MUAC SSAS Process

ES2 WS1-2013 Software Safety Assessment Workshop

7- 8 May 2013

Marinella LEONE, ASD MUAC

Morten Trier HANSEN, ENG MUAC

EUROCONTROL

member of FABEC

Overview

- SSAS procedure in MUAC SMS:
  - Overview of SSAS central process and sub-processes
- Method for SW Assurance in projects/developments
  - Process and tools (AMC) adopted for projects/developments @MUAC and between MUAC and manufactures
- Method for SW Assurance in maintenance:
  - Maintenance process with SW assurance as an integrated set of activities
- Conclusions

SSAS procedure in MUAC SMS

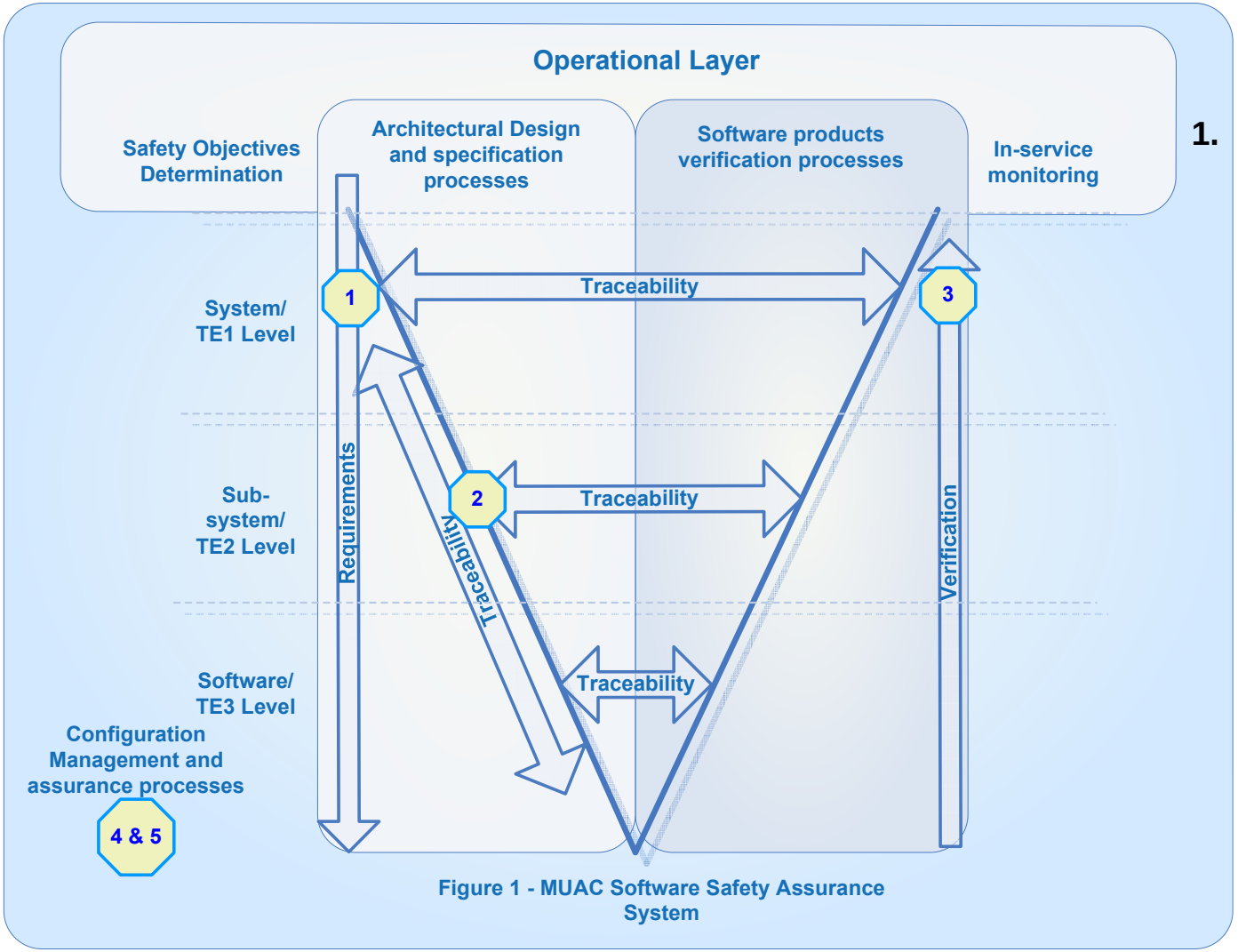
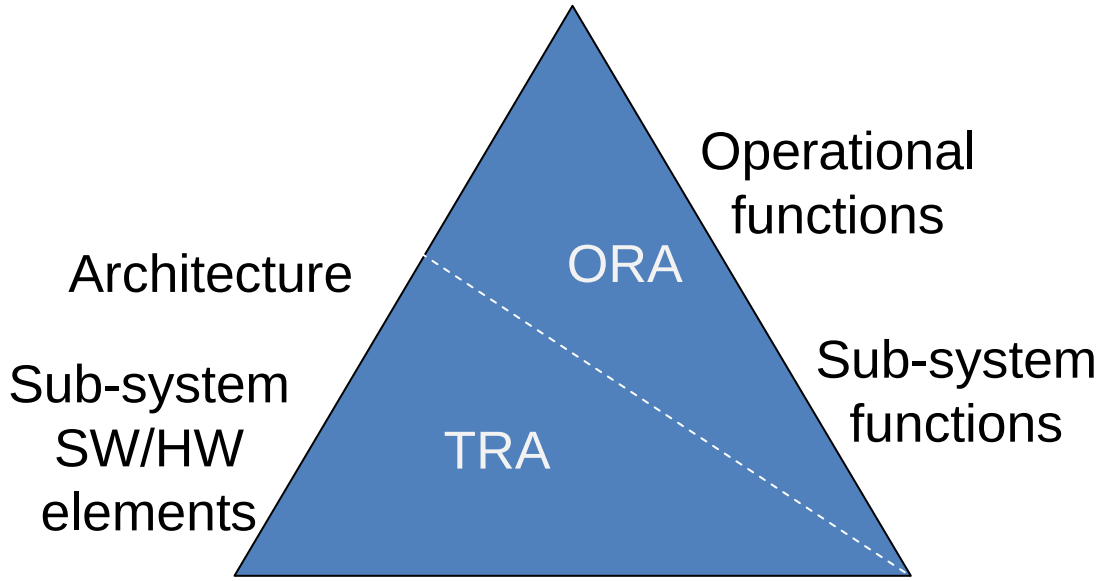


Figure 1 - MUAC Software Safety Assurance System

1. **System or SW safety requirements** are derived → SW requirements are specified

