Network Manager
nominated by
the European Commission

EUROCONTROL

ES²
Experience Sharing Enhanced SMS Lessons Learned

EUROCONTROL ES2 SW Safety Assurance WS

Luxembourg, 7-8 May 2013

Dr. Frederic Lieutaud
ES² Project Manager
DNM/COO/ NOM/SAF-Unit
frederic.lieutaud@eurocontrol.int

Tony Licu
Head of DNM/COO/ NOM/SAF-Unit
antonio.licu@eurocontrol.int

Network Manager
nominated by
the European Commission

ES²-WS03-11, Software Assurance Process – Bled Feedback

EUROCONTROL

Points raised

- Need to understand the impact of new regulations, if any, by 2013
- Different approaches for AMC's because different ANSPs, furthermore various depth of complexity of requests that leads Manufacturers to tailor the approach
- ED-153 and ED-109, the most frequently mentioned, but still at high level
- Interface/interaction ANSPs/Manufacturers
  - ✓ How should safety requirement issued from the IRs be considered in the global system/equipment safety assessment?
  - ✓ When or how compliance to objectives can be determined?
  - ✓ How can we get a better/common (ANSP/Manufacturer) view of what we really need to do to show compliance to EC482?
  - ✓ What should be the content of EC 552 declaration of conformity in relation with safety assessment?
  - ✓ Roles and responsibilities in providing SW requirements and SW assurance.

Network Manager nominated by the European Commission

ES²-WS03-11, Software Assurance Process – Bled Feedback

EUROCONTROL

Points raised

- How can one give a satisfactory answer to all the regulation requirements using:
  - ✓ results of the safety analysis integrated with
  - ✓ outputs of a good software engineering practice
- Do we have enough information in GM (EDs etc) for COTSs and SWAL
- Degraded modes of Operations to be considered – complementary to the "design & implementation" SSA
- Maintenance aspects
- Input to EASA groups dealing with SW and Safety Assessment and Need to work with EASA to support the SW oversight harmonisation
- Need to have a forum to share best practices and clarify role, responsibilities of each party (including NSA) - Involve more NSAs
- Integration of other activities HF, security in one pack !
- How to avoid having "regulator focused documents", i.e.
  - ✓ Documents made just to please the regulator?

Network Manager
nominated by
the European Commission

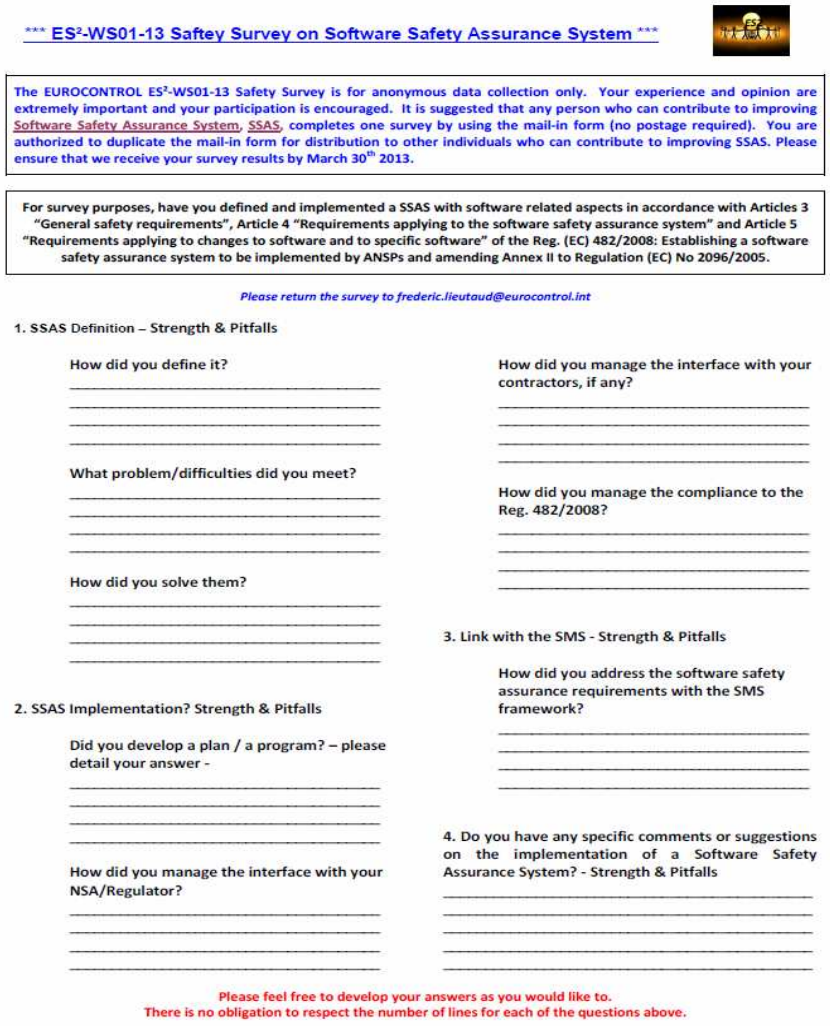
Regulation EC482/2008
Establishing a Software Safety Assurance System

