RESILIENCE IN AVIATION: THE CHALLENGE OF THE UNEXPECTED

Jean Pariès  Dédale SAS France
The current aviation safety "paradigm"

- Design, build and maintain "reliable" and "safe" technology
- Anticipate all situations
- Automate what can be automated
- Specify the "right" behavior (procedures)
- Select the "right" operators
- Train them to follow procedures
- Detect and explain "errors" to prevent them
- Blame the deviants (violations)
- Monitor the outcome
- Modify the system accordingly
Aviation safety: the total predetermination dream

More order
Less uncertainty
Does it work?
One hundred time safer

GLOBAL PASSENGER FATALITIES PER 100 MILLION PASSENGER MILES, SCHEDULED COMMERCIAL AIR TRANSPORT OPERATIONS, EXCLUDING ACTS OF UNLAWFUL INTERFERENCE

1968: 0.5  After 1997: < 0.05
Still improving

One flight per day = 9000 years between 2 fatal accidents
But...
“Things that have never happened before happen all the time”
Scott D. Sagan (The Limits of Safety)
15th Feb 2009: US Airways 1549

2,818 feet
Hit flock of Canada Geese
An anticipated event

- Bird strike, dual engine failure, ditching, are anticipated events
- In real life:

  • "It was the worst sickening pit of your stomach, falling through the floor feeling, I've ever felt in my life. I knew immediately it was very bad"

  • "My initial reaction was one of disbelief. 'I can't believe this is happening. This doesn't happen to me"

Captain Sullenberger
US Airways Flight 1549
58, 19663 flight hours
Patrick Harten
Air Traffic Controller

- 35, 10 years of experience, 12 emergencies
- “We’re gonna be in the Hudson”:
  - “I asked him to repeat himself, even though I heard him just fine. I simply could not wrap my mind around those words.”
- When A/C disappeared from radar screen:
  - “The truth was, I felt like I was hit by a bus”
Use of procedures

- Engine Dual Failure
  - 3 pages long, 3 parts: fuel, relight, prepare for ditching
  - Crew was able to complete most of part 1, not able to start parts 2 and 3.

- Ditching
- Evacuation on water

NTSB report: “None of the contacted A320 operators included in their training curricula a dual-engine failure scenario at a low altitude or with limited time available.”
Sacrificing decisions

- "I quickly determined that we were at too low an altitude, at too slow a speed, and therefore we didn’t have enough energy to return to La Guardia, because it’s too far away and we headed away from it. After briefly considering the only other nearby airport which was Teterboro in New Jersey, I realized it’s too far away. And the penalty for choosing wrongly, and attempting to make a runway I could not make might be catastrophic for all of us on the airplane plus people on the ground”.

- An implacable trade off:
  - the Hudson: almost certainly bad, but possibly not catastrophic.
  - Surrounding airports: possible happy end, but almost certainly catastrophic in case of failure of the attempt.

- Minimizing the odds of a disaster by deliberately sacrificing the most ambitious, potentially happy ending – but intolerant-branch of the options tree.
4th November 2010 Qantas 32
Uncontained engine failure

- Departure from Singapore.
- Passing 7 000 ft initial climb, a loud « bang bang » from one engine is heard by the crew.
- Climb is stopped, emergency message sent to Air Traffic Control;
- ECAM indicates engine #2 overheat then fire. Extinguishers used twice, no feedback
- Engines #1 & 4 in downgraded mode.
- Crew starts check-lits: will last 55 minutes
3 ECAM pages of inoperative systems

- **Hydraulic circuits**: (2 on A380: green and yellow):
  - green is lost, as well as 2 pumps on engine # 4. Crew wonders why, as engine still running

- **Flight controls in alternate law**:
  - speed and bank angle protections are lost
  - Leading edge slats are lost, ailerons and spoilers are partially lost

- **Fuel system**: (11 tanks on A380: 4 feed tanks -1 per engine, + 3 tanks in each wing, + 1 trim tank in the horizontal stabilizer)
  - Fuel imbalance develops, but no leak message, while FO2 could see a leak on left wing from the cabin. Crew decides not to follow ECAM instruction to transfer fuel.
  - Fuel dump system does not work
  - Fuel transfer from trim tank inoperative: balance will slowly shift to the rear.

- **Brakes**: (1 front gear, 2 fuselage gears, 2 wing gears, 22 wheels)
  - Anti-skid lost on wing gears, braking lost on left wing gear

- **Electrical circuits**: (1 generator per engine + 2 on APU). Each one feeds a BUS with automated transfer.
  - BUS 1 and 2 are lost. Crew starts APU but automated transfer fails.

- **Pneumatic circuit**: a leak triggers avionic system overheat

- **Auto-thrust and Auto-land systems inoperative**

- **Software unable to compute will all these failures**.
  - Landing distance calculation task entrusted to 5th pilot. Only most relevant failures are retained.
  - Calculation gives a margin of 134 meters on a 4000m long dry runway!
Time to go back...

