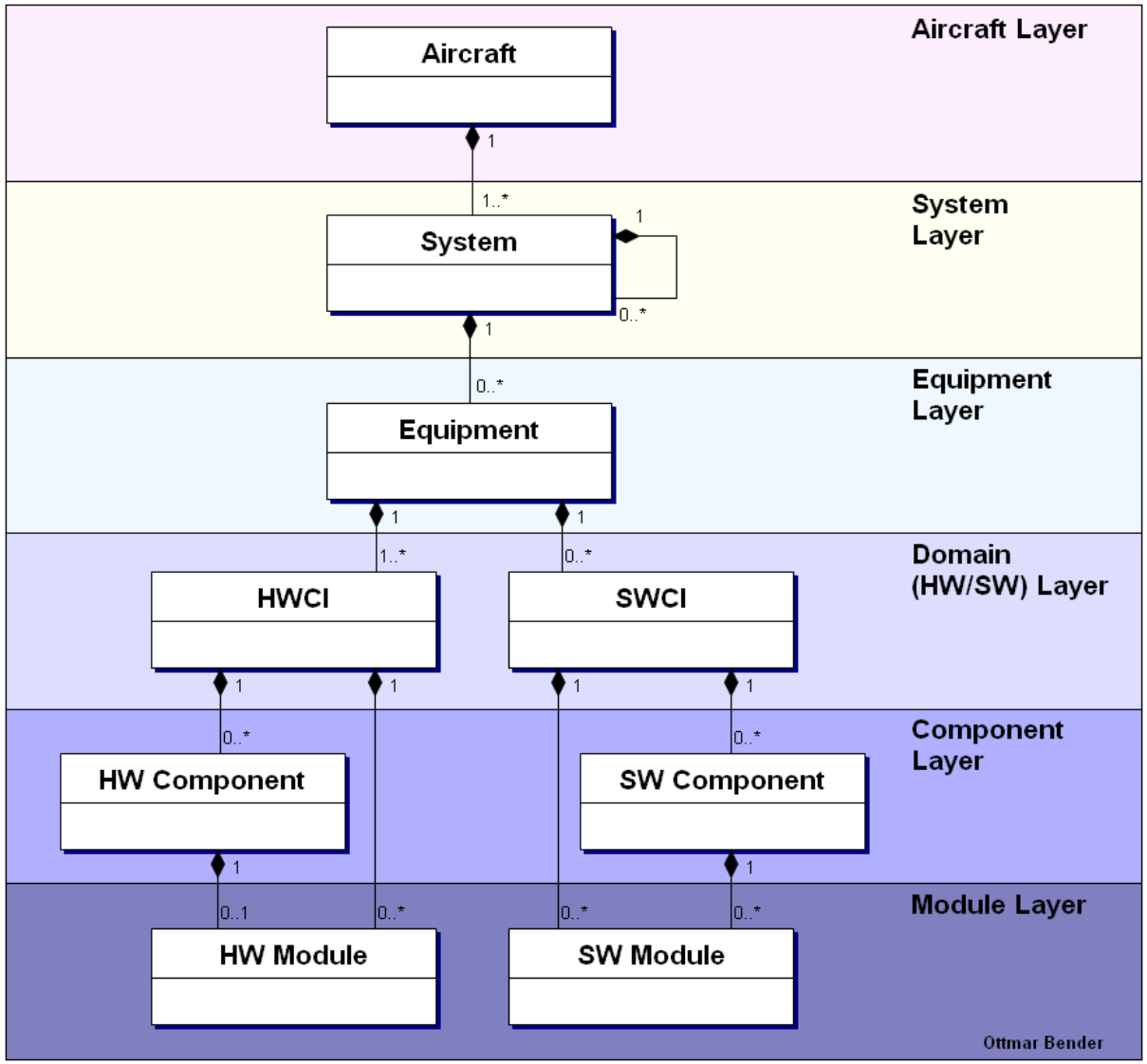
Das bedeutet:

- Es dürfen nur akzeptierte Anforderungen implementiert werden.
- Die Anforderungen müssen bis zur Implementierung verfolgt werden.
- Es darf keine Implementierung ohne Anforderungen geben. Um das sicher zu stellen, muss die Implementierung zu den Anforderungen zurück verfolgt werden.

