Management of Change in ATM

AFI FRA Risk Assessment Workshop

Jean-Michel De Rede
Senior Safety Expert
EUROCONTROL
https://www.eurocontrol.int/safety
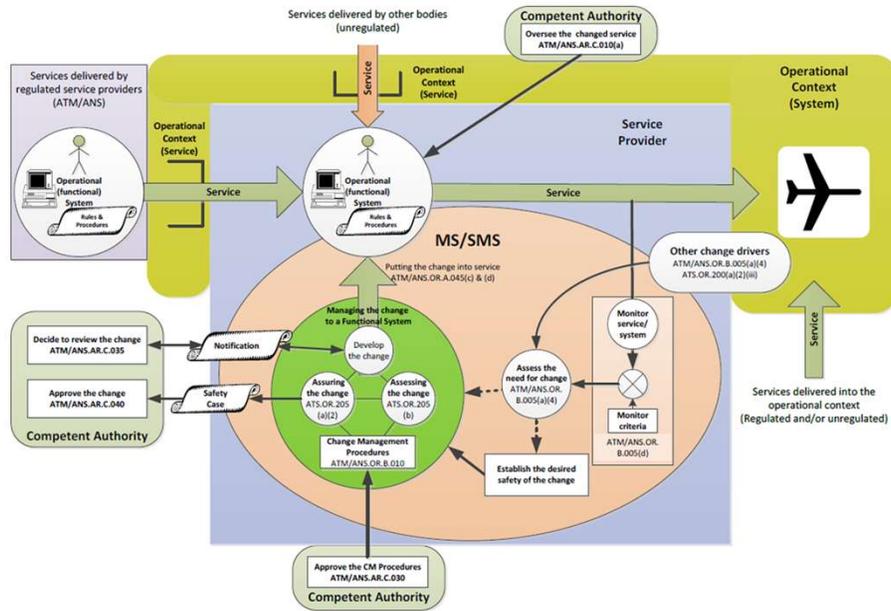
Our journey together

- Change Management within the SMS
- Change Management Procedures
- Safety Assessment Process
- Examples
  - Even Tree Analysis
  - FMEA

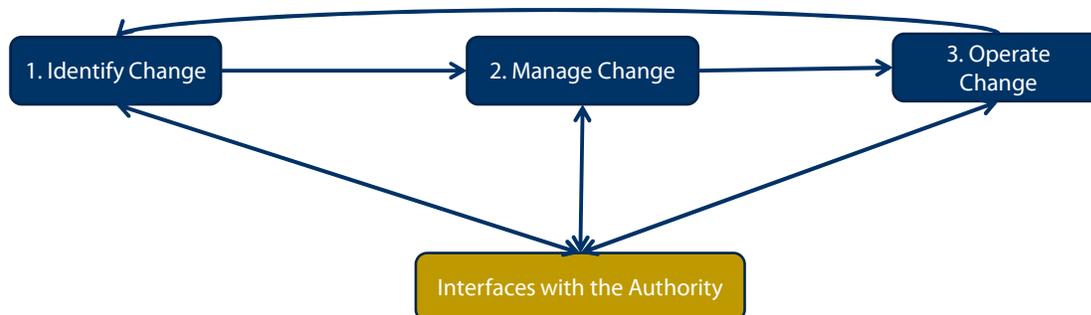# Change Management within the SMS

Change Management

Change Management Procedure

CMP - Simplified View

1. Identify changes

As part of the SMS - Safety assurance

- A process to identify changes within
  - the service provider's organization
  - the context in which it operates
  - the management system
  - the functional system
- That may affect the level of safety risk associated with its service.

