Automotive SPICE® for Cybersecurity

Abstract

In February 2021, the VDA Yellow Print "Automotive SPICE® for Cybersecurity" has been published. Based on ISO/IEC 33020:2015 and ISO 21434, it defines a process assessment model that extends the familiar Automotive SPICE® model. Rating guidelines with rules and recommendations are also included.

How is it applied?

Automotive SPICE® for Cybersecurity (ASC) enables evaluation of cybersecurity-relevant development processes. An Automotive SPICE® 3.1 VDA scope assessment is required either as a separate assessment or combined with Automotive SPICE® for Cybersecurity. Therefore, Automotive SPICE® for Cybersecurity cannot be seen as a standalone model but as an extension. With this approach the repetition of Automotive SPICE® system and software engineering indicators (SYS.x and SWE.x) is avoided. But in case of existing assessment the SUP processes need to be re-evaluated.

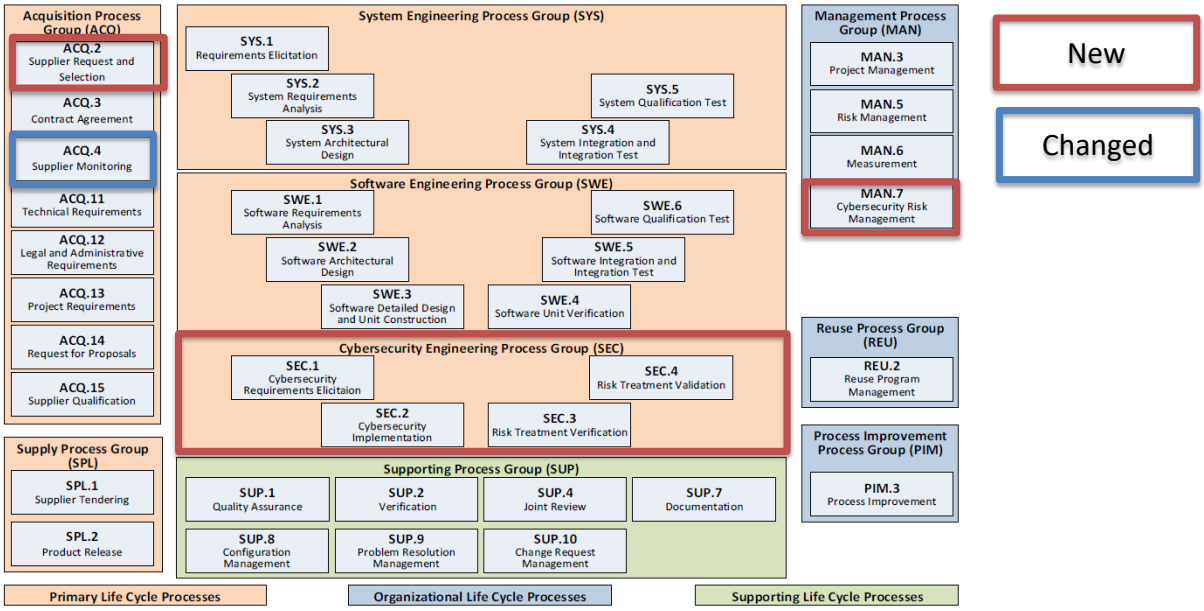
What is the structure?

Basically, the yellow volume contains 2 parts:

- A process reference and assessment model for cybersecurity engineering: definition of the processes including indicators for level 1 (base practices)
- Rating guidelines for level 1: rules and recommendation for rating (similar to Automotive SPICE® Guidelines)

What is the scope?

The following picture shows the Automotive SPICE® and Automotive SPICE® for Cybersecurity scope. Processes marked in red and blue are defined in Automotive SPICE® for Cybersecurity.



The basic idea is that the SEC processes extend the already existing SYS and SWE processes, For example the process ***SEC.2 Cybersecurity implementation*** defines the following base practices:

- ***SEC.2.BP1:*** *Refine the details of the architectural design. …*
- ***SEC.2.BP2:*** *Allocate cybersecurity requirements. …*
- ***SEC.2.BP3:*** *Select cybersecurity controls. …*
- ***SEC.2.BP4:*** *Define interfaces. Identify and describe interfaces between the elements of the architectural design and operating environment.*
- ***SEC.2.BP5:*** *Analyze architectural design. Analyze the software architectural design to identify and evaluate vulnerabilities.*
- ***SEC.2.BP6:*** *Refine the details of the detailed design. …*
- ***SEC.2.BP7:*** *Develop software units*
- ***SEC.2.8P8:*** *Establish bidirectional traceability. Establish bidirectional traceability between the refined architectural design and the detailed design.*
- ***SEC.2.BP9:*** *Ensure consistency.*

In addition to the SEC processes MAN.7 and ACQ.2 have been added:

- ***MAN.7 Cybersecurity Risk Management Process:*** *The purpose of the Cybersecurity Risk Management Process is to identify, prioritize and analyze risks of damage to relevant stakeholders as well as monitor and control respective risk treatment options continuously.*

- ***ACQ.2 Supplier request and selection:*** *The purpose of supplier request and selection process is to award a supplier a contract/agreement based on relevant criteria.*

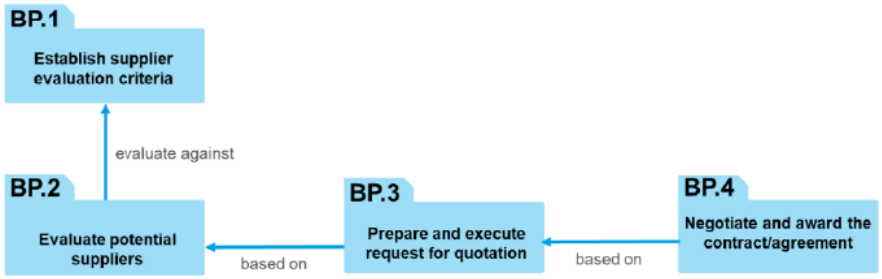
An already known process from Automotive SPICE® is also included in Automotive SPICE® for Cybersecurity:

- ***ACQ.4 Supplier Monitoring:*** *The purpose of the Supplier Monitoring Process is to track and assess the performance of the supplier against agreed requirements and agreed corrective actions.*
    - It specifies the same Base Practices as included in Automotive SPICE® but puts the focus on Cybersecurity, e.g. *"NOTE1: Cybersecurity requirements and responsibilities need to be aligned between customer and supplier"*
    - An assessment of two ACQ.4 instances (Automotive SPICE® and Automotive SPICE® for Cybersecurity) is recommended

How are the Rating Guidelines structured?

The ASC Rating Guidelines are structured in the same way than the Automotive SPICE® Guidelines: for every process in ASC Scope (see above) there are

- Rating recommendations: rules and recommendations, e.g.
  [ACQ.2.RL1] If the indicator BP1 is downrated due to an inappropriate, insufficient or incomplete definition of the supplier evaluation criteria, the corresponding indicator BP2 shall be downrated.
- Rating consistency: consistency between base practices, e.g.



How will this influence future Assessments?

So far assessments are only based on Automotive SPICE® as customers refer to their agreed requirements. But as cybersecurity is already part of current development projects, this will change soon. Pilot assessments will be performed this year, and as the assessment scope will change, companies should prepare for ASC. Processes need to be checked for compliance with ASC indicators and, if necessary, an update of standard processes will be necessary.

Process Fellows GmbH | Schlegelleithe 8 | 91320 Ebermannstadt | GERMANY

Phone: +49 9194 3719 957 | Fax: +49 9194 3719 – 579

Website: www.processfellows.de | E-Mail: info@processfellows.de