Technische Universität Berlin
Institute for
Aeronautics & Astronautics

Robert Luckner
Flugmechanik,
Flugregelung und Aeroelastizität

4 April 2006

Flugführungssysteme zur Pilotenassistenz - Was kann man aus der Luftfahrt lernen?

2. Tagung: Aktive Sicherheit durch Fahrerassistenz, TU München

Übersicht

- **Einleitung**
- **Systementwicklung**
  - Sicherheitsforderungen
  - Entwurfsprinzipe
- **Entwicklungsprozess**
  - V-Modell
  - Softwareentwicklung
- **Zusammenfassung**

1. Einleitung

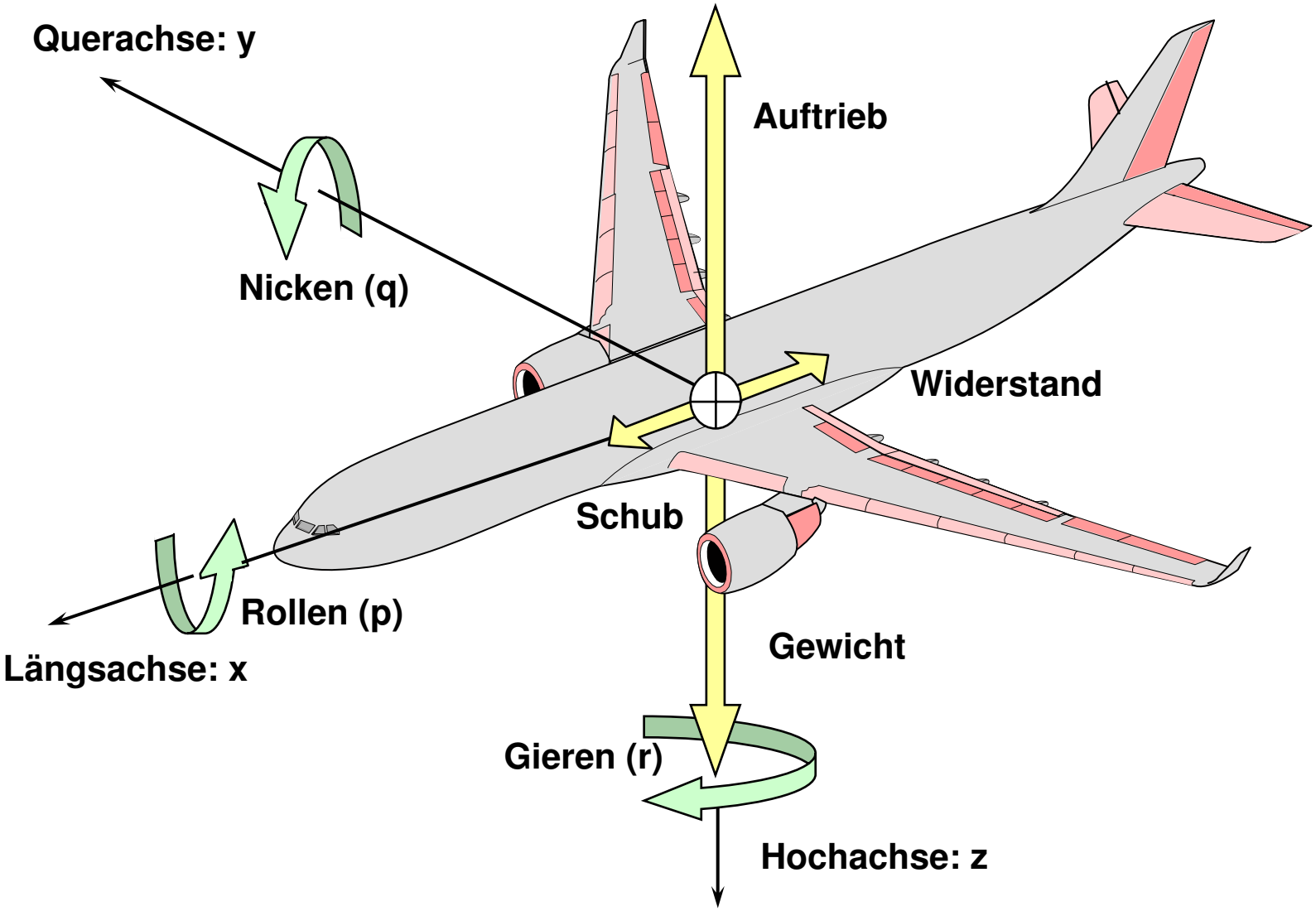
- Assistenzsysteme
  Systeme, die den Fahrer beim Führen eines Fahr-/ Flugzeugs unterstützen

- Unterteilung in:
  - sicherheitskritisch
  - nicht sicherheitskritisch (Komfort erhöhend)

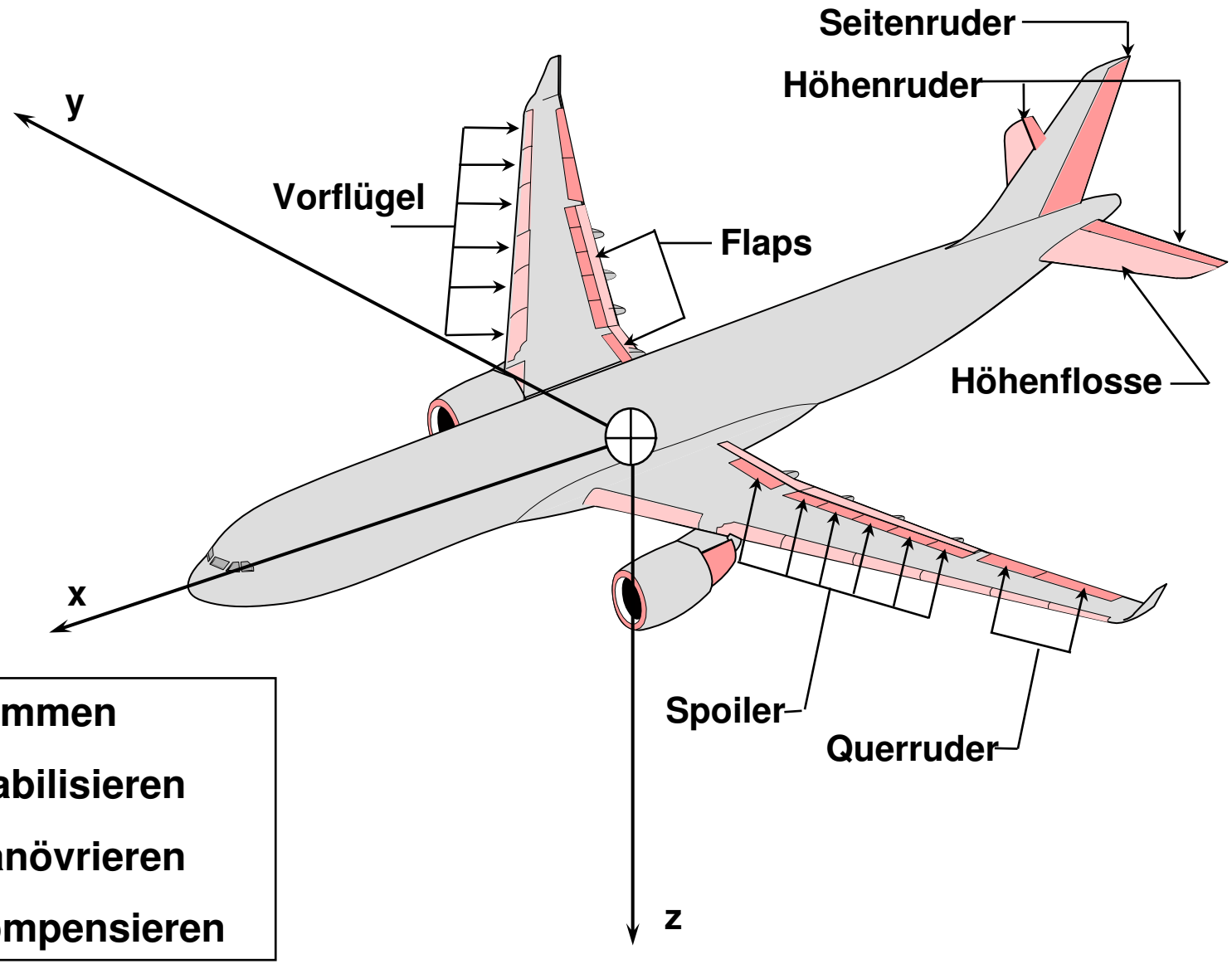
- Herausforderung:
  komplex, sicherheitskritisch, verfügbar

- Frage: Wie schafft es die Luftfahrt solche Systeme zuzulassen?
  Luftfahrt hier: zivile Verkehrsflugzeuge größer 5,7to

Wie wird ein Flugzeug gesteuert?