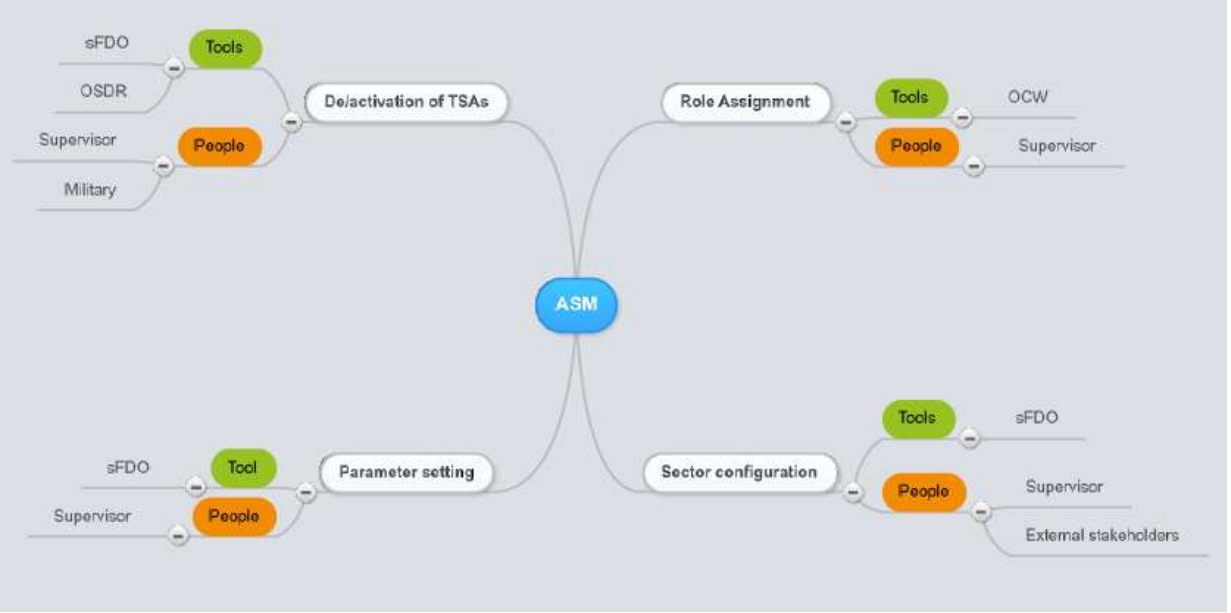
1. System and SW safety requirements

- **Operational Risk Assessment** → Functional risk analysis and mitigation process to derive SWAL requirements as well as functional and availability requirements
- **Technical Risk Assessment** → drive requirements and keep trace of procedures to recover from failures of sub-systems



Operational Risk Analysis

- Operational Risk assessment is constructed on the basis of Functional failure analysis for operational service functions:
  - Allocation of SWAL to interfacing sub-systems according to severity and likelihood
  - Requirements are propagated to feeding sub-systems



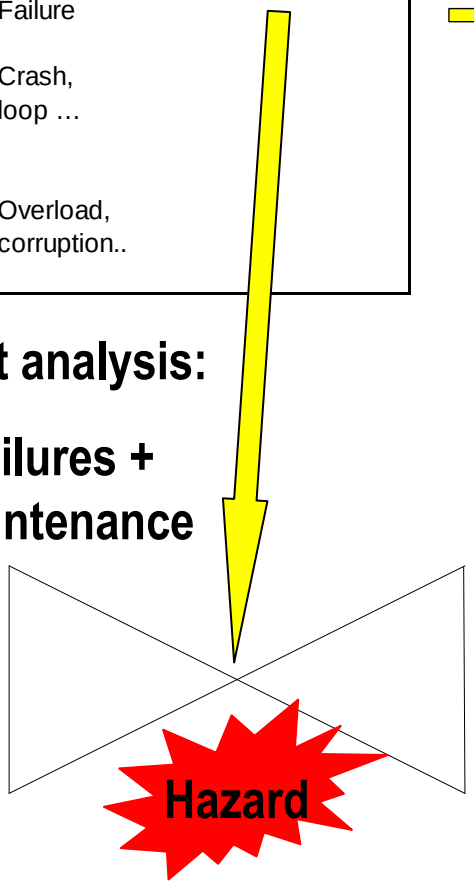
Technical Risk Assessment (TRA)

FMEA

Component	Failure mode	TE	OE	MA
<HW>	Failure			
…				
<SW>	Crash, loop …			
…				
<interfaces>	Overload, corruption..			
…				

MAEA

MA	Proc.	When	TE	OE
Replace	MPR	Night		
<corrective, e.g. replace HW>				
<adaptive, e.g. install release>				
<preventive, e.g. health check>				



FMEA: Failure mode effect analysis:

- **Assess effects of all failures + define a corrective maintenance activity**

MAEA: Maintenance activity effect analysis:

- **Assess effects of all maintenance activities**

SSAS procedure in MUAC SMS

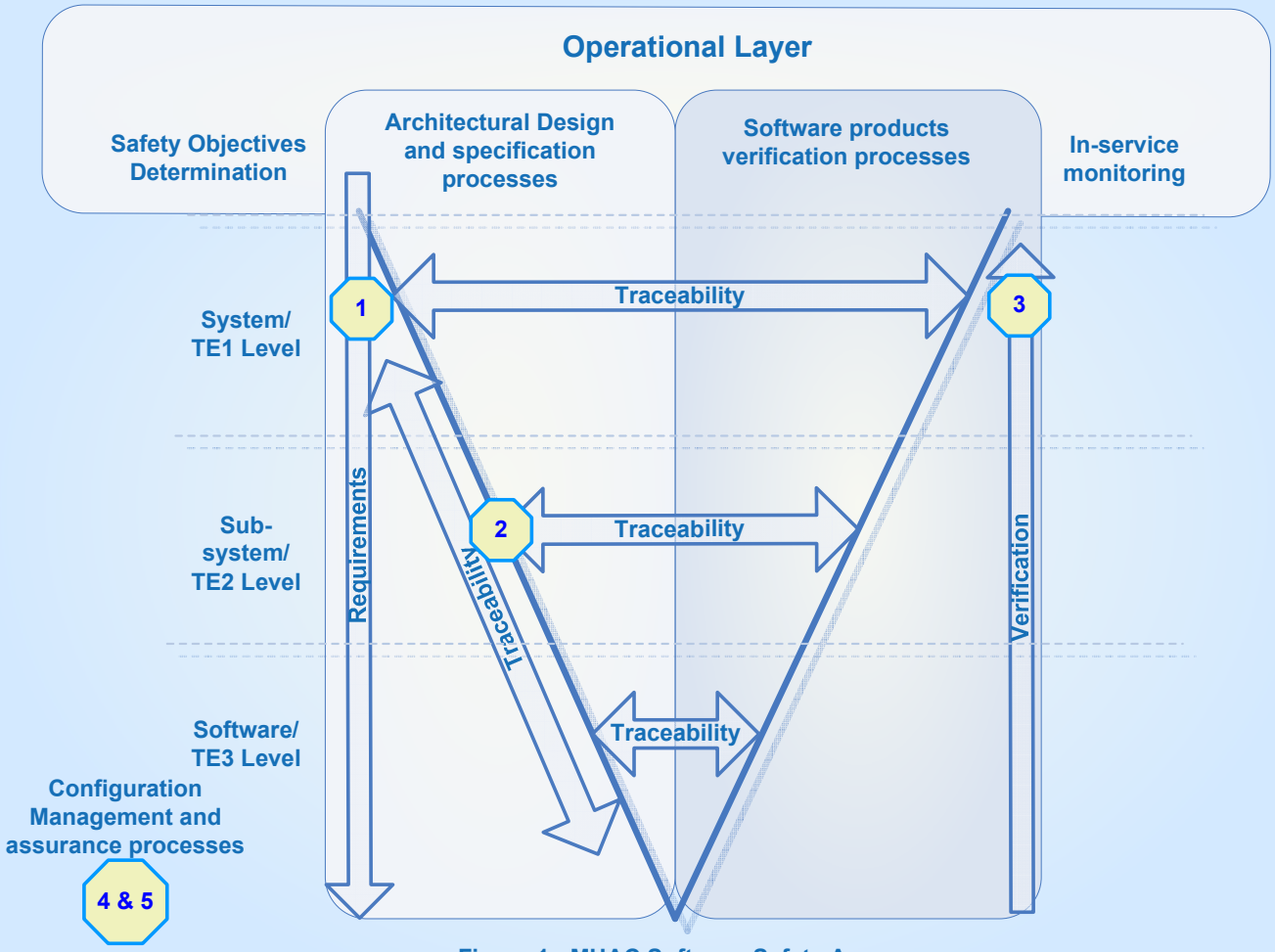


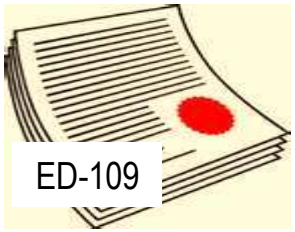
Figure 1 - MUAC Software Safety Assurance System