EUROCONTROL

In accordance with:

- Articles 3 “General safety requirements”,
- Article 4 “Requirements applying to the software safety assurance system” and
- Article 5 “Requirements applying to changes to software & to specific software”

- Definition
- Implementation
- Integration into SMS Framework
- Any Specific Comments & Suggestions



*** ES²-WS01-13 Saftey Survey on Software Safety Assurance System ***

The EUROCONTROL ES²-WS01-13 Safety Survey is for anonymous data collection only. Your experience and opinion are extremely important and your participation is encouraged. It is suggested that any person who can contribute to improving Software Safety Assurance System, SSAS, completes one survey by using the mail-in form (no postage required). You are authorized to duplicate the mail-in form for distribution to other individuals who can contribute to improving SSAS. Please ensure that we receive your survey results by March 30th 2013.

For survey purposes, have you defined and implemented a SSAS with software related aspects in accordance with Articles 3 “General safety requirements”, Article 4 “Requirements applying to the software safety assurance system” and Article 5 “Requirements applying to changes to software and to specific software” of the Reg. (EC) 482/2008: Establishing a software safety assurance system to be implemented by ANSPs and amending Annex II to Regulation (EC) No 2096/2005.

Please return the survey to frederic.lieutaud@eurocontrol.int

1. SSAS Definition – Strength & Pitfalls

How did you define it?

What problem/difficulties did you meet?

How did you solve them?

2. SSAS Implementation? Strength & Pitfalls

Did you develop a plan / a program? – please detail your answer -

How did you manage the interface with your NSA/Regulator?

How did you manage the interface with your contractors, if any?

How did you manage the compliance to the Reg. 482/2008?

3. Link with the SMS - Strength & Pitfalls

How did you address the software safety assurance requirements with the SMS framework?

4. Do you have any specific comments or suggestions on the implementation of a Software Safety Assurance System? - Strength & Pitfalls

Please feel free to develop your answers as you would like to.
There is no obligation to respect the number of lines for each of the questions above.

1- SSAS Definition

How did you define it

- Activities/Processes implementing risks approach:
  - on the ATM service associated with Sw failures
  - to reach a safe product, through the whole Sw Development Lifecycle
- Updates of internal processes related to project or equipment maintenance.
- According to EUROCONTROL Document ANS Sw Lifecycle and Recommendations for ANS Software (later ED-153)
- Common sense and experience from another domain (aeronautical, space …..)
- Use of independent audit results. From the existing experienced Engineering Quality System (bottom up), development of compliance matrix based on interpretation of high level requirements (top-down) and assessment of its level of compliance

Software Safety Assurance System is not defined as a system as such, common sense is used looking at the adaptation of the existing SMS processes

1- SSAS Definition

Problem difficulties met

- Resistance/Inertial behaviour in the Company, the coverage of the objectives of Reg. requires adaptation of existing processes and maintenance procedures for all the different sub-systems that exist
- Benefit expected wrt Reg & SSAS as the word “safety” is confusing to the staff looking at the connection with the safety and area of responsibilities of staff
- Adaptation of requirements into a practical methodology
- Training needs vs resources available, lack of Sw safety engineers
- Understanding the regulation:
  - what defines Sw as the first and most important problem encountered
  - linking high level requirements to low level of practicability (procedures/evidence) to show compliance because a large number of objectives has to be fulfilled and distract from the main ones
- Lack of guidance vs requirements as most of the Reg. aim at New Sw while most systems re-use Sw
- Difficulties to find general procedures as almost always a unique solution must be used based on the different pre-requisite (supplier maturity, amount of Sw, access to relevant field data, etc..)
- SWAL allocation definition

1- SSAS Definition

Solution

- Focus in the essential tasks to fulfill objectives
- Use qualitative assessment for SWAL assignment process
- Making a compliance matrix of ED-153 objectives to the internal processes, identifying gap and defining the best way to cover them
- Use consultancy
- Train staff
- Support from internal developers to get practical solutions
- Tenacity, because huge work to apply it to all sub-systems
- Benchmarking with other ANSPs and contract Sw engineers when relevant
- Meeting people in other industry who faced the same problem and taking training course

No unique solution to define what is a SSAS

Looking around and using ED-153, and Training Staff

2- SSAS Implementation

No Development of a Plan/Programme

- Annex to the main Safety Procedure compiling the SSAS and including dissemination process
- No project initiated, a task was defined
- Stepwise implementation when needed
- Part of the documentation controlling safety arguments
- Chapter dedicated to SSAS

Development of a Plan/Programme

- Plan developed in safety and engineering areas
- Processes, starting with compliance to EU1035/2011 for safety assessment for changes, the compliance to EC482/2008 is made building safety arguments for changes .The plan includes the development of a Product Software Safety Assurance Manual and present generic compliance matrix for ED153 to National Authority
- Using consultancy for the development of a programme to tackle the SSAS definition for ATM network and CNS domain. This programme is customized during the implementation phase on the appropriate pieces of equipment

