AVL ComplyGuard and Capability Adviser

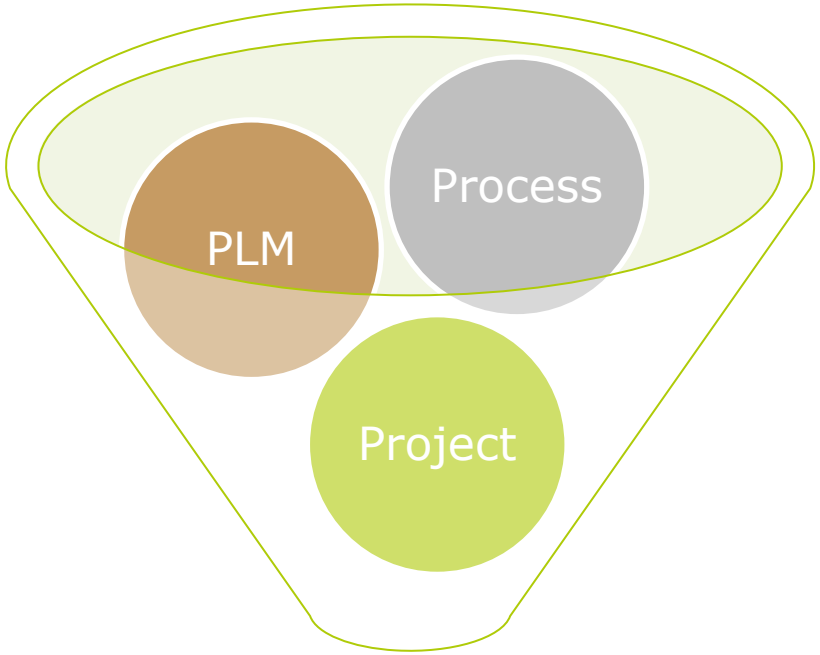
ASPICE 4.0 + Safety Integrated

Dr. Gerhard Griessnig, AVL List GmbH
Dr. Richard Messnarz, ISCN GmbH

ASPICE 4.0 + Safety Integrated

Author(s):	Dr. Gerhard Griessnig Dr. Richard Messnarz
Co-Author(s):	
Approved by:	
Project Leader:	
Version:	1.0
Release date:	02.09.2024
Security level:	Public
Customer:	
Project:	
Task ID:	
Department:	

PLM / Process Tools



Comply Guard

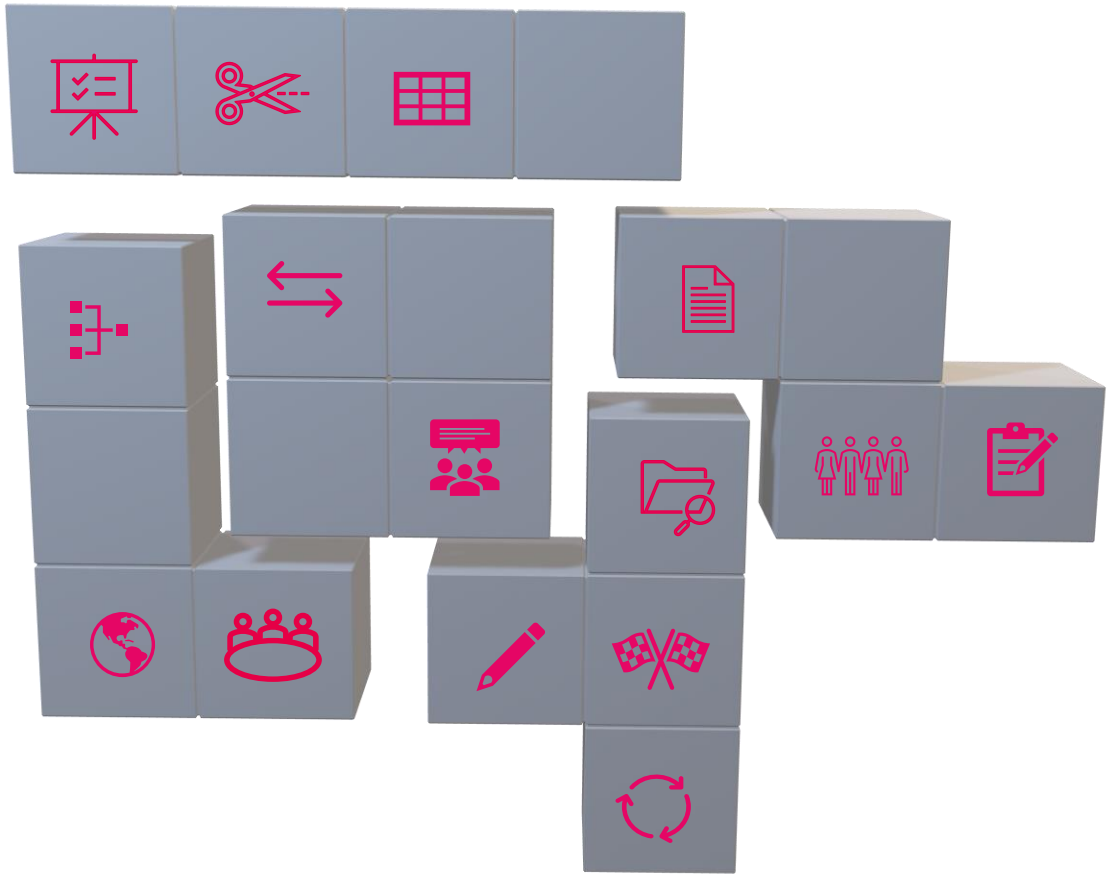
Process Tools
- Their strength is the visual representation of processes
- Examples: Stages, …

