OSS and ASPICE: like water and oil?

How aptly scoped ASPICE assessments can contribute to OSS qualification in FuSa context

21° Automotive SPIN Italia Workshop

30/05/2023
V1R0
Carlo Donzella – exida development SRL

About the Presenter

Carlo Donzella - CEO and co-founder of exida development & exida engineering

Mail: carlo.donzella@exida-dev.com

SPICE Competent Assessor
Certified Functional Safety Expert (CFSE)
Cyber Security Practitioner (CSP)

Projects / Special Interest

Supports automotive customers worldwide in optimizing efforts and developing common procedures to satisfy ASPICE, ISO 26262 and ISO/SAE 21434 models.

Member of the SPICE HW PRM/PAM Working Group.

Member of the Board of Automotive SPIN Italia.

THE PROBLEM

1

(FL)OSS: quality SW, but… only “community assured and enforced”, no objectivity, no evidence, purely “reputation-based”

2

(A)SPICE: a highly regulated assessment model, but… at what cost a superior capability “proven” quality?

3

The respective communities, apparently, do not share many concepts and values…

4

On a second thought, however, beyond actual differences, there are many misunderstandings; once dispelled a fruitful collaboration may start

MISUNDERSTANDINGS: WHAT SPICE REALLY **IS**

- (A)SPICE is a (capability) assessment model
- based on a measurement framework
- that rates living processes
- through demonstrable evidences

… AND WHAT SPICE DEFINITELY IS ***NOT***

- (A)SPICE is NOT a (technical) development model
- based on engineering practices
- that assures quality of work products
- through elaborated verification checklists

(A)SPICE IS ALL ABOUT ASSESSMENTS

- (A)SPICE is complex and *en route* to become even more complex in the next versions that will include currently scattered extensions (*Guidelines, Plug-ins, etc…*)
- Assessments are highly regulated according to both basic SPICE (ISO 33000) and to extra ASPICE requirements
- Still, it remains an *extremely flexible model* that can be adapted to *extremely different projects* thanks to the definition of the assessment **scope**

SCOPING IS (ALMOST) EVERYTHING

- The vast majority of ASPICE assessments are driven by OEMs’ compliance requests and are *shaped* (i.e. *scoped*) according to their needs of supplier control
- However, it is possible to dramatically change their *scope* to serve different purposes *while remaining compliant*, with no need of regulatory changes
- *Scope* is primarily about the choice of processes and the targeted capability level, and by identifying the boundary of the project

SCOPING in Automotive SPICE

In the automotive context, the “traditional” **A**SPICE assessment is conceived of with the 16 processes of the so-called *VDA-scope* and up to CL3

However, even within the **A**SPICE context, it is possible to have “official” assessment (i.e. “loggable” to *intacs*) with significant flexibility

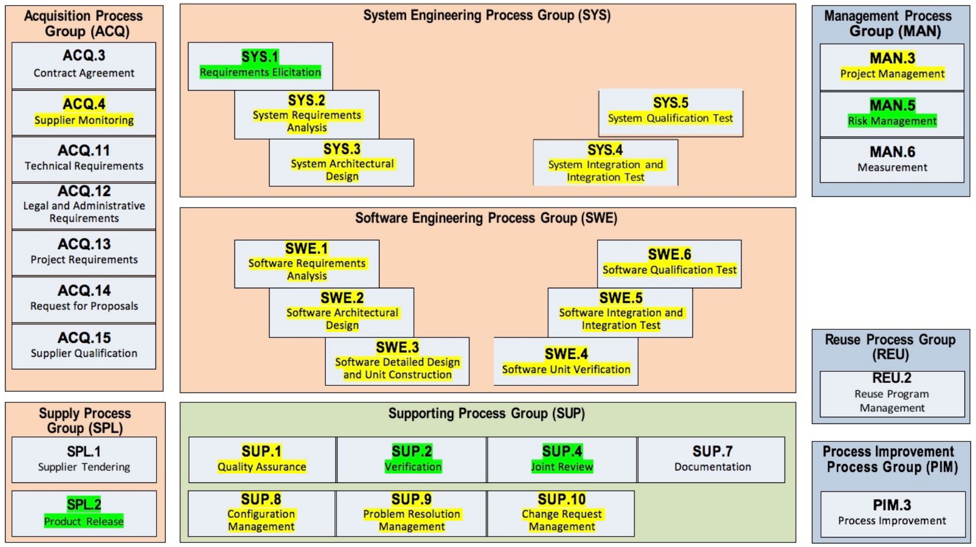
To be “loggable” to intacs, many requirements are to be satisfied, but the most important in terms of *scope* is that an assessment has to include at least *three* process *groups* (as defined in the PRM/PAM)