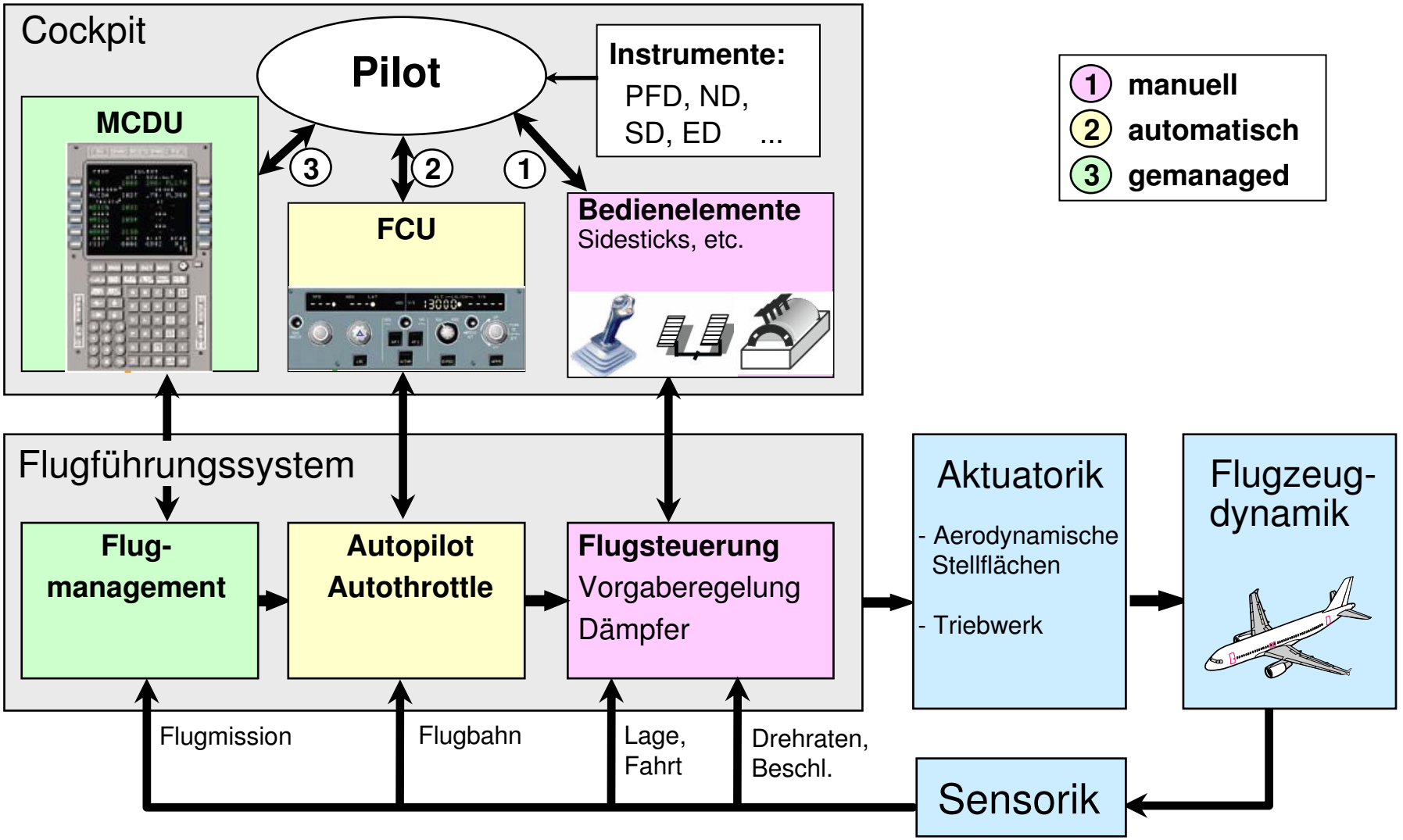


Stellflächen zur Flugsteuerung



- Trimmen
- Stabilisieren
- Manövrieren
- Kompensieren

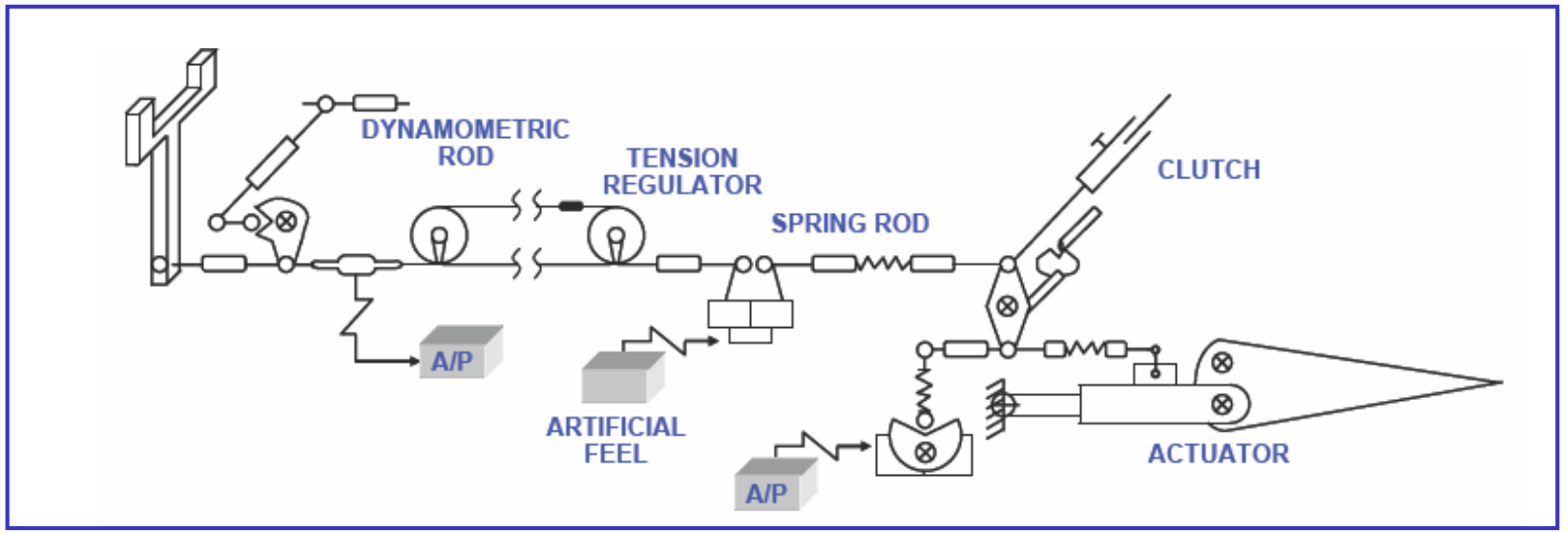
Architektur des Flugführungssystem



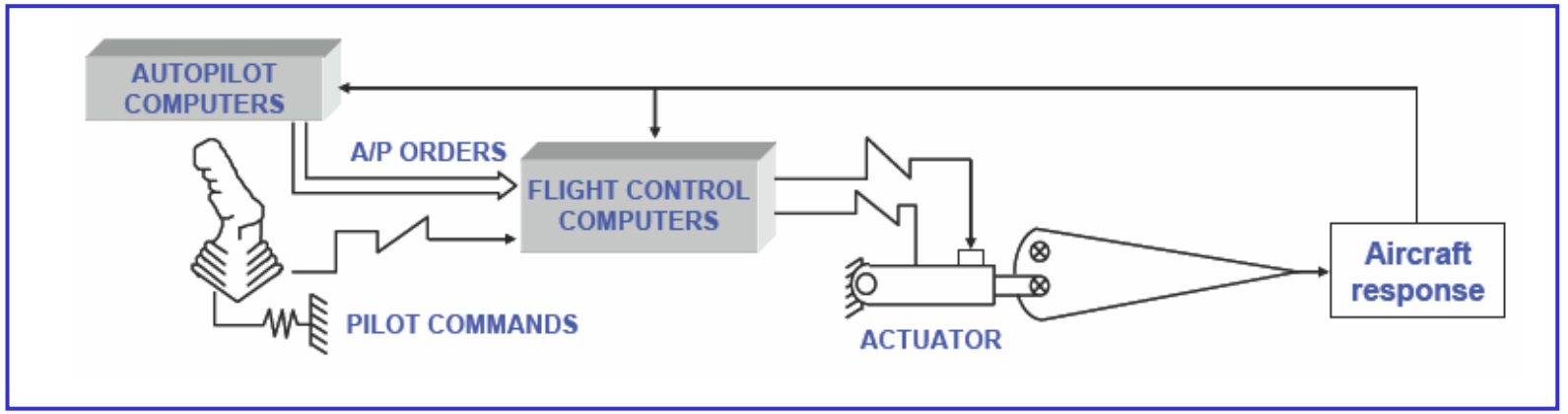
Mensch-Maschine-Schnittstelle

Cockpit A380:

Mechanische Steuerung



Elektrische Steuerung



Funktionen am Beispiel des Flugsteuerungssystems

- Steuerung (manuell, automatisch),
- Dämpfung, Störunterdrückung
- Vorgaberegelung
- Schützen vor Strukturüberlastung, vor Überschreiten von Grenzwerten, vor Verlust der Steuerbarkeit
- Ausregeln von Fehlern (Triebwerksausfall, Reifenplatzer, …)

Ziel: Verringerte Arbeitsbelastung, erhöhte Sicherheit und Effizienz

Unterschiede

	Luftfahrt	Automobiltechnik
Bewegung	Raum (3D)	Fläche (2D)
Pilot / Fahrer	2 (Profis)	1 (Amateure u. Profis)
Wetter	Allwetter, ohne Sicht	Allwetter, mit Sicht
Phasen	Start, Steig- Reise-, Sinkflug, Landung	Stadt, Autobahn, Landstraße, Parken
Stückzahlen	↘ 10^3	↗ 10^6
Kosten (Elektronik)	↗ 10.000 €/kg	↘ 1000 €/kg
Frequenz der Modellwechsel	↘ 20 Jahre	↗ 2 Jahre
Unfalluntersuchungen	sehr aufwendig	
Wartung, Reparatur	zugelassene Betriebe	

Kommerzielle Jet-Flotte 2004: etwa 19.000 Flugzeuge

1959-2004: 1402 Unfälle mit 25.664 Toten

2. Systementwicklung

Airbus Corporate Safety Vision:

"Safety in Air travel is the Airbus' absolute priority and takes precedence over every other aspect of our business. For Airbus, Safety is a question of ethics, and we spare no effort to ensure that air travel continues to be the safest means of transport ."

Noël Forgeard

Sicherheitsziele

Das Auftreten eines Fehlers mit katastrophalen Konsequenzen muss <u>extrem unwahrscheinlich</u> sein

- **Flugzeug:**
  Katastrophaler technischer Fehler, Wahrscheinlichkeit $< 10^{-7}$ 1/fh

- **System:**
  Katastrophaler technischer Fehler, Wahrscheinlichkeit $< 10^{-9}$ 1/fh

Annahme:
Es existieren 100 Bedingungen für Fehler mit katastrophalen Konsequenzen in allen Systemen eines Flugzeuges

Sicherheitsziele

Flugsteuerung: a “safety driven design”

Katastrophale Konsequenzen können aus Fehlern resultieren wie:

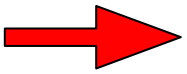
- unbegrenztes Weglaufen einer Stellfäche,
- Verlust der Steuerung um die Nickachse,
- oszillierender Fehler mit einer Frequenz, die kritisch für die Struktur ist,
- nicht ausreichend laterale Steuerwirkungsamkeit nach Triebwerksausfall.