PLM Tools:
- Their strength is the controls development for planning, monitoring, requirements engineering and testing
- Examples: Polarion, C-Place, Codebeamer, …

Safety Tools:
- The strength of existing safety tools mainly focus on safety engineering
- Examples: Medini Analysis, Sox, ..

AVL ComplyGuard
- Direct application in projects of a uniform safety process in your company in compliance with ISO standards
- Safety Lifecycle follows the tailoring
- Safety Management documents are generated out of the tool which ensures consistency in your company
- Reuse of existing company-specific data storages
- Mapping of complete vehicle projects and collaboration with suppliers in one tool
- Confirmation Reviews, Assessments
- Interfaces to e.g. JIRA, PTC, …
- …

AVL ComplyGuard Bricks



	Topic
	Predefined ISO compliant process – ready to start
	Tailoring of the Safety Lifecycle
	Development Interface Agreements (DIA)
	Automated Report Generation from DIA to Safety Case
	Overview and track all single system development of a vehicle in one project
	Perform Audits and Assessments (Multiuser)
	Planning and execution of reviews and confirmation reviews
	Decision History
	Multi-Standards in one Tool
	Semi-Formale Requirements Development
	Agile Development with JIRA IF
	Open Data Interface to flexible store evidences
	Project Management incl. Dashboards
	User and role Management
	Baseline and Release

AVL ComplyGuard
Safety Activities Support Reports

Safety Management Activities	Template	WP req. by ISO 26262	Comments
Tailoring	Performed in the tool	No	As part in the subsequent WPs
DIA	DIA as XLS, Word	Yes	Automatically generated based DIA and tailoring
Safety Plan	Safety Plan as Word	Yes	Automatically generated from a template that passed confirmation reviews
Methods Tailoring	Performed in the tool	Yes	As part in the subsequent WPs
Safety Status Report	Status Report as XLS	No	Automatically generated which shows the Safety activities and WPs in XLS Format
Verification Plan	Verification Plan as Word	Yes	Automatically generated as
Document Management Plan	Performed in the tool	Yes	Automatically generated as part of the functional safety plan
Confirmation Reviews	Performed in the tool	Yes	Planning and tracking based on AVL templates
Verification Reviews	Performed in the tool	Yes	Planning and tracking based on AVL templates
Audit & Assessment Plan	Plan of the assessment	Yes	Planning the assessment
Audit & Assessment Report	Audit/Assessment as XLS	Yes	Automatically generated based on Assessment
Safety Case	Safety Case as Word	Yes	Automatically generated based on Status and Evidences
Safety Release Report	Safety Release as Word	Yes	Automatically generated based on Status and Evidences
Open Issues	OI as XLS	No	Track safety issues in the tool or in JIRA (Interface)
Minutes of Meetings	MoM as Word	No	Write your MoM and link OIs and find statements and decisions in simple manner
Semiformal RQs	Performed in the tool	Partly	Semiformal RQs based on available information as text

Capability Adviser has been updated to an ASPICE 4.0 + ISO 26262 Extension.

Capability Adviser has been updated to generate a safety objectives coverage report in Excel readable by AVL Comply Guard.

ASPICE + Safety Integrated

capadvsupport@iscn.com

ASPICE VS SAFETY

ISCN
www.iscn.com

It is possible in Version 9.1.1 to save both a rating for basic SPICE aswell as Safety. Thus a clearer picture can be gained when it comes to Safety relevant practices and the impact of Safety on the overall rating.

SAFETY

ASPICE

SWE.1.BP1 **Specify software requirements.** Use the system requirements and the system architecture and changes to system requirements and architecture to identify the required functions and capabilities of the software. Specify functional and non-functional software requirements in a software requirements specification. [OUTCOME 1, 5, 7]

ISO 26262 Extended Questions:
- Are software safety requirements in line with the technical safety requirements (Requirements, interfaces, constraints, ?)?
- Are all software safety requirements marked as safety requirements and referred to their source?
- Are semiformal notations used for ASIL C and D?
- Are software safety diagnose requirements assigned to an appropriate diagnose level (e.g. e-gas model with (Level 1 - base diagnosis, Level 2 - independent plausibility checks and functional diagnosis, Level 3 - system control, checking the call sequences, processor, etc.).
- Is the software state machine described and is the safe state clearly separated?
- Is the independence of the monitoring software clearly described?
- Are the software signals specified in the hardware software interface?
- Is there a diagnose matrix describing safety diagnose L2 and L3 functions and the expected fault reaction?
- Are there non functional software requirements relating to the ISO 26262 method tables?
- Are there non functional software requirements relating to the ASIL level assigned influencing the software architecture?
- Is the operating software and the related task management and synchronization of the control software considered?
- Are the appropriate methods used for analysis (see method tables in ISO 26262)?

