FAA National Software Conference, May 2002
EUROCONTROL Software Task Force

EATMP SAFETY MANAGEMENT

SOFTWARE TASK FORCE

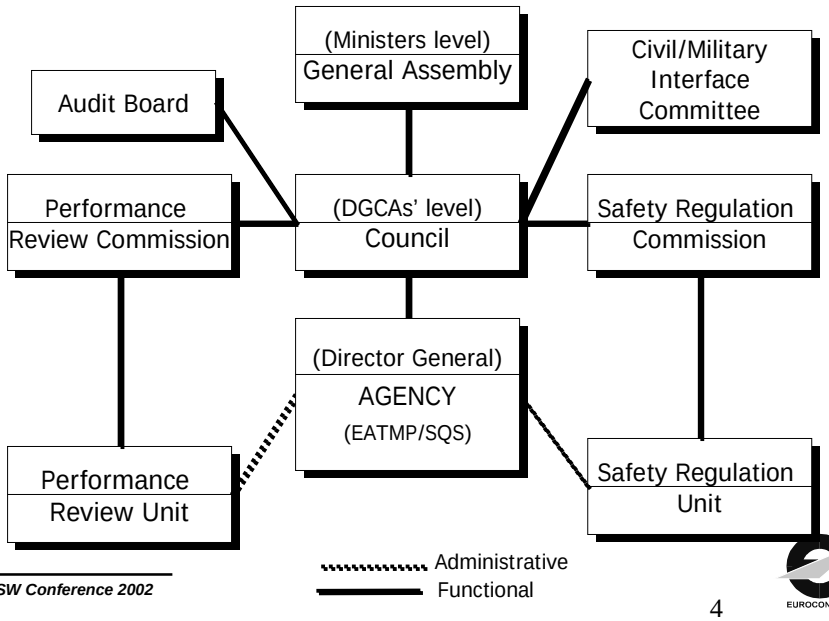
P.MANA
EUROCONTROL
CHAIRMAN

PRESENTATION PLAN

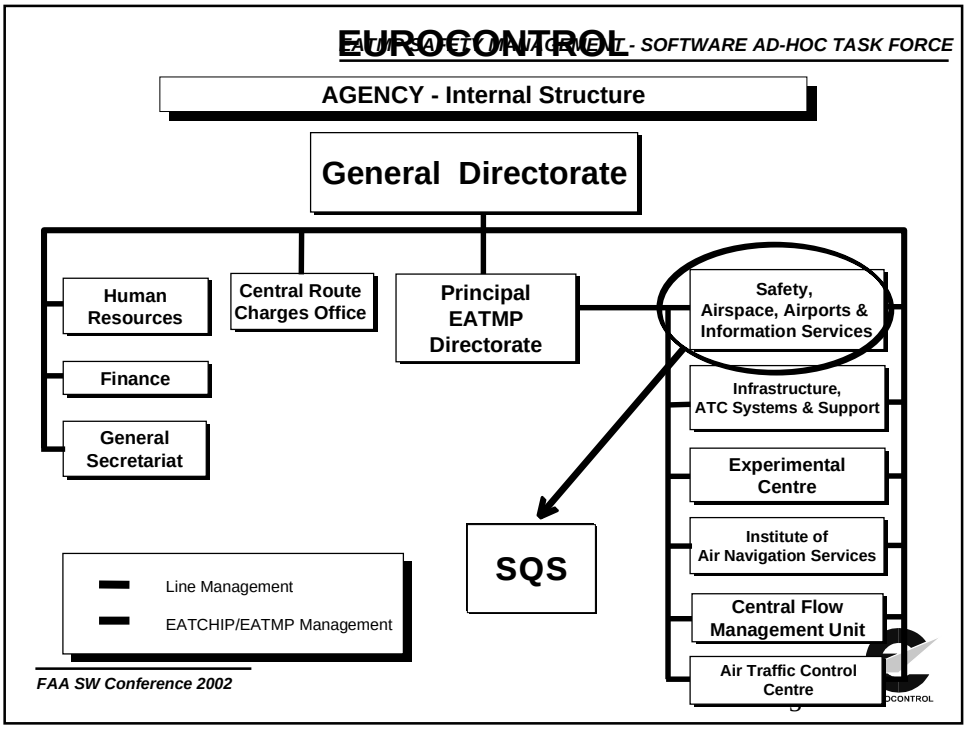
- 1. European Institutional Framework
- 2. System Safety Assessment
- 3. Software Regulatory Requirements
- 4. EATMP Software guidelines

