Safety Assessment Training Workshop

Success & Failure Approaches - Basics

Derek FOWLER
JDF Consultancy LLP

February 2008

EUROCONTROL

Mini-exercise – Safety = Reliability??

Safety = Reliability ??

A system can fail even though none of its individual elements has failed

[after Professor Nancy Leveson, MIT]

Tasks:

- Consider the above quote
- Think of different ways in which a system could fail without any of its individual components failing
- Give some ATM examples

Safety Assessment Training Workshop

Safety = Reliability Mini-exercise – Suggested Solution

Derek FOWLER
JDF Consultancy LLP

February 2008

A Few Thoughts…

- **Inconsistent data**: different parts of the system have different data – eg flight plan data, RNAV Waypoint locations
- **Inconsistent functionality**: different parts of the system trying to do different things – eg ATC and TCAS giving opposite instructions
- **Inadequate performance**: eg surveillance accuracy (cf separation minima); data latency (in AGA datalink); insufficient capacity (cf traffic loading)
- **Abnormal conditions**: eg aircraft emergencies; extreme weather
- **Misuse** – Arianne V !

Mini-exercise – Operational Procedures

The Überlingen Mid-air Collision

Initial Tasks

1. Ignoring the various accident precursors, decide whether you think that the collision was caused directly :
   - by failure of a system component (including human error); **or**
   - by weakness in the system design (or implementation)
2. Explain the rationale for your decision

Note that we are trying to understand what might have gone wrong, not to allocate blame!

Debrief on Initial Tasks

Precursors

- Two aircraft in conflict – same FL, crossing Tracks
- Ground-ground Comms problem - distracted Controller
- STCA not functioning
- No second Controller in Ops Room

This is an illustration, not an exhaustive analysis

EUROCONTROL

The *Collision Avoidance* Stage

- TCAS operated on both aircraft, correctly
- DHL pilot started to descend in response to TCAS RA
- Controller (twice) instructed Russian aircraft to descend – opposite to RA
- Russian pilot complied with (2nd) ATC instruction – **COLLISION**

- Did DHL pilot do what he was supposed to?
  - yes – he followed the RA
  - he was not compelled to report the RA immediately
- Did the Controller do what he was supposed to at that stage?
  - yes - he did not know there was an RA
- Did the Russian pilot do what he was supposed to?
  - did he comply with PANS-OPS / PANS-ATM?
  - did he comply with own procedures and training?

We need to look at PANS-OPS / PANS-ATM !!

EUROCONTROL

Follow-up Tasks

1. Consider the extracts (next 2 slides) from PANS-OPS and PANS-ATM concerning TCAS and ATM
2. Is there anything in them that supports or weakens your decision regarding Überlingen ?
3. Are there any other inconsistencies (ie the potential for dysfunctional interactions)
4. Could any of these lead to an unsafe state ?

“Rules” Regarding TCAS and ATC- as at May 2006 (1)

- **Who does what and when:**

PANS-OPS (Doc 8168), Part VIII, Chap 3, Para 3.1.2 states:

Nothing in the procedures specified in 3.2, “Use of ACAS indicators”, shall prevent pilots-in-command from exercising their best judgement and full authority in the choice of the best course of action to resolve a traffic conflict or avert a potential collision.

Para 3.2c) states that *in the event of an RA, pilots shall:***:**

1) respond immediately by following the RA as indicated, unless doing so would jeopardize the safety of the aeroplane;

2) follow the RA even if there is a conflict between the RA and an air traffic control (ATC) instruction to manoeuvre;

PANS-ATM (Doc 4444) states:

- ➢ *15.6.3.2 When a Pilot reports a manoeuvre induced by an ACAS resolution advisory (RA), the Controller shall not attempt to modify the aircraft flight path until the Pilot reports returning to the terms of the current air traffic control instruction or clearance but shall provide traffic information as appropriate.*
- ➢ *15.6.3.3 Once an aircraft departs from its clearance in compliance with a resolution advisory, the Controller ceases to be responsible for providing separation between that aircraft and any other aircraft affected as a direct consequence of the manoeuvre induced by the resolution advisory. The Controller shall resume responsibility for providing separation for all the affected aircraft when:*
  - *a) the Controller acknowledges a report from the flight crew that the aircraft has resumed the current clearance; or*
  - *b) the Controller acknowledges a report from the flight crew that the aircraft is resuming the current clearance and issues an alternative clearance which is acknowledged by the flight crew.*

“Rules” Regarding TCAS and ATC- as at May 2006 (2)

- **Reporting**

PANS-OPS (Doc 8168), Part VIII, Chap3, para 3.2c) states:

4) as soon as possible, as permitted by aircrew workload, notify the appropriate ATC unit of the RA, including the direction of any deviation from the current air traffic control instruction or clearance;

PANS-ATM (Doc 4444), para 12.3.1.2 states:

Para.	**Circumstances**	**Phraseologies**	
r	*... after modifying vertical speed to comply with an ACAS resolution*	***Aircrew:***	*TCAS CLIMB (or DESCENT)*
		Controller:	*(acknowledgement)*

Debrief on Follow-up Tasks

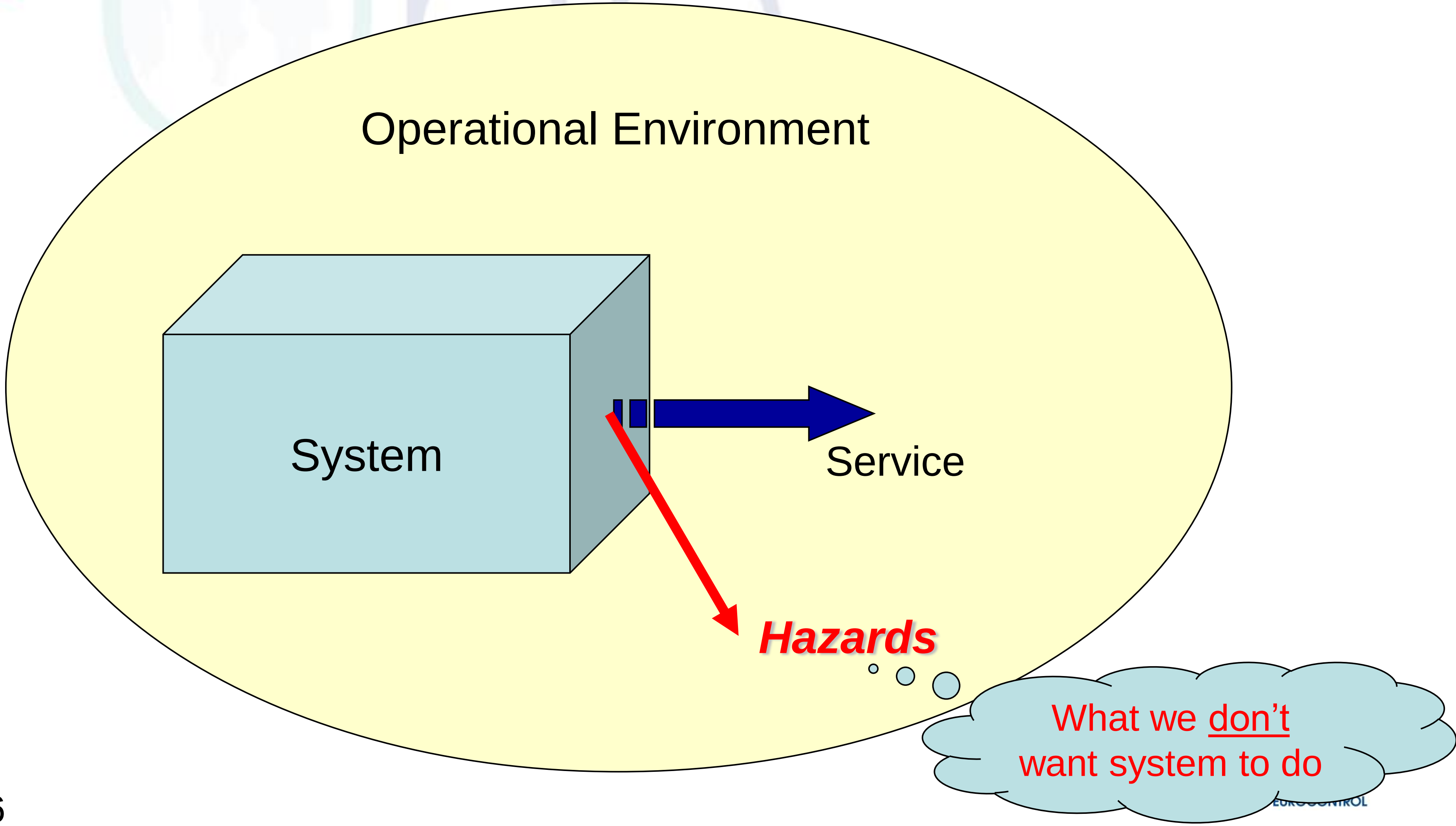
See PANS-OPS and PANS-ATM extracts with additional commentary

