A Practical Implementation of
EC 482/2008 in the context of an ANSP

Etienne Paquay
Patrick Gilles
Revision Identification : 1.0
Revision date : 2013-05-03
January 2013
- Plan of the presentation
  1. Introduction
  2. How to consider Software in the context of an ANSP?
  3. ANSP Structure
  4. Understanding Regulation EC482/2008 in a real world context
  5. The real implementation
  6. Software categories within an ANSP
  7. Software Lifecycle
  8. Relationship with the Regulator
  9. Opened Questions
  10. Any Questions?
Introduction

- The aim of this presentation is to:
  - Demistify Software
  - Consider it at the right place in the equipment
  - Take Care of it with the adequate consideration

- We will consider in the context of our ANSP, BELGOCONTROL:
  - The technical approach
  - The safety approach
  - How to match those complementary approaches
Remember!

- Plan of the presentation

1. Introduction
2. How to consider Software in the context of an ANSP?
3. ANSP Structure
4. Understanding Regulation EC482/2008 in a real world context
5. The real implementation
6. Software categories within an ANSP
7. Software Lifecycle
8. Relationship with the Regulator
9. Opened Questions
10. Any Questions?
How to consider Software in an ANSP?

- Technical approach
How to consider Software in an ANSP?

- Technical approach
  - Software is an intangible part of the equipment.
  - Software is not really measurable, quantifiable but its contribution to the behaviour of the equipment is.
  - Software is a Versatile way to change the behaviour of the equipment.
  - Versatility is:
    - A strenght.
    - A huge weakness.
  - Engineering defines working methods to cope with the versatility in order to achieve:
    - Goals to be fullfilled by the software.
    - Reduce as much as possible unwanted behaviour.

⚠️ Technical approach often neglects functional approach
How to consider Software in an ANSP?

- Safety approach
How to consider Software in an ANSP?

- Safety approach
  - Software is an equipment constituent contributing in the realization of functions within a context
  - Due to its nature, software reproduces exactly the same behaviour in the same circumstances. Software is causal: When it fails to fulfill a function for a specific reason, it is always in the same way.
  - Software is a versatile way to change the behaviour of an equipment. To avoid this to become a weakness, any change must be done in a controlled way

- How to have the assurance of a controlled production of software?
  - Via a quality process with measurable assurance level
Remember!

- Plan of the presentation
  1. Introduction
  2. How to consider Software in the context of an ANSP?
  3. ANSP Structure
  4. Understanding Regulation EC482/2008 in a real world context
  5. The real implementation
  6. Software categories within an ANSP
  7. Software Lifecycle
  8. Relationship with the Regulator
  9. Opened Questions
  10. Any Questions?
Remember!

- Plan of the presentation
  1. Introduction
  2. How to consider Software in the context of an ANSP?
  3. ANSP Structure
  4. Understanding Regulation EC482/2008 in a real world context
  5. The real implementation
  6. Software categories within an ANSP
  7. Software Lifecycle
  8. Relationship with the Regulator
  9. Opened Questions
  11. Any Questions?
Understanding Regulation EC-482/2008 in a real world context

- Is an extension of EC1035/2011 (System approach)
- Software Safety Assurance System is a part of System Safety Assurance
- Whatever the change, an ANSP is required to implement a risk assessment and mitigation process (EC 1035/2011)
- EC 482/2008 describes what is required for software specific aspects of the changes. It has to be seen as some kind of pluggin to the safety assurance system
- By change, we understand corrections, modifications and projects
Understanding Regulation EC-482/2008 in a real world context

- Regulation requires:
  . To establish a software safety assurance system
  . To allocate adequate SWAL for a change
  . To produce evidence for supporting arguments
  . Requirement correctness, satisfaction and traceability
  . To know your software version (documentation included) => Configuration management + documentation process
  . To manage the risks linked to unintended functions => it does not mean they should not exist, but at least controlled
  . Any change shall be notified to the NSA
Remember!