FAA National Software Conference, May 2002
EUROCONTROL Software Task Force

1. European Institutional Framework



FAA National Software Conference, May 2002
EUROCONTROL Software Task Force



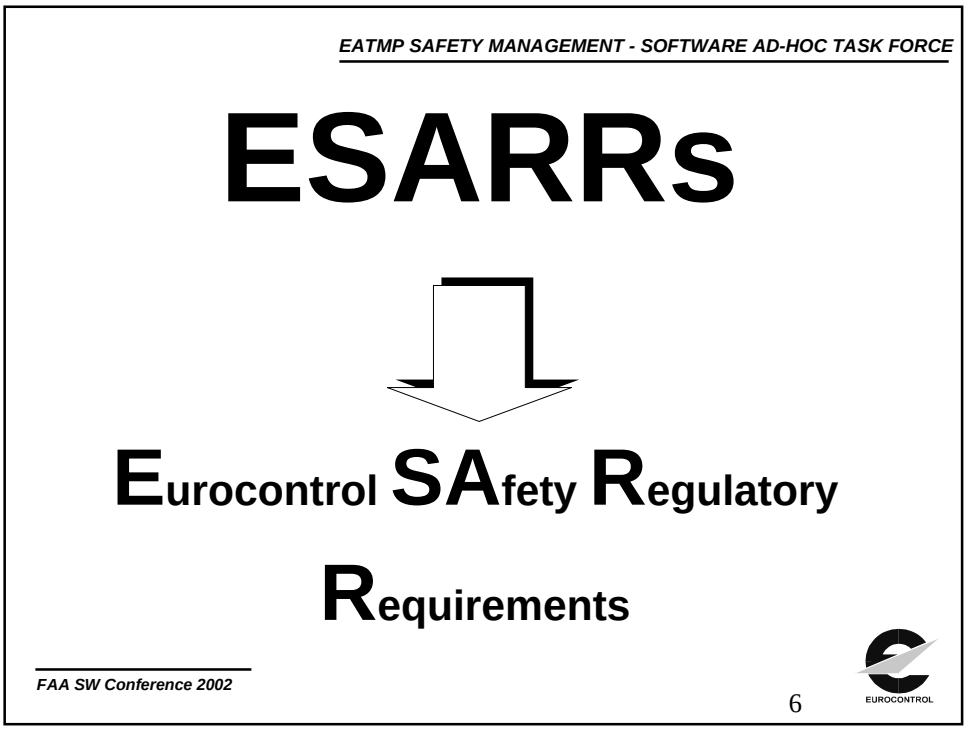
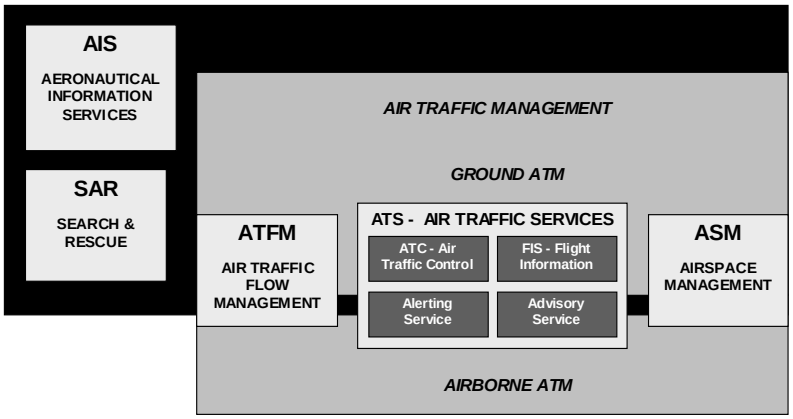
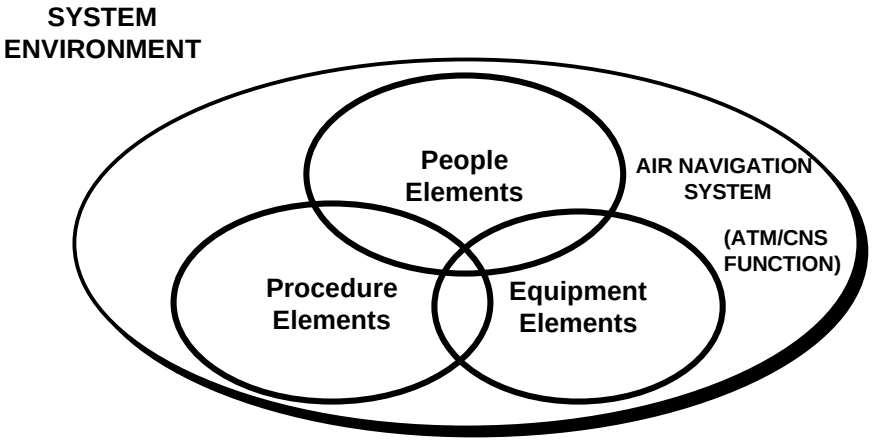


