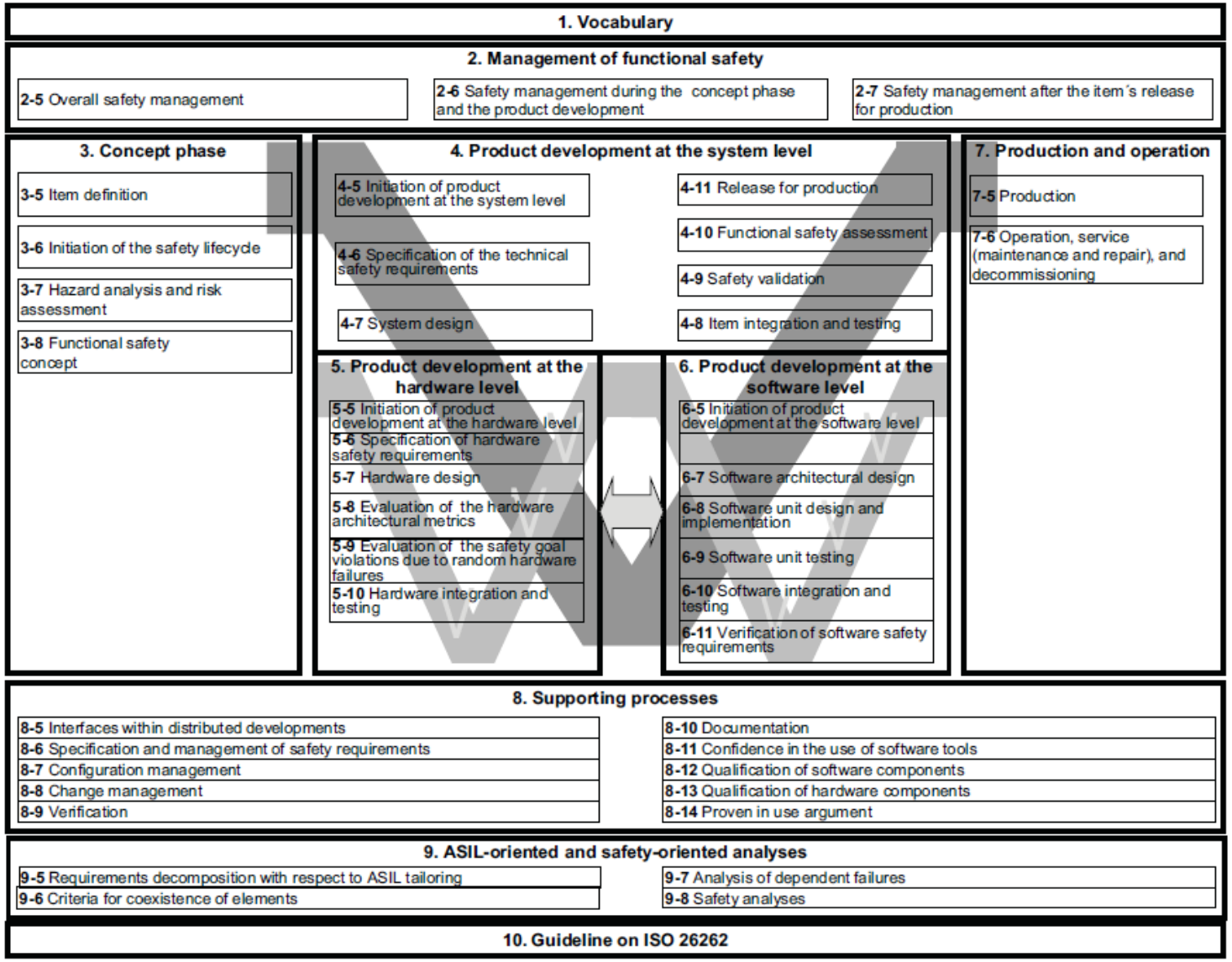
Az ISO 26262

- Alkalmazási terület
  - sorozatgyártott,
  - 3.500 kg-ot nem meghaladó
  - személygépjárművek
  - elektromos és/vagy elektronikus (E/E) komponenseket tartalmazó
  - biztonságreleváns rendszereire.
- Cél: funkcionális biztonság
  - kizárva az elektromos áramütés, tűz stb. veszélyeztetések

