DSNA policy on software aspects

Yann Carlier
DSNA/MSQS/SDS
Safety Management Unit
Presentation outlines

DSNA compliance with software regulation

DSNA SSAS

- Scope of application
- Software confidence level definition (SWAL, Current, Upgraded) and allocation process
- Software confidence level satisfaction process
- SSAS monitoring process

DSNA Hot spots

- COTS,
- How to justify that software functions do not adversely affect safety?
- Legacy software
- Current flawed architectures (ARTAS…)
- Forthcoming network with routers…
DSNA compliance with CE n°482/2008
SSAS methodology (May 2009)

Transposition of CE n°482 into an internal methodology → MET006, applicable from May 2009.

SSAS definition so as to provide assurances regarding:

- Validity of software requirements (all of them)
- Verification of software requirements
- Traceability,
- Software configuration management
- No adverse safety effect from a software functionality

Difficulty: No AMC available, nor envisioned for this regulation.

At that time, no ED153, nor CS SWAL published.

DSNA choice: to rely on ED109 and current practices in addition to complementary assurances to address maintenance, installation, and operation phases.

However confidence levels for legacy software not defined!

Significant pressure from the NSA on software aspects.
August 2011: release of a guidance to improve the SSAS application. Dedicated to project/safety practitioners with key enablers:

- to which type of software the software regulation applies
- leaflet to address the: organisation of the activities/evidences for the required assurances (who, what and how)
- COTS treatment policy,
- legacy software confidence level definition
- translation of ED109 into French to avoid English misunderstanding and jump into ED12B.
DSNA SSAS: generalities

Scope of application

Software confidence level allocation process
- new software
- legacy software

Software confidence level satisfaction process
- Validity of software requirements (all of them)
- Verification of software requirements
- Traceability,
- Software configuration management
- No adverse software safety effect

SSAS Monitoring (in progress)
- ensure that the confidence level is appropriately allocated
- ensure the satisfaction of the confidence level is adequate
- modify the SSAS accordingly (new measures, corrective actions to avoid deficiencies in applying the directives)
DSNA SSAS : scope of application

- SSAS applies to any software creation/modification as part of the ATM/CNS system
  - Software definition (EC482) = sw version + config data
  - corrective maintenance bug fixing,
  - software new functionalities,
  - local development (e.g. intrusive or passive supervision),
  - configuration data modification,
  - Command script in Unix to launch equipment, reload, reset
  - etc…
- but limited to software that are safety-related.
  - No bureautics software involved…

SSAS applies not necessarily in the frame of CE n°2096 change.
DSNA SSAS : scope of application

DSNA Strategy: to avoid triggering a safety process that could result with no software assurance required: so a change impact analysis is performed.

Criterion to seek safety-related software: 2 rules (not mutually exclusive) have been defined

- Rule 1:

  Any software connected to the operational network. Yet, when a change impact analysis shows that any failure mode of the software under study has no safety impact, no software assurance is required for the software (e.g. non-intrusive spying or data extracting software for the purpose of statistics).

- Rule 2:

  Any software off operational network whose output are consumed by the ATM/CNS system (Human, Equipment, Procedure). However, if a change impact analysis shows that software outputs are valid and verified before operational consumption, therefore no software assurance is required. (e.g: adaptation data configurator whose output are verified before equipment usage, planning resources software whose output are humanly verified before distribution, EFB-like software for maintenance staff).

Of course, where software modification is part of the ATM/CNS system functional envelope, no additional assurance is required. E.g Instanciation of adaptation data already covered by a safety study will be accomplished by ensuring adherence to this latter.
Software Confidence level
Determination
2 methods for the SWAL
1 method for legacy software
Paramount question: on which part of the software is the allocation performed?

- On the overall software (drivers, middleware, applicative, ...) that runs on a hardware platform (microprocessor).

- On the software component level for those components running on a microcontroller, where isolation can be substantiated between them (e.g. by the use of partitioning techniques to ensure spatial and temporal segregation).
Why isolation is needed to allocate at component level?

