NAV

NAV Portugal, E.P.E.

Software development at NAV Portugal

ES2 WS3-11 Bled/Slovenia 21/22 September 2011
Software Safety Assurance & Degraded Modes of Operations

Paula Santos

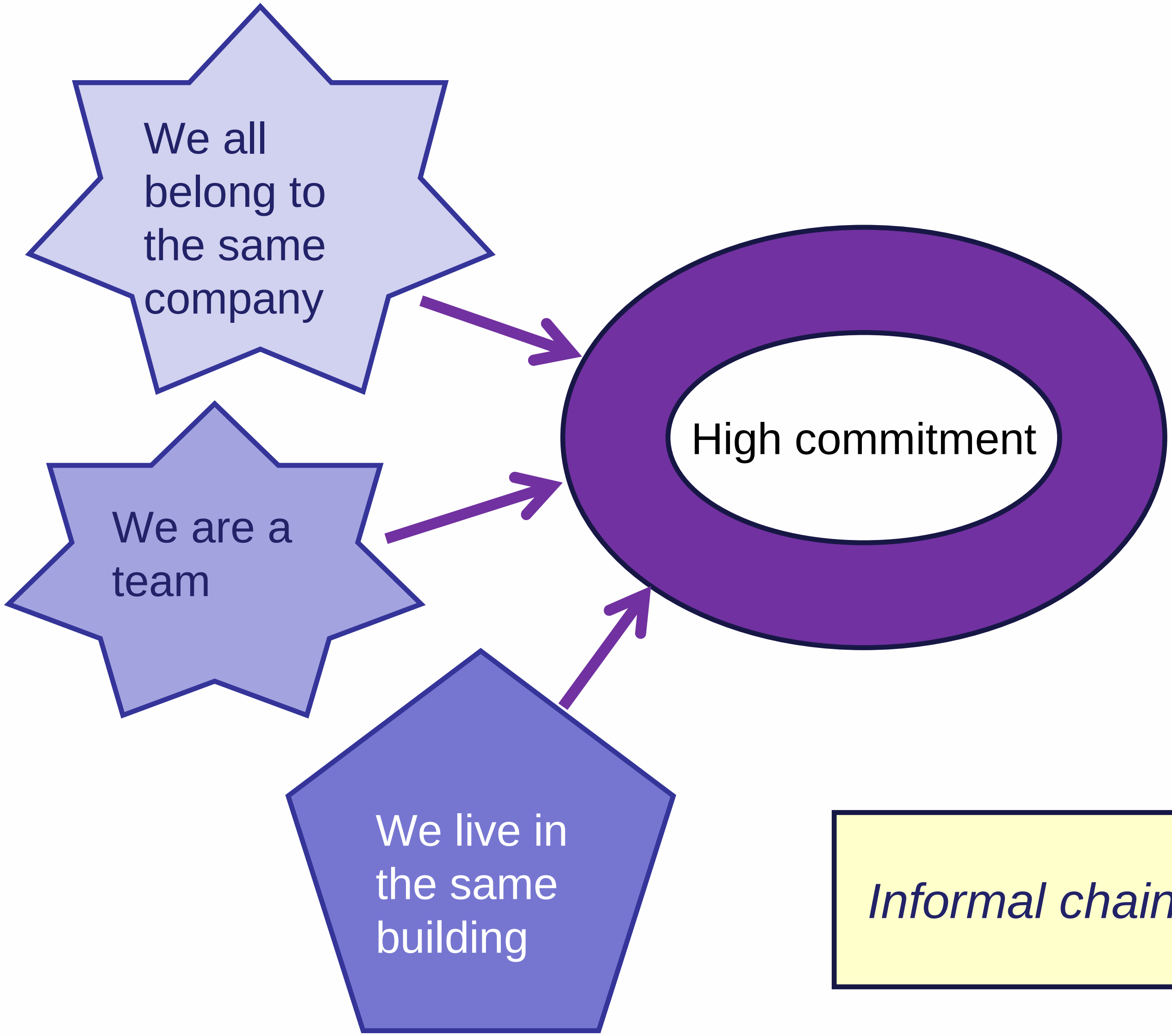
Once upon a time

Agenda

Software development at NAV Portugal

- Pros & Cons of internal developments
- The process
  - Difficulties
  - Achievements
- Regulation

