

# EUROCONTROL

## Safety Regulatory Requirements

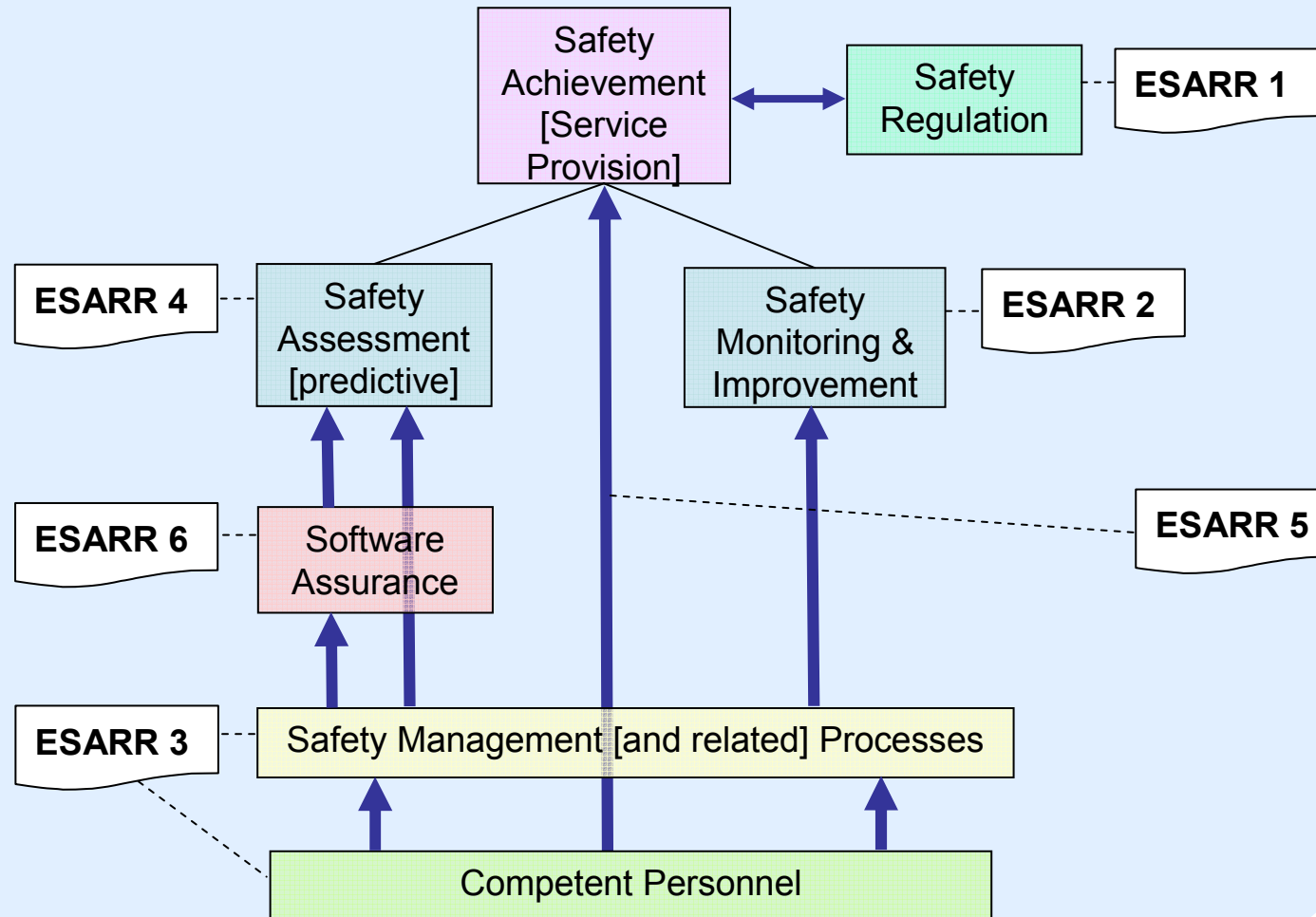
### Practical Application

# ESARRs - Overview

1. Requirements for **safety regulation** by State authorities
2. Safety **monitoring and improvement**
3. Implementation of **SMSs**
4. **Risk assessment** [predictive]
5. **Competence** of ATM personnel
6. **Software assurance** in ATM systems [ground elements]