Felépítés

1. Terminológia
2. Funkcionális biztonság menedzsment
3. Koncepció fázis
4. Rendszerszintű termékfejlesztés
5. Hardver-szintű termékfejlesztés
6. Szoftver-szintű termékfejlesztés
7. Gyártás és üzemeltetés
8. Támogató folyamatok
9. ASIL-orientált és biztonságorientált elemzések
10. Alkalmazási irányelvek

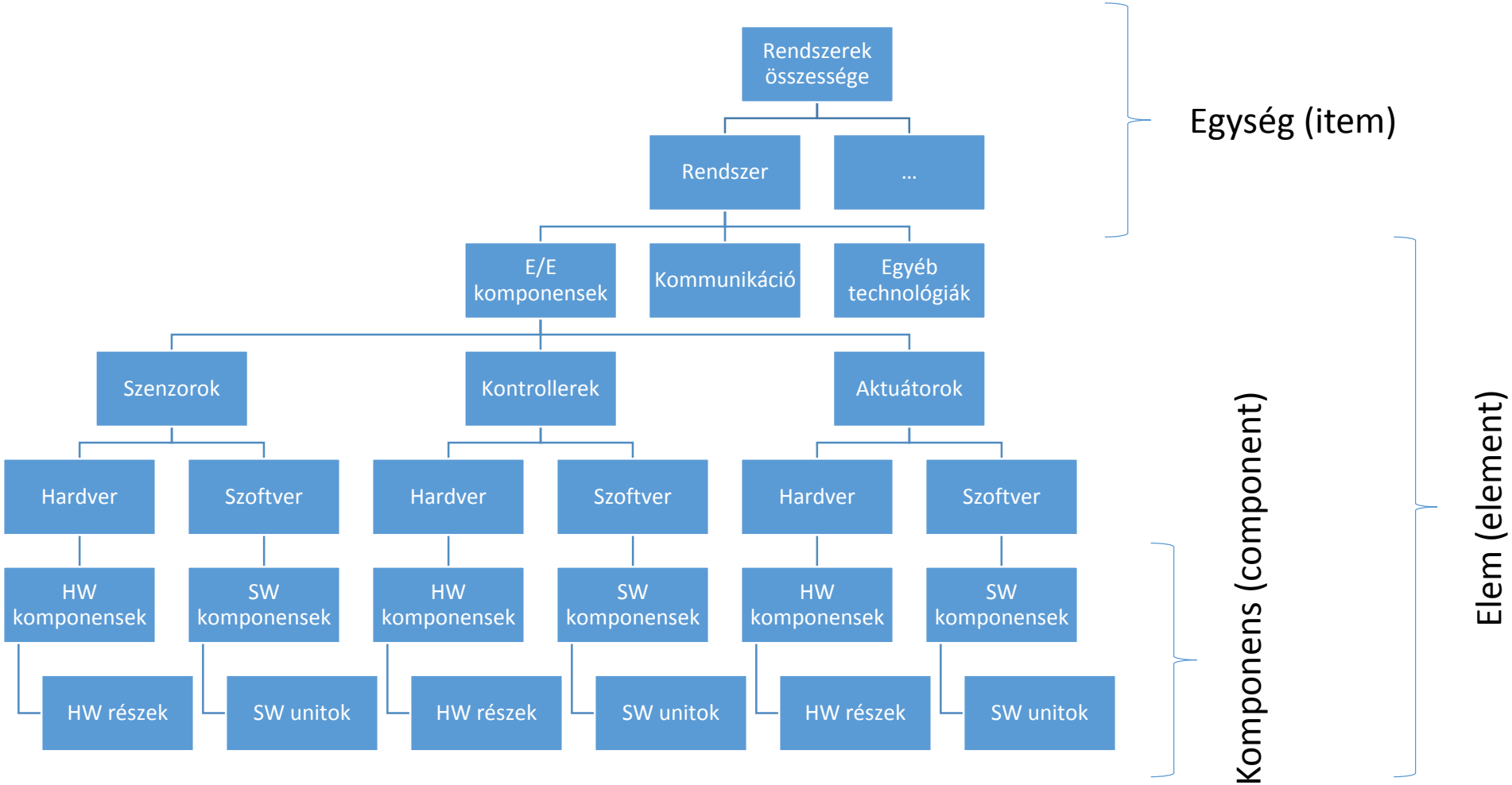
Az ISO 26262 részeinek felépítése



3. Koncepció fázis

5. Egység definiálása
    - Az egység, kapcsolatai, interfészei leírása
6. Biztonsági életciklus indítása