We are still considering only failure of the ATM system

But that's still not enough!!

Consider this situation ……………….

Here is a System – is it Safe??



Operational Environment

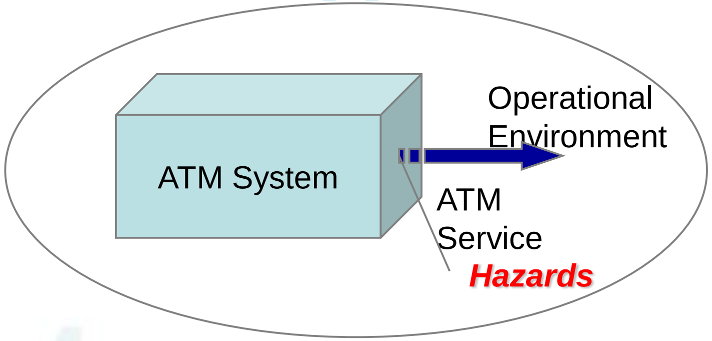
System

Service

Hazards

What we <u>don't</u> want system to do

The “Traditional” Approach



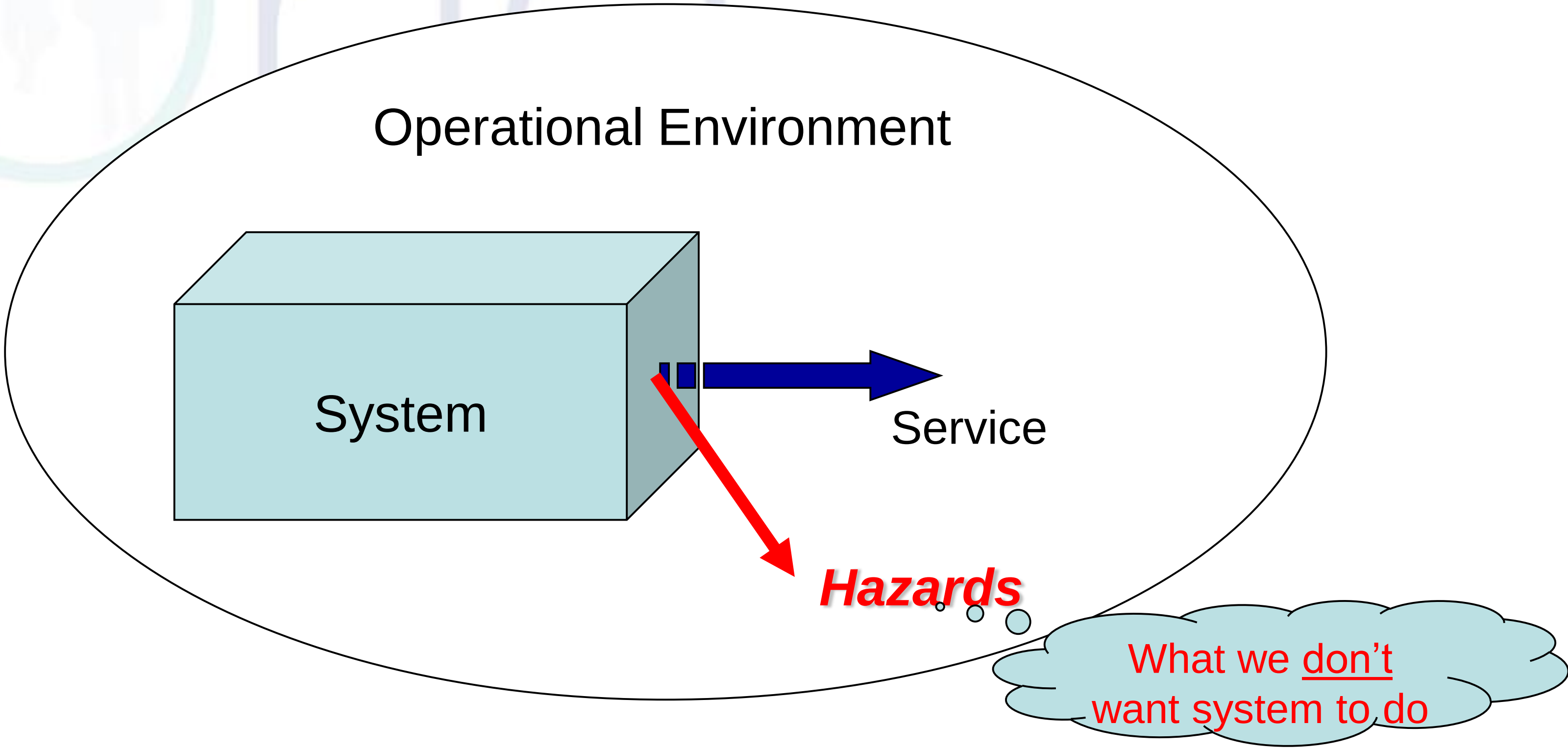
- Hazards:
  - represent some kind of failure inside the box
- Consequence Analysis:
  - how serious the Hazards are
- Safety Objectives:
  - how often we can allow the Hazards to occur

FHA

10^{-n} fixation!!