Alle diese Fehler sollen „*Extremely Improbable (<10^{-9} / flight hour)*“ sein und dieses muß den Luftfahrtbehörden für die Zertifizierung demonstriert werden

Die Demonstration wird durch eine komplette, detaillierte und dokumentierte Sicherheitsanalyse unterstützt, die von Anfang an eine der wesentlichen Säulen des System-Entwicklungsprozesses ist

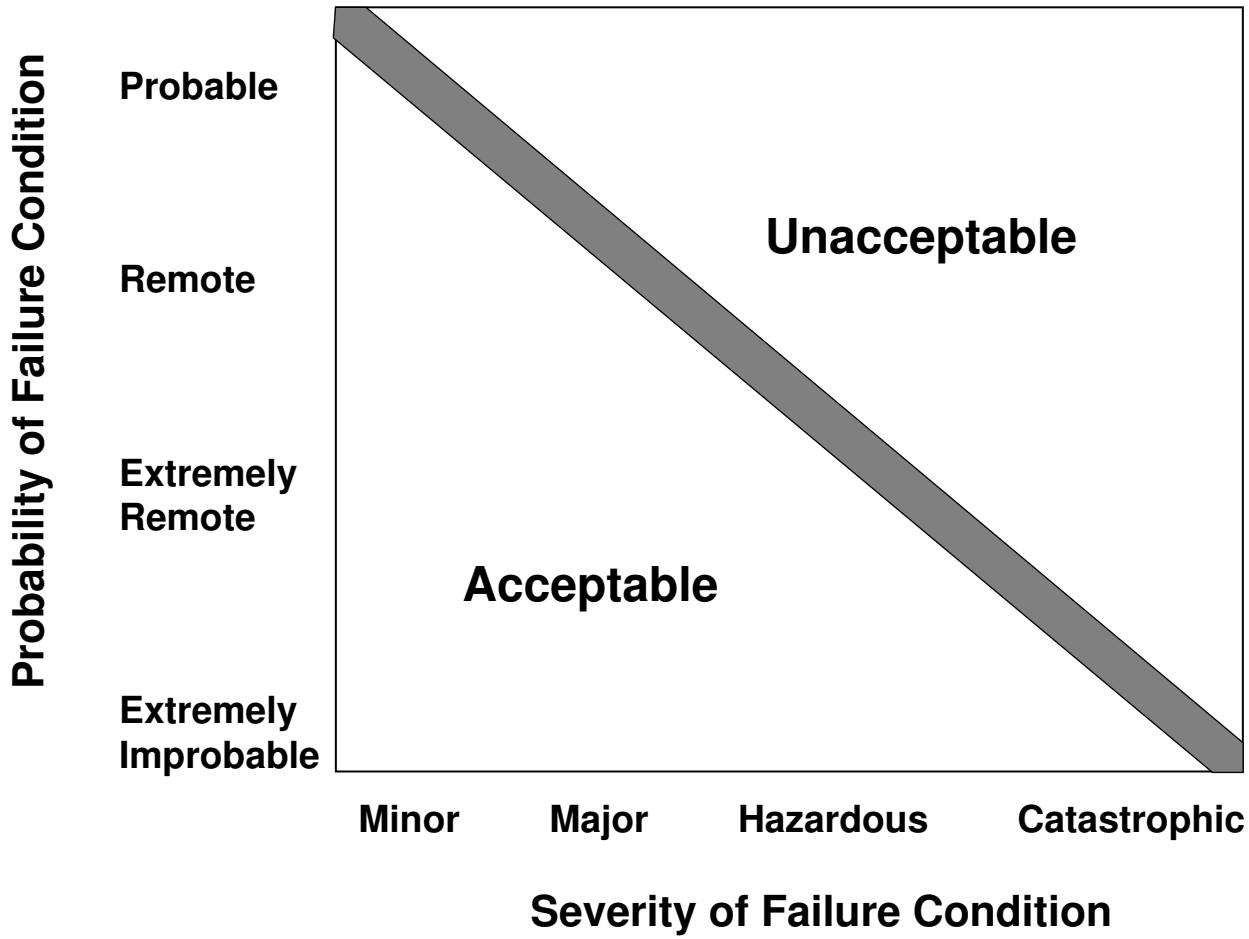
Luftfahrtbauvorschriften

FAR Part 25	**Airworthiness Standards, Transport Category Airplanes**	
EASA CS-25	**- Subpart B: Flight**	**25X20 - 25X261**
	- Subpart D: Design and Construction	**25.601 - 25.X899**
	- Subpart F: Equipment	**25.1301 - 25.1315**
SC	**Special Conditions (Airbus A340: ≈30 SC's)**	
AC	**Advisory Circular (FAR)**	
ACJ	**Acceptable Means of Compliance and Interpretations**	
AMJ	**Advisory Material Joint**	
EASA CS-AWO	**All Weather Operation**	



Certification Basis of an Aircraft

Zusammenhang Fehlerwahrscheinlichkeit und Schwere



Fehler-Kategorien

Fehler-Kategorien nach EASA CS-25.1309 (AMC)

Classification	Probability [1/fh]	Consequences		
		Crew	Passenger	Aircraft
Minor	$\geq 10^{-2}$ 10^{-2}-10^{-3}	**normal**	normal	not affected
	10^{-3}-10^{-5}	**slight increase** in crew workload	some inconvenience	slight reduction in safety margins or functional capabilities
Major	10^{-5}-10^{-7}	**significant increase** in crew workload or in conditions impairing crew efficiency	discomfort to occupants possibly including injuries	significant reduction in safety margins or functional capabilities
Hazardous	10^{-7} - 10^{-9}	**physical distress** or higher workload such that the crew cannot be relied upon to perform their tasks accurately or completely	serious or fatal injury to a relatively small number of the occupants.	large reduction in safety margins or functional capabilities
Catastrophic	$\leq 10^{-9}$	**unable to control** the a/c	multiple deaths	loss of a/c

Software-Klassifikation

Software-Klassifikation nach RTCA DO-178B

Failure Condition	Software Level
catastrophic	A
hazardous	B
major	C
minor	D
no effect	E

Illustration der Sicherheitsziele

Events caused by a system failure:

Failure Effect	Probability	Number	Events Based on 4000 Flight hours per aircraft and year
minor	$< 10^{-3}$ 1/fh	1 aircraft	4 per year
major	$< 10^{-5}$ 1/fh	100 aircraft (fleet of an airline)	4 per year
hazardous	$< 10^{-7}$ 1/fh	1000 aircraft (all a/c of one type)	2 in 5 years
catastrophic	$< 10^{-9}$ 1/fh	1000 aircraft in 20 years (80,000 fh)	0.08 during life cycle of an a/c type (50 years)

Spezifikationen und Standards

SAE (Society of Automotive Engineers) **http://www.sae.org**

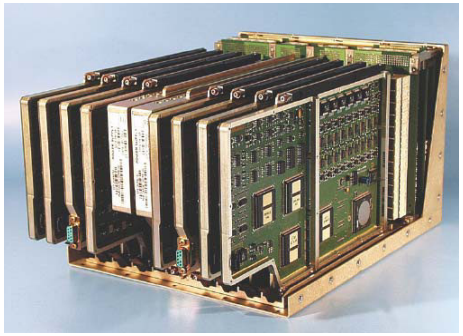
ARP 4754	Certification Considerations for Highly-Integrated Or Complex Aircraft Systems November 1996
ARP 4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment December 1996

RTCA (Radio Technical Corporation of America) **http://www.rtca.org**

RTCA DO-178 B	Software Considerations in Airborne Systems and Equipment Certification
RTCA DO-254	Design Assurance Guidance for Airborne Electronic Hardware
RTCA DO-297	Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations

Bestandteile des Flugsteuerungssystems

- Bedienelemente im Cockpit
- Anzeige-Instrumente
- Sensorik
- Aktuatorik, Stellflächen
- Computer
- Software
- Datenbusse
- Energieversorgung (hydraulisch, elektrisch)



„Goldene Regeln“

Monitoring:

Permanentes Überwachen von Sensoren, Aktuatoren, Computern…

Redundanz

A320 und A330/A340: 5 Rechner, 3 hydr. Leistungsquellen für Stellflächenbetätigung

Zusätzliche Vorsichtsmaßnahme: Dissimilarität

2 in Hardware und Software verschiedene Rechnertypen

Segregation bei der Installation:

Elektrische und hydraulische Leitungen
Installation der Komponenten (FBW Computer sind an verschiedenen Orten installiert).

Qualität, Zuverlässigkeit

Software qualifiziert nach DO178B Level A,
Computer MTBF >= 20 000 FH/Computer

Robustness

Keine Fehler, keine Störungen bei totalem Verlust der Kühlung, Blitzschlag, EMI, …

Redundanz

Vermehrfachung gleicher Funktionen zur Verringerung der Ausfallwahrscheinlichkeit

- **Vermehrfachung**
  - **ein einzelner Kanal hat eine Ausfallwahrscheinlichkeit von 10^{-4} 1/fh**
  - **parallele Kanäle**
  - **ökonomische Grenzen**
  - **Verfügbarkeit (MTBF)**
- **Redundante Konfigurationen**
  - **Energieversorgung (elektrisch, hydraulisch)**
  - **Stellflächen**
  - **Rechner**
  - **Sensoren**
  - **simplex, duplex, triplex, quadruplex**

Redundanzprinzipien (1)

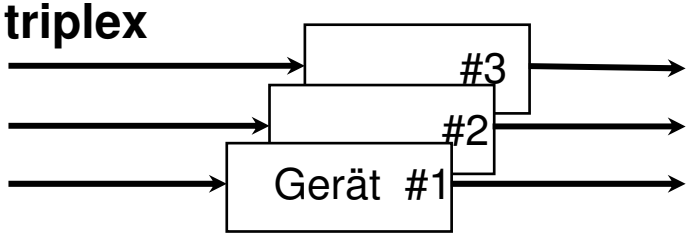
simplex

- keine Fehlererkennung möglich
- Begrenzung erforderlich

duplex

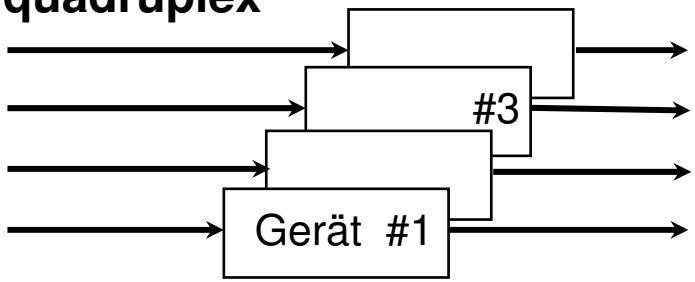
- 1 Fehler kann erkannt werden
- sicheres Abschalten (fail passive, FP)

triplex



- 2 Fehler können erkannt werden
- 1. Fehler wird toleriert (fail-op, FO-FP)
- Beispiel: Flugsteuerung Concorde

quadruplex



- 3 Fehler können erkannt werden
- 2 Fehler werden toleriert (FO-FO-FP)
- Beispiel: Tornado, EF2000, C17