- Crew checked aircraft maneuverability at 235kts
- Descent to 4000ft, flaps to position 1 then 2 then 3 (landing). Maneuverability check again.
- Emergency landing gear operation
- Fixed thrust on engines 1 & 4, speed controlled by engine #3 only
- Landing at 168 Kts, max braking, max reverse thrust on engine #3.
- A/C stops 100m short of runway end, as per calculation!
- Brakes temperature reaches 900°C
- 3 engines stopped: #1 unstoppable
- Impossible to connect APU: no air conditioning, only one radio
- Passengers evacuation: what is best?
  - emergency evacuation among fire brigade trucks and one running engine?
  - Lengthy stool disembarkation with high fire risk from overheated brakes?
Uncertainty management

- Multiple risk assessment / decisions
  - Land asap or do check-lists?
  - Transfer fuel or not?
  - Overweight landing or extended flight duration? Evacuation or disembarkment?

- 5 pilots:
  - 1 CAPT, 2 Fos,
  - 1 CAPT being trained as a check airman, 1 CAPT supervising the “trainee”

- Adaptability: use of procedures framed by an overall assessment of the situation risks balance
  - Presented as: we followed all procedures...
30th May 2009 Air France 447
Flight plan

- Take off from Rio de Janeiro at 22H29 UTC
- About 10h40 flight duration
- Last radio contact with ATLANTICO (Brazil) at 01 h 35 on INTOL, FL 350
- No transfer between ATLANTICO and DAKAR
Flight events

02h08’07” PNF suggests heading change to the left.

3rd unsuccessful attempt to reach DAKAR CONTROL

02h 02 : CAPT leaves cockpit for rest

01h 55’: CAPT wakes FO1 up

01h 59’ 30” – 02h01’ 45”: CAPT attends briefing between FO2 and FO1

01h 45’- 01h58: CAPT and FO2 discuss navigation strategy (turbulence) - FO suggests level change, CAPT disregards

01 35 : Last radio contact (with Atlantico)
02h11’42”
CAPT back to the cockpit
“we have lost control on the aircraft;
There is no one instrument left”

02h10’50”
Stall warning
Thrust levers on TOGA
Pitch up input maintained
Pitch about 12°

02h10’27” to 37”
PNF: “beware of your speed” ;
“descend”
PF: “OK, OK, I descend”

02h10’14” to 26”
PF fights with roll instability
Pitch inputs lead to increasing pitch (up to 20°) and VS up to +7000ft/mn

02h 10’05”:
AP and ATHR disconnect
PF: “I have controls”
8° roll to the right
Side stick input to the left and pitch up
Speed drops from 275kt to 60 on CAPT PFD then to 130Kt on ISIS.
Altitude drops -300ft

02h 10’09 to 13 ” Stall warning (twice)
PNF: “what’s that?”
Pitot probes and ice crystals

- Ice crystals bounce against very cold surface:
  - No ice accretion on aircraft airframe
  - Not detected by aircraft ice detector
  - Not visible on weather radar
  - Not known to affect Pitot probes
Use of procedures

**UNRELIABLE SPEED INDICATION/ADR CHECK PROC**

- **If the safe conduct of the flight is impacted:**
  - **MEMORY ITEMS**
    - AP/FD OFF
    - A/THR OFF
    - PITCH/THRUST:
      - Below THRUST RED ALT 15° TOGA
      - Above THRUST RED ALT and Below FL 100 10° CLB
      - Above THRUST RED ALT and Above FL 100 5° CLB
    - FLAPS: Maintain current CONFIG
    - SPEEDBRAKES: Check retracted
    - L/G: UP
  - **LEVEL OFF**
  - When at, or above MSA or Circuit Altitude:
    - Level off for troubleshooting

- **GPS ALTITUDE**
  - Display on MCDU

**To level off for troubleshooting:**

*NOTE: Check the actual flap configuration on ECAM, since flap auto-retraction may occur.*

**PITCH / THRUST FOR INITIAL LEVEL OFF**

<table>
<thead>
<tr>
<th>FLAPS EXTENDED</th>
<th>Above 65 kts</th>
<th>65 kts - 85 kts</th>
<th>Below 85 kts</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONF</td>
<td>Speed</td>
<td>Pitch (°) / Thrust (kN)</td>
<td>Pitch (°) / Thrust (kN)</td>
</tr>
<tr>
<td>3</td>
<td>F</td>
<td>/ /xxx</td>
<td>/ xxx</td>
</tr>
<tr>
<td>2</td>
<td>F</td>
<td>/ /xxx</td>
<td>/ xxx</td>
</tr>
<tr>
<td>1-F</td>
<td>S</td>
<td>/ /xxx</td>
<td>/ xxx</td>
</tr>
<tr>
<td>1</td>
<td>S</td>
<td>/ /xxx</td>
<td>/ xxx</td>
</tr>
</tbody>
</table>

**LEVEL OFF**

**TROUBLE SHOOTING**

**PITCH & THRUST TABLES**
ECAM display following AP disconnection

No mention of the origin and nature of the problem
16 events similar to AF447 (6 within AF)

- In all of them poor understanding of the situation
- “Unreliable airspeed” procedure rarely implemented
- Stall warning perceived but mostly not believed
- Memory item 5° pitch / CLB felt irrelevant (when not unknown)
LESSONS?
Underlying assumption of the current safety model

- Pilots will, while focused on their current preoccupations, ...
  - recognize any abnormal situation as abnormal
  - implement “memory items” if relevant
  - identify the situation abnormaly, and implement the relevant procedure
The ironies of procedural expectations

The system is too complex for front line operators to find out what to do in any given situation

Provide detailed procedural solutions for any situation (what to do)

Need to understand the situation sufficiently to identify the applicable procedure

Front line operators need to identify the relevant applicable procedure
In real life...

