EUROCONTROL FRA Safety Case Approach

AFI FRA Workshop

27 February – 2 March 2023

Alexander Krastev
Senior safety expert
EUROCONTROL

Network Manager

Supporting European Aviation

Contents

- Regulatory framework
- Methodological framework
- Safety Argument & GSN
- FRA Safety Case scope
- FRA Safety Argument
- FRA Safety Assessment & Report

Network Manager

Supporting European Aviation

Regulatory Framework: Regulation (EU) 2017/373

- ATS.OR.205 Safety assessment and assurance of changes to the functional system
- (a) For any change notified in accordance with point ATM/ANS.OR.A.045(a)(1), the air traffic services provider shall:
  - (1) ensure that a safety assessment is carried out covering the scope of the change, …
  - (2) provide assurance, with sufficient confidence, via a complete, documented and valid argument that the safety criteria identified via the application of point ATS.OR.210 are valid, will be satisfied and will remain satisfied.
- AMC1 ATS.OR.205(a)(2):
  - The air traffic services provider should ensure that the assurance required by ATS.OR.205(a)(2) is documented in a safety case.

What is a Safety Case?

- A means of structuring and documenting the demonstration of the safety of an ATM service or new / modified ATM/CNS system, i.e. the safety case is the documented assurance (argument and supporting evidence) of the achievement and maintenance of safety.
- Unit safety case - demonstrates acceptable level of safety of an on-going service (e.g. ATC) by an ATS unit
- Project safety case - demonstrates acceptable level of safety of a change to the functional system of an ATS unit (e.g. FRA safety case)

Methodological Framework

- AMC and GM to annexes II and III of Regulation 2017/373
- EUROCONTROL Safety Case Development Manual, version 2.2
- EUROCONTROL Safety Assessment Methodology, version 2.1

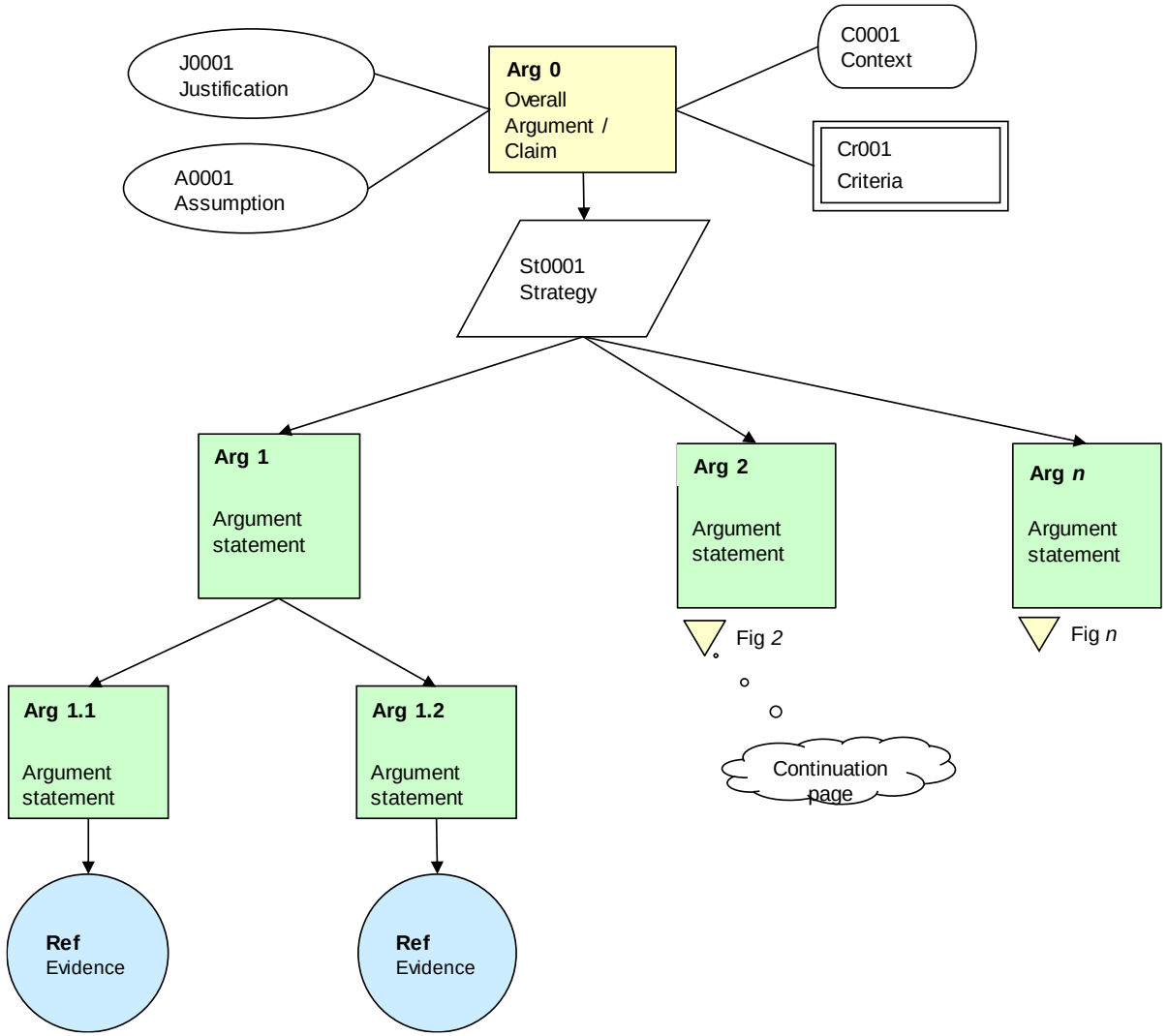
Safety Argument

- The safety argument is a set of statements used to assert that the service or system is safe to use after the change
- It starts with a top-level statement (claim) about what the safety case is aimed to demonstrate in relation to the safety of the service or system
- The claim must be supported by safety criteria that define what is safe in the context of the claim
- The claim is decomposed into lower-level arguments to provide the necessary links between the claim and the evidence needed to show that the claim is valid
- Arguments should be clear, comprehensive, dependable and defensive

Goal Structured Notation (GSN)

- Provides a graphical means of setting out hierarchical safety arguments, with textural annotations and references to supporting evidence
- Brings rigour into the process of developing safety arguments
- Enables braking down the argument in manageable chunks, but still keeping the overall picture
- Supports establishing of a Safety plan
- Enables scoping of safety related work
- Identifies the evidence needed to produce the safety case

GSN Symbology



FRA Safety Case scope - Introduction

- Introduction
  - Short description of the FRA implementation project
- Document purpose & scope
  - Purpose: to provide assurance to the ATS provider and the CAA
  - Scope: all safety assessment and safety related project implementation activities that support the safety claim

FRA Safety Case scope - ATS domains covered (1)

- Airspace design and management, including definition of FRA, transitions points and routes, ATC sectors, etc.
- ATM procedures, including flight plan filing and submission, FRA transition procedures, etc.
- ATM personnel competence
- Flight data processing and distribution, in particular trajectory calculation and inter-sector and inter-centre coordination and transfer
- Surveillance, in particular FRA surveillance coverage

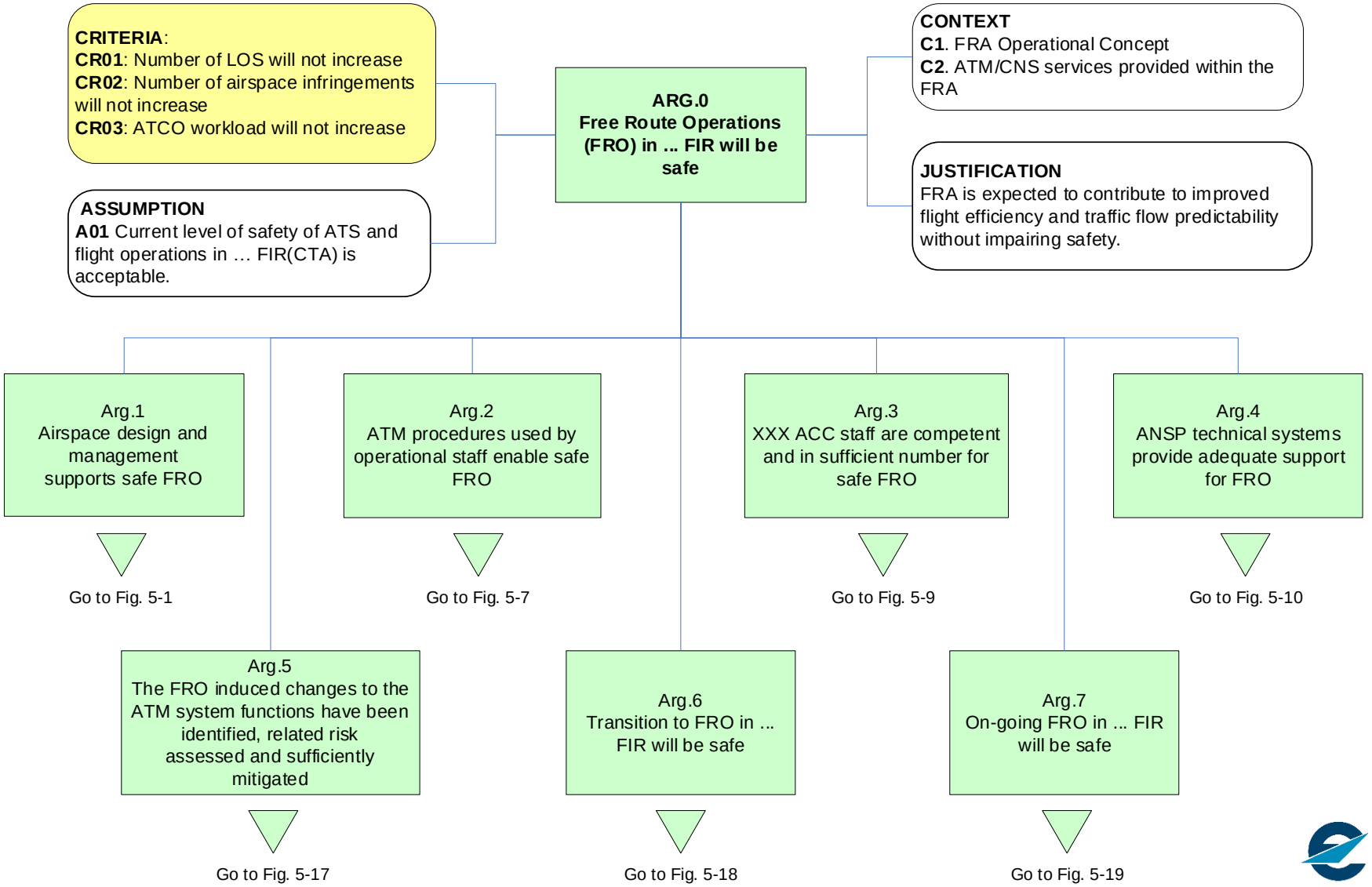
FRA Safety Case scope - ATS domains covered (2)

