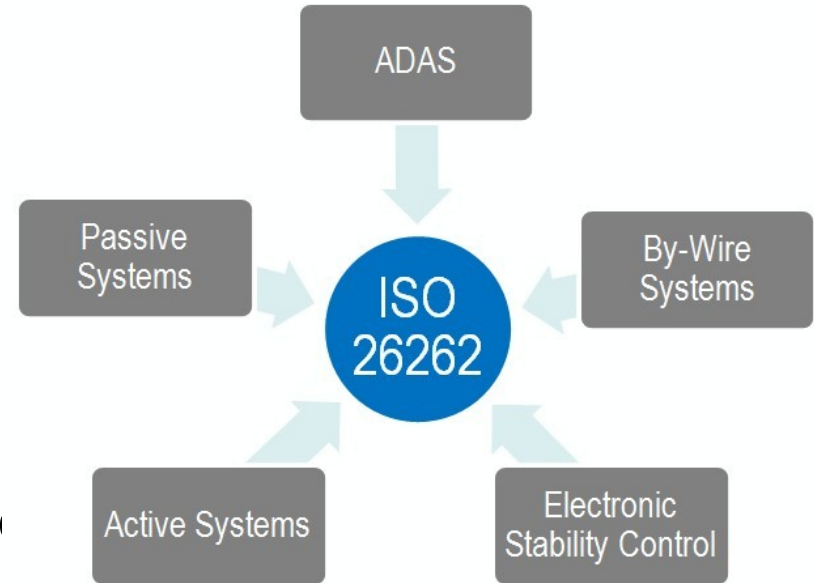


ISO26262

Zakres ISO26262

- ADAS – Advanced driver-assistance systems (np. LiDAR, image processing, car-net, image processing)
- Passive systems – systemy bezpieczeństwa pasywnego
- Active systems – systemy bezpieczeństwa aktywnego
- By-wire systems – systemy sterowania
- Electronic Stability Control – systemy stabilizacji jazdy i pokonywania zakrętów



Elementy normy ISO26262

- Norma składa się z 10 części:
 1. Słownik (ang. Vocabulary)
 2. Zarządzanie bezpieczeństwem funkcjonalnym (ang. Management of functional safety)
 3. Faza koncepcji (ang. Concept phase)
 4. Tworzenie produktu na poziomie systemu (ang. Product development at the system level)
 5. Tworzenie produktu na poziomie komponentów sprzętowych (ang. Product development at the hardware level)
 6. Tworzenie produktu na poziomie oprogramowania (ang. Product development at the software level)
 7. Produkt i operacje (ang. Product and operation)
 8. Procesy wspierające (ang. Supporting processes)
 9. Poziomy ASIL (ang. Automotive Safety Integrity Level and safety-oriented analysis)
 10. Wytyczne standardu (ang. Guideline ISO26262)

