Safety and Fault Tolerance in a Complex Human Centred Automation Environment
Sicherheit und Fehlertoleranz im Umfeld komplexer Assistenzfunktionen
Regelungstechnisches Kolloquium
Universität Dortmund, 25.06.2009
What we are going to talk about

Index:

• the nature of complexity
• fault tolerance an element of safety coping with complexity
• the approach to machine centred fault tolerance
• some examples
• human centred automation in the cockpit
• some examples of automatic assistance functions
• man vs. machine properties: risks and means to maintain fault tolerant man-machine co-operation
• cooperative automation
• cognitive automation
• items of research on FTC in complex HC automation
From mechanical Automaton …..

Roll controls / air brake of Boeing 737

The functions of roll- and air brake surfaces for any operating case
(Rejected Take Off, A/C On Ground, Cruise, ...) purely mechanical design
...to digital Algorithms – "virtual Functions"

Roll controls / air brake of A340

Flight Control Computer
- lateral normal law
  - turn coordination
  - bank angle protection
  - sideslip limitation
- roll direct law
- roll alternate law
- load alleviation
- lift augmentation
- mode switching logic
- ground spoiler logic
- speedbrake control
- priority logic
- autopilot mode logic
- servoloop control

Servo loop priorities

Hydraulic circuits

Ailerons

Spoilers

Functions 100% Software design
Function Software and Signal Interfaces on A/C Systems

by "emergence", "hidden links" and "dys-functionality"

Function SW in MB
Signal Interfaces x 1000

Sources: 14. DASC Boston, MA Nov. 1995 & Airbus Data
Complexity of Software Functions

The software functions of A/C systems incorporate many meshed algorithms and servo-loops.

Due to numerous operation modes and failure conditions a software function can feature considerable numbers of states (TCAS e.g. $10^{40}$).

This complexity goes far beyond the feasibilities of mechanical representation.

The SAFETY goal is to guarantee 100% integrity of all functional states for all modes and failure conditions while operating in front of an ambiguous environment.

In order to keep the function within admissible limits in spite of the prevailing complexity the „SAFETY – DESIGN PROCESS“ has been established that leads to the „SAFETY ARCHITECTURE DESIGN“
Safety <> Reliability, Availability, Integrity

- **Function**: 1st Fault detected
- **Fault Tolerance**: N-th fault detected
- **Reliability**: 1st Fault detected
- **MTBF**: No Fault detected
- **Availability**: Integrity problem
- **Emergency function**: LAND AS SOON AS POSSIBLE !!!
- **No Redundancy**: T/O prohibited
- **Increased Work load**: Inspection

**Safety Margin**:
- Increased Work load
- No Redundancy
- Availability problem

**Endurance / Continuity**:
- Safety Margin
- Fault Tolerance
Technical – Functional Causes that corrupt Safety

Design error (generic fault)

Component failure (deterioration, over load, bad material, finite life…) ➔ MTBF

„Common Mode“ effects (multiple failures caused by one fault)

Undetected erroneous behaviour (Integrity problem!!)

Unexpected, adverse behaviour (e.g. powered runaway = activation of function without command)
Four “TOOLS” to maintain SAFETY

- Component failure (deterioration, over load, bad material, finite life) ➔ MTBF
- Design error (generic fault)
- „Common Mode“ Effects (multiple failures caused by one fault)
- Unexpected, adverse behaviour (e.g. powered runaway = activation of functions without command)
- Undetected failures (Integrity problem!!)

