Pannon Egyetem
University of Pannonia

Gyakorlati útmutató

Biztonságkritikus rendszerek

Interaktív alkalmazások, Colab-notebookok és mintapromptok a kézikönyvhöz

Abonyi János

Pannon Egyetem · Veszprém, 2026

Pannon Egyetem
University of Pannonia

Biztonságkritikus rendszerek – gyakorlati útmutató

Interaktív alkalmazások, Colab-notebookok és mintapromptok a kézikönyvhöz

Abonyi János

Pannon Egyetem
University of Pannonia

Veszprém, 2026



Abonyi János: Biztonságkritikus rendszerek – gyakorlati útmutató

Interaktív alkalmazások, Colab-notebookok és mintapromptok a kézikönyvhöz

© 2026 Abonyi János

Kiadó: Pannon Egyetem, Veszprém

Változat: 1.0.0, 2026. november 21.

A mű a Creative Commons Nevezd meg! – Ne add el! – Így add tovább! 4.0 Nemzetközi licenc (CC BY-NC-SA 4.0) feltételei szerint használható fel; a mellékelt programkód licence MIT.

Webes változat: https://complexsystemsintelligence.github.io/biztonsagkritikus-rendszerek/gyakorlat/

Forrás, hibajelzés és javaslat: https://github.com/ComplexSystemsIntelligence/biztonsagkritikus-rendszerek

DOI: 10.5281/zenodo.24413011 (a kiadások közös azonosítója a Zenodón)

Betűkészletek: IBM Plex Serif, IBM Plex Sans, Raleway (SIL Open Font License 1.1). Szedés: Quarto és XeLaTeX.

Tartalom

Bevezetés 1

Veszélyazonosítás és kockázat 5

1. Balesetelemzés három szemüvegen át 7
2. Kockázati mátrix, egyéni és társadalmi kockázat 9
3. HAZOP a ReaktorVéd adagolókörére 11
4. FMEA és FMEDA 13
5. STPA-munkalap 15

Kvantitatív módszerek 17

6. Élettartam-eloszlások és megbízhatósági becslés 19
7. Megbízhatósági blokkdiagramok 21
8. Hibafa-elemzés 23
9. LOPA és eseményfa 25
10. Markov-modellek és rendelkezésre állás 27
11. PFD és SIL-igazolás 29

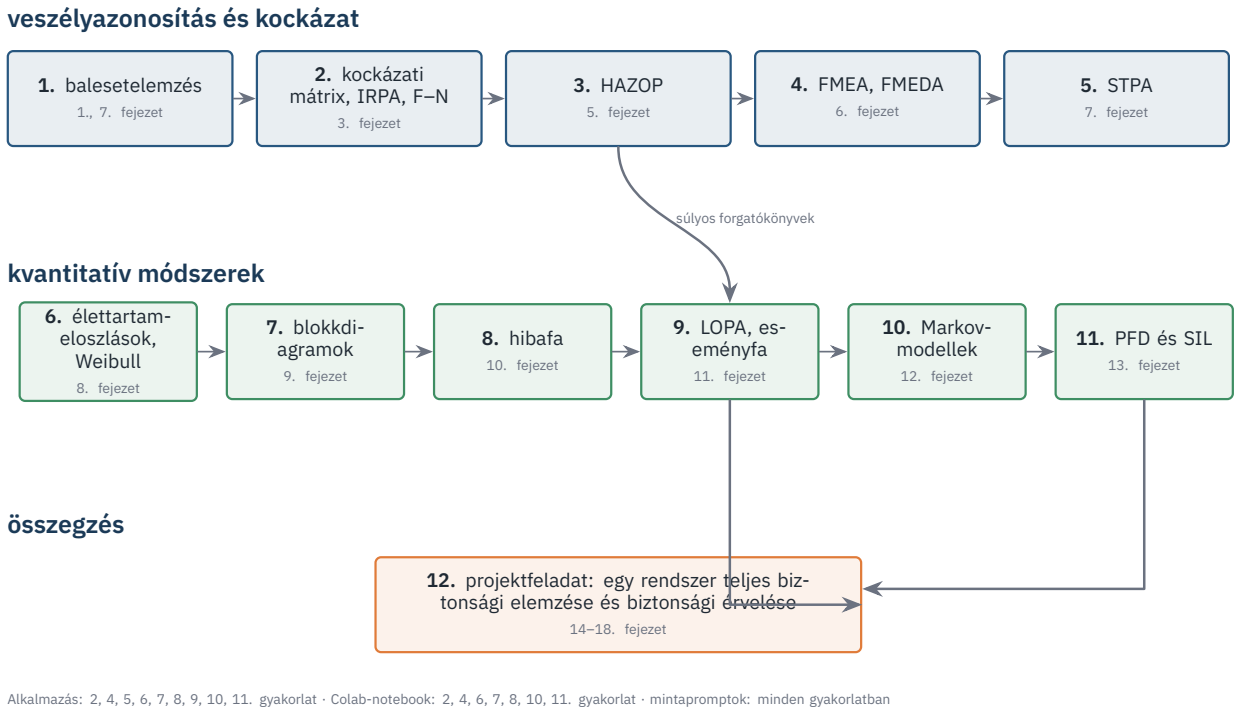
Összegzés 31

12. Projektfeladat: egy rendszer teljes biztonsági elemzése 33

Irodalom 37

Bevezetés

Ez a gyakorlati útmutató a *Biztonságkritikus rendszerek* kézikönyv párja. A kézikönyv a módszerek elméletét és indoklását adja, az útmutató pedig azt, hogy a módszereket a saját kezeddel, valós léptékű példákon alkalmazd. A tizenkét gyakorlat a kézikönyv fejezeteit követi, és ugyanazt a három futó esetet használja: a ReaktorVéd exoterm reaktor védelmi rendszerét, a VészFék vészfékező asszisztenst és a KoboCella kollaboratív robotcellát.



1. ábra. A gyakorlatok kapcsolata egymással és a kézikönyv fejezeteivel. A HAZOP súlyos forgatókönyvei a LOPA-gyakorlatba, a kvantitatív gyakorlatok eredményei a projektfeladatba kerülnek.

Mit kínál az útmutató?

Böngészős alkalmazások. Kilenc gyakorlathoz önálló, telepítés nélkül futó alkalmazás tartozik (kockázati mátrix, FMEA-munkalap, STPA-munkalap, élettartam-eloszlások, blokkdiagram, hibafa-elemző, LOPA és eseményfa, Markov-szerkesztő, PFD- és SIL-kalkulátor). Az alkalmazások az útmutató oldalaiba ágyazva és külön lapon is megnyithatók,

internetkapcsolat nélkül is működnek, és a munkádat a böngésző helyi tárolójában megőrzik (ha a böngésző ezt engedi). Az eredmények CSV- vagy Markdown-fájlként letölthetők.