- CWP HMI, in particular flight route presentation, coordination and transfer;
- Conflict detection and resolution by ATC
- ATC tools, support for conflict detection
- Safety nets
- Air ground communication; in particular FRA radio coverage
- Ground-ground communication and coordination

FRA Safety Case scope - FRO description (2)

- The short description of the free route operations (FRO) should include following sections:
  - The FRA Operational concept (ref. to ConOps document)
  - The FRA area of applicability (airspace and time periods)
  - Flight planning rules and procedures
  - FRA airspace management (ASM procedures, e.g. airspace reservations)
  - ATS and procedures in the FRA airspace
  - ACC environment of operations (incl. system support)

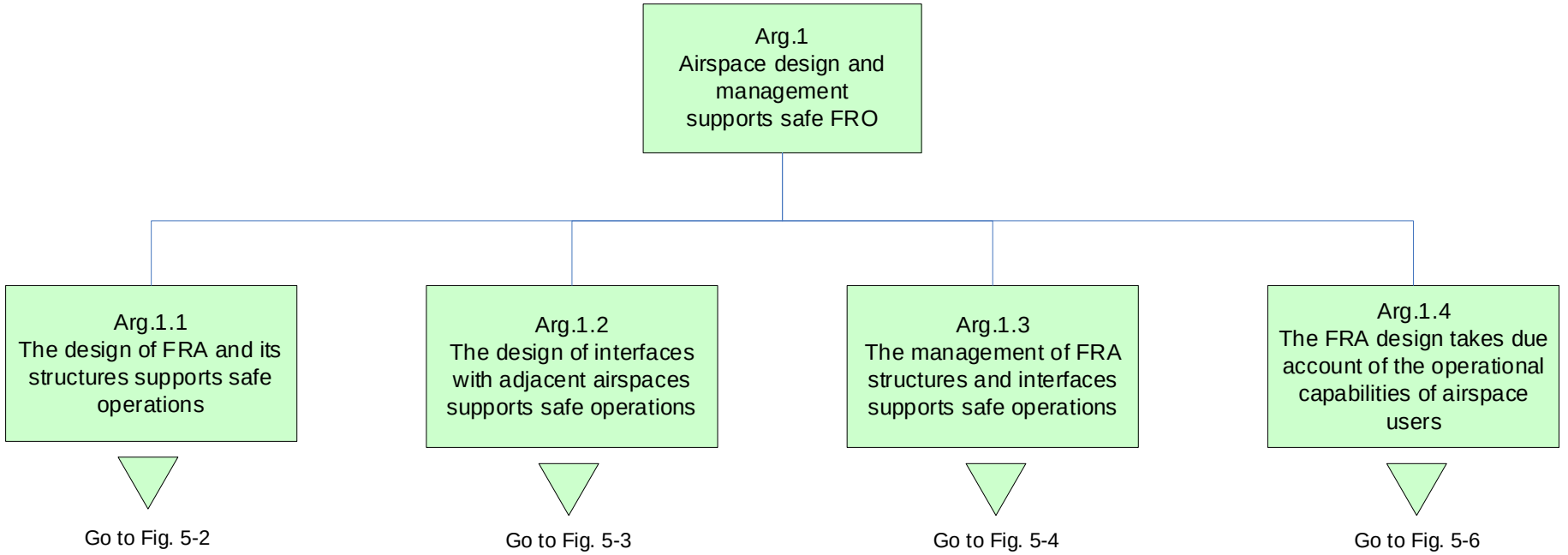
FRA Safety Case - Overall Safety Claim



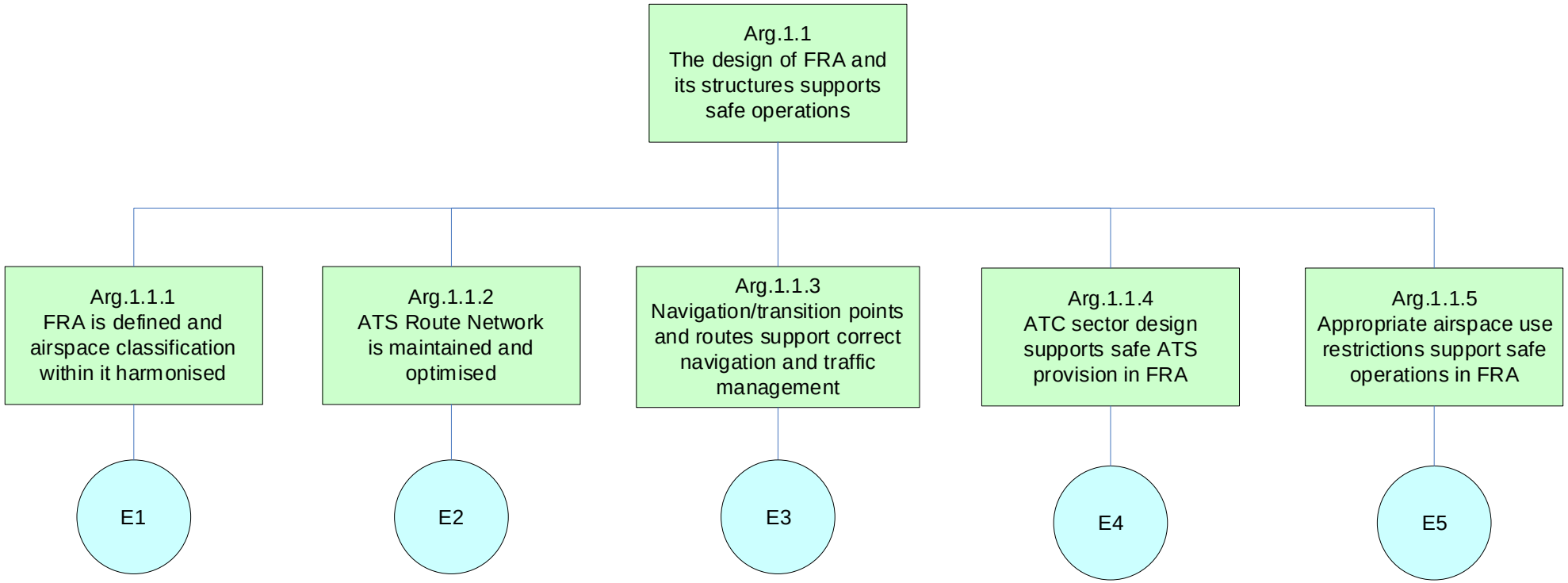
Network Manager

Supporting European Aviation

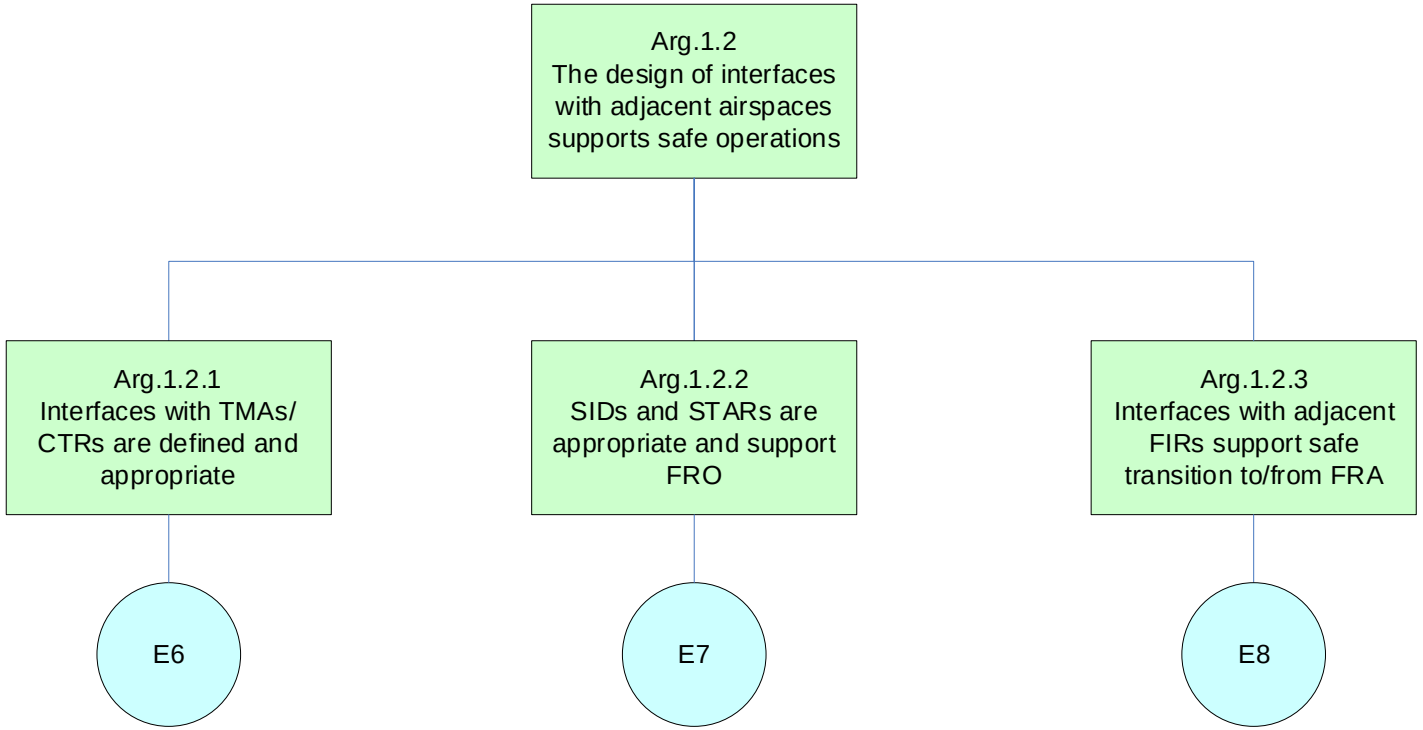
FRA Safety Case - ASD&M Safety Argument



FRA Safety Case - FRA Design Safety Argument



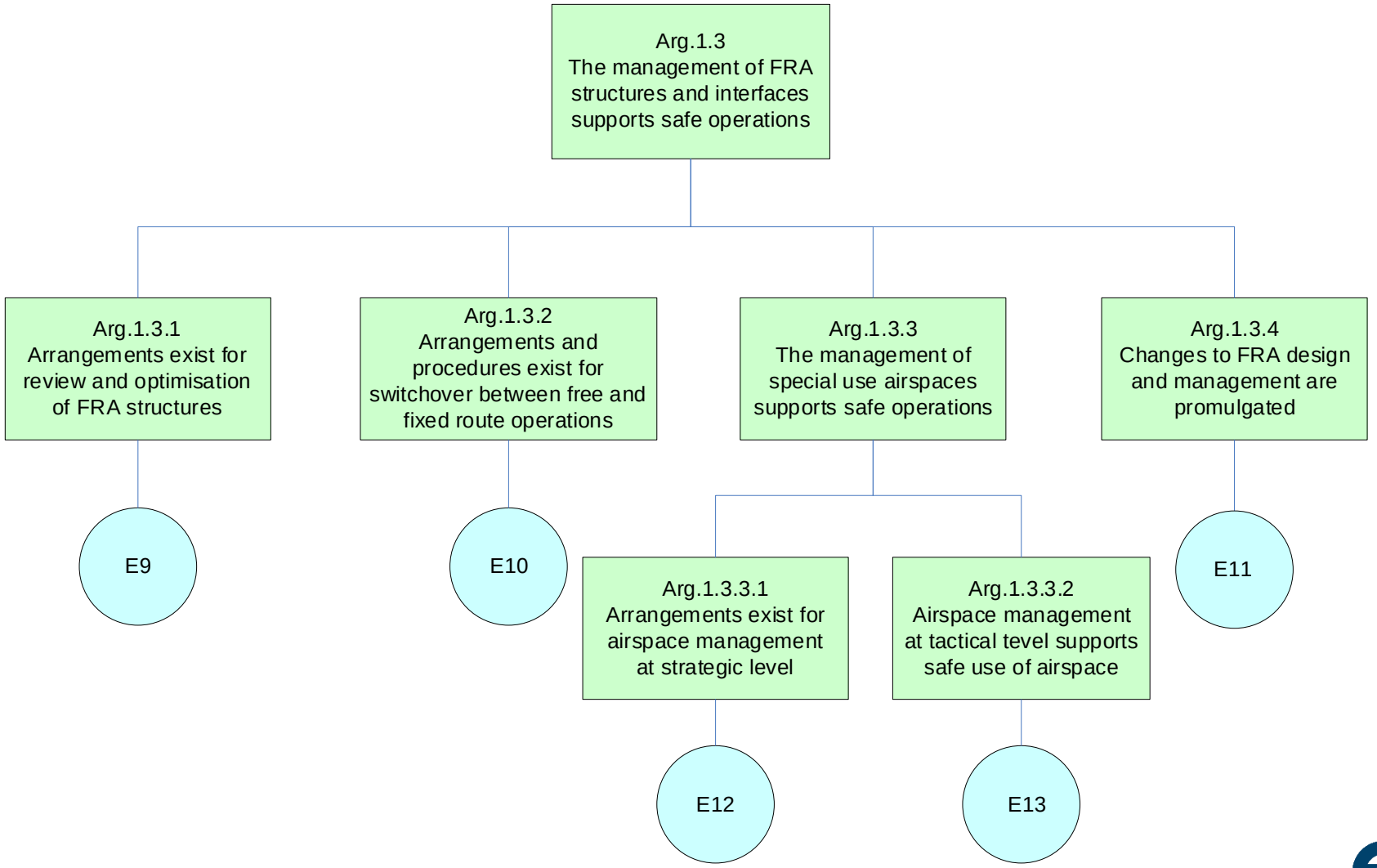
FRA Safety Case - Interface Safety Argument



Network Manager

Supporting European Aviation

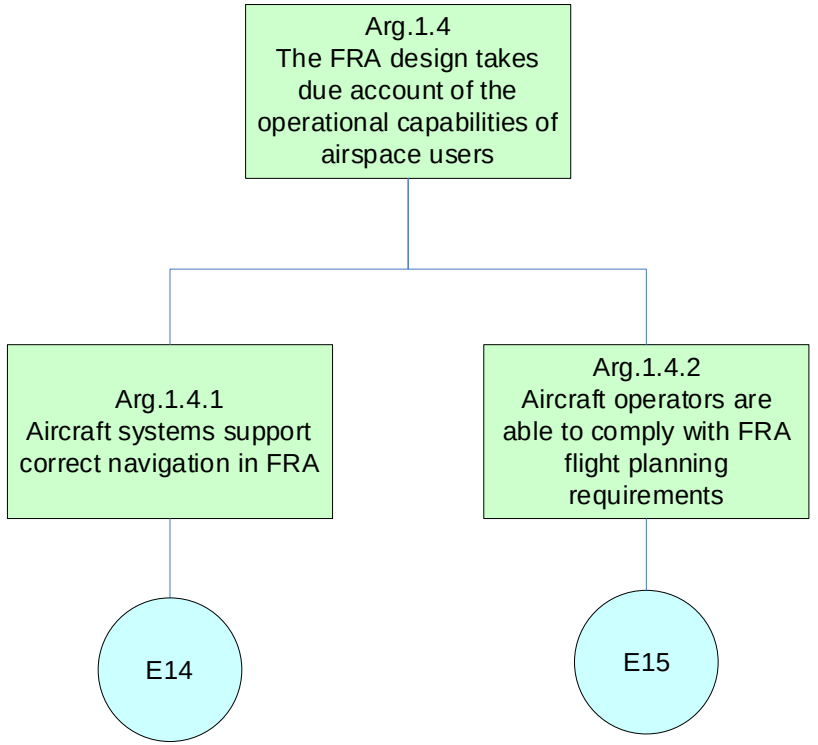
FRA Safety Case - FRA Management Safety Argument



Network Manager

Supporting European Aviation

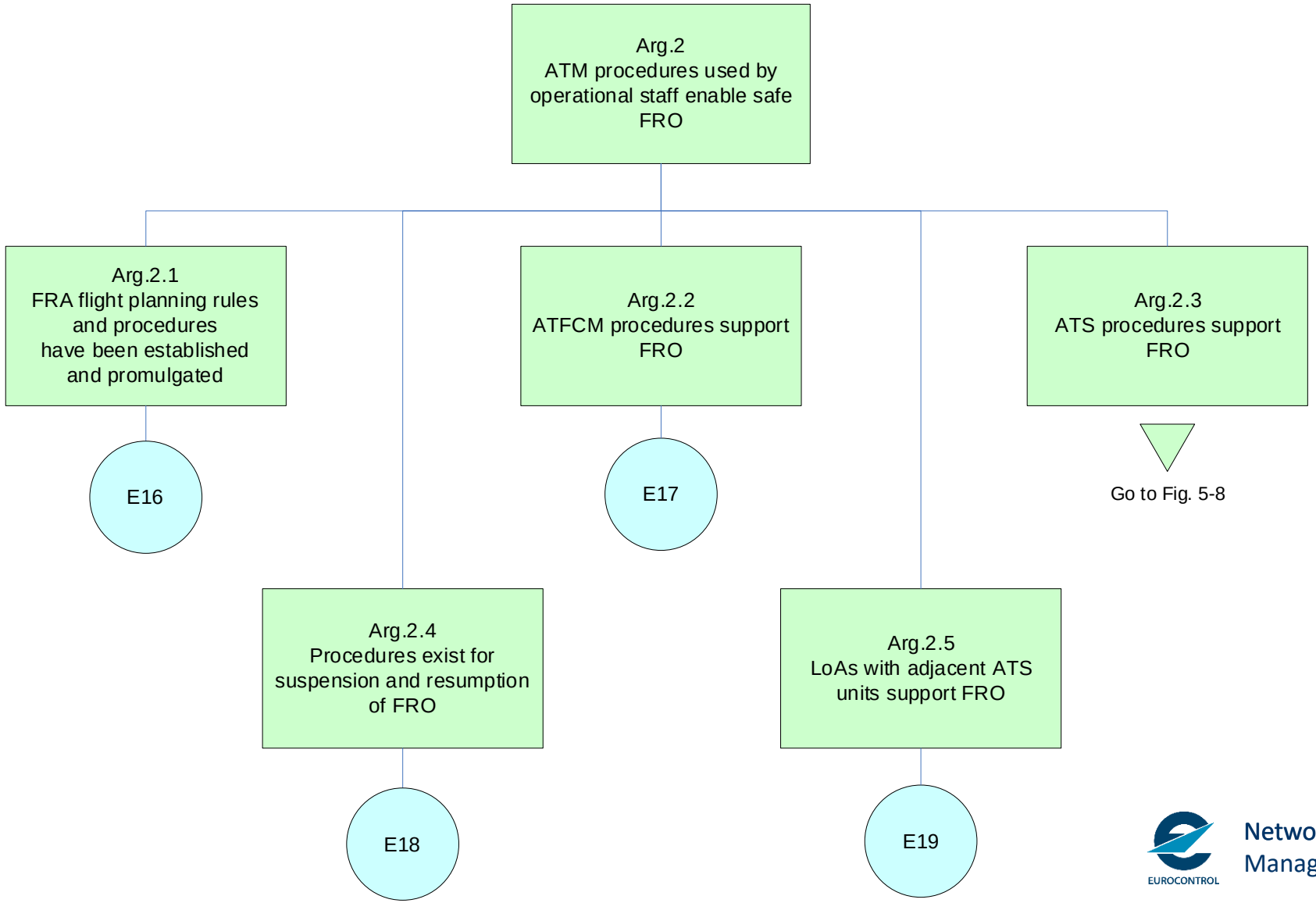
FRA Safety Case - User Capability Safety Argument