2- SSAS Implementation

Interface with Authority/Regulator

- Face to face meetings and agreeing controversial aspects of the SSAS
- Regular contacts
  - Keeping up to date on the progress all along the SSAS development and implementation
- Sending documentation
  - All major output and asking for approval, plus plan to discuss proposed means of compliance through the developed compliance matrix
  - A framework for the SSAS, how to comply with EC482/2008 plus identification of evidences
- Audits of safety assessments and procedures implemented / Audit of the SSAS, part of the SMS already accepted by the regulator

Interface with Contractors/Manufacturers

- Use of Sw Safety Assurance expert when needed, agreeing on tasks, scope and objectives
- Identification of SWAL with the Call for Tender / Sw requirements as part of the contract, letting open the extension to maintenance contract and enhancements
- Use of ED153 as an applicable document for process and responsibilities of the suppliers, plus additional internal process for the collection of evidences against safety arguments to get a complete traceability of all changes and upgrades during the lifecycle of the equipment

2- SSAS Implementation

- **Compliance to Reg. 482/2008 for the establishment of SSAS**
  - **Traceability matrix with ED-153 and wih EC482/2008**
  - **Agreed SWAL Compliance Matrix document filled in with evidences, any alternate method needs to be presented to Regulator for approval**
  - **Use relevant part of ED-153 as means of compliance plus Article 5 from EC482/2008 and producing a safety folder gathering evidences**
  - **Through the SSA Plan**
  - **A dedicated unit who controls the evolution of the SSAS over the various domain (ATM, Network and CNS)**
  - **Need to further look at best practices**

Network Manager
nominated by
the European Commission

3- Integration into SMS framework

EUROCONTROL

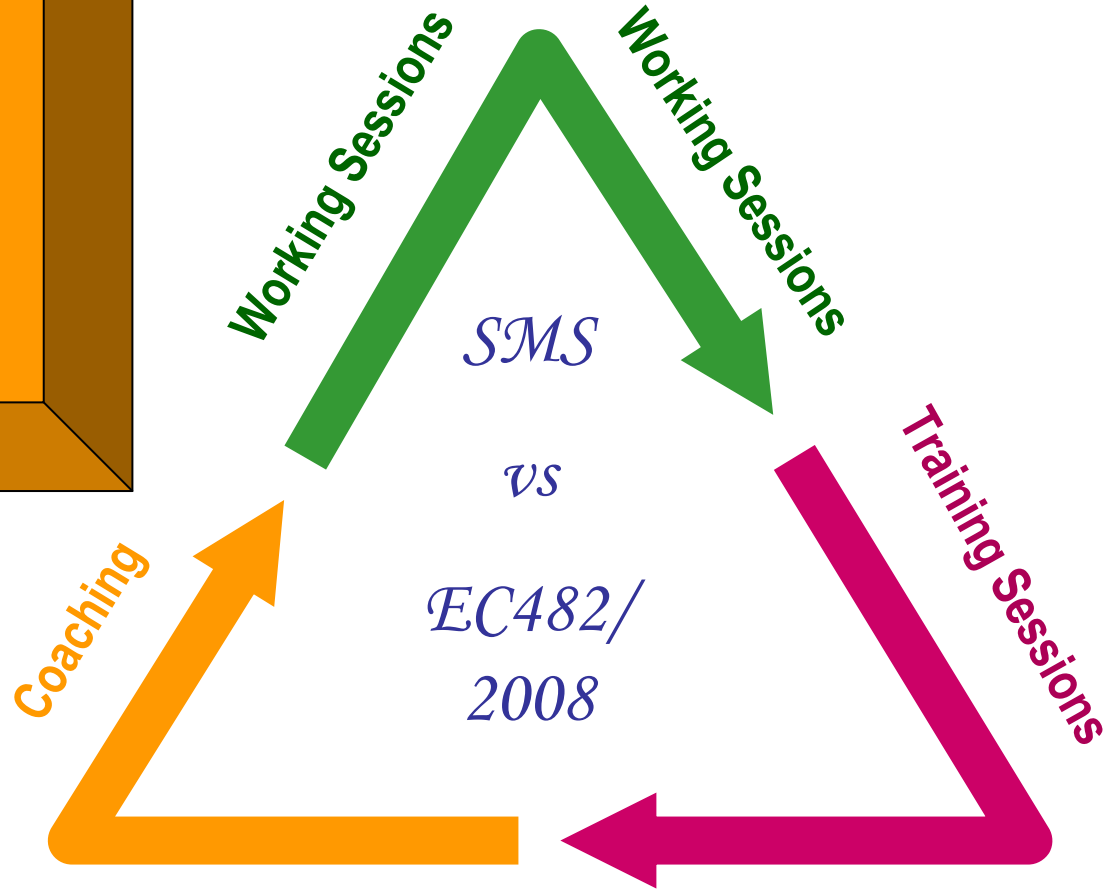
- **Main SMS Procedures maintaining links with Sw Safety Assurance process (generic aspect of Safety Management Manual)**
  - In each phase of the Safety Assessment process
    - FHA
    - PSSA
    - SSA
  - Within a Safety Assessment Handbook (whole Safety Assessment process) including a link to a Sw Assessment Handbook:
    - Theory, Practical Guidance on SSAS & EC482/2008
  - Part of the documentation controlling safety arguments
  - Dedicated chapter to SSAS