- Plan of the presentation
  1. Introduction
  2. How to consider Software in the context of an ANSP?
  3. ANSP Structure
  4. Understanding Regulation EC482/2008 in a real world context
  5. The real implementation
  6. Software categories within an ANSP
  7. Software Lifecycle
  8. Relationship with the Regulator
  9. Opened Questions
  11. Any Questions?
The real implementation

- Working Rules
  - SSAS
  - QA
  - Process

- My SW 1.00
- My SW 1.01
- My SW 1.02

- Concept
- Specifications
- Requirements
- User Input

- Problem Reports
- Change Reports

ZZZZZZ !!! Alone, I am nothing !!!
No Input !
I am switched on but I can do nothing !!!

With loaded software, I am now working and can produce effects !!!

The real implementation
The real implementation – Software Production Environment
The real implementation

- Your Software Safety Assurance System shall be realistic to be effective! Otherwise, people will not use it.

- Your Software Safety Assurance System includes nearly all layers of the ANSP

- Some of the needed processes already exist and are recurrent in change management (e.g. acquisition...), Do not re-invent the wheel!

- Software Safety Assurance has a cost that might have a heavy weight in management decision... Do not neglect it!

- Software Safety Assurance activities will not stop at the end of the change/project. Do not forget to identify maintenance activities in the long term budget planning
The real implementation

- Corporate Process

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIMS-33.5 Processes et Support</td>
<td>BIMS Belgocontrol Imaginary Management System</td>
</tr>
<tr>
<td>BIMS-21.2 Processus Dirigente</td>
<td>BIMS-33.5 Decon de la securite et de la qualite</td>
</tr>
<tr>
<td>BIMS-33.1 Processus Operationnels</td>
<td>BIMS-33.1 Compte rendu, evaluation et correction</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIMS-33.5 Processes et Support</td>
<td>BIMS Belgocontrol Imaginary Management System</td>
</tr>
<tr>
<td>BIMS-21.2 Processus Dirigente</td>
<td>BIMS-33.5 Decon de la securite et de la qualite</td>
</tr>
<tr>
<td>BIMS-33.1 Processus Operationnels</td>
<td>BIMS-33.1 Compte rendu, evaluation et correction</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIMS-33.5 Processes et Support</td>
<td>BIMS Belgocontrol Imaginary Management System</td>
</tr>
<tr>
<td>BIMS-21.2 Processus Dirigente</td>
<td>BIMS-33.5 Decon de la securite et de la qualite</td>
</tr>
<tr>
<td>BIMS-33.1 Processus Operationnels</td>
<td>BIMS-33.1 Compte rendu, evaluation et correction</td>
</tr>
</tbody>
</table>
The real implementation: What the SWAL means

A Software Assurance Level

- **SWAL 4**
- **SWAL 3**
- **SWAL 2**
- **SWAL 1**

To mitigate:

- Software functional error
- Design / low level functional error
- Credible corruption until implementation (Source code level)
- Credible corruption until implementation (Executable code level)
The real implementation

- Focus on results
  . Aim of a software is not being safe, it is to fulfill operational goal
  . Regulation shall be a safeguard in software practices
- Assign a realistic and maintainable SWAL
The real implementation

- Maintaining the SWAL as part of the maintainance process
  - SWAL Verification (is it still valid since the last change)
  - Change Management
  - Version and Configuration Management
- Gather and produce evidences as outcomes of your processes
  - SWAL Compliance Matrix
  - Change / Project documentation
- **Software Safety Assurance shall be part of your activities...**
The real implementation

- **Ju_0_1**  
  Change or Project Justification

- **Ct_0_1**  
  The System (and its software constituant) shall be used only in its defined context

- **Arg_0**  
  The Operational Use of the System (including its software constituant) is acceptably safe

- **Co_0_1**  
  System Concept of Operation

- **Cr_0_1**  
  Corporate, achievable Safety level

- **St_0**  
  The necessary Safety Assurance is obtained by demonstrating the acceptibility of the risk associated to each stage of the project / change: Definition, Design, Implementation, Transfer in Operations and Operations. All activities being supported by a quality process

- **Co_0_2**  
  The demonstration is supported by a set of safety activities and corresponding evidences of results performed for each stage to satisfy Cr_0_1

- **Arg_1**  
  The System Definition (including its software constituant) is acceptably safe

- **Arg_2**  
  The System Design (including its software constituant) is acceptably safe

- **Arg_3**  
  The System Implementation (including its software constituant) is acceptably safe

- **Arg_4**  
  The System Transfer into Operation (including its software constituant) is acceptably safe

- **Arg_5**  
  The System Operation (including its software constituant) is acceptably safe

- **Arg_6**  
  Quality process is followed
Remember!

