DSNA policy on software aspects

Yann Carlier

DSNA/MSQS/SDS

Safety Management Unit

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Écologie, du Développement durable, des Transports et du Logement

Ressources, territoires, habitats et logement
Énergies et climat
Développement durable
Prévention des risques
Infrastructures, transports et mer

Présent pour l'avenir

Direction générale de l'Aviation civile
Direction des services de la Navigation aérienne

dgac

DSNA

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 routeurs)…

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.

DSNA compliance with CE n°482/2008 Guidance for the SW methodology (August 2011)

August 2011 : release of a guidance to improve the SSAS application. Dedicated to project/safety practitionners 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 condifence level is adequate
- modify the SSAS accordingly (new measures, corrective actions to avoid deficincies in applying the directives).

DSNA SSAS : scope of application

- SSAS applies to any sofware 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 purpise 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 outuput 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

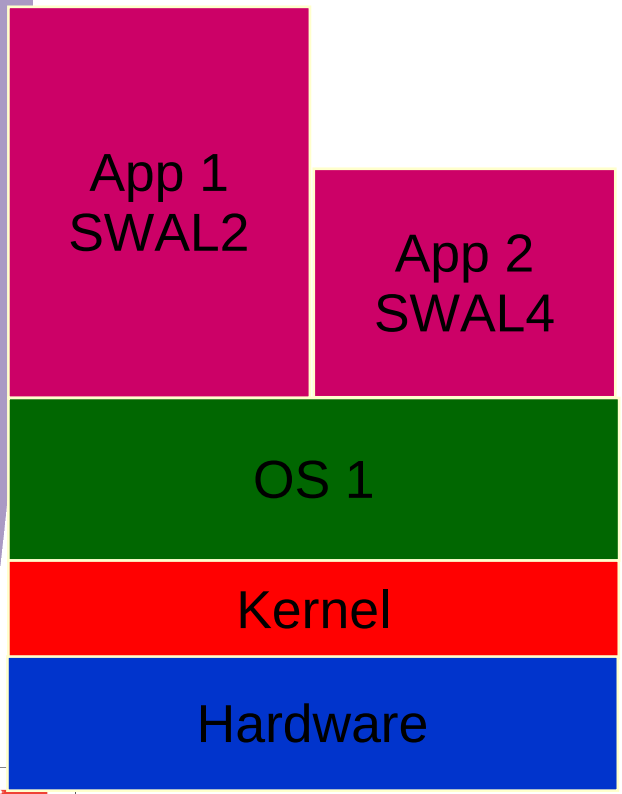
1 method for legacy software

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 microcontroler, where isolation can be substantiated between them (e.g by the use of partitioning techniques to ensure spatial and temporal segregation

Why isolation is nedded to allocate at component level ?

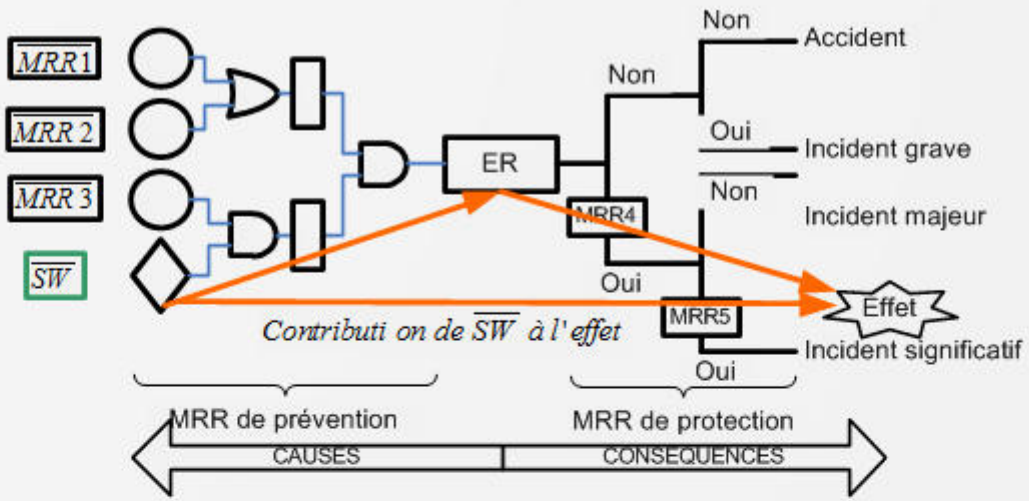


Quid when App2 exceeds its time frame or spatial allocation quantum; can App1 execute correctly ?
Isolation techniques are therefore required to allocate different SWAL.