- **As a separate high level procedure of the SMM**
  - Extensive references to more detailed processes used by engineering and project teams
  - Guidance and use of ED-153

Network Manager
nominated by
the European Commission

EUROCONTROL

Document added to SMS Covering the SSAS Adaptation to internal processes to be included in the processes themselves As a Guidelines or As specific activities



Network Manager
nominated by
the European Commission

4- Specific Comments and Suggestions

EUROCONTROL

- **Reg. EC482/2008 content**
  - Need to Clarify the following items:
    - Qualitative SWAL assignment / COTS / Legacy of Sw / Maintenance and Monitoring
  - Needs a lot of interpretation, therefore requires extensive knowledge of the requirements at high level and what they mean in practice

- **Reg. 482/2008 vs Performance Regulation**
  - Question is whether such requirements for Sw alone add any benefit when it is supposed to take a total systems approach
  - Where are hardware, staff, procedures requirements that have an impact on safety performance

- **Implementation: Methods/Guidance vs EC Reg. requirements and I/F with Industry**
  - Implementation of EC requirements can differ drastically and not a lot of guidance is available
  - ED-153 which is a proposed AMC, induces workload on project and maintenance team
    - Some objectives are not clear and covers more than required by Reg. EC482/2008
  - EC requirements are complex and difficult to find best practice to use
  - Guidance or Best Practice method should be developed to be used by the Industry and the ANSPs

Network Manager
nominated by
the European Commission

EC482/2008 – Article 4 Definition for

EUROCONTROL

- **Software Safety Assurance System**

  The organisation shall ensure, as a minimum, that the SSAS:

  1. **is documented, specifically as part of the overall risk assessment and mitigation documentation**
  2. **allocates software assurance levels to all operational EATMN software in compliance with the requirements set out in Annex I**
  3. **includes assurances of:**

     (a) software safety requirements validity in compliance with the requirements set out in Annex II, Part A

     (b) software verification in compliance with the requirements set out in Annex II, Part B

     (c) software configuration management in compliance with the requirements set out in Annex II, Part C

     (d) software safety requirements traceability in compliance with the requirements set out in Annex II, Part D

- **Rigour of software assurance level**

  4. **determines the rigour to which the assurances are established; the rigour must be defined for each software assurance level, and increase as the software increases in criticality; for that purpose:**

     (a) the variation in rigour of the assurances per software assurance level must include the following criteria:

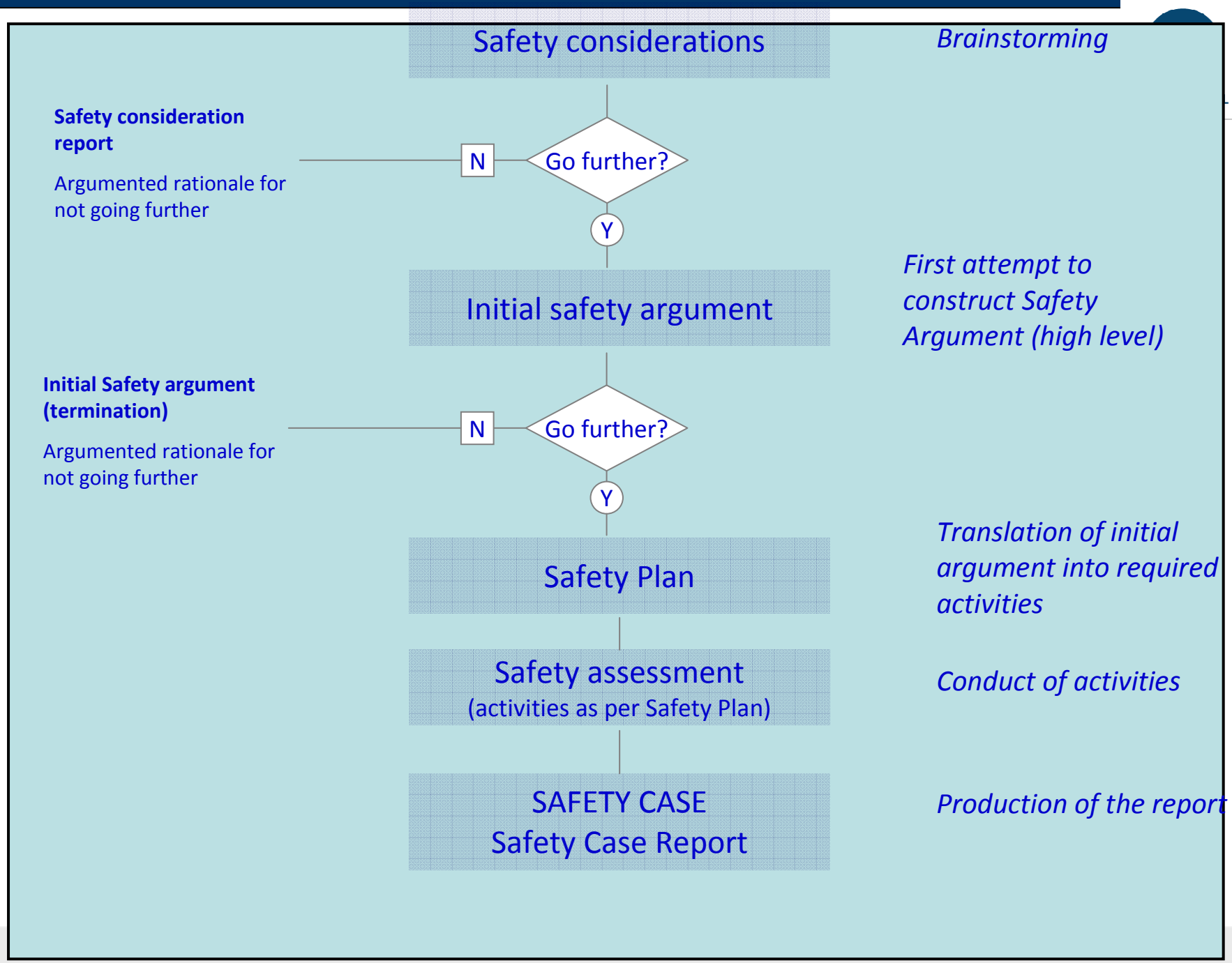
        (i) required to be achieved with independence;