2. Manage Changes

2.2 Develop the Change
Run all the activities of the project

2.3 Do Safety Assessment

2.1 Evaluate Impact

2.4 Build Safety Assurance

2.6 Implement Change

2.5 Coordinate with stakeholders (as needed)

Interfaces with the Authority

Deliver Safety Case

3. Operate changed functional system - Monitoring

- As part of the conclusions of the S.A. - Demonstration:
  - the changed functional system is supported by a monitoring system
    => demonstration that the service delivered will continue to meet the safety criteria.
- As part of the SMS
  - The continuous demonstration that the provided services achieve an acceptable level of safety risk.
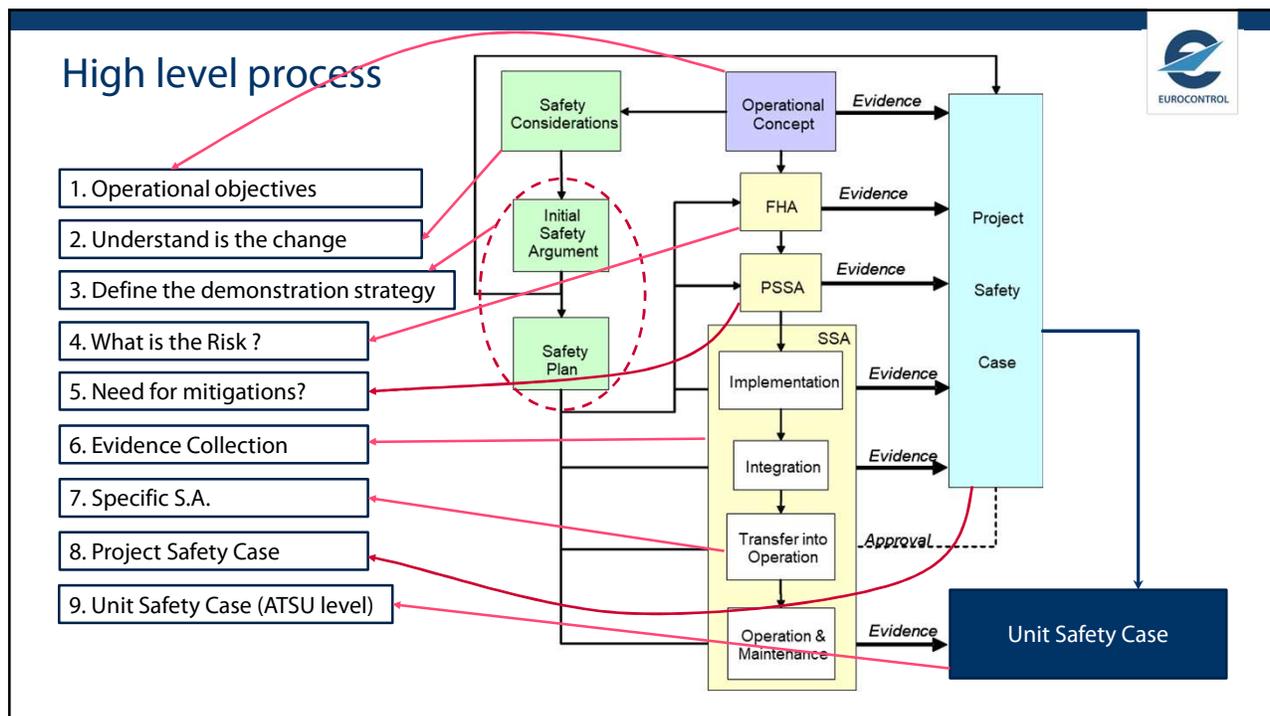

Steps of the Safety Assessment (S.A.)

Deliverables (1/2)

- **Operational Concept:**
  - Future use of the changed functional system
  - Users requirements
  - Expected ops benefits

- **Safety Considerations**
  - What is "the" change?
  - Scope, impact on the other parts of the F.S. and on the service provided
  - "How easy will it be to demonstrate that the safety criteria will be met?"