SWAL determination : general method (ED153)

« Détermination du SWAL (méthode générale) »

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 :

Degré de gravité de l'effet / Contribution à l'effet	1	2	3	4
Très Possible	SWAL 1	SWAL 2	SWAL 3	SWAL 4
Possible	SWAL 2	SWAL 3	**SWAL 3**	SWAL 4
Improbable	SWAL 3	**SWAL 3**	SWAL 4	SWAL 4
Extrêmement Improbable	SWAL 4	SWAL 4	SWAL 4	SWAL 4

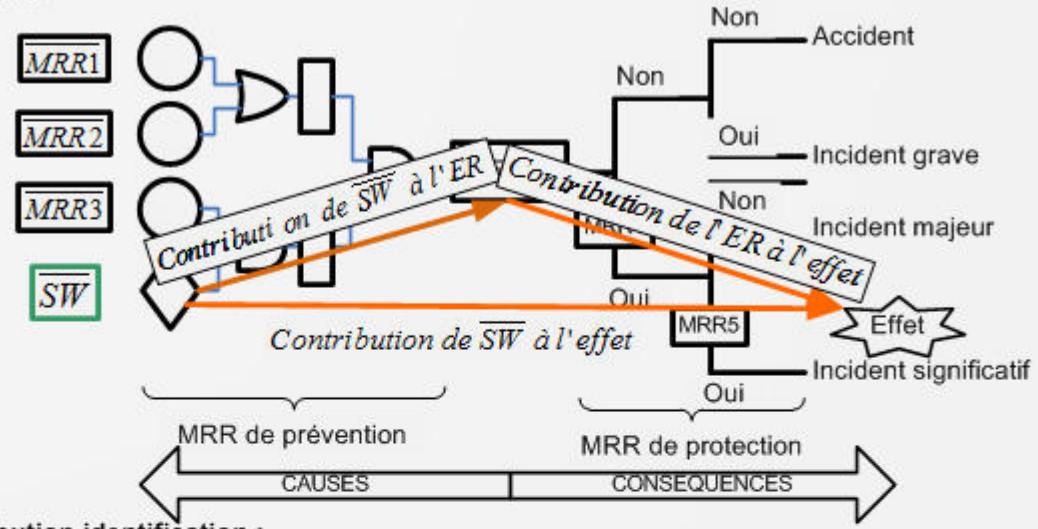
SWAL determination : DSNA alternate method

« Détermination du SWAL (méthode alternative) »

General principle :

Valid method in case no common modes exist between preventive and protective MM; otherwise, general method applies.

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 HAZ by exploiring 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.

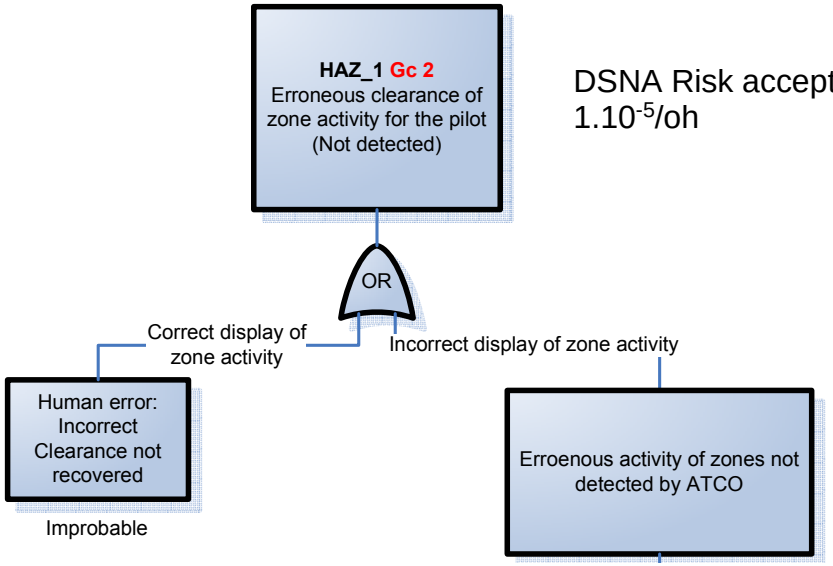
Multiple Combination : when exists a set of MM (external to the SW failure) that is very efficient and independent.

