www.thalesgroup.com

SW Safety Workshop

IANS EUROCONTROL
7th & 8th May 2013 Luxembourg
Bernard Pauly

THALES

Acronyms/ Vocabulary

ANS Life Cycle	Set of Reference Processes for Safety SW Management System
ANS SW Recommendations	Set of SWALs Objectives as defined according to ANS Life Cycle Processes
ANSPs	Air Navigation Services Providers
ASM	Air Space Management
ATFM	Air Traffic Flow Management Unit
CATF	Conformity Assessment task Force
CS	Community Specification
EASA	European Agency for the Safety of Aviation
EC482-2008	European Directive transposition of ESARR6 into european Law for the SW
EC552	European Directive for Interoperability
ED109	Guidelines for the SW
ED153	Guidelines for a SW Assurance System in ATM
ERs	Essential Requirements
ESARRs	European Safety Regulatory Requirements (ESARR4 Risk and mitigation on ATM- ESARR6 for SW in ATM)
FABs	Functional Airspace Blocks
GSN	Goal Structured Notation – Formalisation of How to build Safety Arguments
IR	Implementing Rules
SES	Single European Sky
SESAR	Single European Sky ATM Research
SRC	Safety Regulation Commission (Eurocontrol)
SWAL	SW Assurance Level

Background

Bled SW Workshop in 2011 a lot of points have been discussed and raised regarding

- Compliance with regulation (EC482, ESARR6, EC552…)
- Interfaces between stakeholders (CA authorities, ANSPs, Industry)
- Use of standards (ED153, ED109…)
- Legacy SW (COTS, NDI…)
- ……

Following derived questions should be addressed

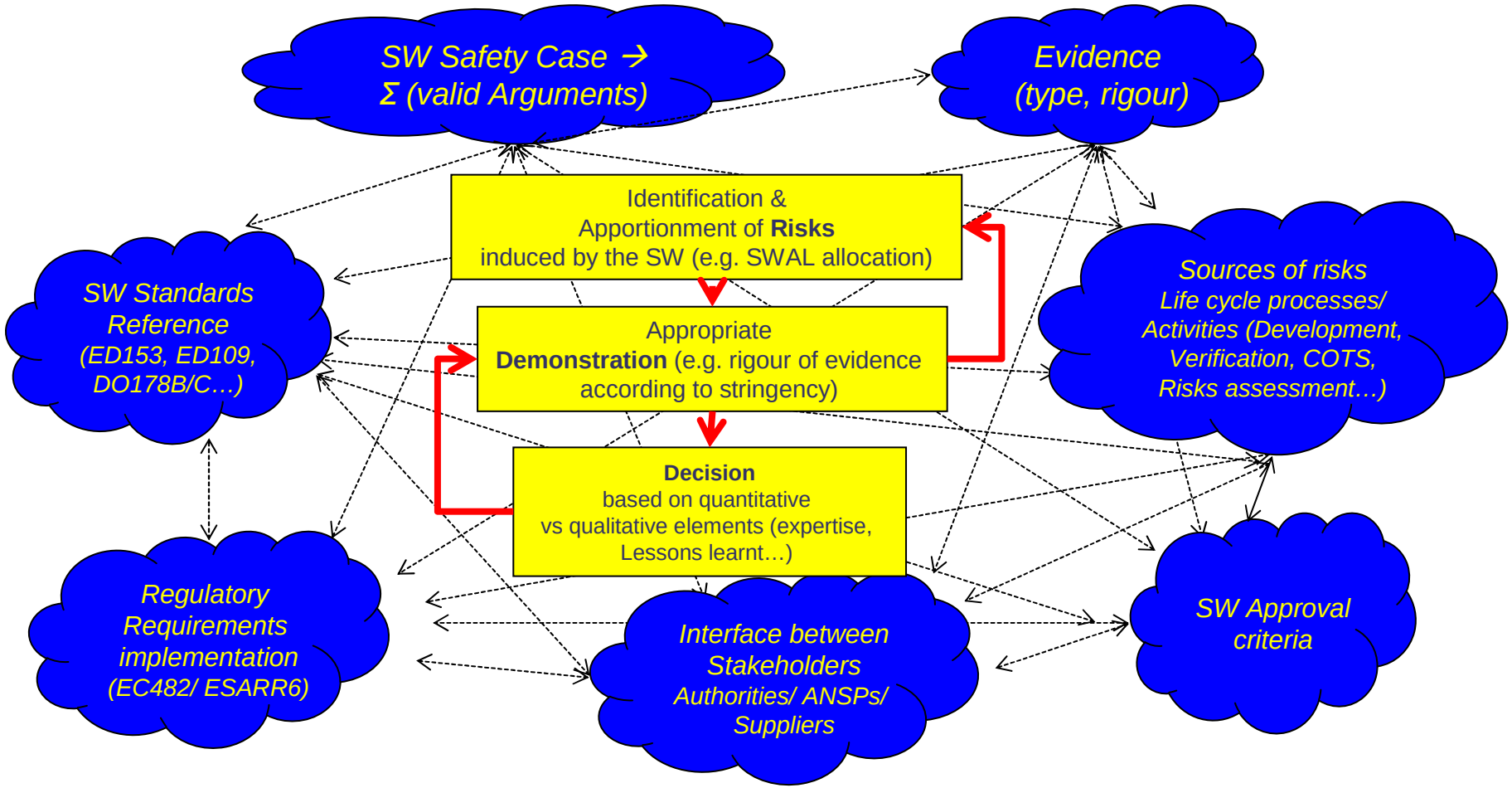
- Could we have a benefit to define and promote a « standardised » approach to develop SW Safety Arguments?
- Which place should have SW standards in this « Argument development » approach?
- How could we use safety risks models like IRP (Integrated Risks Picture) or AIM (Accident Incident Model) as used in SESAR (e.g. SWALs allocation consolidation)?
- Which impact on stakeholders roles (CA authorities, ANSPs, Industry)
- Could it be an opportunity to converge with Airborne SW (SW certification vs SW Safety Case) for some integrated functions?
- How to decide about the rigour of safety evidence ?

A SW Safety Assurance System view shall be shared between stakeholders in a perspective of a total aviation system