        (ii) required to be achieved;

        (iii) not required;

     (b) the assurances corresponding to each software assurance level must give sufficient confidence that the EATMN software can be operated tolerably safely;

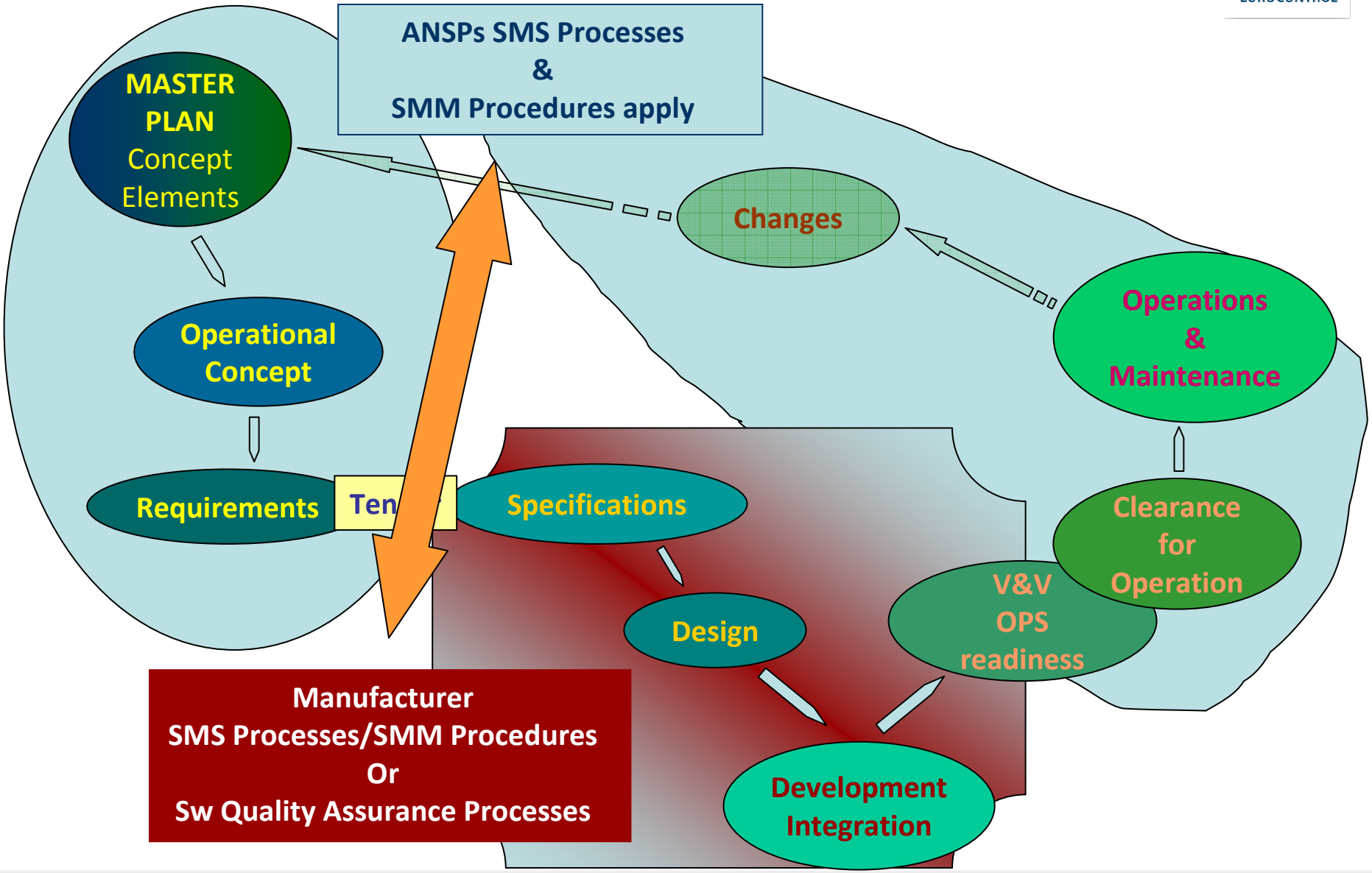
  5. **uses feedback of EATMN software experience to confirm that the software safety assurance system and the assignment of assurance levels are appropriate. For that purpose, the effects from a software malfunction or failure reported according to the relevant requirements on reporting and assessment of safety occurrences shall be assessed in comparison with the effects identified for the system concerned as per the severity classification scheme established in Section 3.2.4 of Annex II to Regulation (EC) No 2096/2005.**