1. **System or SW safety requirements** are derived → SW requirements are specified
2. **Traceability** through the relevant system architectural levels down to the design and with verification records
3. **SW** satisfies requirement to **level of confidence** equivalent to criticality of software
4. **Configuration management** processes in place
5. **Relevant stakeholders** are involved

Overview

- SSAS procedure in MUAC SMS:
  - Overview of SSAS central process and sub-processes.
- **Method for SW Assurance in projects/developments**
  - **Process and tools (AMC) adopted for projects/developments @MUAC and between MUAC and manufactures**
- Method for SW Assurance in maintenance:
  - Maintenance process with SW assurance as an integrated set of activities
- Conclusions

Derivation of Tender Safety Requirements



- Coming from SIL (IEC61508) and FHA/FTA or RBD for apportionment of requirements
- Moving to SWAL from Functional failure analysis:
  - Allocation to interfacing system according to severity and likelihood
  - Requirement propagation to feeding sub-systems
- Easy in principle to change approach at the beginning of a new project. However initial effort to align expectations of stakeholders and some lessons learned are lost

C-SOW Requirements

[SOW - 647] The Contractor **shall**:

- adopt the procedures, guidance and templates of the Customer's SMS for the following activities, as required:
  - Safety Management Plan (SMP).
  - Preliminary System Safety Assessment (PSSA).
  - System Safety Assessment (SSA).
  - System Safety Case (SSC).
- adopt the EUROCAE Guidelines ED-153 for the development and/or selection of all software deliverables, or demonstrate that the Contractor's method of software development and/or selection is fully consistent with ED-153.
- adopt the international standard IEC61508 (Part 2; particularly Tables A.16 to A.18 and B.1 to B.5) for the development and/or selection of all hardware deliverables, or demonstrate that the Contractor's method of hardware development and/or selection is fully consistent with IEC61508. This is to ensure the hardware is consistent with the requirements for Mean Time Between Failures (MTBFs) and software integrity.
- adopt the Regulation (EC) No 552/2004 dated 10 March 2004 as amended by Regulation (EC) No 1070/2009 (or subsequent version/ requirements applicable at time of PA), safety part.

[SOW - 823] The Contractor **shall** comply with the SWAL-3 as required by the compliance tables.

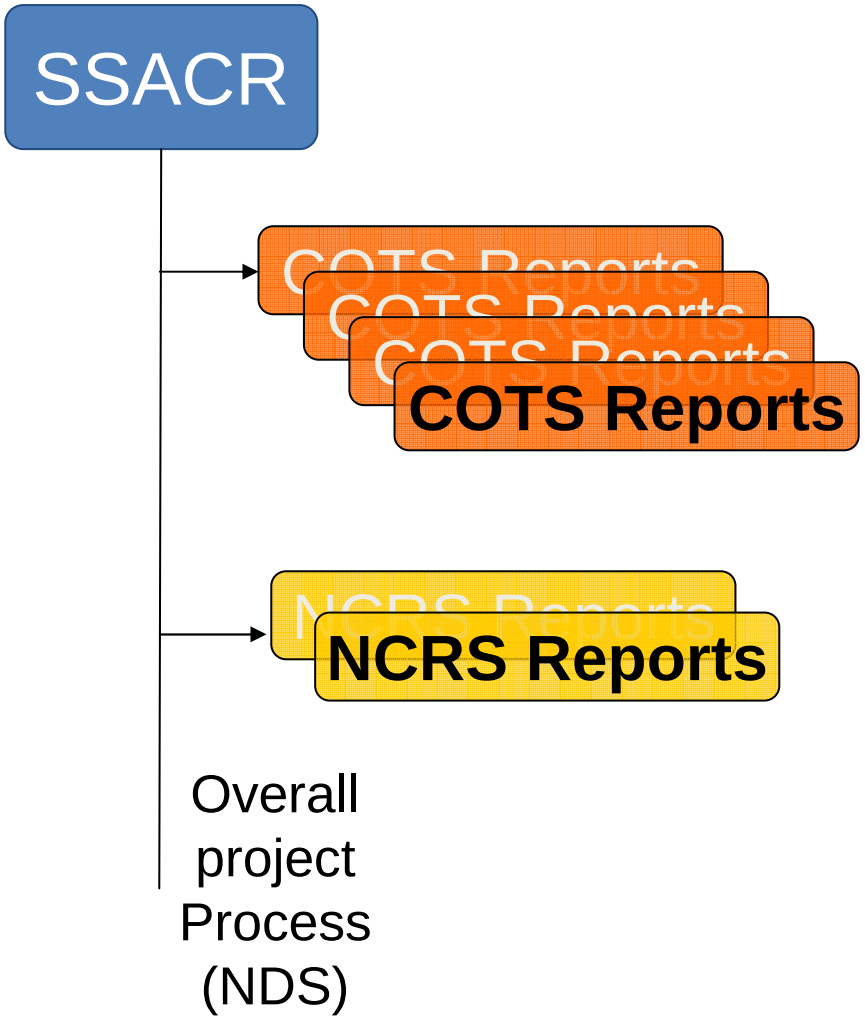
Ed-482 Compliance approach

[SOW - 665] Compliance to the DSRs **shall** be demonstrated as follows:

- for Software DSRs: SWAL compliance via individual compliance statements with supporting evidence for each applicable Objective from the compliance tables in ED-153, as follows:
    - For **Newly Developed Software (NDS)**, the Contractor shall show compliance to SWAL 3 objectives in the tables from Sections 3 to 7.1 with the following structure:
        a) If all NDS are developed by the same supplier and the same process is applied, only one set of SWAL compliance tables (from Section 3 to Section 7.1) shall be provided by the Contractor.
        b) If any NDS is developed by a different supplier or according to a different process, a separate set of SWAL compliance tables (from Section 3 to Section 7.1) shall be provided by the Contractor for that software.
    - For **Commercially available Off-The-Shelf (COTS)**, the Contractor shall show compliance to SWAL objectives in the tables from Section 3 and Section 7.2 with the following structure:
        a) Separate sets of SWAL compliance tables (i.e. from Section 3 and Section 7.2) shall be provided for each COTS item.