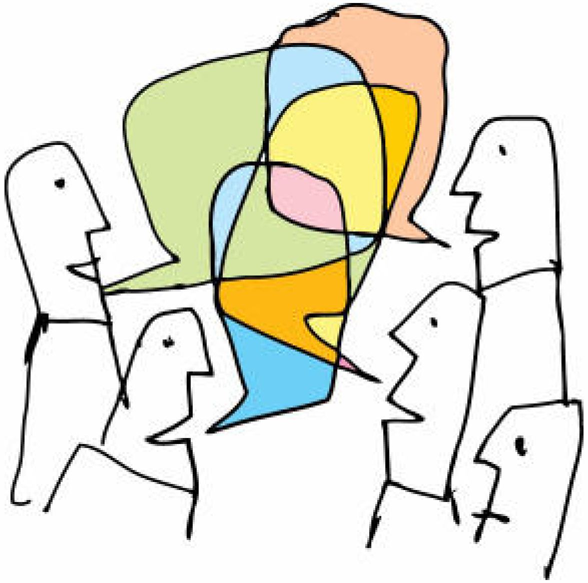
Pros & Cons


We all belong to the same company
We are a team
We live in the same building
High commitment

Informal chains are cherished

Pros & Cons

- Proximity
  - Every day learning
  - Speaking the same dialect
    - Mutual understanding
  - Informal communication channels
    - Earlier knowlege of “news”
    - Explore different approaches
    - Access other lines of thinking
  - Insight knowledge
    - Allows counter proposals
  - Short change chain
    - Product aligned with “dream”



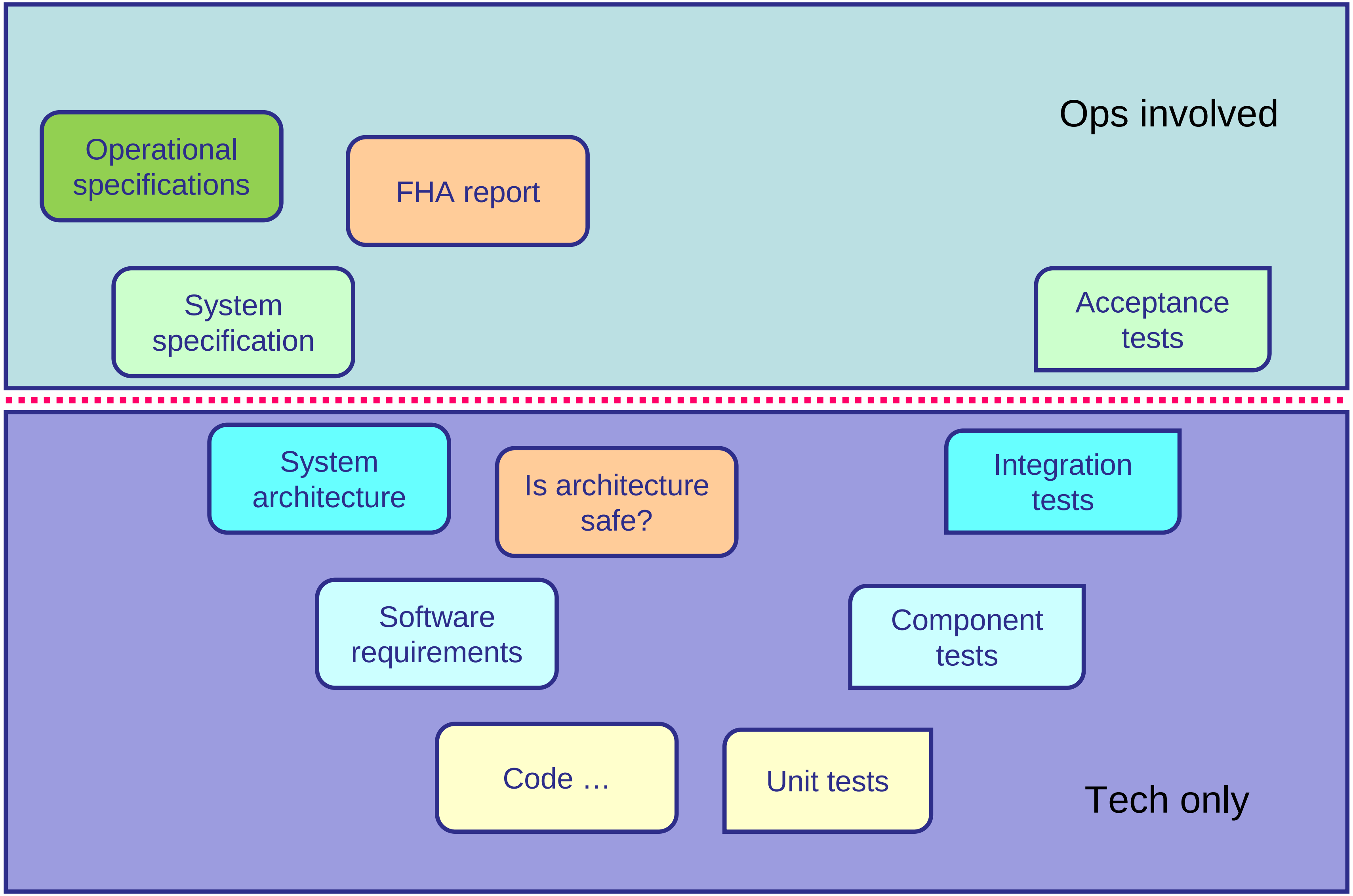
Pros & Cons

fresh & easy™
Neighborhood Market

- Easy changing
  - Too many change requests
  - Immature change requests
  - Request for changes too late (It’s so easy…)

