Automotive SPICE – kontrola nad vývojem mechatronických komponent v kontextu (nejen) automobilového průmyslu

Část 1.

Petr Švimberský

aSPICE je pro většinu dodavatelů především požadavek zákazníka. V následující úvaze se pokusíme představit, co tento požadavek ve skutečnosti znamená a jaký může mít i pro vás přínos. V první části se nyní soustředíme na obsah a rozsah aplikace normy a v druhé v příštím čísle PK na přínosy a samotné hodnocení.

Co je aSPICE

Automotive SPICE definuje sadu procesů a jejich výstupů, včetně jejich minimálního obsahu, a dává metodický pokyn, jak ohodnotit jejich kvalitu.

Respektive aSPICE umožňuje vyhodnotit, zda projekt vývoje produktu odpovídá procesnímu popisu v rámci firemní implementace a zda tato firemní implementace odpovídá požadavkům standardu (a tedy i požadavkům zákazníka).

Tedy požadavek zákazníka na *„Projekt vývoje produktu musí plnit Capability Level 2 na alespoň VDA sadě procesů aSPICE“* neznamená pouze požadavek na strukturu vývojového procesu, ale také definuje minimální nutný rozsah aktivit v projektu a produkovaných výstupů (včetně definice jejich obsahu).

Díky tomu, že aSPICE předepisuje, jaké výstupy mají jednotlivé procesy vytvářet, umožnuje také následující zajímavá tvrzení ve vztahu k ostatním standardům v automobilovém průmyslu:

VDA 2 (2020) – Zajišťování kvality před sériovou výrobou – 6.2 uvolňování výrobku / Příloha 5 – Krycí list PPF software – Aplikujte proces vývoje SW aSPICE na CL2 na projekt a máte ve správný čas k dispozici kompletní sadu dokumentace pro uvolnění výrobku z hlediska software.

IATF 16949:2016 – Způsob, jak prokázat během auditu, že vývoj plní požadavky kapitol 6-9 – opět prokázáním plnění aSPICE, tentokrát ovšem na Capability Level 3.

ACMSM (Automotive Cybersecurity Management System Audit) – Od roku 2021 je uvolněn doplněk Automotive SPICE for cybersecurity, za pomoci kterého lze prokázat plnění ACMSM na úrovni projektu.

Formel Q – způsobilost software – Jedinou reálnou možností, jak naplnit požadavky na způsobilost, je aplikovat aSPICE (Formel Q → KGAS → aSPICE).

PEP – proces vývoje produktu – VW – opět, vývoj vestavěného SW (a samotného produktu) se řídí požadavky standardu aSPICE.

Tedy aSPICE není jen pro aSPICE, ale jeho implementace vám umožňuje jednoduše prokázat mnoho dalšího než pouhou shodu s požadavkem zákazníka.

Než se ponoříme do vlastních výhod, které nám aSPICE přináší, nejdříve se blíže podíváme na strukturu a obsah.

aSPICE se skládá z následujících procesních skupin: (viz obr. 1)

Acquisition Process Group (ACQ) – tato skupina zahrnuje procesy pro řízení subdodavatelů, jejich kvalifikaci a komunikaci požadavků na subdodávku. Dá se říct, že i když nemáme subdodavatele, stejně je pro nás tato skupina procesů zajímavá, protože také popisuje, jaké má požadavky a jak by nás měl řídit zákazník. Jsme-li tedy na pochybách, zda je naše zadání kompletní, je možné se o tyto procesy opřít.

Management Process Group (MAN) – sada procesů pro řízení projektu, od roku 2019 je k dispozici dodatek AGL.1 – proces pro řízení vývoje agilním způsobem. Tedy aSPICE také pokrývá tento přístup k projektovému managementu, navíc ke standardním modelům typu iterative development či waterfall.

