Safety Assessment Training Workshop

# The Generic Safety Argument

Derek FOWLER
JDF Consultancy LLP

February 2008

EUROCONTROL

Remember this??!!

# What is a Safety Case?

- Evolved from the Legal Case
- Comparison with Legal Cases:
  - ☑ Argument and Evidence - in safety work, Argument + Evidence = Assurance
  - ☑ Case for the "Defence"
  - ☑ Argument is paramount - basis for whole Safety Case
  - ☑ Rules of Evidence apply - much of it comes from safety assessments etc

☒ **Burden of proof rests with the "Defence" !!!**

EUROCONTROL

# Consider these statements

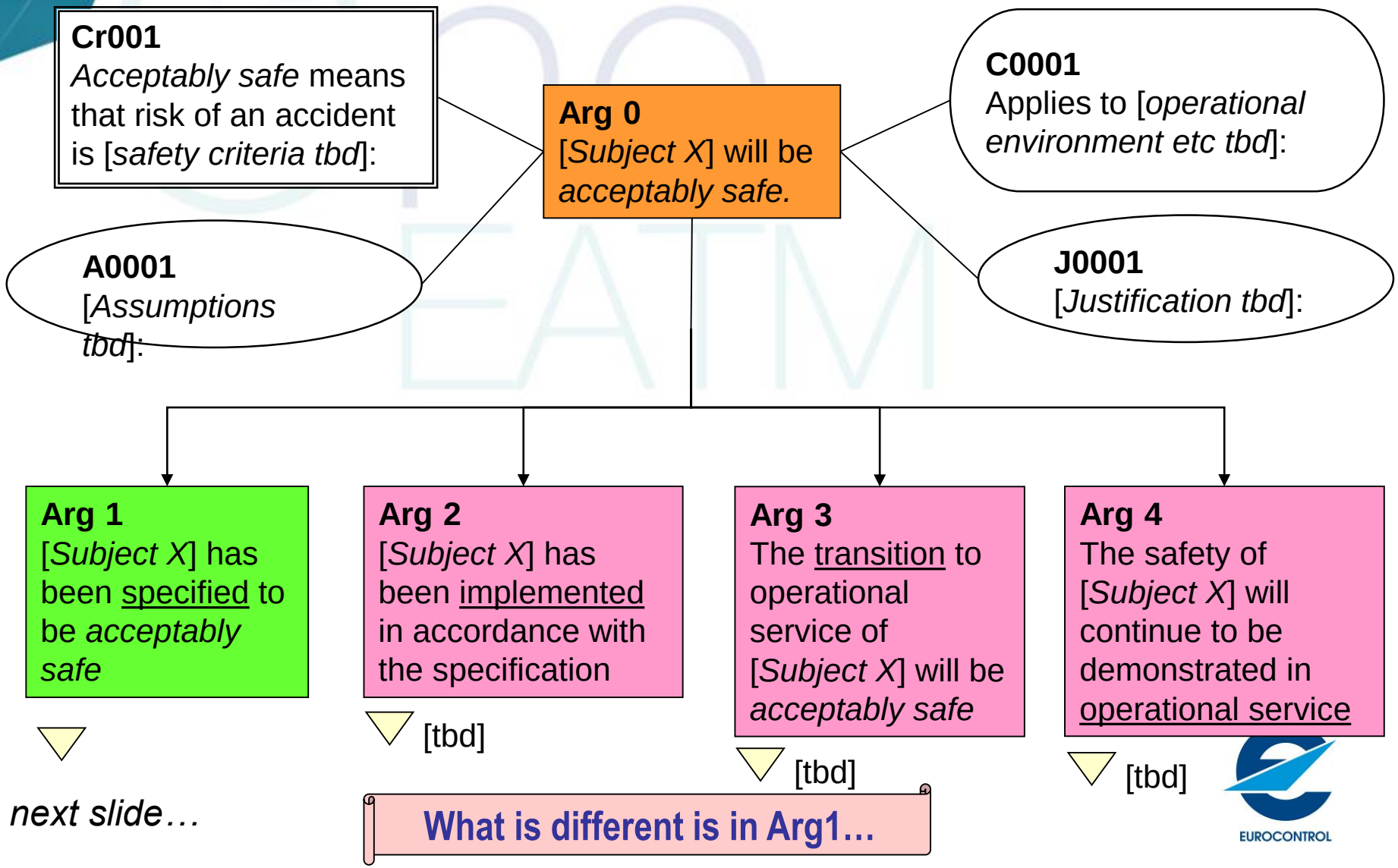
- [Subject X] will be *acceptably safe:*
  - as defined by the agreed Safety Criteria
  - in a defined operational environment

