2020 Foresight - A Systems-Engineering Approach to Assessing the Safety of the SESAR Operational Concept

Eric PERRIN (speaker)
Derek FOWLER
Ron PIERCE

Eighth USA/Europe Air Traffic Management Research and Development Seminar (ATM2009)
Napa, California, USA June, 29 – July, 02 2009
Even if it were 100% so, would that answer…?

Radar-like services in NRA using ADS-B

Separation down to “radar” levels i.e. 5 nm or 3 nm

ADS-B end-to-end system needs to be reliable

even if it were 100% so, would that answer…?

Whether ADS-B would be safe enough to support 3-5 nm separation…?

No! Risk of implementing a perfectly reliable but unsafe ADS-B system
**ADS-B IN NON-RADAR AREAS – HOW TO APPROACH SAFETY?**

*What we WANT system to do – Functions and Performance*

*What we DON’T want system to do – Integrity*

---

**Operation**

**ADS-B in NRA**

**Pre-existing**

**System-**

---

Good basis for a case:

ADS-B can provide the same functionality (i.e. data presented to the Controller / support tools) and performance (data accuracy, resolution, latency, refresh rate, coverage etc)

---

**ads**

**ads**

**ads**

**ads**

**ads**

**ads**

---

**radar** separation minima: accuracy, resolution, refresh rate etc

**ADSADS**

**BI N**

**NONB**

**RADAR**

**RADAR**

---

**HOW**

**HOW**

**SAFETY?**

**SAFETY?**

---

**EUROCONTROL**
A BROADER APPROACH TO RISK ASSESSMENT AND MITIGATION

• **Success** approach:
  – to show that an ATM system will be acceptably safe in the **absence** of failure
  – addresses the ATM contribution to aviation **safety**
  – defined by **Functional** Safety Requirements

• **Failure** approach:
  – to show that an ATM system will still be acceptably safe, taking account of the possibility of (infrequent) failure
  – addresses the ATM contribution to aviation **risk**
  – defined by Safety **Integrity** Requirements
Strategic Conflict Mgt

Pre-existing Hazards

Collision Avoidance

Main ATM Functions

People, Equipment, and procedures

Separation Provision

Safety Nets

System - Generated Hazards

Providence

Accident
ICAO GLOBAL ATM OPERATIONAL CONCEPT – RISK GRAPH

- Acceptable Risk
- Pre-existing Risk

Strategic Conflict Mgt

Separation Provision

Collision Avoidance

Providence

Risk R

RA

RU

RU'
Enables us to specify success \((P_{nn})\) as well as failure \((F_{nn})\) attributes.
• SESAR is required to provide capacity to meet a 1.7-fold increase in traffic by 2020 – [SESAR Deliverable D2]

• SESAR safety performance is “to improve safety levels by ensuring that the [annual] number of ...accidents ...do not increase and, where possible, decrease” - [SESAR Deliverable D2]

• EP3 Whitepaper on SESAR Safety Targets shows that satisfying both of the above requires the accident rate per flight hour to reduce, from 2005 levels, by:
  – x3 for MAC accidents
  – x1.7 for CFIT accidents
• Safety ... requirements will address both:
  – the need for ATM to maximize its contribution to aviation safety and
  – the need for ATM to minimize its contribution to the risk of an accident

[SESAR Deliverable D4]

• End-to-end ATM system needs to deliver:
  – greater functionality & performance – to mitigate the (pre-existing) risk of an accident, inherent in aviation
  – improved integrity (plus some additional f&p) – to mitigate the (system-generated) risk of failure within the ATM system causing an accident

• Need to address both bullets in each case – addressing only the second is not enough!!

[SESAR Safety Management Plan]
THE BIG QUESTIONS FOR THE SESAR DEVELOPMENT PHASE

- Will the ATM system have sufficient safety functionality & performance?
- Will it work properly, under all normal conditions of the operational environment that it is likely to encounter?
- What happens under abnormal conditions of the operational environment?
- What happens in the event of a failure within the ATM system?
- Are the Safety Requirements realistic – i.e. could a system be built to deliver them?
- Can we believe the answers to the above?

So how does one go about it?!
But how do we develop a satisfactory Safety Argument?
WE USE A REQUIREMENTS-ENGINEERING MODEL!

Each of the “think bubbles” is a logical statement – hence can be expressed as an Argument.
Arg 0
SESAR En-route Operations will be acceptably safe.

Arg 1
SESAR En-route ATM system has been specified to be acceptably safe

Arg 2
SESAR En-route ATM system has been designed to be acceptably safe

Arg 3
SESAR En-route ATM system Design has been implemented completely & correctly

Arg 4
Transition from current state to full SESAR En-route ATM system will be shown to operate acceptably safely throughout its service

Arg 5
SESAR En-route ATM system will be acceptably safe

Cr001
Acceptably safe is defined by the Safety Targets – see Arg 1.1

A0001
Assumptions as per section 8.1 of the PSC

J0001
Justification as per Section 2.2 of the PSC

So, what about the safety activities and evidence??
Activities are driven by the Argument!
CONCLUSION

• In the face of more radical changes, we cannot sustain:
  – piecemeal approach to safety, or
  – pre-occupation with system failure at the expense of functionality and performance

• The solution – a broader approach to safety assessment
  – usage of a model of aviation safety that will provide suitable safety criteria for the components of the overall SESAR concept
  – the inclusion of the operational perspective within the scope of risk assessment

“Application of good systems-engineering practices to system safety assessment”!
A FEW FUNCTIONAL SAFETY REQUIREMENTS

- The AMAN sub-function shall compute a Controlled Time of Overfly (CTO) for waypoints extending out well into En-route Airspace (typically as far as 200 nm) and down to a CTA at the Final Approach Fix or at a final merge point.
- The AMAN sub-function shall generate speed advisories for Aircraft without an RTA capability.
- The EXEC shall resolve any conflicts, as follows:
  - where the situation is time-critical, issue an “openloop” clearance to one or both Aircraft involved, or
  - where possible, and the situation is less time-critical, issue a trajectory change to resolve the conflict but return the Aircraft to its original route, or
  - where proposed by the PLNR and judged appropriate, for crossing / passing traffic, delegate separation responsibility to the FCRW according to the agreed and authorized RBT.
Aircraft wants to climb

1. FCRW
2. FMS
3. FDP
4. EXEC
5. MTCD
6. SDP(G)

Aircraft climbs

1. FCRW
2. FMS
3. FDP
4. EXEC
5. MTCD
6. SDP(G)

Repeat from 1

FCRW rejects

Conflict free

Conflict

Aircraft climbs

1. FCRW
2. FMS
3. FDP
4. EXEC
5. MTCD
6. SDP(G)

Repeat from 1

FCRW accepts