VDA Scope is not the only possible one

- *VDA Scope* (formerly known as *HIS Scope*) has always been controversial as arbitrary and monolithic
- It's mentioned in PAM 3.1 but it's not normative
- Various OEMs have defined their own scope
- There is now even an unofficial *extended VDA Scope*
- Proposal: let's identify and define an *OSS Scope* to best serve the purpose of OSS qualification

Yellow: official *VDA Scope*

Green: unofficial extension of *VDA Scope*



Acquisition Process Group (ACQ)
- ACQ.3 Contract Agreement
- ACQ.4 Supplier Monitoring
- ACQ.11 Technical Requirements
- ACQ.12 Legal and Administrative Requirements
- ACQ.13 Project Requirements
- ACQ.14 Request for Proposals
- ACQ.15 Supplier Qualification

System Engineering Process Group (SYS)
- SYS.1 Requirements Elicitation
- SYS.2 System Requirements Analysis
- SYS.3 System Architectural Design
- SYS.4 System Integration and Integration Test
- SYS.5 System Qualification Test

Management Process Group (MAN)
- MAN.3 Project Management
- MAN.5 Risk Management
- MAN.6 Measurement

Software Engineering Process Group (SWE)
- SWE.1 Software Requirements Analysis
- SWE.2 Software Architectural Design
- SWE.3 Software Detailed Design and Unit Construction
- SWE.4 Software Unit Verification
- SWE.5 Software Integration and Integration Test
- SWE.6 Software Qualification Test

Reuse Process Group (REU)
- REU.2 Reuse Program Management

Supply Process Group (SPL)
- SPL.1 Supplier Tendering
- SPL.2 Product Release

Supporting Process Group (SUP)
- SUP.1 Quality Assurance
- SUP.2 Verification
- SUP.4 Joint Review
- SUP.7 Documentation
- SUP.8 Configuration Management
- SUP.9 Problem Resolution Management
- SUP.10 Change Request Management

Process Improvement Process Group (PIM)
- PIM.3 Process Improvement

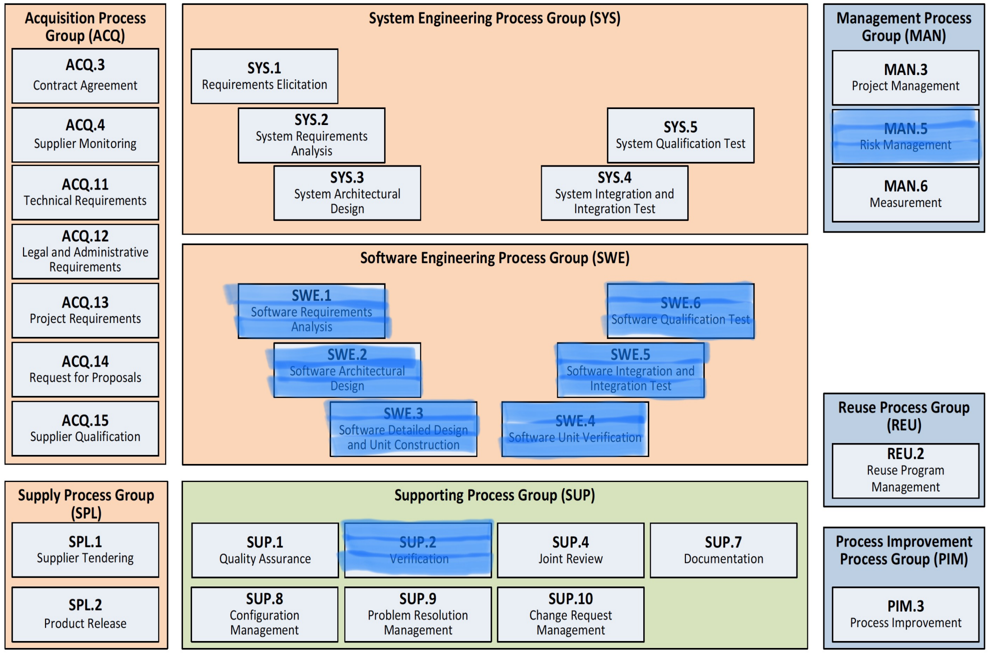
DRIVERS FOR DEFINITION OF OSS Scope

- **Conformity** (not in contrast with any SPICE/ASPICE requirements)
- **Simplicity** (minimal possible number of significant processes)
- **Comprehensibility** (processes have to be well understood and meaningful to OSS community)
- **Usability** (assessment results have to give advantage to the purpose of OSS qualification)

Definition of the OSS Scope

- *OSS Scope* includes the full SWE Process Group
- It includes MAN.5 of the Management Group
- It includes SUP.2 of the Supporting Process Group
- Contrary to the *VDA Scope*, it defines not only a Process scope, but also a Capability Level scope, defined to be CL2