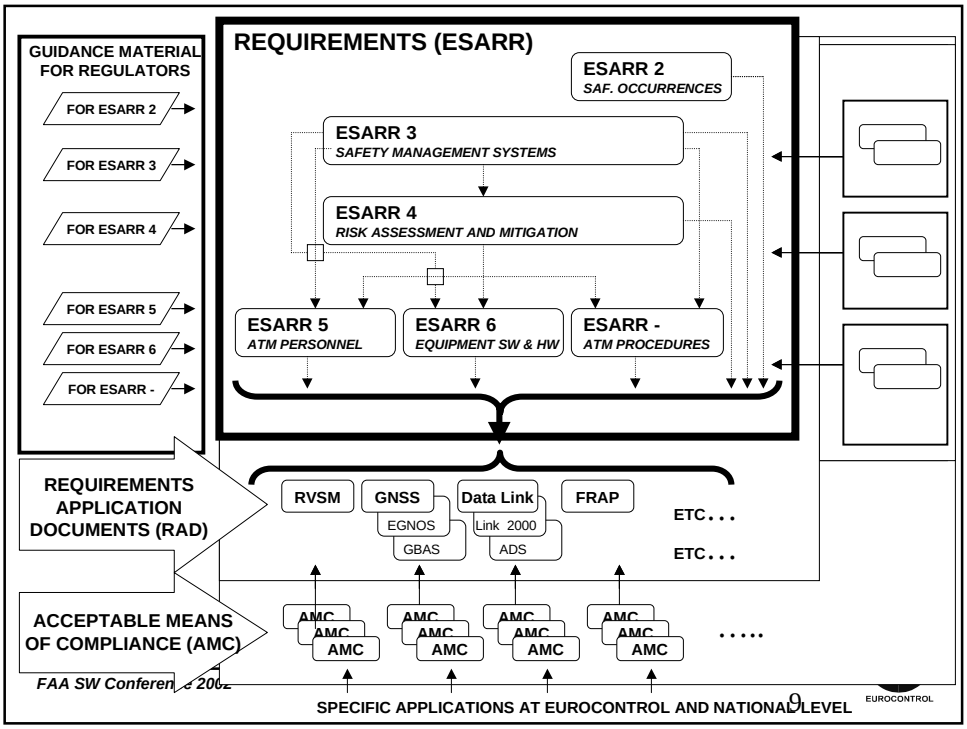
FIG.1 AIR NAVIGATION SYSTEM

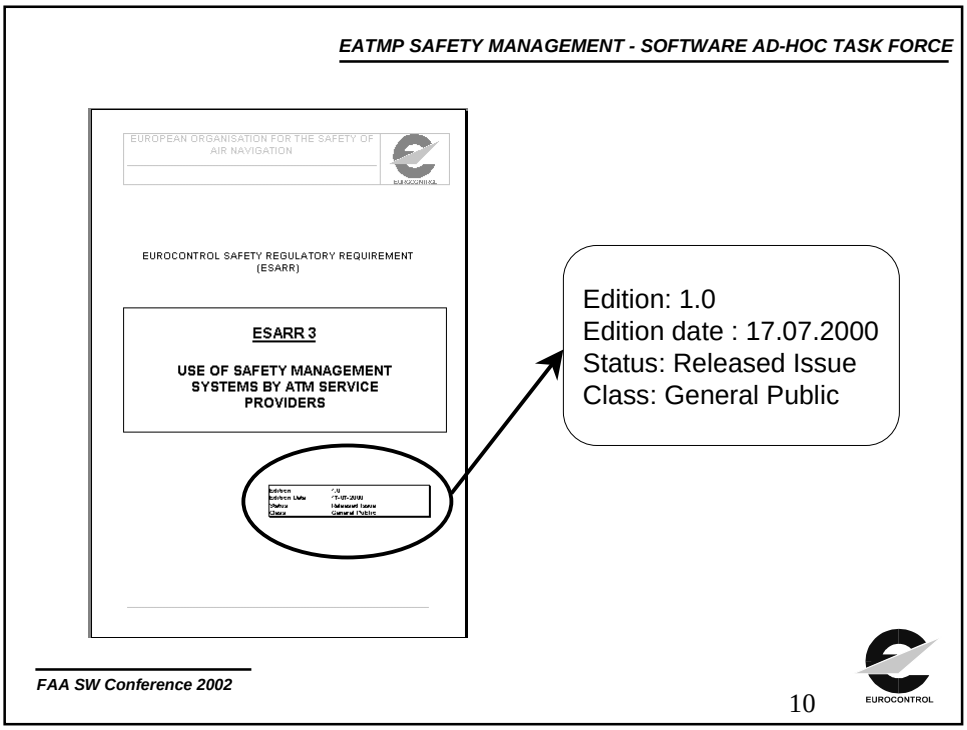


What is a System?