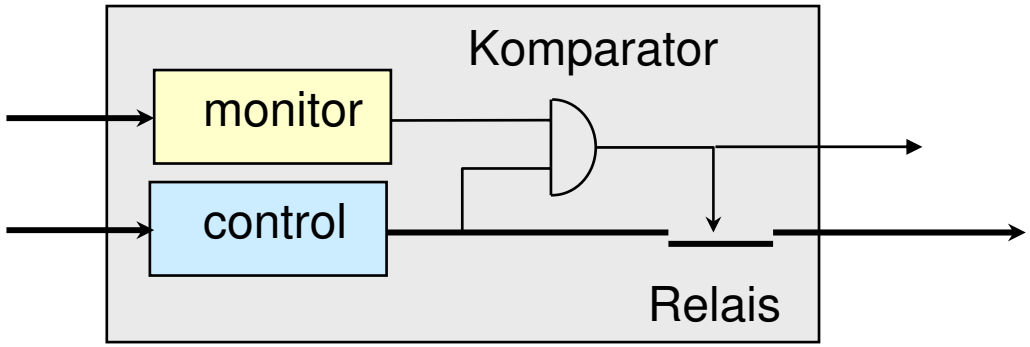
Problem: gleichartiger Fehler (S/W) und gleichzeitige Fehler

Redundanzprinzipien (2)

Dissimilare Redundanz

Maßnahme, um einen Fehler in der Software oder Hardware der Flugsteuerungsrechner auszuschließen, der zum gleichzeitigen Versagen von allen redundanten Kanälen führen kann (Common Mode Fehler)

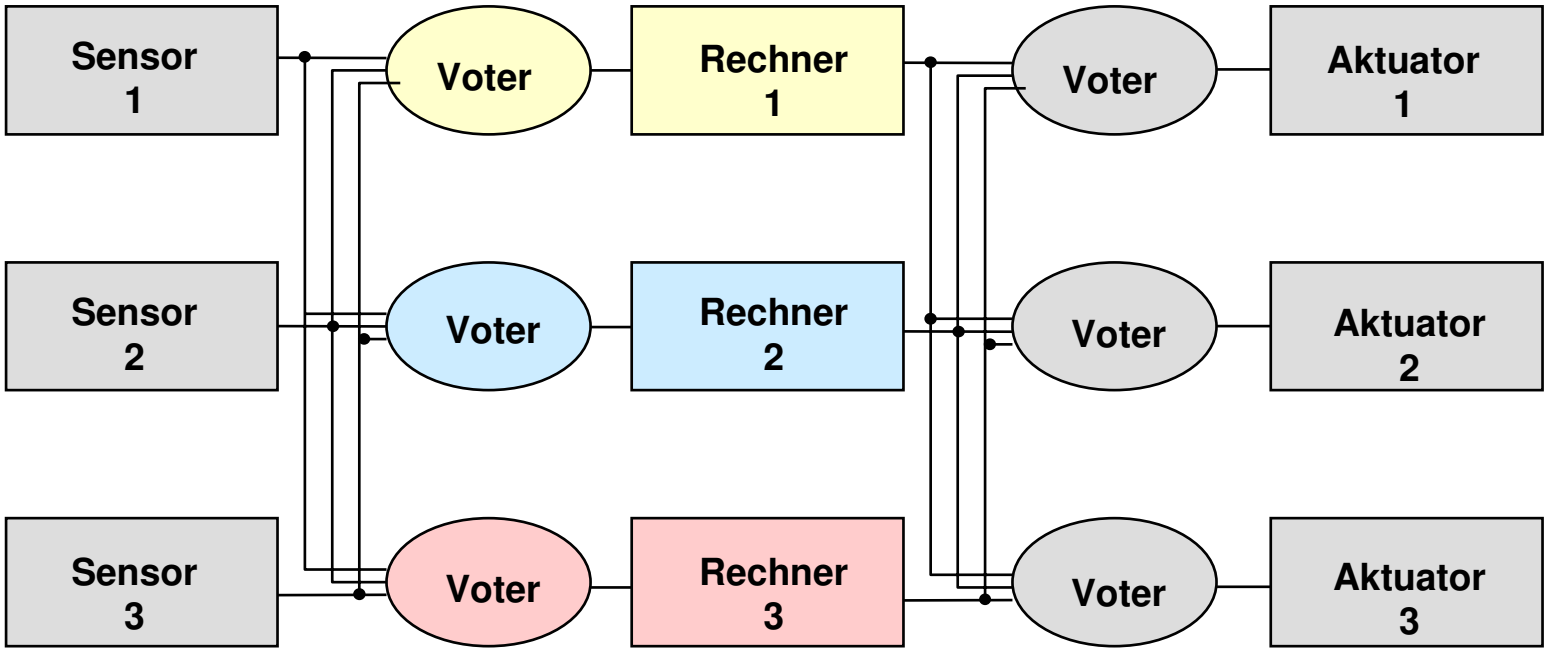
Control- und Monitor-Prinzip



- Airbus
- Control- und Monitor-Kanal dissimilar

Redundanzprinzipien (3)

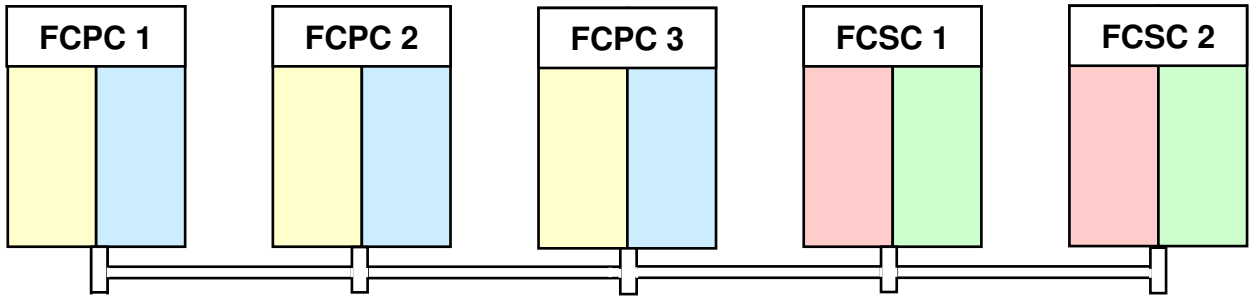
Triplex-Architektur (generisch)