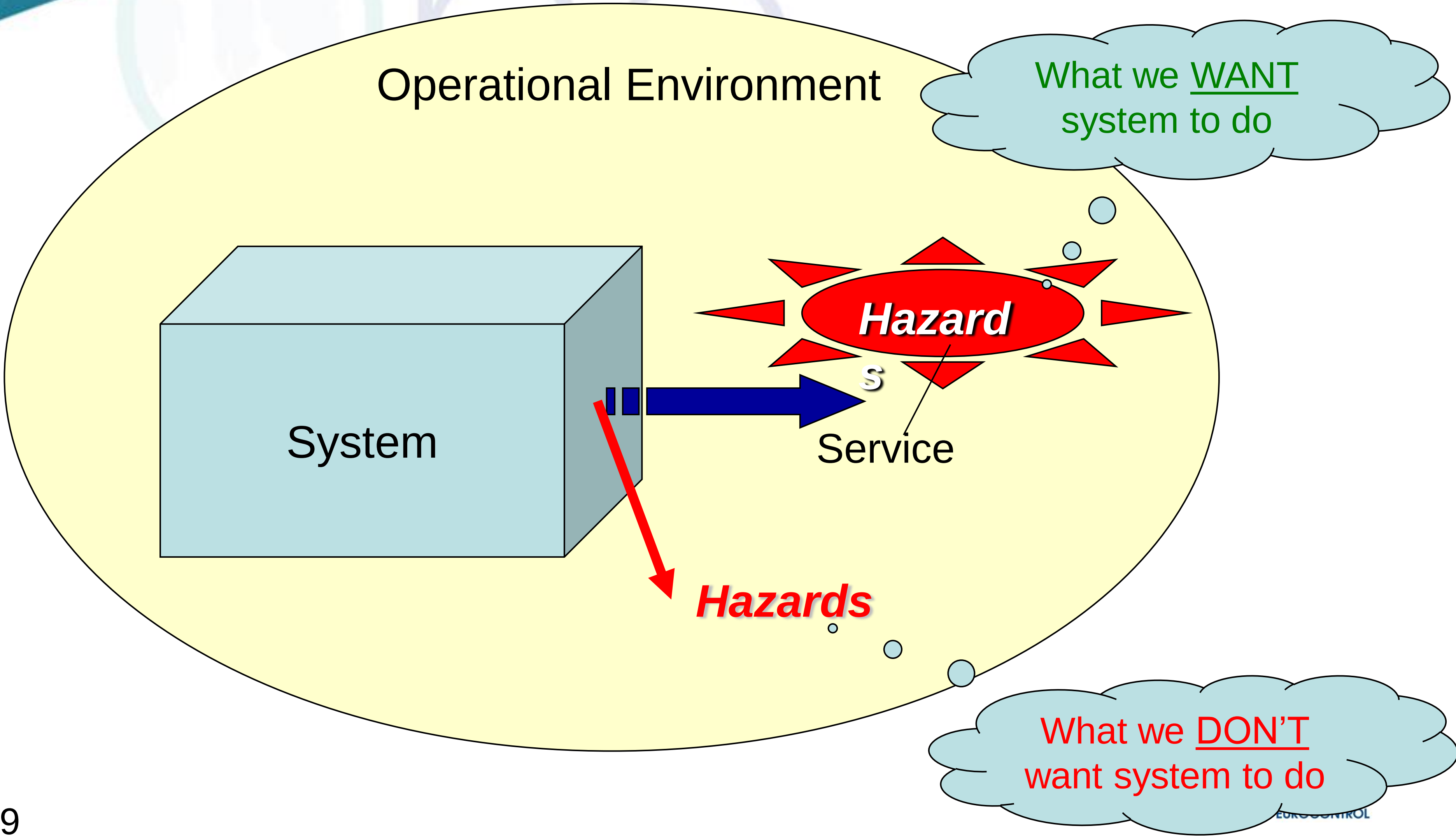
- Causal Analysis:
  - what could cause the Hazards
- Safety Requirements:
  - how often we can allow the **Causes** to occur
  - ie how reliable the box needs to be

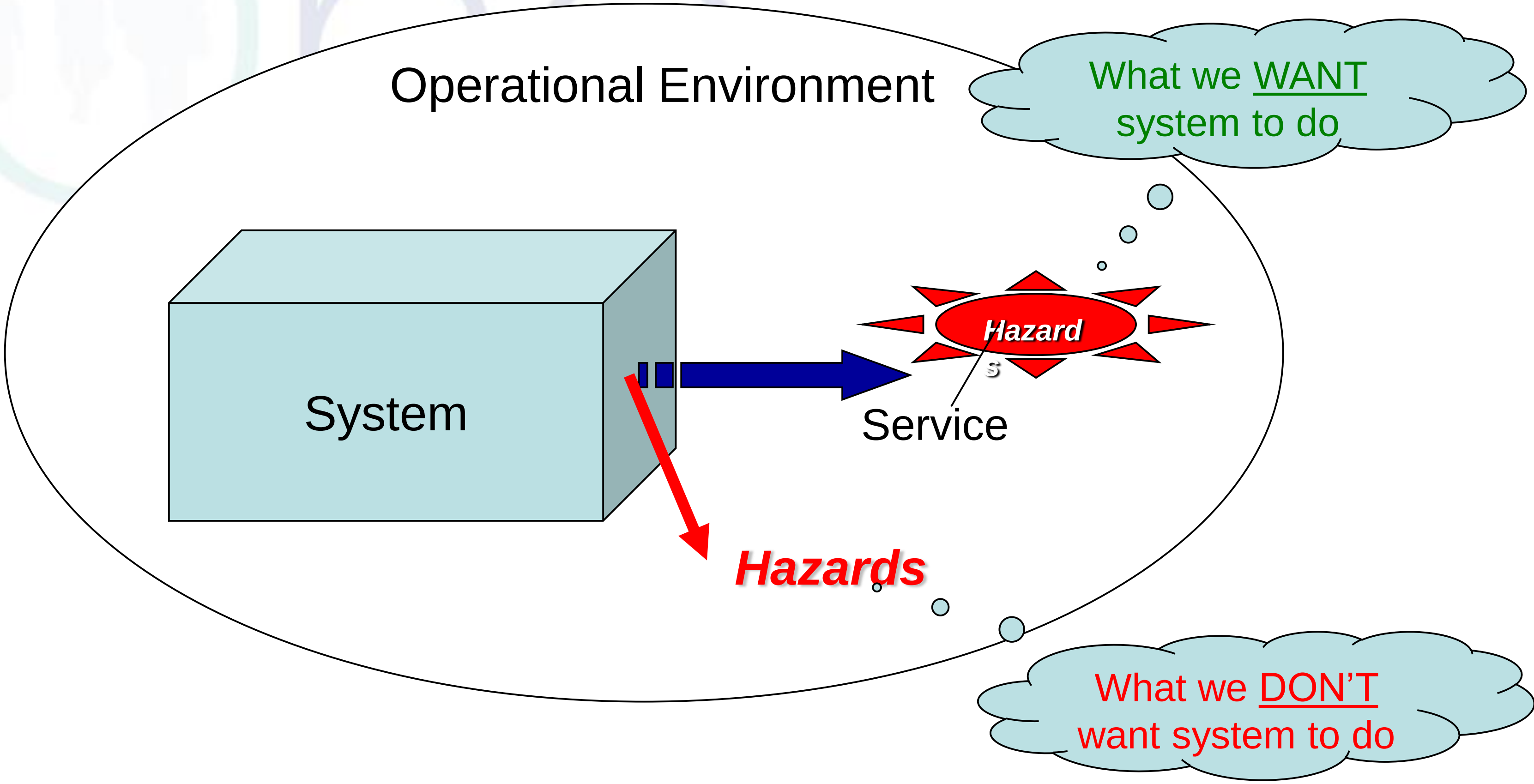
PSSA



This is OK for a nuclear power station etc!!

Now we have a different sort of System!