Colab-notebookok. Hét gyakorlathoz Python-notebook tartozik, amely a Google Colab felületén egy kattintással megnyílik, és a kézikönyv számpéldáit reprodukálja: a megbízhatósági becslésektől a hibafa-elemzésen és a Markov-modelleken át a SIL-igazolás Monte Carlo-bizonytalanságáig. A notebookok kódja szabadon módosítható; a feladatcellák a továbbgondolást segítik.

Mintapromptok. Minden gyakorlat ad mintapromptokat a nagy nyelvi modellek felelős használatához: kritikus olvasótársként, ötletgyűjtő partnerként vagy a saját számításaid ellenőrzőjeként. A promptok mindig kérik, hogy a modell jelölje a bizonytalanságait, és ne találjon ki adatokat vagy hivatkozásokat.

Tanulási eredmények

Az útmutató teljes feldolgozása után képes leszel

- egy balesetvizsgálati jelentést a lineáris, a rétegmodell alapú és a rendszerelméleti balesetmodell szemléletével elemezni, és a tanulságokat tervezési követelményekké alakítani;
- veszélyazonosítást végezni HAZOP-, FMEA- és STPA-módszerrel, és a módszerek eredményeit összevetni;
- kalibrált kockázati mátrixot tervezni, felismerni a korlátait, és egyéni és társadalmi kockázatot számolni;
- élettartam-adatokból megbízhatósági jellemzőket becsülni, és a becslés bizonytalanságát számszerűsíteni;
- blokkdiagramot, hibafát, eseményfát és Markov-modellt felállítani és kiértékelni, és tudni, melyik kérdéshez melyik modell illik;
- LOPA-val meghatározni egy biztonsági funkció integritási követelményét, és a tervezett funkcióról PFD-számítással, architekturális korlátokkal és érzékenységvizsgálattal igazolni, hogy teljesíti;
- egy választott rendszer teljes biztonsági elemzését elkészíteni, és az eredményeket biztonsági érvelésbe rendezni;
- a nagy nyelvi modelleket a biztonsági elemzés támogatására felelősen, a kimenetek ellenőrzésével használni.

1. táblázat. A gyakorlatok áttekintése

Gyakorlat	Kézikönyv	Alkalmazás	Notebook	Fő kompetencia
1. balesetelemzés	1., 7. fejezet	–	–	baleseti okok rendszerszintű elemzése
2. kockázati mátrix, IRPA, F–N	3. fejezet	igen	igen	kockázatértékelés és -elfogadhatóság
3. HAZOP	5. fejezet	–	–	szisztematikus veszélyazonosítás
4. FMEA, FMEDA	6. fejezet	igen	igen	meghibásodási módok és diagnosztika

Gyakorlat	Kézikönyv	Alkalmazás	Notebook	Fő kompetencia
5. STPA	7. fejezet	igen	–	irányítási hibák feltárása
6. élettartam-eloszlások	8. fejezet	igen	igen	megbízhatósági becslés adatokból
7. blokkdiagramok	9. fejezet	igen	igen	rendszermegbízhatóság
8. hibafa	10. fejezet	igen	igen	deduktív elemzés, fontosság
9. LOPA, eseményfa	11. fejezet	igen	–	integritási követelmény meghatározása
10. Markov-modellek	12. fejezet	igen	igen	javítható és tesztelt rendszerek
11. PFD és SIL	13. fejezet	igen	igen	a biztonsági integritás igazolása
12. projektfeladat	14–18. fejezet	–	–	teljes elemzés és biztonsági érvelés

Hogyan dolgozz a nagy nyelvi modellekkel?

A nagy nyelvi modellek hasznos segítők lehetnek a biztonsági elemzésben: ötleteket adnak a veszélyazonosításhoz, összefoglalnak hosszú jelentéseket, magyaráznak, kódot írnak és ellenőriznek. A kézikönyv 18. fejezete azonban arra is figyelmeztet, hogy a javaslataik egy része téves vagy irreleváns, és a magabiztos megfogalmazás könnyen automatizálási torzításhoz vezet. Néhány elv, amelyet minden gyakorlatban érdemes követni:

1. **Előbb te gondolkodj.** Készítsd el a saját elemzésed első változatát, és csak utána kérd a modell véleményét. Így a modell kiegészít, nem helyettesít.
2. **Adj kontextust, és kérj bizonytalanságjelölést.** Írd le a rendszert, a feltevéseket és a célt; kérd, hogy a modell jelölje a bizonytalan állításait, és ne találjon ki számokat vagy hivatkozásokat.
3. **Ellenőrizz mindent.** Különösen a számokat, a szabványpontokat, a jogi állításokat és a hivatkozásokat. A modell kimenete csak akkor kerülhet az elemzésbe, ha egy szakértő ellenőrizte.
4. **Dokumentáld a modell szerepét.** A jegyzőkönyvben vagy a biztonsági érvelésben rögzítsd, mire használtad a modellt, és ki ellenőrizte a kimenetét.
5. **Vigyázz a bizalmas adatokkal.** Valós tervadatokat csak a munkahelyed adatvédelmi szabályainak megfelelő eszközzel ossz meg.

> **Általános keretprompt**
>
> *„Biztonságkritikus rendszerek elemzésében segítesz. A feladat: [a feladat rövid leírása]. A rendszer: [a rendszer leírása, határai, üzemállapotai]. Az eddigi elemzésem: [saját eredmény]. Kérlek, (1) mutass rá a hiányosságokra és a téves feltevésekre, (2) javasolj kiegészítéseket, (3) minden állításodnál jelöld, mennyire vagy biztos benne, (4) ne találj ki számadatot, szabványpontot vagy hivatkozást; ha valamit nem tudsz, mondd meg.”*

Technikai tudnivalók

Az alkalmazások modern böngészőben (Chrome, Firefox, Edge, Safari) futnak. A notebookok megnyitásához Google-fiók kell; a Colab ingyenes változata minden számításhoz elegendő. A notebookok helyi Jupyter-környezetben is futtathatók (NumPy, SciPy, Matplotlib és pandas szükséges). Az útmutató, az alkalmazások és a notebookok forrása a könyv GitHub-tárolójában található. A szöveg CC BY-NC-SA 4.0, a kód MIT licenc alatt használható.

Veszélyazonosítás és kockázat



Pannon Egyetem
University of Pannonia

1.

Balesetelemzés három szemüvegen át

Tanulási eredmények

A gyakorlat végére képes leszel

- egy nyilvános balesetvizsgálati jelentésből az eseménysort, az aktív hibákat és a látens feltételeket kiemelni;
- ugyanazt a balesetet a sajtszelet-modell és a STAMP szemléletével is értelmezni, és megmagyarázni a két magyarázat különbségét;
- a tanulságokat ellenőrizhető tervezési és szervezeti követelményekké alakítani;
- egy nagy nyelvi modellt kritikus olvasótársként használni, a forrásra visszakereshető állításokkal.

Háttér: a kézikönyv 1. fejezete (balesetmodellek) és 7. fejezete (STAMP és STPA).