- **Safety Plan - Initial Safety Argument**
  - What activities as part of the project safety management plan?
  - How to argue, what evidence expected

- **FHA – Risk Assessment**
  - Hazard identification
  - Risk assessment (from hazard to effect)
  - Safety criteria and safety objectives

Deliverables (2/2)

- **PSSA – Risk Mitigation**
  - From the proposed architecture, causes to hazards
  - Safety requirements

- **SSA – Evidence collection**
  - Implementation
  - Transfer into operations
  - Operations and Monitoring

- **Safety Case**
  - For the change under consideration
  - Structured argument
  - Assurance collection

- **Unit Safety Case** (at ATS Unit level)
  - Daily operations (NOT in relation with a specific change to the functional system)
  - Assurance and monitoring
  - Regular updates

Safety Assessment Process

Safety Assessment Methodology

- Why do we have a Safety Assessment Methodology?
  - Proactive
  - Systematic
  - Formalised

SAM Toolkit

The EUROCONTROL Safety Assessment Methodology (SAM) is a framework, carry out safety assessment of changes to the functional systems of the Air N

- More info about the "Safety Assessment Methodology"
  https://skybrary.aero/sam-toolkit

What is SAM?

- A Methodology for the safety assessment of Air Navigation Services

- Developed under the Eurocontrol Safety Assessment Methodology (SAM) Task Force,

- Reflects the Task Force view of best practice in this domain, along with guidance on how to apply it

- Describes a generic process for Safety Assessment throughout a system lifecycle
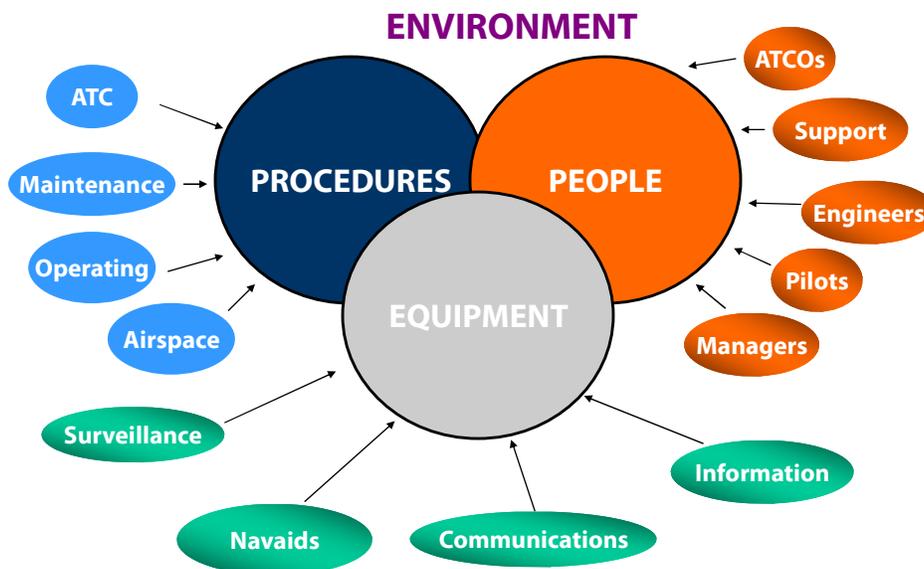
Lifecycle