    - A fejlesztés és módosítás megkülönböztetése
    - Az életciklus tevékenységek meghatározása
7. Veszélyelemzés és kockázatértékelés
    - Az egység helytelen működésével kapcsolatos veszélyeztetések kategorizálása
    - Biztonsági célok meghatározása
8. Funkcionális biztonsági koncepció
    - Funkcionális biztonsági követelmények származtatása a biztonsági célokból
    - A biztonsági követelmények allokálása

3. Koncepció fázis – 5. Az egység definiálása



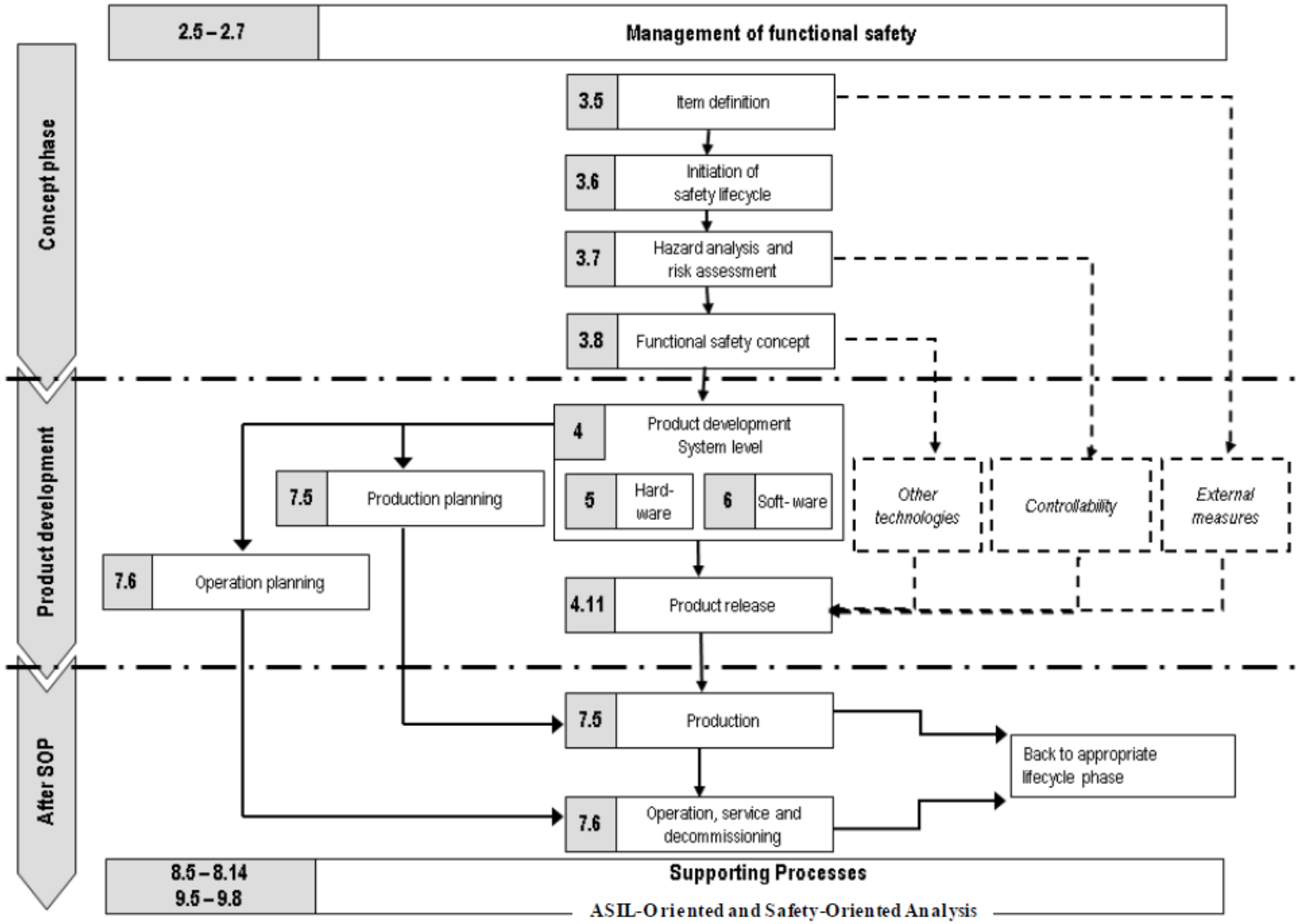
3. Koncepció fázis – 5. Az egység definiálása