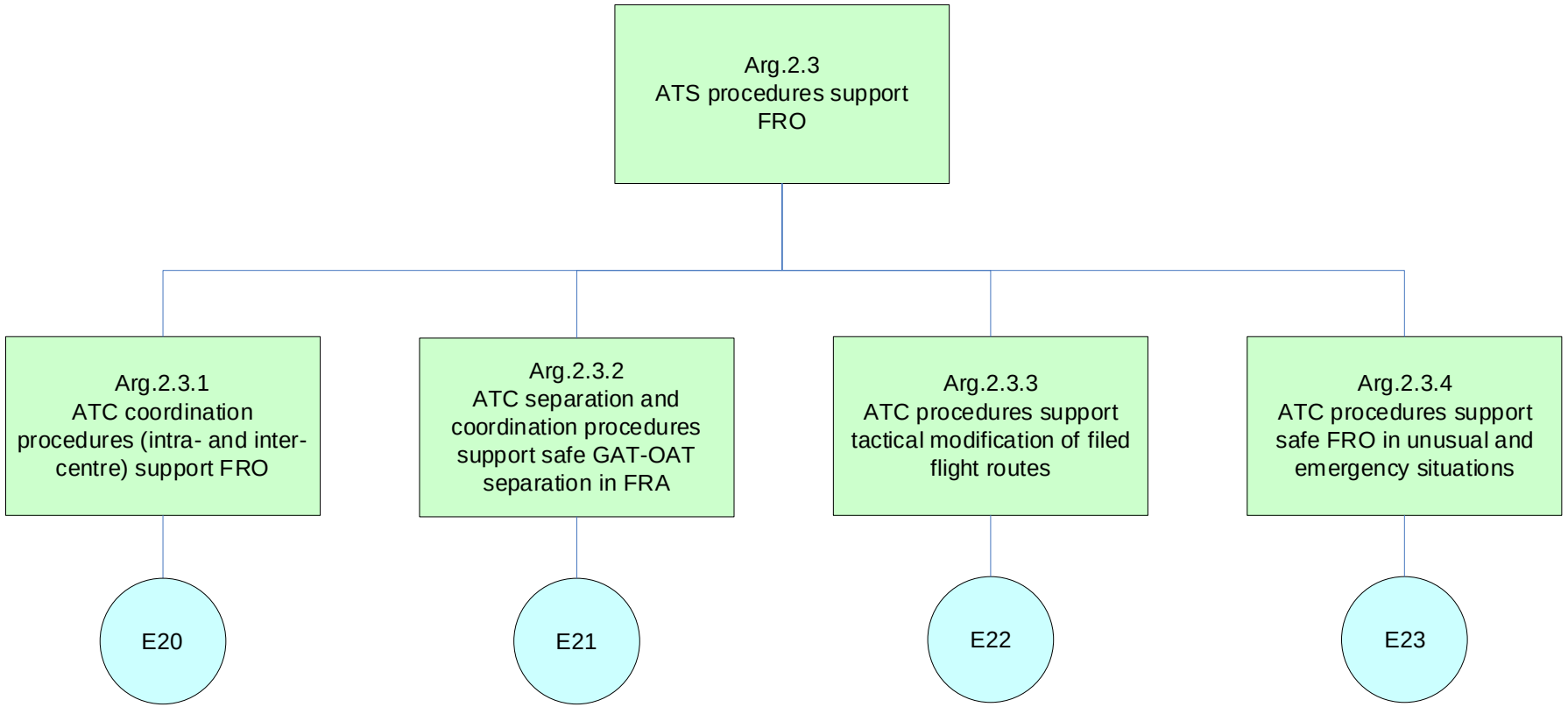
Network Manager

Supporting European Aviation

FRA Safety Case - ATM Procedures Safety Argument



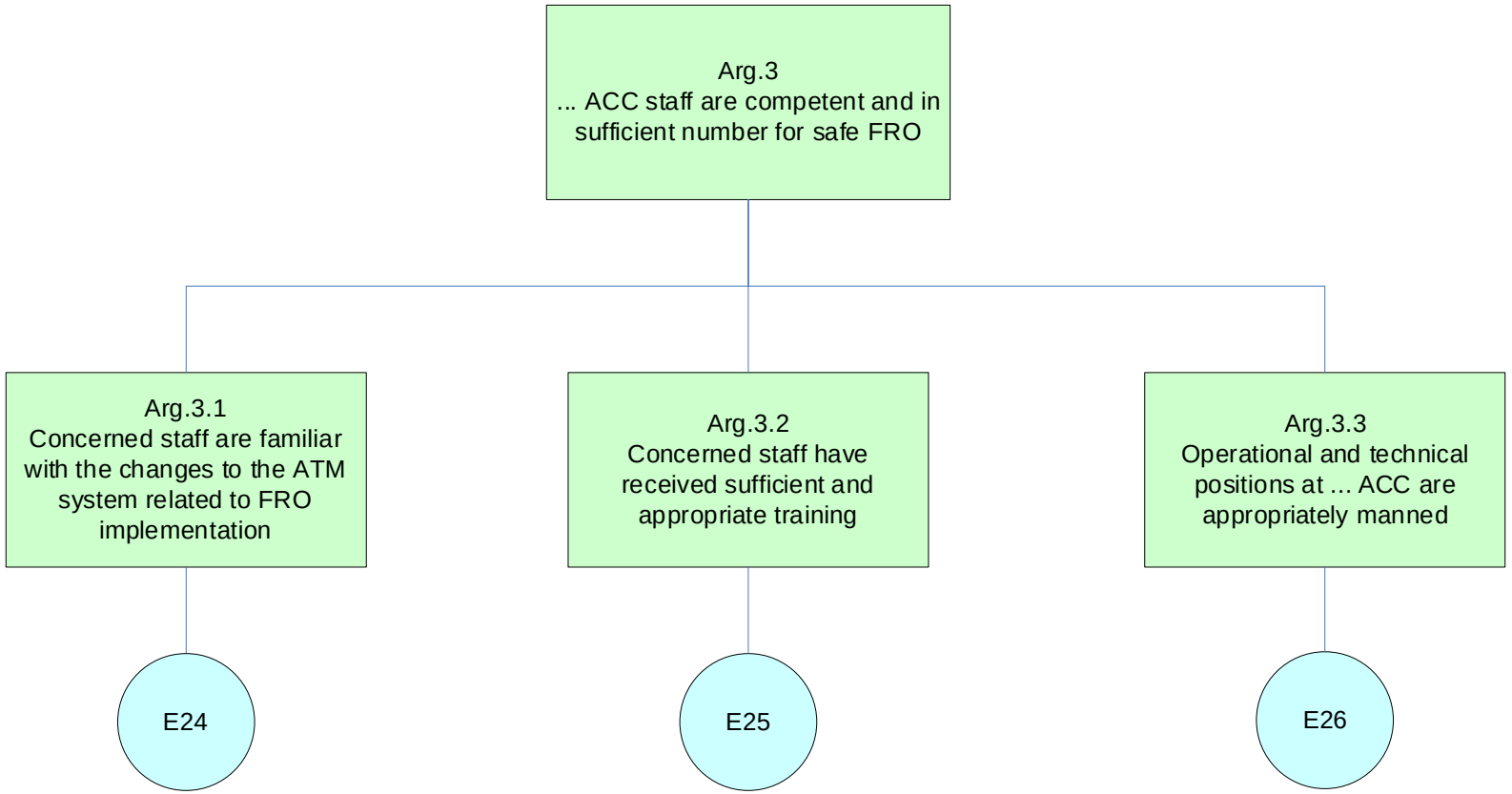
FRA Safety Case - ATS Procedures Safety Argument