- Support the demonstration that safety is being managed during the entire lifecycle:
  - Definition
  - Design
  - Implementation
  - Transfer to Operations
  - Operations and Maintenance
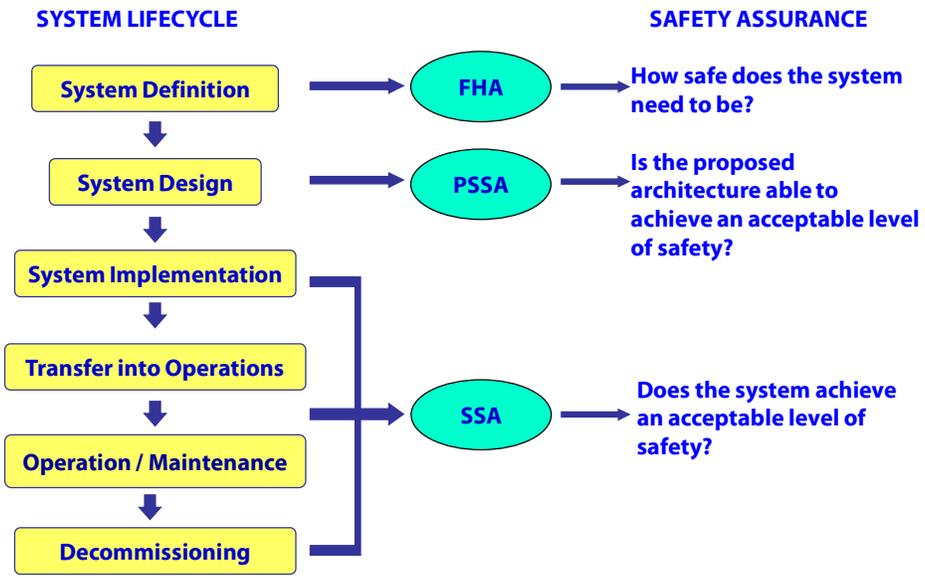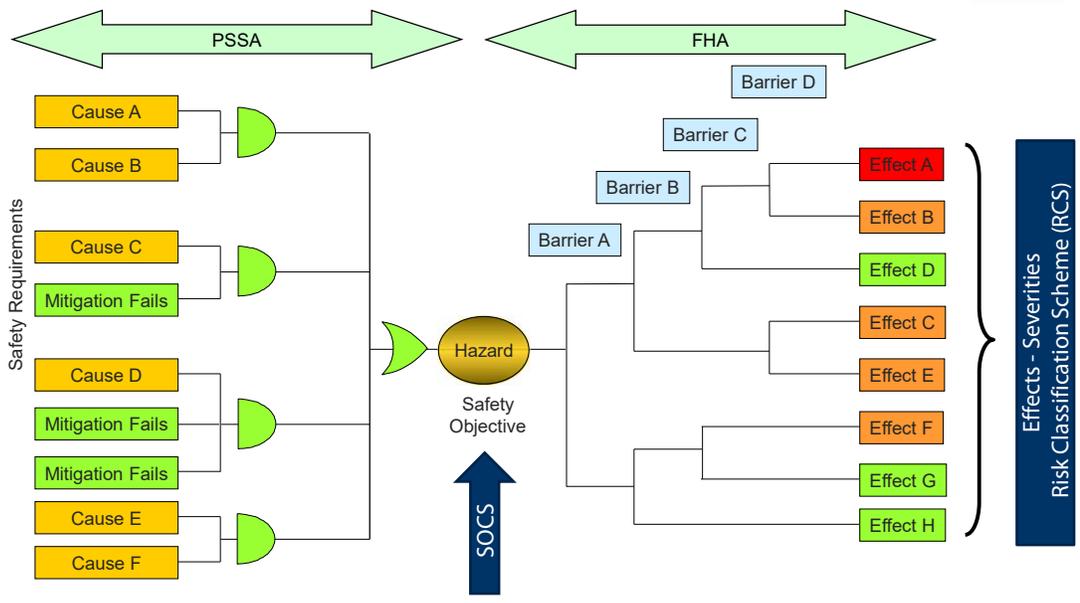 - Decommissioning

17

Total System Approach

18

SAM & System Lifecycle

SYSTEM LIFECYCLE

SAFETY ASSURANCE

- **System Definition** → **FHA** → How safe does the system need to be?
- **System Design** → **PSSA** → Is the proposed architecture able to achieve an acceptable level of safety?
- **System Implementation**
- **Transfer into Operations**
- **Operation / Maintenance** → **SSA** → Does the system achieve an acceptable level of safety?
- **Decommissioning**

Bow-tie

PSSA

FHA

Barrier D

Barrier C

Barrier B

Barrier A

Safety Requirements

Cause A
Cause B
Cause C
Mitigation Fails
Cause D
Mitigation Fails
Mitigation Fails
Cause E
Cause F