⚠ N ○ P ● L ○ F ○ Not App. ○

N ○ P ○ L ○ F ● Not App. ○ Note

Assessor: Demo Assessor Level: 1

BP	1	2	3	4	5	6	7	8	9	10
SWE.1	F	F	F	F	F	F	F	F		
⚠ SWE.1	P	P	P	P	P	P	P	P		

Calculation

Show Level Profile | Show Percentage | Overrule

Process	Assessor	PA	1.1	2.1	2.2	3.1	3.2
MAN.3	Demo Assessor		F				
SWE.1	Demo Assessor		F				
⚠ SWE.1	Demo Assessor		P				

Safety Audit, ASPICE Assessment & Safety Assessment

Challenge:

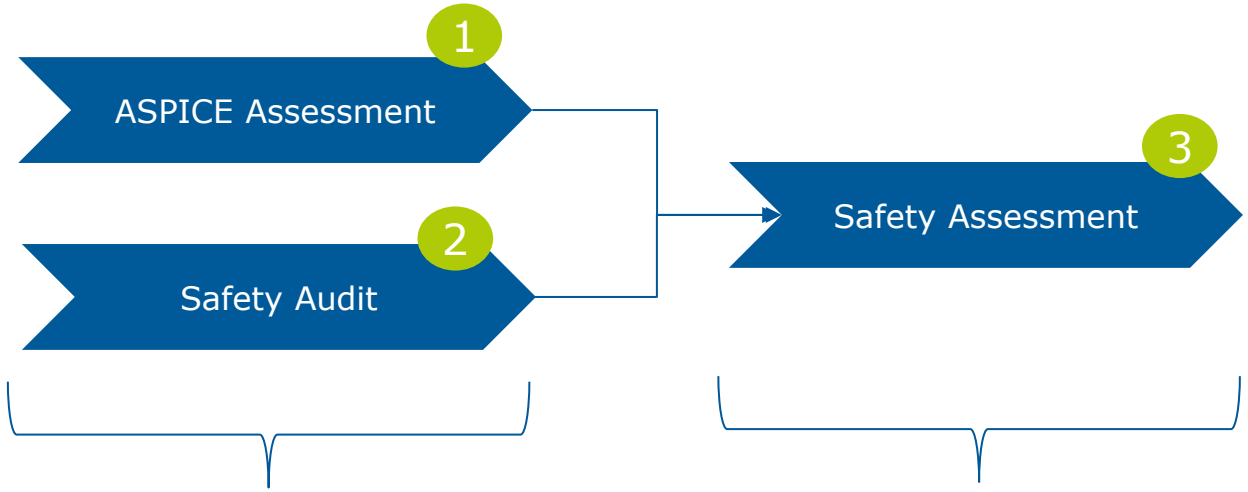
- Audits and assessments are mandatory activities in the safety life cycle
- All evidences and findings must be documented in a traceable way
- Evidence of compliance with the requirements and objectives of the standard should be demonstrated
- Assessments are typically done by more than 1 assessor

Questions:

- Assessor:
  - How can a tool support me to perform audits and assessments with reasonable effort?
  - How can we as assessors work on the same information in real time?
  - How ensure that findings are connected to evidences and actions?
- Engineer/Manager:
  - How can I prepare the relevant information for an audit or assessment?
  - How can I prepare for possible questions from the assessor?

Safety Audit, ASPICE Assessment & Safety Assessment

ISO 26262 requires a **safety audit** and a **safety assessment**. Often the product development requires an **ASPICE Assessment**. How to efficiently combine these activities?



1 and **2** have a very similar focus, can be done in **parallel** if in addition safety-related work products and methods are checked (e.g. traceability, process, …)

3 the product-specific implementation and compliance with the standard will be assessed

To improve efficiency the results of the ASPICE Assessment and Safety Audit shall be available for the Safety Assessment

- Ratings
- Rationales
- Evidences

Advantage to reuse existing information

Detailed information maintained in the project execution or independent safety assessment about:

- Safety activities and their status
- All evidences
- Tailoring
- Responsibilities
- Assessments results
- …

Detailed information gained in an ASPICE assessment or independent safety assessment about:

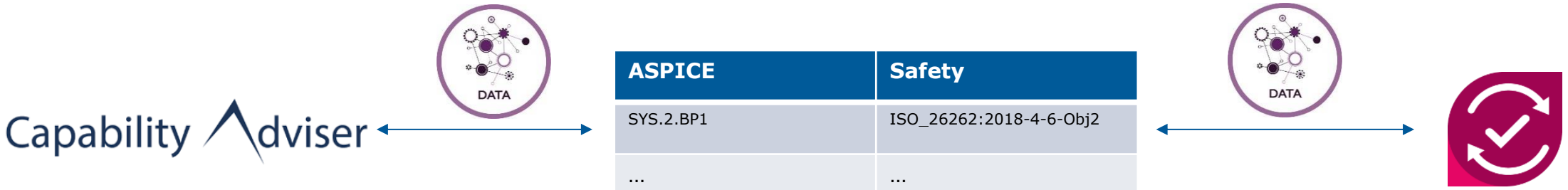
- ASPICE assessment results
- Safety assessment results (if applicable)
- Evidences checked

- Work immediately on findings by creating open issues
- Consider gained ASPICE results for safety assessments

- Reuse names and paths from imported evidences
- Understand responsibilities and safety activities

Example USE CASE
AVL ComplyGuard <-> Capability Adviser

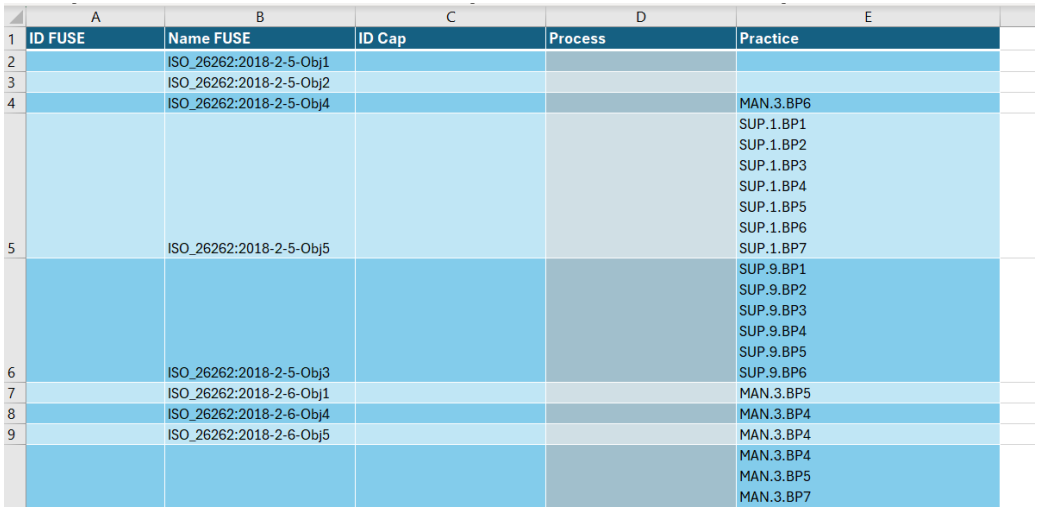
- Perform ASPICE assessments in Capability Adviser
- Perform Safety assessments in AVL ComplyGuard or Capability Adviser
- Merge Results in a commonplace
- To ensure a common basis ASPICE and Safety Objectives are mapped with each other
- Make use of both tools and exchange data



Mapping between ASPICE 4.0
and ISO 26262:2018 Objectives

The Interface

- In the SoQrates working group we did a mapping between ASPICE 4.0 and ISO 26262:2018 Safety Objectives
- The mapping is available in our common Excel template and can be simply adapted to company-specific needs
- The mapping table will be considered by the import from Capability Adviser and AVL ComplyGuard



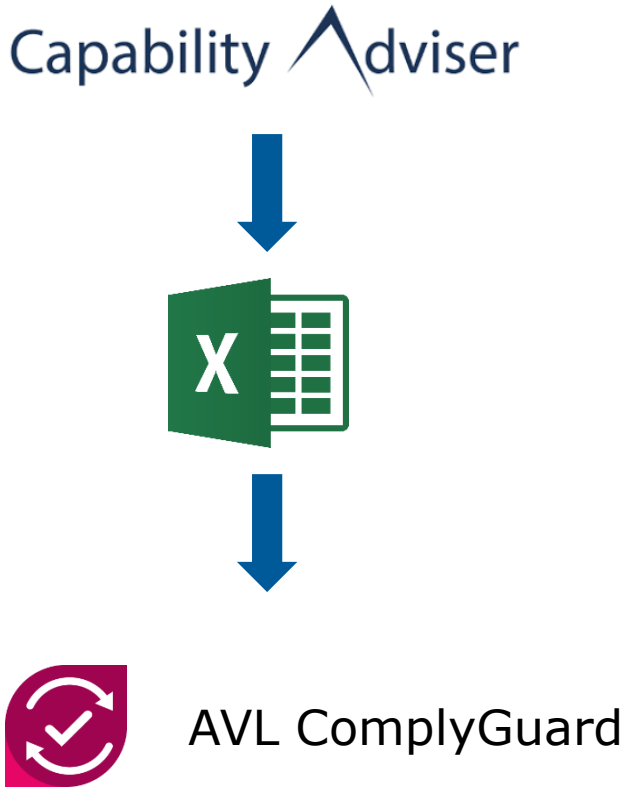
	A	B	C	D	E
1	ID FUSE	Name FUSE	ID Cap	Process	Practice
2		ISO_26262:2018-2-5-Obj1			
3		ISO_26262:2018-2-5-Obj2			
4		ISO_26262:2018-2-5-Obj4			MAN.3.BP6
5		ISO_26262:2018-2-5-Obj5			SUP.1.BP1 SUP.1.BP2 SUP.1.BP3 SUP.1.BP4 SUP.1.BP5 SUP.1.BP6 SUP.1.BP7
6		ISO_26262:2018-2-5-Obj3			SUP.9.BP1 SUP.9.BP2 SUP.9.BP3 SUP.9.BP4 SUP.9.BP5 SUP.9.BP6
7		ISO_26262:2018-2-6-Obj1			MAN.3.BP5
8		ISO_26262:2018-2-6-Obj4			MAN.3.BP4
9		ISO_26262:2018-2-6-Obj5			MAN.3.BP4
					MAN.3.BP4 MAN.3.BP5 MAN.3.BP7