THALES

Introduction-Context of a SSAS

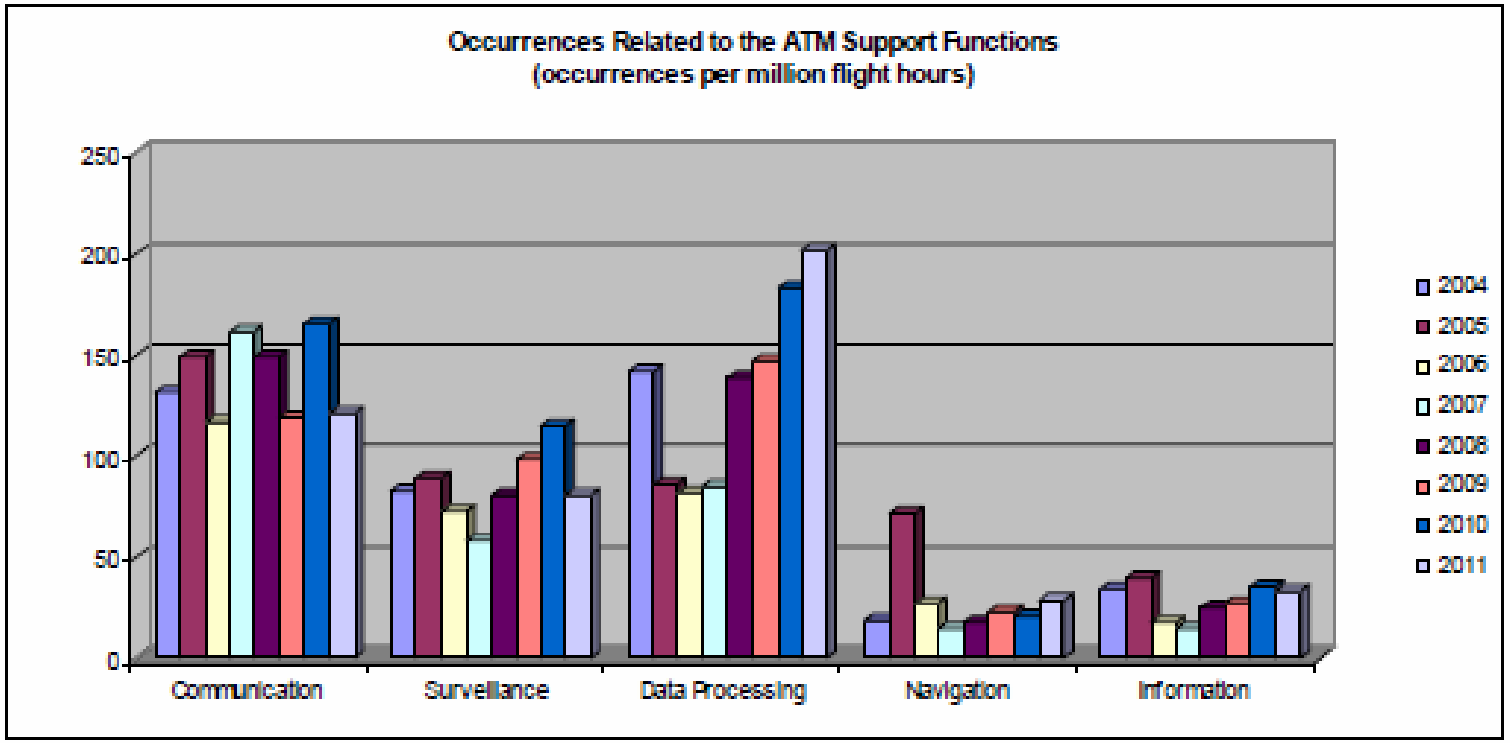
Which context for SW Safety Assurance System?



"Safety performance based" demonstration → avoid bottleneck and shortcoming potentially induced by some systematic "Compliance based" approaches

THALES

ATM Support Function Safety Occurrences

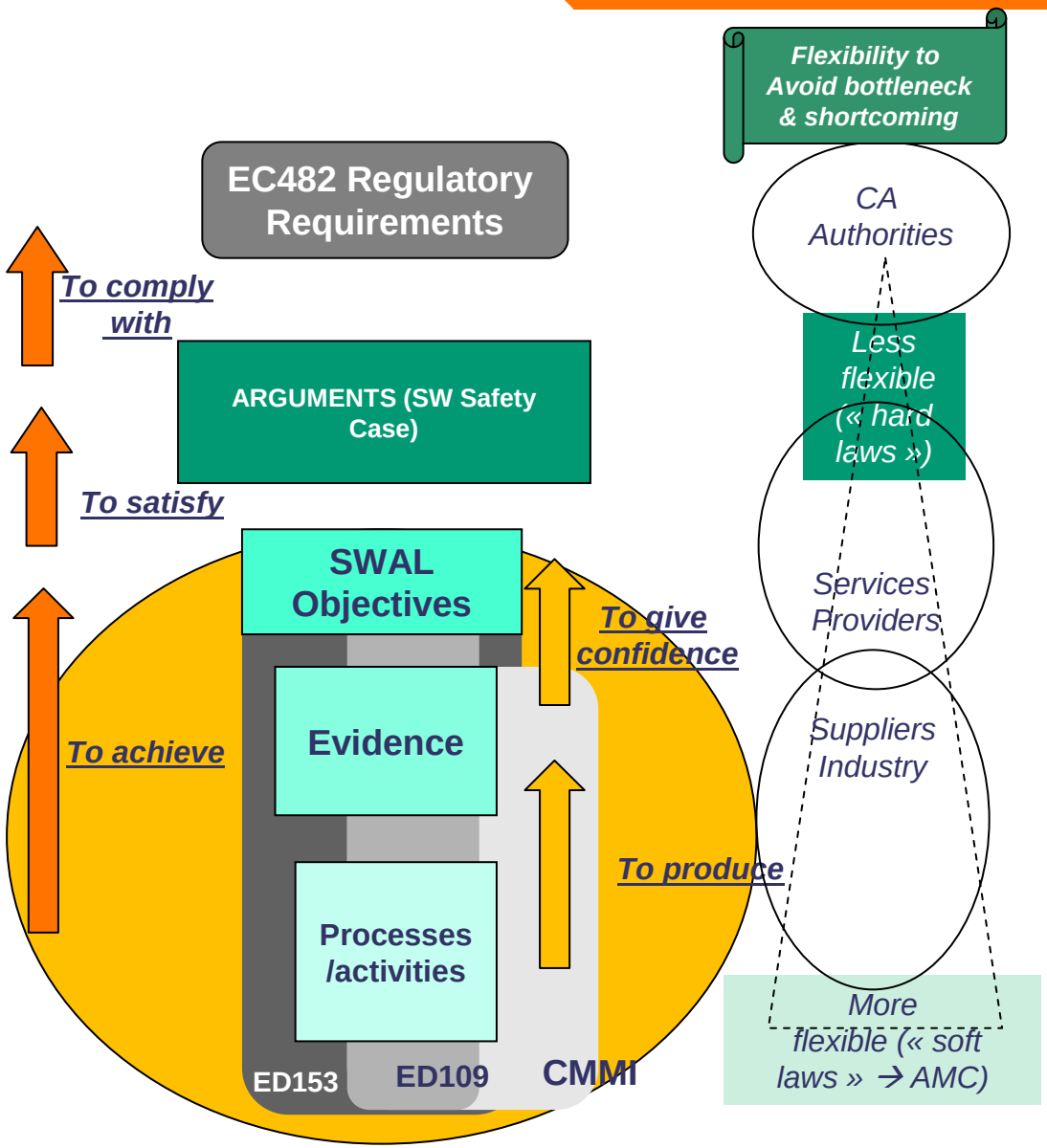


Occurrences Related to the ATM Support Functions (occurrences per million flight hours) [source SRC Annual report 2012]

Keep in mind

THALES

A structured SSAS approach to be shared by stakeholders



- ***Comply with Regulatory Requirements (EC482)***

  Compliance with SW regulation is supported by a set of comprehensive, unambiguous and complete arguments provided in the SW safety case

- ***Satisfy SW Safety Arguments*** :

  The validity of SW safety arguments is based on a set of relevant evidence (« direct » and « backing »)

  Standards SWAL objectives can be seen as a « bridge » between arguments and supporting evidence

- ***Achieve SWAL Objectives:***

  According to the allocated SWAL the set of relevant objectives are achieved by executing a complete set of processes/ activities of the life cycle able to produce evidence with the right level of rigor

- ***Produce evidence and give confidence:***

  « Performance based » approach supposes more flexibility but confidence is assured through relevant quantification (SW Metrics)