1. Vocabulary

2. Management of functional safety

2-5 Overall safety management

2-6 Safety management during the concept phase and the product development

2-7 Safety management after the item's release for production

3. Concept phase

3-5 Item definition

3-6 Initiation of the safety lifecycle

3-7 Hazard analysis and risk assessment

3-8 Functional safety concept

4. Product development at the system level

4-5 Initiation of product development at the system level

4-6 Specification of the technical safety requirements

4-7 System design

4-11 Release for production

4-10 Functional safety assessment

4-9 Safety validation

4-8 Item integration and testing

7. Production and operation

7-5 Production

7-6 Operation, service (maintenance and repair), and decommissioning

5. Product development at the hardware level

5-5 Initiation of product development at the hardware level

5-6 Specification of hardware safety requirements

5-7 Hardware design

5-8 Evaluation of the hardware architectural metrics

5-9 Evaluation of the safety goal violations due to random hardware failures

5-10 Hardware integration and testing

6. Product development at the software level

6-5 Initiation of product development at the software level

6-7 Software architectural design

6-8 Software unit design and implementation

6-9 Software unit testing

6-10 Software integration and testing

6-11 Verification of software safety requirements

8. Supporting processes

8-5 Interfaces within distributed developments

8-6 Specification and management of safety requirements

8-7 Configuration management

8-8 Change management

8-9 Verification

8-10 Documentation

8-11 Confidence in the use of software tools

8-12 Qualification of software components

8-13 Qualification of hardware components

8-14 Proven in use argument

9. ASIL-oriented and safety-oriented analyses

9-5 Requirements decomposition with respect to ASIL tailoring

9-6 Criteria for coexistence of elements

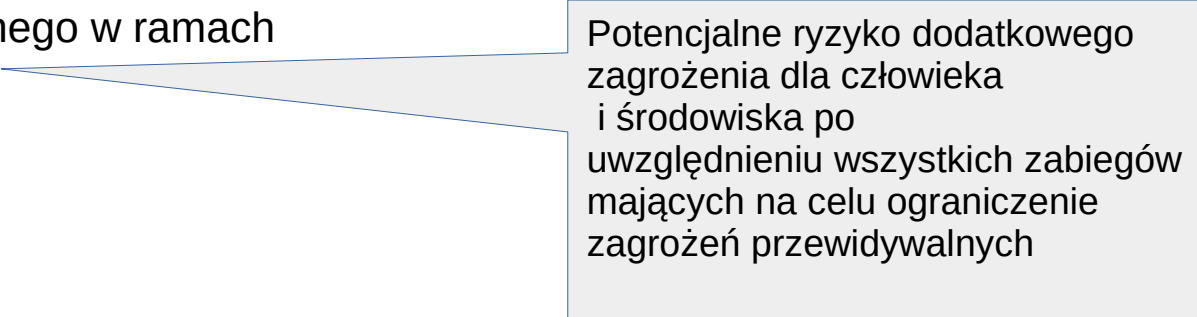
9-7 Analysis of dependent failures

9-8 Safety analyses

10. Guideline on ISO 26262

Cykl wytwarzania oprogramowania

- Norma promuje dobre praktyki związane z procesem wytwarzania oprogramowania w obszarze procesowym (ang. Automotive Safety Lifecycle):
 - Zarządzanie (ang. management)
 - Tworzenie (ang. development)
 - Produkcja (ang. production)
 - Operacje (ang. operation)
 - Serwisowanie (ang. service)
 - Likwidacja (ang. decommissioning)
- Do każdego z tych etapów, dostarcza opis aktywności występujących w danym cyklu
- Ma bezpośrednie odzwierciedlenie w Automotive SPICE (ISO15504)
- Bazuje na szacowaniu ryzyka rezydualnego w ramach ASIL (dalej)

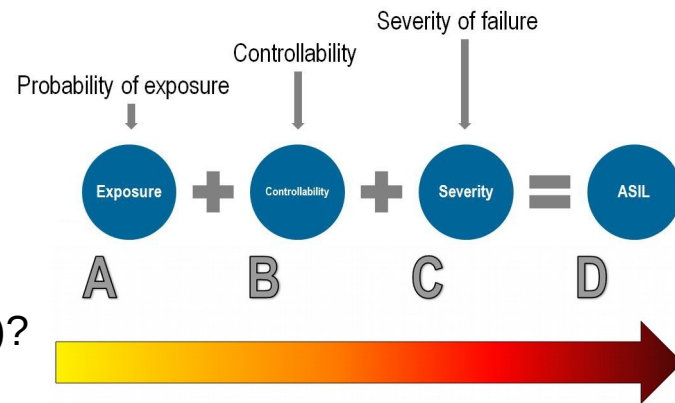


Potencjalne ryzyko dodatkowego zagrożenia dla człowieka i środowiska po uwzględnieniu wszystkich zabiegów mających na celu ograniczenie zagrożeń przewidywalnych

ASIL

- Norma ISO26262 jest dedykowaną dla branży Automotive pochodną IEC61508 która adresuje potrzeby bezpieczeństwa dla wszystkich systemów E/E
- Pojęcia poziomów bezpieczeństwa SIL (ang. Safety Integrity Level), zostały zmodyfikowane pod potrzeby przemysłu samochodowego
- Odpowiadają na pytanie: Jakie reperkusje czekają kierującego w przypadku awarii jeśli dane awaria wystąpi?
- O poziomie ASIL decyduje:
 - Jak długo występuje narażenie na negatywny efekt (ang. Exposure)?
 - Jak dokładnie możemy zminimalizować jego skutki (ang. Controllability)?
 - Jak poważne są konsekwencje wystąpienia awarii (ang. Severity)?

