Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Méréstechnika és Információs Rendszerek Tanszék

Kiberfizikai rendszerek modellalapú kiberbiztonsági analízise

Diplomaterv

Készítette
Csernátony Döme Máté

Konzulens
Dr. Vörös András

2024. május 8.

Tartalomjegyzék

HALLGATÓI NYILATKOZAT

Alulírott *Csernátony Döme Máté*, szigorló hallgató kijelentem, hogy ezt a diplomatervet meg nem engedett segítség nélkül, saját magam készítettem, csak a megadott forrásokat (szakirodalom, eszközök stb.) használtam fel. Minden olyan részt, melyet szó szerint, vagy azonos értelemben, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Hozzájárulok, hogy a jelen munkám alapadatait (szerző(k), cím, angol és magyar nyelvű tartalmi kivonat, készítés éve, konzulens(ek) neve) a BME VIK nyilvánosan hozzáférhető elektronikus formában, a munka teljes szövegét pedig az egyetem belső hálózatán keresztül (vagy autentikált felhasználók számára) közzétegye. Kijelentem, hogy a benyújtott munka és annak elektronikus verziója megegyezik. Dékáni engedéllyel titkosított diplomatervek esetén a dolgozat szövege csak 3 év eltelte után válik hozzáférhetővé.

Budapest, 2024. május 8.

Csernátony Döme Máté
hallgató

Kivonat

A modern gépjárművekben egyre jelentősebb szerepet kapnak a számítástechnikai megoldások. Ma egy prémium személyautó közel 150 elektronikus vezérlőegységgel (ECU) és számos kommunikációs sínnel rendelkezik.

Ezek a feltételek egyrészről lehetővé tették komplexebb üzembiztonsági (safety) megoldások és fejlett vezetéstámogató rendszerek (ADAS) használatát, másrészről viszont a járműbe integrált elektronikai eszközök és azoknak az infokommunikációs hálózatokhoz való csatlakozása megnövelte a lehetséges kiberbiztonsági fenyegetések számát.

Az elmúlt években a járművek ellen elkövetett kibertámadások száma évről évre folyamatosan növekedett és ez a szám hálózati kommunikációban résztvevő járművek terjedésével csak tovább fog növekedni.

Az autóiparban a kockázatalapú biztonság-kezelés terjedt el, mint kiberbiztonsági alapelv, amely a felfedezett fenyegetésekhez, a megállapított kockázat alapján határozza meg az egyes védelmi mechanizmusok szükségességét.

Ezen fenyegetések, kockázatok és védelmi mechanizmusok megállapítására vonatkozó előírások már megtalálhatóak a modern autóipari szabványok közt, viszont az alkalmazásuk még további támogatást igényel. Ebben nyújthatnak segítséget a már elterjedt általános IT biztonsági keretrendszerek, valamint az autóiparban már régóta jelenlévő üzembiztonsági elemzés eszközei.

A feladatom célja, hogy adjak egy metodológiát amely segíti az autóipari rendszerek tervezési fázisban történő kiberbiztonsági analízisét, valamint megvalósítsak egy eszközt ami minnél magasabb szintű automatizálással teszi lehetővé az elemzés elvégzését.

Abstract

Electrical and Electronic (E&E) solutions are playing an increasingly important role in modern automotives. Today, a premium car contains around 150 electronic control units (ECU) and several communication buses.

On the one hand, these conditions enabled the use of more complex safety solutions and advanced driver assistance systems (ADAS), but on the other hand, the electronic devices integrated in the vehicle and their connection to infocommunication networks increased the number of possible cyber security threats.

In recent years, the number of cyber attacks against vehicles has increased year by year, and this number will only continue to increase with the spread of vehicles participating in network communication.

In the automotive industry, risk-based security management has spread as a basic cyber security principle, which determines the need for individual protection mechanisms for discovered threats based on the established risk.

Provisions for establishing these threats, risks and defense mechanisms can already be found in modern automotive industry standards, but their application still requires further support. The general IT security frameworks that are already widespread, as well as the operational safety analysis tools that have been present in the automotive industry for a long time, can help in this.