THALES

Develop SW Safety Arguments-overview

Arguments are driven by « Sources of safety risks »

- **Claims shall reflect the whole set of potential sources of safety risks induced by SW through People/ SW Processes as refered in standards (e.g. ED153, ED109)/ SW Products and their interactions (similar to « People/ Procedure/ Equipment » for a System Safety Case)**

Arguments are driven by « SW safety regulation »

- **Claims shall reflect the whole set of applicable SW Regulatory Requirements (e.g. EC482)**

Then Arguments satisfaction are based on evidence

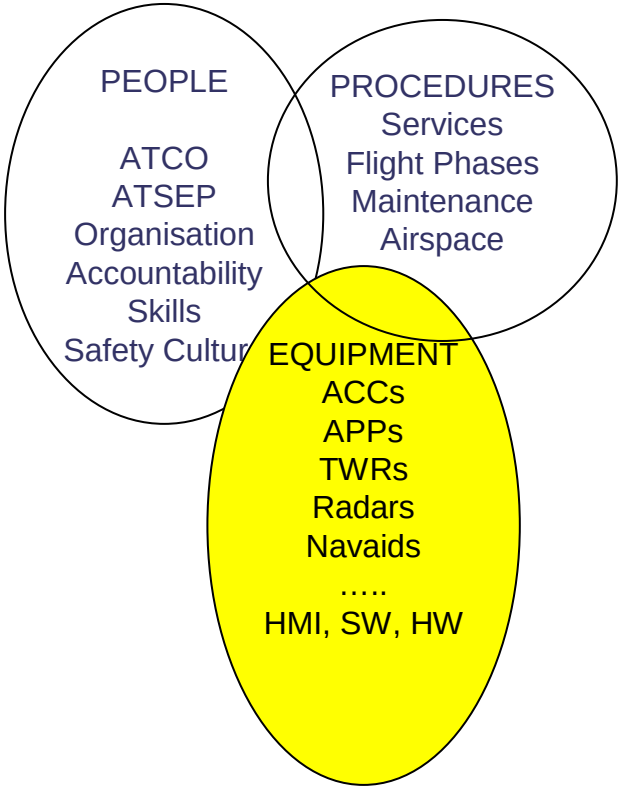
- Claims are usually supported by objective evidence (True/ False) according to assumptions/ context/ strategy/ justification
- Identification of evidence and related rigor can be facilitated by the reference to SW standards but some concerns remain regarding the identification and rigour of expected evidence (e.g. very often standards do not clearly & completely specify relevance and rigour of evidence)
- Moreover Problem of counter evidence shall be addressed

Currently there is no "standardised" way to develop SW safety argument but……2 main drivers: sources of risks & SW safety regulation

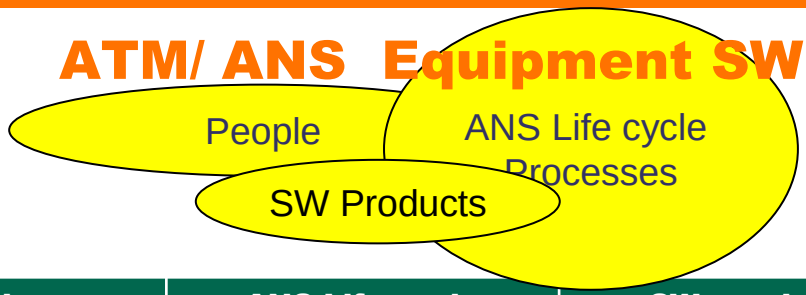
THALES

Develop SW Safety Arguments: consider Source of safety risks

ATM/ ANS System



ATM/ ANS Equipment SW



People	ANS Life cycle Processes	SW products
Software Safety Assurance System: SW Safety Case		
Organisation **Skills** **Responsabilities** **Independancy criteria** **Safety culture**	**Acquisition** **Supply** **Risks assessment** **Documentation** **Development** **Improvement** **Change** **Training** **Verification** **Configuration management** **Quality** **COTS** **……**	**Requirements validity** **Requirements satisfaction** **Requirements traceability** **Non unintended functions** **SW configuration**

