A BIZTONSÁGINTEGRITÁS ÉS A BIZTONSÁGORIENTÁLT ALKALMAZÁSI FELTÉTELEK TELJESÍTÉSE

A VASÚTI BIZTOSÍTÓBERENDEZÉSEK TERVEZÉSE ÉS LÉTREHOZÁSA SORÁN

Szabó Géza

certuniv

Bevezetés

- Az előadás célja, vasúti alrendszerekre való érvényessége.
- Kapcsolódások: CSM

- Előadói háttér: gyakorlat (Certuniv), elmélet (BME KJIT)
- A téma aktualitása
- Kapcsolódó kutatásaink: Biztonsági fejlesztési folyamat minősítése; biztonságorientált alkalmazási feltételek felhasználása

Bevezetés

Megfelelésértékelés a vasúti technikában

- Interoperabilitás (NoBo);
- Hazai jogszabályoknak való megfelelés (OVSZ I. vagy OVSZ II. és feltétfüzetek) (Debo);
- Biztonságértékelés (MSZ-EN 50129,50128).
- (Építési termékek /NME vs. vasúti specifikációk/)

Interoperabilitás:alrendszer és rendszerkomponens.

Hazai jogszabályoknak való megfelelés: alrendszer, rendszerkomponens (generikus termék).

Biztonságértékelés: általános termék, általános alkalmazás, specifikus alkalmazás (plusz: modularitás).

Biztonságorientált alkalmazási feltételek

Az alrendszerrel / rendszerkomponessel kötelezően átadandó szabálygyűjtemény

Tartalmazhat műszaki, alkalmazási (tervezési), kezelési eljárási, üzemeltetési (karbantartási) eljárási stb. szabályokat.

Rendszerszállító – rendszerüzemeltető közötti interfész

Belső interfészek:

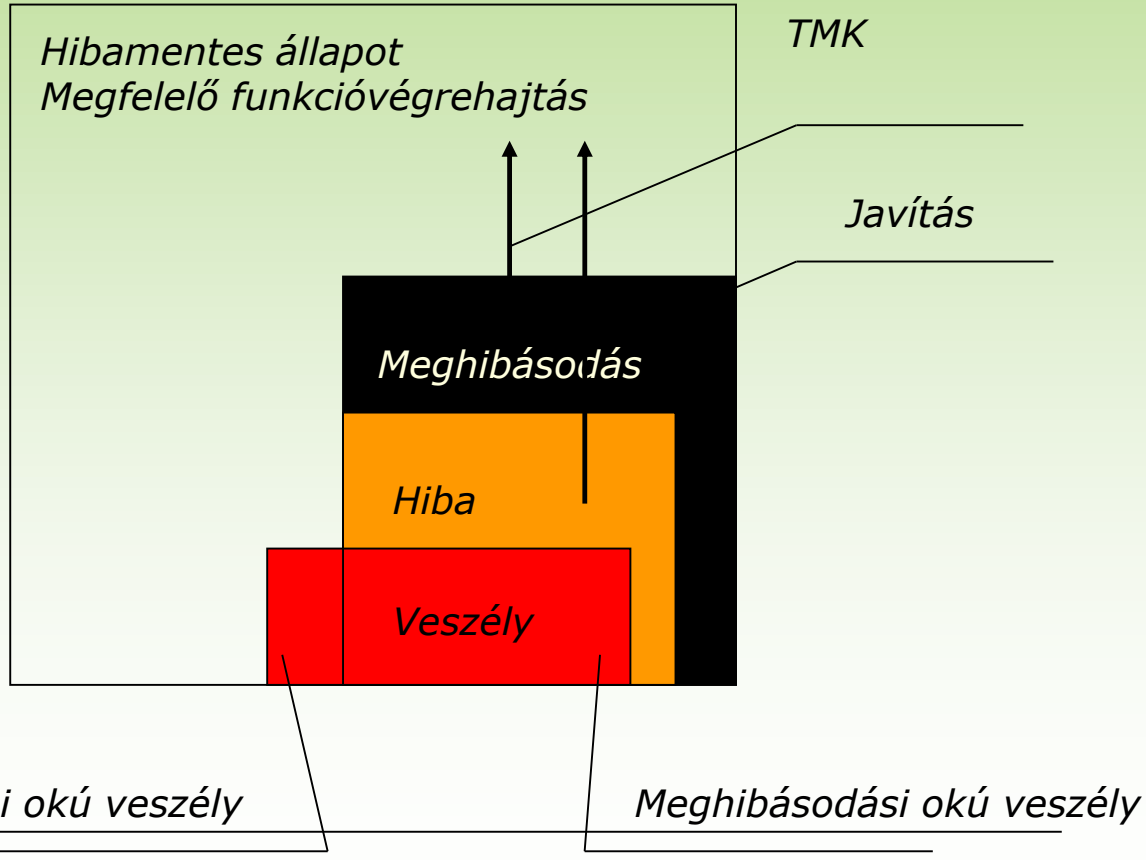
- Fejlesztési fázisok között,
- Generikus termék és specifikus alkalmazás között.