Hazard

Safety Objective

SOCS

Effect A
Effect B
Effect D
Effect C
Effect E
Effect F
Effect G
Effect H
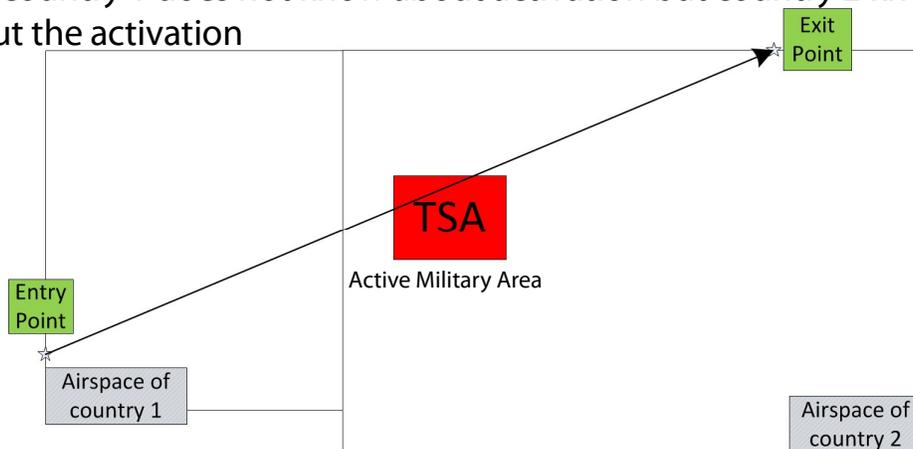
Effects - Severities
Risk Classification Scheme (RCS)

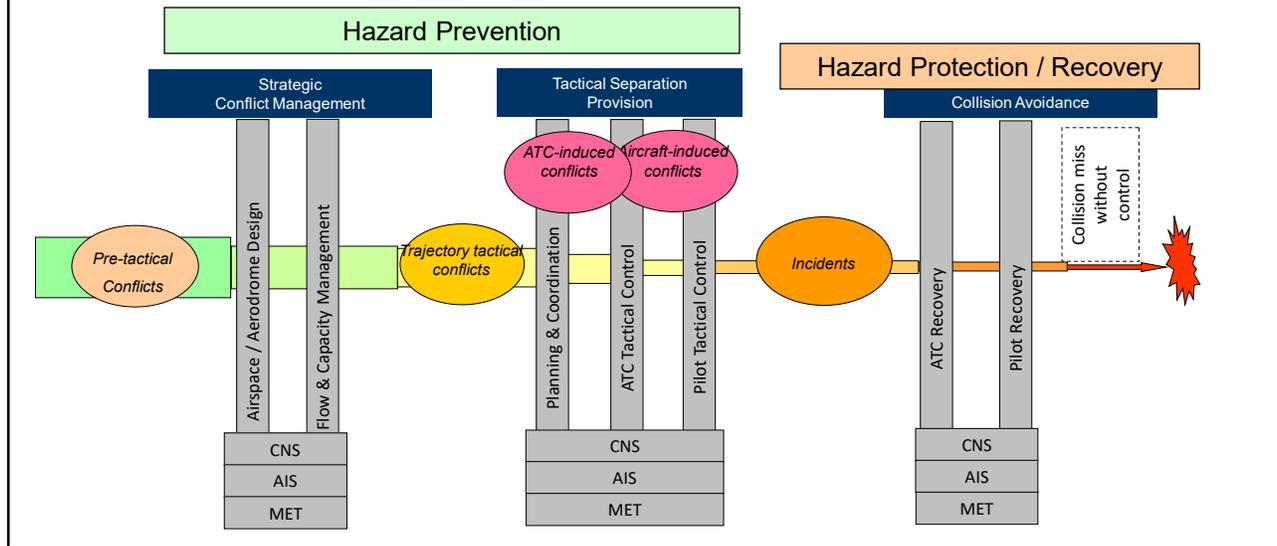## Safety Assessment Example

Safety Assessment - Example

- SFPL trajectory inconsistent with current airspace configuration
- E.g.: country 1 does not know about activation but country 2 knows about the activation

Hazard Effect Identification (Barrier Model)