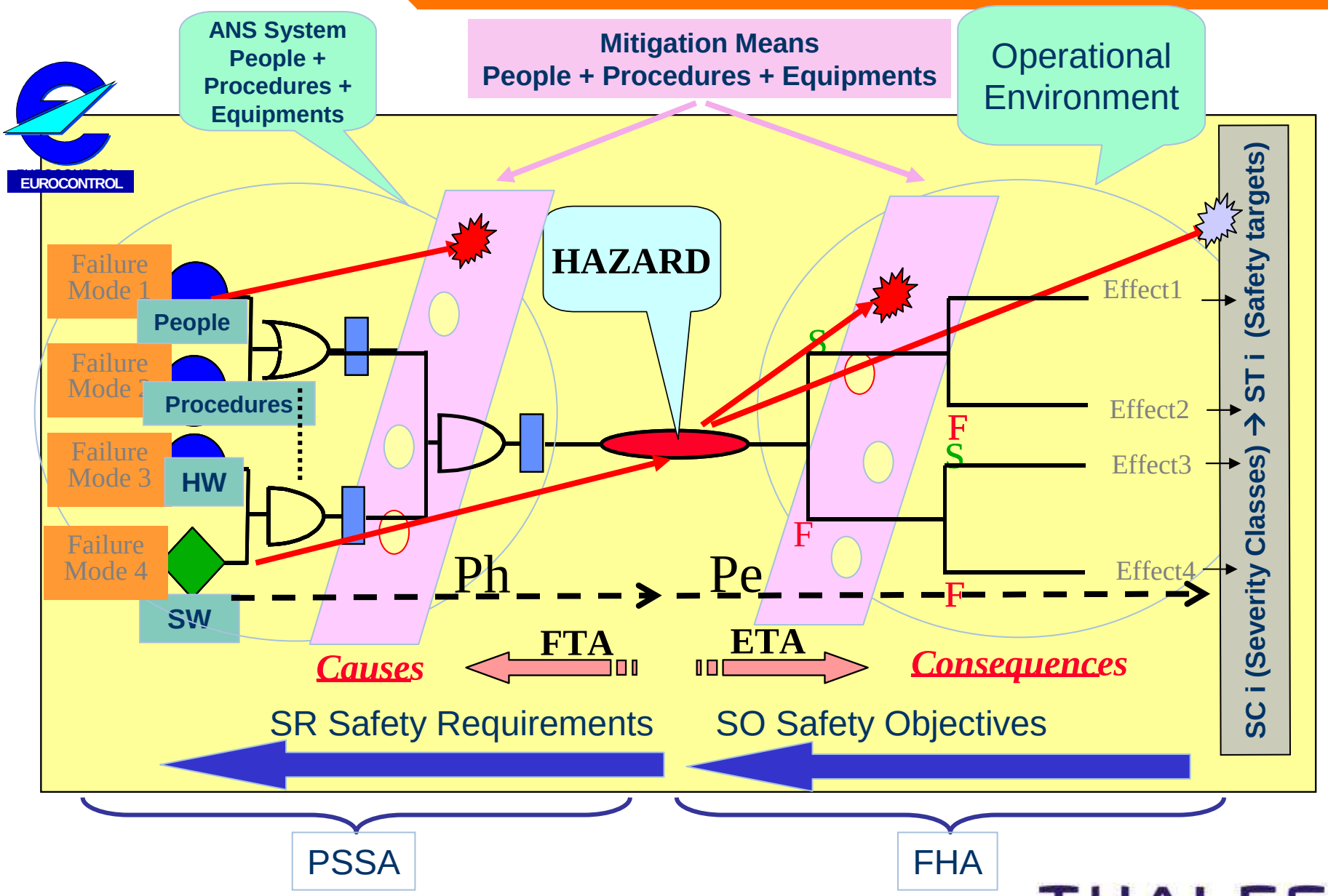
Backing Evidence

Direct Evidence

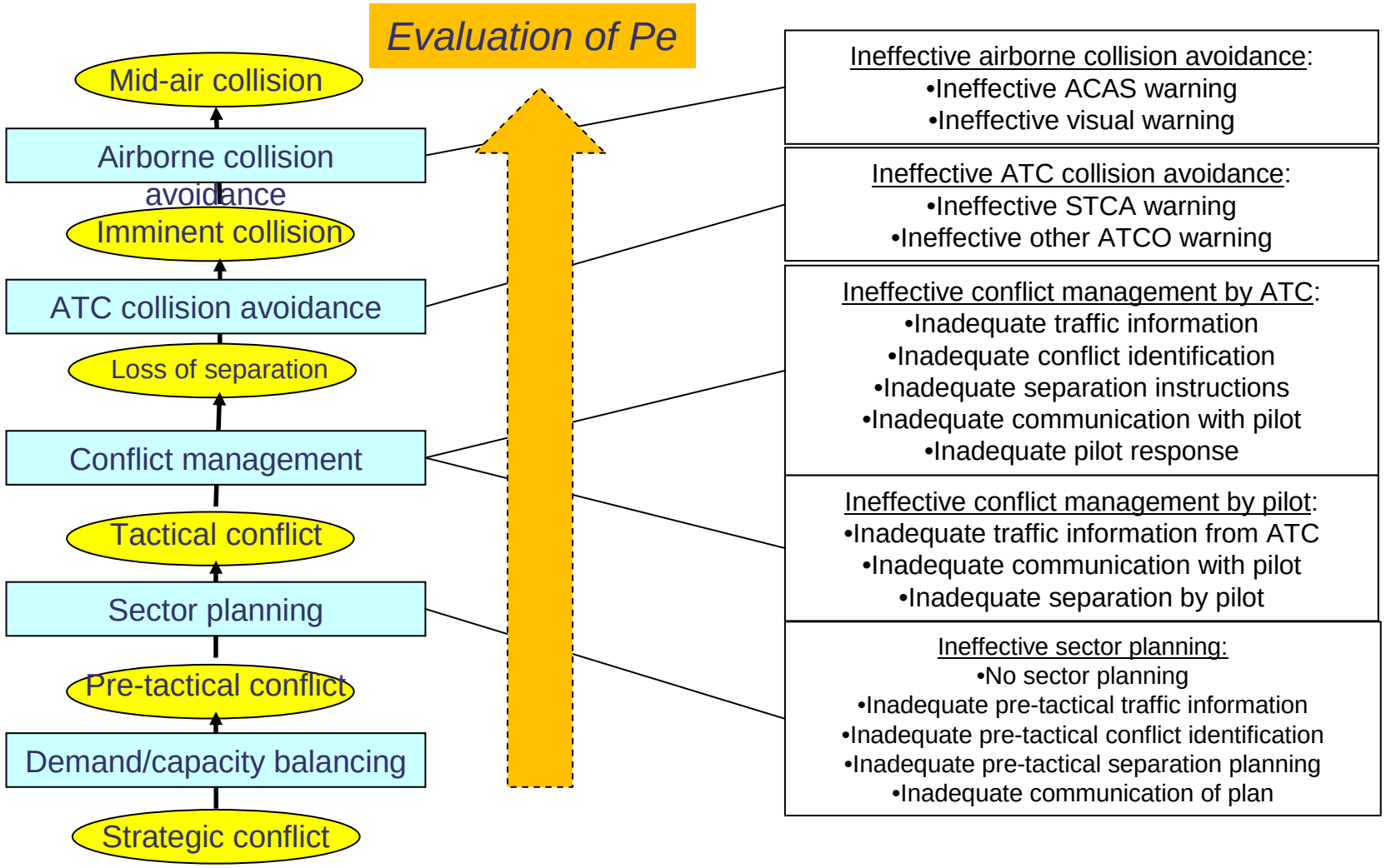
Consider People/ Processes/ SW Products (according to « People/ Procedure/ Equipment » for a System Safety Case)

THALES

Source of safety risks (Failures – Hazards- End Effects)



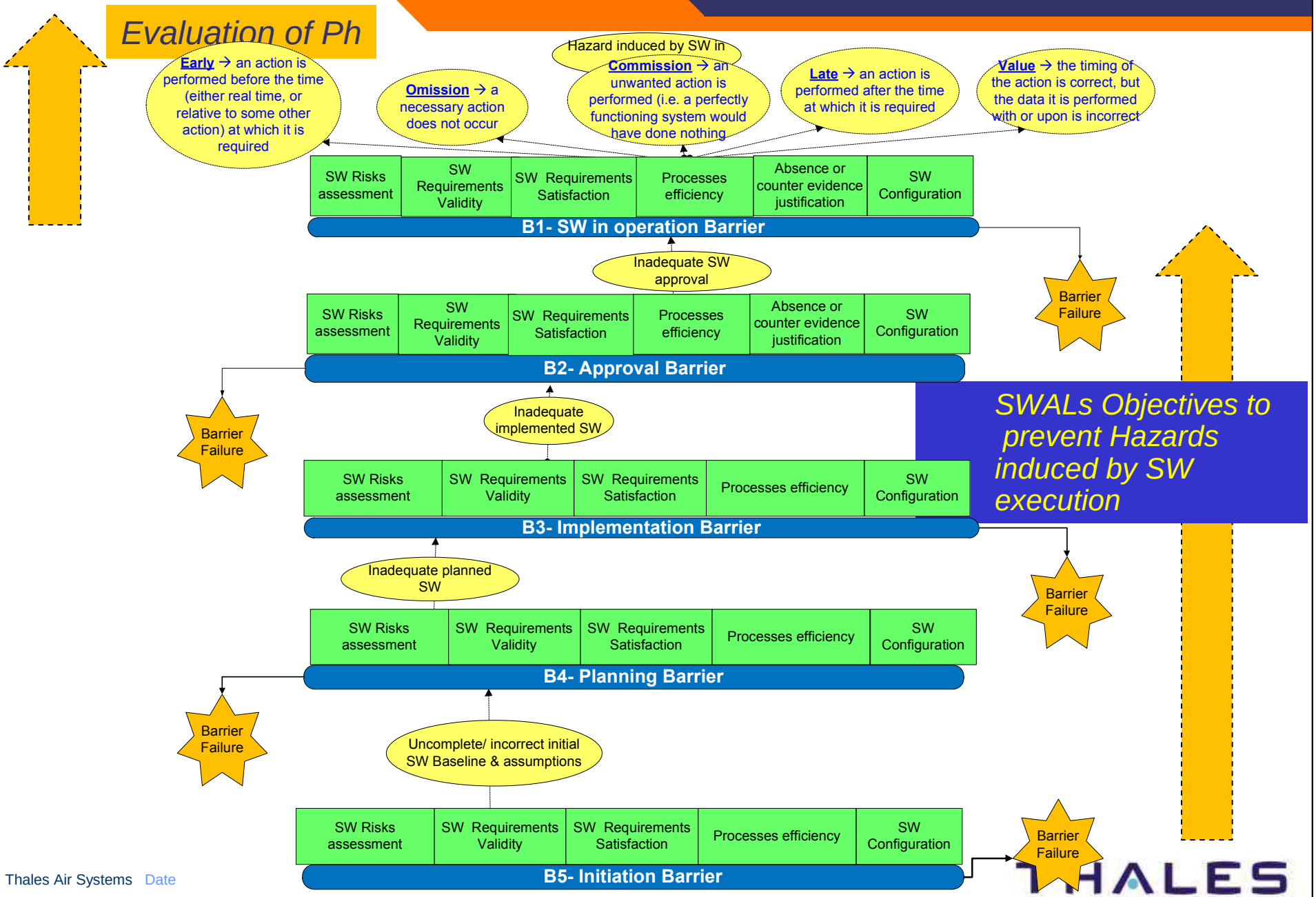
Source of safety risks (Pe Evaluation)



