



Testy systemów bezpieczeństwa w branży motoryzacyjnej

zgodnie z normą ISO 26262 (Pojazdy drogowe – Bezpieczeństwo funkcjonalne)
i Automotive SPICE – w oparciu o normę ISO/IEC 15504 (Software Process
Improvement and Capability Determination (SPICE))

ISO 26262 (Pojazdy drogowe – Bezpieczeństwo funkcjonalne)

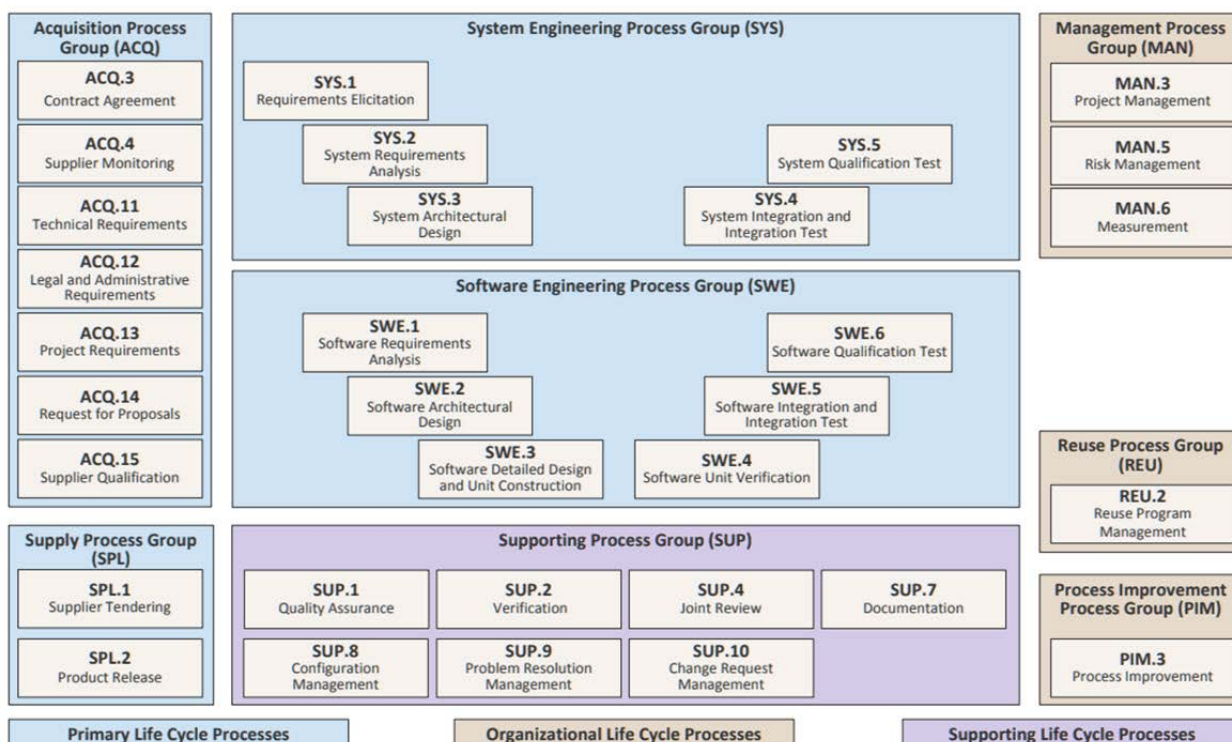
Norma dla bezpieczeństwa funkcjonalnego określa sposób szacowania wpływu projektowanego systemu na bezpieczeństwo człowieka. Dzięki zaangażowaniu specjalistów ds. technicznych, projektantów, ekspertów ds. bezpieczeństwa funkcjonalnego itp. istnieje możliwość przewidzenia zagrożeń, które mogą wystąpić podczas korzystania z projektowanego systemu. Przeprowadza się również ocenę liczbową dla trzech parametrów:

| | | |
|--------------------|-----|---|
| dotkliwość | 0-3 | W przypadku poziomie 0 sytuacja nie ma wpływu na bezpieczeństwo człowieka (nie jest poważna, narażenie na wystąpienie sytuacji jest niskie, a możliwość kontroli jest wysoka), podczas gdy poziom 3 i 4 odnoszą się do sytuacji mających największy wpływ na zdrowie i życie człowieka. |
| narażenie | 0-4 | |
| możliwość kontroli | 0-3 | |

Na podstawie tych trzech wartości szacowany jest poziom integralności bezpieczeństwa motoryzacyjnego Automotive Safety Integrity Level (ASIL D – największy wpływ na bezpieczeństwo, ASIL A – najmniejszy wpływ i poziom Quality Management QM – brak wpływu), który pozwala uzyskać ogólny obraz sytuacji w kontekście wymagań bezpieczeństwa, które należy dodatkowo wdrożyć.

Automotive SPICE

Automotive SPICE jest standardem określającym sposób prowadzenia dalszych prac nad systemem. Wszystkie etapy ASPICE mają zdefiniowane produkty pracy i zależności między nimi – jest to gotowa ścieżka, pod warunkiem, że (jeśli wykorzystywana w sposób poprawny) wszystkie wymagania zostały przeanalizowane, wdrożone i przetestowane, a także wszystkie informacje z tego procesu są zachowane i proste do znalezienia.