Operational Environment

What we <u>WANT</u> system to do

System

Hazards

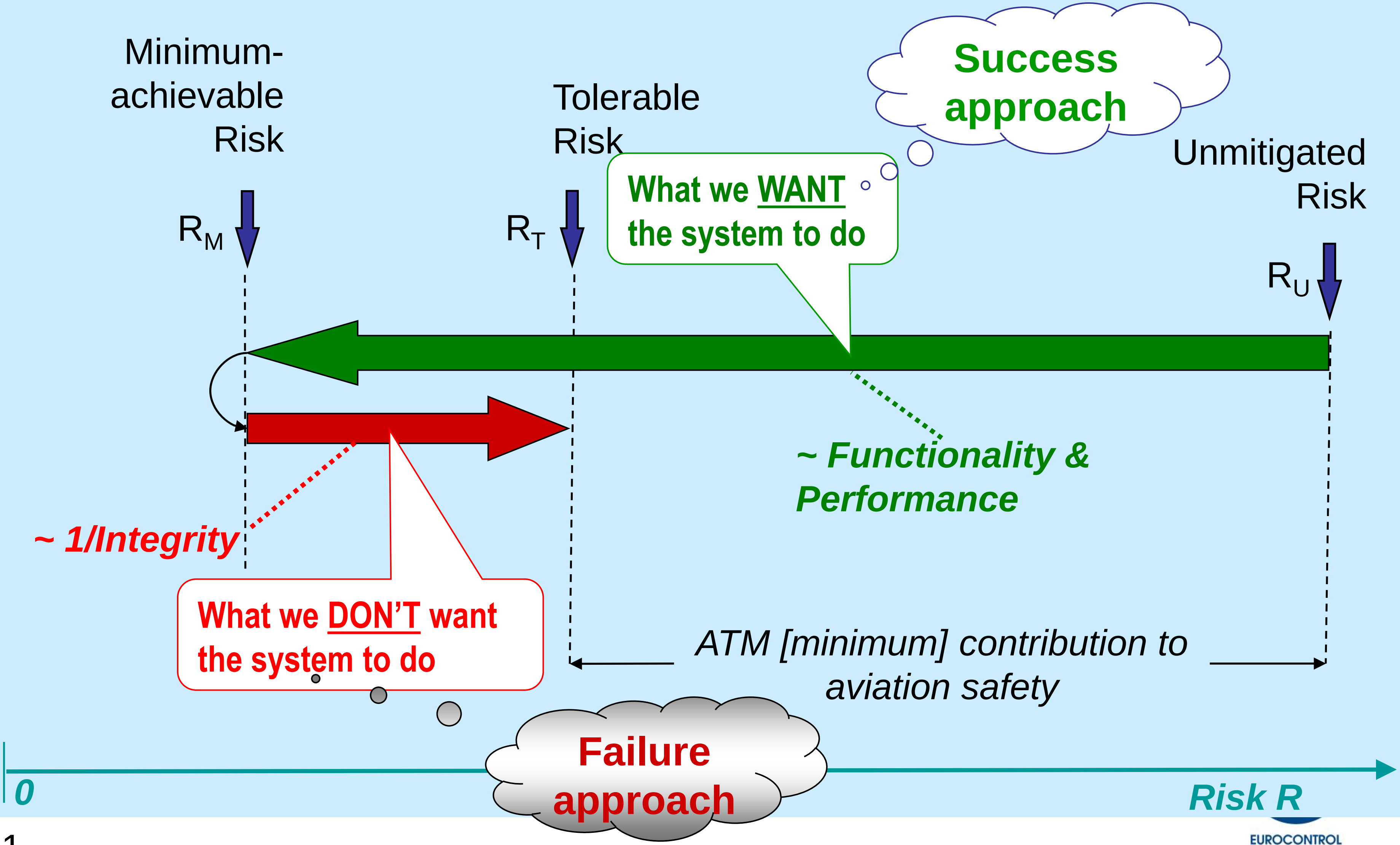
Service

Hazards

What we <u>DON'T</u> want system to do

<u>This</u> applies to ATM !!

Success and Failure Approaches



Minimum-achievable Risk

R_M

Tolerable Risk

R_T

Success approach

What we **WANT** the system to do

Unmitigated Risk

R_U

~ Functionality & Performance

~ 1/Integrity

What we **DON'T** want the system to do

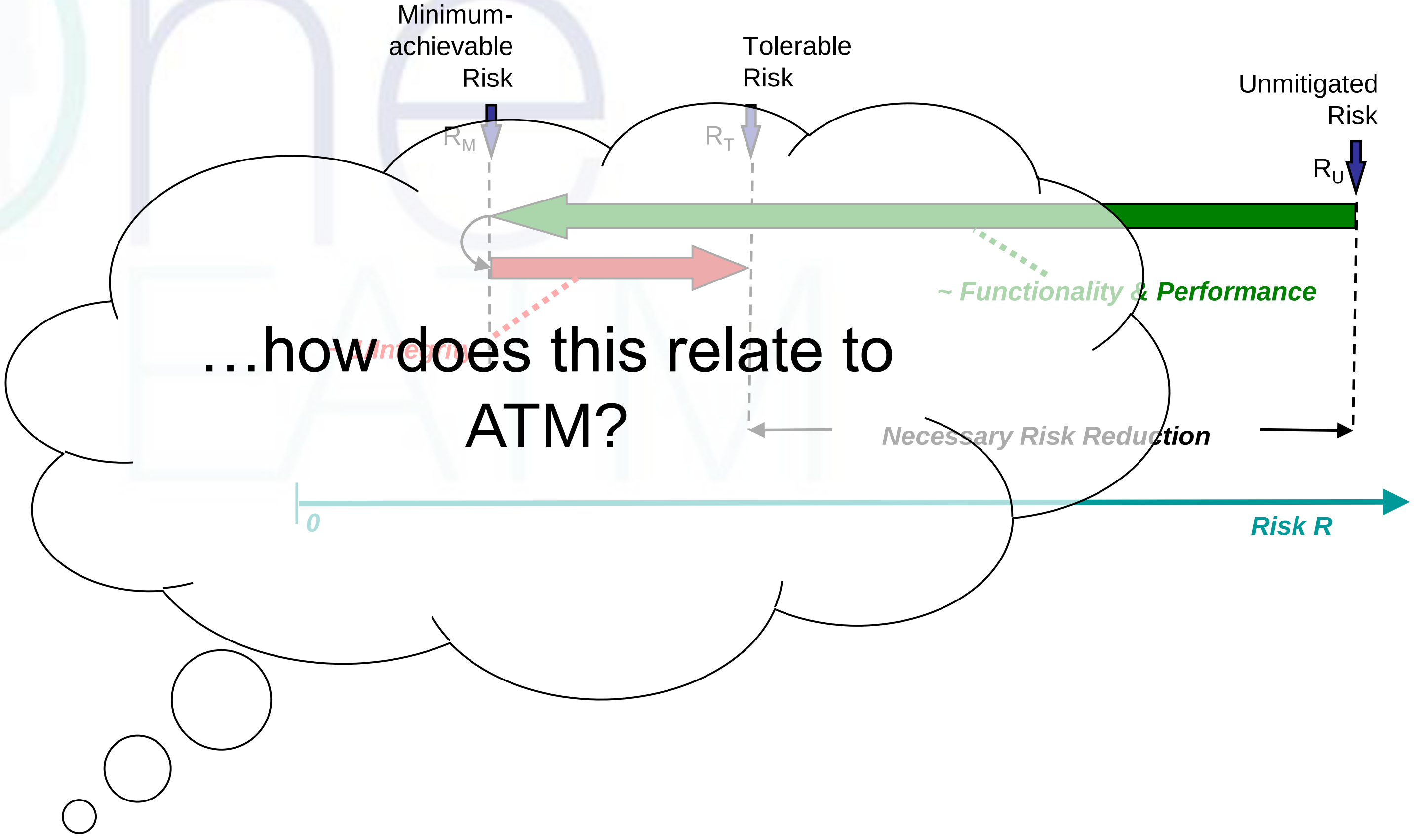
ATM [minimum] contribution to aviation safety