- Boeing
- alle 3 Kanäle dissimilar

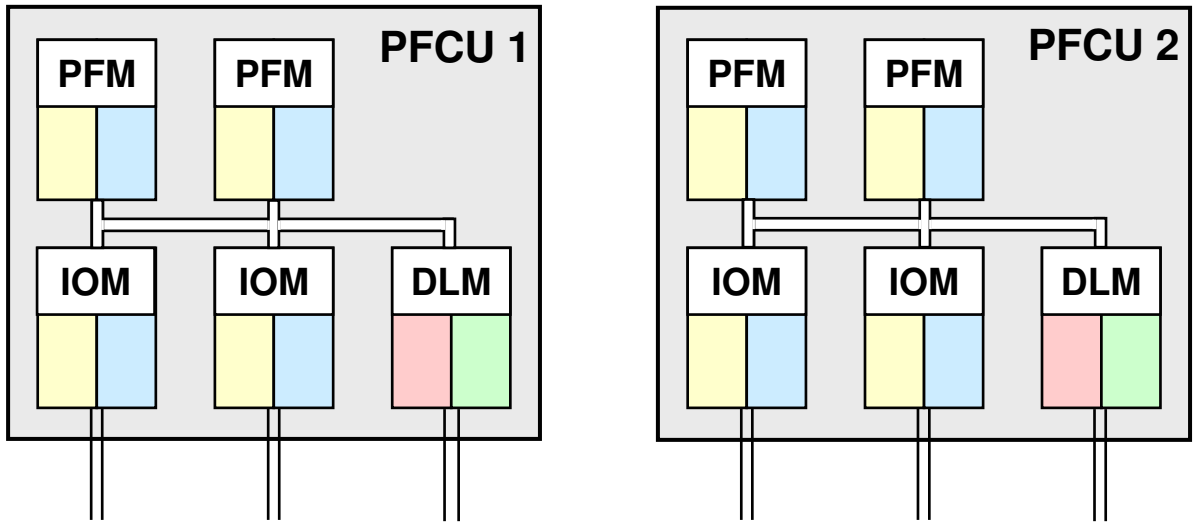
Beispiele Control / Monitor-Prinzip

- **Beispiel: Rechnersystem Airbus A330/340:**



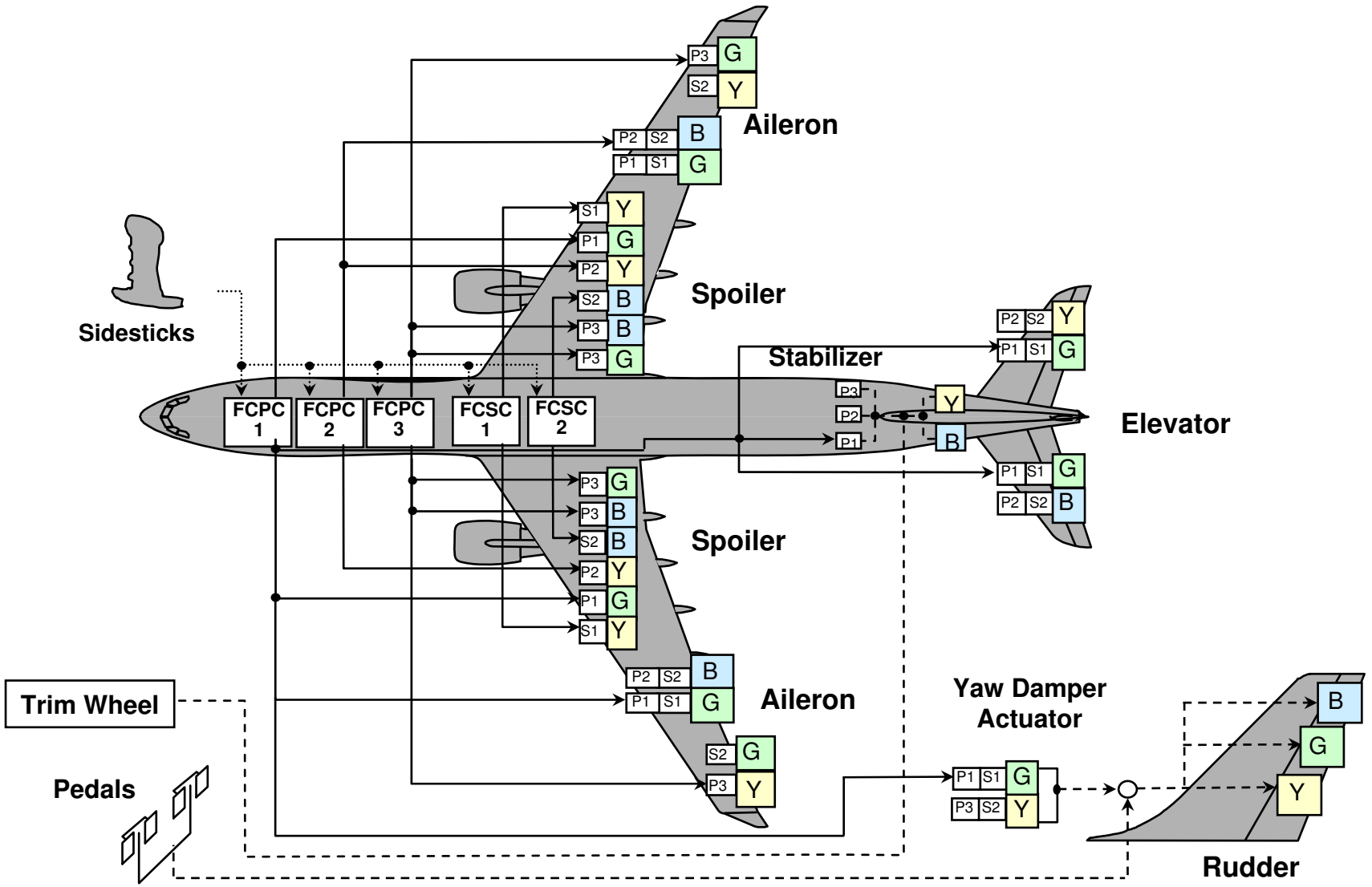
FCPC	Flight Control Primary Computer
FCSC	Flight Control Secondary Computer

- **Beispiel: Rechnersystem VFW614-ATD**

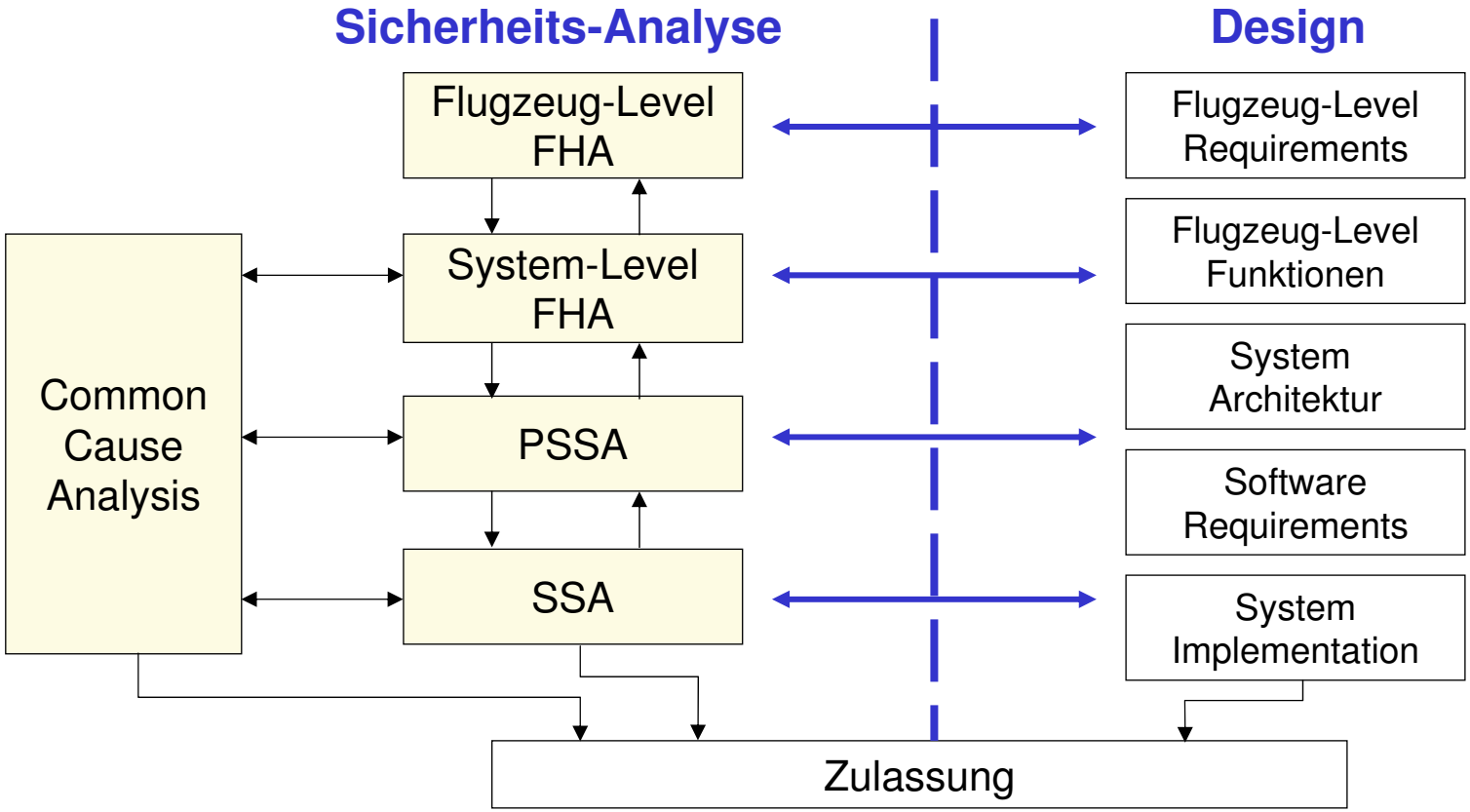


PFCU	Primary Flight Control Unit
PFM	Primary Flight Module
IOM	Input / Output Module
DLM	Direct Link Module

Architektur der Flugsteuerung A330



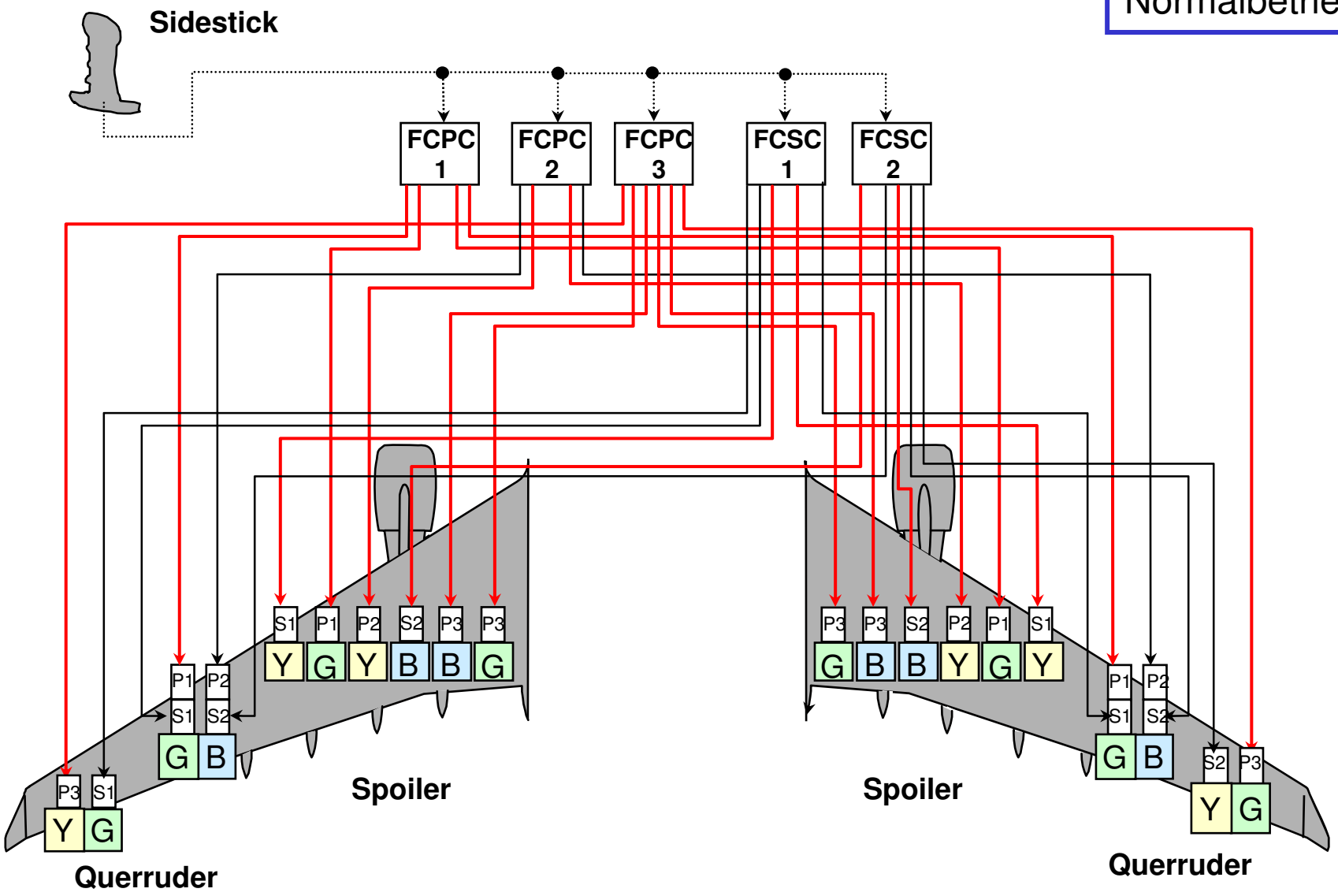
Sicherheits-Prozess



FHA	Functional Hazard Analysis	Potentielle Fehler und ihre Konsequenzen (Forderungen)
PSSA	Preliminary System Safety Analysis	Zeigt wie das Design die Forderungen erfüllt
SSA	System Safety Analysis	Zeigt daß das Design die Forderungen erfüllt
CCA	Common Cause Analysis	Identifiziert Common Mode Fehler