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

Niveau de gravité corrigé de l'ER Contribution à l'ER	1	2	3	4	5
Directe	SWAL1	SWAL2	SWAL3	SWAL4	SWAL4
Combinaison simple	SWAL2	SWAL3	**SWAL3**	SWAL4	SWAL4
Combinaison multiple	SWAL3	**SWAL3**	SWAL4	SWAL4	SWAL4

Example of SWAL allocation



DSNA Risk acceptability matrix
1.10^{-5}/oh

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

« Détermination du niveau de confiance Actuel, Renforcé »

Confidence level Determination : either Current or Upgraded

The confidence level determination is obtained by considering:

1) the software criticality

2) the nature of the software modification

Nature of SW Modification / Criticality	Minor	Major
Low	Current	Current
High	Current	Upgraded
From low to high	Upgraded	Upgraded

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.

Oterhwise, the criticality is **HIGH**.

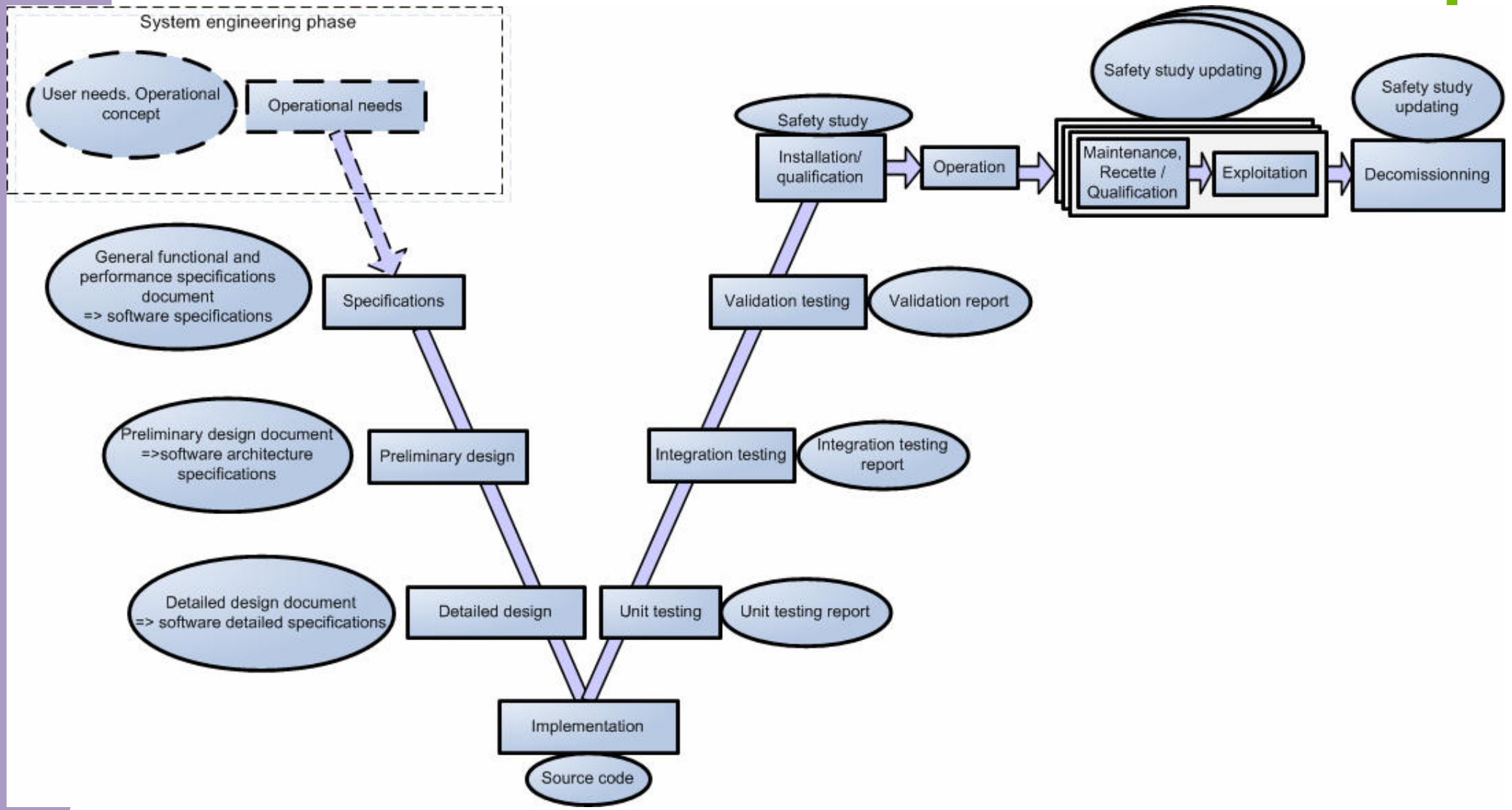
2) Nature of software modification

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.

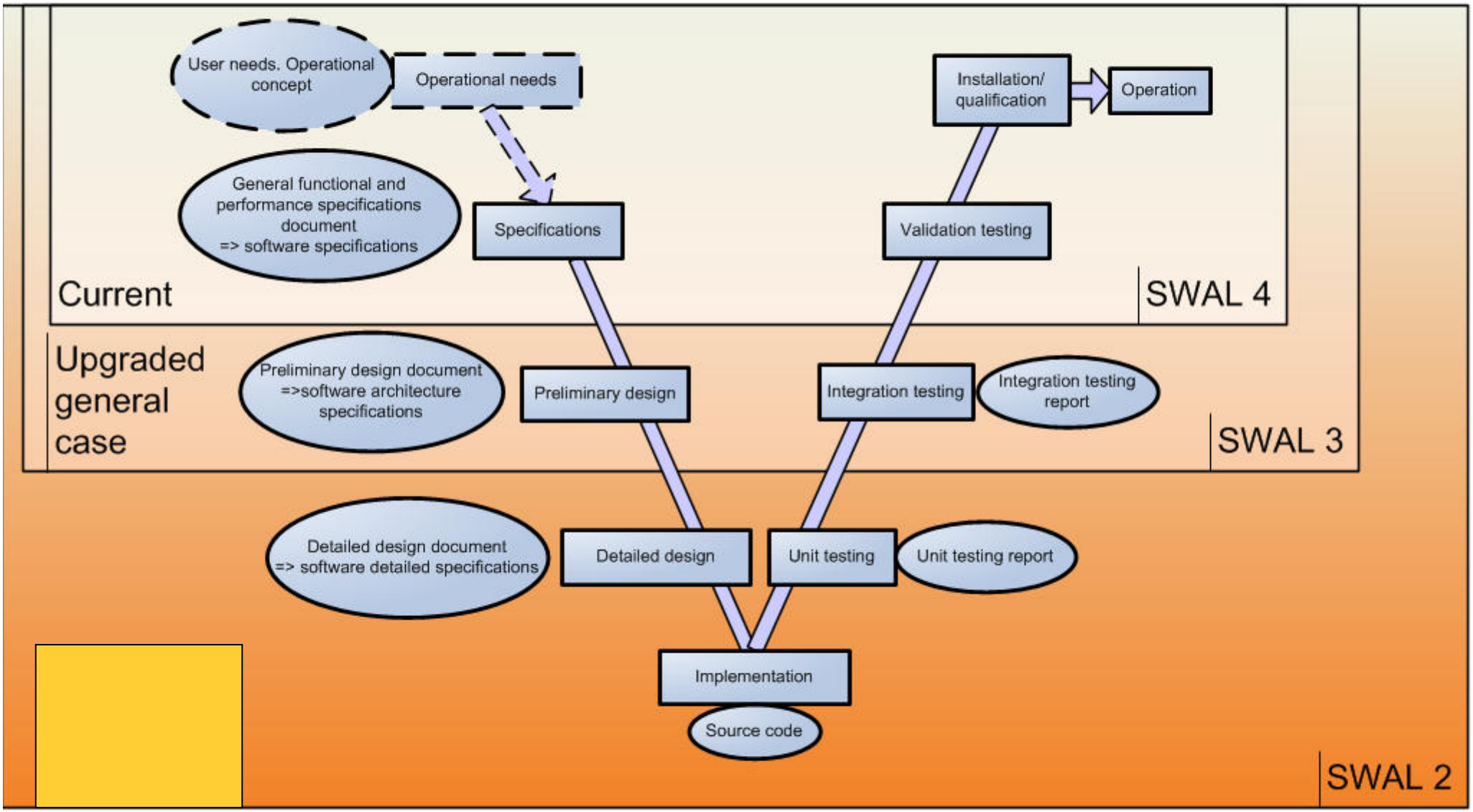
A software modification is said MINOR otherwise.