Failure approach

0

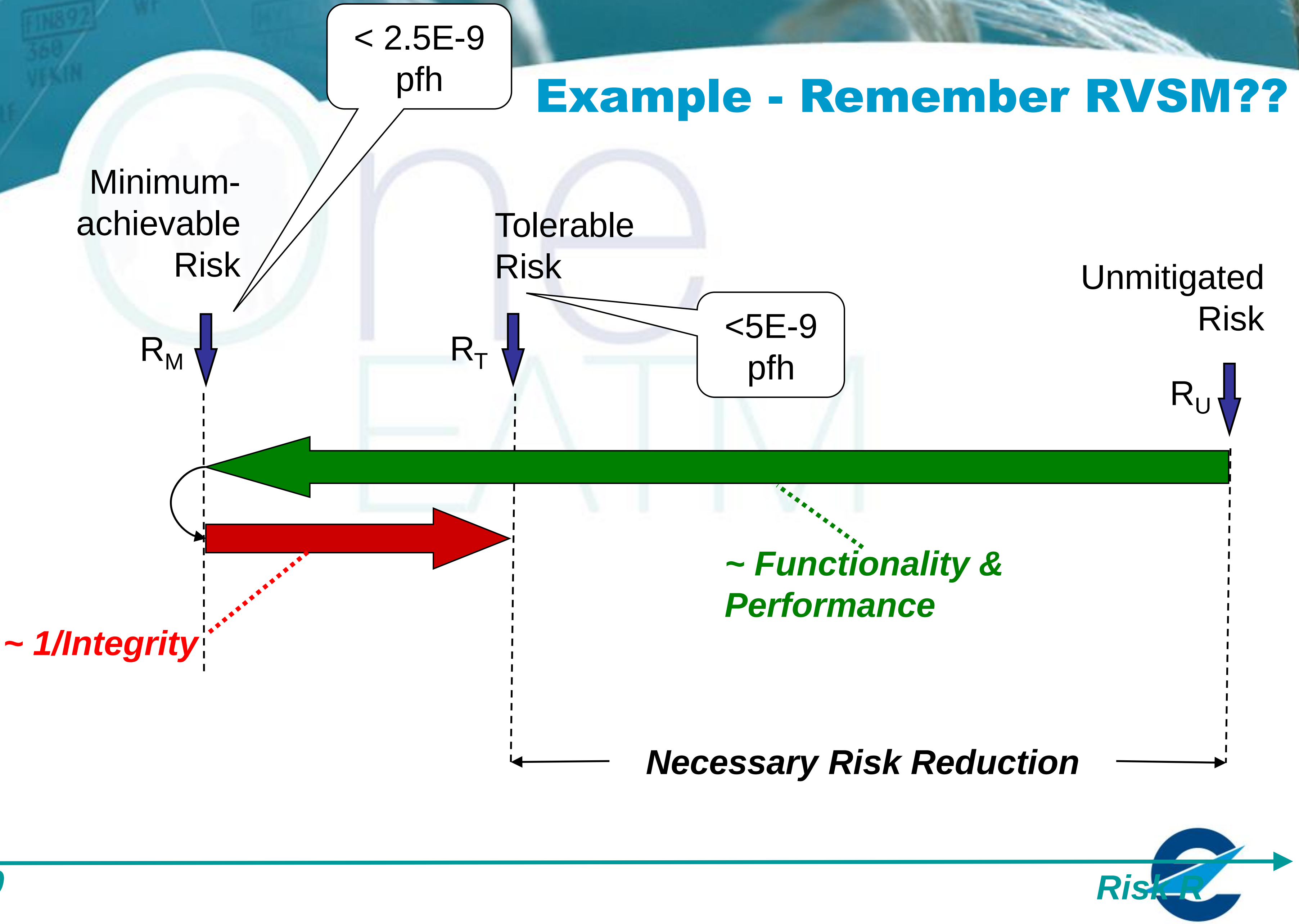
Risk R

But………

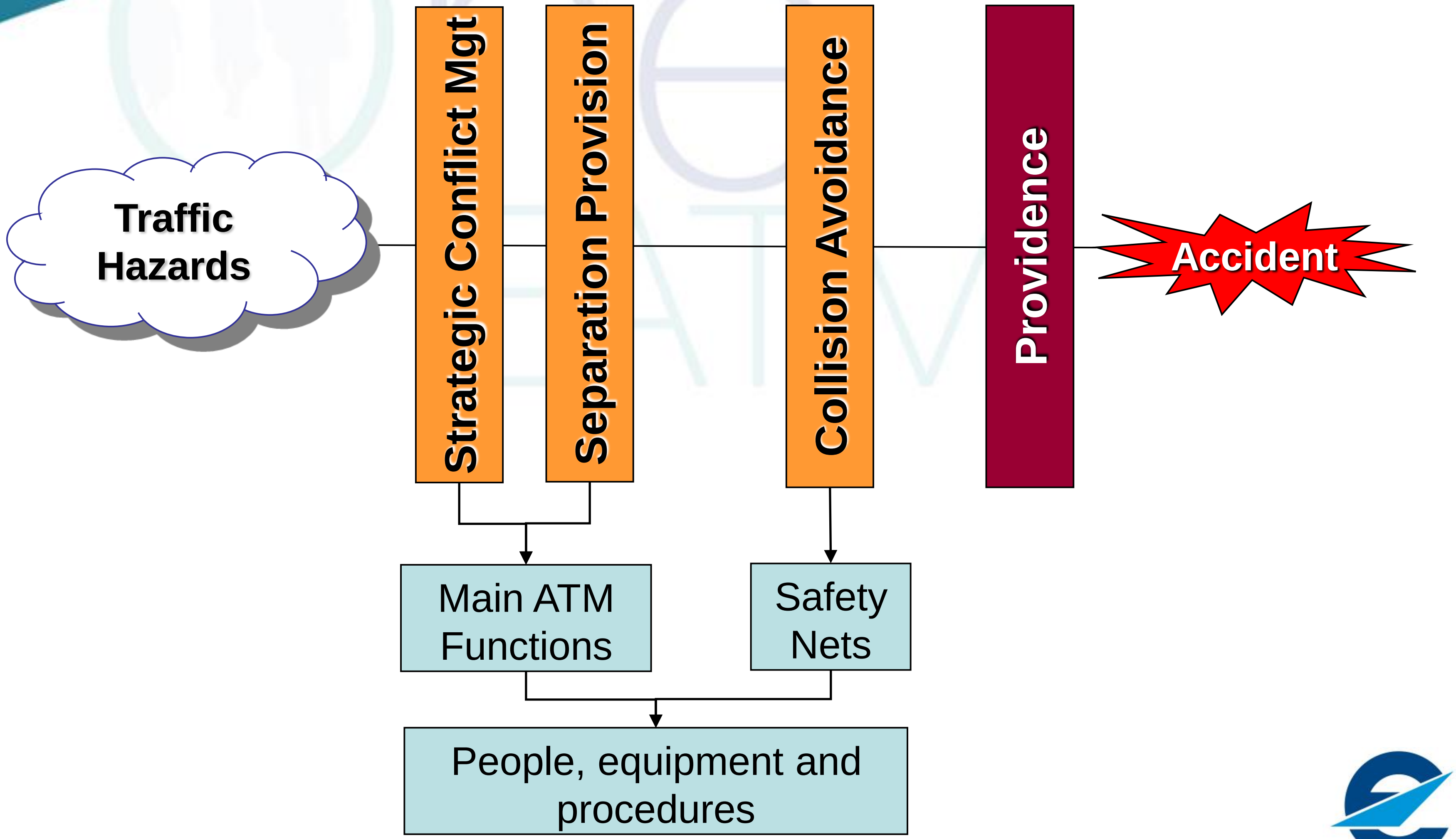


…how does this relate to ATM?