Hazard Prevention

Hazard Protection / Recovery

Strategic Conflict Management

Tactical Separation Provision

Collision Avoidance

Pre-tactical Conflicts

Trajectory tactical conflicts

ATC-induced conflicts

Aircraft-induced conflicts

Incidents

Collision miss without control

Airspace / Aerodrome Design

Flow & Capacity Management

Planning & Coordination

ATC Tactical Control

Pilot Tactical Control

ATC Recovery

Pilot Recovery

| CNS |
| AIS |
| MET |

| CNS |
| AIS |
| MET |

| CNS |
| AIS |
| MET |

23

Risk Assessment Example - FMEA

Id No	Hazard ID	Failure Mode	Failure Effect	Effect on ATC/Operations	Mitigations & Assumptions	Seve-rity	Remark/ Comments
FPF-01	**Hz-01**: SFPL trajectory inconsistent with current airspace organisation	Incorrect route – filed free route outside FRA	The SFPL trajectory will not follow fixed ATS route network as semantic route validation is not performed at local level	Increased workload caused by route verification and re-routing	A1:IFPS will reject FPLs with incorrect routes PLC shall verify planned trajectory ATCO shall issue tactical re-routing clearance A2: IFPS ENV data/RAD restrictions are correct and up-to-date	4	In FRA it will be more difficult to identify inconsistency between SFPL trajectory and current airspace organisation

24

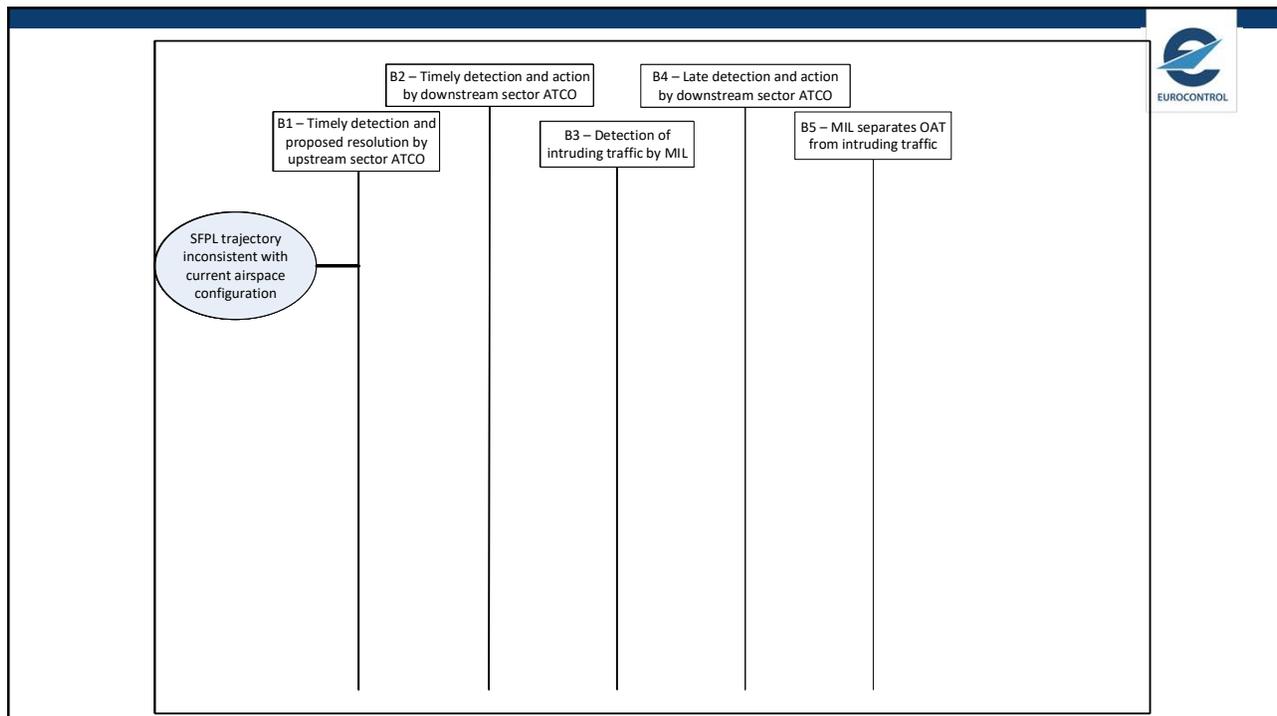## Risk Assessment Example - Building an Event-Tree