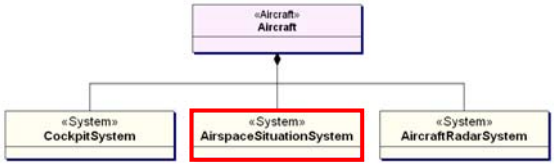
Systementwicklungsprozess

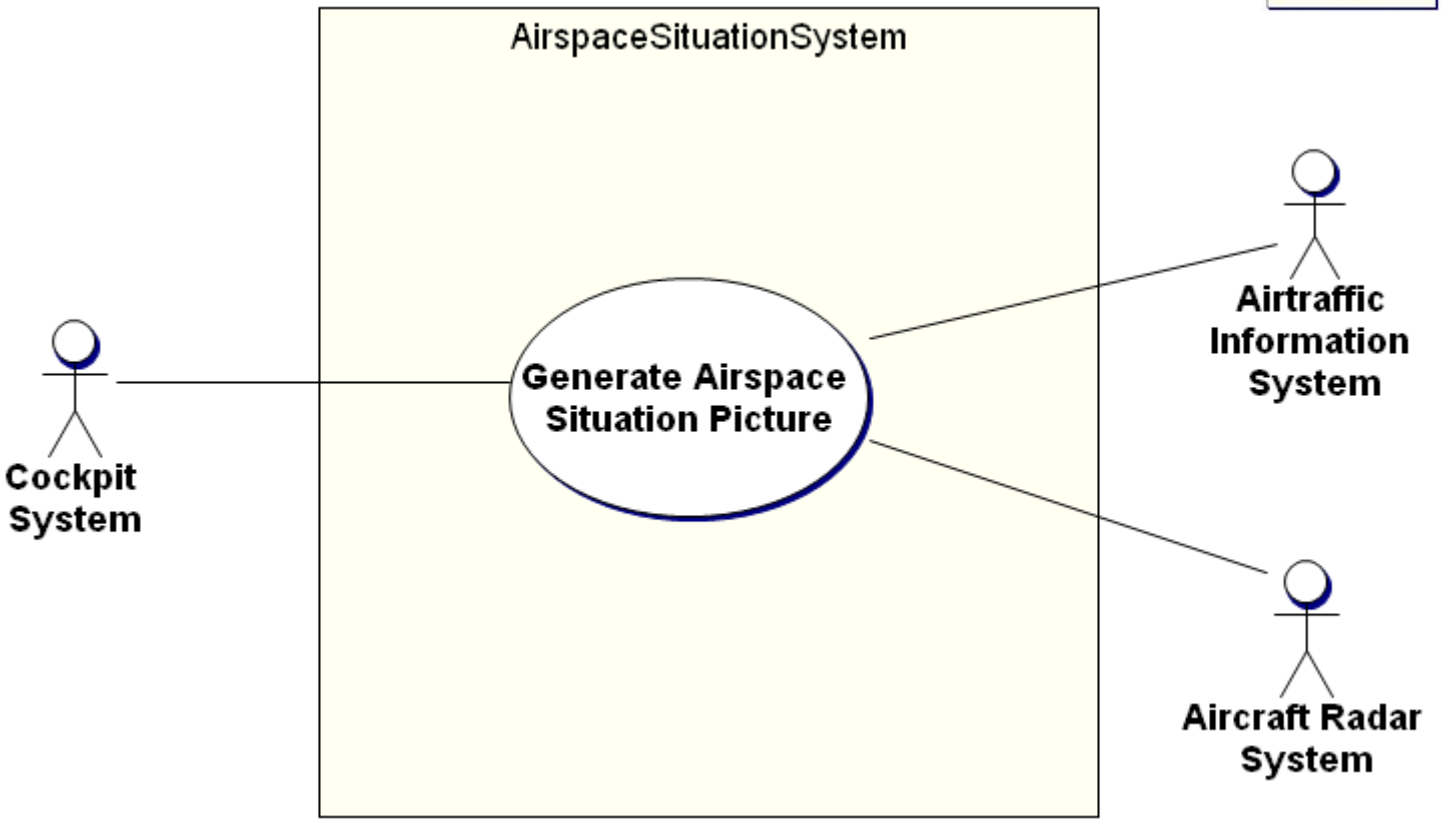


System, Systemelemente und Abstraktionsebenen

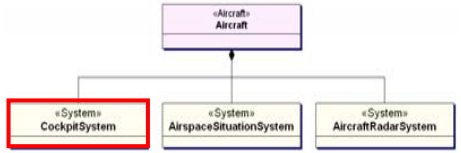