According to IRP/ SESAR AIM (Integrated Risks Picture/ Accident Incident Model)→ example of Mid-Air Collision

THALES

Source of safety risks/ towards a SW Risks models



SW Safety Arguments: SW Safety Regulation (EC482)

EC 482 (2008) main High level Regulatory requirements (ATS/ ATFM/ CNS/ ASM)

■**SWAL allocation** → A software assurance level shall be allocated and commensurate with the most severe effect that software malfunctions or failures may cause according to applicable severity and risks classification schemes

■**SW requirements validity** → Are the SW requirements the "*good requirements*" ?

- *functional behaviour, (nominal & downgraded mode), capacity, performance, timing properties, robustness…..*
- *The SW requirements are correct, complete and totally compliant with the system requirements) ?*

■ **SW requirements satisfaction** → Are the SW requirements completely and correctly verified?

■ **SW requirements traceability** → For correctness and completeness purpose at each step of the life cycle, external consistency of requirements with upper level requirements is required

■ **Configuration management** → The right configuration of operating SW is always required

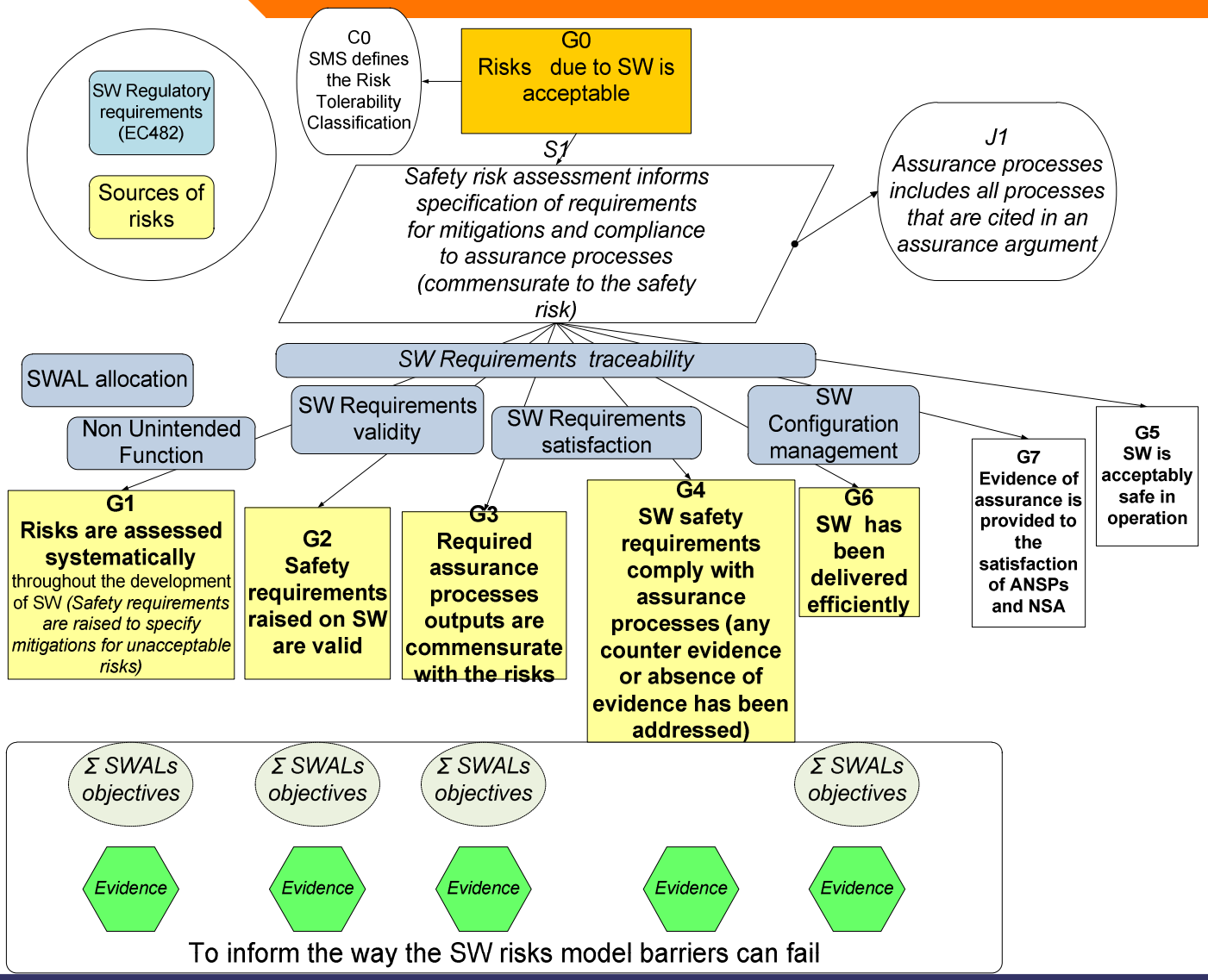
- *identification, traceability, status accounting, problem reports…..*

■ **Unintended Functions** → Unintended functions are functions in the software that are either performed in addition to those required or that are not performed on demand

Claims shall reflect the applicable SW Safety Regulatory Requirements

THALES

Towards a SW Safety Arguments overall structure



SW safety arguments structure should reflect a consistent view between sources of risks & SW regulatory requirements

SW Safety Arguments Demonstration

The demonstration of SW Safety Arguments could be structured according to the following steps:

- **Prerequisite: Inform the barriers of SW risks model with relevant SWALs objectives by using SW standard (e.g. ED153)** ***(Note: not mentionned here)***
- **For each SW Argument decomposition (except G4 argument)**
  - **Step 1** → identify expected evidence
  - **Step 2** → identify SWALs objectives facilitating provision of expected evidence
  - **Step 3** → Match the SWALs objectives of SW arguments with SWALs objectives of the Risks model barriers (ref Prerequisite)
  - **Step 4** → identify the way the SW argument could not be demonstrated (by using model barrier failures scenarios)
- **For G4 Argument related to counter evidence**
  - **Step 5** → compute the weight of related SWAL objective & evidence according to their contribution to barrier failures (filter evidence by using direct vs backing evidence) → **inform the rigour of evidence**
- **SW Risks model consolidation**
  - Populate the model with historical data regarding root cause analysis of hazards induced by SW in order to assess the efficiency of barriers (% failure rate)