1. *Subject X* has been **specified** [ie defined and designed] to be *acceptably safe* [ie the specified Safety Requirements would meet Safety Criteria];
2. *Subject X* has been **implemented** in accordance with that safety specification
3. The **transition** to operational service of *Subject X* will be *acceptably safe*
4. The safety of *Subject X* will continue to be demonstrated in **operational service**

The first bullet is true *iff* statements 1 to 4 are all true

EUROCONTROL

# Generic Safety Argument: Arg0 (to Level 1)



# Arg1 (to Level 2)

*Fig 1*

**C002**
Applies to Concept of Operations [*ref tbd*]:

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

**Arg 1.1**
The underlying concept is intrinsically safe

[tbd]

**Arg 1.2**
The corresponding system design is complete

[tbd]

**Arg 1.3**
The system design functions correctly & coherently under all normal environmental conditions

[tbd]

**Arg 1.4**
The system design is robust against external abnormalities

[tbd]

**Arg 1.5**
All risks from internal system failures have been mitigated sufficiently

[tbd]

**Arg 1.6**
That which has been specified is realistic

[tbd]

**Arg1.7**
The Evidence for safety specification is trustworthy

[tbd]

EUROCONTROL

# 1.1 Underlying concept is intrinsically safe

- The objectives here are to show:
  - that the Concept is has the potential (in the absence of failure) to satisfy the safety criteria, assuming that a suitable system design could be produced and implemented; and
  - what the key parameters are that make it so.

EUROCONTROL

# 1.2 System Design is Complete

- The objective here is to show that:
  - Safety Requirements have been specified to cover everything, in terms of system design, that is necessary to implement the Concept (except issues relating to failure)

# 1.3 System functions correctly & coherently under all expected environmental conditions

- The objective here is to show that the system design functions correctly and coherently under all normal environmental conditions from two perspectives:
  - Static analysis of the system design
  - Analysis of dynamic behaviour

EUROCONTROL

# 1.4 System design is robust against external abnormalities

- Objective is to consider the reaction of the system to abnormal events in its operational environment:
  - Failures external to the system [cf Arg1.5]
  - Other abnormal conditions in the operational environment [cf Arg1.3]

EUROCONTROL

# 1.5 All risks from internal system failure mitigated sufficiently

- Objective is to assess internal failure of the system from two perspectives:
  - how loss of functionality would reduce the effectiveness of the system.
  - how anomalous behaviour of the system could induce risks that might otherwise not occur.

EUROCONTROL

# Arg1.6 Specification is Realistic

- Objective is to show that:
  - All Safety Requirements are verifiable – ie satisfaction can be demonstrated by direct means (eg testing) or (where applicable) indirectly through appropriate assurance processes [11]
  - All Safety Requirements are capable of being satisfied in a typical implementation in hardware, software, people and procedures.
  - All Assumptions are necessary and valid

EUROCONTROL

# Arg1.7 Direct Evidence is Trustworthy

- For Arg1.1 to 1.6, we need to provide Backing Evidence to show that the (Direct) Evidence supporting these Arguments is *trustworthy*
- This would normally be done from two perspectives:
  - the processes, tools and techniques used
  - the competence of the personnel using them

**Now for an illustration - RVSM**

EUROCONTROL

Safety Assessment Training Workshop

# EUR RVSM – Suggested Solution

Derek FOWLER
JDF Consultancy LLP

February 2008

EUROCONTROL

# Why Use RVSM Example?

- Well documented – in public domain
- Simple idea that gets quite complex!
- Still one of the best examples of an ATM Safety Case
- Takes a *success and failure* approach (see later!)