Supply process Group (SPL) – naši pozornost si zasluhuje především proces SPL.2 – product release, který popisuje, jakým způsobem a co má dodávka našeho produktu zákazníkovi obsahovat.

Reuse a Process Improvement Process Group (REU + PIM) – tyto procesní skupiny jsou užitečné především při implementaci aSPICE na vyšší CL, ale velmi je oceníme, pokud budeme chtít prokazovat plnění požadavků IATF či ACMS.

Supporting process Group (SUP) – procesní skupina pokrývající veškeré aktivity, které jsou přímo nutné

Obrázek 1

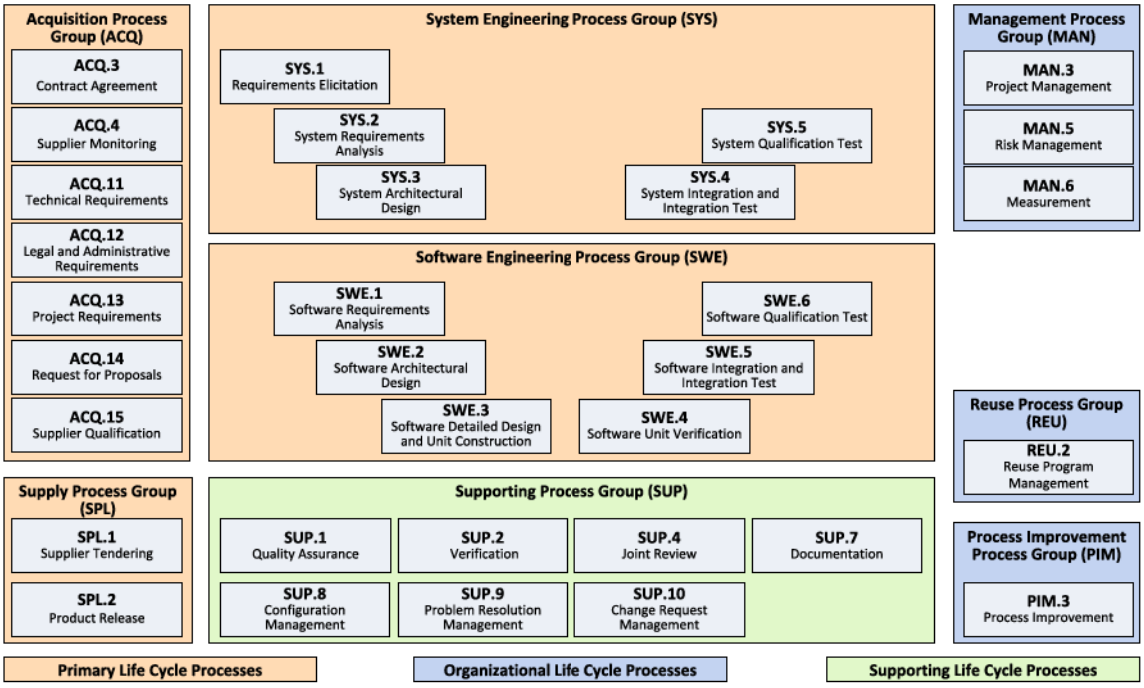


Figure 2 — Automotive SPICE process reference model - Overview

pro podporu projektu, ale nejsou procesy vyžadující inženýrské/doménově specifické schopnosti. Většina z nich se týká všech v projektu.

SUP.1 kvality management poskytuje kontrolu nad plněním požadavků normy (jak procesní, tak produktovou).

SUP.8 poskytuje kontrolu nad veškerými vstupy a výstupy v projektu (včetně prostředí, kde se prolíná s požadavky na metrologii, respektive podporuje v tomto aspektu veškeré verifikační procesy).

SUP.9/SUP.10 obstarávají management potřebný pro řízení změn a řešení problémů.