A biztonság kockázati alapú megközelítése

- Kockázati alapú megközelítések bevezetése
  - (régen: mechanikai függések és túlméretezések – egyszerűen átlátható biztonság; jelfogófüggések: már törekvés az uniformizálásra; elektronikus eszközök: túl nagy állapottér)
- Abszolút biztonság nem létezik
- A teljes kitesztelés egyre inkább lehetetlen (bizalom kell)
- Védekezés a véletlen meghibásodások és a szisztematikus hibák ellen,
- Védekezés mértéke a kockázat, illetve az elvárt kockázatcsökkentés függvénye.
- THR és SIL
  - Véletlen hibák ellen: THR (Tolerable Hazard Rate)
  - Szisztematikus hibák ellen: SIL (Safety Integrity Level)

Mi ellen kell védekezni?

- Számolni kell un. szisztematikus hibával is (mindig tervezési – emberi hiba)
  - Természetesen ez is felfedhető – csak a felfedése nehéz (lásd paksi kazetta tisztítás)



Kockázatok értelmezése

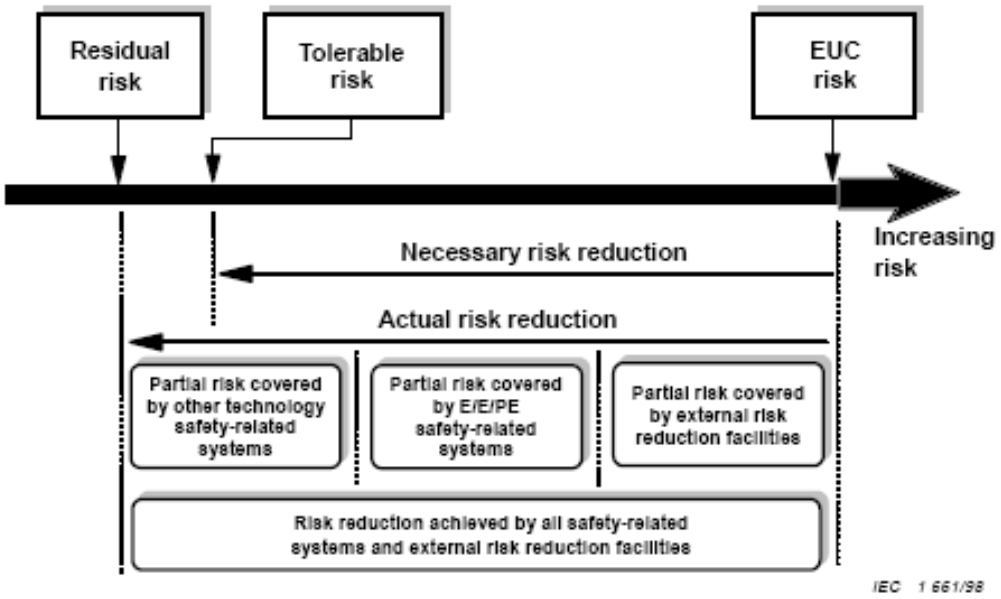


Figure A.1 – Risk reduction: general concepts

Igény szerinti üzem:
A kockázatcsökkentés valószínűségi

Folyamatos üzem:
A kockázatcsökkentés gyakorisági
(ECU risk = 1)

Fontos! A kockázatelemzés, illetve a szabványok azt deklarálják, hogy lesz egy adott mértékű maradék kockázat, vagyis a rendszerünkbe beépítjük a veszteség lehetőségét!

