Safety systems testing in the Automotive Sector

according to ISO 26262 (Road vehicles – Functional Safety) and Automotive SPICE – based on ISO/IEC 15504 (Software Process Improvement and Capability Determination (SPICE))

ISO 26262 (Road vehicles – Functional Safety)

The functional safety standard determines how to estimate impact of the designed system on human safety. With contribution of technical specialists, designers, functional safety officers, etc., it is predicted which hazards may occur while using the designed system. Also, three quantity factors are estimated:

severity	0-3	Zero is a level where the situation does not impact human safety (it is not severe, exposure to situation is low and controllability is high), while three and four are situations having the highest impact on human health and life.
exposure	0-4	
controllability	0-3	

Based on the value of these three elements, Automotive Safety Integrity Level is estimated (ASIL D - the highest impact on safety, ASIL A – least impact, and Quality Management Level QM – no impact), which gives an overview of which safety requirements have to be additionally implemented.

Automotive SPICE

Automotive SPICE is a standard which describes how to continue work on the system. All stages of ASPICE have defined work products and traceability between them – it is a ready-to-use path, providing (if used correctly) that all requirements were analyzed, implemented and tested, as well as all information from this process is preserved and easy to find.

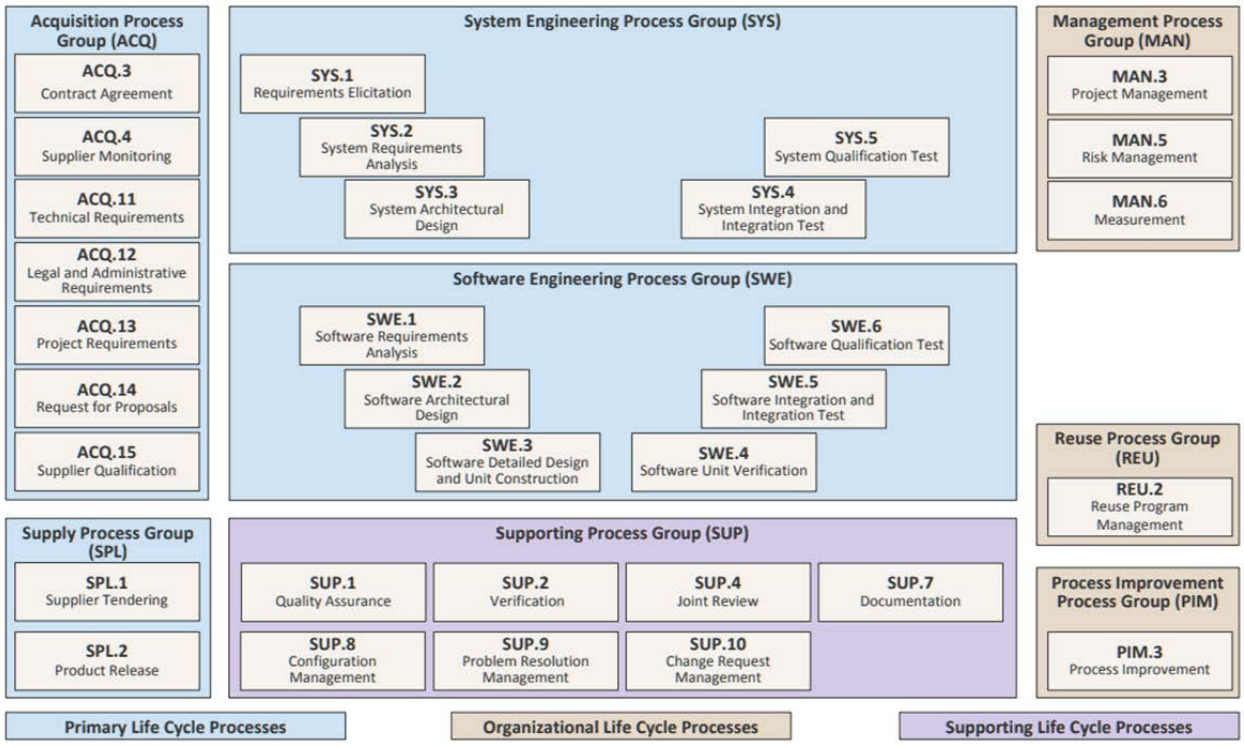


Figure 1 Automotive SPICE overview (source: ASPICE standard)

It is based on V-model – well-known from software development lifecycle for other industries – which has also been adapted to the automotive sector. All requirements – from describing the functionality of the system to functional safety requirements – are passing through the stages of V-model. They are collected (SYS.1), analyzed (SYS.2) and it is decided if they are SW (standard), ME (micro), EE (enterprise) requirements etc. Next, they are gathered into overall system architecture (SYS.3).

Depending on the analysis' result on stage SYS.2, they proceed accordingly to their type. Software requirements are analyzed (SWE.1), gathered into architecture (SWE.2) and coded (SWE.3). Then, the testing phase takes place: starting from SWE.4, which is unit testing, then testing mutual coordination of software components via implemented interfaces (SWE.5) to checking if the software was implemented accordingly to software requirements analyzed on SWE.1 stage (SWE.6). Next, the system is considered as one all over again (SW, ME, EE and other – depending on the type of the system). It is tested if all system components and interfaces (defined on SYS.3 stage) are working as it is expected (SYS.4), and if the entire system is implemented as was defined in system requirements (SYS.5). There are also many other elements, which support the implementation of the system.