Na zbylé Supporting procesy lze také nahlížet jako na „protikusy" – například SUP.4 Join Review je přímý protikus k ACQ.10,11,12, které vysvětlují požadavky zákazníka, SUP.2 Verification podporuje ACQ.4 Supplier monitoring, ale také naše verifikační (testovací) procesy atd.

Zbylé procesní skupiny jsou „inženýrské – produktové", resp. technické procesy.

Zde je třeba se zamyslet nad tzv plug-in konceptem procesního modelu aSPICE, a především nad rozsahem, v jakém má být aSPICE aplikován.

Předem se zamysleme nad termínem Systém. – Jedná se o velmi arbitrární termín. Z hlediska odběratele je náš produkt vždy komponentou, z hlediska našeho by měl náš produkt být vždy systémem (byť by byl pouze softwarovým systémem).

Jak se chovat vůči interním dodavatelům a interním zákazníkům? Neexistuje přece pouze jediná vrstva integrace. Do naší dodávky můžeme zahrnout i naše komponenty z naší platformy či různých produktových řad.

Zde doporučují spolehnout se na přesné definice ze standardu KGAS, které vymezují dodávku vůči koncovému zákazníkovi.

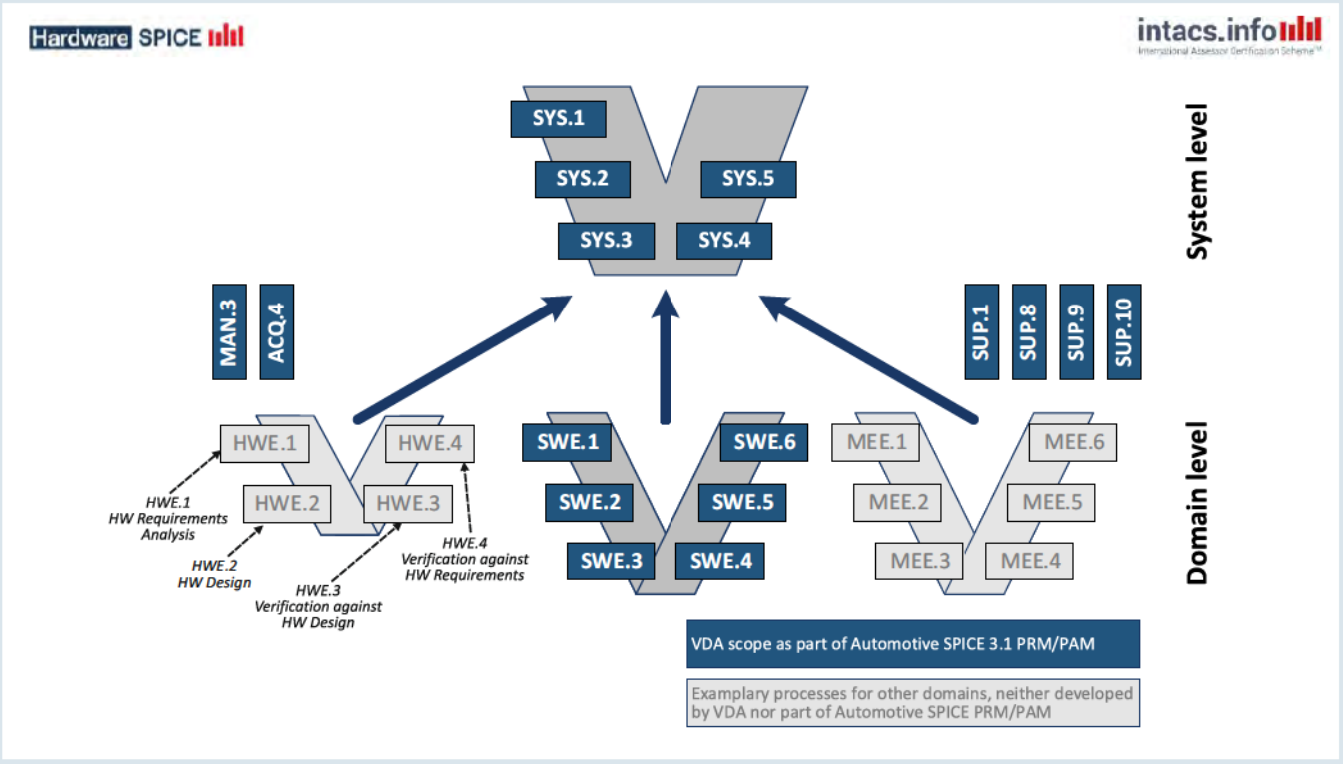
KGAS_2877/2879/3604/3606 definují následující:

- Systém je celá dodávka od dodavatele.
- Systém sestává ze systémových komponent popsaných v systémové architektuře.
- Typickými systémovými elementy jsou software (může být v produktu více než jednou, např. aplikační SW a basis SW), hardware (senzory, akční členy, pcb, konektory) a mechanické části (housing…).

Tedy i když samotný standard Automotive SPICE (Software Process Improvement and Capability determination – tedy „Vylepšování procesů vývoje softwaru a určení jeho způsobilosti") má přímo v názvu software, jeho rozsah se vztahuje na vývoj celého mechatronického produktu.

Následující procesní skupiny pokrývají vývoj celé dodávky:

Obrázek 2



System Process Group (SYS) – skupina procesů, které pokrývají definici a zpřesnění systémových požadavků a architektury a verifikačních procesů, které testují tuto specifikaci, tedy integrační a kvalifikační testování.

Z této skupiny vyčnívá // je vydělen proces **SYS.1 – Requirement elicitation**, který je protipólem ACQ 12,11,10, ale který má za úkol shromažďovat například požadavky interních stakeholderů (produkce, logistika, metrologie), ale i strategických úvah, jako jsou požadavky na znuvupoužitelnost (REU.2) či požadavky z ostatních domén, jako je například doména Functional Safety. O tomto procesu lze tvrdit, že i kdybychom dodávali tu nejdrobnější z komponent, stále by měl v projektu být přítomen, stejně jako MAN.3 project management. (viz obr. 2)

Skupiny Software engineering, Hardware engineering a **Mechanical engineering** pokrývají „své“ komponenty ve stejné logice – specifikace na funkcionalitu za pomoci požadavků, strukturování produktu za pomoci architektury a ověření obojího za pomoci integračního a kvalifikačního testingu.

Do procesních skupin v roce 2021 díky **VDA Automotive SPICE for Cybersecurity** přibyla nová procesní skupina Cyber Security engineering group (SEC), která pokrývá požadavky na cybersecurity opět ve formě požadavků a jejich ověření. Tento dodatek ale také přidal nové procesy do skupin ACQ a MAN – tedy požadavky na řízení dodavatelů z hlediska CySEC a analýza rizik z hlediska CySEC.

Předtím, než si ukážeme, jak vypadá popis konkrétního procesu, pojďme se na okamžik obrátit ke struktuře normy.

Logika normy aSPICE spočívá v tom, že existuje AutomotiveSPICE PAM – Process Assessment Model a PRM – Process Reference Model, od verze aSPICE 3.1 (aktuálně platná verze) sloučené do jediného dokumentu. Dále k tomuto dokumentu existují jednotlivé plug-in moduly, v současnosti HW/Mechanical a Agile. Toto vše je dostupné a volně ke stažení na www.automotivespice.com. Pro AutomotiveSPICE for Cybersecurity plugin je třeba se obrátit na VDA a zde tuto Red Volume zakoupit.

Každý z výše zmíněných souborů obsahuje následující sekce:

Process Capability determination – obsahuje, jakým způsobem se hodnotí procesy, je v souladu s rodinou norem ISO 33000.

Process reference model and performance indicators – obsahuje popis procesů a jak vyhodnotit jejich naplnění.