1.1. Választható jelentések

Válassz egyet az alábbi, nyilvánosan elérhető vizsgálati jelentések közül (vagy egy hasonló terjedelmű másikat, a gyakorlatvezetővel egyeztetve):

- a texasi finomító 2005-ös robbanásáról szóló CSB-jelentés (U.S. Chemical Safety and Hazard Investigation Board 2007);
- a Buncefield-olajtároló 2005-ös robbanásáról szóló vizsgálóbizottsági zárójelentés (Buncefield Major Incident Investigation Board 2008);
- az Air France 447 2009-es katasztrófájáról szóló BEA-zárójelentés (Bureau d'Enquêtes et d'Analyses 2012);
- az Uber automatizált tesztjárművének 2018-as tempei balesetéről szóló NTSB-jelentés (National Transportation Safety Board 2019);
- az Ariane 5 501-es repüléséről szóló vizsgálóbizottsági jelentés (Lions 1996).

1.2. Feladatok

1. **Eseménysor.** Készíts időrendi táblázatot a baleset közvetlen előzményeiről (legalább tíz esemény): időpont, esemény, szereplő, forrás (a jelentés oldalszáma).

2. **Sajtszelet-modell.** Gyűjtsd össze a frontvonalbeli aktív hibákat és a látens feltételeket (tervezési, karbantartási, szervezeti, szabályozói). Rendezd őket rétegekbe, és jelöld, melyik „lyuk” mióta állt fenn.
3. **Irányítási struktúra.** Rajzold fel a releváns irányítási struktúrát legalább négy szinten (például üzemeltetői kezelő, műszakvezető, üzemvezetés, vállalati vezetés, hatóság). Minden szinten add meg az irányítási műveleteket és a visszacsatolásokat.
4. **Nem biztonságos irányítás.** Legalább három szinten azonosíts egy-egy nem biztonságos irányítási műveletet, és magyarázd meg, miért volt a döntéshozó folyamatmodellje hibás (milyen információ hiányzott, torzult vagy késett).
5. **Összevetés.** Egy rövid bekezdésben hasonlítsd össze a két magyarázatot: mit tesz láthatóvá a STAMP, amit a sajtszelet-modell nem, és fordítva?
6. **Követelmények.** Fogalmazz meg legalább öt tanulságot ellenőrizhető követelményként („A …-nak … kell …, amit … igazol”). Legalább egy szervezeti, egy emberi tényezői és egy műszaki követelmény legyen köztük.

> **A modell mint kritikus olvasótárs**
>
> *„Egy balesetvizsgálati jelentést elemzek: [a jelentés címe]. Az eseménysor általam készített összefoglalóját alább másolom. Kérlek, (1) jelöld, mely állításaim nem következnek egyértelműen a jelentésből, (2) kérdezz rá, hol hiányzik forrás, (3) javasolj további látens feltételeket, de mindegyiknél add meg, a jelentés melyik részéből következtetsz rá; ha nem tudod, írd, hogy ez feltételezés. Ne találj ki idézetet vagy oldalszámot.”*
> *„Az alábbi irányítási struktúrát rajzoltam fel a balesethez: […]. Milyen visszacsatolások hiányoznak belőle? Melyik szinten látsz olyan irányítási műveletet, amelynek nincs megfelelő visszacsatolása?”*

1.3. Ellenőrző szempontok

Egy jó megoldásban az eseménysor minden eleme forrásra visszakereshető; a látens feltételek nem csak a frontvonalat érintik; az irányítási struktúra visszacsatolásokat is tartalmaz; a nem biztonságos irányítási műveletek kontextussal együtt vannak megfogalmazva; és a követelmények ellenőrizhetők, nem általános jókívánságok („legyen jobb a biztonsági kultúra”).

2.

Kockázati mátrix, egyéni és társadalmi kockázat

Tanulási eredmények

A gyakorlat végére képes leszel

- kalibrált kockázati mátrixot tervezni számszerű gyakorisági és súlyossági kategóriákkal;
- kimutatni a mátrix rangsorhibáit és a tartományösszevonás hatását;
- egyéni kockázatot (IRPA) és F–N görbét számolni, és kritériumokkal összevetni.

Háttér: a kézikönyv 3. fejezete.

2.1. Alkalmazás: kockázati mátrix tervező

Az alkalmazás megnyitása külön lapon

2.2. Feladatok az alkalmazással

1. **Kalibrálás.** Töltsd be a ReaktorVéd példát. Nézd meg, melyik cellába kerül a reaktorfelhasadás a biztonsági funkcióval és anélkül. Mennyit változik a kvantitatív kockázat, és mennyit a mátrix színe?
2. **Rangsorhiba.** Töltsd be a „Cox rangsorhibája” példát. Magyarázd meg, miért kap az A forgatókönyv magasabb szint, mint a nyolcszor nagyobb kockázatú B. Keress egy olyan színezési szabályt, amely ezt megszünteti; okoz-e ez máshol új ellentmondást?
3. **Tartományösszevonás.** Keress két saját forgatókönyvet, amelyek ugyanabba a cellába esnek, de kockázatuk legalább százszorosan eltér. Mi a következménye ennek a döntéshozatalban?
4. **Tervezés.** Javasolj a ReaktorVéd üzemre egy 5×5-ös mátrixot a vállalati kritériumokkal összhangban (a halálos kimenetelű forgatókönyv tolerálható gyakorisága 10^{-5}/év). Indokold a kategóriahatárokat.

2.3. Notebook: egyéni kockázat és F–N görbe

Megnyitás a Google Colabban · a notebook letöltése

A notebook a kézikönyv IRPA-példáját reprodukálja (egy kezelő egyéni kockázata $4{,}3 \cdot 10^{-6}$/év), és egy kis létesítmény F–N görbéjét veti össze kockázatkerülő kritériumvonallal. Oldd meg a notebook három feladatát.

> **Mintapromptok**
>
> *„Egy 5×5-ös kockázati mátrixot terveztem az alábbi kategóriahatárokkal: […]. Mutass rá, hol okozhat a mátrix rangsorhibát, és javasolj olyan forgatókönyvpárt, amely ezt szemlélteti! Számolj a gyakoriság és a következmény szorzatával, és ellenőrizd a számaidat.”*
> *„Magyarázd el egy vezetőnek közérthetően, miért nem szabad a kockázati mátrix színeit összeadni vagy átlagolni több forgatókönyvre! Maximum öt mondatban.”*

2.4. Ellenőrző szempontok

A jó megoldás számszerű kategóriahatárokat használ, a rangsorhibákat konkrét számokkal mutatja ki, és megkülönbözteti a mátrix szerepét (gyors szűrés, kommunikáció) a kvantitatív döntéstámogatástól.

3.

HAZOP a ReaktorVéd adagolókörére

Tanulási eredmények

A gyakorlat végére képes leszel

- egy csomópont tervezési szándékát pontosan megfogalmazni;
- a vezérszavak és a paraméterek szisztematikus kombinálásával eltéréseket, okokat és következményeket azonosítani;
- a meglévő védelmeket és a szükséges javaslatokat rögzíteni, és a súlyos forgatókönyveket a LOPA-ba továbbadni.