The goal of my task is to provide a methodology that helps the cyber security analysis of automotive systems in the design phase, as well as to implement a tool that enables the analysis to be carried out with the highest possible level of automation.

1. fejezet

Bevezetés

A járműelektronika, mint olyan elektronikus rendszer amely járművek belsejének valamelyik részén kerülnek integrálásra egy adott feladat ellátására, már a járművek történelmének korai korszakában is fellelhetőek. Ami a kezdetekben csak egy fedélzeti rádió volt az 1930-as években, az később bővült a gyújtási rendszer elektronikai alapokra helyezésével az 1960-as évektől, később pedig a technológia és a félvezetők fejlődésével egyre több és több feladatot láttak el.

Ha csak belegondolunk, hogy milyen elektronikai eszközök lehetnek egy modern gépjárműben akkor hamar észrevesszük, hogy az ablaktörlő, az oldalsó ablakok és ülések mozgatása, környezetvédelmi szempontokból a motort szabályozó különböző érzékelők, kamerarendszerek vagy a napjaink prémium járműveiben már érintőképernyős fedélzeti számítógépek és akár a szervókormányok elektomos rásegítése mind ilyen elektronikai rendszerek használatával történnek.

Ezeket a beágyazott rendszereket általánosan elektronikai vezérlőegységeknek (ECU, electronic control unit) nevezzük.

Az elmúlt 10-20 évben több technológiai forradalom is elindult az autóiparban, ebből az egyik az először hibrid, majd teljesen elektromos hajtásláncú járműveknek a drasztikus terjedése, bizonyos adatok szerint évente akár 50%-kal több is kerülhet forgalomba. Ezek az elsősorban környezetvédelmi szempontok miatt, kőolaj és egyéb nemfenntartható energiaforrástól való elszakadást szolgálják. Ennek a forradalomnak egyik nagy eredménye ami az én témámhoz is kapcsolódik az a tendencia, miszerint már a legkomplexebb mechanikai folyamatokat amelyek egy járművet működtettek is villamossági alapokra terelték át, ezzel technikailag a járművekre mint komplex beágyazott rendszerekre is lehet tekinteni.

A másik nagy forradalom ami az én témámat érinti az a kezdetekben fejlett vezetéstámogató rendszerek (ADAS, advanced driver assistance systems), ma viszont már akár teljes önvezetésre képes járműveknek a megjelenése. Ez bizonyos szempontból összefügg az előzővel, hiszen a komplex jármű folyamatok áttterelését villamossági alapokra, részben az önvezetésre való törekvésnek is köszönhető. Azonban érdemes kiemelni, hogy már az önvezetés nélkül is, a jármű évjáratától és felszereltségétől függően, találhatunk rengeteg vezetéstámogató rendszert. Ezek a rendszerek már olyan komplexitással rendelkeznek amiben a jármű különböző komponensei, amelyek akár külön beszállítóktól is érkezhetnek, koordinált feladatvégrehajtást is képesek ellátni. Ezeknek a rendszereknek a feladata lehet egyrészről kényelmi (pl. tempomat, parkolás segítő, stb.) vagy biztonsági (pl. vonalkövetés, holttérfigyelő, fáradtságérzékelő, stb.).

Habár ezeknek a rendszereknek az ismertetése egy külön fejezetet is megérne, az amivel én foglalkozok, hogy ezeknek a rendszereknek a jelenléte és a elektronikai megoldásoknak terjedése egy olyan kockázatot von magával amelyre az autóipar és járműgyártás rugalmatlan struktúrái még viszonlyag limitáltan vannak felkészülve, ez

pedig a kiberbiztonsági kockázatoknak a megjelenése.

Habár a biztonsági kockázatok kezelése nem új dolog az autóiparban, hiszen az üzembiztonság már több mint egy évtizede szabványosítva (ISO 26262, 2011) működik, addig a kiberbiztonság még csak pár éve került szabványosításra (ISO 21434, 2021). Ez azt jelenti, hogy a kiberbiztonsági elemzése ezeknek a rendszereknek még sokkal kevesebb magas érettségű technikával rendelkezik, mint az üzembiztonsági elemzések.