Process Capability levels and process attributes – poskytuje framework (rámec) pro hodnocení procesů na úrovni CL1-5.

Anex B – Workproduct characteristics – obsahuje popisy minimálního obsahu jednotlivých výstupů z procesů.

A konečně k popisu konkrétního procesu:

Process ID	SWE.1
Process name	Software Requirements Analysis

Hlavička, identifikace a název procesu

Process purpose	The purpose of the Software Requirements Analysis Process is to transform the software related parts of the system requirements into a set of software requirements.

Hlavní cíl procesu, kritérium, vůči kterému se posuzuje, zda byl důvod existence / přínos procesu naplněn

Process outcomes	As a result of successful implementation of this process: 1) the software requirements to be allocated to the software elements of the system and their interfaces are defined; 2) software requirements are categorized and analyzed for correctness and verifiability;

Čeho má být procesem dosaženo. Nyní si povšimněte barvy okraje, který se změní, a to proto, že přecházíme z PRM do PAM.

Base practices	**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]

Otázky/aspekty, pomocí kterých assessor může vyhodnotit, zda bylo process outcomes dosaženo. Všimněte si odkazu OUTCOME: poukazuje na oblasti, které je třeba zkontrolovat a které obsahují důkazy o naplnění procesu.

Output work products	17-08 Interface requirements specification →	[OUTCOME 1, 3]
	17-11 Software requirements specification →	[OUTCOME 1]
	17-50 Verification criteria →	[OUTCOME 2]

Mapování outcomes na annex B (workproducts)

17-11	Software requirements specification	• Identifies standards to be used • Identifies any software structure considerations/constraints • Identifies the required software elements • Identifies the relationship between software elements • Consideration is given to: - any required software performance characteristics - any required software interfaces - any required security characteristics required - any database design requirements - any required error handling and recovery attributes - any required resource consumption characteristics

Obsah jednotlivého workproduktu

Pokud již známe strukturu normy a popis procesů, mohli bychom se soustředit na samotné hodnocení, ale jako první je třeba si vyjasnit pojem VDA Scope, který bývá v požadavcích zákazníka a který je často špatně (dez?)interpretován.

Pokud zaostříme blíže na číslování procesů, všimneme si nekonzistence. Zatímco engineering procesy jsou číslovány v podstatě logickým pořadím, od 1 do N, kde je proces ACQ.1? MAN.1? – Tato zdánlivá nekonsistence je dána tím, že jsme se nezamysleli, proč Automotive SPICE. aSPICE je totiž jen podmnožinou standardu SPICE, který obsahuje další procesy, jež do automobilové domény nebyly převzaty. Doporučuji pro zajímavost srovnat jiné implementace SPICE, a to například Spice4Space a MedicalSPICE.

Tedy z celého rozsahu 53 původních (bez addonů) procesů bylo jen 32 vybráno do Automotive.

Co je to ale VDA Scope – tato definice 16 procesů není odvozená od rozsahu, které procesy máte implementovat, nýbrž od rozsahu, který je KONTROLOVÁN – jedná se o redukci kontroly na nejkritičtější a zákazníku neznámé faktory. Například proč vyžadovat kontrolu procesu SYS.1 requirement Elicitation, když se ho jako zákazník přímo účastním? Z hlediska rozsahu kontroly – assesmentu je obtížné zvládnout tento redukovaný rozsah za týden.

Tedy VDA Scope mluví o rozsahu kontroly, nikoli o rozsahu implementace, a jak si v druhé části příspěvku příště ukážeme, nedostatky v nekontrolovaných procesech se stejně přímo projeví na nedostatcích ve VDA Scope.

Autor:

Petr Švimberský – Konzultant, Principal aSPICE assessor, iNTACS regionall representative, VW Software Quality Improvement Leader a soudní znalec v oboru Kybernetika – vývoj softwaru.

Kontakt: *info@petrsvimbersky.cz*