FAA National Software Conference, May 2002
EUROCONTROL Software Task Force

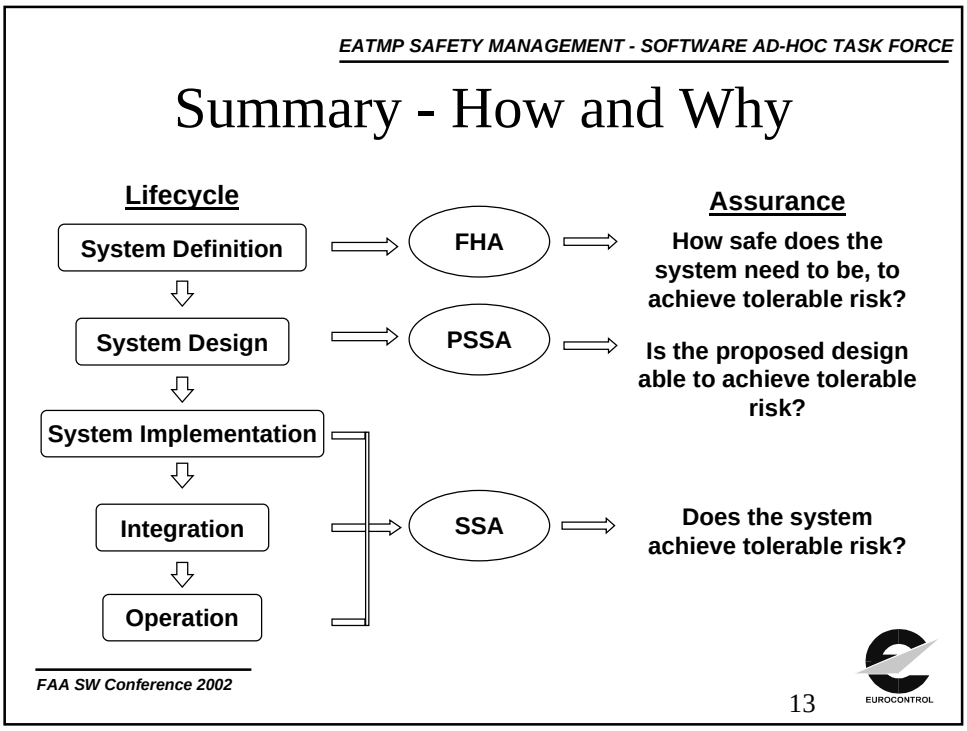


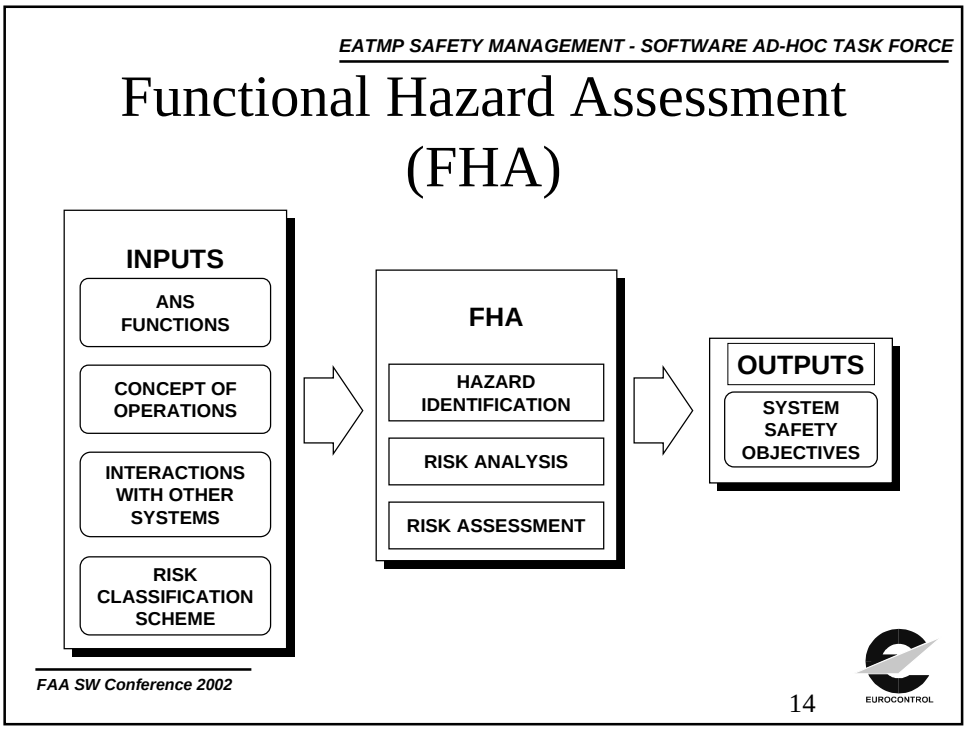


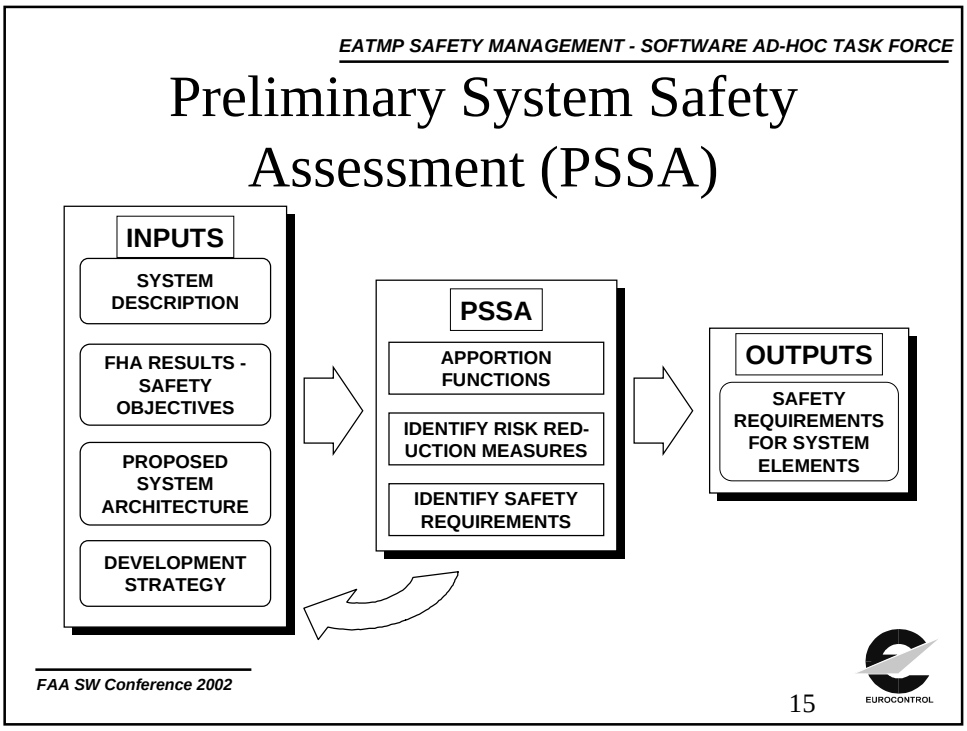
ESARR4 Applicability to Airborne ATM

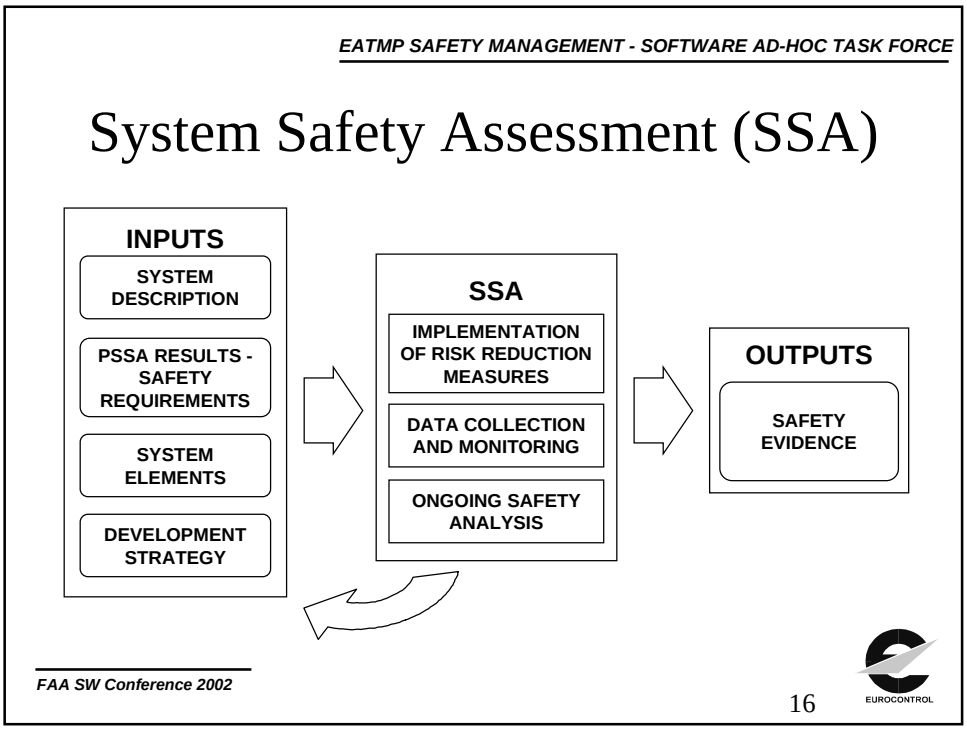
- (1) These objectives and related safety requirements allocated to the airborne part of the ATM System should be considered as ADDITIONAL to those requirements derived from applicable Joint Aviation Requirements (e.g,, JAR 25-1309 and JAR 25-11). Indeed, some elements of the airborne part of the ATM System contribute both