        Note: Compliance in Section 3 can be demonstrated via reference to the NDS Section 3 tables, if the evidence provided in those tables have accounted for the COTS. (Section 3 provides objectives relating to overall project initiation, planning and safety, in which it would be valid to include COTS evidence).
    - For **Non-COTS Reused Software (NCRS)**, all the SWAL 3 objectives in the compliance tables from Sections 3 to 7.2 shall be used, thus including both development & COTS tables. This is because a properly substantiated combination of the NDS and COTS approaches is acceptable to the Customer when demonstrating SWAL 3 compliance; i.e. a lack of development evidence for the NCRS can be mitigated by COTS evidence and vice versa. The following structure shall be used:
        a) If evidence for NCRS is provided from the same supplier and follows the same process, only one set of compliance tables shall be provided by the Contractor.
        b) If any NCRS is developed by a different supplier or following a different process then separate SWAL compliance tables will be provided by the Contractor for that software.

Compliance Reports

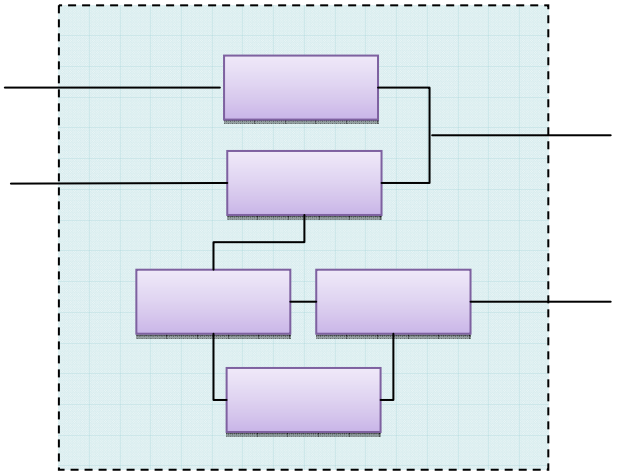


- Ability to meet objectives?
  - CRs from start
- Discrepancy of processes?
  - Company processes
  - ED-153 expectation table
- Quality of documents?
  - Constructed assurance
- In-service history?
  - Monitoring method
- Unintended (unspecified/unused/unneeded) functionality?
  - Identify/assess

Component definition

- **NDS** – possible to design/define the correct decomposition; appropriate level of detail for SWAL analysis (SRS)?
- **NCRS** - Existing software might not be modular or might be decomposed in too low level components

- Creating logical CSCI level to abstract from detail?
- Artificial documentation structure not reflected by software packaging. Difficult/redundant to redefine interfaces at logical level that are covered by low level components (in specifications and tests)



SSS & SRS

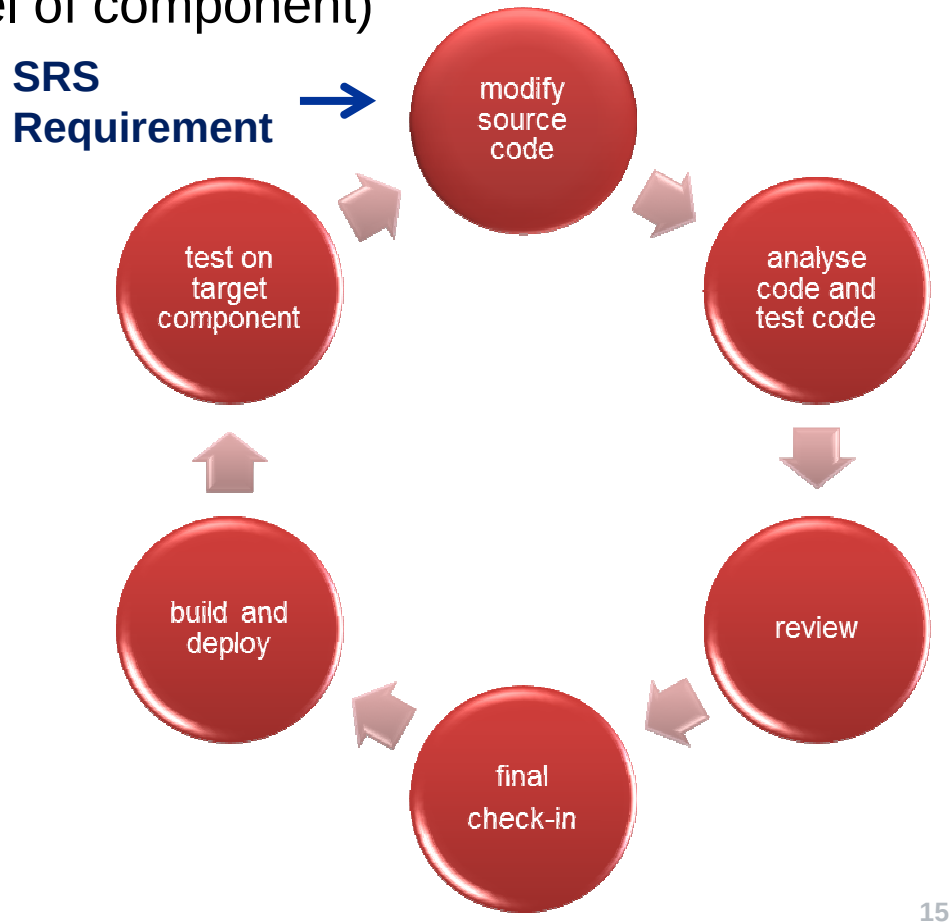
- Low level SSS and poor SRS?
- Facing fear for “explosion” of SW requirements and tests
- Sometimes missing in the SRS (startup management, shutdown management, logic to transform inputs into outputs, mode of operations, error handling, boundary condition, etc…) directly incorporated in design documentation (e.g. algorithm)

- No need for SRSs? Important when different actors involved and criticality/complexity of the system
- Knowledge gap not reconciled between system and software engineers?

Approach for changes to legacy

- **NCRS** - No SRS exist for some legacy software (often just SSS, maybe SRS at lower level of component)
- SRS that introduce change are refined up to the level that the logic/algorithms supporting the corresponding functions can be tested