- Cél: az érintett egység definiálása és leírása, beleértve a kapcsolatokat és interakciókat más elemekkel
- Bemenő információk: termék ötlet, projekt vázlat, releváns szabadalmak, előzetes vizsgálatok stb.
- A definiálás során világossá kell válnia
  - a funkcionális követelményeknek
  - a nem-funkcionális követelményeknek,
  - a többi egységgel és a környezettel való kapcsolatnak, hatásnak.

3. Koncepció fázis – 5. Az egység definiálása

- Ennek érdekében meg kell határozni
  - a funkcionális koncepciót, az egység célját és funkcionalitását, üzemmódjait, állapotait,
  - üzemi és környezeti feltételeket/kényszereket,
  - törvényi szabályozásokat,
  - a helytelen működés következményeit.
- Definiálni kell a rendszerhatárokat, meg kell határozni
  - az egység elemeit
  - az egység működésének hatását más egységekre
  - a más egységekkel való interakciót
  - más egységek által elvárt funkciók
  - más egységektől elvárt funkciók
  - a feladatmegosztást a más egységekkel
  - működési szcenáriók.

3. Koncepció fázis – 6. Biztonsági életciklus



3. Koncepció fázis – 6. Biztonsági életciklus

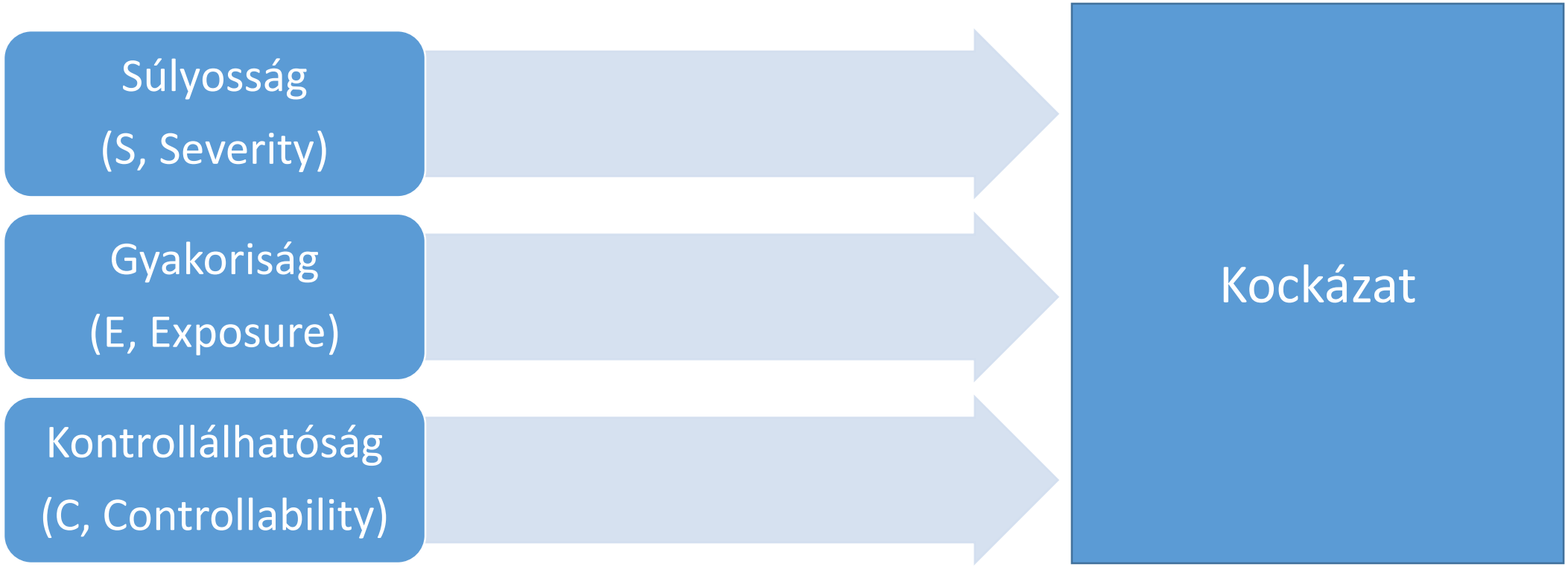
- Módosítás vagy új fejlesztés?
  - Módosítás
    - hatáselemzés szükséges
    - az életciklus testreszabása, a szükséges tevékenységek újbóli elvégzése
  - Új fejlesztés
    - A teljes életciklust végig kell vinni
    - Következő lépés: veszélyelemzés és kockázatértékelés