Rys. 1. Automotive SPICE – informacje ogólne (źródło: Standard ASPICE)

Opiera się on na Modelu V, czyli znanym w wielu branżach modelu cyklu życia oprogramowania, który został również dostosowany do specyfiki sektora motoryzacyjnego. Wszystkie wymagania, od opisu funkcjonalności systemu po wymogi bezpieczeństwa funkcjonalnego, przechodzą przez poszczególne etapy Modelu V. Są zbierane (SYS.1), analizowane (SYS.2) oraz klasyfikowane jako wymagania SW (standardowe), ME (mikro), EE (komercyjne) itp., a następnie zebrane i uwzględnione w ogólnej architekturze systemu (SYS.3).

W zależności od wyniku analizy na etapie SYS.2 postępuje się w sposób odpowiedni dla wskazanego typu. Wymagania dotyczące oprogramowania są analizowane (SWE. 1), zebrane i uwzględniane w architekturze oraz kodowane (SW.3). Następnie przechodzi się do fazy testowej: od SWE.4, czyli testów jednostkowych, przez testy wzajemnego oddziaływania komponentów oprogramowania za pośrednictwem zaimplementowanych interfejsów (SWE.5), aż po weryfikację zgodności wdrożenia oprogramowania z wymaganiami dotyczącymi oprogramowania, analizowanymi na etapie SWE.1 (SWE.6). Od tego momentu system jest ponownie traktowany jako całość (SW, ME, EE i inne – w zależności od typu systemu). Sprawdza się, czy wszystkie komponenty systemu i interfejsy (zdefiniowane na etapie SYS.3) działają zgodnie z oczekiwaniami (SYS.4) oraz czy cały system jest zaimplementowany tak, jak zostało to określone w wymaganiach systemowych (SYS.5). Istnieje również wiele elementów, które wspierają wdrażanie systemu.

Testy w przypadku organizacji Software Engineering Process Group (SWE) traktuje się jako czynnik determinujący jakość systemu. Projektuje się je tak, by umożliwiały dokładną weryfikację zachowania oprogramowania i zminimalizowanie jego wpływu na resztę systemu.

Testy systemów odbywają się na specjalnie zaprojektowanych stanowiskach testowych, które komunikują się z systemem za pomocą magistrali komunikacyjnej w taki sam sposób, jak w przypadku prawdziwego pojazdu. Znajdują się tu elementy takie jak zasilacze, generatory sygnałów itp. Tester manipuluje wartościami wejściowymi i sprawdza wartości wyjściowe poprzez symulację na typowym komputerze PC. Wykorzystywany interfejs użytkownika prezentuje całą komunikację z testowanym systemem oraz sposoby manipulowania nim. System może mieć graficzny interfejs użytkownika (GUI), który pomaga w testowaniu manualnym, lub być testowany automatycznie skryptami.

Testowanie systemu nie jest ostatnim etapem w przypadku testów automotive. Istnieją również testy walidacyjne i akceptacyjne (przede wszystkim, jeśli system jest zainstalowanym w pojeździe).

Podczas testów walidacyjnych oczekuje się, że system spełni wymagania uwzględniające czynniki fizyczne: wibracje, temperaturę i wilgotność, poziom hałasu itd. Testy wykonywane są w laboratoriach ze specjalistycznym wyposażeniem, takim jak, chociażby dźwiękoszczelne pomieszczenia.

Testy akceptacyjne przeprowadza się w pojeździe. Polegają na użytkowaniu systemu w docelowy sposób, jednak z uwzględnieniem przypadków brzegowych – na przykład, jeśli system wykorzystuje kamery do obserwacji pasażerów pojazdu, sprawdzane jest, czy aktywuje go obraz osoby, która jest ubrana w nietypowy sposób. Może się zdarzyć, że system wdrożony zgodnie z wymaganiami zawiedzie w pewnym momencie z powodu braku istnienia wymogu dla konkretnego przypadku brzegowego, którego nikt wcześniej nie wziął pod uwagę.

Jak opisano powyżej, testy mogą przynieść zaskakujące wyniki, pozwalając zaobserwować niespodziewane zachowania systemu. Ważne jest, aby przejść przez wszystkie etapy procesu testowania i zweryfikować również nieoczekiwane scenariusze – nawet jeśli możliwość wystąpienia takiego scenariusza wynosi 1%, nadal dotyczy on wielu pojazdów, ponieważ w tym przypadku ich liczba sięga tysięcy.

W wysoce ustrukturyzowanym sektorze motoryzacyjnym jakość oprogramowania układowego i testy mają kluczowe znaczenie dla użytkownika końcowego.

Dlaczego Sii?

Sii Polska, jako wysoce wyspecjalizowana organizacja, posiada zespoły doświadczonych inżynierów oraz wszystkie technologie niezbędne do przeprowadzenia procesów testowania oprogramowania zgodnie z normą ISO 26262 i Automotive SPICE. Od lat wspieramy największych dostawców Tier1 na świecie, realizując projekty dotyczące testowania systemów wbudowanych.



Jeśli jesteś producentem oprogramowania działającym w branży motoryzacyjnej, zapoznaj się z naszą ofertą:

Motoryzacja

Systemy wbudowane