For the purposes of this example, the actual RVSM Argument structure has been changed to the *Safety Assessment Made Easier* approach

EUROCONTROL

**Definition:**
Risk of an accident:
1 Within TLS
2 is no higher than pre-RVSM;
**and**
3 has been reduced AFARP

**Justification**:
Increase capacity to meet traffic demand

**Context**
ECAC airspace only

**Claim**
RVSM is *acceptably safe.*

**Assumption:**
ATM service pre-RVSM is **tolerably** safe

**Arg 1**
RVSM has been specified to be *acceptably safe*

next slide…

**Arg 2**
RVSM will be implemented in accordance with the specification

**Arg 3**
The Switchover to operational service of RVSM will be *acceptably safe*

[tbd]

**Arg 4**
The safety of RVSM will continue to be demonstrated in operational service

[tbd]

Arg 2.1
Guidance will ensure implementation in accordance with the specification

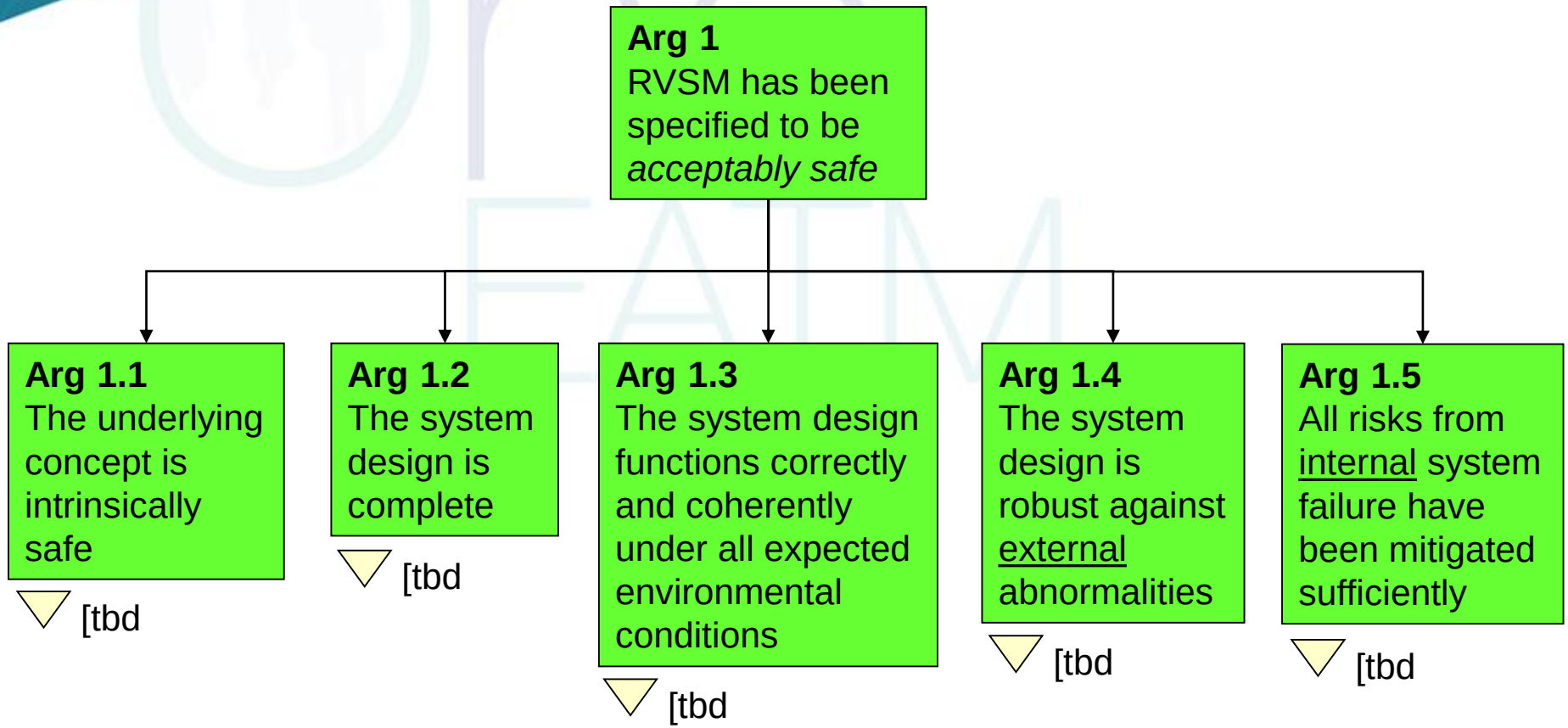
[tbd]

Arg 2.2
RVSM has been implemented in accordance with the specification

[tbd]

EUROCONTROL

# Argument 1


Arg 1
RVSM has been specified to be *acceptably safe*
Arg 1.1
The underlying concept is intrinsically safe
[tbd
Arg 1.2
The system design is complete
[tbd
Arg 1.3
The system design functions correctly and coherently under all expected environmental conditions
[tbd
Arg 1.4
The system design is robust against external abnormalities
[tbd
Arg 1.5
All risks from internal system failure have been mitigated sufficiently
[tbd