SAFETY – DESIGN - PROCESS

- Douplex Signal Processing
  - Command / Monitoring
- Dissimilar Function-Processing
- Multiple Redundant Functional Units
How to get „SAFETY“ into Functions

Design-Process according to Certified Standards (ARP4754 / DO178B /...) quite similar to ISO26262. ! Under supervision of authorities (EASA, FAA)! JAR25

Fault Monitoring & Majority Voting

Fault Monitoring

Faults

Design Error

Common Mode Faults

Finite Reliability

Undetected design errors

Unexpected behaviour

Component failure

Technical measures:
Multi channel, dissimilar signal processing, redundancy

yield

Dissimilar & Redundant Topologies with pre-designed Reconfiguration-Strategies and Back-up Functions

* Max Fault Tolerance, Integrity and Availability
A330 Flight Control Fault Recovery Scheme - Wing

Primary Computer
P1, P2, P3

Secondary Computer
S1, S2

---Ground lift damper air brake---
------------Roll control surfaces-------------
--Manoeuvre load alleviation--

Hydraulic Power Supply (Y, B, G)
A/C 3-D Positioning, Overview Navigation Devices

**Radio Navigation**
- Radio/GPS Position
- Landing aids

**Probes**

**Air Data & Inertial System**
- Altitude
- Temperature
- Acceleration
- Speed
- Inertial position
- Route

**Global Positioning System (GPS)**

**Flight Management**
- Position computation
- Flight planning
- Guidance
- Performances (fuel...)
- Datalink
- ...

**Airline Operations Control (AOC)**

**Air Traffic Control (ATC)**
Performance Factors

- ACCURACY: “The degree of conformance between the estimated or measured value and its true value”

- AVAILABILITY: “The percent of time that a navigation system will meet its operational tolerances within a specified area of coverage.”

- CONTINUITY: “The probability that a navigation system will be available for the duration of a task.”

- INTEGRITY: “The ability to warn users that the system should not be used”

Integrity is the most Decisive Factor of Navigation Avionic Safety!
Navigation Sensors

• Primary Navigation Aid: Satellite Navigation

• GPS is a US DOD System
• Space Segment
  ‣ 21+3 Space Vehicles (SVs = Satellites) nominal (3 spares)
  ‣ 29 Healthy SV (July 2005)
  ‣ 6 orbital planes, 4 SVs per plane
  ‣ Semi-synchronous, circular orbits
• 5-8 Visible Satellites in flight conditions (typical)
• Dynamic Accuracy (mil.):
  ~ 20m (lateral),
  ~ 40m (vertical)
• European Equivalent GALILEO starts in 2012 TBC
Signal Integrity Corruption  CRPA, P/Y-Code

Error Properties:
• GPS signals are subject to various interference:
  ‣ Civil jamming sources, unintentional interference
    – defective transmitter stations
      (VHF-transmitter, TV-stations)
    – personal electronic devices on board
      (mobile phones, Laptops, ...)
    – Wideband Radar
  ‣ Intentional interference (military conflicts, terror)
    – „Jammer“ = blind GPS signals by strong transmitters
    – „spoofing“ = fake up and twist of GPS signals

→ Protection by using sophisticated antenna technologies and cryptographic GPS Codes!
  ‣ Controlled Reception Pattern Antenna (CRPA)
    – suspends the direction of the jammer’s transmission beam
    – Simultaneous compensation of multiple jammers feasible
  ‣ P/Y Code ciphering of GPS signals
Inertial Navigation LASER- Gyro- Platform

- Inertial Platform bridging the phases where GPS signals are not available
- Error property: ramp up of position error with time (drift)
**Strength and Weaknesses of Navigation Sensors:**

- **Inertial platform**
  - + high availability and reliability
  - - low long term precision (drift)

- **GPS**
  - + high precision
  - - precarious availability and reliability

- **Air Data and TRN**
  - + adequate availability
  - - low Integrity
GADIRU Concept

- **GADIRU**
  - GPS, Air Data, Inertial Reference Unit
    - Combination of all available Navigation Sensors on one Platform
    - Compensation of individual Strength and Weaknesses
    - Method: “Hybridisation” by means of Kalman Filters
GADIRU architecture

GADIRU: GPS Air Data Inertial Reference Unit
GADIRS architecture (for LLF & AA)

- A/C System (Split Cockpit)
- Other A429 users (demanding)
- Consolidation & monitoring B
- FCGS
- Consolidation & monitoring B
- A/C System (Split Cockpit)

All GADIRS Data available on AFDX

Coaxial Cable

AFDX

ARINC 429
Cockpit constitutes the point of convergence of all aircraft systems through communication and visualization means.