Safety considerations
Brainstorming
Safety consideration report
Argumented rationale for not going further
N
Go further?
Y
Initial safety argument
First attempt to construct Safety Argument (high level)
Initial Safety argument (termination)
Argumented rationale for not going further
N
Go further?
Y
Safety Plan
Translation of initial argument into required activities
Safety assessment
(activities as per Safety Plan)
Conduct of activities
SAFETY CASE
Safety Case Report
Production of the report

Network Manager
nominated by
the European Commission

Generic Project Management Process

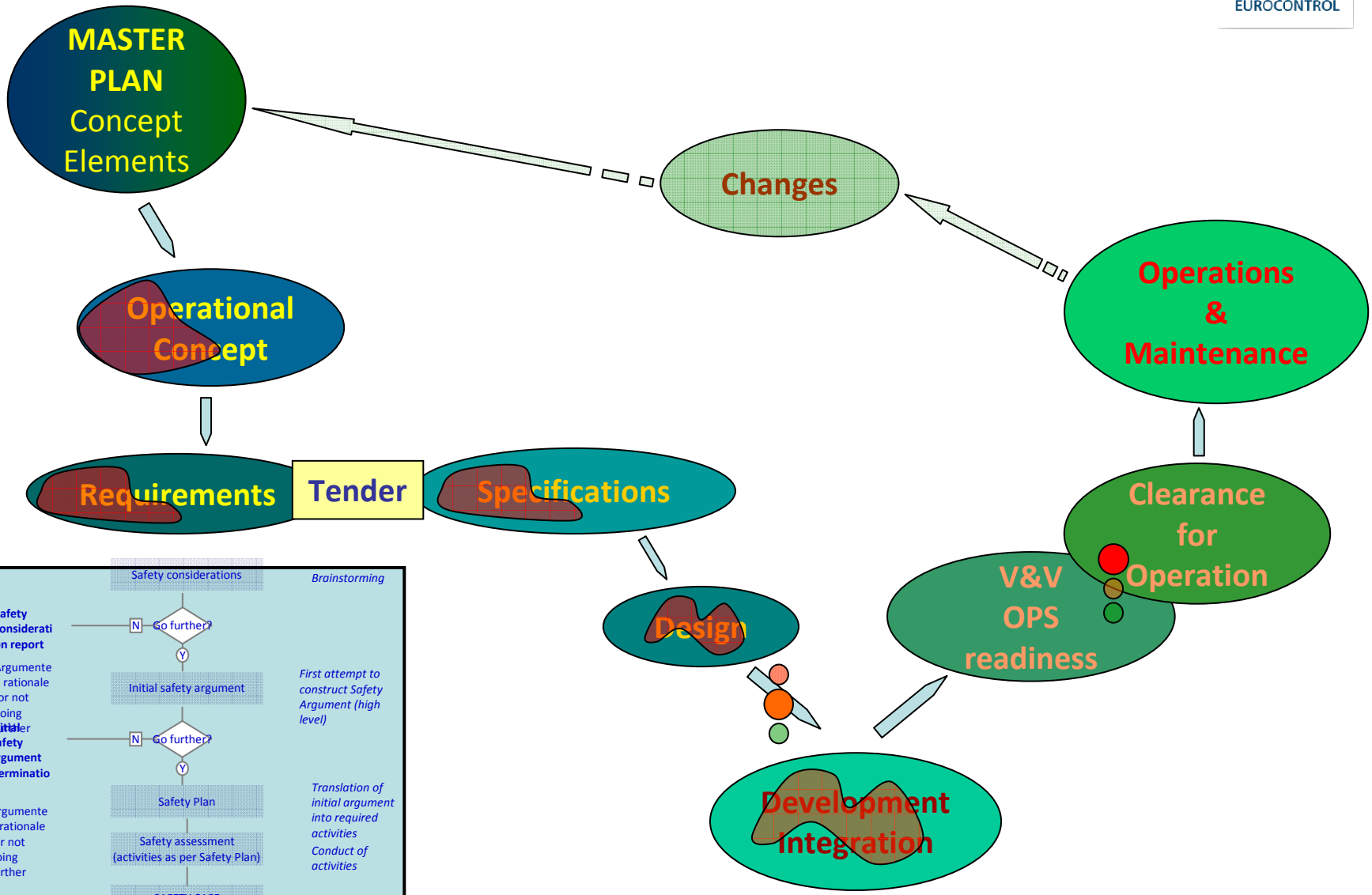
EUROCONTROL



Network Manager
nominated by
the European Commission

Generic Project Management Process for Changes

EUROCONTROL



Quality of Software

- **Factors specifying the Quality of a Sw(#11)**