THALES

SW Safety Arguments Demonstration (example Argument G1 Risks Assessment) steps1 & 2

G1 *Risks are assessed systematically throughout the development of SW (Safety requirements are raised to specify mitigations for unacceptable risks):*

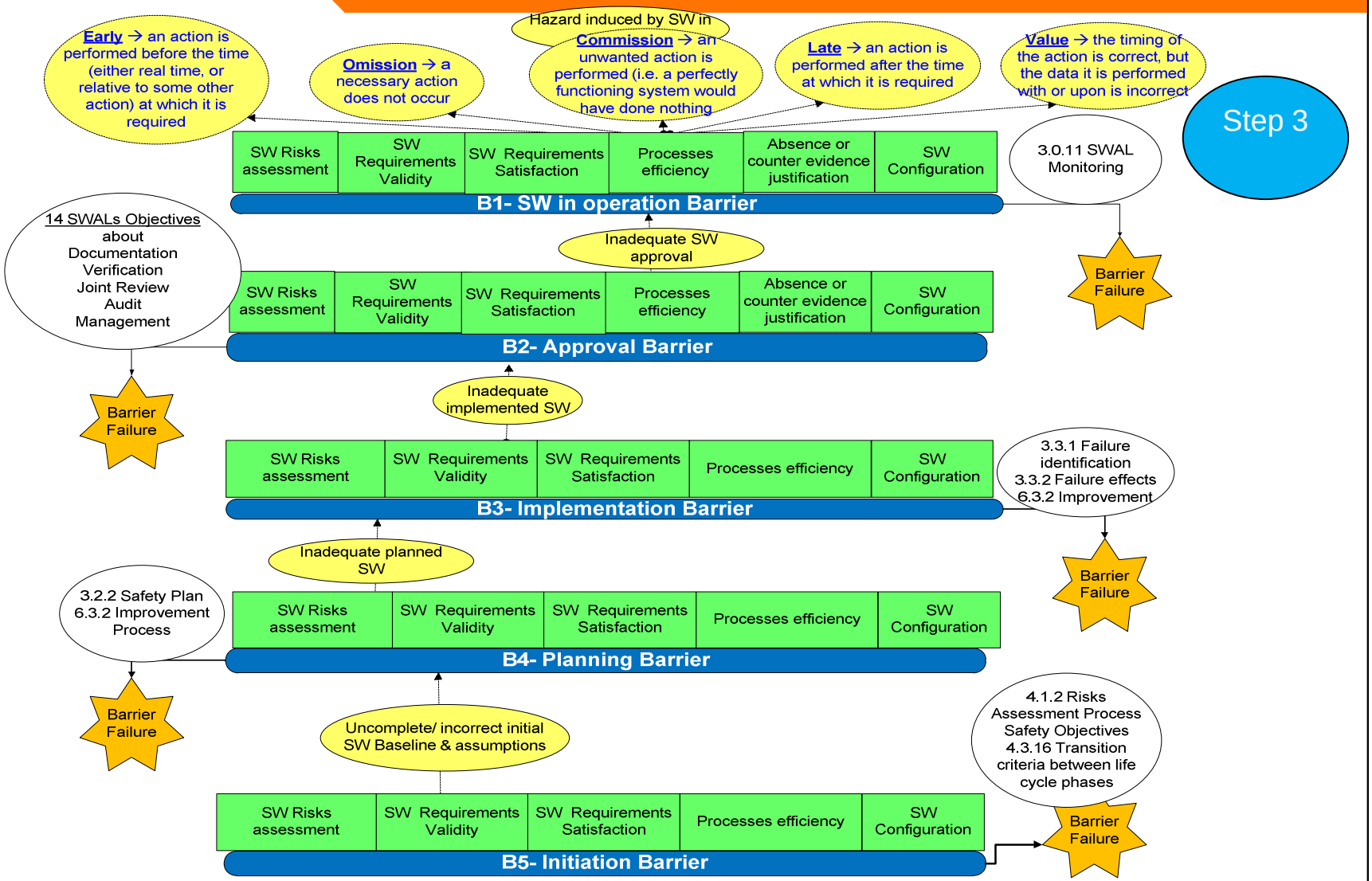
G1 Risks are assessed systematically			Step 1 (expected evidence)	Step 2 (SWAL objectives)
		EV 1.2.1a	FFA process definition	
G1.2.1	FFA has been conducted in accordance with FFA process	EV 1.2.1b	**Output of the FFA process**: Who was involved, what was analysed, what input material, potential hazards identified, review records?	From failure point of view 3.0.11 SWAL Monitoring 3.3.1 Failure Identification 3.3.2 Failure Effects From Hazards point of view 3.2.2 Software Safety Assessment Plan 3.3.2 Failure Effects 3.4.2 Software Safety Assessment Verification 4.1.2 Risk Assessment and Mitigation Process – safety objectives From Analysis point of view 4.3.16 "Transition criteria a) between life cycle phases (for req analysis and verification phases)b) describe the SW life cycle process to be used" From Results point of view 3.5.1 Document Software Safety Assessment Process Results 5.4.12 Verification of Verification process results 5.4.5 Verification of software architectural design 5.4.6 Verification of detailed design 5.4.8 Verification of executable code 5.6.1 Process implementation_Joint Review Process 5.7.1 Process implementation_Audit Process 5.7.2 Audits at SW requirement level 5.7.3 Audits down to SW design level 5.7.4 Quality audits down to source code level 5.7.5 Quality audits down to executable level 6.1.3 Execution & control 6.1.5 Closure 6.3.2 Process assessment_Improvement Process

Step 1 & Step 2

Example: G1.2.1 FFA (Functional Failure Analysis) has been conducted according to FFA process

THALES

SW Safety Arguments Demonstration (example Argument G1 Risks Assessment) Step 3



Example: G1.2.1 FFA (Functional Failure Analysis) has been conducted according to FFA process

THALES

SW Safety Arguments Demonstration (example Argument G1 Risks Assessment) Step 5

Example: G1.2.1 FFA (Functional Failure Analysis) has been conducted according to FFA process

Step 4 → identify the way the SW argument could not be demonstrated (by using model barrier failures scenarios)

Step 4

➢B5 Initiation Barrier

- **SWAL 4.1.2 → Safety objectives determination for the SW not appropriate or wrong assumptions regarding apportionment of safety objectives to SW safety requirements**
- **SWAL 4.3.16 → Inadequate transition criteria definition for SW life cycle phases (e.g. completeness of SW failures scenarios)**

➢B4 Planning Barrier

- **SWAL 3.2.2 Inadequate FFA description in SW Safety Plan (e.g. FFA template)**
- **SWAL 6.3.2 Improvement action plan not existing or inadequate (e.g. lack of lessons learnt from former analysis)**

➢B3 Implementation Barrier

- **SWAL 3.3.1 Inadequate analysis of various ways the SW components could fail (e.g. due to incorrect documentation)**
- **SWAL 3.3.2 Inadequate identification of failure effect (e.g. wrong assumption about operational environment and then incorrect assessment of the end effect severity)**
- **SWAL 6.3.2 Continuous Improvement actions not existing or not performed (e.g. Hazards Log not regularly assessed)**

THALES

SW Safety Arguments Demonstration (example Argument G1 Risks Assessment) Step 5

Example: G1.2.1 FFA (Functional Failure Analysis) has been conducted according to FFA