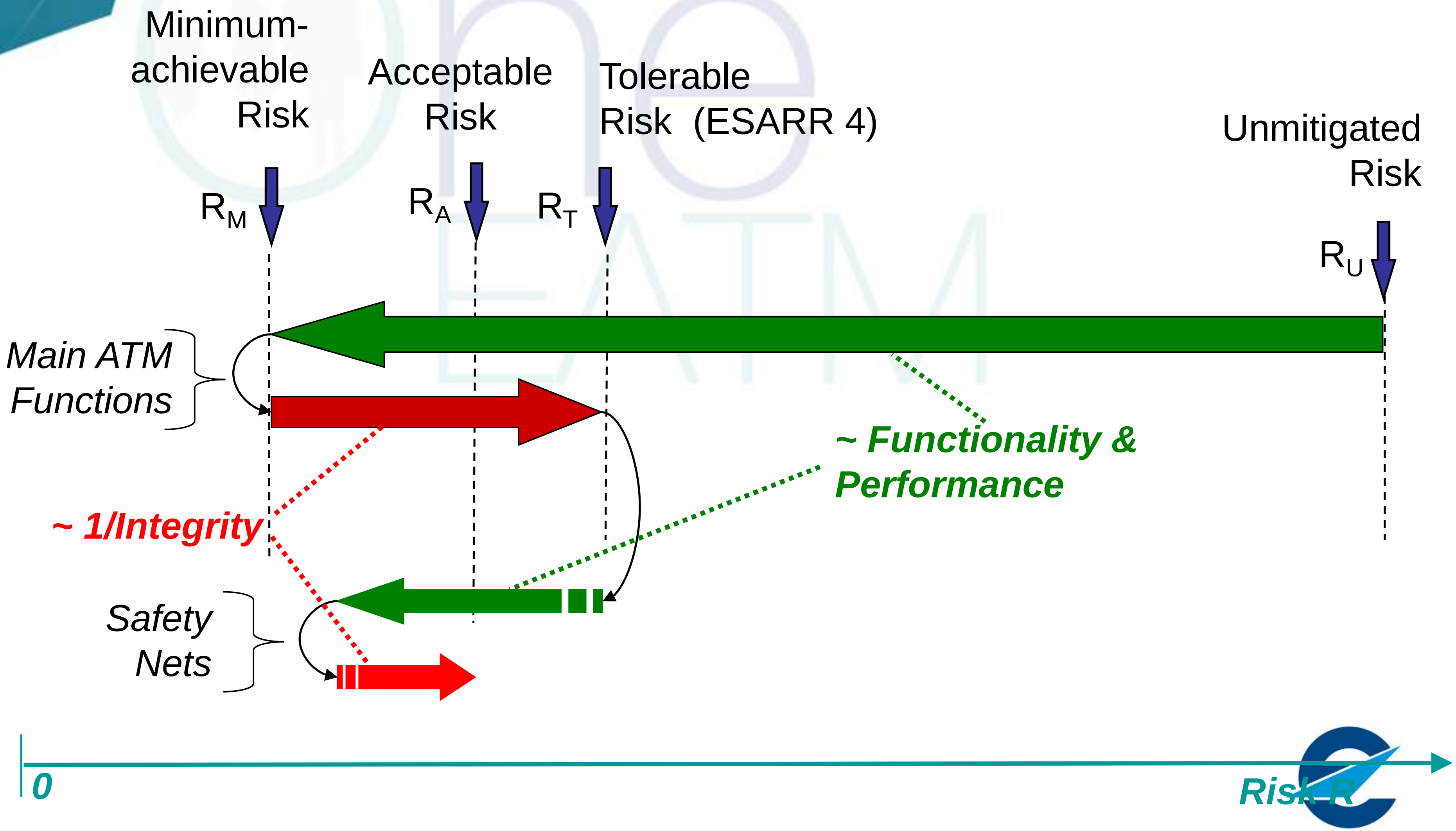
Example - Remember RVSM??



ICAO Global ATM Operational Concept 2005

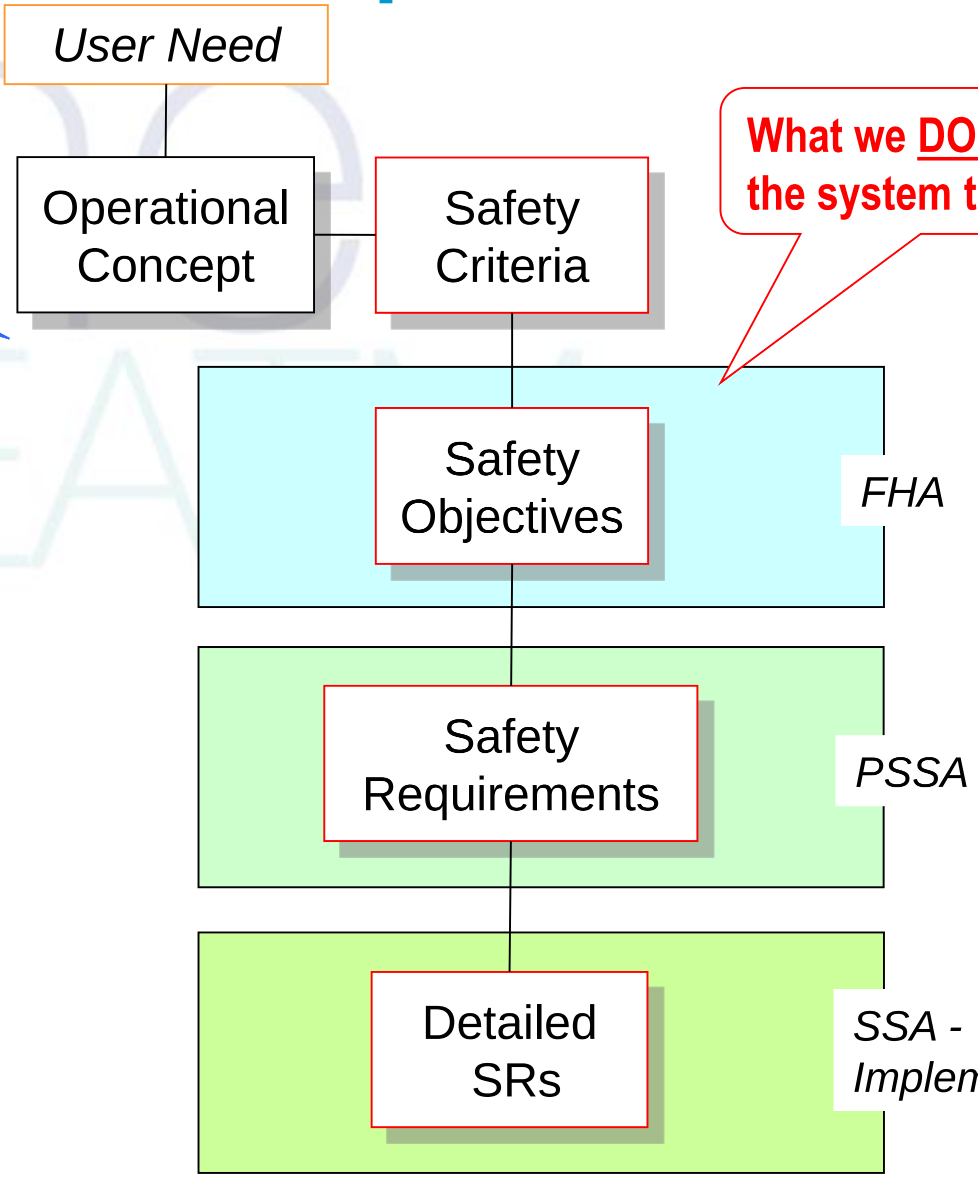


"Safety Nets"


Minimum-achievable Risk
Acceptable Risk
Tolerable Risk (ESARR 4)
Unmitigated Risk
R_M
R_A
R_T
R_U
Main ATM Functions
~ Functionality & Performance
~ 1/Integrity
Safety Nets
0
Risk R