Confidence level satisfaction

Activities along the V cycle



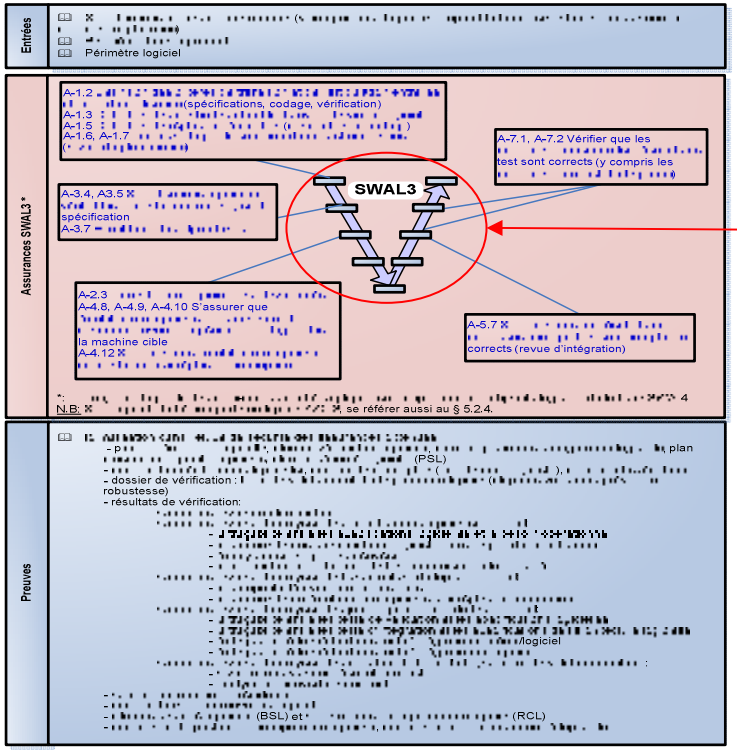
Software confidence level gradation policy

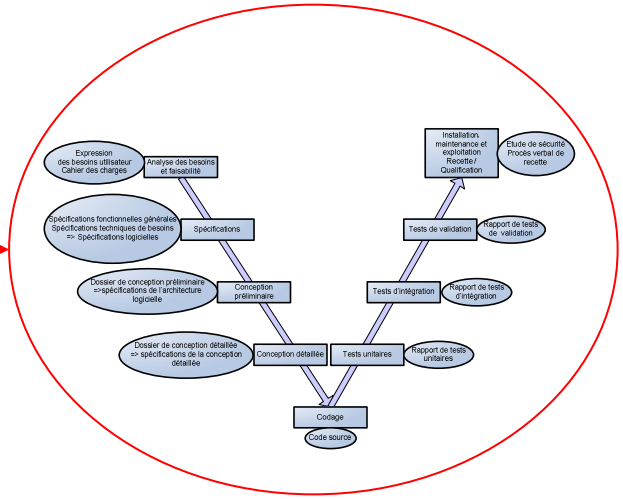


Guide Leaflet
Confidence level satisfaction leaflet structure

Definition of activites and expected evidence along the V cycle for each confidence level