Continuous Integration during SW development for NCRS

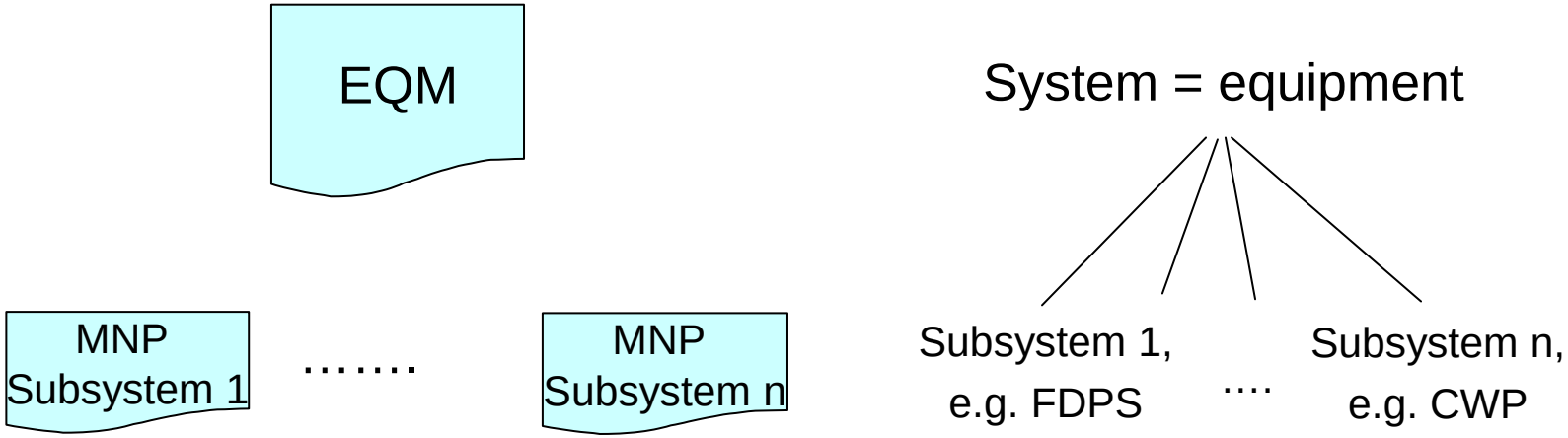


Overview

- SSAS procedure in MUAC SMS:
  - Overview of SSAS central process and sub-processes.
- Method for SW Assurance in projects/developments
  - Process and tools (AMC) adopted for projects/developments @MUAC and between ANSP and manufactures
- **Method for SW Assurance in maintenance:**
  - **Maintenance process with SW assurance as an integrated set of activities**
- Conclusions

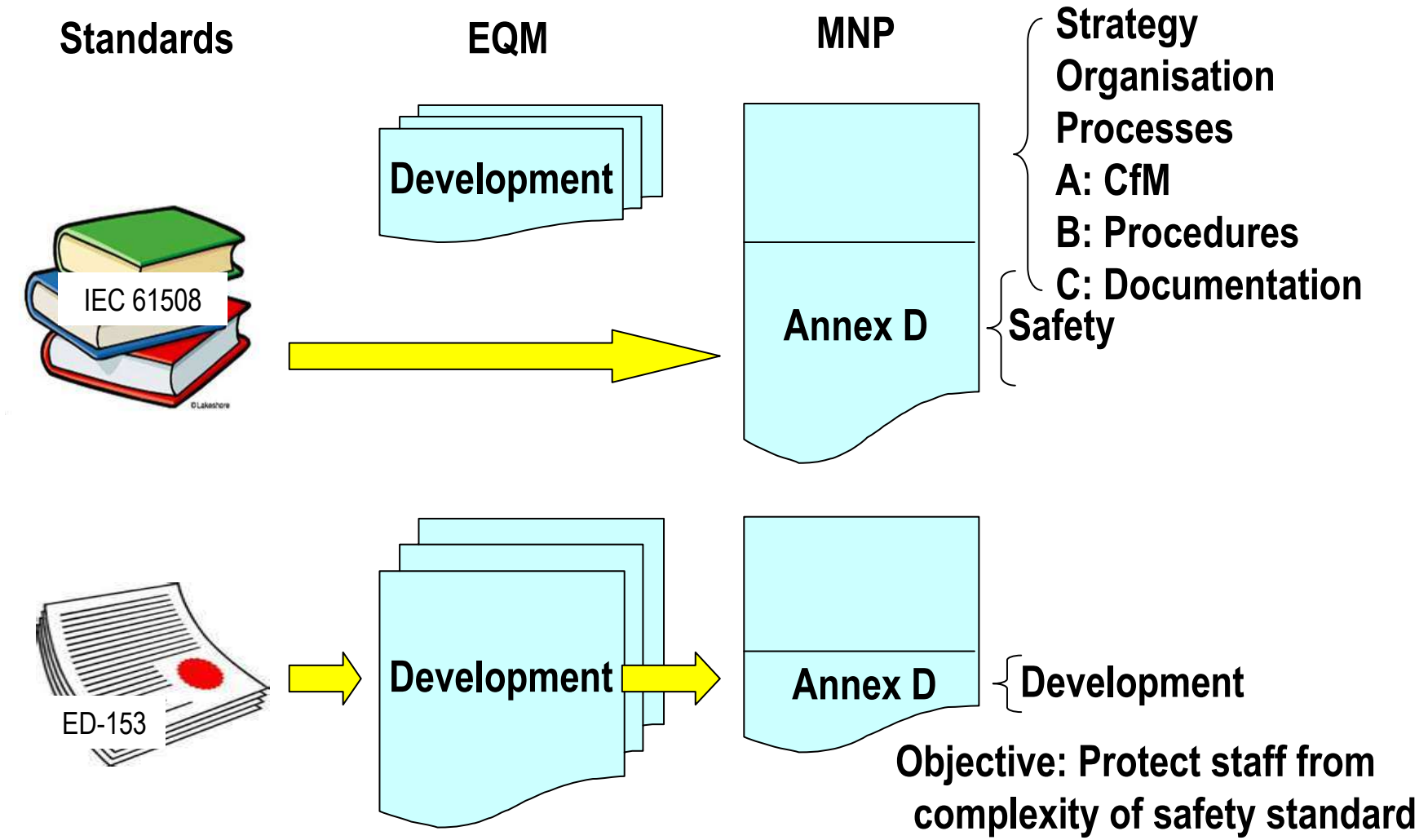
Engineering Quality Manual (EQM)

- Maintenance is easy:
  - No PMP, CMP, SDP, RMP, SVP, … - just:



- But not so easy anyway:
  - Process changes have large consequences
  - One process needs to fit all

Safety in EQM



ED-153 example: Requirements

ED-153

What does it mean ?

EQM translation

ED-153					Interpretation		Implementation			
							Maintenance			
Obj No	Obj Title/Topic	Requirements	SWAL3	SWAL4	Clarification /remarks	Evidence	Process	Detail	Evidence	Explanation
4.3.4	SW requirements analysis	Annex A Section A.3.3 The developer shall 4.3.4.1 establish and document software requirements, using software requirements standards/rules as defined per Objectives 4.3.9 & 4.3.10.	y	y		Documented software requirements.	EQM.ATM.DEV-10	SuRA SoRA	TE2.<subs>.AND.SSS TE3.<subs>.AND.SRS	Software requirements may be documented as part of the subsystem requirements document - ther requirement is on existence of the requirements, not on a specific document.
		The Soft • specify th … accuracy, timing performances, so… …ware, robustness to abnormal operating conditions, overload tolerance. • be complete and correct; • comply with the System Requirements; • an identification of the configuration/adaptation data range.	y	y		Documented requirements with scope as described in req. Traceability to higher level reqs to demonstrate completeness.	EQM.ATM.DEV-10	SuRA SoRA	TE2.<subs>.AND.SSS TE3.<subs>.AND.SRS Traceability to higher level requirements to show completeness.	