3. Koncepció fázis – 7. Veszélyelemzés és kockázatértékelés

- Veszélyelemzés
  - Az egység funkcionális viselkedését kell figyelembe venni (a belső felépítés ismerete lényegtelen)
  - A tervezett biztonsági mechanizmusokat figyelmen kívül kell hagyni
- Lépések
  - Szituáció analízis
    - Figyelembe kell venni a járművek helyes és helytelen (nem üzemszerű) használatát is – ésszerű mértékig
  - Veszélyeztetések azonosítása
    - Szisztematikus, dokumentált eljárással (brainstorming, ellenőrző lista, FMEA stb.)
    - A veszélyeztetéseket a jármű szintjén kell meghatározni (azaz mi a hatás a jármű egészét vizsgálva)
    - A veszélyeztetések következményeinek azonosítása

3. Koncepció fázis – 7. Veszélyelemzés és kockázatértékelés

- A veszélyeztetések osztályozása (kockázat meghatározása)



3. Koncepció fázis – 7. Veszélyelemzés és kockázatértékelés

- Kockázat: $R = F(f, C, S)$
  - f: gyakoriság (frequency of occurence)
  - C: kontrollálhatóság (elkerülhetőség, menekülési lehetőség)
  - S: súlyosság (severity)
- Gyakoriság: $f = E \times \lambda$
  - E: a veszélyeztetés fellépésének gyakorisága/valószínűsége, mennyi ideig vannak az egyes személyek a potenciálisan veszélyeztető helyzetben
    - ISO 26262: az adott vezetési szcenárió fellépésének valószínűsége
  - λ : az egység meghibásodási gyakorisága (szisztematikus és véletlenszerű), amely a veszélyes szituációhoz vezet
    - ezt nem ismerjük a fejlesztés kezdetén, ezért nem vesszük figyelembe, illetve éppen a megfelelő mérték elérésére törekszünk

Súlyosság
Abbreviated Injury Scale

- AIS 0 : nincs sérülés
- AIS 1 : könnyű sérülés (bőrsérülés, izomfájdalom stb.)
- AIS 2 : mérsékelt sérülés (mélyebb vágás, max 15 perc eszméletvesztés
- AIS 3 : súlyos, de nem életveszélyes (csonttörés [nem koponya], ízületi sérülés…)
- AIS 4 : súlyos, életveszélyes, valószínű túléléssel (súlyos csontsérülések, 12 óra eszméletvesztés)
- AIS 5 : kritikus sérülés, életveszélyes, bizonytalan túléléssel (12+ óra eszméletvesztés, belső vérzés …)
- AIS 6 : extrém kritikus, halálos sérülés, haláleset

Súlyosság

- AIS → ISO 26262 súlyossági kategóriák

	Class of severity (see Table 1)			
	S0	**S1**	**S2**	**S3**
Reference for single injuries (from AIS scale)	— AIS 0 and less than 10 % probability of AIS 1-6 — Damage that cannot be classified safety-related	More than 10 % probability of AIS 1-6 (and not S2 or S3)	More than 10 % probability of AIS 3-6 (and not S3)	More than 10 % probability of AIS 5-6

	Class			
	S0	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Példák súlyossági kategóriákra Vezetési szcenáriók alapján

- S0: könnyű ütközés, súrolás, parkolóhelyre be- és kiállás során keletkező sérülések, útelhagyás ütközés, borulás nélkül
- S1: oldalsó ütközés (pl. fának) nagyon kis sebességgel, oldalsó, hátsó, első ütközés másik személyautóval nagyon kis sebességgel
- S2: ütközés kis sebességgel, gyalogos/biciklis ütközés kanyarodás során (városi kereszteződés)
- S3: ütközés közepes sebességgel stb.