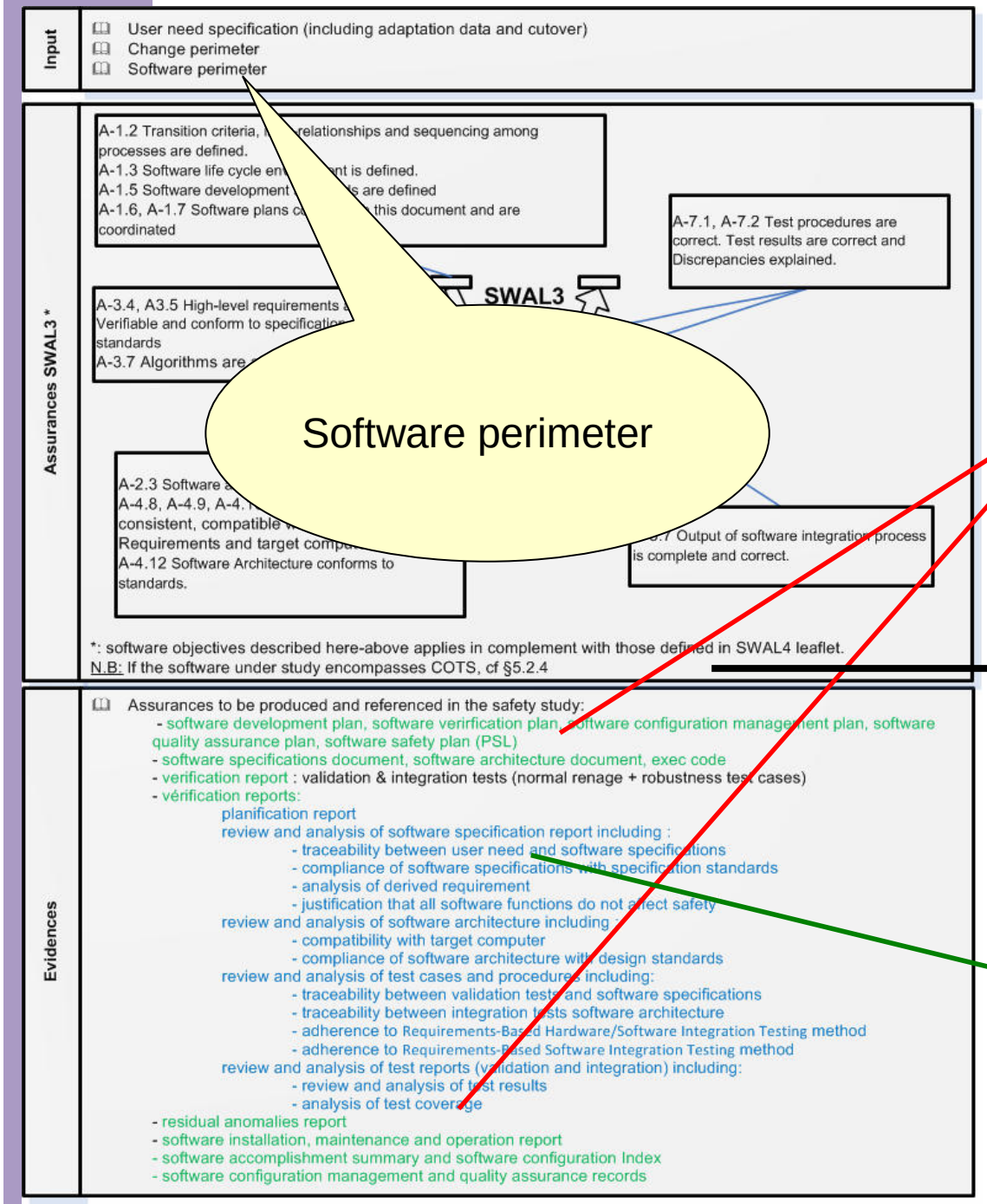
- work sharing (site, supplier…)





Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Ministère de l'Écologie, du Développement durable, des Transports et du Logement

Confidence level satisfaction leaflet



Annex 1

Software life cycle data (ED12B)

COTS considerations (ED109)

Annex 2

Software verification (ED12B)