to the airworthiness of the aircraft (perceived as isolated form its environment) as well as to the provision of a safe Air Traffic Management System.

2. System Safety Assessment

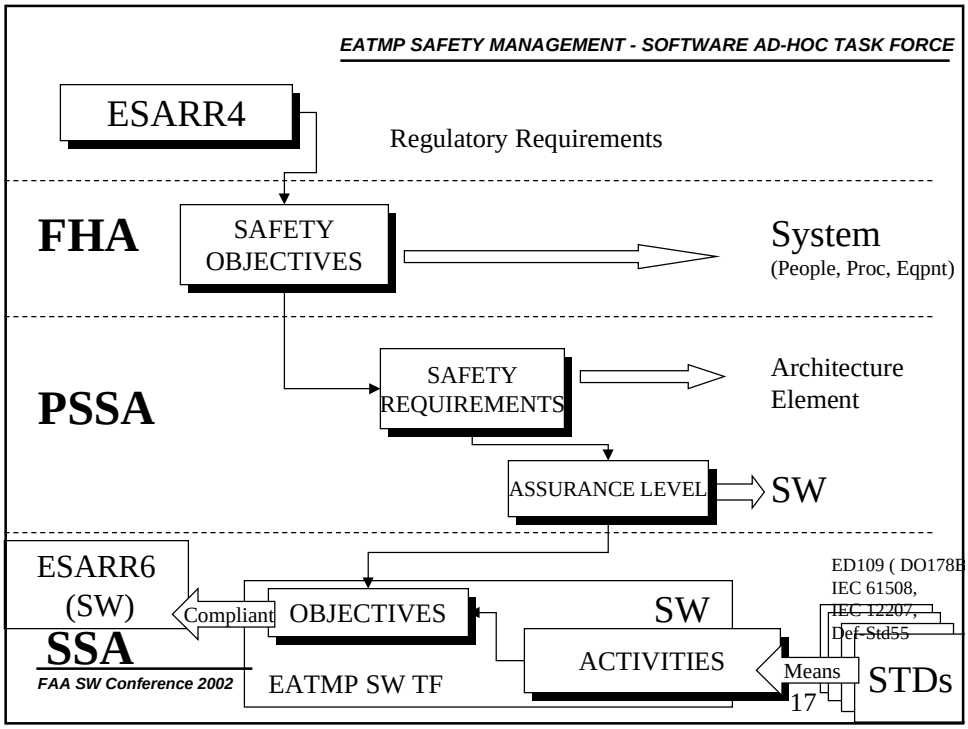

EATMP SAFETY MANAGEMENT - SOFTWARE AD-HOC TASK FORCE
Summary - How and Why
Lifecycle
System Definition
System Design
System Implementation
Integration
Operation
FHA
PSSA
SSA
Assurance
How safe does the system need to be, to achieve tolerable risk?
Is the proposed design able to achieve tolerable risk?
Does the system achieve tolerable risk?
FAA SW Conference 2002
13
EUROCONTROL