Védekezés a hibák ellen

- THR és SIL kapcsolata: arányosság elve

Table 3 – Safety integrity levels: probability of failure on demand

DEMAND MODE OF OPERATION		
Safety integrity level (SIL)	Target average probability of failure on demand	Target risk reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	>10 000 to ≤100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	>1 000 to ≤10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	>100 to ≤1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	>10 to ≤100

Table 4 – Safety integrity levels: frequency of dangerous failures of the SIF

CONTINUOUS MODE OF OPERATION	
Safety integrity level (SIL)	Target frequency of dangerous failures to perform the safety instrumented function (per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Követelményteljesítések

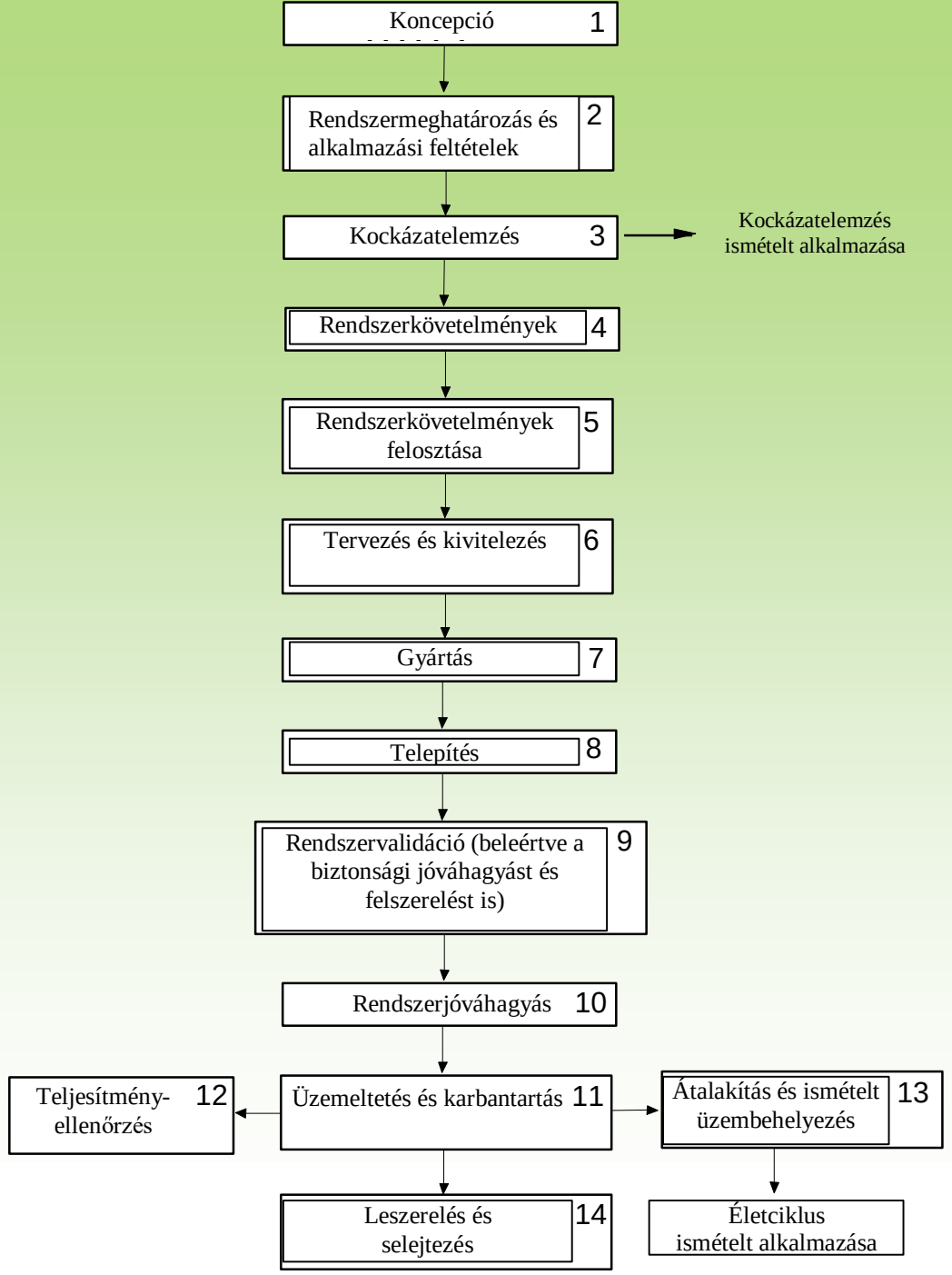
- THR teljesítése
  - Architektúra,
  - Redundancia,
  - Egyedi elem megbízhatóságok.
- SIL teljesítése
  - Életciklus, biztonsági életciklus
  - Kompetencia,
  - Függetlenség,
  - Dokumentáltság (információáramlás),
  - Módszerek és eljárások

- A SIL követelmények teljesítése életciklus-szerű
  - Utólag nem pótolható,
  - Utólag nehezen igazolható.