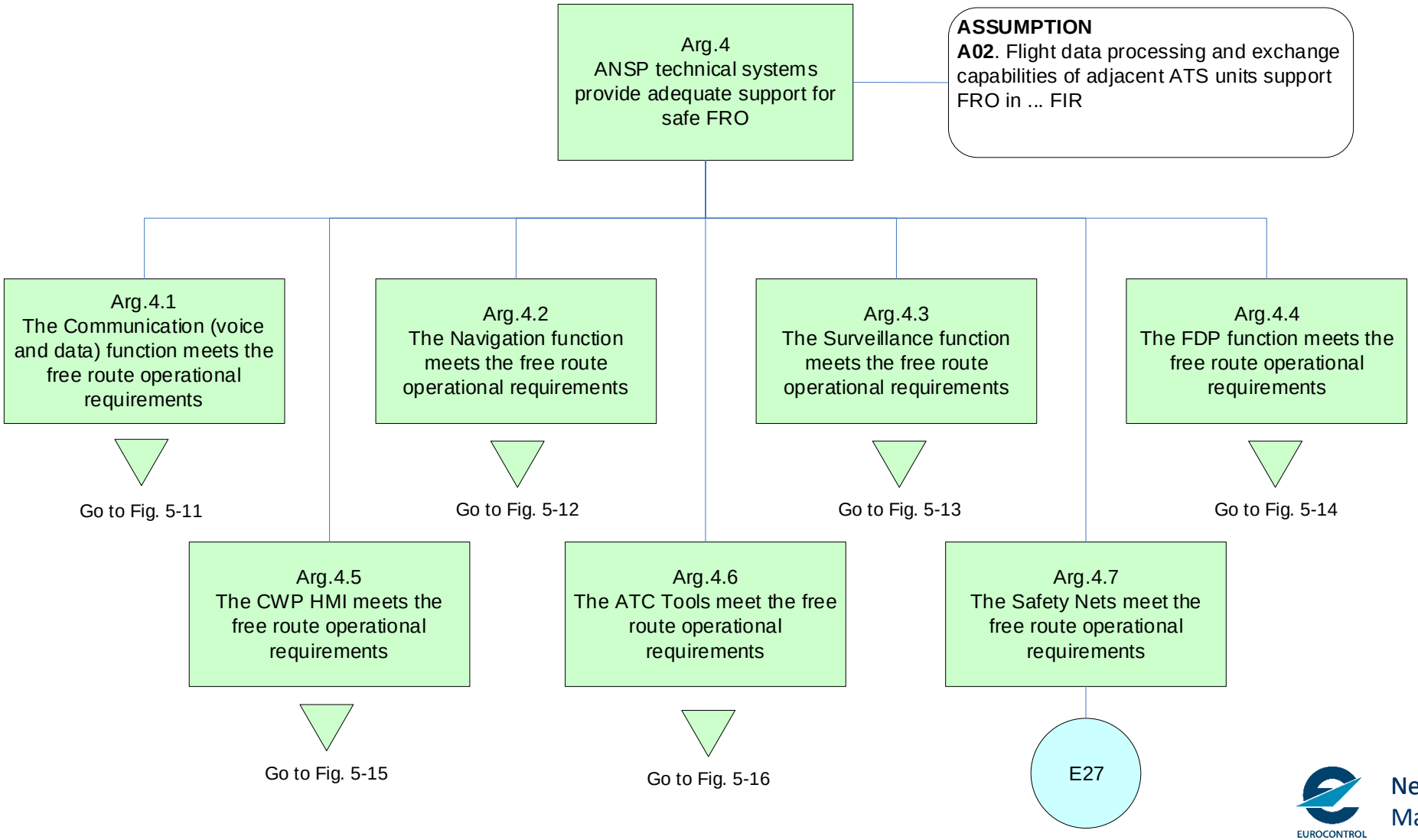
Network Manager

Supporting European Aviation

FRA Safety Case - Staff Safety Argument



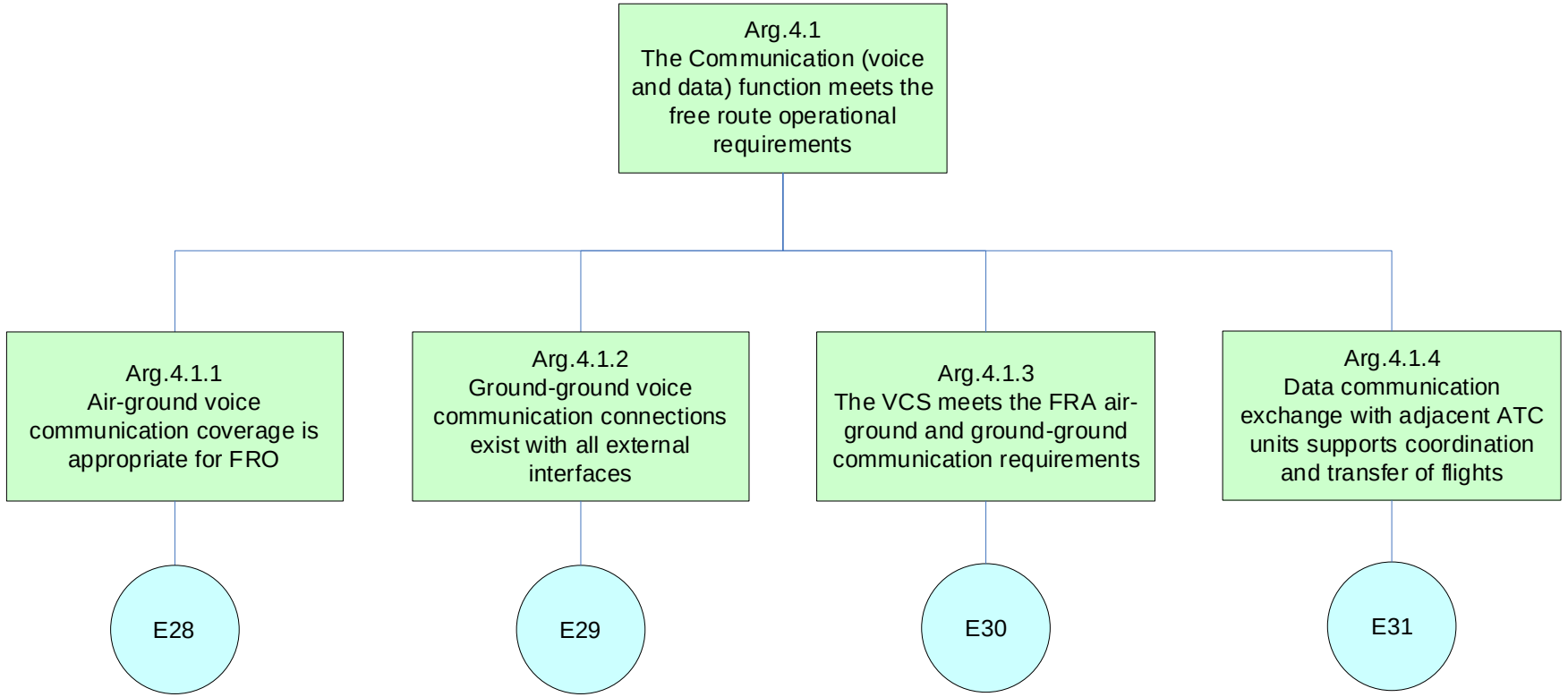
FRA Safety Case - Equipment Safety Argument



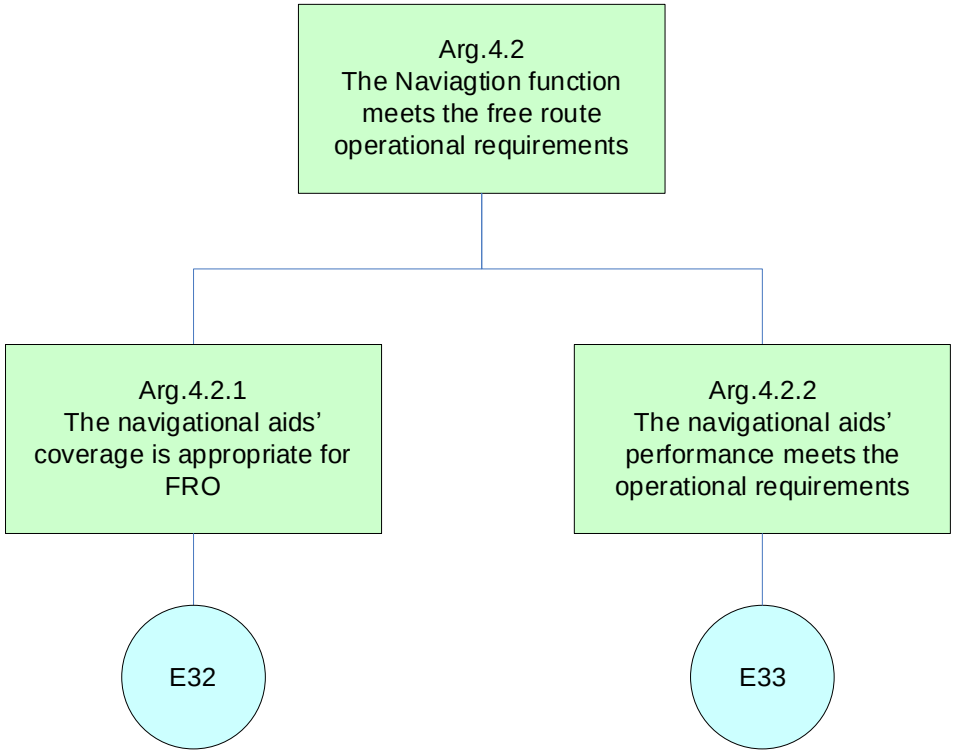
Network Manager

Supporting European Aviation

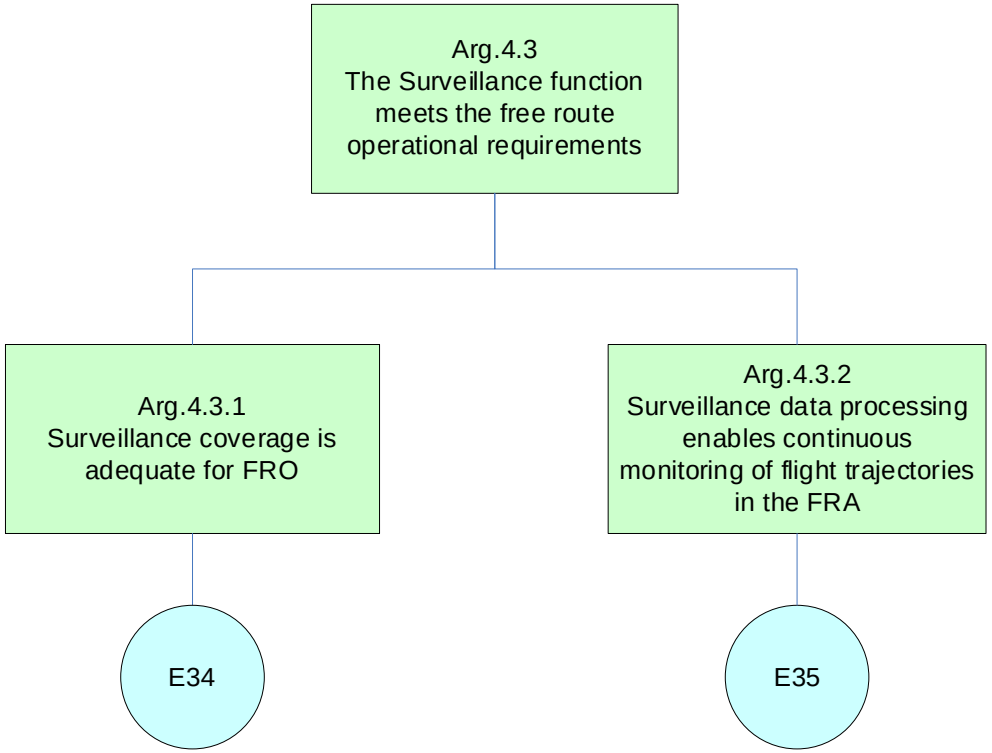
FRA Safety Case - Comm System Safety Argument