Üzembiztonság esetén a kockázatok már korai fázisban felmérésre kerülnek és azokhoz a fejlesztési időt megelőzően, tervezési fázisban meghatározzák a mitigációkat. Ez annyit tesz, hogy már az egyes komponensek tervezésekor, lehetnek azok rendszer-, szoftver- vagy hardverszintű hibák, a kezdeti architektúra is úgy van meghatározva, hogy ezeknek a potenciális hibáknak az előfordulása minimális legyen.

Ezzel szemben a kiberbiztonság egy fiatal terület a kiber-fizikai rendszerek világában, viszont az is rendelkezik egy pár évtizedes múlttal az IT rendszereknél. Itt jellemzően már kész integrált rendszereknek történik az elemzése, felmérik a potenciális belépésipontjait egy támadónak, azoknak a lehetséges céljait, majd ezekre határoznak meg további szoftveres (pl. tűzfal) vagy hardveres (pl. DMZ) védelmeket, ezt a folyamatot nevezik általánosságban fenyegetésmodellezésnek (threat modelling). Még szintén fontos megemlíteni a monitorozás és utánkövetést, hiszen újabb és újabb sérülékenységek kerülhetnek elő a termék életciklusa során amelyeket utólag kell javítani ezeknél a rendszereknél.

Ezzel együtt is a korábban említett ISO 21434 szabvány tesz több ajánlást az IT rendszerek biztonsági elemzésére felhasznált módszerek adaptálására egy az üzembiztonsághoz hasonló kockázatalapú tervezési fázisú felmérésre, ezt nevezik úgy, hogy Threat Analysis and Risk Assessment (TARA).

Az én célom először egy olyan automatizmus készítése, amely az autóiparra már jellemző modellekből kiberbiztonsági elemzésre alkalmas modelleket készít, ez egyfajta származtatás lenne a rendszermodell és a fenyegetésmodell között. Majd ennek a származtatott modellnek az elemzésére fejlesztek egy eszközt, ami egyrészről követi az ISO 21434-ben definiált TARA követelményeit és ajánlásait, másrészről pedig felgyorsítja a kiberbiztonsági mérnökök munkáját támadási fák valamint dokumentumok automatikus generálásával.

A *Háttérismeretek* fejezetben bemutatom az autóipari kiberbiztonsg szabályozási területét, bevezetem a szükséges fenyegetésmodellezési fogalmakat valamint bemutatom a megvalósításhoz használt eszközöket.

A *Kapcsolódó tanulmányok* fejezetben a már a témában létező és általam elemzett kutatásokat mutatom be, azoknak az alkalmazhatóságát az én feladatomnál valamint a megközelítésükben lévő hibákat amelyeket én orvosolni próbálnék.

A kiberbiztonsági analízis metodológiája a modellező eszköz részeiről, azok működéséről valamint a használatuk bemutatásával fog foglalkozni.

A modellező eszköz megvalósítása az eszközhöz felhasznált technológiákról és az azokban lévő architektúrális megoldásokról, valamint döntésekről szól.

Az *Esettanulmány* című fejezet egy példán való bemutatása az analízis végrehatásának, valamint az eredmények értelmezése

Végül pedig az *Összegzés* alatt lesznek találhatóak az elért célok kiértékelése, alkalmazási lehetőségek, bővítési lehetőségek, valamint a használt források pedig az *Irodalomjegyzékben* lesznek találhatóak.

2. fejezet

Háttérismeretek

A célja ennek a fejezetnek, hogy átadjam a témám értelmezéséhez szükséges alapismereteket, fogalmakat és bemutassam a használt technikai eszközöket. Ebben a fejezetben leírtak lesznek szükségesek ahhoz, hogy a későbbi fejezeteket teljességükben lehessen értelmezni.

Először szeretném a későbbiekben használt szakszavakat definiálni, az elterjedt szakirodalmakban található leírások alapján.