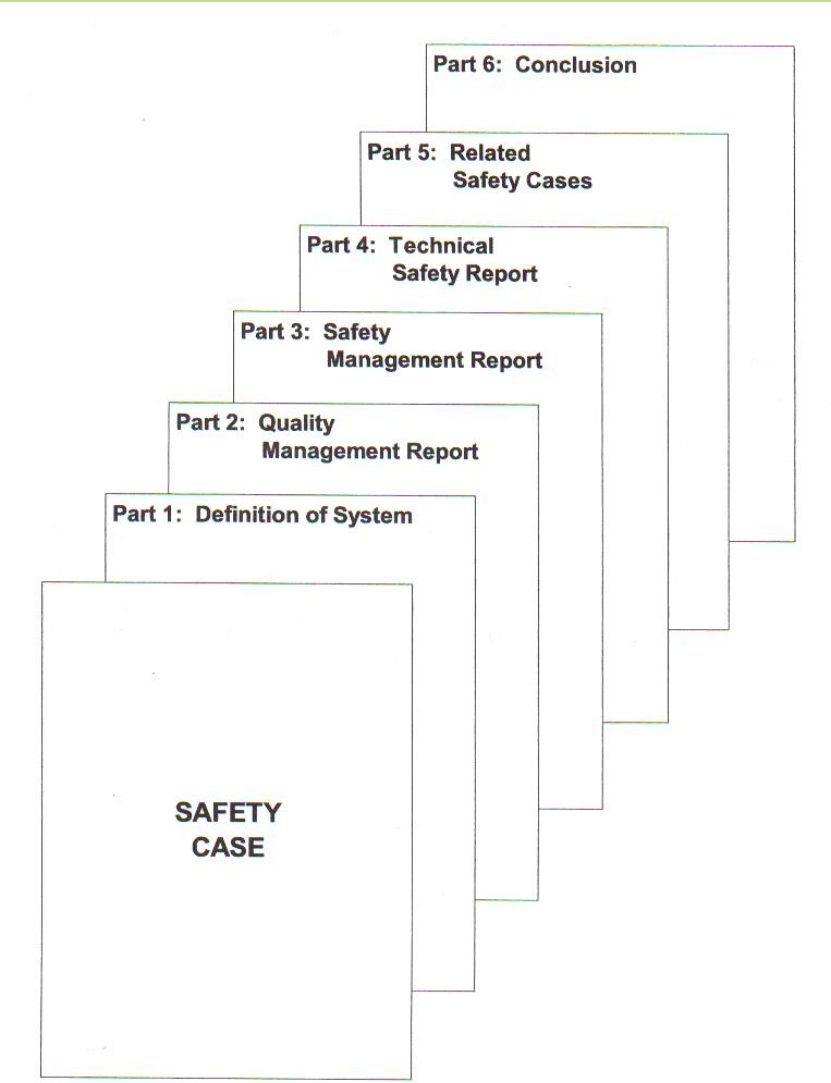
RAMS követelmények teljesülésének igazolása

- THR
  - Alapadatok adatbázisból
    - Saját adatok (azonos vagy hasonló alkalmazás)
    - Általános adatok, pl. MIL-HDBK 217F
    - A kettő kombinálása, súlyozása
  - Rendszerelemzések
    - FMEA
    - Hibafa
    - Megbízhatósági blokkdiagram
- SIL
  - Dokumentáció,
  - Biztonsági életciklus követelmények (felelősségek, kompetencia, függetlenségek),
  - Életciklus,
  - Módszerek és eljárások.
- Biztonságértékelés (assessor)