Step 4

Step 4 → identify the way the SW argument could not be demonstrated (by using model barrier failures scenarios)

➢B2 Approval Barrier

- SWAL 3.4.2 SW safety requirements not consistent (e.g. with functions to mitigate hazards reflected by safety objectives)
- SWAL 3.5.1 SW safety assessment process is not adequately documented
- SWAL 5.4.12 Verification process is not adequate (e.g. verification procedures are not complete and/ or inadequate whatever the scope specification/ design/ code)
- SWAL 5.4.5/6 Verification results (requirements/ design/ code) are not satisfactory
- SWAL 5.7.(2,3,4) Audits not performed or inadequate
- SWAL 6.1.5 Closure The completeness of the results and records of the SW products, activities and tasks is not checked

➢B1 SW in operation Barrier

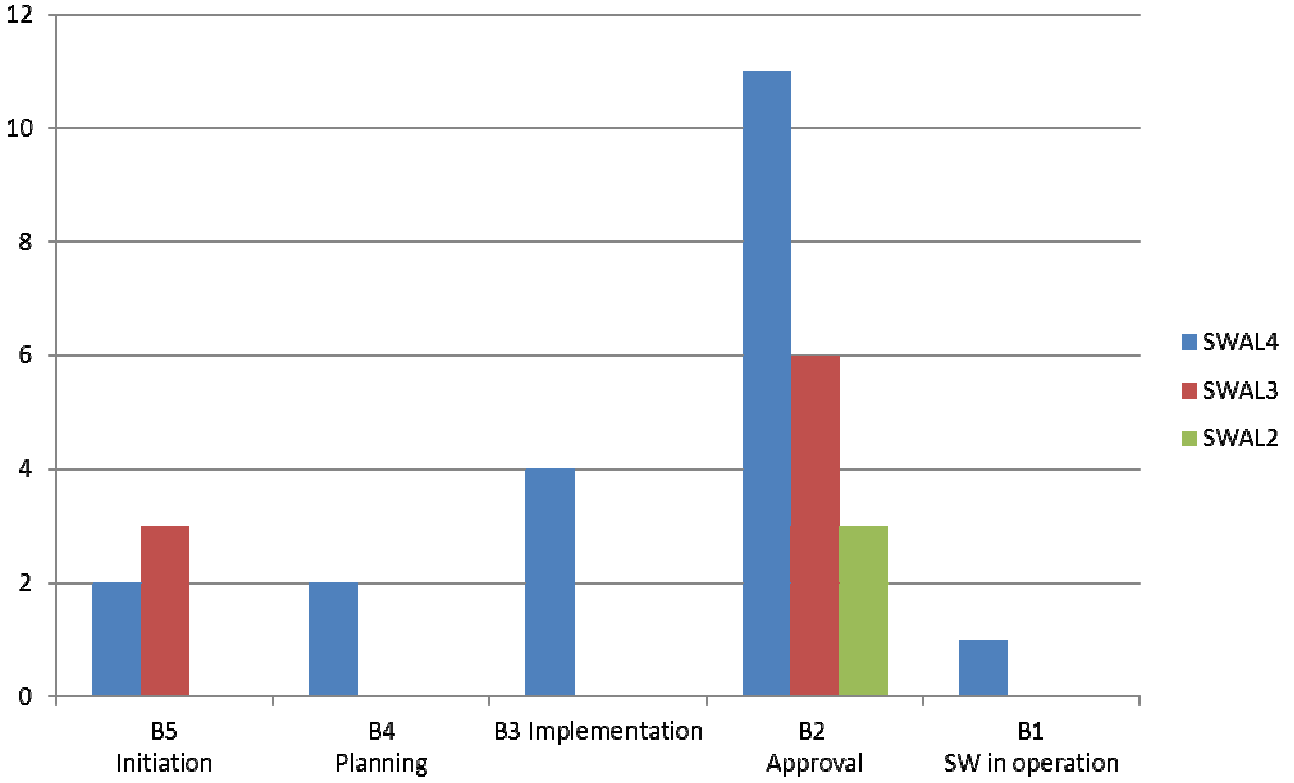
- SWAL 3.0.11 Inappropriate monitoring of safety occurrences due to SW malfunctions. The SWAL level of SW components could be inadequate from end effects severity point of view.

SW Safety Arguments Demonstration (example Argument G4 Counter evidence)

Based on G1.2.1 argument development findings how to develop G4 Argument related to absence/counter evidence ?

"G4- SW safety requirements comply with assurance processes (any counter evidence or absence of evidence has been addressed)"

Step 5→ compute the weight of related SWAL objective & evidence according to their contribution to barrier failures (filter evidence by using direct vs backing evidence)



Step 5

THALES

SW Safety Arguments Demonstration (example Argument G4 Counter evidence)

Step 5

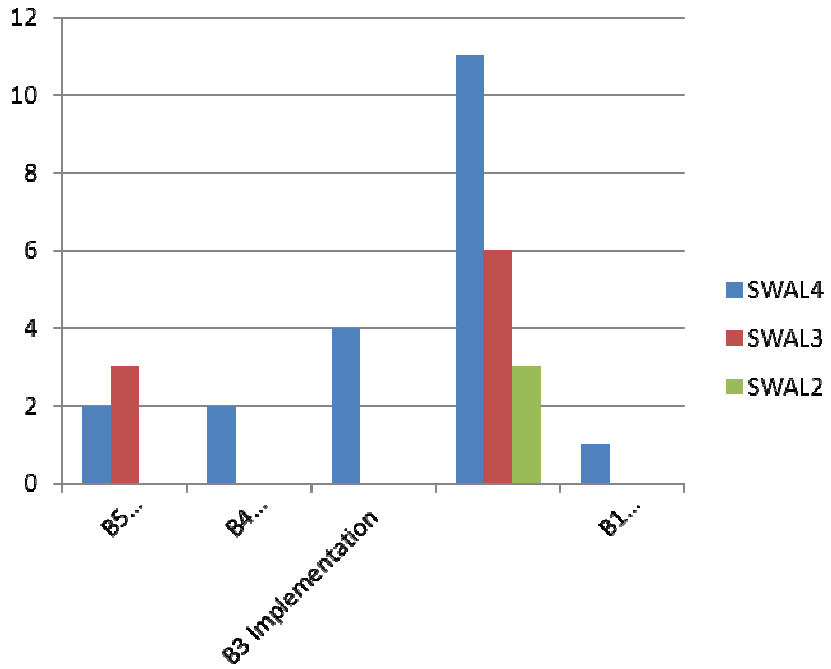
Rigour of evidence:

✓Consider per barrier the Nb of involved SWAL objectives with related SWAL stringency

✓Per barrier the confidence in the demonstration of the « FFA argument G1.2.1 » is related to the compliance with the number of corresponding SWAL objectives for this barrier and their « diversity »

✓According to SWALs objectives definition SW Metrics could be defined and computed

✓Example of SW Metric for the SW Verification



N° SWAL	Objective	SWAL 2	SWAL 3	SWAL 4	Question	Metric
5.4.5	Verification of Software architectural design	*	*		Is there adequacy between Software requirements and software architectural solutions ?	Percentage of compliance of SW safety specification checklist with SW safety design checklist