  - Blurred frontiers (Operational / Technical staff)
  - Who takes the lead?
  - Who does what?
  - Project team
    - Availability / in competition with other work

Process



Ops involved

Operational specifications

FHA report

System specification

Acceptance tests

System architecture

Is architecture safe?

Integration tests

Software requirements

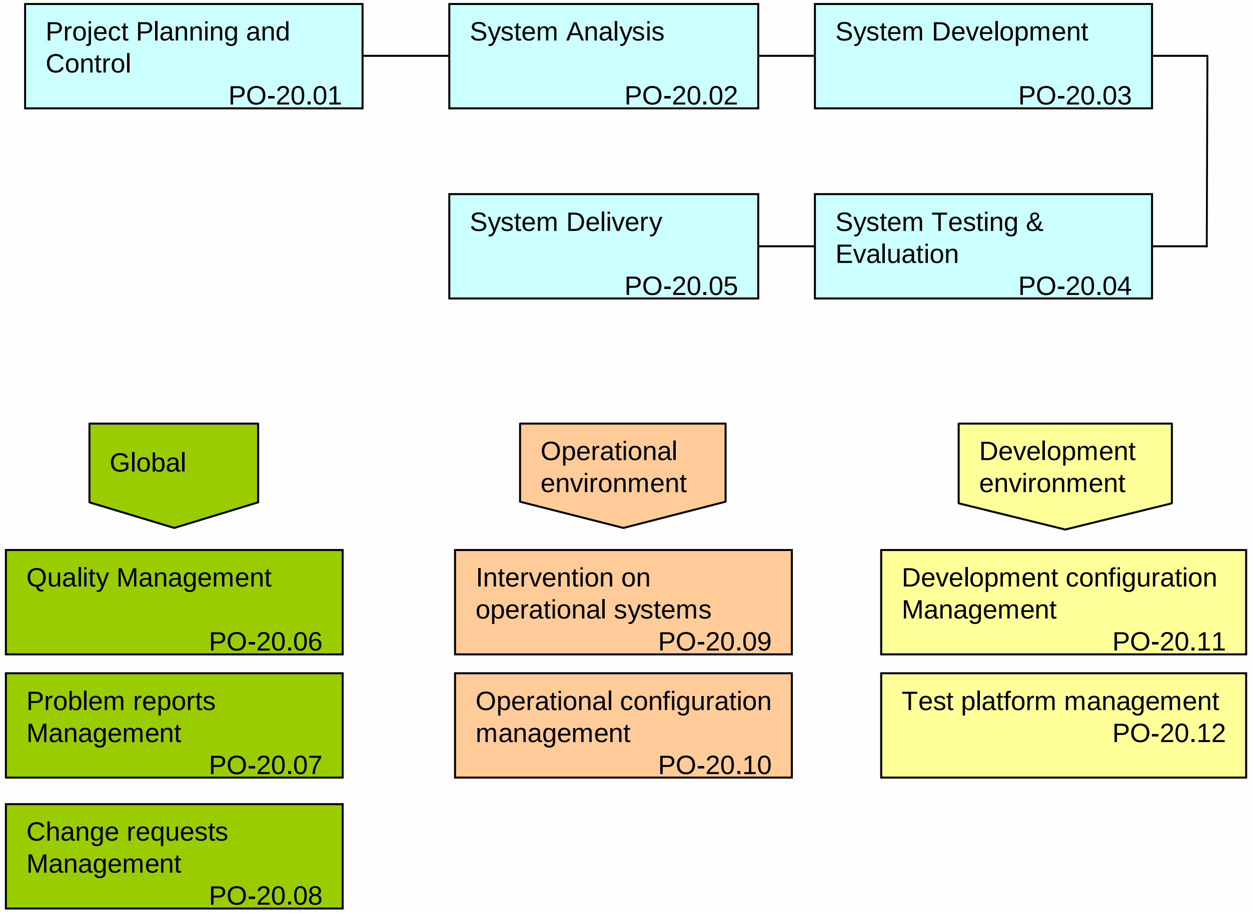
Component tests

Code …

Unit tests

Tech only

The Process



Project Planning and Control PO-20.01

System Analysis PO-20.02

System Development PO-20.03

System Testing & Evaluation PO-20.04

System Delivery PO-20.05

Global

Quality Management PO-20.06

Problem reports Management PO-20.07

Change requests Management PO-20.08

Operational environment

Intervention on operational systems PO-20.09

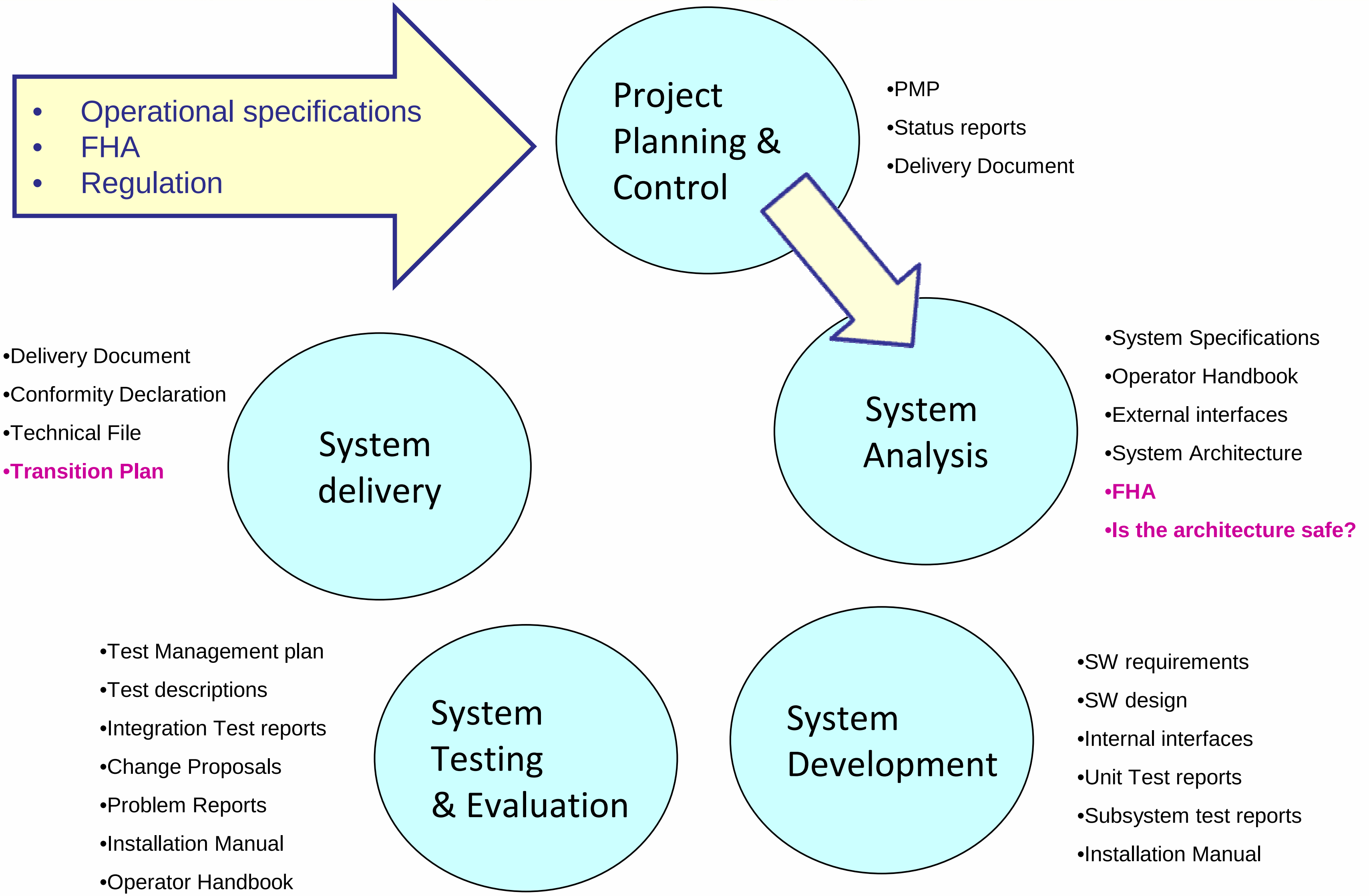
Operational configuration management PO-20.10

Development environment

Development configuration Management PO-20.11

Test platform management PO-20.12

Produced documents



- Operational specifications
- FHA
- Regulation

Project Planning & Control

- PMP
- Status reports
- Delivery Document

System Analysis

- System Specifications
- Operator Handbook
- External interfaces
- System Architecture
- **FHA**
- **Is the architecture safe?**

System Development

- SW requirements
- SW design
- Internal interfaces
- Unit Test reports
- Subsystem test reports
- Installation Manual

System Testing & Evaluation

- Test Management plan
- Test descriptions
- Integration Test reports
- Change Proposals
- Problem Reports
- Installation Manual
- Operator Handbook

System delivery

- Delivery Document
- Conformity Declaration
- Technical File
- **Transition Plan**

Standards -> practice

- What’s in a standard?