A rendszer életciklusa

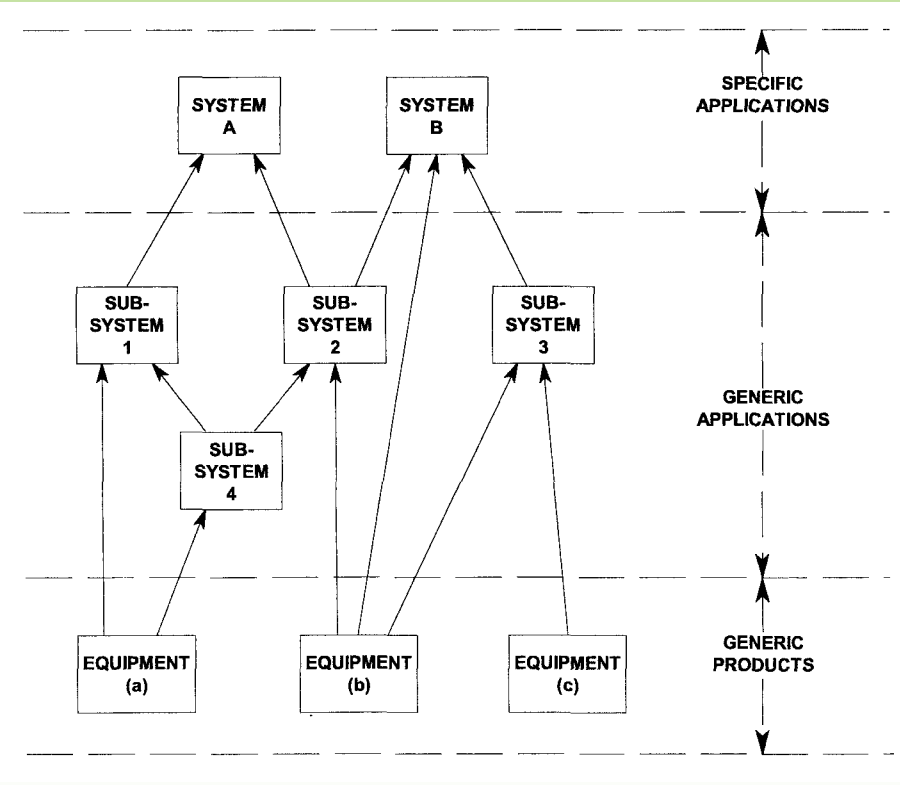


A biztonsági ügy (Safety Case)



- Olyan strukturált dokumentum, amely tartalmazza:
  - A minőségmenedzsment bizonyítékait,
  - A biztonságmenedzsment bizonyítékait,
  - A funkcionális és a technikai biztonság bizonyítékait.
- Biztonságmenedzsment
  - Biztonsági életciklus létrehozása,
  - Biztonsági szervezet (kompetencia, függetlenség),
  - Biztonsági terv,
  - Veszélynapló,
  - Biztonsági követelményspecifikáció,
  - Strukturált, ellenőrzött tervezés,
  - Ellenőrzések,
  - Verifikáció és validáció,
  - Döntés a megfelelőségről,
  - Üzemeltetés, karbantartás, leszerelés kezelése.

A fejlesztés költségeinek csökkentése: Hierarchikus építkezés



Három szintre különválasztott (különválasztható) fejlesztés:

- **Általános termék**
(pl. elektronikus biztonsági számítógép) – azt igazoljuk, hogy teljesíti a biztonsági specifikációt.
- **Általános alkalmazás**
(pl. biztonsági számítógéppel megvalósított útátjáró-fedező)
- **Specifikus alkalmazás**
(pl. teljes biztosítóberendezés egy konkrét állomásra).

Biztonságorientált alkalmazási feltételek

- Életciklus végrehajtás közben bárhol keletkezhetnek;
- Tovább kell őket adni (a továbbadást ki kell kényszeríteni);
- Fel kell őket dolgozni, ha feladatot definiálnak, azt végre kell hajtani (interfészeket létrehozni...).

A BIZTONSÁGINTEGRITÁS ÉS A BIZTONSÁGORIENTÁLT ALKALMAZÁSI FELTÉTELEK TELJESÍTÉSE

A VASÚTI BIZTOSÍTÓBERENDEZÉSEK TERVEZÉSE ÉS LÉTREHOZÁSA SORÁN

Szabó Géza
e-mail:
szabo.geza@certuniv.hu

certuniv