Háttér: a kézikönyv 5. fejezete (a ReaktorVéd folyamatábrája és a hűtőkör HAZOP-részlete).

3.1. A csomópont

2. csomópont: a B reaktáns adagolása a tárolótartálytól a P-101 szivattyún és a két sorba kötött gyorszáró szelepen (XV-101, XV-102) át a reaktorig, a FIC-102 áramlásszabályozóval. **Tervezési szándék:** a B reaktáns 0,8–1,0 m³/h áramlással, 20–30 °C-on, a reakcióhőmérséklet (70 ± 3 °C) elérése után, legfeljebb a recept szerinti összmennyiségig kerüljön a reaktorba.

A kézikönyv egyszerűsített folyamatábrájához képest a gyakorlathoz két elemet feltételezünk: az adagolást a FIC-102 áramlásszabályozó (FT-102 áramlásmérő, FV-102 szabályozószelep) tartja az alapjelen, és az FAH-102 nagyáramlás-riasztás a kezelőt figyelmezteti. A vezeték visszacsapó szelepet nem tartalmaz.

3.2. Feladatok

1. Készíts HAZOP-jegyzőkönyvet a csomópontra az alábbi oszlopokkal: vezérszó és paraméter, eltérés, okok, következmények (a védelmek figyelmen kívül hagyásával), meglévő védelmek, javaslat, felelős. Legalább a következő kombinációkat vizsgáld: NINCS / TÖBB / KEVESEBB / FORDÍTOTT áramlás; TÖBB / KEVESEBB hőmérséklet; MÁS MINT összetétel; KORÁN / KÉSŐN (az adagolás időzítése); TÖBB mennyiség.
2. Jelöld meg azokat a forgatókönyveket, amelyek súlyos következményhez (megfutó reakció, mérgező kibocsátás) vezethetnek. Ezek kerülnek a 9. gyakorlat LOPA-elemzésébe.

3. Vizsgáld meg, hogy a meglévő védelmek közül melyik független a kezdő eseménytől. Például: véd-e a FIC-102 szabályozó a saját meghibásodása ellen?
4. Fogalmazz meg legalább három javaslatot, amelyek közül legalább egy inherens megoldás legyen (a kézikönyv 14. fejezete).

3.1. táblázat. Minta a jegyzőkönyv egy sorára

Vezérszó + paraméter	Eltérés	Okok	Következmények	Védelmek	Javaslat
TÖBB áramlás	a B adagolása a tervezettnél gyorsabb	FIC-102 hibája; a szabályozószelep nyitva ragad; kezelői beállítási hiba	a B felhalmozódik, a hőfejlődés meghaladja a hűtés kapacitását, megfutó reakció	FAH-102 riasztás; SIF (TT-101/102 → XV-101/102)	az adagolás fizikai korlátozása szűkítőperemmel; LOPA

Mintaprompt a vezérszavas ötletgyűjtéshez

„Egy félszakaszos reaktor B reaktáns adagolókörének HAZOP-vizsgálatát végezzük. A tervezési szándék: [lásd fent]. Az elemek: tárolótartály, P-101 szivattyú, FIC-102 áramlásszabályozó (FT-102, FV-102), FAH-102 riasztás, XV-101 és XV-102 gyorszáró szelep, visszacsapó szelep nincs. Vedd sorra a KORÁN, KÉSŐN és FORDÍTOTT vezérszót az adagolásra! Minden eltérésnél sorolj fel okokat (berendezés, ember, közmű, külső hatás) és következményeket a védelmek figyelmen kívül hagyásával. Jelöld, ha egy állításod bizonytalan, és ne adj meg konkrét számértéket.”

Önellenőrzés

Ellenőrizd a jegyzőkönyvedet: szerepel-e benne a következő négy, gyakran kimaradó forgatókönyv?

Megoldás.

(1) **KORÁN:** az adagolás a reakcióhőmérséklet elérése előtt indul, a B nem reagál, felhalmozódik, majd egyszerre reagál el (a kézikönyv hűtőkörös HAZOP-jának harmadik sorához hasonló „rejtett” veszély). (2) **FORDÍTOTT áramlás:** a szivattyú leállásakor a reaktor tartalma visszaáramolhat a B tárolótartályba, ahol nem kívánt reakció indulhat; visszacsapó szelep vagy reteszelés kell. (3) **MÁS MINT összetétel:** rossz anyag vagy szennyezett B kerül a reaktorba (címkézés, mintavétel, betöltési eljárás). (4) **TÖBB mennyiség:** a teljes adagolt mennyiség meghaladja a receptet, mert a mennyiségmérés hibás vagy a szakaszt kétszer indítják; adagoltmennyiség-felügyelet és szakaszos reteszelés kell.

3.3. Ellenőrző szempontok

A jó jegyzőkönyvben a tervezési szándék számszerű, az okok konkrét eszközökhöz vagy tevékenységekhez kötődnek, a következmények a védelmek nélkül értendők, a védelmeknél a függetlenség is szerepel, és a javaslatok között az inherens megoldások is megjelennek.

4.

FMEA és FMEDA

Tanulási eredmények

A gyakorlat végére képes leszel

- tervezési FMEA-t készíteni egy érzékelőre a harmonizált (AIAG–VDA) lépések szerint;
- összevetni a kockázat-prioritási számot és a cselekvési prioritás logikáját, és megindokolni az eltéréseket;
- FMEDA-táblázatból kiszámolni a λ_S, λ_{DD}, λ_{DU}, DC és SFF értékét, és értékelni a diagnosztikai fejlesztéseket.

Háttér: a kézikönyv 6. fejezete.

4.1. Alkalmazás: FMEA-munkalap

Az alkalmazás megnyitása külön lapon

4.2. Feladatok az alkalmazással

1. Töltsd be a VészFék radarérzékelő példáját. Keresd meg azokat a sorpárokat, ahol az RPN és a cselekvési prioritás sorrendje ellentmond egymásnak, és magyarázd meg az okát.
2. Készíts saját FMEA-t a VészFék **kamerájára** vagy a KoboCella **lézerszkennerére** legalább nyolc meghibásodási móddal. Minden módnál add meg a megelőző és az észlelő intézkedést.
3. Válassz ki két magas prioritású sort, és javasolj intézkedéseket először a súlyosság, majd az előfordulás, végül az észlelés csökkentésére. Hogyan változik az RPN és a prioritás?
4. Figyeld meg az RPN-értékek eloszlását az alkalmazás alján: miért félrevezető az „RPN > 100” típusú küszöb?

4.3. Notebook: FMEDA

Megnyitás a Google Colabban · a notebook letöltése

A notebook a TT-101 távadó FMEDA-ját számolja végig (DC = 60%, SFF = 73,3%), majd megmutatja a két távadó eltérésfigyelésének és egy jobb A/D-ellenőrzésnek a hatását.