IEC 12207_2008: (*Purpose, Outcomes, Activities and tasks)*

“As a result of a successful implementation of System Requirements Analysis:

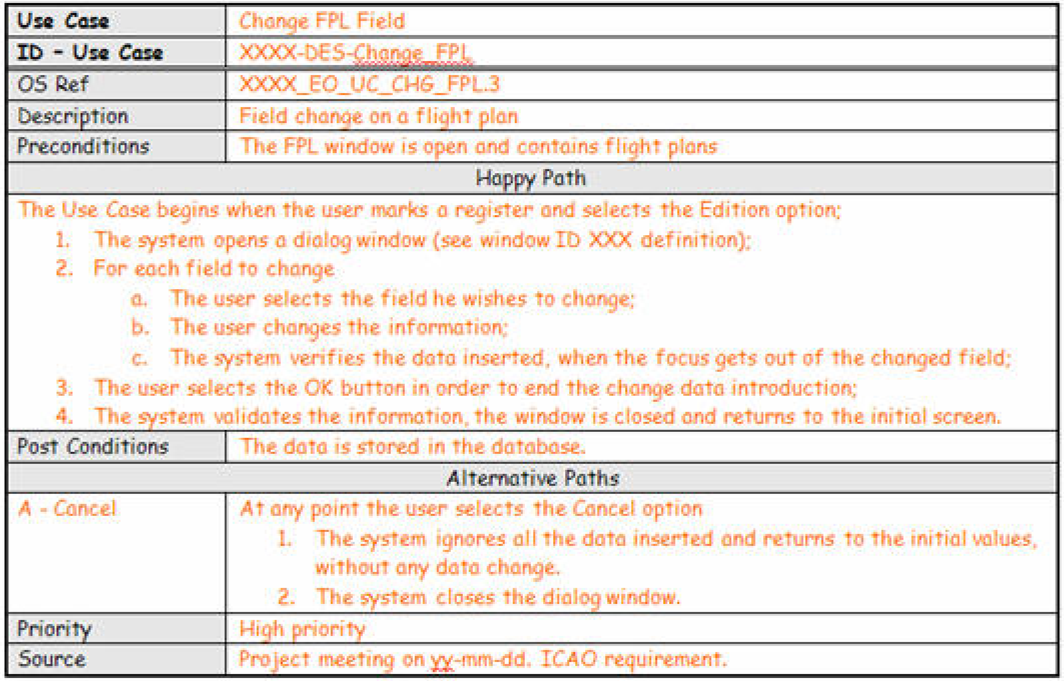
a) A defined set of system functional and non-functional requirements describing the problem to be solved are established

(…)”