Obj 4.3.4

EQM example: Requirements

Service & Maintainability

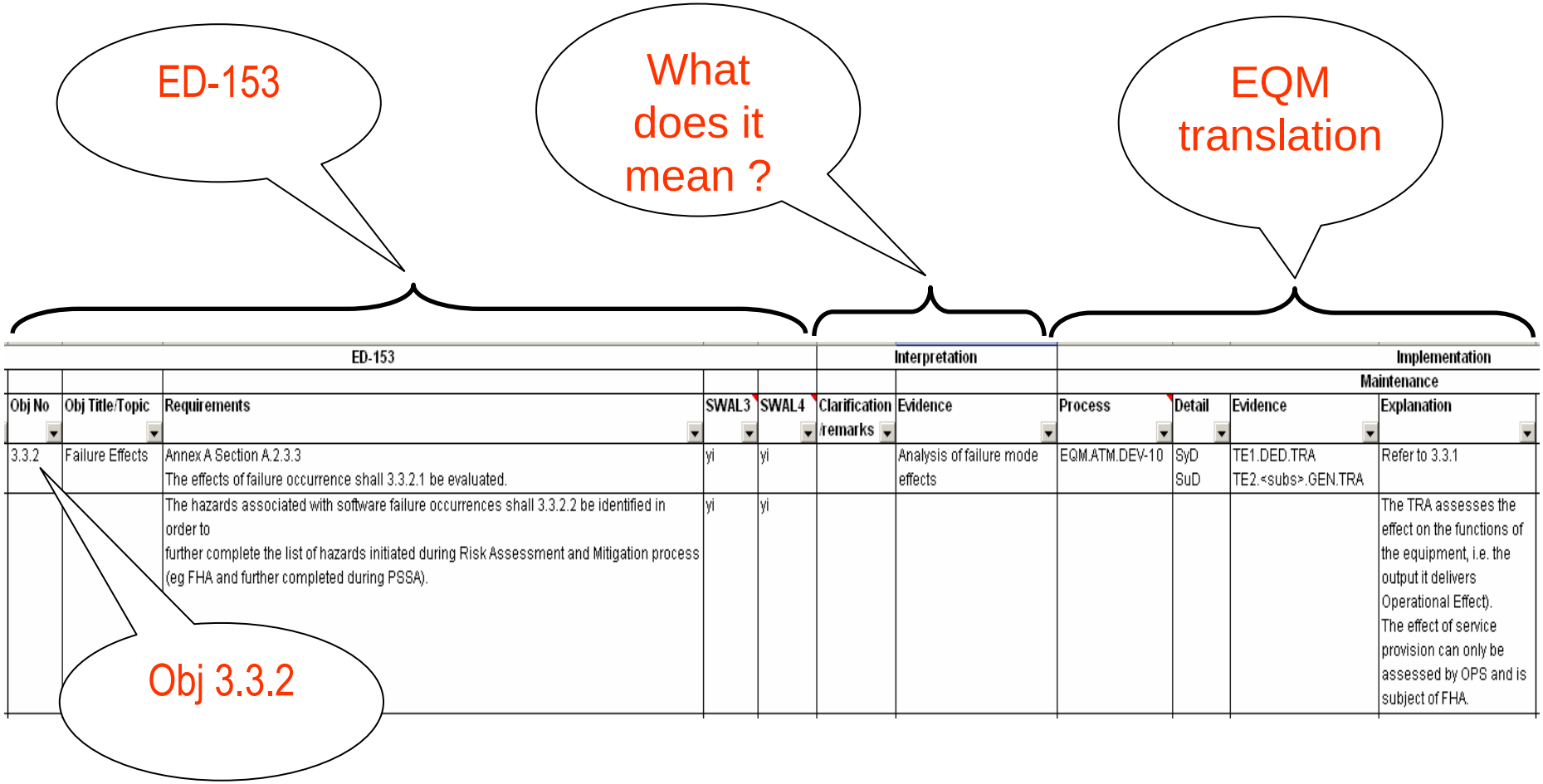
Id	Requirement	EQM reference	S&M	SWAL 4	SWAL 3	ED-153 reference
SuRA-1	All subsystem requirements must be documented	TE2 SSS	X	X	X	Obj 4.3.4 Obj 4.3.12
	Subsystem requirements must specify: - functional behaviour - capacity - accuracy - timing performances - software resource usage and margins (e.g. memory, CPU load, disk space, communication bandwidth, ...) on target hardware - adaptation/configuration data ranges and interface boundaries - robustness to abnormal operating conditions - overload tolerance	TE2 SSS	X	X		Obj 4.3.4 Obj 4.3.13
	Subsystem requirements must specify hardware requirements, e.g. MTBF and MTTR, for maintainability.	TE2 SSS	X			
	Subsystem requirements review must verify that ements are: - c nd complete - cons - feasibl - unambig - traceab ant	RID	X	X	X	Obj 5.4.3
	Subsy requir (e.g. W rules	RID	X	X	X	Obj 5.4.3 i
	All requir 1 level) must be trac	TE2 SSS (traces)	X	X	X	Obj 4.3.15 a Obj 5.4.10 a
	Traceability must be	RID	X	X	X	Obj 5.4.12

Obj 4.3.4

Obj 4.3.4

Subsystem Requirements Analysis (SuRA)

ED-153 example: Failure analysis



ED-153					Interpretation		Implementation			
							Maintenance			
Obj No	Obj Title/Topic	Requirements	SWAL3	SWAL4	Clarification /remarks	Evidence	Process	Detail	Evidence	Explanation
3.3.2	Failure Effects	Annex A Section A.2.3.3 The effects of failure occurrence shall 3.3.2.1 be evaluated.	yi	yi		Analysis of failure mode effects	EQM.ATM.DEV-10	SyD SuD	TE1.DED.TRA TE2.<subs>.GEN.TRA	Refer to 3.3.1
		The hazards associated with software failure occurrences shall 3.3.2.2 be identified in order to further complete the list of hazards initiated during Risk Assessment and Mitigation process (eg FHA and further completed during PSSA).	yi	yi						The TRA assesses the effect on the functions of the equipment, i.e. the output it delivers Operational Effect). The effect of service provision can only be assessed by OPS and is subject of FHA.

EQM example: Failure analysis

Id	Requirement	EQM reference	S&M	SWAL 4	SWAL 3	ED-153 reference
SuD-1	Subsystem design must be reviewed against architectural design constraints and design standards	RID	X	X	X	Obj 5.4.5 d
	Algorithms must be described.	TE2 SSDD	X	X	X	Obj 4.3.4
	Subsystem design must describe the use, version and configuration of COTS tools.	TE2 SSDD	X	X	X	Obj 7.2.1 Obj 7.2.4 Obj 7.2.8 Obj 7.2.10
SuD-2	Effect of failure of HW, SW and interfaces must be described.	TE2 T			X	Obj 3.1.5 Obj 3.3.1 Obj 3.3.2
	Effect of failures of COTS tools ibed.	TE2 TRA		X	X	Obj 3.3.2
	Effects of undesired COT mitigated by safety req	TE2 TRA TE2 SSS		X	X	Obj 7.2.6
	COTS tool performance or stability	TE2 SSDD			X	Obj 7.2.6
	Effect of release installati	T			X	Obj 4.5.4
	Subsystem test description must e mode behaviour.	T			X	Obj 5.4.3 e
SuD-3	Software must be broken down into software items.	TE2 SSDD			X	Obj 4.3.5
	Software requirements must be allocated to software items.	TE2 SSDD			X	Obj 4.3.15 b
	Software item interfaces must be described.	TE2 SSDD			X	Obj 3.1.1

Obj 3.3.2

Subsystem Design (SuD)

Obj 3.3.2

EQM development process

Phase applicability depends on SWAL:

Phase	System Requirements Analysis (SyRA)	System Design (SyD)	Subsystem Requirements Analysis (SuRA)	Subsystem Design (SuD)	Software Requirements Analysis (SoRA)	Software Design (SoD)	Coding and Unit Testing (CUT)	Software Integration (SoI)	Software Verification (SoV)	Subsystem Integration (SuI)	Subsystem Verification (SuV)	System Integration[2] (SyI)	System Verification (SyV)
Phase applicability	SWAL 4	SWAL 4	SWAL 4	SWAL 4			SWAL 4			SWAL 4	SWAL 4	SWAL 4	SWAL 4
	SWAL 3	SWAL 3	SWAL	SWAL 3	SWAL 3		SWAL 3		SWAL 3	SWAL 3	SWAL 3	SWAL 3	SWAL 3
	SWAL 2	SWAL 2	SW	SWAL 2	WAL 2	SWAL 2	SWAL 2	SWAL 2	SWAL 2	SWAL 2	SWAL 2	SWAL 2	SWAL 2
Activities	Verify completeness of RfC. Review against design constraints	Specify system design. Identify affecte subsystems Specify	ify ystem irements. ecify ubsystem nterfaces. race subsystem ements to ts.	Design subsystem architecture (HW, SW, COTS). Trace design units to subsystem requirements. Perform technic risk analysis. Specify failu mode testing Decompose software into software items (SWAL 3).	fy software od re nts	Decompose software items into software units. Specify software	Develop software. Perform code analysis Perform code review	Integrate software units.	Plan software verification. Integrate software items. Execute software verification.	Plan subsystem verification. Accept and integrate subcontractor deliverables incl. COTS. Integrate software and hardware.	Execute subsystem verification. Verify SWAL compliance	Integrate subsystem releases.	Specify test descriptions. Plan baseline verification. Install subsystem releases in TDS and test. Install subsystem releases in ONL. Execute ONL verification. Backout subsystem releases.
Inputs			DD 1 MIDD	TE2 SSS PRB(s) Design standard	TE2 SSDD		TE3 SRS TE3 SDD Coding standard	TE3 SDD	TE3 STD TE3 STP	TE2 SSS TE2 STD	TE2 STD TE2 STP	TE1 MIDD	RfCs TE1 SSS TE2 SVDs,STRs
Outputs	Authorize rejected RfC TE1 SSS TE1 MIDD	TE1 SSDD TE1 MIDD TE1 TRA	TE2 SSS TE2 STD	TE2 SSDD TE2 TRA TE2 STD[5]	TE2 SSDD TE3 SRS TE3 STD	TE3 SDD	Source code	TE3 STR	TE3 STP TE3 STR	TE2 STP TE2 STR	TE2 SVD TE2 STR	TE1 STR	TE1 STD[6] TE1 STP TRR report TE1 STR SRN MSIR MIBI
			MNP scope										

Subsystem Requirements Analysis (SuRA)

Subsystem Design (SuD)

MNP: EQM compliance matrix

- **Completed as part of each MNP for each CI**
- **No “cryptic” requirements**
- **Fulfillment of each requirement to be justified with reference to evidence**

Req. Id	Subject	EQM	SWAL 4	SWAL 3	Implementation	Compliant (Y/N)
SuRA-1	Subsystem requirements	X	X	X		
SuRA-2	Subsystem description		X			
SuD-1	Subsystem design	X				
SuD-2	Failure analysis					
SuD-3	Software decomposition					
SuD-4	Design rationales					
SuD-5	Design standards			X		
SoRA-1	Software requirements			X		
SoRA-2	Software test description			X		
SoD-1	Software design				3 and 4	
CUT-1	Coding standards					
SoI-1	Software integration				4	
SoV-1	Software test plan					
SoV-2	Software test report					
SuI-1	Subsystem test plan	X				
SuI-2	Subcontractor deliverables					
SuI-3	Subsystem integration			X		
SuV-1	Subsystem test report	X	X	X		
SuV-2	Subsystem SWAL compliance		X	X		
Tools-1	Tools confidence		X	X		
Tools-2	Development environment	X	X	X		
COTS-1	Problem reporting		X	X		
COTS-2	Service experience		X	X		
COTS-3	Reputable vendors	X				

Subsystem Requirements Analysis: SuRA-1

Subsystem Design SuD-2

Development process summary

SWAL 4:

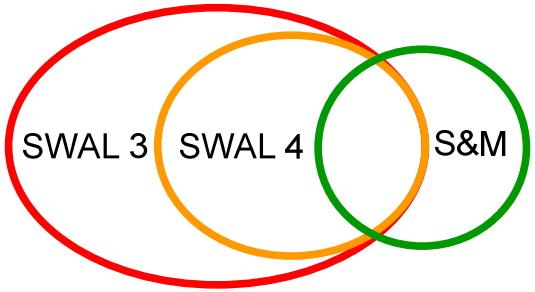
- **Subsystem requirements, review, traceability**
- **Subsystem design**
- **Subsystem tests, traceability**
- **Systematic failure mode analysis**
- **Subcontractor deliverable review/acceptance (SWAL)**
- **Development tools identification**
- **Tools and COTS assurance**

SWAL 3 (in addition to SWAL 4):

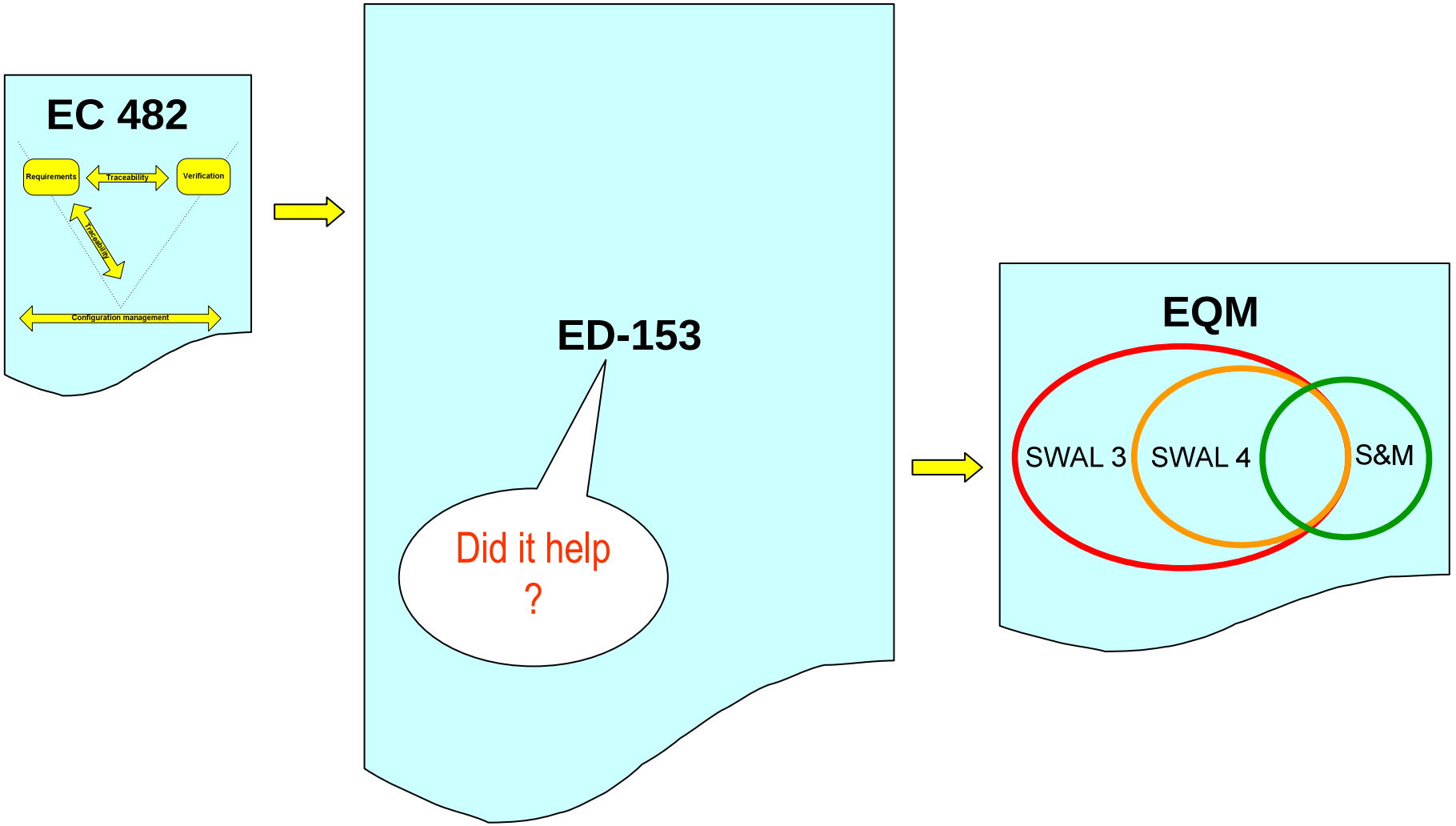
- **SW decomposition, SW item requirements, review, traceability**
- **SW item tests, traceability**
- **Design choices/rationales + standards**
- **Failure mode testing**