> **Mintapromptok**
>
> *„Egy autóipari radarérzékelő tervezési FMEA-ját készítem. Az alábbi meghibásodási módokat azonosítottam: [...]. Milyen fontos meghibásodási módok hiányozhatnak a listámból (környezeti hatások, öregedés, szoftver, interfészek)? Mindegyiknél add meg, mi alapján gondolod, és jelöld, ha bizonytalan vagy."*
> *„Magyarázd el, miért lehet egy alacsony RPN-ű, de 10-es súlyosságú meghibásodási mód fontosabb, mint egy 300-as RPN-ű, 4-es súlyosságú! Hivatkozz az AIAG–VDA módszertan elveire, de konkrét táblázatértéket ne idézz fejből."*

4.4. Ellenőrző szempontok

A jó FMEA-ban a hatás és az ok egyértelműen elkülönül, a súlyosság a hatáshoz, az előfordulás az okhoz, az észlelés az intézkedéshez kötődik; a prioritásoknál a súlyosság az elsődleges; az FMEDA-nál pedig minden veszélyes módhoz konkrét diagnosztika és lefedettség tartozik.

5.

STPA-munkalap

> **Tanulási eredmények**
>
> A gyakorlat végére képes leszel
>
> - veszteségeket, rendszerszintű veszélyeket és biztonsági korlátokat megfogalmazni;
> - irányítási struktúrát felrajzolni irányítási műveletekkel és visszacsatolásokkal;
> - a négy típus szerint nem biztonságos irányítási műveleteket azonosítani, és mindegyikhez okozati forgatókönyveket és követelményeket rendelni.

Háttér: a kézikönyv 7. fejezete.

5.1. Alkalmazás: STPA-munkalap

Az alkalmazás megnyitása külön lapon

5.2. Feladatok

Válaszd a VészFék vagy a KoboCella esetet (a példák betölthetők), és egészítsd ki az elemzést:

1. Legalább két veszteség és három rendszerszintű veszély, mindegyik veszélynél a kapcsolódó veszteségekkel.
2. Az irányítási struktúra legalább két szinten (például a vezető vagy a szerelő mint irányító is szerepeljen).
3. Minden irányítási műveletre mind a négy UCA-típus vizsgálata; ahol egy típus nem értelmezhető, indokold.
4. Minden UCA-hoz legalább két okozati forgatókönyv (F1, F2…) a négy jellegzetes csoportból (hibás folyamatmodell, hiányos vagy késő visszacsatolás, a művelet nem hajtódik végre, külső zavar), és legalább egy követelmény (K1…).
5. Az alkalmazás „Ellenőrzés” része jelzi a hiányosságokat; a végén töltsd le a munkalapot Markdown-fájlként.

> **Mintapromptok**
>
> *„STPA-elemzést végzek egy kollaboratív robotcellára. Az irányítási struktúra: [...]. Az irányítási műveletek: sebességcsökkentés, biztonságos megállás, újraindítás. Mind a négy UCA-típusra javasolj eseteket kontextussal! Utána kérdezz rá azokra a visszacsatolásokra, amelyek a javasolt UCA-k megelőzéséhez hiányoznak a struktúrámból.”*
> *„Az alábbi UCA-hoz írtam két okozati forgatókönyvet: [...]. A négy jellegzetes forgatókönyvcsoport közül melyik hiányzik? Javasolj egyet abból a csoportból, és fogalmazz meg hozzá egy ellenőrizhető követelményt!”*

5.3. Ellenőrző szempontok

A jó elemzésben a veszélyek rendszerállapotok (nem meghibásodások), az UCA-k kontextussal együtt szerepelnek, a forgatókönyvek az irányító folyamatmodelljének hibáit is vizsgálják, és a követelmények a forgatókönyvekből vezethetők le, nem általánosak.

Kvantitatív módszerek



Pannon Egyetem
University of Pannonia

6.

Élettartam-eloszlások és megbízhatósági becslés

> **Tanulási eredmények**
>
> A gyakorlat végére képes leszel
>
> - értelmezni az exponenciális, a Weibull- és a lognormális eloszlás függvényeit és a kádgörbét;
> - terepi adatokból állandó meghibásodási rátát becsülni konfidenciakorlátokkal;
> - Weibull-eloszlást illeszteni cenzúrázott adatokra, és a becslés bizonytalanságát bootstrap-módszerrel számszerűsíteni.

Háttér: a kézikönyv 8. fejezete és az A függelék.

6.1. Alkalmazás: élettartam-eloszlások

Az alkalmazás megnyitása külön lapon

6.2. Feladatok az alkalmazással

1. Állítsd a Weibull-eloszlás alakparaméterét 0,5-re, 1-re és 3,5-re. Hogyan változik a meghibásodási ráta és a B10-élettartam? Melyik esetben értelmes a megelőző csere?
2. Exponenciális eloszlásnál ellenőrizd, hogy $R(\mathrm{MTTF}) = e^{-1} \approx 0{,}368$ bármely λ-ra. Mi ennek a gyakorlati jelentése?
3. A kádgörbe nézetben változtasd a korai szakasz paramétereit (β_1, η_1). Mennyi idő után csökken az összesített ráta a hasznos élettartam szintjére? Ebből becsüld meg, mennyi ideig érdemes beégetni (*burn-in*) az eszközöket, és mi szól a beégetés ellen (költség, élettartam-fogyasztás).

6.3. Notebook: terepi becslés és Weibull-elemzés

Megnyitás a Google Colabban · a notebook letöltése

A notebook a kézikönyv két esetét számolja végig: a távadók terepi adataiból $\hat{\lambda} = 3{,}42 \cdot 10^{-7}$/h és a 70%-os felső korlát $5{,}44 \cdot 10^{-7}$/h; a KoboCella csapágyaira $\hat{\beta} = 2{,}73$, $\hat{\eta} = 10\,170$ h (rangregresszióval $3{,}19$ és 9460 h), majd bootstrap-intervallumot ad: β 90%-os intervalluma 1,83–4,87.

> **Mintaprompt**
>
> *„Weibull-elemzést végeztem 12 csapágy adatán, amelyek közül három cenzúrázott. A ML-becslés β = 2,73, η = 10 170 h, a rangregresszió β = 3,19, η = 9460 h. Magyarázd el, miért térhet el a két módszer eredménye, és melyiket mikor érdemes előnyben részesíteni! Hivatkozz megbízható forrásra, ha tudsz, és jelöld, ha bizonytalan vagy.”*

6.4. Ellenőrző szempontok

A jó megoldás megkülönbözteti a pontbecslést és a konfidenciakorlátot, helyesen kezeli a cenzúrázott adatokat, és a karbantartási következtetést (csere vagy nem) az alakparaméterre és a bizonytalanságra alapozza.

7.

Megbízhatósági blokkdiagramok

> **Tanulási eredmények**
>
> A gyakorlat végére képes leszel
>
> - soros, párhuzamos és k-ból-n struktúrák megbízhatóságát és MTTF-jét kiszámolni;
> - nem soros-párhuzamos rendszereket minimális utakkal kezelni;
> - értékelni a komponensadatok bizonytalanságát és a közös okú meghibásodás hatását.