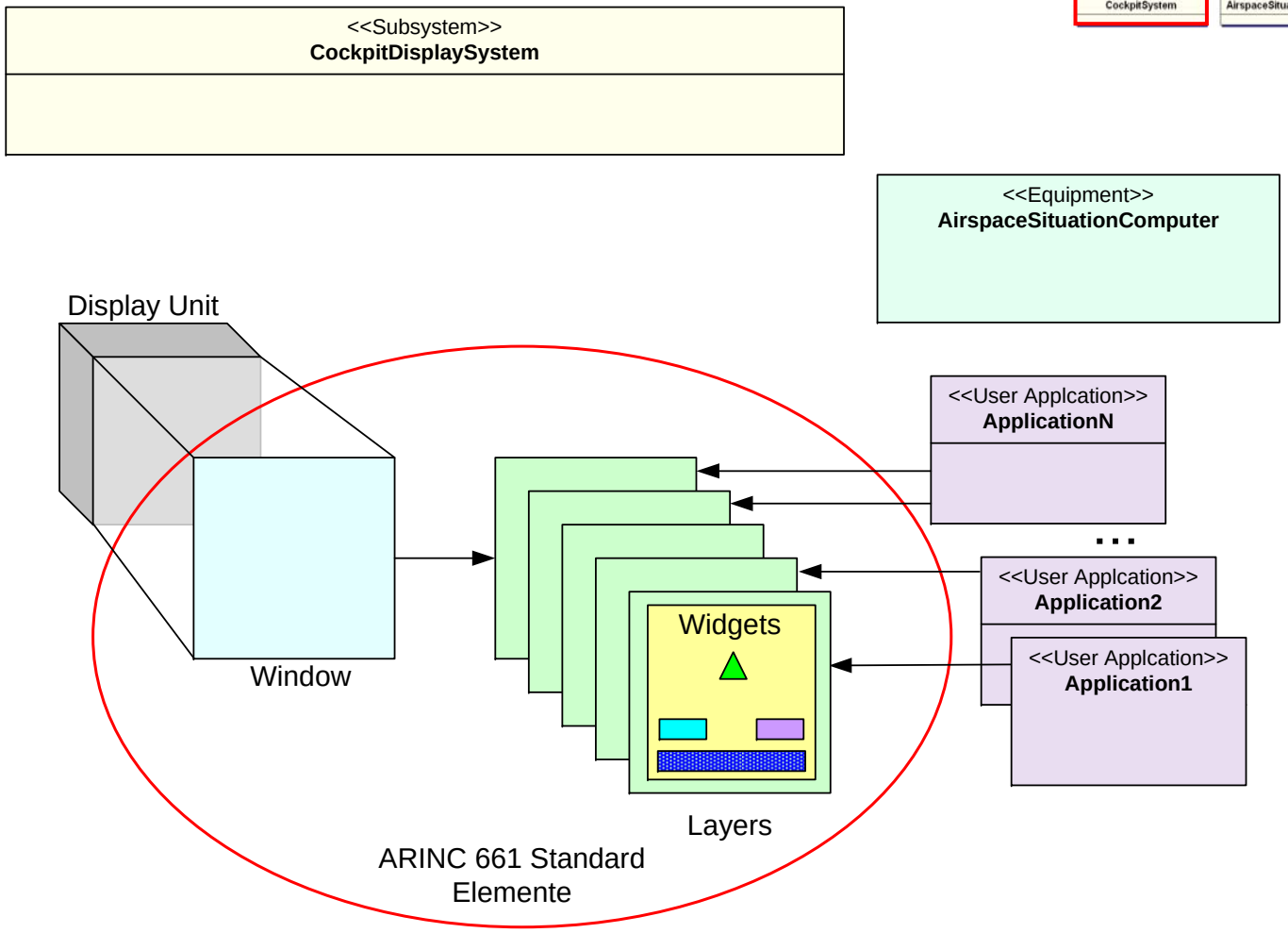
AirspaceSituationSystem-Kontext





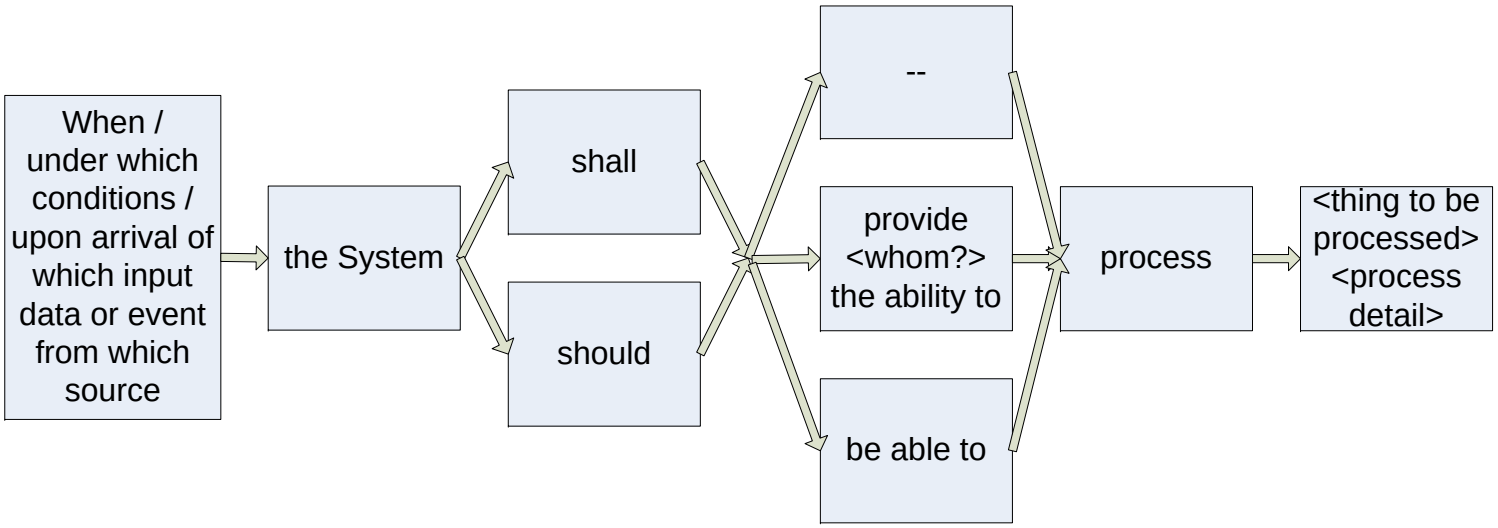
Partitionierung der verschiedenen Anzeigen durch ARINC 661 Technologie





Quelle: ARINC 661 Standard.

Wie kommt man zu guten Anforderungen?



Source of quotation: [Cassidian RfA No. PE-0258-EN]
[Rupp 2009]

Übergang zur Software Prozessvorgaben RTCA/DO-178B

CASSIDIAN
AN EADS COMPANY

Was ist RTCA/DO-178B?