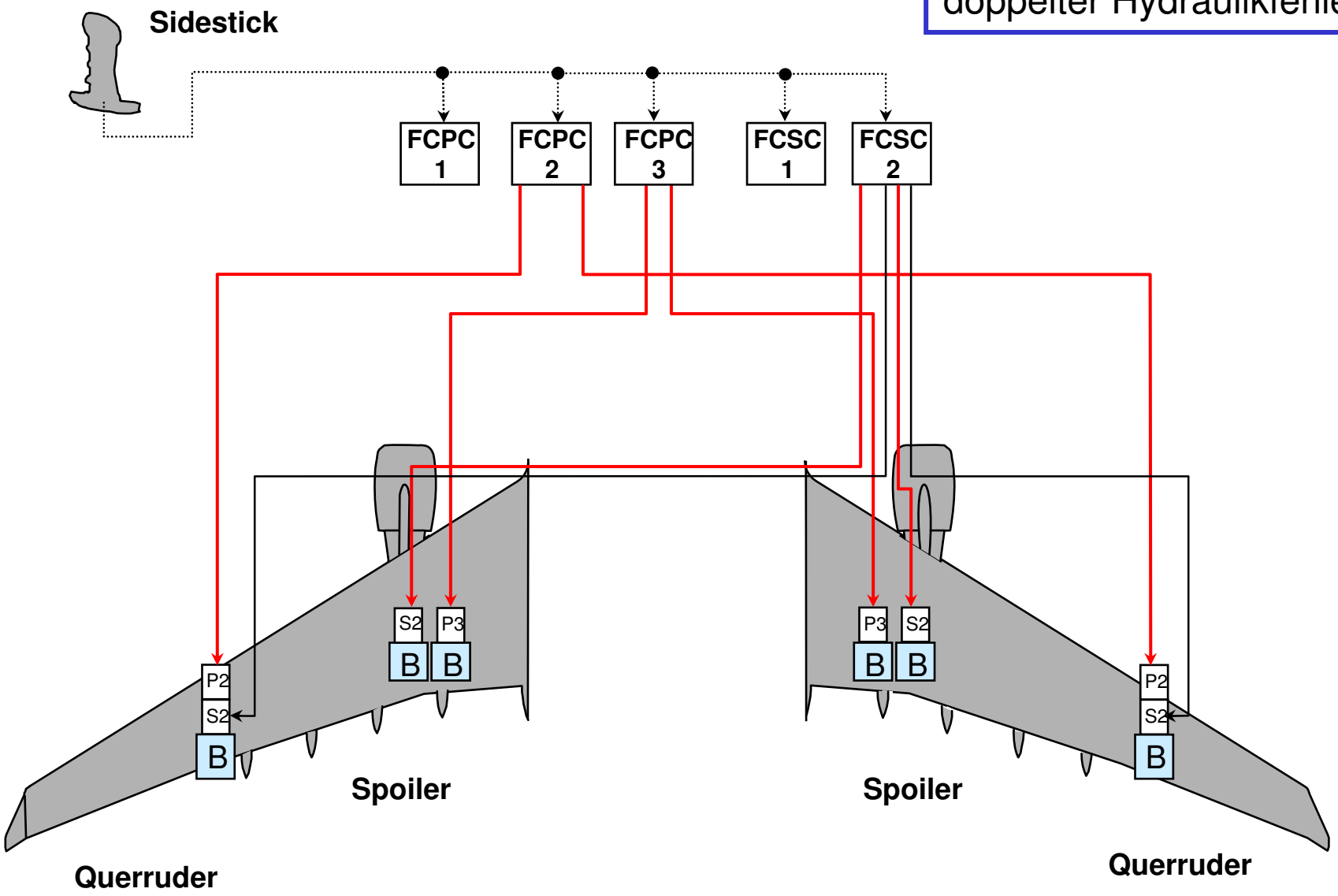
Redundante Rollsteuerung, Airbus A330

Normalbetrieb



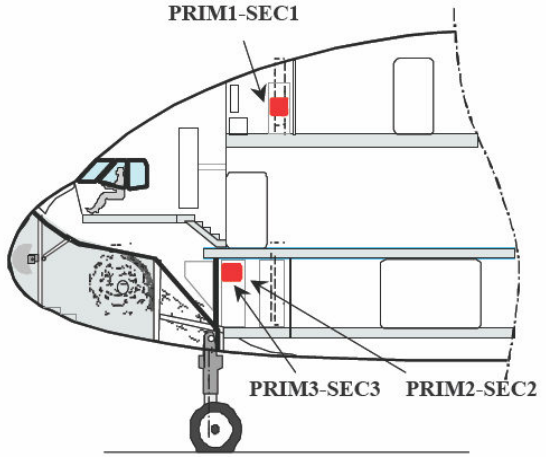
Redundante Rollsteuerung, Airbus A330

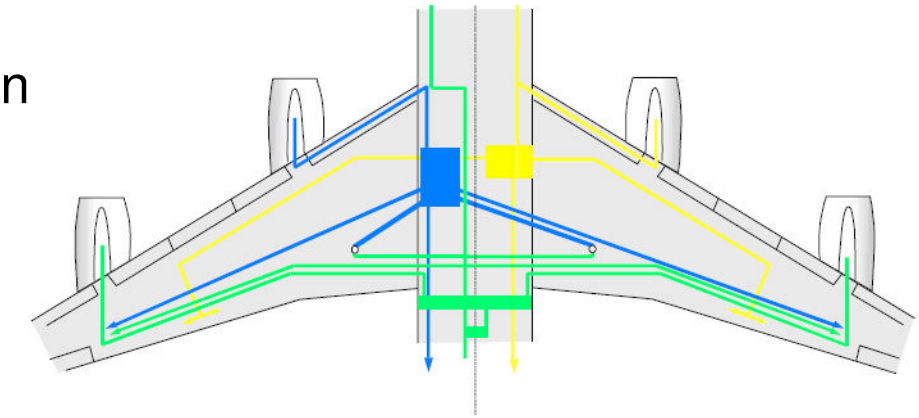
doppelter Hydraulikfehler



Segregation

- Funktionen (Rechner)
- Datennetzwerke
- Einbauort
- Signal und Versorgungsleitungen





Trends

- Nutzen von Konzepten aus kommerzieller Elektronik
  - Standardisierte Rechnerkomponenten:
    Integrated Modular Avionik (IMA)
  - Ethernet High speed data network
    AFDX: full duplex Ethernet for avionic communication
  - PC / Windows / HUB / Firewall
    Für nicht sicherheitskritische Bord-Informationssysteme
- Commercial of the Shelf (COTS) ist kurzfristig nicht realisierbar:
  - Sicherheit und Zulassung: Beweis der korrekten Entwicklung
  - Umgebungsbedingungen: Temperatur, Vibrationen, EMV, EMI, Neutronen
  - Verfügbarkeit: Programmabbruch (blauer Schirm) ist unakzeptabel
  - Obsolescence: Produktion über 25 Jahre, Wartung 50 Jahre

Integrated Modular Avionic

Traditionell:

- LRUs bestehend aus H/W und S/W
- 1 Computer = 1 Funktion = 1 Entwicklung

IMA:

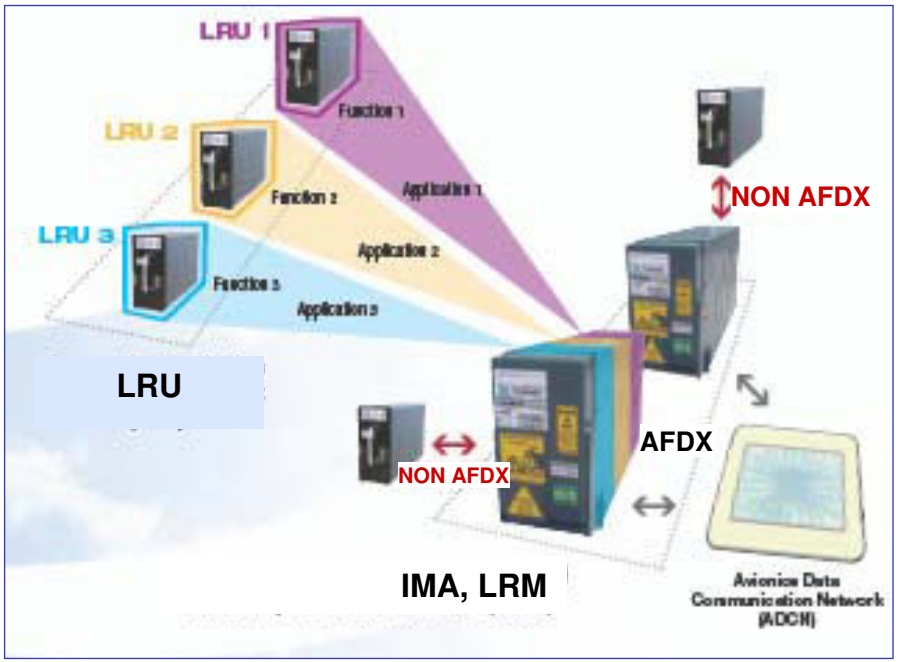
- Konzept der kommerziellen Elektronik
- Standardisierte Rechner
- Ethernet high speed data network (AFDX)

Vorteile

- verschiedene Funktionen auf einem Rechner (Partitionierung)
- Reduktion von Kosten, Volumen / Gewicht, Entwicklungsaufwand, Ersatzteile
- Hardware-Module, Software und H/W-S/W-Integration von verschiedenen Lieferanten
- Flexibel bei Funktionsänderungen