Háttér: a kézikönyv 9. fejezete.

7.1. Alkalmazás: blokkdiagram

Az alkalmazás megnyitása külön lapon

7.2. Feladatok az alkalmazással

1. Hasonlítsd össze az 1oo2, a 2oo3 és az 1oo1 struktúra megbízhatóságát az idő függvényében azonos elemekkel. Ellenőrizd, hogy a 2oo3 MTTF-je $5/(6\lambda)$, azaz kisebb, mint egyetlen elemé!
2. Töltsd be a hídkapcsolást, és ellenőrizd, hogy $t_0 = 1053{,}6$ óránál (ahol egy elem megbízhatósága 0,9) a rendszeré 0,97848. Melyik elem Birnbaum-fontossága a legnagyobb, és miért?
3. Próbáld meg a hídkapcsolást kifejezéssel leírni úgy, hogy az E elem kétszer szerepel. Miért ad hibás eredményt? (Az alkalmazás figyelmeztet.)
4. A ReaktorVéd példában melyik alrendszer javítása növeli leginkább a rendszer megbízhatóságát?

7.3. Notebook: hídkapcsolás, Monte Carlo, közös ok

Megnyitás a Google Colabban · a notebook letöltése

> **Mintaprompt**
>
> *„Egy 2oo3 szavazású érzékelőrendszer megbízhatóságát számoltam binomiális képlettel: […]. Ellenőrizd a levezetést, és magyarázd el, miért lehet a 2oo3 hosszú távon rosszabb, mint egyetlen érzékelő! Ne a végeredményt add meg, hanem a gondolatmenet hibáit jelöld.”*

7.4. Ellenőrző szempontok

A jó megoldás tudatosan kezeli a függetlenségi feltevést, a többször előforduló elemeket minimális utakkal vagy dekompozícióval számolja, és a redundancia értékét a közös okú meghibásodás figyelembevételével ítéli meg.

8.

Hibafa-elemzés

Tanulási eredmények

A gyakorlat végére képes leszel

- hibafát szöveges leírásból felépíteni és ellenőrizni;
- minimális vágatokat meghatározni, és felismerni az egypontos hibákat és az ismétlődő eseményeket;
- a csúcsesemény valószínűségét többféle módszerrel számolni, és a fontossági mértékekből tervezési javaslatot levezetni;
- házeseményekkel tervváltozatokat összevetni, és a közös okú meghibásodást beépíteni.

Háttér: a kézikönyv 10. fejezete.

8.1. Alkalmazás: hibafa-elemző

Az alkalmazás megnyitása külön lapon

8.2. Feladatok az alkalmazással

1. Töltsd be a ReaktorVéd energiával működtetett változatát. Ellenőrizd a minimális vágatokat és a csúcsesemény valószínűségét ($2{,}17 \cdot 10^{-3}$). Melyek az egypontos hibák?
2. Kapcsold ki a HEN házeseményt (energiamentesítéssel működtetett, hibabiztos kialakítás). Hogyan változnak a vágatok és a valószínűség ($1{,}73 \cdot 10^{-4}$)?
3. Töltsd be a közös okú meghibásodást is tartalmazó változatot. Ellenőrizd az $1{,}335 \cdot 10^{-3}$ értéket, és értelmezd a Fussell–Vesely-fontosságokat. Mi a következő legfontosabb tervezési lépés?
4. Írd be a kézikönyv MOCUS-példáját, és ellenőrizd kézzel a vágatokat és a pontos értéket (0,00217).
5. Építs saját hibafát a VészFék „indokolatlan erős fékezés” csúcseseményére legalább hat alapeseménnyel!

8.3. Notebook: MOCUS, BDD, fontosság, Monte Carlo

Megnyitás a Google Colabban · a notebook letöltése

> **Mintapromptok**
>
> *„Az alábbi hibafát írtam fel a »[csúcsesemény]« eseményre: [...]. Ellenőrizd a NUREG-0492 szerkesztési szabályai alapján (hibaként megfogalmazott események, teljes kapuk, nincs kapu–kapu kapcsolat)! Sorold fel a szabálysértéseket, de ne írd át helyettem a fát.”*
> *„Az energiával működtetett változat fontossági mértékei: [...]. Magyarázd el közérthetően egy üzemvezetőnek, mit jelent a 460-as kockázatnövelési érték a tápegységekre, és milyen üzemeltetési szabály következik belőle!”*

8.4. Ellenőrző szempontok

A jó megoldásban a csúcsesemény pontosan megfogalmazott, az ismétlődő események következetesen azonos névvel szerepelnek, a vágatok minimálisak, a valószínűség mellett a fontossági mértékek értelmezése is megjelenik, és a tervezési javaslat a domináns vágatokra irányul.

9.

LOPA és eseményfa

Tanulási eredmények

A gyakorlat végére képes leszel

- egy forgatókönyvre LOPA-táblázatot készíteni, és meghatározni a biztonsági funkció szükséges PFD-jét és SIL-jét;
- a független védelmi rétegek négy kritériumát alkalmazni, és indokolni, ha egy védelem nem számítható be;
- értékelni a feltételes módosítók hatását, és a forgatókönyvet eseményfaként is értelmezni.

Háttér: a kézikönyv 11. fejezete; a forgatókönyvek a 3. gyakorlat HAZOP-jegyzőkönyvéből származnak.

9.1. Alkalmazás: LOPA és eseményfa

Az alkalmazás megnyitása külön lapon

9.2. Feladatok az alkalmazással

1. Töltsd be a ReaktorVéd példát, és ellenőrizd az eredményt (RRF ≥ 500, SIL 2). Miért nem számítható be a TIC-103 és az RD-101?
2. Tegyük fel, hogy a hasadótárcsa kétfázisú méretezését igazolták. Jelöld be mind a négy kritériumot: hogyan változik a SIL-követelmény? Milyen új kérdéseket vet fel ez a döntés?
3. Kapcsold be a feltételes módosítókat. Mennyivel enyhül a követelmény? Miért tiltja ezt sok vállalat?
4. Töltsd be a benzintartály-példát. Melyik réteg sérti a függetlenség, melyik az auditálhatóság és melyik a hatásosság követelményét? Kapcsold össze a kézikönyv Buncefield-elemzésével: melyik réteg hibája játszott ott szerepet?
5. Végezd el a LOPA-t a saját HAZOP-jegyzőkönyved két súlyos forgatókönyvére.