Specification Hierarchy

“Traditional” (failure-based) approach

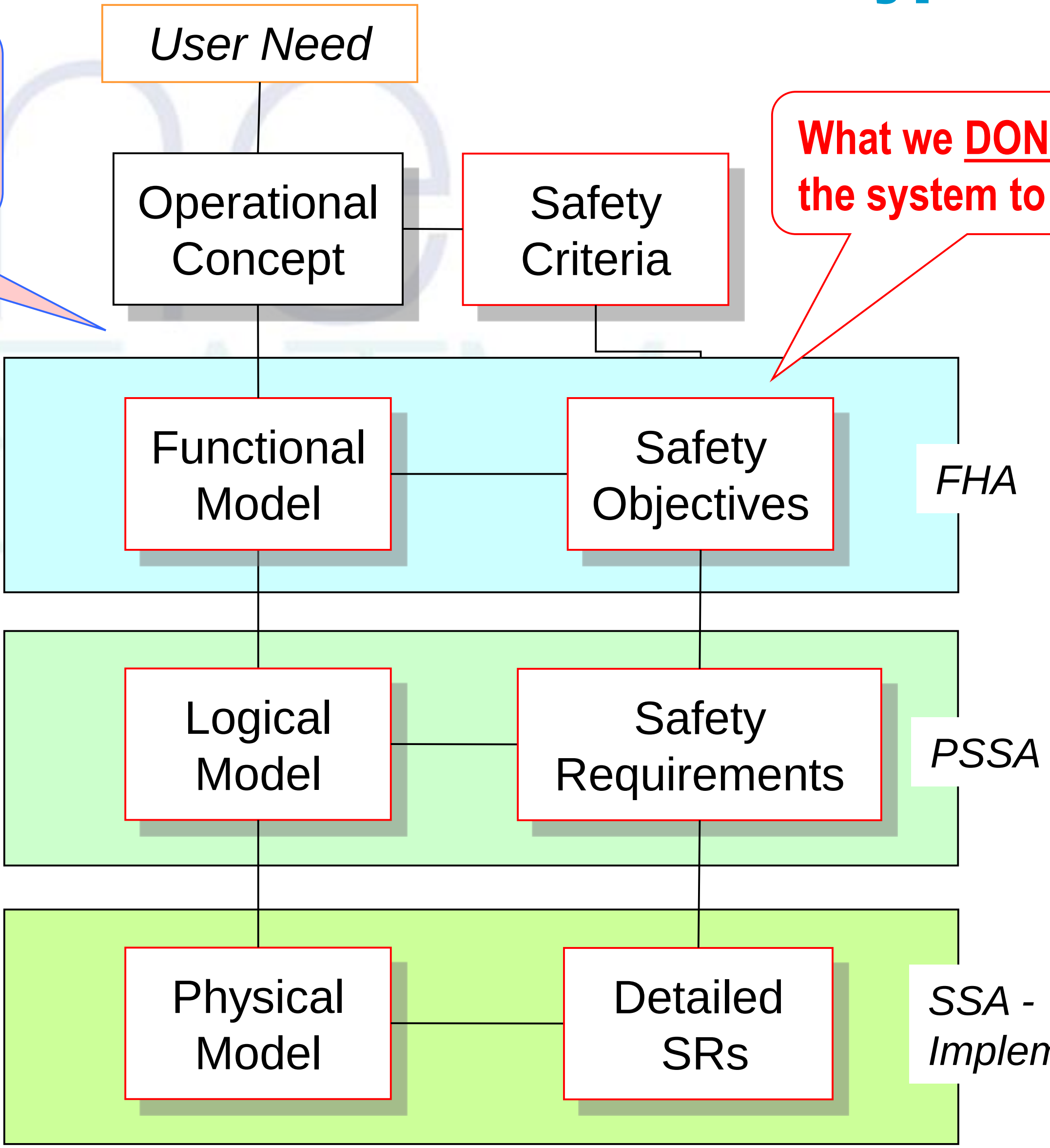


What we DON’T want the system to do

EUROCONTROL

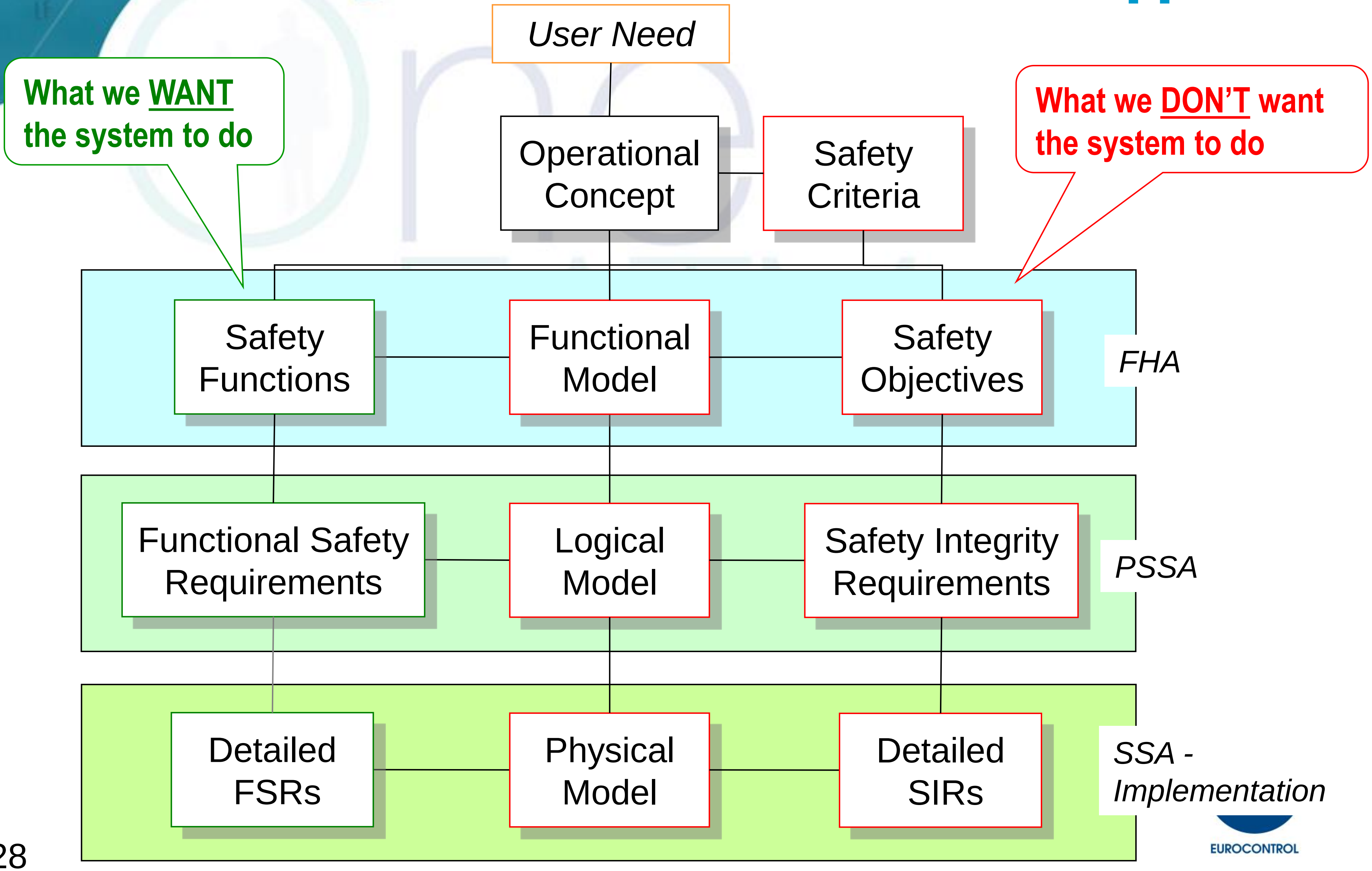
More Typically…!