EATMP SAFETY MANAGEMENT - SOFTWARE AD-HOC TASK FORCE
Functional Hazard Assessment (FHA)
INPUTS
ANS FUNCTIONS
CONCEPT OF OPERATIONS
INTERACTIONS WITH OTHER SYSTEMS
RISK CLASSIFICATION SCHEME
FHA
HAZARD IDENTIFICATION
RISK ANALYSIS
RISK ASSESSMENT
OUTPUTS
SYSTEM SAFETY OBJECTIVES
FAA SW Conference 2002
14
EUROCONTROL


EATMP SAFETY MANAGEMENT - SOFTWARE AD-HOC TASK FORCE
Preliminary System Safety Assessment (PSSA)
INPUTS
SYSTEM DESCRIPTION
FHA RESULTS - SAFETY OBJECTIVES
PROPOSED SYSTEM ARCHITECTURE
DEVELOPMENT STRATEGY
PSSA
APPORTION FUNCTIONS
IDENTIFY RISK RED-UCTION MEASURES
IDENTIFY SAFETY REQUIREMENTS
OUTPUTS
SAFETY REQUIREMENTS FOR SYSTEM ELEMENTS
FAA SW Conference 2002
15
EUROCONTROL


EATMP SAFETY MANAGEMENT - SOFTWARE AD-HOC TASK FORCE
System Safety Assessment (SSA)
INPUTS
SYSTEM DESCRIPTION
PSSA RESULTS - SAFETY REQUIREMENTS
SYSTEM ELEMENTS
DEVELOPMENT STRATEGY
SSA
IMPLEMENTATION OF RISK REDUCTION MEASURES
DATA COLLECTION AND MONITORING
ONGOING SAFETY ANALYSIS
OUTPUTS
SAFETY EVIDENCE
FAA SW Conference 2002
16
EUROCONTROL

FAA National Software Conference, May 2002
EUROCONTROL Software Task Force



ESARR 6

- States WHAT to do,

  and not HOW to do it (Goal-based regulation)
- The HOW is covered by potential means of compliance, yet to be assessed
- ESARR with large number of potential means of compliance e.g.
  - IEC 61508
  - ED 109
  - ED 12 B / DO178 B
  - MILITARY STANDARDS
  - etc….

ESARR 6 activity

- Requirements applying to
  - Software Safety Assurance System, as part of Safety Management System, and includes requirements for :
  - Software Assurance Level (link with ESARR 4)
  - Software Verification Assurances
  - Software Configuration Management Assurances
- No explicit requirements for Quality Management
- Requires *a priori* safety assessment process
- For COTS, ESARR 6 principles apply, but alternative assurances are required

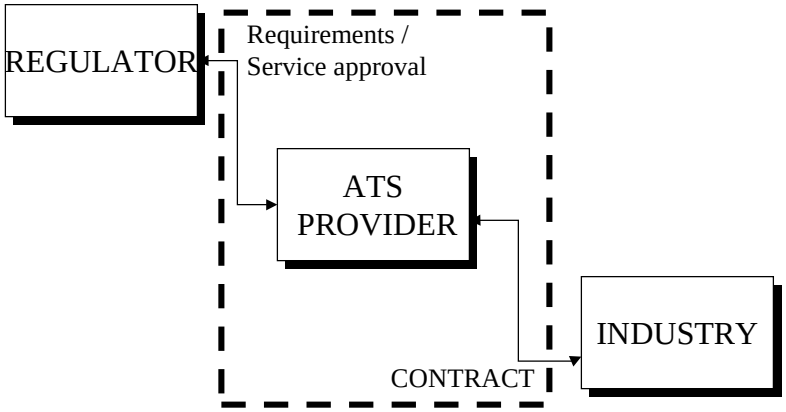
ESARR 6 activity

- **Issues raised that requires solutions before progressing ESARR 6**
  - ①Legal aspects
    - The Status of ESARRs;
    - Adopting ESARRs,
    - Duty of Designated Authority
    - The EU dimension
  - ②Requirements for regulators

4. EATMP Software Guidelines

FAA National Software Conference, May 2002
EUROCONTROL Software Task Force

SCOPE



EATMP SWTF TORs (1)

- Target audience: **ATS providers**
  - 1. Expand safety Regulatory Requirements into assurance safety objectives (Minimum)
    - Means for ATS providers on HOW to manage SW safety aspects (full lifecycle)
    - Means to comply with ESARR6
    - Means to subcontract industry

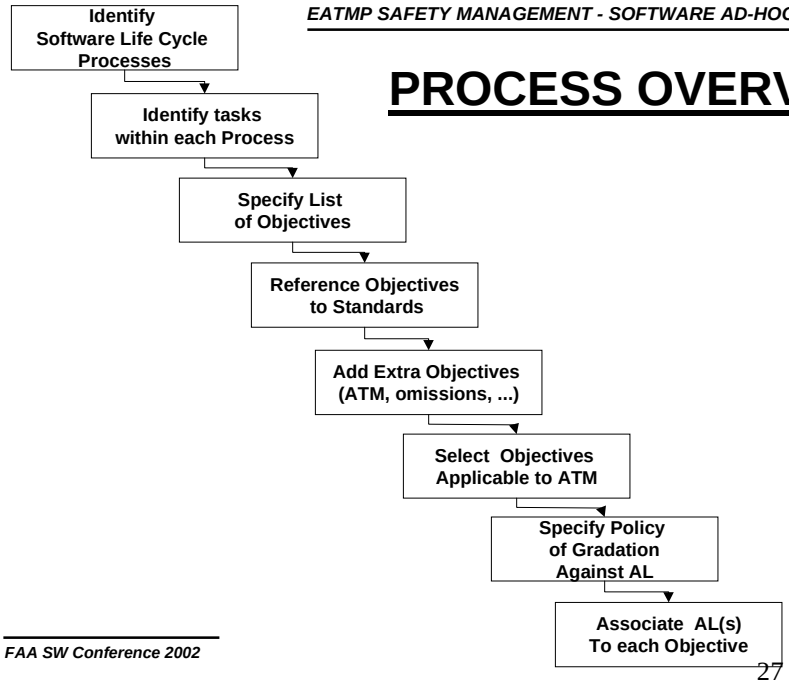
EATMP SWTF TORs (2)