**Low level/short term tasks nearly fully automated:** crew workload reduction, e.g. “steering the A/C”, system control etc.

**High level/long term tasks still pilot’s obligation:** high level information synthesis, process management. E.g. flight planning, ATM coordination etc. (progressively automated)
Flight deck controls and displays have a huge deal of COMPLEX AUTOMATIC FUNCTIONS and PROTECTION MECHANISMS in between.
Automation in aircraft has two purposes:

- to make flying safer
- to make flying more efficient

For any technical evolution both objectives have to be very carefully evaluated and balanced in order **not** to make **any compromise on safety** for efficiency purposes
Examples: **Manipulator**

1. Autopilot:

The autopilot is a manipulator that substitutes the crew on cruise and at auto landing procedures.

With two double channel autopilots engaged being tuned to the airport instrument landing system (ILS) automatic landings are feasible with an average success rate of far over 99.9% in very poor weather conditions where man would not even attempt (CAT IIIB approach: no DH – RVR = 125m)

Increased safety and efficiency both significantly relieve the crew from work load and thus decreases psychological tension and stress.

![Diagram](image_url)

- 3° angle
- Runway Centreline

25.06.2009 Seite 25

© AIRBUS DEUTSCHLAND GMBH. Alle Rechte vorbehalten. Vertrauliches und geschütztes Dokument.
2. Protections:

to prevent the aircraft and her systems from dangerous exceeding of operational and physical limits

to allow for immediate „full power“ actions in critical situations, which often develop at the border of the operation envelope in order to get maximal available performance without adding additional hazard

Examples:

Anti-skid system releases the brakes when skidding is detected and thus allows to apply full pedals down when required (RTO, short runway)

Bleed bias in the compressor and resp. fuel air mixture in the combustion chamber avoids thermal obstruction and prevents the engines from stall when pushing the thrust levers full forward rapidly e.g. at TOGA situations

Flight envelope protection prevents the A/C from aerodynamic stall and structure overstressing in safety critical escape manoeuvres
CFIT Escape Manoeuvre

GPWS

Altitude

Duck under

bucket distance
and bucket time

Landing conf.
V/S = 1500 ft/min

500 1000 1500 2000 2500  Distance (ft)

7 sec 12 sec 15 sec

CFIT escape trajectories
Protected (---) vs. non-protected (- - -) aircraft

<table>
<thead>
<tr>
<th>Parameter</th>
<th>non-protected</th>
<th>protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duck under (ft)</td>
<td>125</td>
<td>80</td>
</tr>
<tr>
<td>Bucket distance (ft)</td>
<td>2500</td>
<td>1500</td>
</tr>
<tr>
<td>Bucket time (sec)</td>
<td>12</td>
<td>7</td>
</tr>
<tr>
<td>Safety margin (sec)</td>
<td>3</td>
<td>8</td>
</tr>
</tbody>
</table>

Discriminating parameters of CFIT escape trajectories
Flight Envelope Protection on Pull-Up Manoeuvres

- **Side stick movement**
- **Angle of Attack**
- **climb**

*Pull-up maneuver in landing configuration, AFT Cg Protected aircraft versus flying stall warning*
Examples: Complex Planning, Monitoring, Prognostic

Flight Management System, FMS:

• is a multi system: FM + AP + FD + A/THR + MCDU + PFD + ND
• works in numerous modes (pilot cmd. & auto mode switching logics)
• supports the pilot on his decision tasks based on complex calculations
• features a redundant COM/MON architecture to achieve integrity
• converts the flight plan into a flight trajectory respecting environmental conditions, nav. aids, economic constraints and many other criteria
• continuously provides the crew with flight data (pos., hdg, speed, trk, ...)
• monitors secondary tasks, while the pilot concentrates on primary ones
• can be considered as “part of the crew” – an electronic crew member
• makes the flight safer relieving the crew from error prone calculations and by providing an excellent situational awareness to the crew
Flight Management - operation

Flight Management Computer (FMC)

Crew

Multipurpose Control Display Unit (MCDU) or new A380 displays

Future Air Nav. System (FANS)

Free Flight (ADS-B)

Negotiation

Flight Plan Display

Lateral & Vertical Guidance

Predictions: fuel, position, altitude, speed, time...