Mintapromptok

„LOPA-t végzek az alábbi forgatókönyvre: [...]. A független védelmi rétegként beszámított védelmek: [...]. Vizsgáld meg mindegyiket a négy IPL-kritérium (hatásos, független, megbízható, auditálható) szerint, és

> *kérdezz rá azokra az információkra, amelyek a döntéshez hiányoznak! A CCPS-irodalom tipikus értékeit csak tájékoztatásul említsd, és jelöld, ha bizonytalan vagy.”*

9.3. Ellenőrző szempontok

A jó LOPA-ban a kezdő esemény gyakorisága és a rétegek PFD-je forráshoz kötött, minden beszámított réteg függetlensége indokolt, a feltételes módosítók használata a vállalati szabállyal összhangban van, és a szükséges SIL mellett a nem beszámított védelmek sorsáról is döntés születik.

10.

Markov-modellek és rendelkezésre állás

Tanulási eredmények

A gyakorlat végére képes leszel

- egy rendszer viselkedését állapotokkal és átmeneti rátákkal leírni;
- pillanatnyi és tartós rendelkezésre állást, valamint MTTF-et számolni;
- értékelni a javítás, a közös okú meghibásodás, az indulási hiba és a periodikus tesztelés hatását.

Háttér: a kézikönyv 12. fejezete.

10.1. Alkalmazás: Markov-szerkesztő

Az alkalmazás megnyitása külön lapon

10.2. Feladatok az alkalmazással

1. Töltsd be a javítható elem szemléltető változatát, és figyeld meg, hogyan közelít a rendelkezésre állás a tartós értékhez. Mitől függ az időállandó?
2. Az 1oo2 példában ellenőrizd a kézikönyv értékeit ($U = 4{,}1 \cdot 10^{-5}$, MTTF $= 1{,}94 \cdot 10^{5}$ h). Állítsd a közös okú átmenetet nullára: mennyivel nő az MTTF?
3. Modellezz két javítócsapatot: a „rendszerhiba → egy jó” átmenet rátáját állítsd $2\mu = 0{,}25$/h-ra. Mi változik és mi nem? Miért hat ez a módosítás jóval kevésbé, mint a közös okú átmenet csökkentése?
4. A hideg tartalék példájában az A elem $\lambda = 10^{-4}$/h rátája két átmenetre oszlik: sikeres átkapcsolás $(1-p)\lambda$ és sikertelen indulás $p\lambda$ (a példában $p = 0{,}02$). Változtasd p-t, és keresd meg, mekkora indulási hiba mellett lesz a hideg tartalék MTTF-je kisebb, mint a meleg tartaléké ($1{,}5/\lambda$)! Hogyan módosítja az eredményt a tartalék rejtett meghibásodása (a „B rejtett hiba” állapot)?

10.3. Notebook: Markov-modellek és többfázisú PFD

Megnyitás a Google Colabban · a notebook letöltése

> **Mintaprompt**
>
> *„Egy 2oo3 szavazású, javítható rendszer Markov-modelljét írtam fel: [állapotok és átmenetek]. Ellenőrizd, hogy az intenzitásmátrix sorösszegei nullák-e, hogy minden fizikailag lehetséges átmenetet felvettem-e, és hogy a közös okú meghibásodást helyesen modelleztem-e! A megoldást ne számold ki.”*

10.4. Ellenőrző szempontok

A jó modellben minden állapot fizikai jelentése egyértelmű, az átmenetek rátái forráshoz kötöttek, a kérdéstípus (tranziens, tartós, elnyelő állapotos) helyesen választott, és az eredmény értelmezése a modell feltevéseinek (exponenciális tartózkodási idő) korlátait is figyelembe veszi.

11.

PFD és SIL-igazolás

Tanulási eredmények

A gyakorlat végére képes leszel

- egy biztonsági funkció PFDavg-értékét az IEC 61508-6 képleteivel kiszámolni;
- ellenőrizni az architekturális korlátokat, és becsülni a téves leállások gyakoriságát;
- érzékenységvizsgálattal és Monte Carlo-szimulációval megítélni az igazolás robusztusságát;
- javaslatot tenni a tesztelési stratégiára (próbaidőköz, részleges löketpróba, a próba lefedettsége).

Háttér: a kézikönyv 13. fejezete.

11.1. Alkalmazás: PFD- és SIL-kalkulátor

Az alkalmazás megnyitása külön lapon

11.2. Feladatok az alkalmazással

1. Töltsd be a ReaktorVéd példát, és ellenőrizd a kézikönyv értékeit (PFD = $1{,}37 \cdot 10^{-3}$, RRF = 731, STR = 0,133/év).
2. Állítsd a szelepek próbalefedettségét 0,9-re. Teljesül-e a követelmény? Ezután adj meg havi részleges löketpróbát 0,6-os lefedettséggel (PST időköz 730 h, DCPST 0,6, PTC 1). Mekkora a tartalék?
3. Cseréld a távadók architektúráját 2oo3-ra. Hogyan változik a PFD és a téves leállások gyakorisága?
4. Redundáns tápellátásnál két tápegység egyidejű kiesése kell a téves leálláshoz: az egyéb téves leállási ráta $2 \cdot (2\lambda_{PSU}^2\,\mathrm{MTTR}) = 8 \cdot 10^{-10}$/h ($\lambda_{PSU} = 5 \cdot 10^{-6}$/h, MTTR = 8 h). Írd be ezt az értéket: ellenőrizd, hogy az MTTFS a kézikönyv szerinti mintegy 22 év lesz, és nézd meg, melyik alrendszer vált dominánssá.
5. A tornádódiagram alapján fogalmazd meg, mely üzemeltetési feltevéseket kell a biztonsági érvelésben mutatóval követni!

11.3. Notebook: SIL-igazolás és bizonytalanság

Megnyitás a Google Colabban · a notebook letöltése

A notebook a képleteket reprodukálja, tornádódiagramot rajzol, és Monte Carlo-szimulációval megmutatja, hogy a bizonytalanság figyelembevételével mekkora a valószínűsége a követelmény túllépésének.

> **Mintaprompt**
>
> *„Egy biztonsági funkció PFD-számítását végeztem: [adatok, architektúrák, eredmény]. Készíts listát azokról a feltevésekről, amelyekre a számítás épül (például a próba lefedettsége, a javítási idő, a közös okú tényezők, az adatok forrása), és mindegyikhez javasolj egy üzem közben mérhető mutatót! Szabványpontra csak akkor hivatkozz, ha biztos vagy benne.”*

11.4. Ellenőrző szempontok

A jó igazolás mindhárom pillért (PFD, architekturális korlátok, szisztematikus képesség) kezeli, minden adat forrását rögzíti, az érzékenységvizsgálatból üzemeltetési követelményeket vezet le, és a téves leállásokat is értékeli.

Összegzés



Pannon Egyetem
University of Pannonia

12.

Projektfeladat: egy rendszer teljes biztonsági elemzése

Tanulási eredmények

A projektfeladat végére képes leszel

- egy általad választott rendszer biztonsági elemzését a veszélyazonosítástól a biztonsági érvelésig önállóan elvégezni;
- a módszereket a kérdéshez illesztve kiválasztani és összekapcsolni;
- az eredményeket ellenőrizhető biztonsági érvelésbe rendezni, és az üzemeltetési feltevéseket mutatókká alakítani;
- a nagy nyelvi modelleket a munka minden lépésében felelősen, dokumentáltan használni.