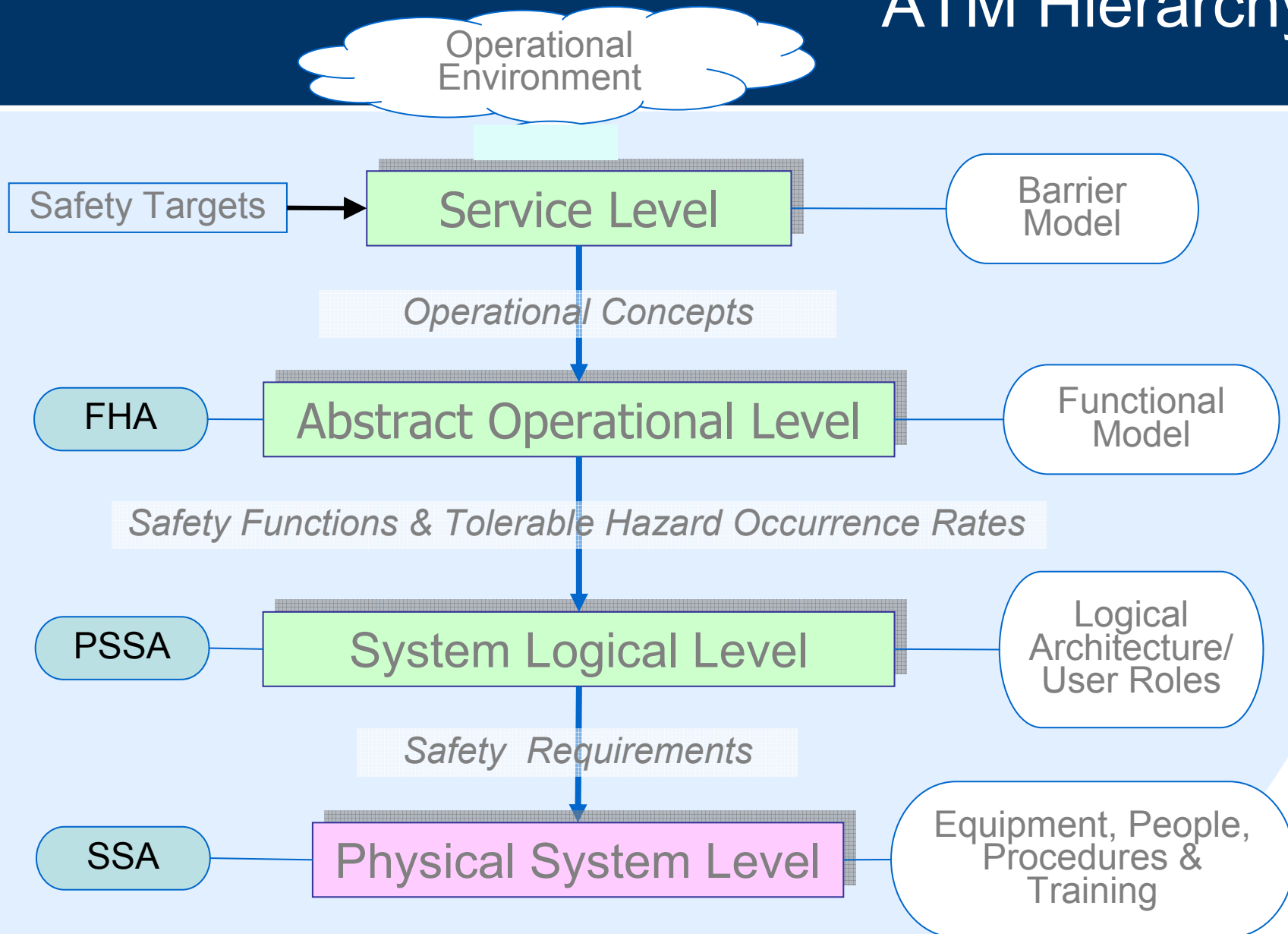
All about process (*how!*), except ESARR 4, Appendix A which specifies design targets for product (*what!*)