Optimisations: fuel, speed, altitude (cost index)

- Flight Plan
- Wind & Temperature
- Flight Level
- Speed

- Flight Parameters
- Radio Data

Radio Navigation, ADIRU

Data Link Com.
Handling Devices to Automated Systems

Highly automated processes require quite refined input signals on very low amplitude levels. Thus, large input devices with large displacement are not suited.

Human sensitivity and accuracy are best at the minimum threshold of perception.

Human ergonomic properties match best to the features of assistance systems with side stick, track ball and keyboards.
Automation – Complement to Men

Decision Maker

Support by automated systems

Automated systems shall

• play to man’s strengths and
• compensate for man’s weaknesses

If you look at those S & W you’ll soon discover
where automation is needed and where not
Properties of two Different Kinds of Intelligence

Man:
• is very complex with the capacity of analysis and synthesis in ambiguous situations
• has a special memory: lots of sensations, experiences, feelings, procedures
• can adapt to new environment and situations by learning and reasoning
• association from experience, intuition and discernment take him to rapid decisions
• this is the feature of „cognitive intelligence“ – we call this – Airmanship

Automaton:
• is very complex with the capacity of analysis and synthesis in clear-cut situations
• relies on numerous and very sensitive sensors
• performs very precise calculations within extremely short time intervals
• provides immediate reaction
• no stress, no nerves, no fatigue → provides a constant performance
Human Factors: Human – Machine Interaction

System Function

Operator Function

Device

HF Fault Moderation

Technical Assistance

Operating Procedures

Human

Human as a Hazard (risk factor)
- slips
- lapses
- mistakes
- violations

Human as a Hero (cognitive monitor)
- adjustments
- compensations
- recoveries
- improvisation

Operation Rules
- Transparency
- Congruent Semantics
- Obvious Intentions
- Check Options
- Escape Options

Automaton Function

Fault Compensation
Risks of Advanced Human Centred Assistance Systems

Risk 1

some operating modes may be so complex that they are not properly understood and therefore misused by the operator.

Risk 2

an automatic decision of the assistance function to change the operating mode or strategy may not or only poorly perceived by the operator (lack of awareness)
Alleviation of Risks of Advance Human Centred Assistance Systems in the field of Aeronautic Operation

Countermeasures to defeat the risks of automation

• get the operator involved into the **principles** of interacting function modes and mode switching logics by **teaching and training**

• **exercise operating procedures** that prepare the operator for situations where function reversions occur

• provide the operator **signals and messages** that indicate the system’s operating conditions, intentions and goals (**cooperative automation**)

• provide the operator signals and means to **crosscheck** the assistance function behaviour with other information (**plausibility check**)

• allow the operator to **cut the assistance function** and to **take over by himself** (maybe supported by lower level, but more transparent assistance functions)

**General principle:** the operator may be surprised but **never puzzled nor paralysed**
Operational Safety

The concept of dissimilarity, redundancy and command/monitoring equally is applied to Cockpit and ATM / ATC operations.