Who - Actors

- EXEC and PLN of ANSP-1
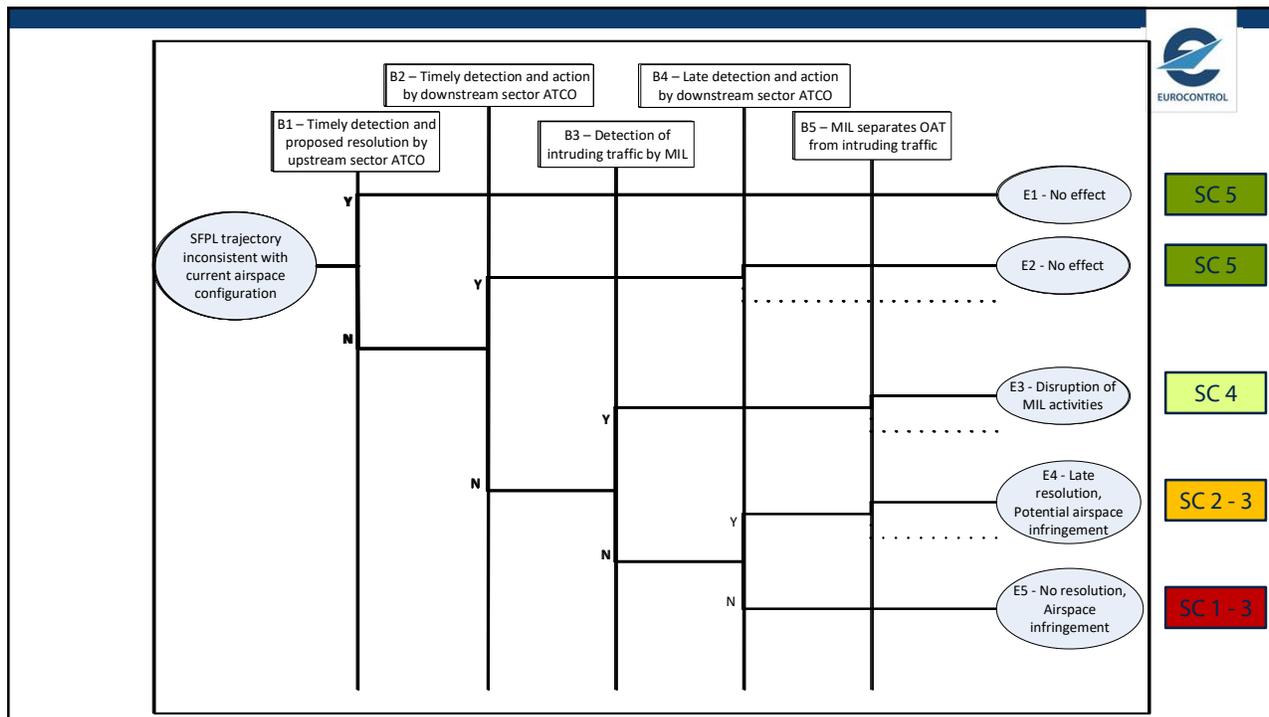- EXEC and PLN of ANSP-2
- Pilots
- Military authorities

What – Detection/Action

- Coordination between ATSU (voice or silent)
- Flight monitoring tools (MONA, MTCD,…)
- Active areas maps on CWP
- CIV-MIL coordination tool (LARA, …)