# 1.1 Underlying concept is intrinsically safe

- 1960s baro-altimetry errors above ~FL290 set VSM at 2000ft
- modern altimetry / autopilot systems are able to maintain aircraft at assigned altitude to an accuracy commensurate with 1000ft VSM
- Key parameters are specified in RVSM Minimum Aircraft System Performance Specification (MASPS)
- EUR Height Monitoring Programme shows MASPS compliance
- CRM shows compliance with failure-free TLS
- Procedures / equipment modifications to address effects of RVSM on safety of the operational environment including:
  - interfaces with non-RVSM airspace (imperial and metric)
  - what to do with non-RVSM-capable aircraft (civil and State)
  - Effects on TCAS and STCA etc

EUROCONTROL

# 1.2 System design is complete

- **Airspace Design** eg:
  - FL orientation,
  - RVSM / CVSM transition areas
  - resectorisation
- **Flight Crew Procedures** eg:
  - aircraft operational procedures,
  - RT phraseology
- **Aircraft Equipment** – included in MASPS
- **ATC Procedures** eg:
  - ATC operational procedures
  - RT phraseology
- **ATC Equipment** eg:
  - display of RVSM status
  - modification of STCA parameters
- **Flight Planning** eg:
  - AOs procedures
  - IFPS procedures and equipment modifications

All specified as Safety Requirements for implementation.

EUROCONTROL

## 1.3 System functions correctly & coherently under all expected environmental conditions

- about four years previous operational experience of RVSM in the NAT Region
- a five-year programme of fast- and real-time simulations, in 11 key areas of EUR airspace
- issues encountered and addressed include;
  - interfaces with non-RVSM airspace, especially provision of buffer areas (or unidirectional routing)
  - increase in TCAS (V7.0) Nuisance alerts

EUROCONTROL

# 1.4 System design is robust against external abnormalities

- Led to development of additional Flight Crew and ATC procedures (and associated training) for reporting and handling of, eg:
  - aircraft emergencies
  - loss of RVSM capability
  - RT failure
- Also needed to assess the risks to RVSM from the (pre-existing) effects of:
  - "level busts"
  - the severity of Wake Vortex and Mountain Wave encounters.

EUROCONTROL

# 1.5 All risks from internal system failure mitigated sufficiently

- Applied a 'conventional' SAM-type safety assessment approach, including analysis of, inter alia:
  - initial flight-planning errors – wrong RVSM status, wrong routing
  - Flight Crew operational errors,
  - ATC operational errors
  - aircraft equipment failures,
  - ATC equipment failures
- Additional (Functional) Safety Requirements for mitigations
- Safety Integrity Requirements to control hazard frequency, to keep risk within failure component of TLS

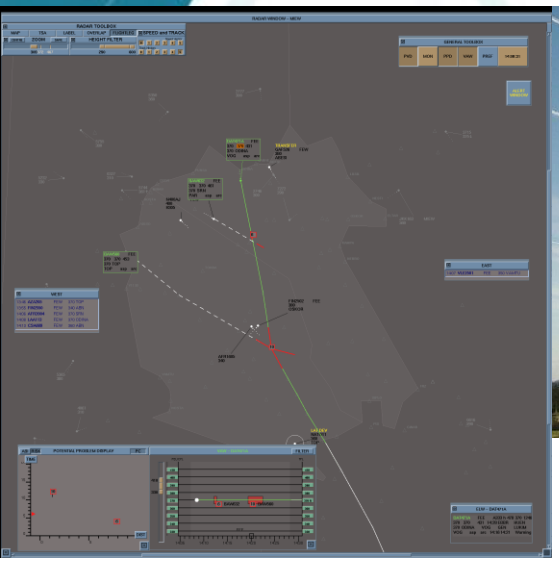
Early attempts at using RCS gave some very misleading results !

EUROCONTROL

# Conclusions on "Success and Failure" Approach

- Two types of safety-related system – those that merely present a risk to their environment and those that have a specific role – ie reducing pre-existing risk
- First type requires a **failure**-based approach, leading to the specification of the system's required **integrity**
- Second type requires an additional, **success**-based approach in order to specify the **functionality & performance** required of the overall system, since it these parameters that determine its ability to reduce pre-existing external risk
- Having established the need for the broader approach, it is no longer necessary to express this in terms of *success* and *failure* approaches
- Generic Safety Argument supports the broader approach

# Questions ??



?

EUROCONTROL