THALES

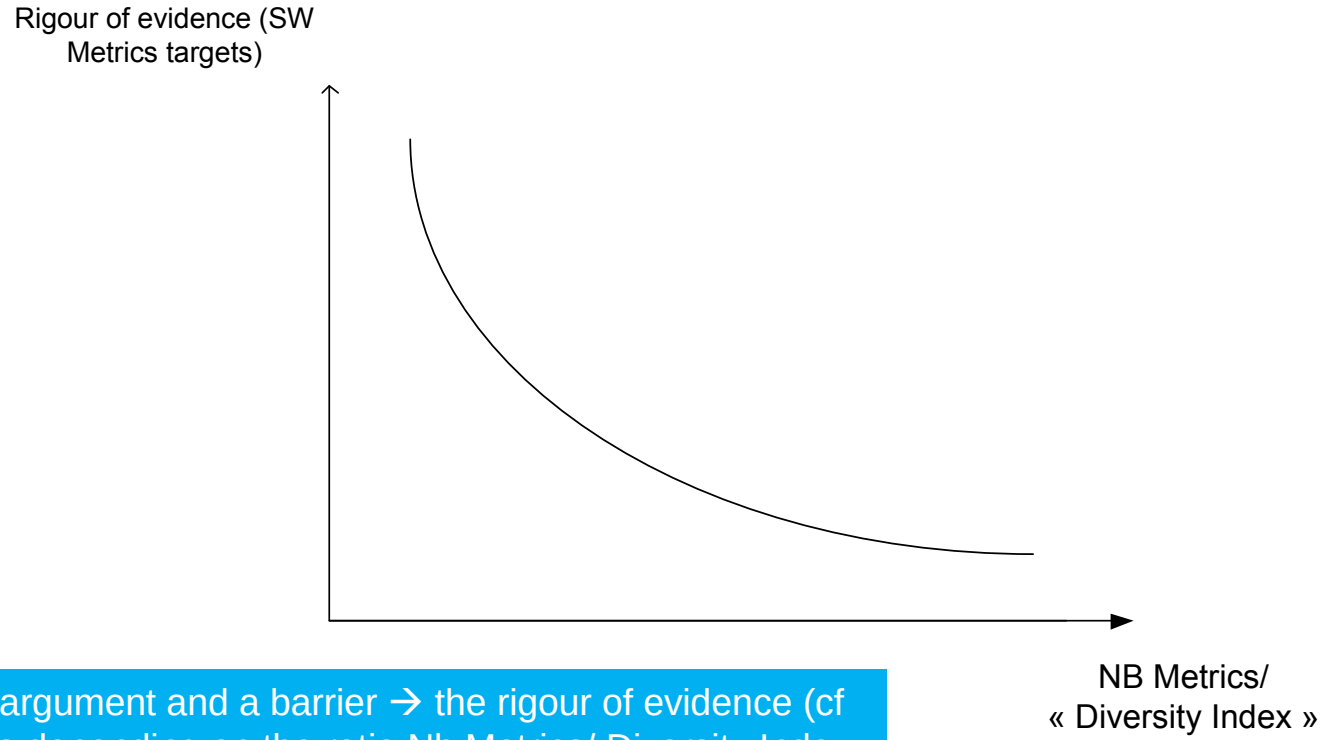
SW Safety Arguments Demonstration (example Argument G4 Counter evidence)

Step 5

Rigour of evidence:

✓A « diversity index » could be defined and computed between these SW Metrics based on « diversity » of activities/ processes natures, organisation independancy…

✓An assessment of the rigour of evidence could be performed according to the following model (for example for SW Verification → ~40 SW Metrics can be used)



Principle: For an argument and a barrier → the rigour of evidence (cf Metric threshold) is depending on the ratio Nb Metrics/ Diversity Index

THALES

Evidence rigour: SW Verification Metrics Definitions (example)

- Metrics are based on SWAL objectives related to Verification Process (SWAL4, SWAL3, SWAL2)
- Metrics are defined according to different aspects embedded in the definition of the SWAL objectives

Used for G1.2.1 Argument Evidence « B2 Approval Barrier »

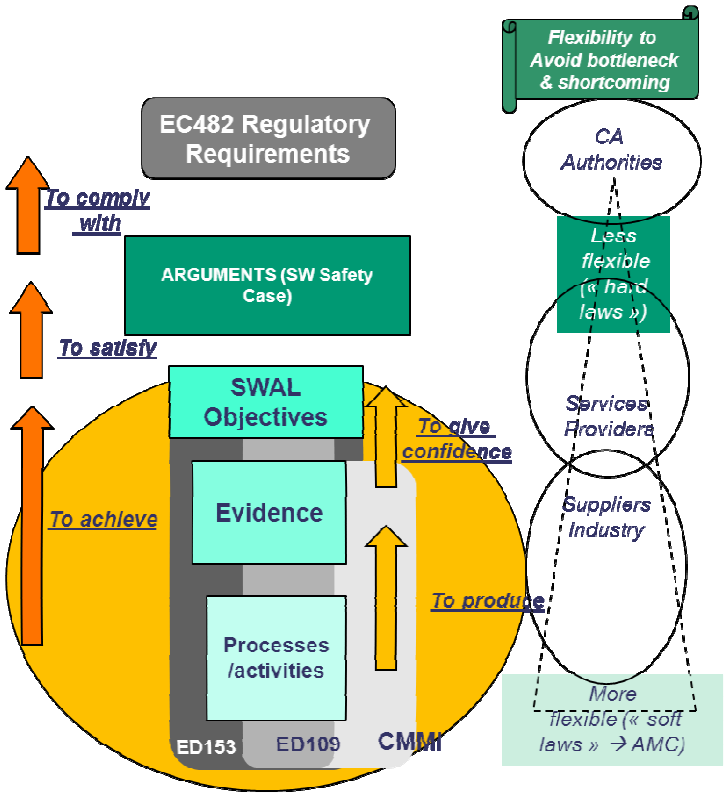
N°SWAL Objective	Definition	SWAL 2	SWAL 3	SWAL4
5.4.3	Verification of Software Requirements			
5.4.4	Integration verification			
5.4.5	**Verification of SW architectural design**			
5.4.6	**Verification of detailed design**			
5.4.9	Data verification			
5.4.10	Traceability			
5.4.11	Complexity Measures			
5.4.12	Verification of verification process results			
5.4.13	Verification of retrieval and release process			

The totality of the SWAL Objective is applicable for the corresponding SWAL level

Only a specific sub-part of the SWAL objective is applicable for SWAL 3

Only a specific sub-part of the SWAL objective is applicable for SWAL 4

CONCLUSION



Regarding the SW Argument development a structured approach is proposed by:

- **Justifying the use of SWALs objectives per argument in compliance with a SW risks model**
- **Clarifying the rôle of each process/ activity regarding the reduction of risks (ref description of the model and the respective contribution of processes/ activities for each barrier)**
- **Facilitating the scope of expected SWALs objectives evidence according to the demonstration of the claim of arguments (ref mapping Argument vs Set of SWAL objectives)**
- **Assessing the expected rigour of evidence in order to satisfy SW Safety Case (ref « diversity index »**

However there is a need to populate & validate the SW Risks Model (probably in the scope of ATM SW community?)

"…..If we were presented the options of choosing between goal-based regulation and prescriptive processes, we would in effect be caught between the devil and the deep blue sea. Prescription hampers the continual move forward in technological approach, while goal-based leaves us without suitable advice on achieving assurance….." [R. Weaver 2009 Safety Systems (the UK Safety-Critical Systems Club Newsletter)]

THALES

Thank you for your attention

THALES