Next Steps:

- In Comply Guard and Capability Adviser further detailed questions for safety assessments are available
- In SoQrates we plan to further align these questions and extend the interface between those tools.

AVL ComplyGuard
Import from Capability Adviser

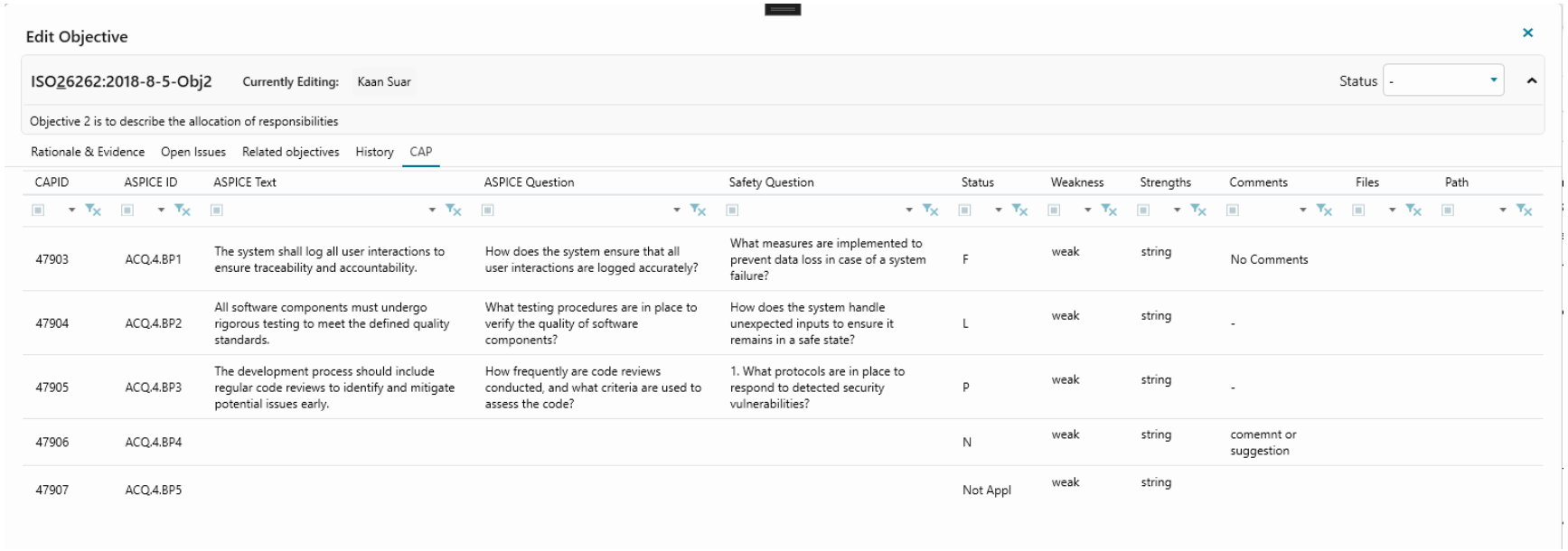
- ASPICE Assessment performed in Capability Adviser
  - Setting Status, Weaknesses, Strengths
- Export Results to Excel Report
  - Mapping between ISO & ASPICE Objectives
- Import Excel to AVL ComplyGuard
  - Show Results in the correct ISO objective to better rate the safety objective

