A broader approach towards SESAR Safety Assessment

Eric PERRIN
EUROCONTROL

EUROCONTROL Annual Safety R&D Seminar
22-24 October 2008, Southampton
Outlines

• Main threads of the safety approach
• SESAR: A complex portfolio to manage
• Model of aviation safety
• Success approach
• Conclusion
• Human central in the system as manager and decision-maker
• Enhanced automation
• New separation modes

Defined in 4D, gate-to-gate, including turnaround operations
 Executed as close as possible to owner's intention
 User-preferred routing (except where capacity requires structured network)

Collaborative Decision Making
 System Wide Information Management

Starting in strategic planning phase
 Continuous in the "Network Operations Plan"
 Dynamic airspace design & management
Safety approach in SESAR – Main Threads
(SESAR D6 DLM & SMP DLT)

Based on a generic safety argument
(E-OCVM, ESARR4, EC CR 2096/2005)

Consideration of human aspects in safe(r) design

Balances:
(positive) contribution to safety – “success approach”
against (negative) effect on risk - “failure approach”

A model of aviation safety

SESAR potential net contribution to aviation safety
About the need for a model of aviation safety...
Complexity of the portfolio of projects related to SESAR

- Tens of OIs
- Tens of OCEs
- A few DODs
- Hundreds of OI steps
- A few LoCs
- Hundreds of Use Cases
Three types of projects

- Potentially detrimental to safety
  - delegation of separation and ultimate responsibility in separation assurance

- Safety neutral
  - introduction of Trajectory deconfliction barrier

- Net safety benefit
  - Strengthening of the Incursion Prevention barrier by improved ground positional information and guidance facilities
Questions deserving an answer

- ATM contribution to safety?
- Suitable safety target?
- Target compliance?
- Still on target during implementation?
- Interactions understood?
- Strong and weak safety areas?
- Sequence & timing sensitive?
- If expected safety impacts fall short?
The solution: aviation risk model

The output of each project in the SESAR portfolio contributes to Operational improvements, leading to ATM changes.

These individual contributions should fit together to form an overall risk picture meeting the relevant Safety target.

A tool for piecing together individual project contributions to the overall risk picture is contained in a Safety Target Achievement Roadmap (STAR).
SESAR Portfolio Management

Portfolio Management

- Areas Oversupplied?
- Correct Level of Investment?
- Areas Undersupplied?
- Is there a possibility for a positive safety impact (design)?
- Need to screen in new projects?
- Is it acceptable?

>0

=0

<0
‘bank account’ of safety driven ATM changes.

This can be drawn upon by projects to enhance their approach to meeting challenging safety targets.
Assurance of safety in ATM needs a wider approach...
Risk Assessments – historical perspective

Derived from SAE ARP 4754 / 4761 (civil airborne systems):

- Equipment focused
- Failure based:
  - Safety Requirements mainly about reliability
  - Allowing Systems to be “reliably unsafe”...

- Maybe not a major problem historically for ATM because:
  - Systems have not been highly integrated
  - Changes have been largely equipment replacement
  - Operational changes have been evolutionary

It is a problem for the future – new concepts, automation etc
Here is a System – is it safe?

Operational Environment

System

Service

Hazards

What we don’t want system to do
Now consider a different sort of System...

Operational Environment

System

Service

Hazards

What we WANT system to do

Pre-existing

System-generated

What we DON’T want system to do
Applicability examples

- the whole of ATM (SESAR, NextGen)
- a “layer” of ATM – e.g. Separation Provision
- a new element of the ATM system – e.g. introducing ADS-B in NRA
- replacement / substitution of an element of the ATM system – e.g. GBAS
- Etc.
**A broader approach to a priori 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 is acceptably safe, taking account of the possibility of (infrequent) failure
  - addresses the ATM contribution to aviation **risk**
  - defined by **Safety Integrity Requirements**

Addressed in much more detail in the paper as well as in Eurocontrol SAME documentation and SESAR SMP (&D6)
Success & Failure approach: development and usage

- RVSM
- FARADS
- A380 WV
- STCA
- UAVs
- ACAS
- ALC in LV
- FASTI
- EUROAT
- TMA 2010+
- ADS-B
- GBAS
- TBS
- RNAV
- FABs
- Contingency Operations
- SESAR – EP3

EUROCONTROL
A few results from ongoing application to SESAR DODs Direct inputs to the design - questions to designers

- How effective is MTCD in detecting and resolving conflicting RBTs, and to what extent and degree is the need for tactical intervention thereby reduced?
- Need to show that the system needs of MONA, MTCD and TCT do not place excessive demands on the Controllers by, for example, needing excessive Controller input to keep the RBT up to date.
- How is the changeover between a TMA predefined route structure during periods of high traffic levels, and user-preferred routes during quieter periods, accomplished?
- During periods of delegated separation responsibility to the Flight Crew, does ATC continue to monitor the situation? If so, under what circumstances would ATC intervene to resolve an apparent problem?
Conclusion

- In the face of more radical changes
  - piecemeal approach to safety
  - 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.” !!
-- Questions? --

eric.perrin@eurocontrol.int
Success & Failure approach

Minimum-achievable Risk

Tolerable Risk

Pre-existing Risk

What we WANT the system to do

~ Functionality & Performance

ATM [minimum] net contribution to aviation safety

What we DON’T want the system to do

~ 1/Integrity

Failure approach

Success approach
Arg 0
[Subject X] will be acceptably safe.

Arg 1
[Subject X] has been specified to be acceptably safe

Arg 2
[Subject X] has been implemented in accordance with the specification

Arg 3
The transition to operational service of [Subject X] will be acceptably safe

Arg 4
The safety of [Subject X] will continue to be demonstrated in operational service

Cr001
Acceptably safe means that risk of an accident is [safety criteria tbd]:

A0001
[Assumptions tbd]:

C0001
Applies to [operational environment etc tbd]:

J0001
[Justification tbd]:
Arg 1
[Subject X] has been specified to be acceptably safe

Arg 1.1
The underlying concept is intrinsically safe
Arg 1.2
The corresponding system design is complete
Arg 1.3
The system design functions correctly & coherently under all normal environmental conditions
Arg 1.4
The system design is robust against external abnormalities
Arg 1.5
All risks from internal system failures have been mitigated sufficiently
Arg 1.6
That which has been specified is realistic
Arg 1.7
The Evidence for safety specification is trustworthy
Why safety assurance?

- To strengthen Safety Case:
  - Arguments are only true or false (deliberately so!)
  - Evidence is rarely absolutely conclusive
  - Assurance process tells us: how much, how obtained, how good, etc

- To demonstrate Safety Integrity Requirements satisfaction:
  - Difficult to do through testing alone – issues about software-
    test coverage, amount of hardware testing (10x MTBF),
    repeatability of human performance assessment etc.
  - Show that Safety Integrity Requirements are achievable (in
    PSSA)
  - Apply specified assurance process in SSA to give indirect
    Evidence that they have been achieved

- Content and rigour of assurance processes determined by
  criticality of system / system-element concerned –
  Assurance Levels
The application of good systems-engineering practices to system safety assessment.”