Quid when App2 exceeds its time frame or spatial allocation quantum; can App1 execute correctly? Isolation techniques are therefore required to allocate different SWAL.
SWAL determination : general method (ED153)

General Principle:
For all HAZ in which the SW is involved, apply step 1 to 3 here-after. The final SWAL is the most stringent one.

1) Contribution identification:
In the WCC, assess the distance from the SW failure to the effect. 4 choices: Very Possible, Possible, Improbable and Extremely Improbable.

2) Contribution justification:
Very Possible: when no efficient & independent MM (external to the SW failure) exists
Possible: when exists a set of MM (external to the SW failure) that is efficient and independent.
Improbable: when exists a set of MM (external to the SW failure) that is very efficient and independent.
Extremely Improbable: when exists a set of MM (external to the SW failure) that is extremely efficient and independent.

3) SWAL allocation:
Determination based on the combination effect severity class and SW failure contribution to the effect, as shown in the here-below matrix:

<table>
<thead>
<tr>
<th>Degre de gravite de l'effet</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contribution à l'effet</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Très Possible</td>
<td>SWAL 1</td>
<td>SWAL 2</td>
<td>SWAL 3</td>
<td>SWAL 4</td>
</tr>
<tr>
<td>Possible</td>
<td>SWAL 2</td>
<td>SWAL 3</td>
<td>SWAL 3</td>
<td>SWAL 4</td>
</tr>
<tr>
<td>Improbable</td>
<td>SWAL 3</td>
<td>SWAL 3</td>
<td>SWAL 4</td>
<td>SWAL 4</td>
</tr>
<tr>
<td>Extrêmement Improbable</td>
<td>SWAL 4</td>
<td>SWAL 4</td>
<td>SWAL 4</td>
<td>SWAL 4</td>
</tr>
</tbody>
</table>
SWAL determination : DSNA alternate method

1) Contribution identification :
In the WCC, assess the distance from the SW failure to the HAZ by exploiting the fault trees. 3 choices : Direct, Simple Combination, Multiple Combination.

2) Contribution justification :
Direct : when no efficient & independent MM (external to the SW failure) exists.
Simple Combination : when exists a MM (external to the SW failure) that is efficient and independent.
Multiple Combination : when exists a set of MM (external to the SW failure) that is very efficient and independent.

3) SWAL allocation :
Determination based on the severity level of the HAZ and SW failure contribution to the HAZ, as shown in the here-below matrix.

<table>
<thead>
<tr>
<th>Niveau de gravité corrigé de l'ER</th>
<th>Contribution à l'ER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Directe</td>
<td>SWAL1</td>
</tr>
<tr>
<td>Combinaison simple</td>
<td>SWAL2</td>
</tr>
<tr>
<td>Combinaison multiple</td>
<td>SWAL3</td>
</tr>
</tbody>
</table>
Example of SWAL allocation

DSNA Risk acceptability matrix

1.10^{-5}/oh

HAZ_1 Gc 2
Erroneous clearance of zone activity for the pilot (Not detected)

OR

Correct display of zone activity

Incorrect display of zone activity

Human error: Incorrect Clearance not recovered

Improbable

Erroenous activity of zones not detected by ATCO

1.10^{-6}/oh 10-90% distribution
Severity 2

1.10^{-5}/oh
(DSNA choice to have 2 equipment)
Severity 3

1.10^{-5}/oh
SWAL3
Confidence level determination: legacy software

<table>
<thead>
<tr>
<th>Nature of SW Modification</th>
<th>Minor</th>
<th>Major</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criticality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Current</td>
<td>Current</td>
</tr>
<tr>
<td>High</td>
<td>Current</td>
<td>Upgraded</td>
</tr>
<tr>
<td>From low to high</td>
<td>Upgraded</td>
<td>Upgraded</td>
</tr>
</tbody>
</table>

1) Software Criticality

The criticality is estimated after the SW change.