Testing in Software Engineering Process Group (SWE) is a key factor determining the system's quality. Tests are designed to strictly verify the behaviour of the software, and minimize its impact on the rest of the system.
System testing is conducted on specially designed test benches, which communicate with the system via communication bus in the same way as it will be on a real vehicle. They include elements like power supplies, signal generators, etc. The way in which the tester manipulates input values and checks output is simulation on a typical PC. It includes user interface to present the entire communication with the tested system and provide ways to manipulate it. The system can have graphical user interface (GUI), which mostly helps with manual testing, or be tested automatically through scripts.

System testing is not the last stage in automotive testing. There is also validation and acceptance testing (mainly with the system installed in a vehicle).

During validation testing, the system is expected to fulfil physical requirements like vibration, temperature and humidity endurance, noise level, etc. It is are conducted in laboratories with special equipment, e.g. soundproof rooms.

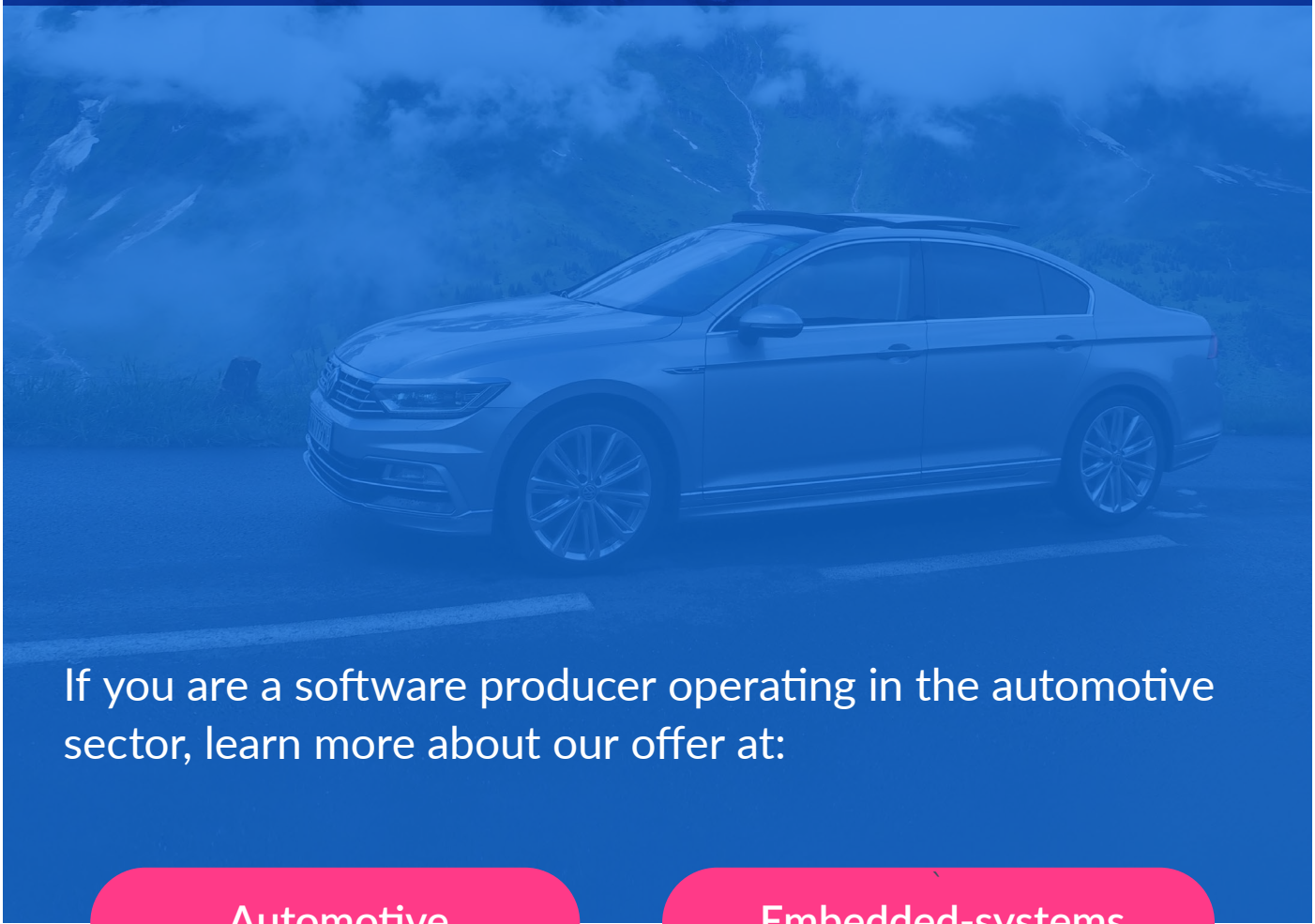
Acceptance testing is performed on a vehicle. It looks like usage of the system which it was designed for, but with the addition of boundary values – for example, if the system is using cameras to observe passengers, it is checked if a picture of a specific person will activate the system if he or she is wearing unusual clothing or accessories. It may happen that the system implemented according to the requirements will fail at some point due to the lack of requirement for some boundary values, which no one has thought of before.

Testing, as described above, may show surprising results and unexpected behaviour of the system. It is important to go through all testing stages and test even unexpected scenarios – even if the possibility of such a scenario is 1%, there are still many such vehicles as their number reaches thousands.

In the highly structured automotive sector, the firmware quality and testing is of crucial value to the end user.

Why choose Sii?

Sii Poland, as a highly specialized organization, has teams of experienced engineers and all necessary technologies to carry out software testing processes in accordance with ISO 26262 and Automotive SPICE. Throughout the years, we have supported the largest Tier1 suppliers in the world in embedded testing projects.



If you are a software producer operating in the automotive sector, learn more about our offer at:

Automotive

Embedded-systems