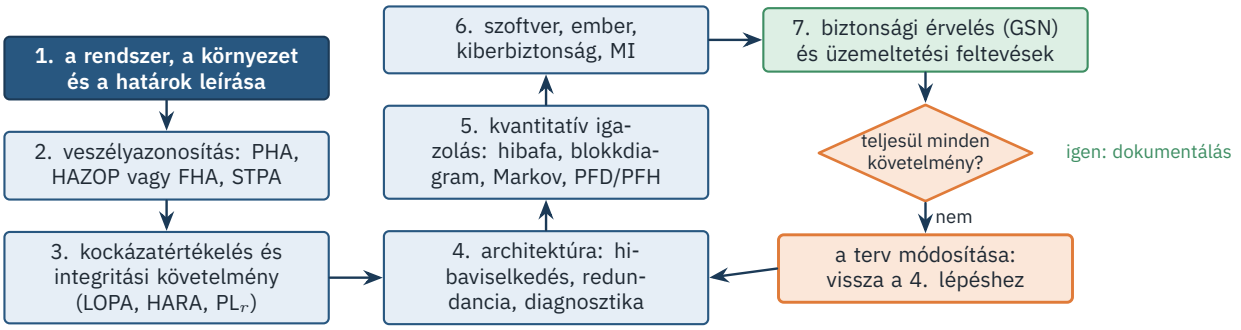
Háttér: a kézikönyv egésze, különösen a 14., 15., 16., 17. és 18. fejezet.

12.1. Választható rendszerek

- automatizált raktári szállítójármű (AMR) emberekkel közös térben;
- orvostechnikai infúziós pumpa;
- vasúti átjáró sorompójának vezérlése;
- hidrogéntöltő állomás nyomásvédelme;
- egy saját, munkahelyi vagy kutatási rendszer (a gyakorlatvezetővel egyeztetve).

12.2. A munka menete

A projekt hét lépésből áll (12.1. ábra). A lépések egymásra épülnek, de a tervezés természeténél fogva iteratív: ha a kvantitatív igazolás nem teljesül, az architektúrához kell visszatérni.



12.1. ábra. A projektfeladat lépései. Az architektúra és az igazolás között iteráció zajlik, amíg minden követelmény teljesül.

12.1. táblázat. A projektfeladat lépései és elvárt eredményei

Lépés	Elvárt eredmény	Kézikönyv
1. rendszer és határok	a funkciók, az üzemállapotok, a környezet és a határok leírása; feltevések	2., 4. fejezet
2. veszélyazonosítás	PHA, illetve a rendszerhez illő HAZOP, FHA/HARA vagy STPA	5–7. fejezet
3. kockázat és integritás	kockázatértékelés; LOPA, HARA vagy PL_r alapján a biztonsági funkciók integritási követelménye	3., 4., 11. fejezet
4. architektúra	hibaviselkedési stratégia, redundancia, diagnosztika, közös okok elleni intézkedések	14. fejezet
5. kvantitatív igazolás	hibafa vagy blokkdiagram, szükség esetén Markov-modell; PFD vagy PFH, érzékenység	8–13. fejezet
6. szoftver, ember, kiberbiztonság, MI	a releváns szempontok elemzése és intézkedései	15., 16., 18. fejezet
7. biztonsági érvelés	GSN-váz a fő állításokkal, bizonyítékokkal és feltevésekkel; az üzemeltetési mutatók	17. fejezet

12.3. Mintapromptok a lépésekhez

> **1–2. lépés: rendszerleírás és veszélyazonosítás**
>
> *„Egy [rendszer] biztonsági elemzését kezdem. A rendszerleírásom: [...]. Kérdezz rá azokra a határokra, üzemállapotokra és külső feltételekre, amelyeket nem adtam meg, és amelyek a veszélyazonosításhoz szükségesek! Utána javasolj egy előzetes veszélylistát, de mindegyik veszélynél jelöld, hogy ez a leírásomból következik vagy általános tapasztalat.”*

> **3–5. lépés: integritási követelmény és igazolás**
>
> *„Az alábbi biztonsági funkcióra [SIL/PL] követelményt határoztam meg ezzel az indoklással: [...]. Ellenőrizd a gondolatmenetet: van-e benne kettős beszámítás, nem független védelem vagy indokolatlan feltevés? Az architektúrámra kapott PFD/PFH-értéket ne számold újra; a feltevéseimet vizsgáld.”*

> **6. lépés: szoftver, ember, kiberbiztonság, MI**
>
> *„A rendszeremben [szoftveres / emberi / hálózati / gépi tanulási] elem is van: [...]. Sorold fel azokat a veszélyforrásokat, amelyeket a hagyományos meghibásodás-alapú elemzés nem tár fel (például a rendeltetésszerű funkció korlátai, az automatizálás iróniái, támadási útvonalak), és mindegyikhez javasolj egy tervezési intézkedést!”*

> **7. lépés: biztonsági érvelés**
>
> *„Az alábbi GSN-vázat készítettem a biztonsági érvelésemhez: [...]. Keress benne rejtett feltevéseket, a bizonyíték és az állítás közötti réseket, és olyan állításokat, amelyek nem ellenőrizhetők! Mindegyikre javasolj pontosabb megfogalmazást.”*

12.4. Ellenőrző szempontok

A projekt akkor jó, ha a lépések következetesen egymásra épülnek (a veszélyekből követelmények, a követelményekből architektúra, az architektúrából igazolás lesz); a módszerválasztás indokolt; minden szám és feltevés forráshoz kötött; a kvantitatív eredmény mellett az érzékenység és a bizonytalanság is szerepel; a biztonsági érvelés a gyenge pontokat is őszintén megmutatja; és dokumentált, mire és hogyan használtad a nagy nyelvi modelleket.

Irodalom

Buncefield Major Incident Investigation Board. 2008. *The Buncefield Incident 11 December 2005: The Final Report of the Major Incident Investigation Board*. HSE Books.

Bureau d'Enquêtes et d'Analyses. 2012. *Final Report on the Accident on 1st June 2009 to the Airbus A330-203 Registered F-GZCP Operated by Air France Flight AF 447 Rio de Janeiro–Paris*. BEA.

Lions, Jacques-Louis. 1996. *ARIANE 5 Flight 501 Failure: Report by the Inquiry Board*. European Space Agency.

National Transportation Safety Board. 2019. *Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian, Tempe, Arizona, March 18, 2018*. NTSB/HAR-19/03. NTSB.

U.S. Chemical Safety and Hazard Investigation Board. 2007. *Investigation Report: Refinery Explosion and Fire, BP Texas City, Texas, March 23, 2005*. 2005-04-I-TX. CSB.



Pannon Egyetem
University of Pannonia

Biztonságkritikus rendszerek – gyakorlati útmutató

Nyílt hozzáférésű tankönyv

https://complexsystemsintelligence.github.io/biztonsagkritikus-rendszerek/gyakorlat/