Der RTCA/DO-178B Software Considerations in Airborne Systems and Equipment Certification) kurz DO-178B:

- ist ein Softwarestandard, herausgegeben von der RTCA (Radio Technical Commission for Aeronautics)
- wurde von der RTCA SC-167 und EUROCAE (European Organization for Civil Aviation Equipment) zusammen erstellt. Die EUROCAE hat dem Standard die Bezeichnung ED-12B geben.
- ist ein Konsensus der internationalen Luftfahrt.
  Bei der Erstellung waren amerikanische, kanadische und europäische Firmen und Zulassungsbehörden involviert.

Der DO178B-Standard gibt „*guidelines*“ für die Software-Entwicklung für Luftfahrtsysteme und Geräte, die ihre beabsichtigte Funktion mit einem Grad an Vertrauen in die funktionale Sicherheit (Safety) gemäß den Luftfahrtzulassungsanforderungen erfüllt. Die *guidelines* bestehen aus:

- Zielen (objectives) an den Software-Entwicklungsprozess
- Aktivitäten und Designberücksichtigungen, um diese Ziele zu erreichen
- Nachweise, die zeigen, dass die Ziele erreicht wurden.

DO-178B *Objectives* z.B. Table A-3 *Verification Of Outputs of Software Requirements Process*

	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Software high-level requirements comply with system requirements.	6.3.1a	●	●	❍	❍	Software Verification Results	11.14	②	②	②	②
2	High-level requirements are accurate and consistent.	6.3.1b	●	●	❍	❍	Software Verification Results	11.14	②	②	②	②
3	High-level requirements are compatible with target computer.	6.3.1c	❍	❍			Software Verification Results	11.14	②	②		
4	High-level requirements are verifiable.	6.3.1d	❍	❍	❍		Software Verification Results	11.14	②	②	②	
5	High-level requirements conform to standards.	6.3.1e	❍	❍	❍		Software Verification Results	11.14	②	②	②	
6	High-level requirements are traceable to system requirements.	6.3.1f	❍	❍	❍	❍	Software Verification Results	11.14	②	②	②	②
7	Algorithms are accurate.	6.3.1g	●	●	❍		Software Verification Results	11.14	②	②	②	

LEGEND:		
	●	The objective should be satisfied with independence.
	❍	The objective should be satisfied.
	(blank)	Satisfaction of objective is at applicant's discretion.
	①	Data satisfies the objectives of Control Category 1 (CC1).
	②	Data satisfies the objectives of Control Category 2 (CC2).

Source of quotation: [RTCA/DO-178B]

DO-178B *Software Life Cycle Data*

- **Planning**
  - Plan for Software Aspects of Certification
  - Software Development Plan
  - Software Verification Plan
  - Software Configuration Management Plan
  - Software Quality Assurance Plan
- **Standards**
  - Software Requirements Standards
  - Software Design Standards
  - Software Code Standards
- **Development**
  - Software Requirements Data
  - Design Description
  - Source Code
  - Executable Object Code
- **Verification**
  - Software Verification Cases and Procedures
  - Software Verification Results
- **Configuration Management**
  - Software Life Cycle Environment Configuration Index
  - Software Configuration Index
  - Problem Reports
  - Software Configuration Management Records
- **Quality Assurance**
  - Software Quality Assurance Records
- **Software Accomplishment Summary**
  - Software Accomplishment Summary

Lessons learned (1)

- Zur Formulierung der Anforderungen muss der Beschreibungskontext klar sein.
- Es darauf zu achten, dass die Anforderungen auf der richtigen Abstraktionsebene formuliert werden.
- Anforderungsschablonen sind ein gutes Hilfsmittel, um zu guten Anforderungen zu kommen.
- Mit den Anforderungen werden am besten gleich die Testfälle definiert und damit das Verifikations-Team aufgebaut.
- Anforderungen müssen *Black-box*-testbar sein.