# The “Building Blocks”





# ATM Hierarchy

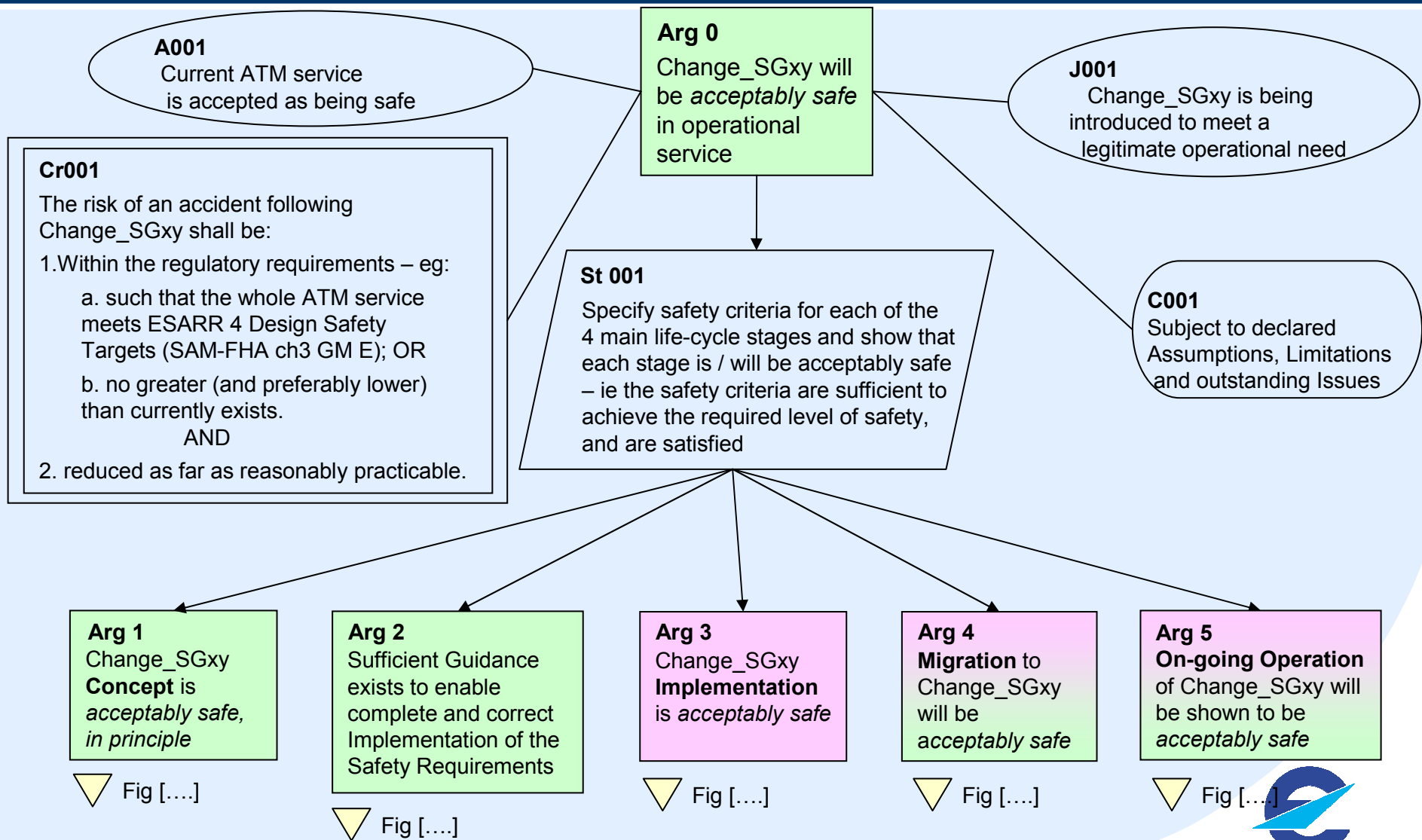


# Safety Cases - Principles

- Needed for on-going operation (Unit Safety Case) and major changes to that operation (Project Safety Case)
- Based on the idea of a Legal Case – presentation of Argument and Evidence that a overall claim is true
- Need to consider two viewpoints:
  - “Success Case” – is the service / system *safe* when it working to specification?
  - “Failure Case” – is the service / system *safe* when it fails
- Evidence comes mainly from:
  - Success Case: simulations, trials, analysis, expert operational judgement etc
  - Failure Case: safety assessment processes – FHA, PSSA, SSA
- Purposes:
  - primarily, for ANSPs to convince themselves that operations are *safe*
  - only secondarily to convince the Regulator that operations are *safe*

Figure 7 Overall Argument Structure

# EUROCONTROL Safety Cases – Safety Argument



# Safety Cases – the Evidence

- Provided only to the degree and extent necessary to support the related Argument
- Source – from safety analysis, design, simulation, test, previous usage, compliance with standards etc – must be appropriate to the Argument
- Two categories:
  - “Direct”: relates to outputs of processes (products)
  - “Backing”: relates to adequacy of those processes
- Must be clear, conclusive and, wherever possible, objective
- Rigour must be appropriate to the associated risk – *Assurance Levels*

Questions?

# Conclusions

- ESARRs provide minimum regulatory requirements for managing safety
- Necessary but not sufficient for demonstrating safety
- Need to supplement ESARRs with processes and procedures that are an Acceptable Means of Compliance – eg EUROCONTROL SAM
- Need to present results of these applying these processes and procedures, in a convincing way – eg a Safety Case
- Safety Cases should be based on rigorous Argument and conclusive Evidence
- Need to consider safety from:
  - Success viewpoint
  - Failure viewpoint