ASIL Level	Random hardware failure target values
<i>D</i>	$< 10^{-8}$ per hour
<i>C</i>	$< 10^{-7}$ per hour
<i>B</i>	$< 10^{-7}$ per hour
<i>A</i>	$< 10^{-6}$ per hour



Szacowanie ASIL (1/2)

- Severity:
 - S0 – brak konsekwencji
 - S1 – małe lub średnie konsekwencje
 - S2 – poważne konsekwencje (przeżycie możliwe)
 - S3 – zagrażające życiu konsekwencje, przeżycie niemożliwe
- Exposure:
 - E0 – nieistotne (pomijalne)
 - E1 – bardzo niskie (niezauważalne - krótkotrwałe)
 - E2 – niskie (krótkotrwałe - zauważalne)
 - E3 – średnie (widoczne)
 - E4 – wysokie (częste)
- Controlability:
 - C0 – kontrolowane
 - C1 – łatwa kontrola
 - C2 – kontrola wymagająca zaangażowania
 - C3 – trudna i bardzo trudna kontrola

Szacowanie ASIL (2/2)

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

Komponenty sprzętowe

- Kwalifikacja elementów sprzętowych odbywa się wg:
 - Wpływu ryzyka ze źródła danego komponentu na całość rozwiązania
 - Oszacowania jego awaryjności
- Komponenty sprzętowe są testowane w środowisku ich naturalnego działania (z wpływem warunków zewnętrznych)
- Na podstawie danych z testów oraz ich analizy statystycznej, następuje kwalifikacja ich awaryjności

Komponenty oprogramowania

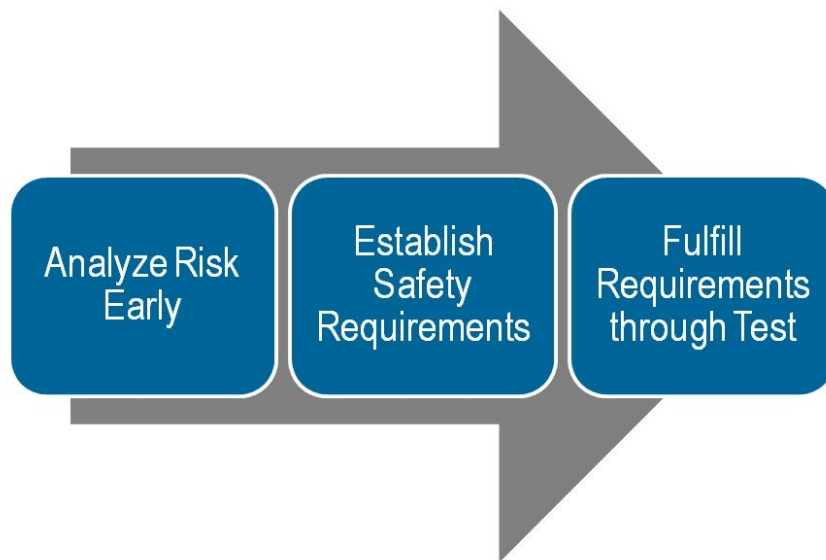
- Dla tych komponentów, przeprowadza się analizy:
 - Wymagań funkcjonalnych wpływających na ich bezpieczeństwo
 - Zużycia zasobów platformy sprzętowej w normalnym, uśpionym (ang. standby) oraz przeciążonym trybie
- Norma promuje użycie przetestowanych rozwiązań, znanych szkieletów aplikacyjnych (ang. frameworks) oraz bibliotek
- Testowanie obejmuje także wymuszanie błędów w komponencie (poprzez odbiegające od normy dane wejściowe)
- Norma wymaga odkładania informacji o odkrytych błędach i ich replikacji przy tworzeniu podobnych lub identycznych komponentów
- Znaleziony błąd który „ucieleśni się” awarią, wpływa na cały proces projektowania oprogramowania (począwszy do etapu „design”)