- 2. To level in stringency the safety assurance objectives per software assurance levels
  - To be done; requires a deep understanding of objectives:
    - feasibility (technical, cost, delay)
    - domain best practice
  - Identification of grading criteria

SWTF SCOPE (3)

- 3. To ensure that the assurance objectives and their gradation allow to gain an acceptable level of assurance and confidence in software.
  - Domain engineering judgement
  - Suitable level of detail/prescription

PROCESS OVERVIEW



Two Documents

- 1°) ANS SW Lifecycle: Released
  - Software Lifecycle Definition
    - From conception of need till decommissioning
    - References to 3 standards:
      - IEC12207, ED12B, IEC61508 (in future: ED109 & CMM)
  - SW Assurance Level definition
- 2°) Recommendations for ANS SW : Draft
  - Grading policy
  - Objectives per SWAL

ANS SOFTWARE LIFECYCLE

ANS SW Lifecycle

- SW Safety Assurance System
  - SWAL Def/Initiation/Planning/Reqnt Specif/V&V/Completion
- Primary Lifecycle
  - Acquisition/Supply/Development/Operation/Maintenance
- Supporting Lifecycle
  - Documentation/CM/QA/V&V/Audit/Problem Resolution
- Organisational Lifecycle
  - Management/Infrastructure/Improvement/Training
- Additional Lifecycle
  - SW Environment/HMI/COTS

EATMP SAFETY MANAGEMENT - SOFTWARE AD-HOC TASK FORCE

SWTF / STDs

EATMP SW TF

Quality

12207

Safety

ED109/ DO278

IEC 61508

Not Tailored to CNS/ATM

FAA SW Conference 2002

31

EUROCONTROL

EATMP SAFETY MANAGEMENT - SOFTWARE AD-HOC TASK FORCE

TRACEABILITY to Standards

Topic	Rationale	ISO/IEC 12207	ED-12B/ DO 178B	IEC 61508
Process Implementation	The developer should define or select a software lifecycle model appropriate to the scope, magnitude, and complexity of the project. The developer should select, tailor, and use those standards, methods, tools, and computer programming languages. The developer should develop plans for conducting the activities of the development process.	• (Ref: 5.3.1)	• (Ref: 3, 4, 11.2)	P (Ref: 7.1.2.1, 7.4.1.3, Part I-7)
Software Development Plan	This plan is used to determine whether the proposed software lifecycle is commensurate with the rigor required for the level of software being developed.		• (Ref: 11.1, 11.2)	
System Requirements Analysis	The system requirements specification should describe: functions and capabilities of the system; business, organisational and user requirements; safety, security, human-factors engineering (ergonomics), interface, operations, and maintenance requirements; design constraints and qualification requirements.	• (Ref: 5.3.2)	• (Ref: 2.1)	• (Ref: Part I-7.6, Part II-7.2 II-7.9)
System Architectural Design	It should be ensured that all the system requirements are allocated among hardware, software, and manual-operations.	• (Ref: 5.3.3)	P (Ref: 2.3)	P (Ref: Part II-7.4)