SPLIT COCKPIT CONCEPT
Independent controls and Displays

AUTOMATION

COM
Pilot
Check
Redundancy
dissimilar

MON
Co-Pilot

Degradation of functional support in case of automation failure

ATC / ATM

Check
MON
ATM Contr.
dissimilar

Back-up Redundancy

MON
Check
COM

Flight Deck ➔ PROCEDURES ➙ ATC
Prospect of Automation

This graph does not only apply to automation in vehicle operation but also to automation in engineering processes where machines perform design tasks and complex CAE function execution with a high level of autonomy.
Levels of Automation

<table>
<thead>
<tr>
<th>Knowledge Based Problem Solving</th>
<th>Rule Based System Interaction</th>
<th>Skill Based Manipulator Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classical Automation</td>
<td>Extended Classical Automation</td>
<td>Classical Automation</td>
</tr>
<tr>
<td>Authority in low level routine actions, full visibility of vehicle functions</td>
<td>Complex intransparent systems truncate operator from vehicle functions</td>
<td>Support, recommendation and explanation. Operator keeps full authority and forward simulation enhanced visibility and planning</td>
</tr>
</tbody>
</table>

- Interpretation, decision, cmd.
- Continuous mutual goal driven reasoning and rule making loop
Human like Problem Solving – Cognitive Process Strategy

Cognitive Automation (Rasmussen's Model of human knowledge processing, 1983):

- **Cognitive Automation**
  - knowledge problem solving
  - rules, context
  - execution manipulat.

- **Conventional Automation**
  - feature formation
  - signs, figures

- **Cognitive Automation**
  - identification
  - decision of tasks
  - association

- **Cognitive Automation**
  - recognition
  - state to task
  - new rules
  - stored rules (for tasks)

- **Cognitive Automation**
  - symbols
  - situational picture
  - signs
  - patterns

- **Cognitive Automation**
  - goals
  - planning
  - commands
  - sensor-actor execution

- **Cognitive Automation**
  - signals
  - actions

- **Cognitive Automation**
  - signs
  - figures

- **Cognitive Automation**
  - symbols
  - situational picture

- **Cognitive Automation**
  - goals
  - planning
  - commands
  - sensor-actor execution

- **Cognitive Automation**
  - signals
  - actions

- **Cognitive Automation**
  - signs
  - figures

- **Cognitive Automation**
  - symbols
  - situational picture

- **Cognitive Automation**
  - goals
  - planning
  - commands
  - sensor-actor execution

- **Cognitive Automation**
  - signals
  - actions

- **Cognitive Automation**
  - signs
  - figures

- **Cognitive Automation**
  - symbols
  - situational picture

- **Cognitive Automation**
  - goals
  - planning
  - commands
  - sensor-actor execution

- **Cognitive Automation**
  - signals
  - actions

- **Cognitive Automation**
  - signs
  - figures

- **Cognitive Automation**
  - symbols
  - situational picture
Research Items on FTC in Complex HC Automation

• To understand the features of complexity – how they emerge – how they can be avoided or at least be restricted

• A new approach on information theory to cope with complex, multi-modal SW functions and their “virtual” nature (classical control theory is obsolete)

• A new paradigm of formal methods, description symbols and semantics to visualise complex mode switching systems in their entirety (incorporating model based design, model checking, theorem proving). Comparable to the invention of cybernetic block diagrams from 1940, and the computer science SW flow chart from 1970)

• To elaborate an appropriate HMI semantic scheme that fits to the perception of human beings in front of complex automation

• A theory of cognitive automation and human-machine interaction (machine learning, reasoning, situation recognition, goal driven decision making, rule making, visualisation of decision paths)

• The scientific concept of this science must become stable within few years, especially semantic, syntax, symbolic, methods and tools. It has to become essential part of the engineering and computer science education.
A330 / A340
setting long-range standards

Thanks
long-range leaders
© AIRBUS S.A.S. All rights reserved. Confidential and proprietary document.

This document and all information contained herein is the sole property of AIRBUS S.A.S.. No intellectual property rights are granted by the delivery of this document or the disclosure of its content. This document shall not be reproduced or disclosed to a third party without the express written consent of AIRBUS S.A.S. This document and its content shall not be used for any purpose other than that for which it is supplied.

The statements made herein do not constitute an offer. They are based on the mentioned assumptions and are expressed in good faith. Where the supporting grounds for these statements are not shown, AIRBUS S.A.S. will be pleased to explain the basis thereof.