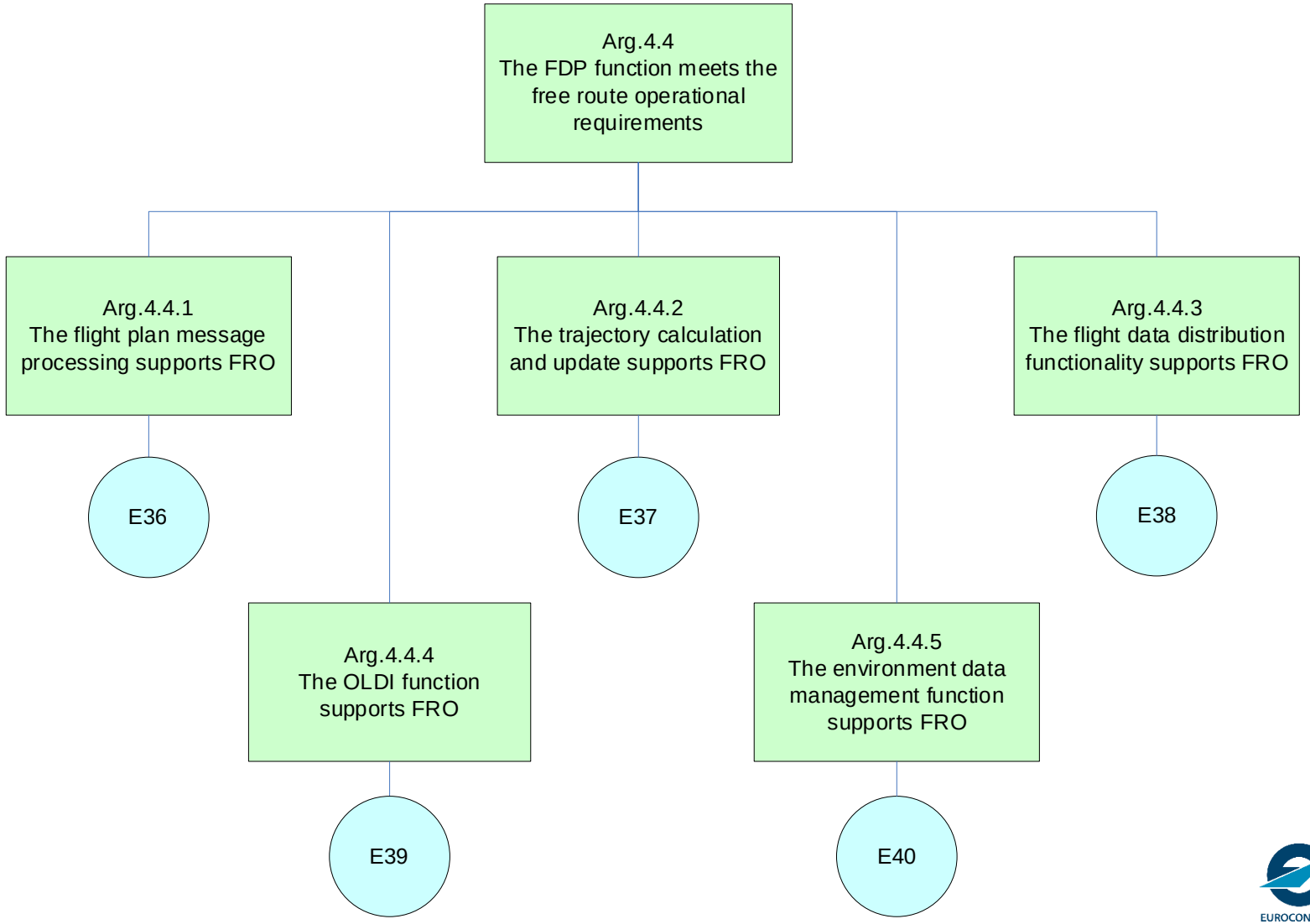
FRA Safety Case - NAV System Safety Argument



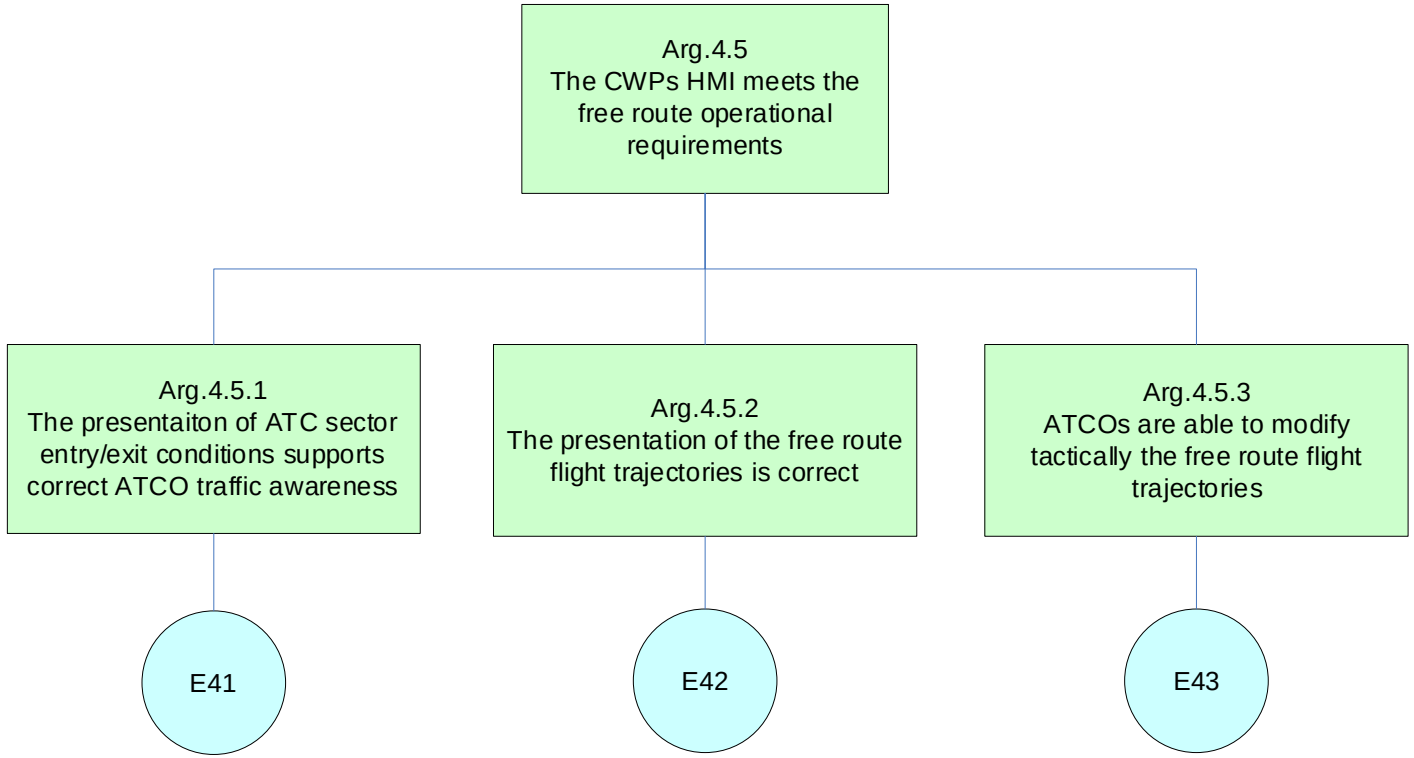
FRA Safety Case - SUR System Safety Argument



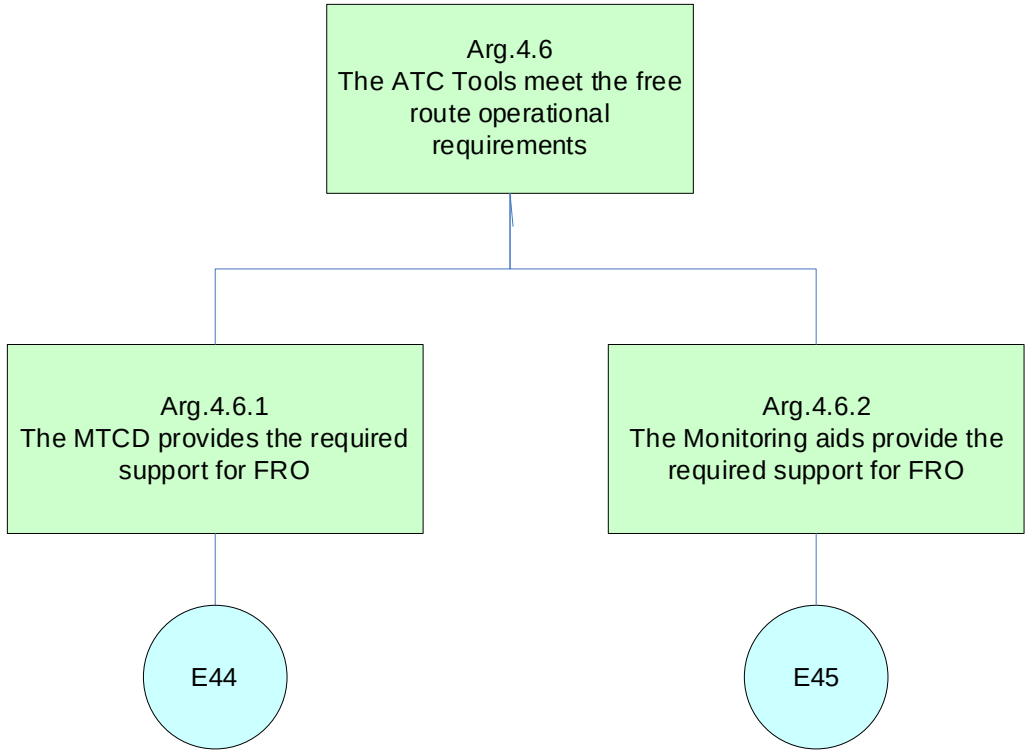
FRA Safety Case - FDP System Safety Argument