„Sprawdzone w działaniu”

- Norma nie wymaga pełnego sprawdzania bezpieczeństwa komponentów sprzętowych jak i programowych które są już wdrożone i obecne na rynku w milionach egzemplarzy
- Zakłada że przed ISO26262 także powstawały bezpieczne systemy
- Obejmuje to:
 - Komponenty występujące w podobnych aplikacjach (np. systemy RTOS)
 - Starsze przetestowane, wdrożone i poprawnie działające systemy
 - Narzędzia testujące które udowodniły swoje poprawne działanie w innych kontekstach związanych z bezpieczeństwem funkcjonalnym

Sznyt procesu

- Norma narzuca by każdy z procesów wytwarzania, przechodził przez ścieżkę:
 - Wczesnej analizy ryzyka jakie niesie ze sobą
 - Tworzenia wymagań bezpieczeństwa
 - Dowodu w postaci testów spełniania tychże wymagań



Testy

- Test wykrywający naruszenie bezpieczeństwa funkcjonalnego w świetle normy ISO26262 (jeśli wykrył błąd), powinien mieć odnotowany przebieg i wpływać także na bieżący i przyszły projekt rozwiązania (zgodnie z wykładnią wzrastającego kosztu likwidacji od procesu tworzenia poprzez wdrożenie aż do użycia – zasada x 10)
- Testy wykonywane są end-to-end (poziom urządzeń elektrycznych, elektronicznych, warstwa oprogramowania)
- Narzędzia testujące tak jak wszystkie inne związane z tworzeniem oprogramowania, kwalifikowane są na poziomach zaufania...

Poziomy TCL

- TCL (ang. Tool Confidence Level) – poziom zaufania narzędzia
- Na poziom zaufania do narzędzia wpływa:
 - Możliwość nieprawidłowego działania oprogramowania i błędnego wyjścia które wpływa na naruszenie jakiegokolwiek wymagania związanego z bezpieczeństwem
 - Prawdopodobieństwo uniknięcia i detekcji takiego zachowania w wynikach pracy narzędzia
- Poziomy numerowane są do 1 do 4 gdzie poziom 1 to niskie zaufanie a 4 wysokie zaufanie do narzędzia.

TCL4

TCL3

TCL2

TCL1

Wymagania kwalifikacji narzędzia

- Wyniki działania narzędzia, odnoszone są do ASIL
- Narzędzie powinno posiadać:
 - Dokumentację użycia
 - Numer wersji
 - Opis celu działania i jego właściwości
 - Opisany proces instalacji i/lub wariantów instalacji
 - Określenie (dokładnego) środowiska pracy
 - Sprawdzone działanie w warunkach anormalnych
- Kwalifikacja narzędzia odbywa się w etapach:
 - STQP (ang. Software Tool Qualification Plan) – etapy: określenie planu kwalifikacji dla narzędzia, określenie przypadków użycia narzędzia
 - STD (ang. Software Tool Documentation) – zebranie i sprawdzenie kompletności dokumentacji narzędzia
 - STCA (ang. Software Tool Classification Analysis) – etapy: określenie wpływu narzędzia (TI – Tool Impact TI1 nie wpływa na bezpieczeństwo, TI2 wpływa), określenie poziomu TD (ang. Tool Error Detection, TD1 słaba diagnostyka TD4 silna)
 - STQR (ang. Software Tool Qualification Report)

Zaufanie przez „sprawdzone w działaniu”

- Nie każde narzędzie powinno podlegać kwalifikacji zaufania w świetle ISO26262
- Norma (jak poprzednio dla komponentów) zakłada że narzędzia sprawdzone w poprzednich projektach mogą zostać uznane za zaufane
- Można sobie na to pozwolić w następujących warunkach:
 - Narzędzie używane w tych samych przypadkach użycia poprzednio
 - Specyfikacja narzędzia nie ulega zmianie (ta sama wersja sprawdzona wcześniej)
 - Narzędzie nie wpływa na aspekty bezpieczeństwa funkcjonalnego