- Help, how?
  - Building instructions
  - Examples
  - Reviews

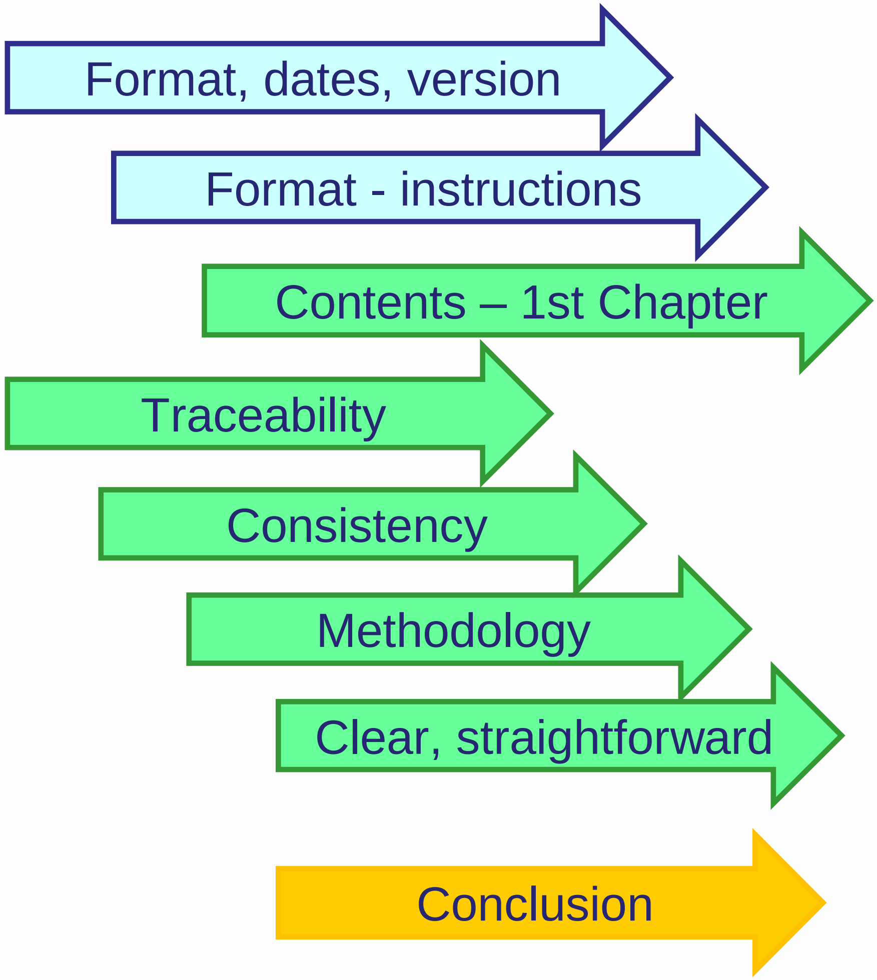
How to - Building instructions

- Use Case (with the Use Case name, unique Use Case identification, reference to the corresponding operational specification)
- Brief Description – brief description of the Use Case meaning
- Preconditions – Previous defined conditions that must satisfy the beginning of the Use Case
- Flow of Events – a section for the basic path and each alternative path
- Post Conditions - list of conditions that must be true when the use case ends successfully
- Priority – choose one of the following alternatives:
  - Not defined
  - Low priority
  - Medium priority
  - High priority
- Source – where the requirement comes from, who asked for it? For example: ICAO document; meeting xxx, stakeholder yyy.



Use Case	Change FPL Field
ID - Use Case	XXXX-DES-Change_FPL
OS Ref	XXXX_EO_UC_CHG_FPL.3
Description	Field change on a flight plan
Preconditions	The FPL window is open and contains flight plans
Happy Path	
The Use Case begins when the user marks a register and selects the Edition option; 1. The system opens a dialog window (see window ID XXX definition); 2. For each field to change a. The user selects the field he wishes to change; b. The user changes the information; c. The system verifies the data inserted, when the focus gets out of the changed field; 3. The user selects the OK button in order to end the change data introduction; 4. The system validates the information, the window is closed and returns to the initial screen.	
Post Conditions	The data is stored in the database.
Alternative Paths	
A - Cancel	At any point the user selects the Cancel option 1. The system ignores all the data inserted and returns to the initial values, without any data change. 2. The system closes the dialog window.
Priority	High priority
Source	Project meeting on yy-mm-dd. ICAO requirement.