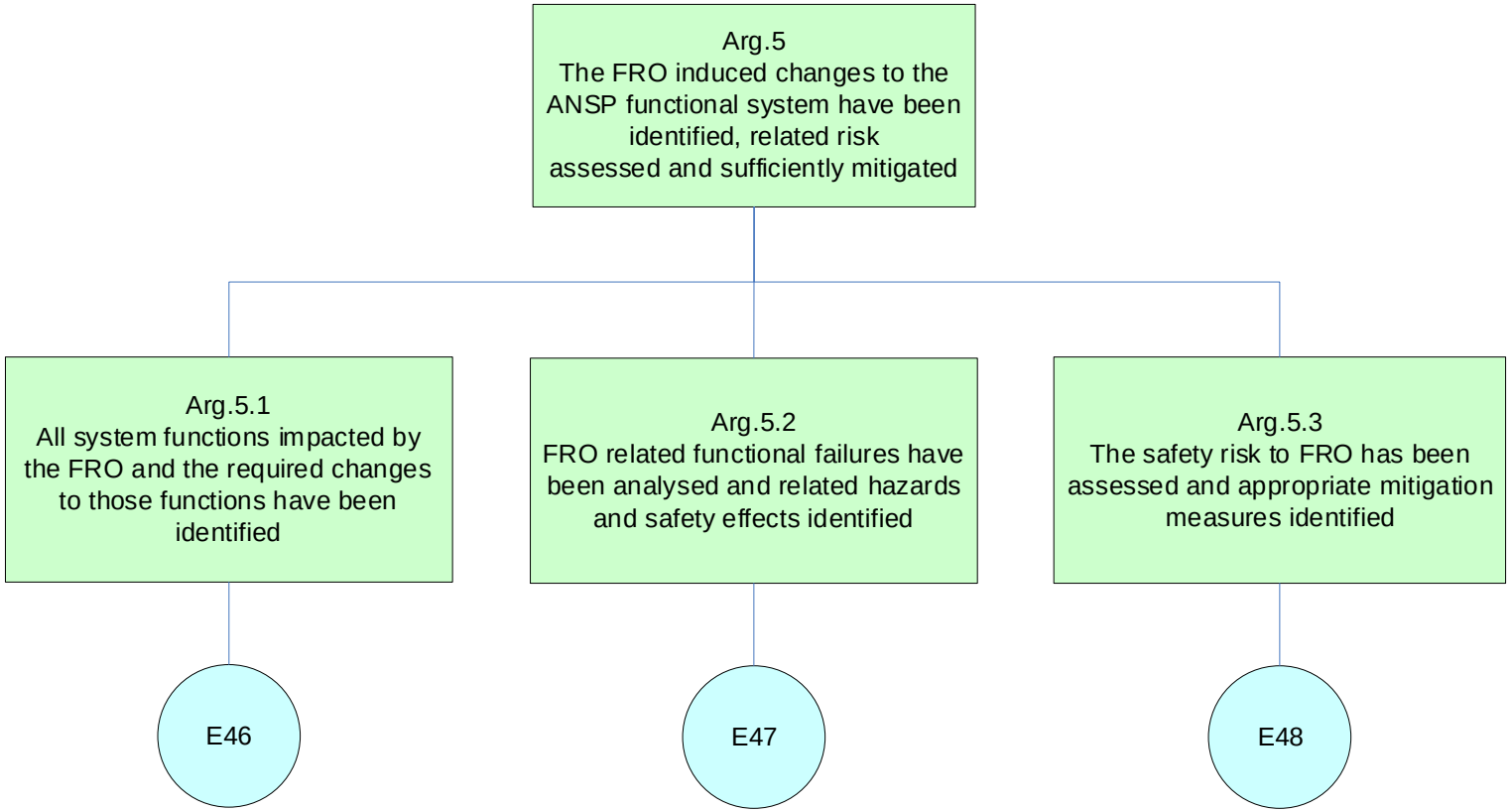
FRA Safety Case - HMI Safety Argument



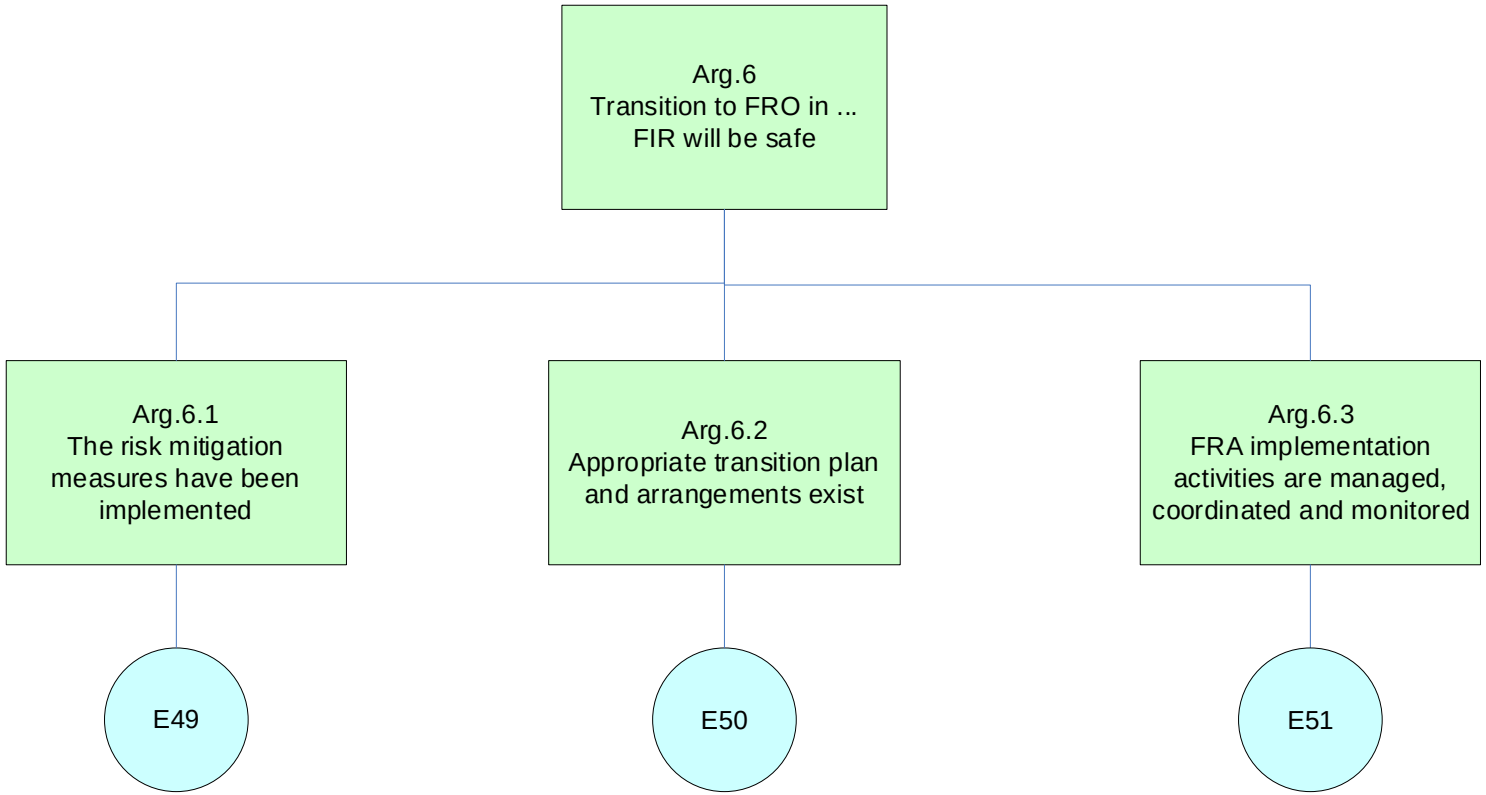
FRA Safety Case - ATC Tools Safety Argument



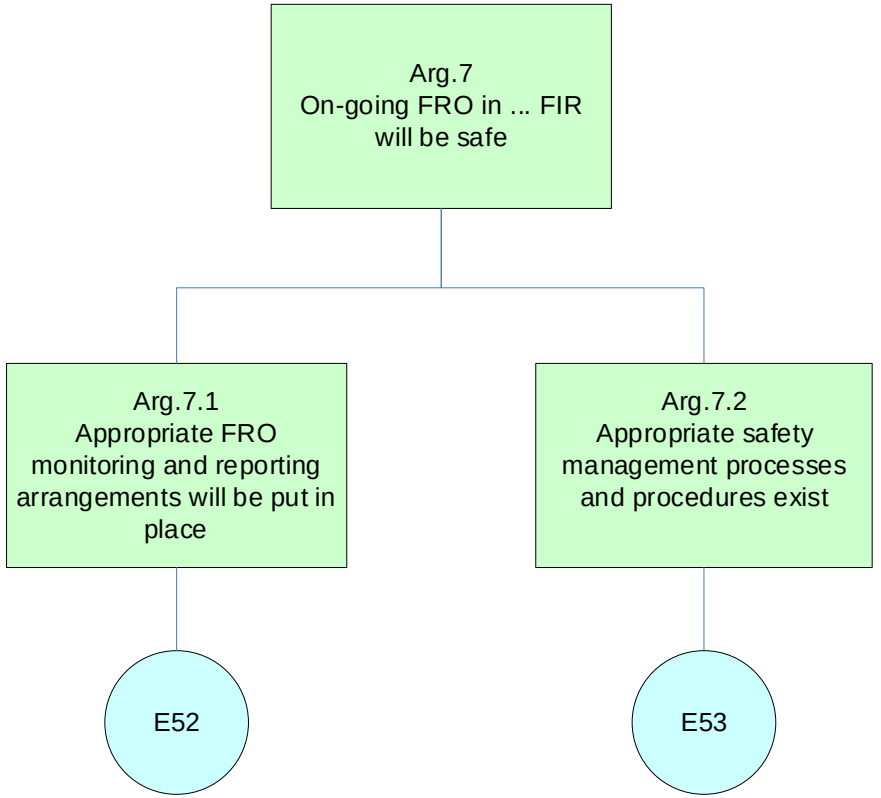
FRA Safety Case - Risk Assessment Safety Argument