Lessons learned (2)

- Bei der Erstellung der Architektur ist besonders auf die Qualitätsanforderungen zu achten.
- Frühe Prototypen helfen bei der Validierung, Performanzabschätzung und Risikoreduzierung.
- Ein sorgfältiges Nebenläufigkeitskonzept reduziert das Risiko von Re-Design wegen problematischen dynamischen Effekten (z.B. durch zu viele Prozesse).
- Kooperation der verschiedenen Disziplinen (z.B. System, Equipment, SW und Verifikation) ist essentiell.
- Lernkurve durch Schulung und Experten unterstützen.
- Test- und Integrationsumgebung frühzeitig aufbauen.
- Problem-Lösungs-Workflow aufsetzen.
- Ziel-HW muss Test- und Debugging-Möglichkeiten bieten.
- Anforderungen müssen zum Test quantitative Spezifikationsanteile besitzen.

Glossar (1)

Analyse	Eine Analyse ergibt einen wiederholbaren Nachweis der Korrektheit einer Prüfung
ARP	Aerospace Recommended Practice
DAL	Development Assurance Level
DCS	Designated Certification Specialist
EUROCAE	Die European Organization for Civil Aviation Equipment oder kurz EUROCAE ist das europäische Pendant zur RTCA
Review	Ein Review ergibt ein qualitatives Ergebnis für die Korrektheit einer Prüfung.
PSAC	Plan for Software Aspects of Certification
PSSA	Preliminary Safety Assessment

Glossar (2)

RMS	Rate Monotonic Scheduling
RTCA inc.	(Radio Technical Commission for Aeronautics) ist eine private und gemeinnützige Gesellschaft, die konsensusbasierte Empfehlungen für Kommunikation, Navigation, Überwachung im Luftverkehr und Systemthemen im Luftverkehrsmanagement (CNS/ATM) entwickelt. Die RTCA inc. hat ihren Sitz in Washington.
SAE	Society of Automotive Engineers
SC	Special Committee
SWCI	Software Configuration Item
WCET	Worst Case Execution Time

Literatur (1)

- [ARINC 653-2003] ARINC 653
  ARINC 653 Avionics Application Software Standard Interface,
  AERONAUTICAL RADIO, inc., 2003

- [ARINC 653-2002] ARINC 661
  ARINC 661 *Cockpit Display System Interfaces to User Systems*
  AERONAUTICAL RADIO, inc., 2002

- [Cassidian RfA No. PE-0258-EN] Cassidian Electronics
  Cassidian Electronics, EADS Deutschland GmbH

- [Habli]
  Ibrahim Habli Overview of Current Progress with DO-178C,
  The University of York

- [INCOSE 2010] INCOSE,
  Systems Engineering Handbook v3.2, 2010]

Literatur (2)

- [ISO/IEC 12207-2008] ISO/IEC
  Systems and software engineering — Software life cycle processes
  2008

- [ISO/IEC 15288-2008] ISO/IEC
  Systems and software engineering — System life cycle processes
  2008

- [SysML 2010] OMG SysML™
  OMG Systems Modeling Language (OMG SysML™)
  formal/2010-06-01, Version 1.2
  Standard Specification URL: http://www.omg.org/spec/SysML/1.2/, 2010

- [RTCA/DO-178B] RTCA inc.,
  Software Considerations in Airborne Systems and Equipment Certification,
  RTCA,1992.

Literatur (3)

- [Rupp 2009] Chris Rupp
  Requirements-Engineering und Management
  Carl Hanser Verlag München
  ISBN 978-446-41841-7, 2009

- [SAE ARP 4754-1996] SAE inc.,
  Certification Considerations for Highly-integrated or Complex Aircraft Systems.
  SAE inc, 1996.

- [SAE ARP 4761-1996] SAE inc.,
  Guidelines and Methods for Conducting the Safety Assessment Process for Civil Airborne Systems and Equipments.
  SAE inc., 1996.

- [Sommerville] Ian Sommerville
  Software Engineering 7,
  Pearson Addison Wesley, ISBN 0-321-21026-3, 2004

Thank you for your attention!

CASSIDIAN
AN EADS COMPANY