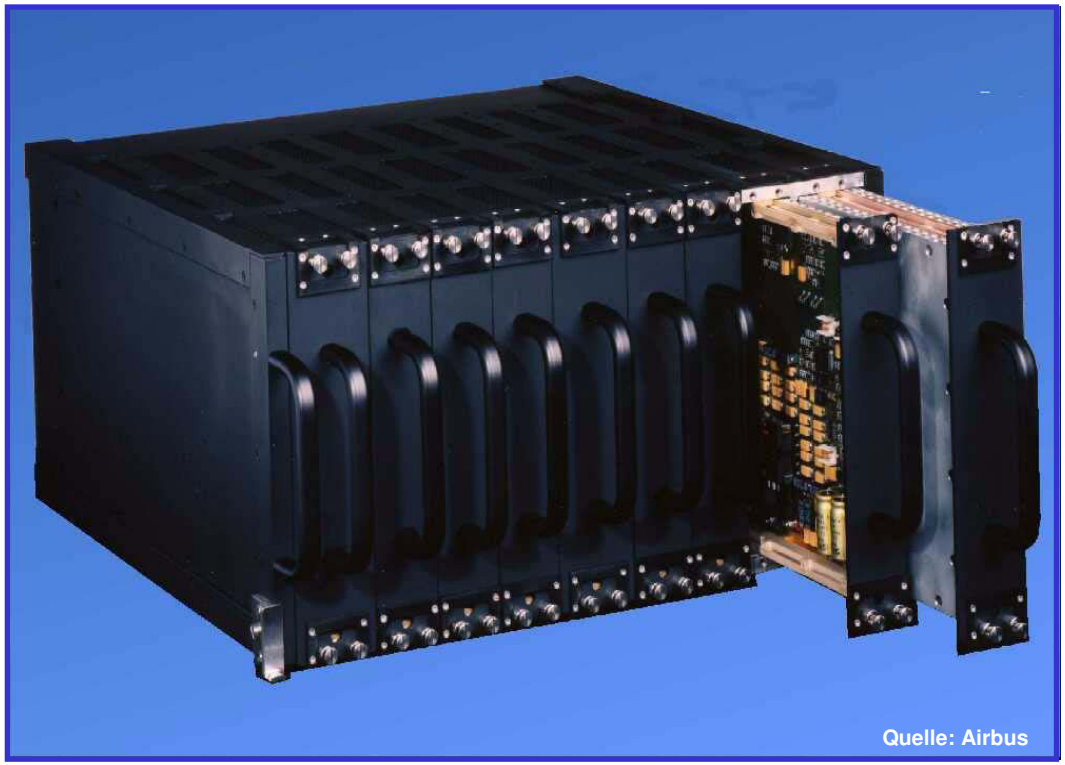
AFDX in Airbus A380, A400M and Boeing 787.

Integrated Modular Avionic (IMA)



AFDX	avionics full duplex ethernet end-system, ARINC 664 protocol and specification
LRM	Line Replaceble Module
LRU	Line Replaceble Unit

Primary Flight Control Unit (PFCU)



Hersteller

Bodenseewerk Gerätetechnik (BGT), 1998

heute: Diehl Avionik Systeme

Technische Daten

Basiszyklus:	22 ms
krit. Funktionen:	11 ms
I/O Signale	~500
Gewicht:	35 kg

ARINC Standards

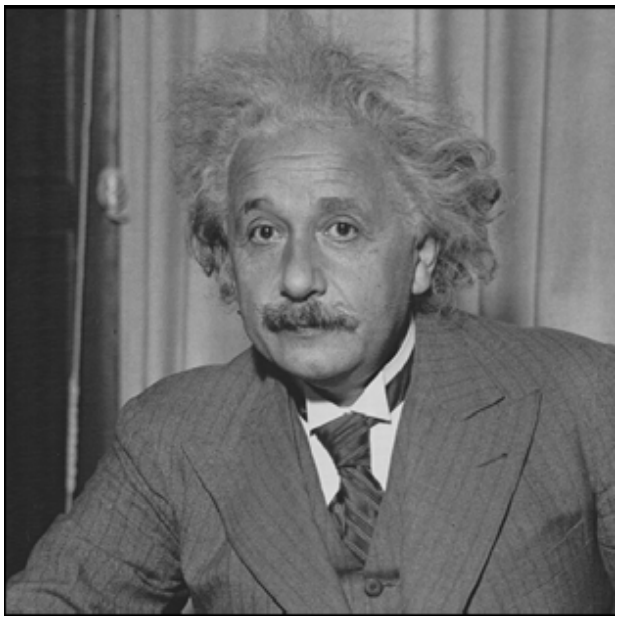
ARINC (Aeronautical Radio, Inc.) **https://www.arinc.com/cf/store/**

ARINC 400-Series Reports and Specifications
- ARINC 429 Mark 33 Digital Information Transfer System (DITS)
  serial data bus, one transmitter multiple receivers

ARINC 600-Series Reports and Specifications
- ARINC 629 Multi-Transmitter Data Bus
- ARINC 651 Design Guidance for Integrated Modular Avionics
- ARINC 652 Guidance for Avionics Software Management
- ARINC 654 Environmental Design Guidelines for Integrated Modular Avionics
- ARINC 659 Backplane Data Bus
- ARINC 664 Aircraft Data Network, Part 1 to 8

ARINC 700-Series Equipment Characteristics
- ARINC 701 Flight Control Computer System
- ARINC 702 Flight Management Computer
- ARINC 704 Inertial Reference System
- ARINC 735-2 Traffic Alert and Collision Avoidance System (TCAS)
- ARINC 762-1 Terrain Awareness and Warning System (TAWS)

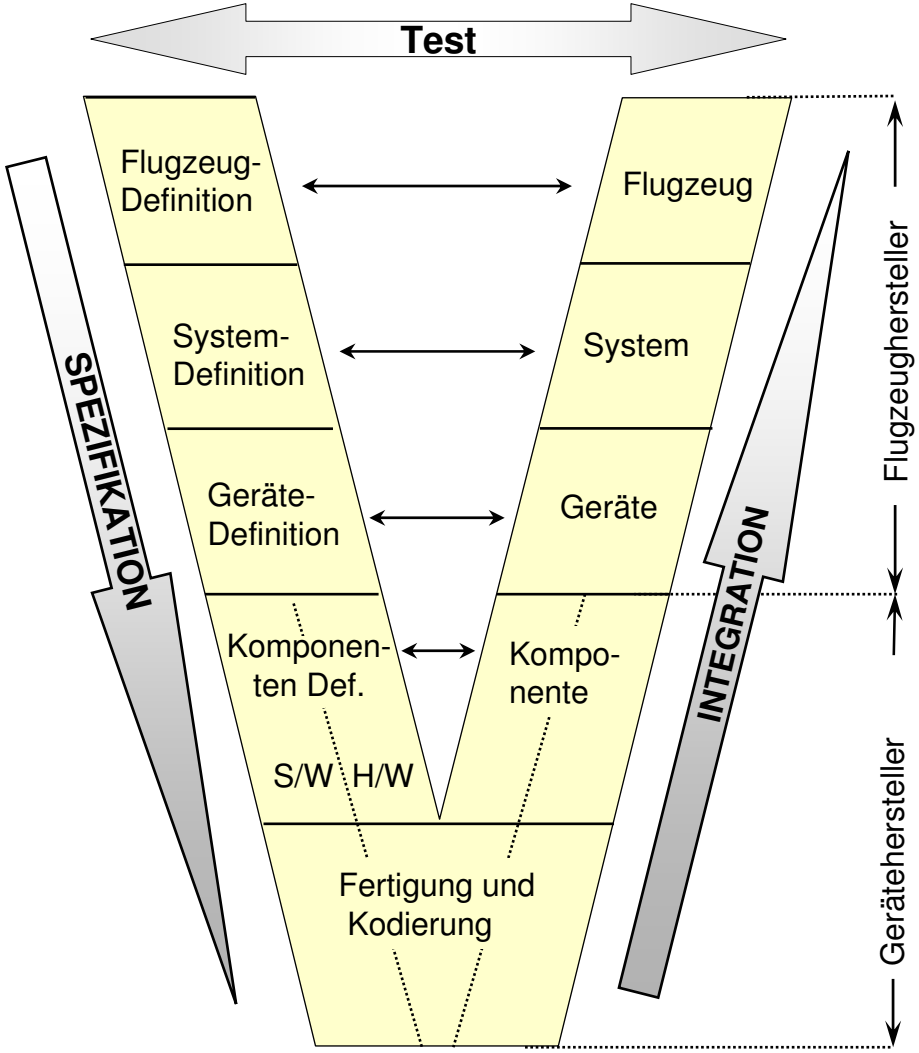
3. Entwicklungsprozeß



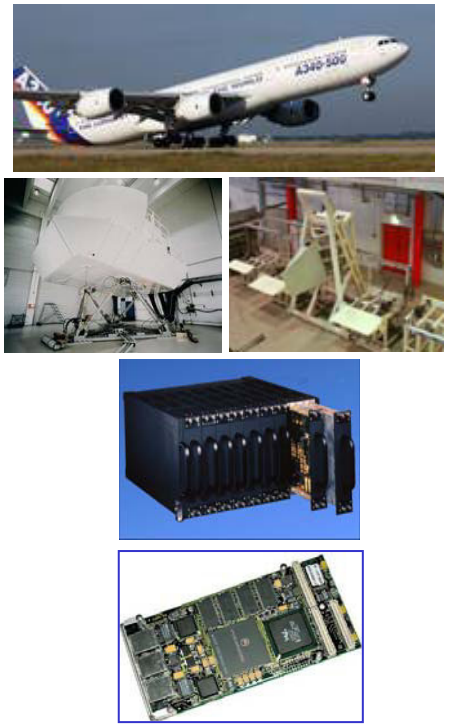
Albert Einstein auf die Frage, wie er ein komplexes Problem in 1 Stunde lösen würde:

„45 Minuten nachdenken,
in 10 Minuten einen Plan anfertigen
und das Problem in 5 Minuten lösen.“

Entwicklungsprozeß (V-Modell)



z.B. Flugregelsystem



Herausforderung: durchgängiger Prozess, Toolkette (Doors, Scade, Matlab, …)

Entwicklungsprozeß (V-Modell)

Systemfunktion

Sicherheit, Ausfallwahrscheinlichkeit

Operationelle Verfügbarkeit:

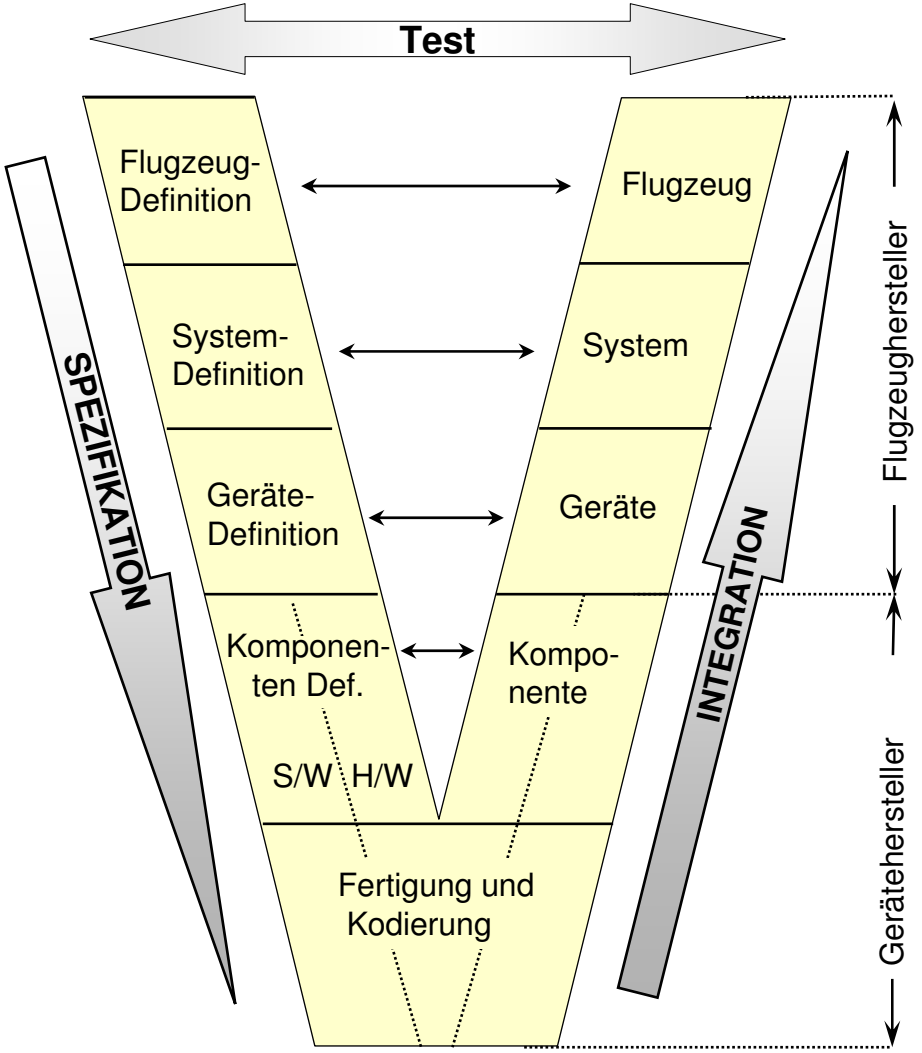
Systemkonzept
- Systemverhalten
- Redundanzmanagement
- Interaktionen mit anderen Systemen
- Energieversorgung

MMI
- Bedienphilosophie
- Gestaltung

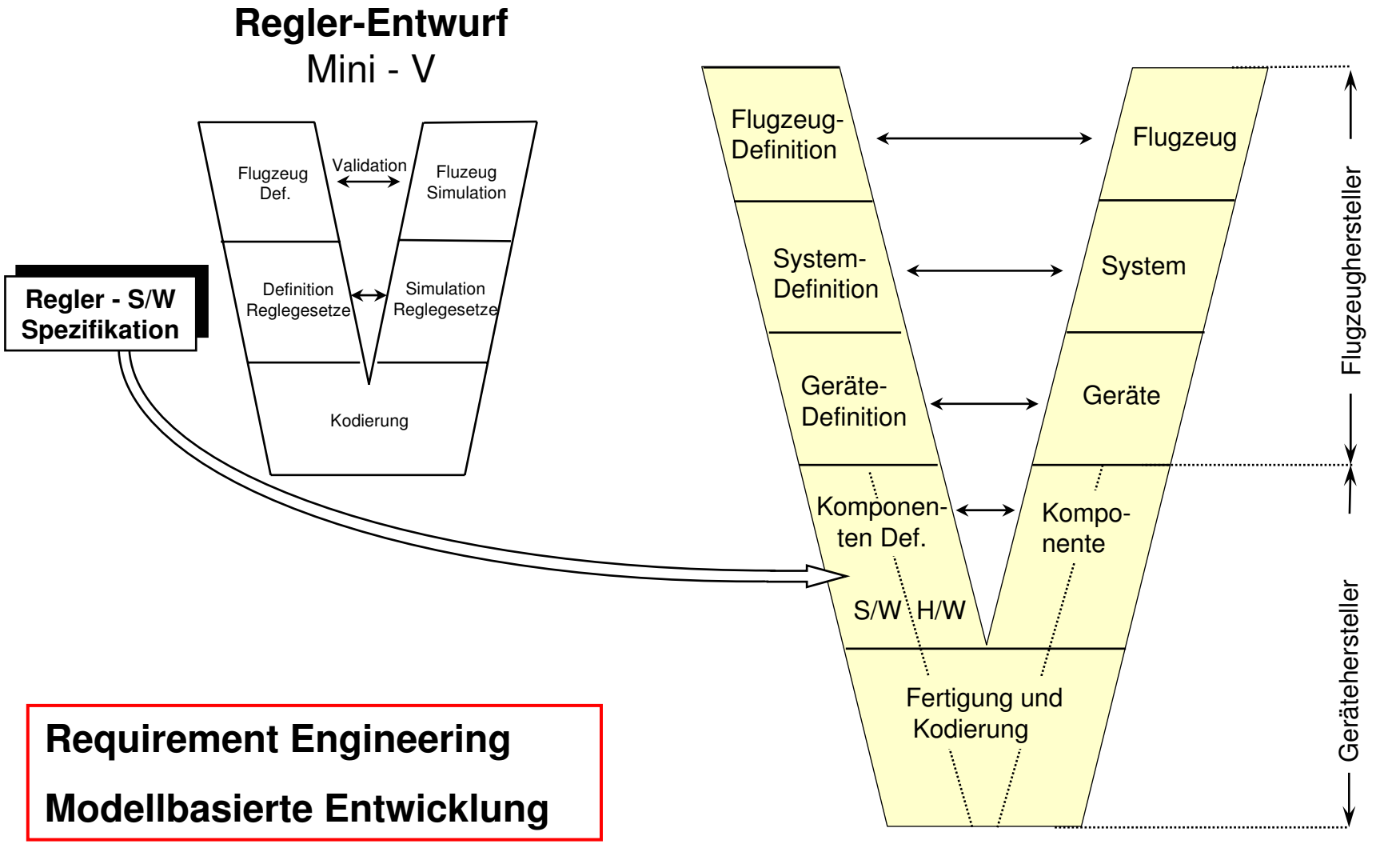
Komponenten
- Technologie
- Einbauort
- Kräfte

Umweltbedingungen (EMV, EMI,…)

Entwicklungsprozess



Entwicklungsprozeß (V-Modell)

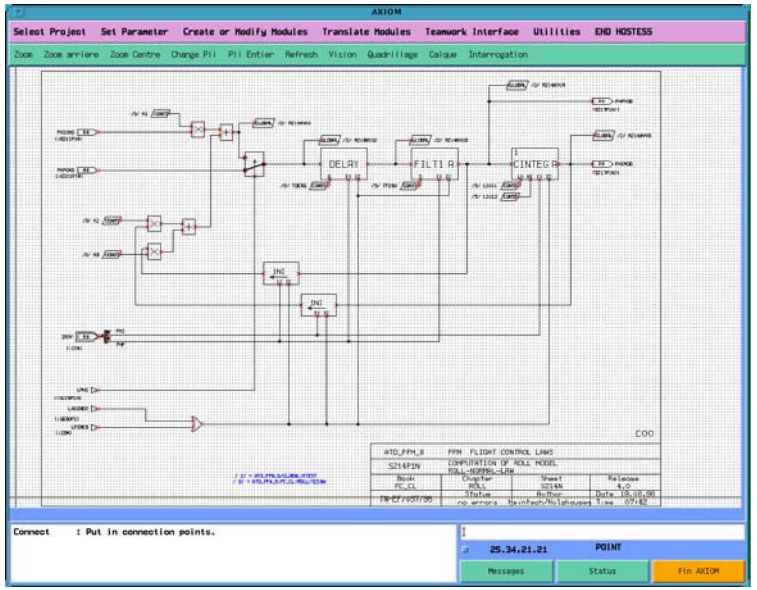


Requirement Engineering

Modellbasierte Entwicklung

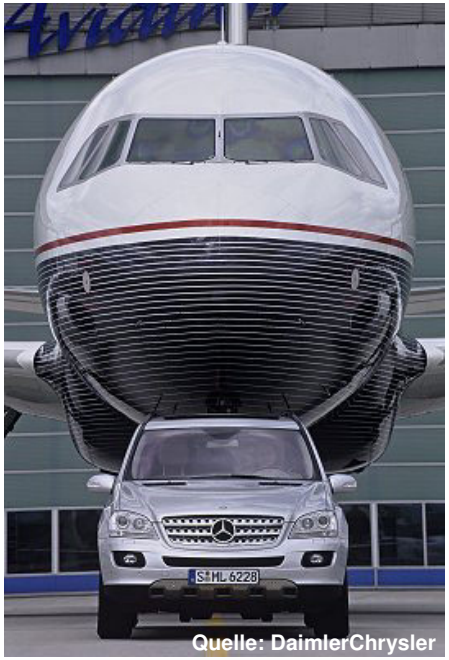
Funktionale Spezifikation

- **Grafische Sprache für Spezifikation**
- **Eindeutige Interpretation**
- **Automatische Code-Generierung für Simulation zur Validierung**
- **Automatische Code-Generierung mit qualifiziertem Tool für die Embedded Software**



Zusammenfassung

**Entwurfsprinzipe,
Entwicklungsprozeß**



**Industriestandards,
Serienprodukte**

Synergien

- **Entwicklungs-Methoden**
  - Requirement Engineering,
  - Modellbasierte Entwicklung,
  - Softwaretechnologie
- **Human Factors**

Vielen Dank !