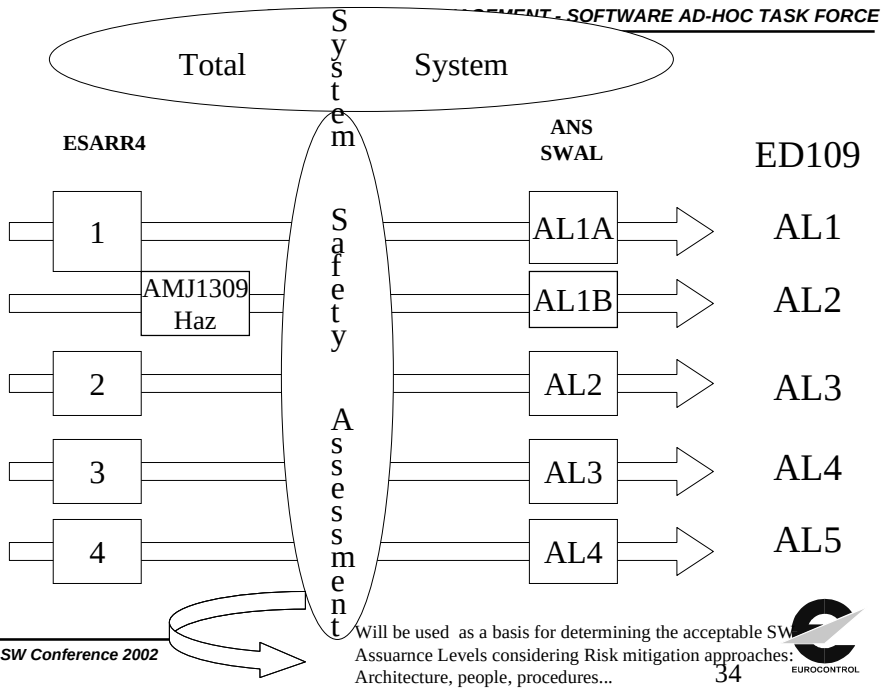
FAA SW Conference 2002

32

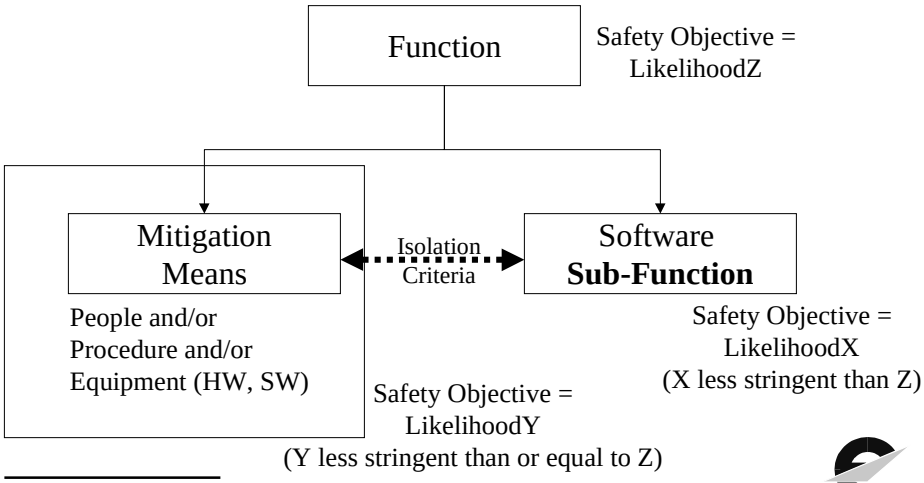
EUROCONTROL

ANS SWAL Definition

- SWAL X= SW whose anomalous behaviour, as shown by System(people, procedure, equipment) Safety Assessment process,
  - either would directly cause a failure of system function whose end effect as a severity ESARR4.X
  - or would cause a failure whose likelihood of occurrence is no greater than LikelihoodX
- Except SWAL 1A= directly cause a failure of system function whose end effect as a severity ESARR4.1



Basics of Mitigation Means Influence



RECOMMENDATIONS FOR ANS SW

SW AL Grading Policy

- Identification of criteria:
  - Required/Not required
  - Independence
  - Number/kind of evidence(s)
    - 1 or 2 (dependent or independent)
    - Test, Analysis, Field experience, …..
    - Process and/or Product
  - Depth of investigation:
    - Black Box,White (Gray ?) Box, Code, Exec

EATMP SAFETY MANAGEMENT - SOFTWARE AD-HOC TASK FORCE

SWAL Grading Policy

- SW AL1A: Executable
- SW AL2: Code (SW Component)
- SW AL3: Preliminary Design (CSC);

a first level of refinement of SW architecture and SW components (CSC) is required, but these SW components (CSC) can be considered as black boxes

- SW AL4: SW as a Black Box
- (SW AL5: Not a SWAL but a SW quality level.)

EATMP SAFETY MANAGEMENT - SOFTWARE AD-HOC TASK FORCE

Recommendations for ANS SW

Obj N°	ALs Objectives Title/Topic	OBJECTIVES	AL 1	AL 2	AL 3	AL 4	AL 5	Output
4.3.3	***Process Implementation***	Including: - end of activity/phase criteria for each activity/phase - joint technical review for each activity/phase ***ref 5.3.1) 12207*** The developer should define or select a software life cycle model appropriate to the scope, magnitude, and complexity of the project. The developer should select, tailor, and use those standards, methods, tools, and computer programming languages. The developer should develop plans for conducting the activities of the development process. Scope: life cycle definition, outputs documentation, outputs configuration management, SW products problems, environment definition, development plan, COTS	*	*	*	*	*	
4.3.4	***SW requirements analysis***	***(ref 5.3.4) 12207*** The developer should establish and document software requirements, using software requirements standard. Algorithms should be specified.	*	*	*	*		
4.3.5	***SW architectural design***	***(ref 5.3.5) 12207*** The developer should transform the requirements for the software item into an architecture that describes its top-level structure and identifies the software components. Scope: top level SW architecture definition, top level interfaces design, SW integration definition, SW architecture definition criteria	*	*	*			
4.3.6	***SW detailed design***	***(ref 5.3.6) 12207*** The developer should develop a detailed design for each software component of the software item using software design standard. Scope: SW detailed design definition, interfaces design, SW Units tests definition.	*	*				
4.3.7	***SW integration***	***(ref 5.3.8) 12207*** The developer should develop an integration plan to integrate the software units and software components into the software item. The plan should include test requirements, procedures, data responsibilities, and schedule. The plan should be documented. Scope: SW integration plan, SW integration definition, user documentation, SW validation preparation, SW integration evaluation (partially)	*	*	*			

FAA SW Conference 2002

39

EUROCONTROL

EATMP SAFETY MANAGEMENT - SOFTWARE AD-HOC TASK FORCE

Safety Management WEB address

www.eurocontrol.int/safety

FAA SW Conference 2002

40

EUROCONTROL

EATMP SAFETY MANAGEMENT

SOFTWARE TASK FORCE

END OF PRESENTATION