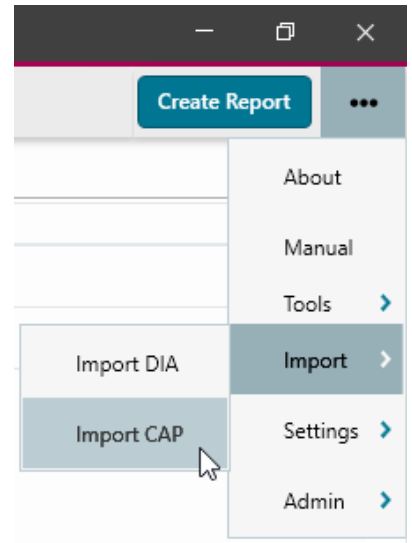


AVL ComplyGuard
Import from Capability Adviser

ASPICE ID	ASPICE Text	ASPICE Question	Safety Question	Status	Weakness	Strengths	Comments
ACQ.4.BP1	The system shall log all user interactions to ensure traceability and accountability.	How does the system ensure that all user interactions are logged accurately?	What measures are implemented to prevent data loss in case of a system failure?	F	weak	string	No Comments
ACQ.4.BP2	All software components must undergo rigorous testing to meet the defined quality standards.	What testing procedures are in place to verify the quality of software components?	How does the system handle unexpected inputs to ensure it remains in a safe state?	L	weak	string	-
ACQ.4.BP3	The development process should include regular code reviews to identify and mitigate potential issues early.	How frequently are code reviews conducted, and what criteria are used to assess the code?	1. What protocols are in place to respond to detected security vulnerabilities?	P	weak	string	-

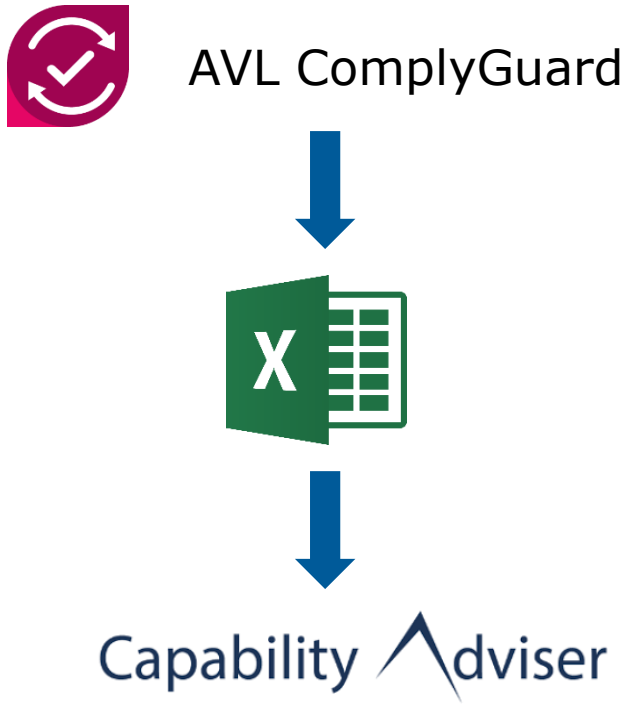
Capability Adviser export is taken and imported into AVL ComplyGuard





AVL ComplyGuard
Export to Capability Adviser

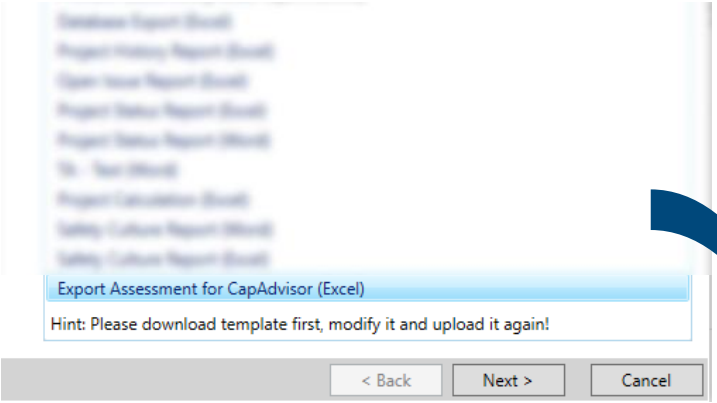
- Safety Assessment performed in AVL ComplyGuard
  - Setting Objectives Status, Rationale & Evidence
- Export Results to Excel Report
  - Mapping between ISO & ASPICE Objectives
- Import Excel to Capability Adviser
  - Correct mapping between ASPICE and ISO