Reviews



Format, dates, version

Format - instructions

Contents – 1st Chapter

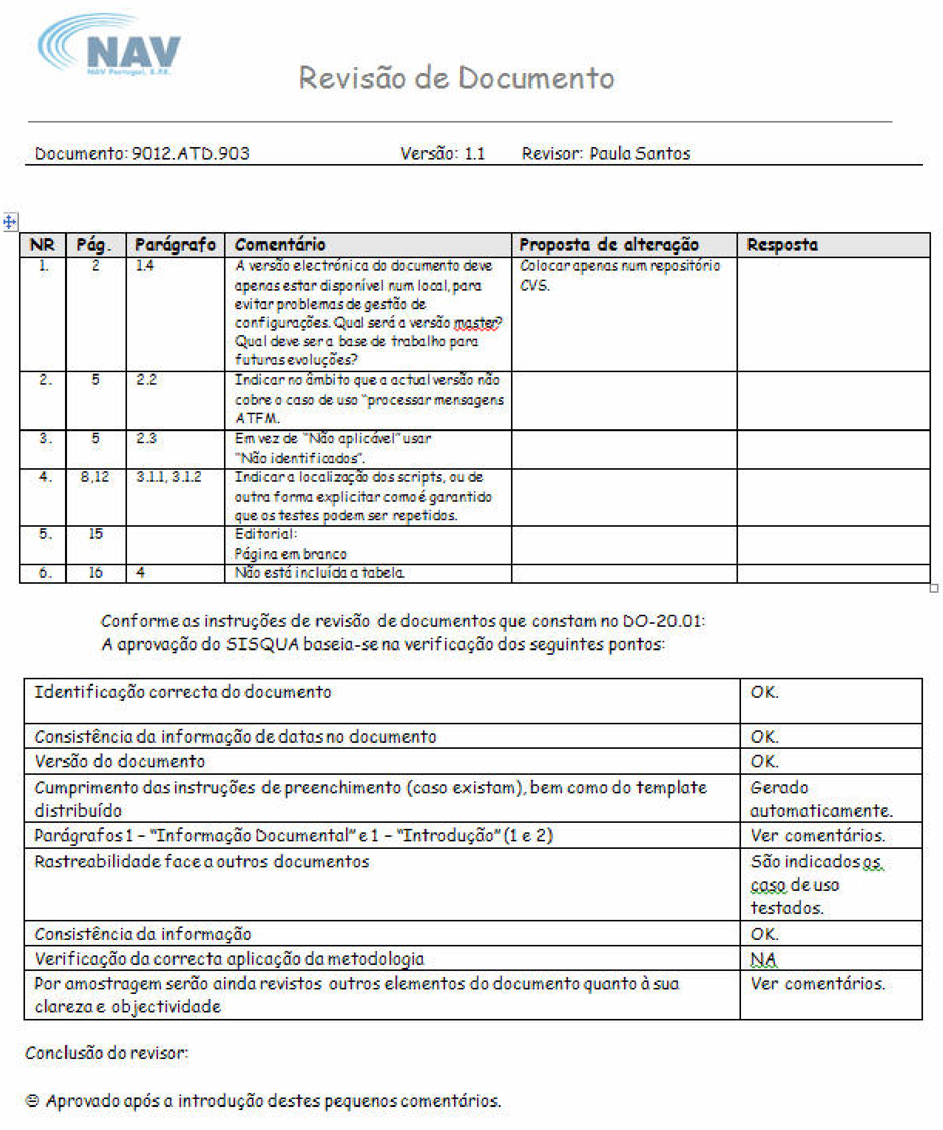
Traceability

Consistency

Methodology

Clear, straightforward

Conclusion



Revisão de Documento

Documento: 9012.ATD.903 Versão: 1.1 Revisor: Paula Santos

NR	Pág.	Parágrafo	Comentário	Proposta de alteração	Resposta
1.	2	1.4	A versão electrónica do documento deve apenas estar disponível num local, para evitar problemas de gestão de configurações. Qual será a versão master? Qual deve ser a base de trabalho para futuras evoluções?	Colocar apenas num repositório CVS.	
2.	5	2.2	Indicar no âmbito que a actual versão não cobre o caso de uso "processar mensagens ATFM.		
3.	5	2.3	Em vez de "Não aplicável" usar "Não identificados".		
4.	8,12	3.1.1, 3.1.2	Indicar a localização dos scripts, ou de outra forma explicitar como é garantido que os testes podem ser repetidos.		
5.	15		Editorial: Página em branco		
6.	16	4	Não está incluída a tabela.		

Conforme as instruções de revisão de documentos que constam no DO-20.01:
A aprovação do SISQUA baseia-se na verificação dos seguintes pontos:

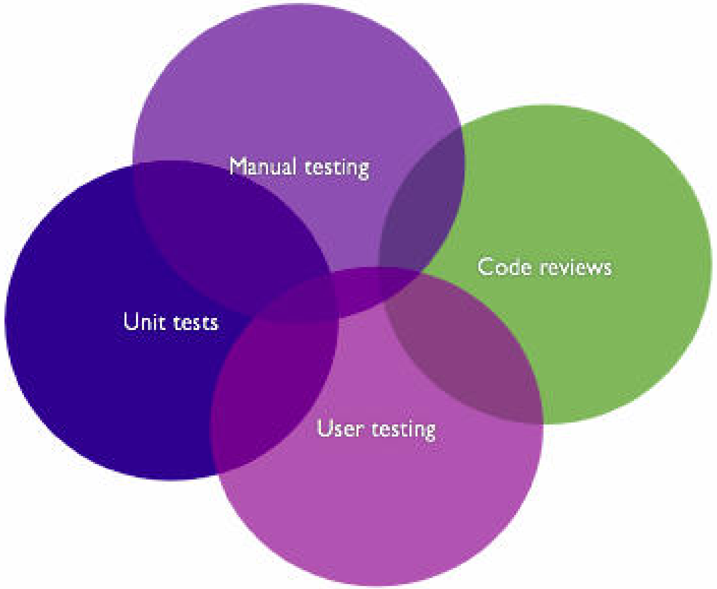
Identificação correcta do documento	OK.
Consistência da informação de datas no documento	OK.
Versão do documento	OK.
Cumprimento das instruções de preenchimento (caso existam), bem como do template distribuído	Gerado automaticamente.
Parágrafos 1 – "Informação Documental" e 1 – "Introdução" (1 e 2)	Ver comentários.
Rastreabilidade face a outros documentos	São indicados os caso de uso testados.
Consistência da informação	OK.
Verificação da correcta aplicação da metodologia	NA
Por amostragem serão ainda revistos outros elementos do documento quanto à sua clareza e objectividade	Ver comentários.