The criticality is **LOW** when a SW failure:
- causes or contributes to a HAZ whose severity level is 4 or 5,
- contributes indirectly to a HAZ whose severity is 3 as it exists a set of MM external to the SW failure that is efficient and independent.
- contribute indirectly to a HAZ whose severity is 2 as it exists a set of MM external to the SW failure that is very efficient and independent.
- contribute indirectly to a HAZ whose severity is 1 as it exists a set of MM external to the SW failure that is extremely efficient and independent.

Otherwise, the criticality is **HIGH**.

2) Nature of software modification

A software modification is said **MAJOR** in either following case:
- internal SW architecture is significantly affected or,
- dynamic behaviour of the SW functionality is significantly affected or,
- the number of software functionalities is significantly increased.

A software modification is said **MINOR** otherwise.
Confidence level satisfaction
Activities along the V cycle
Guide Leaflet
Confidence level satisfaction leaflet structure
Definition of activities and expected evidence along the V cycle for each confidence level
- work sharing (site, supplier…)
Confidence level satisfaction leaflet

Annex 1
Software life cycle data (ED12B)

COTS considerations (ED109)

Annex 2
Software verification (ED12B)
### Software confidence level Satisfaction:

- Either the COTS providers artifacts are sufficient (when completed with necessary assurances for operations)
- Or when insufficient it is compensated by:
  - Reverse-engineering or
  - In service experience.

<table>
<thead>
<tr>
<th>Required software Confidence level</th>
<th>In service experience with management of deficiencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgraded</td>
<td>1 year without safety failure</td>
</tr>
<tr>
<td>SWAL 2</td>
<td>1 year without safety failure</td>
</tr>
<tr>
<td>SWAL 3</td>
<td>6 months without safety failure</td>
</tr>
<tr>
<td>SWAL 4 or Current</td>
<td>No in service experience required</td>
</tr>
</tbody>
</table>

#### Equivalence Confidence level/In service experience

- **Required software Confidence level**
  - **Upgraded**: 1 year without safety failure
  - **SWAL 2**: 1 year without safety failure
  - **SWAL 3**: 6 months without safety failure
  - **SWAL 4 or Current**: No in service experience required

- **In service experience with management of deficiencies**
  - **Upgraded**: 1 year without safety failure
  - **SWAL 2**: 1 year without safety failure
  - **SWAL 3**: 6 months without safety failure
  - **SWAL 4 or Current**: No in service experience required

---

**Assurances SWAL 3**

- A-1.2 Définition des critères de transition et de l’articulation entre les phases de réalisation (spécifications, codage, vérification)
- A-1.3 Définition des méthodes et outils du cycle de vie du logiciel
- A-1.5 Définition de règles de réalisation (conception et codage)
- A-1.6, A-1.7 Les plans logiciels sont coordonnés et conformes (revue de planification)

- **Assurances SWAL 4 or Current**
  - A-7.1, A-7.2 Vérifier que les procédures ainsi que les résultats de test sont corrects (y compris les procédures de test d’intégration)
  - A-5.7 S’assurer que les résultats du processus d’intégration sont complets et corrects (revue d’intégration)

### Software Assurance Levels (SWAL)

- **SWAL 2**: 1 year without safety failure
- **SWAL 3**: 6 months without safety failure
- **SWAL 4 or Current**: No in service experience required