Megj: S0 esetén nincs ASIL hozzárendelés

Gyakoriság

- Kategóriák: E0, E1, E2, E3, E4
- E0: nagyon valószínűtlen; pl. jármű és repülőgép ütközése, természeti katasztrófák (földrengés, hurrikán stb.)
- A többi kategóriát olyan esetekre alkalmazzuk, amikor a szituáció fennállásának időtartama vagy gyakorisága miatt veszélyeztetés alakulhat ki.
  - A fennállás időaránya a teljes időalaphoz képest
  - A fellépés gyakorisága időegység alatt
  - A kettő kombinációja
  - Fellépési gyakoriság és a hibafelfedési idő szorzata ($\sigma \times T$) on-demand jellegű rendszereknél (pl. légzsák)

Gyakoriság

- Időtartam aránya szerint

	Class of probability of exposure in operational situations (see Table 2)			
	E1	**E2**	**E3**	**E4**
Duration (% of average operating time)	Not specified	<1 % of average operating time	1 % to 10 % of average operating time	>10 % of average operating time

- Fellépési gyakoriság szerint

	Class of probability of exposure in operational situations (see Table 2)			
	E1	**E2**	**E3**	**E4**
Frequency of situation	Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average

Kontrollálhatóság

- Annak valószínűsége, hogy egy átlagos (reprezentatív) járművezető meg tudja-e tartani/vissza tudja-e szerezni az irányítást, illetve a környező érintett személyek el tudják-e kerülni a veszélyeztetést

Driving factors and scenarios	Class of controllability (see Table 3)			
	C0	C1	C2	C3
	Controllable in general	99 % or more of all drivers or other traffic participants are usually able to avoid harm	90 % or more of all drivers or other traffic participants are usually able to avoid harm	Less than 90 % of all drivers or other traffic participants are usually able, or barely able, to avoid harm

Kontrollálhatóság példák

- C0 (mindenki): a rádió hangerő váratlan felerősödése, figyelemelterelő jelzések
- C1 (99%+): a vezetőülés pozíciójának helytelen állítása (lefékezés, megállás), kormány blokkolása induláskor
- C2 (90%+): ABS hiba vészfékezésnél, lámpák kikapcsolása sötét úton
- C3 (90%-): fékhiba, hibás légzsák nyitás nagy sebességnél

ASIL meghatározás

- ASIL: Automotive Safety Integrity Level
- ASIL A < ASIL B < ASIL C < ASIL D
- nincs ASIL besorolás: QM elegendő

- Az ASIL besorolás minden azonosított veszélyeztetéshez el kell végezni

ASIL meghatározás

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Biztonsági célok (safety goal) meghatározása

- Minden ASIL besorolású veszélyeztetéshez biztonsági célt kell meghatározni
- Biztonsági cél:
  - magasszintű biztonsági követelmény az egységre vonatkoztatva
  - funkcionális célkitűzésként meghatározva
- Több veszélyeztetéshez együtt is tartozhat egy biztonsági cél
- Minden biztonsági célhoz rendelődik ASIL
- A biztonsági cél adott esetben továbbadódik (karbantartás, üzemeltetés stb.)
- Verifikáció:
  - A veszélyelemzést, a kockázatértékelést, az ASIL hozzárendelést és a biztonsági célok meghatározását független személyeknek kell verifikálnia (review)

3. Koncepció fázis – 8. Funkcionális biztonsági koncepció

- Cél:
  - funkcionális biztonsági követelmények származtatása a biztonsági célokból,
  - a funkcionális biztonsági követelmények allokálása az előzetes architektúrára vagy külső intézkedésekre.
- Funkcionális biztonsági koncepció
  - biztonsági intézkedések, biztonsági mechanizmusok, amelyeket az architekturális elemek szintjén meg kell valósítani
    - hibadetektálás és kezelés
    - biztonságos állapotba juttatás
    - hibatűrési technikák,
    - hibafelismerés és a vezető figyelmeztetése

3. Koncepció fázis – 8. Funkcionális biztonsági koncepció