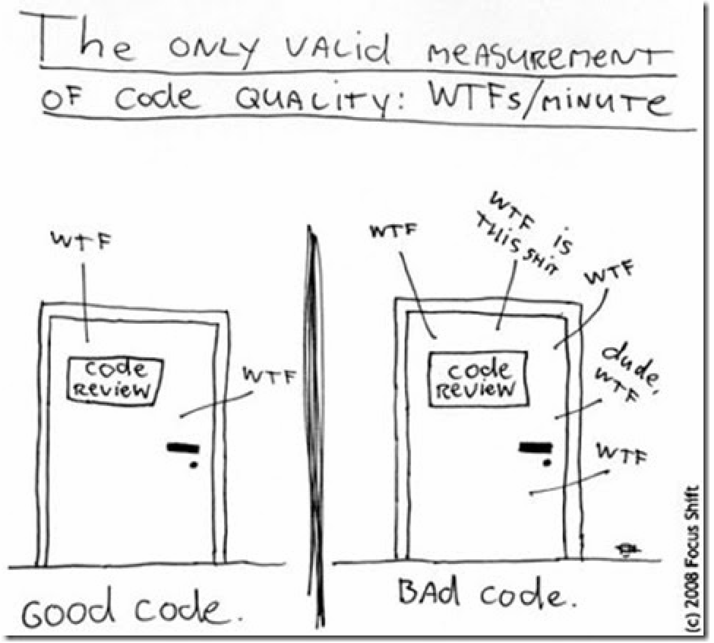
Conclusão do revisor:

☺ Aprovado após a introdução destes pequenos comentários.

Code Reviews / walkthroughs

- Are systematically done
- Are registered (Who, when, …)
- Allow sharing of experience
- Improve product quality





Format vs Contents

- What is the document for?
  - For auditors?
  - To say it's done?
  - To archive?
  - For someone to use?

Doing for the sake of doing them causes frustration and bad documents – crap.

Stakeholders

- What are readers looking for?

I would like to understand how the system works

What SW modules can cause “Radar picture corruption”?

I’m trying to know what the XYZ function does…

Approach

- Planning & Management (PMP, TMP)
- Tests
- Requirements
  - System (High level) - Software
  - Funcional – Non funcional
  - Traceability
- Arquitecture
- Development
- Go back …

The whole team followed the FHA (2004) and SAF-SW (2006) courses

Training

Regulator

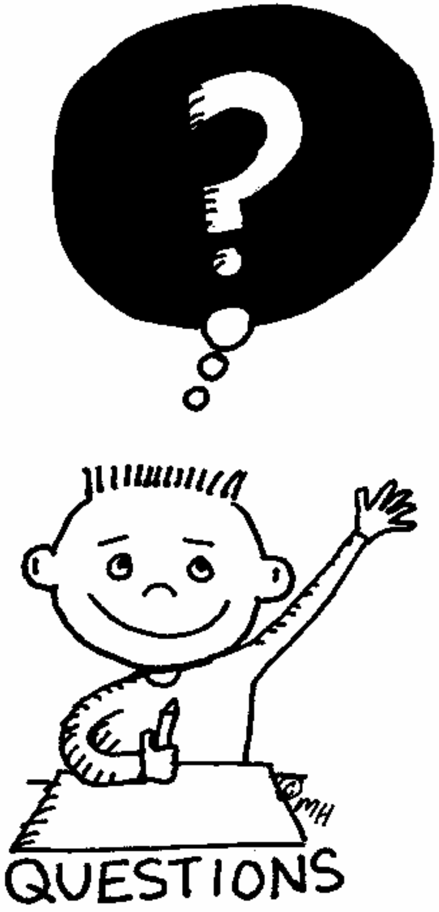
- Regulation cocktail
  - EC 552/2004
    - Declaration of Conformity or suitability for use of constituents
    - Declaration of Verification of Systems
    - Essential requirements – ER3 - Safety
  - EC 2096/2005
    - Annex I, 3 – Safety and Quality Management
    - Annex II, 3 – Safety Management System
  - EC 1315/2007
    - Safety oversight
  - EC 482/2008
    - Software Safety Assurance
  - EC 1070/2009 (amending regulations…)
  - Implementing Rules

Regulator

- Inform all planned changes on operational systems for the year
- Do safety assessment
- Inform about outcome of safety assessment

  (Develop change)
- Before going into operation, send
  - Declaration (DoC of DSU)
  - Declaration of verification of systems
  - Technical file
    - Almost all project documentation
    - Wait for questions

Questions



- How to avoid having “regulator focused documents”, i.e. Documents made just to please the regulator?

- How can one give a satisfactory answer to all the regulation requirements using:
    - The results of the safety analysis integrated with
    - The outputs of a good software engineering practice