Blue: the *OSS Scope*



Acquisition Process Group (ACQ)
- ACQ.3 Contract Agreement
- ACQ.4 Supplier Monitoring
- ACQ.11 Technical Requirements
- ACQ.12 Legal and Administrative Requirements
- ACQ.13 Project Requirements
- ACQ.14 Request for Proposals
- ACQ.15 Supplier Qualification

System Engineering Process Group (SYS)
- SYS.1 Requirements Elicitation
- SYS.2 System Requirements Analysis
- SYS.3 System Architectural Design
- SYS.4 System Integration and Integration Test
- SYS.5 System Qualification Test

Management Process Group (MAN)
- MAN.3 Project Management
- MAN.5 Risk Management
- MAN.6 Measurement

Software Engineering Process Group (SWE)
- SWE.1 Software Requirements Analysis
- SWE.2 Software Architectural Design
- SWE.3 Software Detailed Design and Unit Construction
- SWE.4 Software Unit Verification
- SWE.5 Software Integration and Integration Test
- SWE.6 Software Qualification Test

Reuse Process Group (REU)
- REU.2 Reuse Program Management

Supply Process Group (SPL)
- SPL.1 Supplier Tendering
- SPL.2 Product Release

Supporting Process Group (SUP)
- SUP.1 Quality Assurance
- SUP.2 Verification
- SUP.4 Joint Review
- SUP.7 Documentation
- SUP.8 Configuration Management
- SUP.9 Problem Resolution Management
- SUP.10 Change Request Management

Process Improvement Process Group (PIM)
- PIM.3 Process Improvement

JUSTIFICATION FOR KEY CHOICES: #1

- **Choice**: All SWE group included
- **Justification**: none of the six processes can be reasonably excluded for a complete SW qualification; even in OSS context, SW is never “code only”; tailored “waivers” for other expected work products (*e.g. requirement specification, architectural design, test plans, etc…*) can be negotiated but corresponding processes have to be in place

JUSTIFICATION FOR KEY CHOICES: #2

- **Choice**: no MAN.3 Project Management
- **Justification**: MAN.3 is a very complex process that is unlikely to be fully significant in the OSS context; the minimal level of management (that is anyway expected) is guaranteed by the targeted PA2.1 for all processes (required to achieve the minimum required CL2 for the OSS Scope)

JUSTIFICATION FOR KEY CHOICES: #3

- **Choice**: no SUP.1 Quality Assurance , no SUP.8 Configuration Management
- **Justification**: Fully-fledged Quality Assurance and Configuration Management are unreasonable requests in the OSS context; the minimum of expected work product configuration and quality control is anyway guaranteed by the targeted PA2.2 for all processes (required to achieve the minimum required CL2 for the OSS Scope)

JUSTIFICATION FOR KEY CHOICES: #4

- **Choice**: inclusion of MAN.5 Risk Management
- **Justification**: no OSS aspiring to be qualified in a FuSa context can get by without showing that at least a general *project/product* risk management is in place; for the principle of ‘comprehensibility’ (already mentioned before) it is expected to be a well understood process in the OSS community

JUSTIFICATION FOR KEY CHOICES: #5

- **Choice**: inclusion of SUP.2 Verification
- **Justification**: in ASPICE model, SUP.2 is sometimes seen as a ‘weak replica’ of SUP.1 Quality Assurance, because it has apparently less requirements/coverage; in fact, it is the ‘technical verification’ for work products that has to be anyway in place to integrate the ‘verification by testing’ already captured by the SW testing processes; for the principle of ‘comprehensibility’ (already mentioned before) it is expected to be a well understood process in the OSS community

JUSTIFICATION FOR KEY CHOICES: #6

- **Choice**: minimal capability level scope is CL2
- **Justification**: it is not affordable to exclude *MAN.3, SUP.1, SUP.8* from any meaningful ASPICE "sub" scope without requiring at least CL2; in this way the minimum level of *management* and *configuration and quality control* is at least guaranteed at process level, if not a project level

CONCLUSIONS

- By removing grave misunderstandings about the nature of its model, an ASPICE assessment can become very ‘OSS friendly’ in terms of process qualification
- The biggest hurdle lies in the “traditional” scope of ASPICE assessments, almost invariably based on the VDA Scope, unsuited for the purpose
- It is proposed to adopt (staying fully conformant with the current SPICE/ASPICE versions) a specially designed OSS Scope, that would grant *official* ASPICE compliance without forcing the OSS community (organizations and practitioners) to embrace overshooting practices and procedures

exida®

excellence in dependable automation

Many Thanks for Your Attention

carlo.donzella@exida-dev.com