---

**Formalisation dans l’étude de sécurité des assurances obtenues**

- plan de réalisation logicielle, plan de vérification logicielle, plan de gestion de configuration logicielle, plan d’assurance qualité logicielle, plan de sécurité logicielle
- dossier de spécifications logicielles, dossier de conception (architecture logicielle), code objet exécutable
- dossier de vérification : tests de validation et d’intégration du logiciel (plage de variations prévues et robustesse)
- résultats de vérification:
  - rapport de revue de planification
  - rapport de revues et analyses des spécifications logicielles incluant:
    - la traçabilité entre les spécifications logicielles et le besoin opérationnel
    - la conformité des spécifications logicielles aux règles de spécification
    - l’analyse des exigences dérivées
    - la justification de l’absence de fonction nuisible à la sécurité
  - rapport de revues et analyses de l’architecture du logiciel incluant:
    - la compatibilité avec la machine cible
    - la conformité de l’architecture logicielle aux règles de conception
  - rapport de revues et analyses des jeux et procédures de test incluant:
    - la traçabilité entre les tests de validation et les spécifications logicielles
    - la traçabilité entre les tests d’intégration et les spécifications de l’architecture logicielle
    - l’adéquation à la méthode de test d’intégration matérielle/logiciel
    - l’adéquation à la méthode de test d’intégration du logiciel
  - rapport de revues et analyses des tests d’intégration et de validation incluant:
    - revue et analyse des résultats de tests
    - analyse de couverture des tests
    - rapport des anomalies résiduelles
    - dossier de mise en œuvre du logiciel
    - bilan de sécurité logicielle (BSL) et répertoire de configuration du logiciel (RCL)
    - documents de gestion de configuration logicielle, documents d’assurance qualité logiciel

---

**Direction générale de l’Aviation civile**

**Direction des services de la Navigation aérienne**

**Guide METLOG : COTS Aspects (ED109)**
Whatever COTS that is introduced into an ATM/CNS software, a minima, the following assurances are provided:

- Validity of COTS sw specifications
- Verification of COTS sw specifications
- Introduction of COTS does not adversely affect safety
- Configuration management

At COTS level, additional level of reverse-engineering or EXP to be achieved for a given ATM/CNS software is indicated below

<table>
<thead>
<tr>
<th>Type of Introduced SW COTS</th>
<th>Upgraded</th>
<th>SWAL3</th>
<th>SWAL2</th>
</tr>
</thead>
<tbody>
<tr>
<td>COTS software library</td>
<td></td>
<td>(validity and verification of requirements of library with SC and code review) Or EXP 1 year</td>
<td>(validity and verification of preliminary and detailed design requirements, SC and code review) or EXP 1 year</td>
</tr>
<tr>
<td>Software components COTS (module, firmware, driver, OS, etc)</td>
<td></td>
<td>(validity and verification of preliminary and detailed design requirements, SC and code review) or EXP 1 year</td>
<td>(validity and verification of preliminary and detailed design requirements, SC and code review) or EXP 1 year</td>
</tr>
<tr>
<td>Applicative software COTS</td>
<td>(validity and verification of preliminary design) Or EXP 1 year</td>
<td>validity and verification of preliminary design Or EXP 6 months</td>
<td>(validity and verification of preliminary and detailed design requirements, SC and code review) or EXP 1 year</td>
</tr>
</tbody>
</table>

EXP : in service experience with no safety issue for a given software version
SC : structural coverage
Software COTS acquisition

Vade-mecum at contract level

• Specify to the provider the required software assurances for DSNA.

• When the confidence level is not determined at the date of the contract signature (as dependent on the retained architectural solution)
  • Indicate to the provider the confidence level allocation and satisfaction DSNA processes

• Possible DSNA software audits on site with respect to the software criticality.
DSNA software Hot spots

Legacy software treatment:

- Limited current architectures show that some legacy software are directly contributing to SC2 HAZ and therefore would be SWAL2 now if redeveloped.
- The NSA is very demanding on the level of assurances to be provided for legacy (SWAL3-like or SWAL2-like)
- DSNA has some difficulties to substantiate the confidence level satisfaction.

COTS treatment:

- COTS safety acceptance criteria is based on either reverse engineering techniques or EXP. What else?
- Software common modes of failures can lead to high SWAL in network (drivers or routeurs) when the architectures are not diversified.

No adverse safety effect from COTS

- difficulty to list all COTS functionalities (OS for instance) and deactivate/remove/passivate them.
- the strategy is to perform endurance testing.

Already flawed architectures

- ARTAS used as primary means for the ASP. The HAZ ‘Undetected corruption of ASP’ is deemed SC2, even SC1 (FABEC brainstorming) where ARTAS is shown to be SWAL3.
Questions ?