“Traditional” (failure-based) approach



What we **DON’T** want the system to do

Broader Approach



What we **WANT** the system to do

User Need

Operational Concept

Safety Criteria

What we **DON'T** want the system to do

Safety Functions

Functional Model

Safety Objectives

FHA

Functional Safety Requirements

Logical Model

Safety Integrity Requirements

PSSA

Detailed FSRs

Physical Model

Detailed SIRs

SSA - Implementation

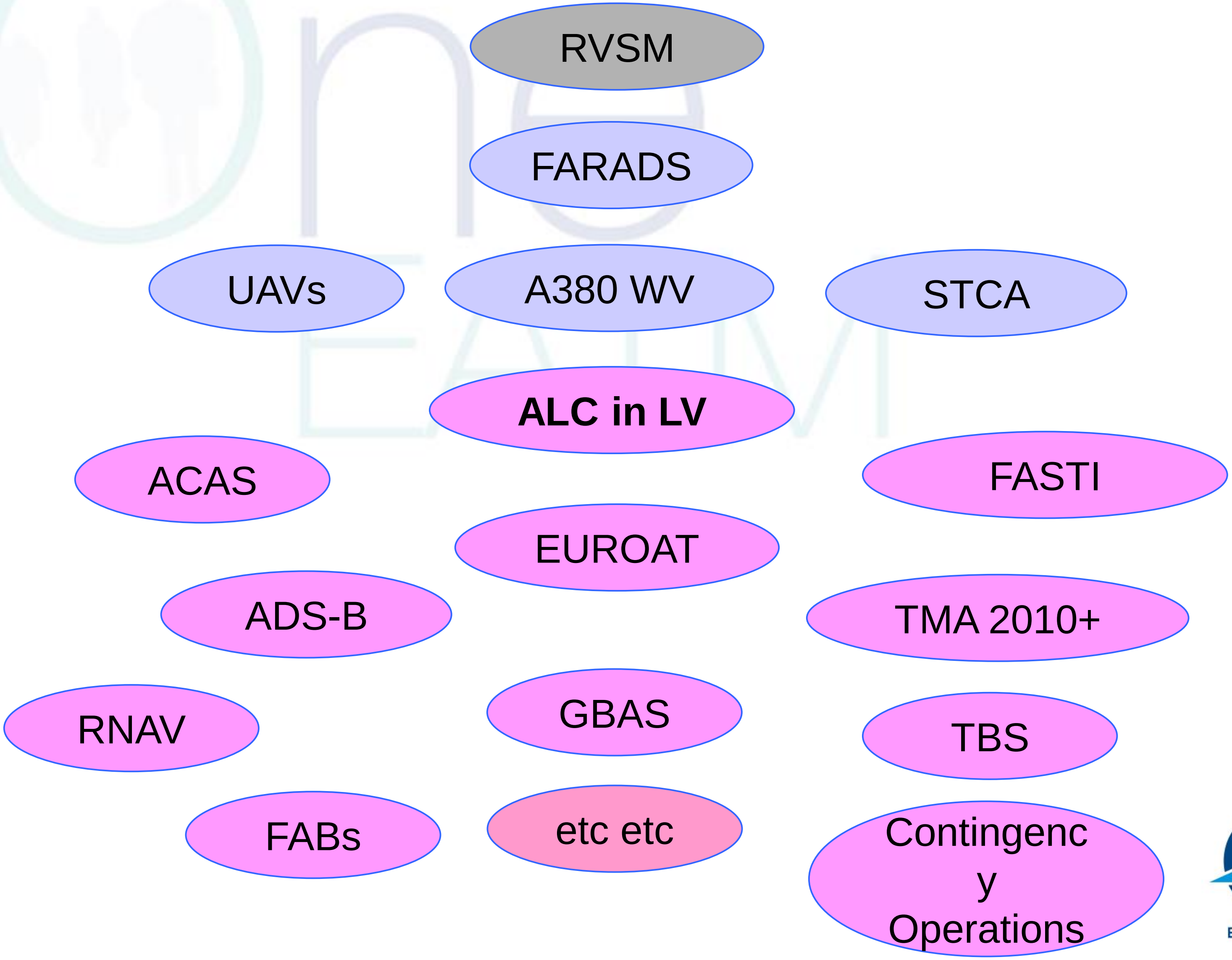
A Simplified Example

- Business case for introducing ADS-B into existing non-radar areas (NRA)
- Need to support separation minima of 3nm (Terminal Airspace) and 5nm (En-route)
- If ADS-B end-to-end system is sufficiently reliable, will it be safe?
- The Safety Case depends fundamentally on:
  - the information provided by ADS-B (to the Controller)
  - the accuracy, resolution, latency, refresh rate etc of that information
- Of course, the ADS-B system <u>also</u> needs to be reliable!

Functional Safety Requirements

Safety Integrity Requirements

Development and EATM Usage



RVSM

FARADS

UAVs

A380 WV

STCA

ALC in LV

ACAS

FASTI

EUROAT

ADS-B

TMA 2010+

RNAV

GBAS

TBS

FABs

etc etc

Contingenc
y
Operations

To summarize so far…

- Need to know what the ATM system is supposed to do (functionality) and how well it needs to do it (performance)
- Need to be sure that it well designed and will work as expected in its environment (robustness)
- Need to that it will not present a significant risk to its environment (reliability /integrity)
- This leads us to the need for a broader approach to safety assessment, to address 2 key issues:
  - How safe will new ATM systems be when working to spec?
  - How safe will they be when they fail?

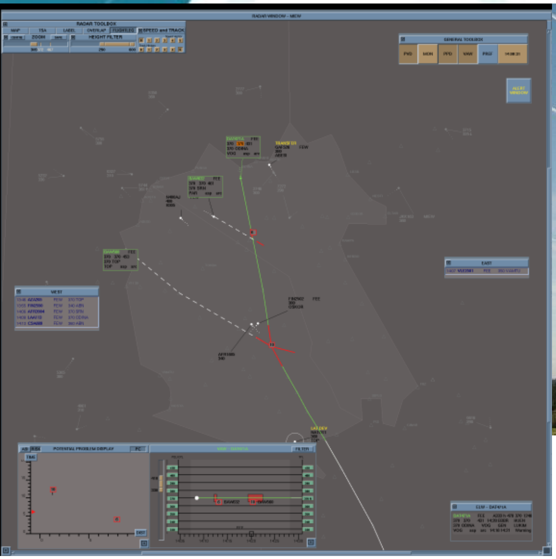
Success Approach

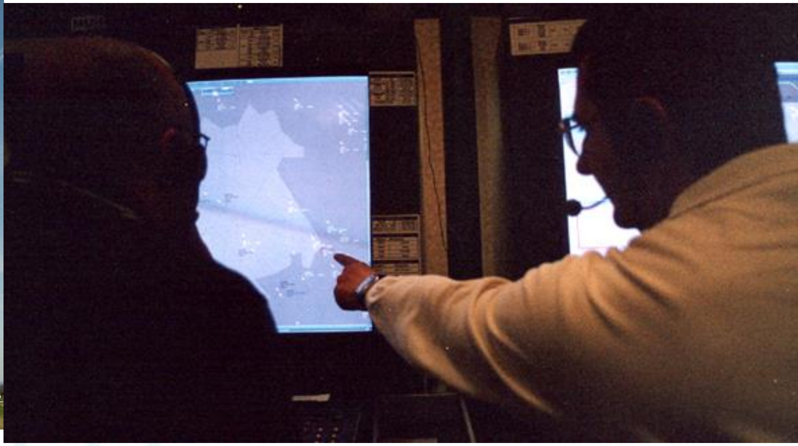
Failure Approach

Captured in a "Generic Safety Argument" – next Session!

EUROCONTROL

Questions ??





?

EUROCONTROL