  - Usability, Integrity, Efficiency, Correctness, Reliability, Maintainability, testability, Flexibility, Reusability, Portability, Interoperability

- **Criteria (#23)**
  - To satisfy each factors, there is a need to achieve defined criteria:
    - ✓ "Reliability: Number of Errors, Accuracy, Error Tolerance, Consistency, Simplicity"
    - ✓ "Testability: Simplicity, Test Coverage, Instrumentation, Self-descriptiveness, Modularity"

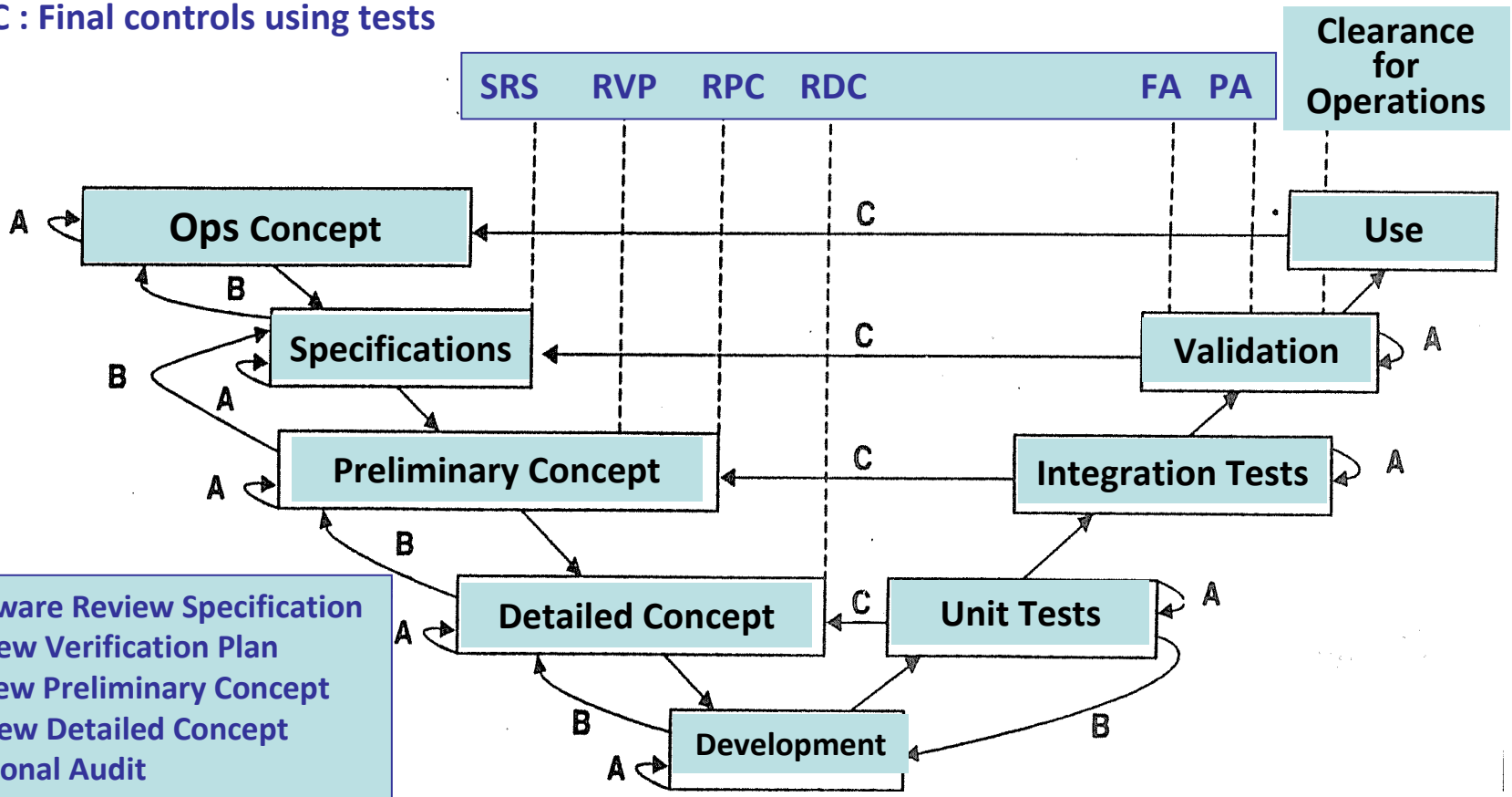
- **Metrics (#127)**
  - Rules to be implemented to allow satisfaction to a given criteria
    - ✓ For "Consistency"
      - ✓ A Standardized Method for specification apply
      - ✓ There is only one formulation to a given concept
      - ✓ A set of given process is processed with the same manner everywhere
      - ✓ …