Service & Maintainability :

- **Coding standards**
- **COTS from reputable vendors**



Reflection over EQM extension



Ongoing: Security extensions

Phase	System Requirements Analysis (SyRA)	System Design (SyD)	Subsystem Requirements Analysis (SuRA)	Subsystem Design (SuD)	Software Requirements Analysis (SoRA)	Software Design (SoD)	Coding and Unit Testing (CUT)	Software Integration (SoI)	Software Verification (SoV)	Subsystem Integration (SuI)	Subsystem Verification (SuV)	System Integration[2] (SyI)	System Verification (SyV)
Phase applicability	**SWAL 4**	**SWAL 4**	**SWAL 4**	**SWAL 4**			**SWAL 4**			**SWAL 4**	**SWAL 4**	**SWAL 4**	**SWAL 4**
	SWAL 3	**SWAL 3**	**SWAL 3**	**SWAL 3**	**SWAL 3**		**SWAL 3**		**SWAL 3**	**SWAL 3**	**SWAL 3**	**SWAL 3**	**SWAL 3**
	SWAL 2	**SWAL 2**		**SWAL 2**	**SWAL 2**	**SWAL 2**	**SWAL 2**	**SWAL 2**	**SWAL 2**	**SWAL 2**	**SWAL 2**	**SWAL 2**	**SWAL 2**
Activities	Verify completeness RfC. Review ag design constraints. Assign safety and security type. Specify system requirements. Specify traceability to regulatory requirements.	Trace element require Perfor safety **secur** assessment.	requirements. Specify subsystem test description.	Perfo risk a Speci mode te Decompose software into software items (SWAL 3).	Specify software items and interfaces. Trace software	Decompose software items into software units.	Develop software. Perform code analysis Perform code review	Integrate software units.	Plan software verification. Integrate software items. Execute software verification.	Plan subsystem verification. Accept and integrate subcontractor deliverables incl. COTS. Integrate software and hardware.	Execute subsystem verification. Verify SWAL compliance **Software handover**	Integrate subsystem releases.	Specify test descriptions. Plan baseline verification. Install subsystem releases in TDS and test. Install subsystem releases in ONL. Execute ONL verification. Backout subsystem releases.
Inputs	RfC(s)	TE1 SSS TE1 SSDD (APC[4]) TE1 MIDD	TE1 SSS TE1 SSDD TE1 MIDD	TE2 SSS PRB(s) Design standard	TE2 SSS TE2 SSDD	TE3 SRS	TE3 SRS TE3 SDD Coding standard **Secure coding standard**	TE3 SDD	TE TE3			E1 MIDD	RfCs TE1 SSS TE2 SVDs,STRs
Outputs	Authorized or rejected RfC TE1 SSS TE1 MIDD	TE1 SSS[4] TE1 SSDD TE1 MIDD TE1 TRA	TE2 SSS TE2 STD	TE2 SSDD TE2 TRA TE2 STD[5]	TE2 SSDD TE3 SRS TE3 STD	TE3 SDD	Source code			TE2 STP TE2 STR	TE2 SVD TE2 STR **Virus scan report** **Nessus scan report**	TE1 STR	TE1 STD[6] TE1 STP TRR report TE1 STR SRN MSIR MIBI **Penetration test report**
			MNP scope										

Security assessment

Secure coding

Virus scanning

Hardening test report

Overview

- SSAS procedure in MUAC SMS:
  - Overview of SSAS central process and sub-processes.
- Method for SW Assurance in projects/developments
  - Process and tools (AMC) adopted for projects/developments @MUAC and between ANSP and manufactures
- Method for SW Assurance in maintenance:
  - Maintenance process with SW assurance as an integrated set of activities
- **Conclusions**

Conclusion 1

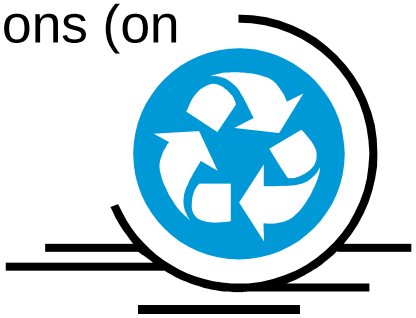
- Difference between MUAC and suppliers' expectations for development processes and tools (AMC) application in projects
- Difference of development processes and compliance approaches for recent and old legacy systems during maintenance @MUAC
- Involvement/understanding of stakeholders about SSAS application
- Compliance for COTS and legacy – Problems of in-service experience monitoring in evolving configuration and used environment
- Unintended functions (potential customization and configurations for NCRS and COTS)

Conclusion 2

- Component definition (SWAL3)
  - System decomposition (where is what I need? What should I analyse? I should get there… long way and many requirements I need an iterative method to focus in the detail/review)
- SRS completeness and correctness:
  - Design documents cover the behaviour and input/output… usefulness not seen
  - Gap between system engineer terminology and software engineer terminology
  - System-software engineer is the same = usefulness?
- Identification of pitfalls after selection of AMC (need guidance on available options and limitations)
  - E.g. Ed-153 – Depth of design transparency

Conclusion 3

- SW Safety Requirements? Where do they come from? Forgot? Are we focusing just on quality process?
- Invest on Software Safety Requirements derivation and implementation analysis:
  - Analysis of DSR from RA and mapping in SRS/design
  - SW Safety Assessment Techniques, e.g. SW FMEA and SHARD
  - HF-Safety Techniques, e.g. HMI design assessment
  - Safety impact assessment of unspecified functions (on the table and in validation)
  - Review of Risk Assessments and SRS from analysis of occurrences



SQS, SSQ, QSS ?

- Management process evolution:
  - EC 1035/2011, sec 3.2: “Air navigation service providers may integrate safety, security and quality management systems into their management system” – that’s what we want.
  - Safety and Security is about management of specific risks
  - Quality defines and assures the overall process

Thank you for your attention

Questions?

marinella.leone@eurocontrol.int
morten-trier.hansen@eurocontrol.int

EUROCONTROL

member of FABEC