- “Fundamental surprise” (Lanir)
  - Cognitive control is (momentarily) lost!
  - It can take just a few seconds to be lost
  - Natural reflexes may be very bad

- Response depends on acquired routines
  - Principle based, generic behavior

- Currently no real training
  - The current safety model bets on “we will stay within the control envelope”
  - When done, emergency training aims at preparing to anticipated emergencies
2005 NASA report on the challenges of emergency and abnormal situations in aviation

- “some situations may be so dire and time-critical or may unfold so quickly” that pilots must focus all of their efforts on the basics of aviation—flying and landing the airplane—with little time to consult emergency checklists. The report indicated that, although pilots are trained for emergency and abnormal situations, it is not possible to train for all possible contingencies.”

- The NASA report noted that a review of voluntary reports filed on the Aviation Safety Reporting System (ASRS) indicated that:
  - over 86 percent of “textbook emergencies” (those emergencies for which a good checklist exists) were handled well by flight crews
  - and that only about 7 percent of non textbook emergencies were handled well by flight crews.
2011: FAA “Flightcrew operational use of flight path management automation” Task Force

- 46 investigation reports (accidents & incidents) issued from 2001 to 2009 as well as ASR and LOSA reports
- 20 LOC fatal accidents, 1841 fatalities, #1 killer
- Hand flying, failure management, and crew automation interaction

- Failure management:
  - Difficulty of Failure assessment,
  - Information automation (presentation of information to pilots),
  - Flight crew preparation to handle non-routine situations
  - Trade-off in proceduralization (problem solving / decision making),
  - Complexity of highly integrated functions.
Motivation: Aircraft LOC Accident Statistics

Worldwide Fatal Accidents from 2001 to 2010 for Transport Aircraft (≥ 60,000 lbs)

Fatalities by CAST/ICAO Common Taxonomy Team (CICTT)
Aviation Occurrence Categories

20 LOC Fatal Accidents: 1841 Fatalities
1756 Onboard, 85 Ground

Top-ten Consequences of Worldwide Fatal Accidents from 1997 to 2006 for Transport Aircraft (≥ 12,866 lbs)

110 LOC Fatal Accidents: ~40% of All Fatal Accidents
3,954 Fatalities: 46% of All Fatalities


The challenge of the unexpected

- It is not merely an “automation complacency” or a “loss of basic skills” issue
- Currently no real training for the unexpected
  - When done, emergency training aims at preparing to anticipated emergencies
    - The current safety model bets on “staying within the anticipation envelope”
  - No room for real surprise
  - Economic pressure
    - Need to know / nice to know
LoC recovery requires a major control mode shift

**Complexity**

- Actions based on overall comprehension of the situational threats
- The goal is to maintain «vital functions»
- Basic protective responses
- Sense-making

**Actions based on a detailed understanding of the situation:**
- Causal understanding of events
- Anticipation of future events
- Ability to trigger desired events

**Crisis control**

**Normal control**

**Situation dynamics**
The ironies of anticipation

- The competencies needed to cope with the unexpected «in real time» are those that are lost in a continuous effort to anticipate and respond to all potential threats at the system.

- Resilience implies to be prepared

... and prepared to be unprepared.
Conclusion

- Current safety strategy seeks anticipation of all potential threats, eradication of variations
- Makes the system more and more reliable within its envelope of designed-for uncertainties
- ... and more and more brittle outside it
- Safety strategies should rather recognize real world unpredictability
- ... and maintain/develop resilience features
- Design and training can help if redirected towards this perspective
- Overall paradigm shift is needed!
Thanks for your attention
What could training deliver?

- Introduce “fundamental surprise” into simulation training
- Define a “crisis management shift” protocol
- Define a typology of threats and response strategies, train to identify them in situation
- Identify and train basic, protective, “vital” actions
- Train to maintain the team: defining control handover and crisis task sharing principles
- Train to recognize when to shift priorities across goal tradeoffs
- Address some of the flight safety/training taboos
  - Blind procedural adherence
  - Simulator exercise failures: training vs checking; loss of confidence issue;
What could design deliver?

Towards a “resilient” crew/AC/ environment interaction:

- Simplify!
- Show ‘margins of manoeuvre’: flight envelope, total energy, angle of attack, potential path angle, A/C “life expectancy” (e.g. fuel endurance, gliding distance)

- Augmented monitoring:
  - Sentinel events monitoring

- Adapt interaction (displayed information, warnings, procedures, task sharing) to crew control capacity (beyond incapacitation)