Need specific & customized approach, impossible to satisfy all factors for a given product

Software Life Cycle & Controls

On the top of that Controls must be performed for the tasks implemented to build the Quality of the Sw all along its Life cycle

- **Type A: Internal controls, documents review and analyse or code review with independent team**
- **Type B : Consistency controls through review and reading**
- **Type C : Final controls using tests**

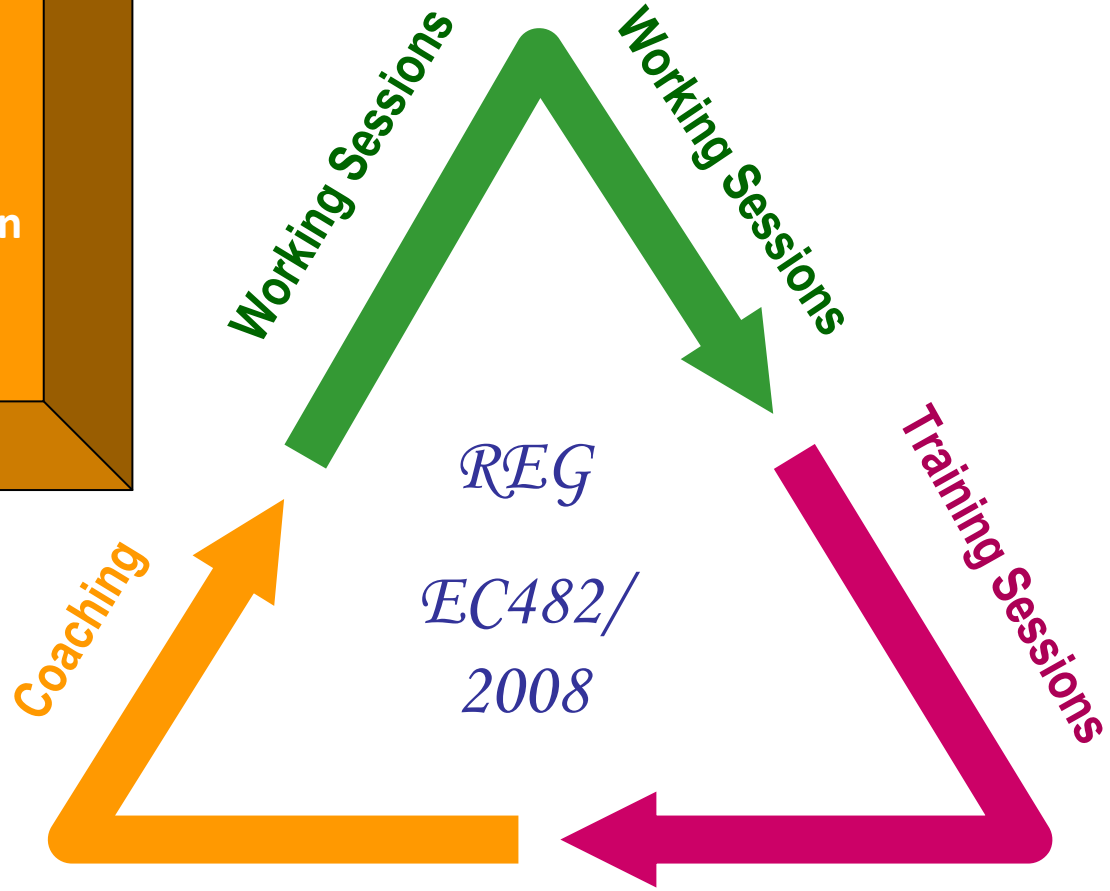


SRS : Software Review Specification
RVP: Review Verification Plan
RPC: Review Preliminary Concept
RDC: Review Detailed Concept
FA: Functional Audit
PA: Physical Audit

Network Manager
nominated by
the European Commission

EUROCONTROL

Not EASY
We have to keep it
as simple as possible
But existing
Documentation & Regulation
Does not HELP



Experience Sharing

To Enhance SMS

frederic.lieutaud@eurocontrol.int