- Plan of the presentation

1. Introduction
2. How to consider Software in the context of an ANSP?
3. ANSP Structure
4. Understanding Regulation EC482/2008 in a real world context
5. The real implementation
6. Software categories within an ANSP
7. Software Lifecycle
8. Relationship with the Regulator
9. Opened Questions
10. Any Questions?
Software Categories within an ANSP

- Bespoke Software
  - In-House
  - Sub-Contracted

The difference is not important. How you will be able to maintain it is the question. What can I afford?

- COTS
  - OS, specific libs, etc...

- Unless the provider can help you to fill in your SWAL Compliance Matrix, it is a black box. Take care to the context of use (unintended functions)

- Legacy

  - Level of documentation can be low or high but rarely what is required to comply with regulation
  - Case by case solution to be found
  - Raise the question: re-engineer or replace?

In any case, SWAL 4 is the minimal level to implement. Think your Software in its context (as part of a system) to allocate the SWAL
Remember!

- Plan of the presentation
  1. Introduction
  2. How to consider Software in the context of an ANSP ?
  3. ANSP Structure
  4. Understanding Regulation EC482/2008 in a real world context
  5. The real implementation
  6. Software categories within an ANSP
  7. Software Lifecycle
  8. Relationship with the Regulator
  9. Opened Questions
  10. Any Questions  ?
Software Lifecycle
Software Lifecycle

Software safety Assurance Level

Primary Lifecycle Processes
- Acquisition Process
- Supply Process
- Development Process
  - Operation Process
  - Maintenance Process

Supporting Lifecycle Processes
- Documentation Process
- Configuration Management Process
- Quality Assurance Process
- Verification Process
- Validation Process
- Joint Review Process
- Audit Process
- Problem / Change Resolution Process

Organizational Lifecycle Processes
- Management Process
- Improvement Process
- Infrastructure Process
- Training Process

Software Safety Assurance System Overall Objectives
- Software Requirement Specification
- Software Safety Assessment Initiation
- Software Safety Assessment Planning
- Software Safety Assessment Validation, Verification and Process Assurance
- Software Safety Assessment Completion

Software Safety Assurance System Overall Objectives

Software Requirement Specification

Software Safety Assessment Initiation

Software Safety Assessment Planning

Software Safety Assessment Validation, Verification and Process Assurance

Software Safety Assessment Completion

Primary Lifecycle Processes

Supporting Lifecycle Processes

Organizational Lifecycle Processes
Remember!

- Plan of the presentation
  1. Introduction
  2. How to consider Software in the context of an ANSP?
  3. ANSP Structure
  4. Understanding Regulation EC482/2008 in a real world context
  5. The real implementation
  6. Software categories within an ANSP
  7. Software Lifecycle
  8. Relationship with the Regulator
  9. Opened Questions
  10. Any Questions?
Relationship with the regulator

The Software Safety Assurance System is a specialization of the Safety Assurance System

- Define your Software policy within a manual => it allows to communicate in the ANSP and with the regulator

- For each change / project when notification is applicable, start with early notification
- Plan of the presentation

  1. Introduction
  2. How to consider Software in the context of an ANSP ?
  3. ANSP Structure
  4. Understanding Regulation EC482/2008 in a real world context
  5. The real implementation
  6. Software categories within an ANSP
  7. Software Lifecycle
  8. Relationship with the Regulator
  9. Opened Questions
  10. Any Questions ?
Opened Questions

- To find a practical solution to make the link between safety related occurrences and software
- What to require from external suppliers (a study is in progress with NLR)?
- What to do with legacy systems?... Update to comply with the regulation or replace?
- What about equipments with embedded software?... How to apply the regulation?
Any questions?