B1 – Timely detection and proposed resolution by upstream sector ATCO

B2 – Timely detection and action by downstream sector ATCO

B3 – Detection of intruding traffic by MIL

B4 – Late detection and action by downstream sector ATCO

B5 – MIL separates OAT from intruding traffic

SFPL trajectory inconsistent with current airspace configuration

B2 – Timely detection and action by downstream sector ATCO

B4 – Late detection and action by downstream sector ATCO

B1 – Timely detection and proposed resolution by upstream sector ATCO

B3 – Detection of intruding traffic by MIL

B5 – MIL separates OAT from intruding traffic

SFPL trajectory inconsistent with current airspace configuration

E1 - No effect — SC 5

E2 - No effect — SC 5

E3 - Disruption of MIL activities — SC 4

E4 - Late resolution, Potential airspace infringement — SC 2 - 3

E5 - No resolution, Airspace infringement — SC 1 - 3

EUROCONTROL

Risk Mitigation - Example

EUROCONTROL

- Hz-01 - SFPL trajectory inconsistent with current airspace organisation

Failure Modes	Causal factors	Potential Causal Mitigations
Incorrect route – filed free route outside FRA;	Operator input error;	Automate airspace management process by implementing interface between ASM tool and ATC system;
Incorrect route – filed route through active area;	Operator not familiar with airspace organisation;	
Incorrect route – filed incorrect transition points/segment;	Erroneous manual FPL correction;	Raise awareness of operator's flight planning departments (e.g. by means of AICs, dedicated meetings with main operators);
Credible incorrect route – no filed transition points/ segment;	FPL not updated according to latest airspace restriction(s);	
Incorrect route – constraints (RAD) not complied with;	AMC process failure;	Implement a procedure to coordinate with ATC sector controllers/OPS SUP actual activation of reserved areas;
FPL which trajectory penetrates active area is not suspended /rejected;	Failure of route verification against current airspace organisation;	
	IFPS ENV database not updated;	
Planed activation of restricted area not communicated or communicated late to NM;	Inconsistent FMS and ATC FPLs (filed/input by different units/staff);	Implement procedure for suspension of FRO, including notification of concerned adjacent civil and military units
Activation of restricted area / TSA not communicated to sector controllers;	MIL GAT flight unable to follow the published transition points/ procedures;	
Suspension of FRO not communicated to adjacent unit(s);	FPL filing tool database not consistent with published airspace organisation;	
Suspension of FRO communicated late to adjacent unit(s)	Danger (and other) areas not included in IFPS ENV database;	
	Restricted area not activated for display at CWP;	
	Restricted area activation message not sent/received/ processed by the ATC system;	
	Restricted area activation not communicated at sector handover;	
	Lack of, inadequate FRO suspension procedure or procedure not followed correctly	
	ATCOs/OPS SUP fails to notify FRO suspension to adjacent unit;	
	Communication failure	

Trustworthiness

- Expertise involved
- Attendance to sessions
- Assurance of "Correctness" of the content

Name	Organization	Background/Competence	Session 1	Session 2	Session 3
Names removed	ANSP1	ATCO	Yes	Yes	Yes
		ATCO	Yes	Yes	Yes
		FDO	Yes	Yes	Yes
		System Engineer	Yes	Yes	No
	ANSP2	ATCO	Yes	Yes	Yes
	ANSP 3	ATCO	Yes	Yes	yes
		FDO	Yes	Yes	No
			Yes	No	No
	ANSP4	OPS SUP	Yes	Yes	Yes
	Project Mgt	-	Yes	No	No
		ATCO	Yes	Yes	Yes
	Eurocontrol	Facilitator	Yes	Yes	Yes
	Eurocontrol	Facilitator	Yes	Yes	Yes

Any Questions

- **Jean-Michel De Rede**
  Senior Safety Expert
  NMD/NOM/SAF
  Tel: +32.2.729.33.17
  Cell: +32.492.13.52.40
  E-Mail: jean-michel.de-rede@eurocontrol.int
  www.eurocontrol.int/safety

- **EUROCONTROL**
  96 Rue de la Fusée
  1130 Brussels
  BELGIUM