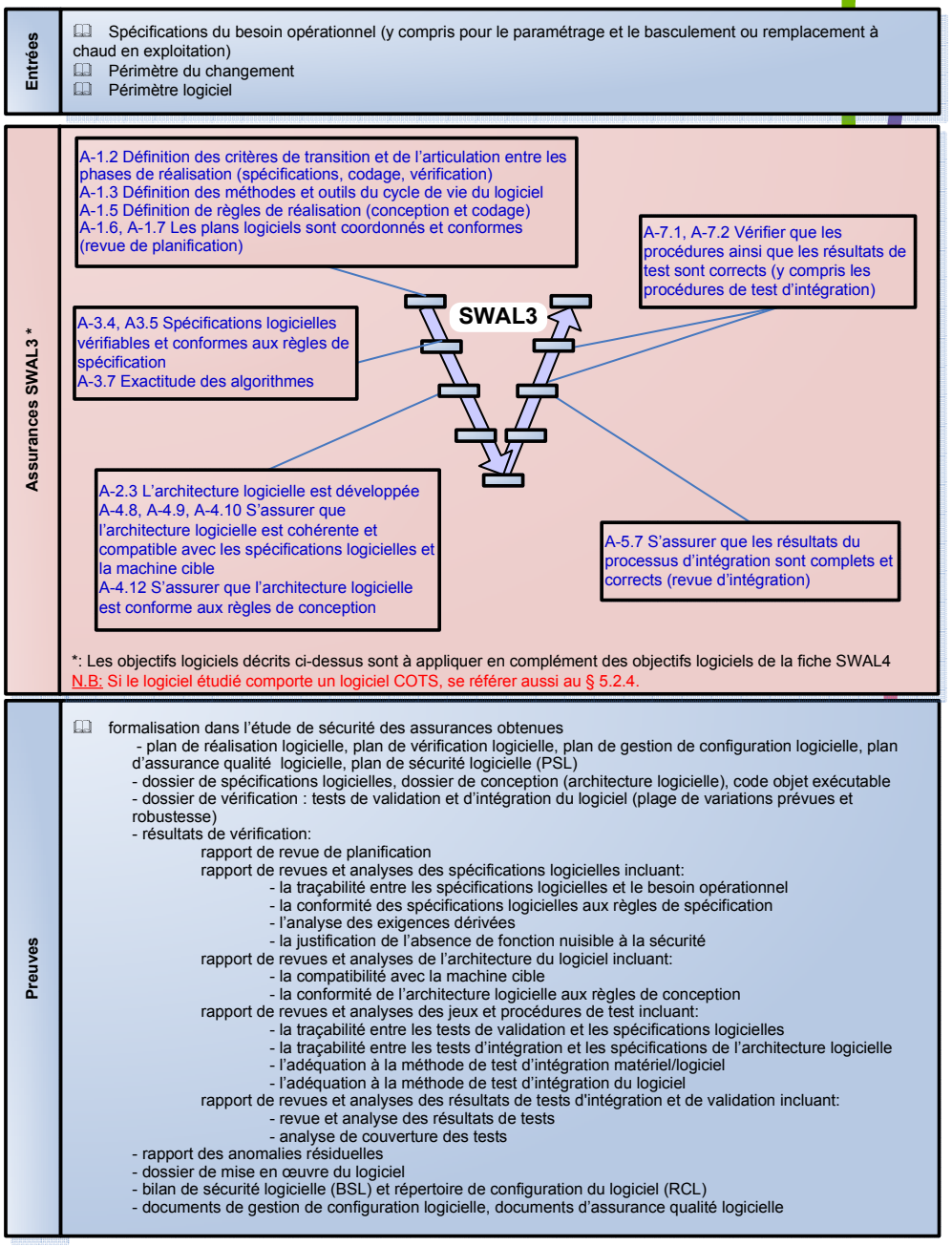
Guide METLOG : COTS Aspects (ED109)

Equivalence Confidence level/In service experience	
Required software Confidence level	**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

- 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.



Guide METLOG : COTS aspects snooping around

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

SW Confidence level required / Type of Introduced SW COTS	Upgraded	SWAL3	SWAL2
COTS software library			(validity and verification of requirements of library with SC and code review) Or EXP 1 year
Software components COTS (module, firmware, driver, OS, etc)			(validity and verification of preliminary and detailed design requirements, SC and code review) or EXP 1 year
Applicative software COTS	(validity and verification of preliminary design) Or EXP 1 year	validity and verification of preliminary design) Or EXP 6 months	(validity and verification of preliminary and detailed design requirements, SC and code review) or EXP 1 year

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 a 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 redevelopped.
- 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 ?

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Écologie, du Développement durable, des Transports et du Logement

Direction générale de l'Aviation civile
Direction des services de la Navigation aérienne

dgac
DSNA