AVL ComplyGuard
Export to Capability Adviser

Objectives

Relevant	Objective	Description	Status	Rationale	Evidence	Open Issues
✓	ISO_26262:2018-3-7-Obj1	Objective 1 is to specify the functional or degraded functional behaviour of the item in accordance with its safety goal	Fully	The functional or degraded functional behavior of the item must be clearly defined to ensure it meets its safety goal. By understanding how the item should perform under normal and degraded conditions, we can design and verify systems that maintain safety even in the presence of faults or failures	ISO-TC_22-SC_32_N1618_ISO_PAS_8800_for_CD_consltation.pdf (v1.0)	New Open Issue
✓	ISO_26262:2018-3-7-ImObj1.1	Objective 1.1 is to derive functional safety requirements from the safety goal, describing the functional or degraded functional behaviour of the item	Largely	This specification is crucial for identifying potential risks and implementing appropriate safety measures.	WT00009894_Green Ocean 4000_D_M_GO_1A HP + LP (P)_Sicherheitsmanagementplan V1.1.docx (v1.0)	New Open Issue
✓	ISO_26262:2018-3-7-Obj2	Objective 2 is to specify the constraints regarding suitable and timely detection and control of relevant faults in accordance with its safety goals;	Not Relevant	Defining the functional or degraded functional behavior of the item is essential to ensure it aligns with its safety goal. This detailed specification allows for the identification and mitigation of potential hazards. By clearly understanding the expected performance under both normal and degraded conditions, we can develop and validate safety mechanisms that ensure the item remains safe and reliable.	ISO-TC_22-SC_32_N1618_ISO_PAS_8800_for_CD_consltation.pdf (v1.0)	New Open Issue
✓	ISO_26262:2018-3-7-ImObj2.1	Objective 2.1 is to define appropriate timing requirements complying with the FTTI on the vehicle level, considering the safety architecture.	Partially	This proactive approach is key to preventing accidents and ensuring the overall safety and integrity of the system.	20230317_This is my Release.docx (v1.3)	New Open Issue

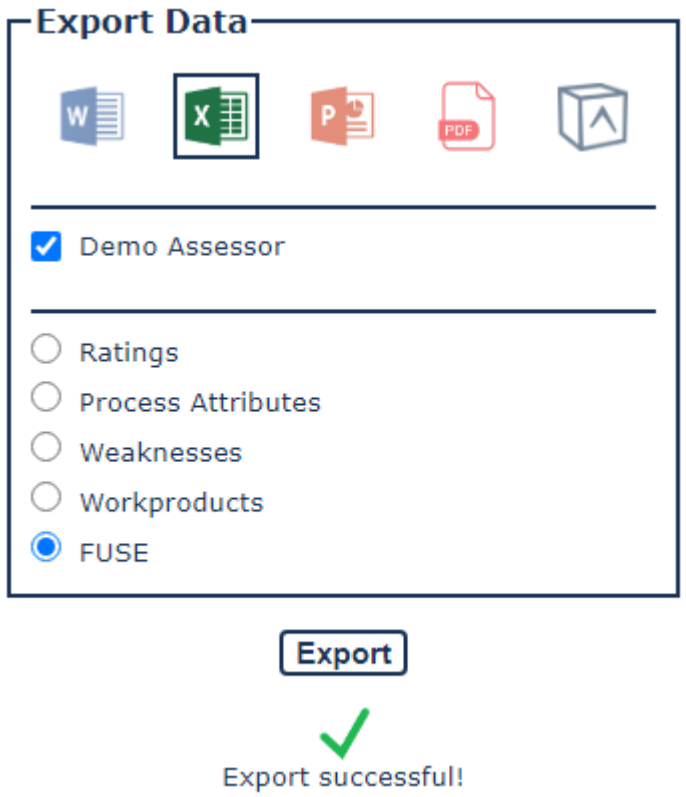


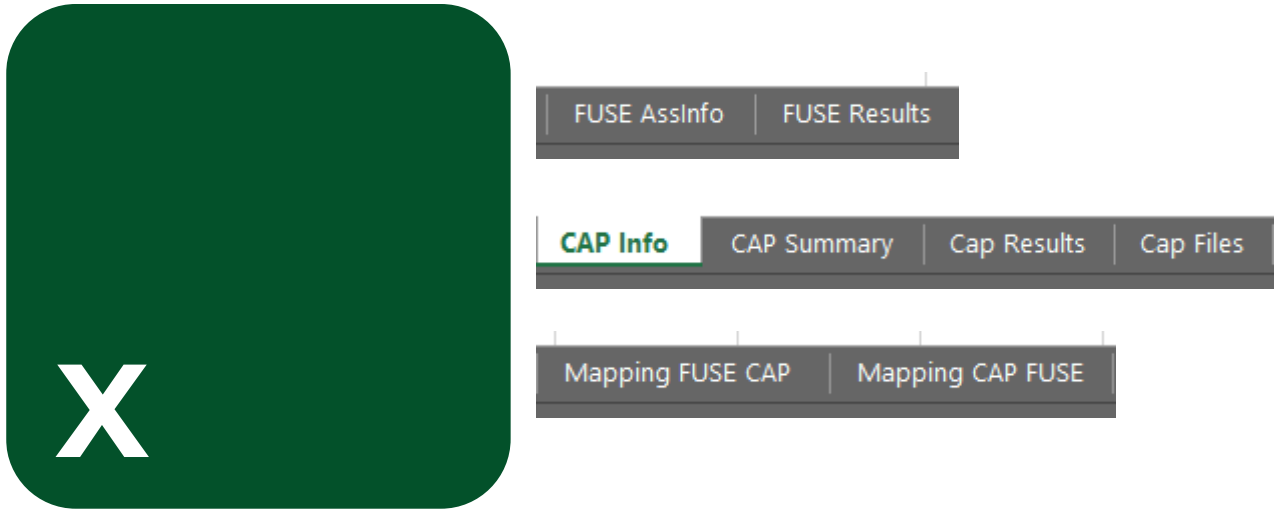
The exchange format is an Excel file which contains the ASPICE, ISO mapping and the results from ComplyGuard and Capability Adviser