FRA Safety Case - Transition Safety Argument



FRA Safety Case - Ongoing Ops Safety Argument



FRA Safety Case - Assumptions

- Document and justify all assumptions used in the safety argument, e.g.
  - Current level of safety of ATS and flight operations in … FIR / CTA is acceptable
  - FDP capabilities of the adjacent ATS units support FRO in … FIR

FRA Safety Case - Conclusions

- Argue the Safety criteria will be met (FRO in … FIR will be safe) with reference to the evidence provided in the document that:
  - ANSP ATM/CNS system meets the functional and performance requirements for FRO
  - The hazards related to the free route operations and their effects have been identified
  - Risk has been assessed and complete set of mitigation measures (SRs) established
  - The SRs will be implemented / have been implemented
  - Assumptions have been validated
- Make any recommendations, if appropriate

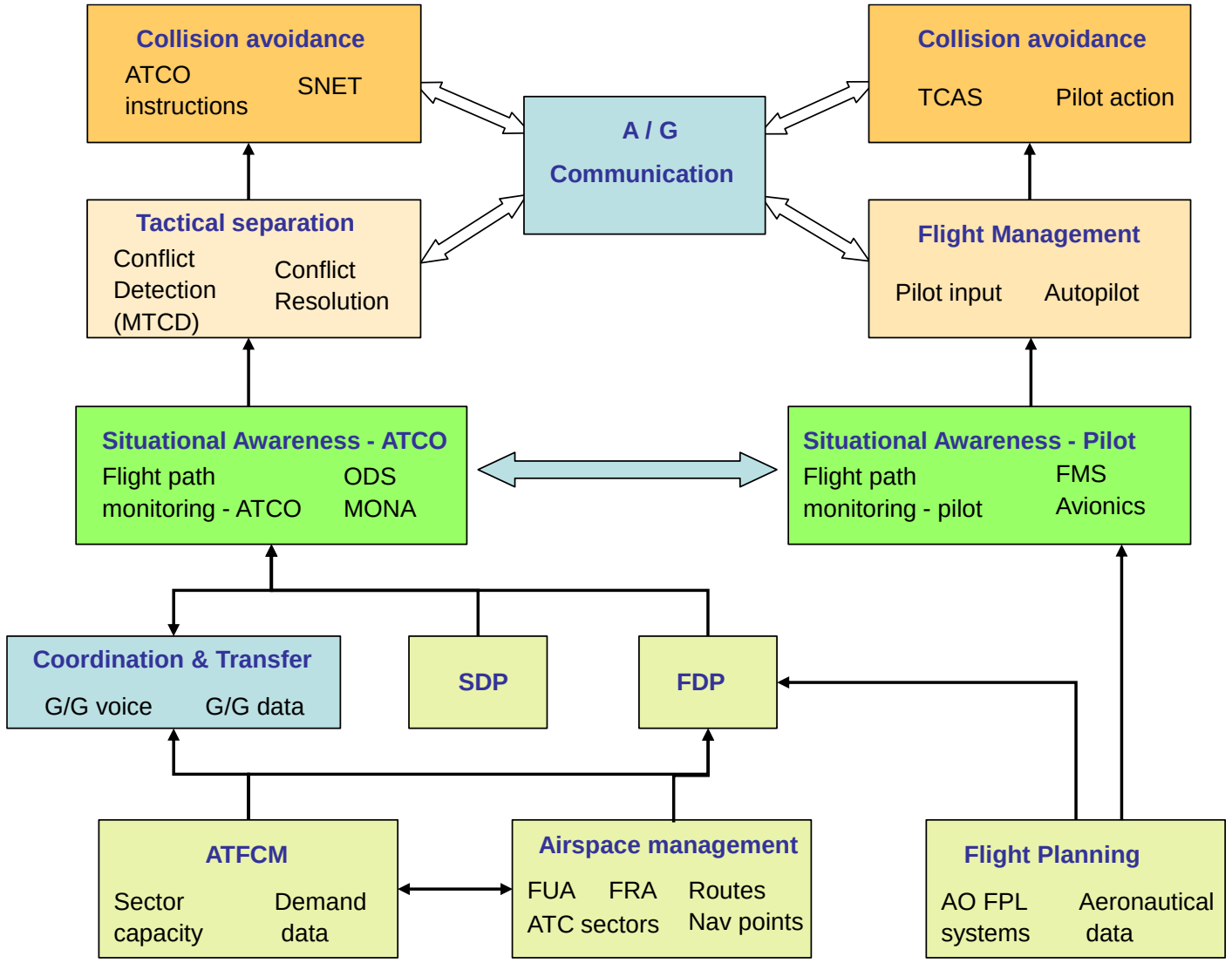
FRA Safety Assessment Report - Purpose

- Supports Arg. 5 “The FRO induced changes to the ATM system functions have been identified, related risk assessed and sufficiently mitigated”
- Documents the results of the FRA safety assessment:
  - Functional Hazard Assessment (FHA), i.e. hazard identification & risk assessment
  - Preliminary Safety Assessment (PSSA), i.e. risk mitigation

FRA Safety Assessment - Scope

- Airspace management, airspace (non)availability notification
- ATM procedures, including flight plan filing and submission, in particular planned route
- Staff competence
- Flight data processing and distribution, in particular trajectory calculation and inter-sector and inter-centre coordination and transfer
- Surveillance
- CWP HMI
- ATC tools
- Safety nets
- Air ground communication
- Ground-ground communication and coordination
- Conflict detection and resolution
- Flight management (navigation) by flight crew

FRA Safety Assessment – Functional model



FRA Safety Assessment Report – Scope

- Introduction
  - Short description of the FRA implementation project
- Document purpose & scope
- Operational environment and system description
  - System boundaries (airspace, procedures, equipment and staff concerned)
  - Eligible flights
  - Operational environment
  - External interfaces
  - FRA functional system

FRA Safety Assessment Report – Scope (continued)

- Safety criteria
  - Proxies, or RCS/SOCS or collision model
  - Monitoring criteria
- Risk assessment
  - Hazard identification (using FMEA)
    - Hazards defined at the ATS interface to flight operations
    - WCE of failure modes and hazards considered only
    - Identification of differences in failure effects (fixed vs free route)
  - Risk assessment (effect severity & likelihood)
  - SOs determination

FMEA Table - Example

Id No	Hazard ID	Failure Mode	Failure Effect	Effect on ATC/Operations	Mitigations & Assumptions	Severity	Remark/ Comments	Probability
Flight Plan Filing								
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	Very unlikely

FRA Safety Assessment Report – Scope (continued)

- Risk mitigation
  - Hazard causal analysis (based on identified failure modes)
    - Identification of system faults, malfunctions and other contributory factors
  - Identification of Safety Requirements to ensure hazard SOs are met
- Assumptions (used in the risk assessment and mitigation)
- Conclusions
  - Argue that safety risk associated to the change has been identified and sufficiently mitigated with reference to scope and trustworthiness of the risk assessment and mitigation
- Annexes
  - Detailed FMEA results
  - Traceability tables

SR Traceability Table - Example

Hazard description and failure modes	Difference Fixed vs Free route	Causal mitigation	Consequential mitigation	Safety requirements
Hz-16: Aircraft does not follow planned or assigned trajectory FLM-01, FLM-02, FLM-03, FLM-04, FLM-05, FLM-07, FLM-08, GGC-14, GGC-15, GGC-18, AGC-07	It will be more difficult in free route environment to verify the planned route/ identify the incorrect route information; hence importance of SFPL update increases GAT flight deviation towards active area without prior coordination is more likely to happen in free route environment In free route environment it will be more difficult to identify the incorrect route information	Implement procedure to ensure that first ACC sector verifies the flight route upon first contact; Strict adherence to applicable RTF; Ensure compliance with Annex 11 principles for establishment and identification of significant points; Implement procedure for manual trajectory update, including input of constraints; Strict adherence to AGC procedures (in particular read-back /hear-back)	MONA alerts reminders for non-compliance with flight entry/exit conditions; Graphical flight leg will help identify deviation from SFPL trajectory; Use of exit point in track label (to a limited degree); ATCO shall verify actually flown route with pilot; Verbal coordination with concerned sector(s) / unit; Forced SFPL distribution to concerned sector(s); Manual system /SFPL update; Change of flight clearance by ATCO – tactical flight rerouting; Use of CPDLC;	Ensure that ATCOs are aware of and use only published navigation points in ATC clearances; Ensure that procedure(s) is published to advise flight crews on the requirements for active TSA/TRA avoidance in FRA; Ensure that NAV points to be used to circumnavigate TSAs are published as “fly over” points; Ensure system support for Mode S data processing and display; Ensure system support for graphical presentation of flight trajectory (flight leg) at CWP; Ensure appropriate procedures and system support for CPDLC exchange; Ensure system support for SFPL monitoring and update, and alerting of ATCO (MONA);