Name	Description	Status	Rationale	Evidence
ISO_26262:2018-3-7-Obj1	Objective 1 is to specify the functional or degraded functional behaviour of the item in accordance with its safety goal	Fully	The functional or degraded functional behavior of the item must be clearly defined to ensure it meets its safety goal. By understanding how the item should perform under normal and degraded conditions, we can design and verify systems that maintain safety even in the presence of faults or failures	ISO-TC_22-SC_32_N1618_ISO_PAS_8800_for_CD_consltation.pdf (v1.0)
ISO_26262:2018-3-7-Obj2	Objective 2 is to specify the constraints regarding suitable and timely detection and control of relevant faults in accordance with its safety goals;	NotRelevant	Defining the functional or degraded functional behavior of the item is essential to ensure it aligns with its safety goal. This detailed specification allows for the identification and mitigation of potential hazards. By clearly understanding the expected performance under both normal and degraded conditions, we can develop and validate safety mechanisms that ensure the item remains safe and reliable.	ISO-TC_22-SC_32_N1618_ISO_PAS_8800_for_CD_consltation.pdf (v1.0)

AVL COMPLY GUARD INTEGRATION

ISCN
www.iscn.com





CapAdv is able to export assessment data in a format that the AVL Comply Guard tool understands. The same format will work both way for importing and exporting.
At the end of the file there is even a mapping section allowing you to implement the import of this file into other tools so the export within CapAdv is not limited to be used with AVL Comply Guard only.

AVL COMPLY GUARD INTEGRATION

Basic assessment information

	A	B
1	**Type**	**Comment**
2	Project	Safety
3	Assessment Name	Test Safety
4	Assessment Status	Ongoing/Planned
5	Assessment Typ	
6	Assessor Names	Demo Assessor
7	Participant Names	
8	Location	
9	Assessment Scope	ACQ.4, MAN.3, SUP.1, SUP.8, SUP.9, SUP.10, SWE.1,
10	Start Date	09.11.2023
11	End Date	21.11.2023
12	Assessment Summary	
13	Assessment Result	
14		

Assessment Rating Data

	B	C	D	E	F	G	H	I
1	**ASPICE ID**	**ASPICE Text**	**ASPICE Question**	**Safety Question**	**Status**	**Weakness**	**Strengths**	**Comments**
2	SWE.1.BP1				F	Found weaknesses	Considered strengths	Some comment that is neither
3	SWE.1.BP2				F			
4	SWE.1.BP3				F			
5	SWE.1.BP4				F			
6	SWE.1.BP5				F			

Assessment Evidence Data

	B	C	D	E	F	G	H	I
1	**Title**	**Description**	**Path**	**Instance**	**Process**	**Practies**		
2	SYS.2.BP5	xxx	xxx	xxx	xxx	xxx		
3	Evidence 1	Describing this evidence further	https://link.to.evidence	1	SYS.2 1, SWE.1	SWE.1.BP1,SWE.1.BP2,SWE.1.BP3,SWE.1.BP4		
4								

AVL COMPLY GUARD INTEGRATION

We did a mapping of the Objectives to Practices in ASPICE that is also par
This will allow other tools to adopt our format more easily.

	A	B	C	D	E
1	ID FUSE	Name FUSE	ID Cap	Process	Practice
2		ISO_26262:2018-2-5-Obj1			
3		ISO_26262:2018-2-5-Obj2			
4		ISO_26262:2018-2-5-Obj4			MAN.3.BP6
5		ISO_26262:2018-2-5-Obj5			SUP.1.BP1 SUP.1.BP2 SUP.1.BP3 SUP.1.BP4 SUP.1.BP5 SUP.1.BP6 SUP.1.BP7

Thank you for cooperating with ISCN GmbH.

ISCN is INTACS certified training provider for Automotive SPICE assessor courses

ISCN organises the EuroSPI conference since 1994 where e.g. VW is organising a workshop community, and VW, Rheinmetall AG, EB, MAGNA, AVL held key notes. http://www.eurospi.net

ISCN is certified by VDA to hold provisional and competent ASPICE assessor

ISCN moderates the German task force SOQRATES (https://soqrates.eurospi.net) since 2003 where >20 Tier 1 collaborate on ASPICE, Safety and Security.

EuroSPI certificates are issued by EuroSPI Certificates & Services GmbH (www.eurospi.net) in cooperation with DRIVES and the Automotive Skills Alliance (ASA). The ASA was founded by the EU Blueprint Project Drives and ALBATTS with support from the European Automobile Manufacturers' Association (ACEA). https://www.eurospi.net. ISCN is founding member.

Thank you for cooperating with EuroSPI² Certificates & Services GmbH.

Academy – Courses and Training Platform

Certification – Exam system and certificates

EuroSPI Conference Series

Assessment Tool – ISO 330xx based