Majd ezután írok az autóipari kiberbiztonság szabályozási környezetéről, azon belül is elsősorban az ISO/SAE 21434 szabványról fogok írni, ami lefedi alapvető irányelveket ehhez a területhez, valamint ad egy kezdetleges metodológiát a kiberbiztonsági kockázatelemzésre.

Később adok egy leírást az IT biztonság területén már ismert fenyegetésmodellezés technikákról és keretrendszerekről.

Végül pedig adok egy rövid leírást a munkám során alkalmazott eszközökről és technológiákról.

2.1. Kiberbiztonsághoz kapcsolódó alapfogalmak

Ebben a fejezetben található minden továbbiakban nem általánosnak vehető, az autóipari és a kiberbiztonsági területeken használt szakszavaknak a definíciói. Ezek a leírások elsősorban a már elérhető kutatásoknak, szabályozásoknak és szabványoknak a szójegyzékére építenek.

- **Termék (product / item):** Egy önmagában is értelmezhető és értékesíthető rendszer, amelynek a biztonságát biztosítani kell. Ez lehet egy komponens vagy komponensek csoportja és egy jármű-szintű funkcionalitást valósít meg, pl. kormányrendszer, fékrendszer, szoftver-frissítési infrastruktúra
- **Komponens (component):** Logikailag és/vagy technikailag szeparálható elem
- **Úthasználó (road user):** Személy aki valamilyen formában az utat használja, pl. gyalogos, autóvezető, utas, stb.
- **Kiberbiztonsági terv (cybersecurity concept):** Kiberbiztonsági követelményei egy terméknek, az üzemeltetési környezetnek, támogató információk a mitigációkhoz
- **Kiberbiztonsági specifikáció (cybersecurity specification):** Részletesebb kiberbiztonsági követelmények allokálva az architektúrális tervre
- **Kiberbiztonsági cél (cybersecurity goal):** Magas-szintű kiberbiztonsági követelmény

- **Kiberbiztonsági állítás (cybersecurity claim):** Állítás egy kockázatról
- **Mitigáció (mitigation / cybersecurity control):** Kockázatmódosító intézkedés
- **Érték (asset):** Egy tárgy ami értékkel rendelkezik
- **Kiberbiztonsági tulajdonság (cybersecurity property):** Egy attribútum amelyet meg kell védeni, pl. sértetlenség, bizalmasság, elérhetőség
- **Károkozás (damage scenario):** Egy kedvezőtlen következmény amely hatással van az úthasználóra
- **Fenyegetés (threat scenario):** Egy lehetséges kompromittálása valamilyen érték kiberbiztonsági tulajdonságának, amely egy károkozáshoz vezethet (pl: egy szoftveres sérülékenység kihasználása)
- **Támadási útvonal (attack path):** Események (pl: egy fenyegetés megvalósulása) egymás utáni bekövetkezése, amelyek egy fenyegetést realizál
- **Támadási lépés (attack step):** Az egyes események amelyeknek az egymás utáni sorozata egy támadási útvonalat realizál

2.2. Autóipari kiberbiztonsági szabályozások és szabványok

Az autóipari kiberbiztonság területe ellentétben az üzembiztonsággal vagy a bővebb IT biztonsággal még csak pár éves múltra tekint vissza, emiatt az itt alkalmazandó szabályozások és szabványok még csak az első alkalommal kerültek kiadásra.

2.2.1. UN ECE R155

Az első specifikusan autóipari szabályozás az Egyesült Nemzetek által kiadott 155-ös számú szabályozás a kiberbiztonságról és a kiberbiztonság kezelő rendszerekről és járművek engedélyeztetésének kapcsolatáról (UN ECE R155[6]). Ennek a szabályozásnak kell megfelelnie a járműgyártóknak és beszállítóiknak az összes 2024 után megjelenő járműmodell engedélyeztetéséhez.

Ez a szabályozás már tartalmazza az igényt a kockázat-alapú kiberbiztonsági kezelés szükségességére. Ami annyit tesz, hogy a biztonsági szolgáltatásokat az alapján kell meghatározni, hogy egy kiberbiztonsági fenyegetés esetleges bekövetkezése mekkora hatással lenne a védendő autóipari termékre.

Szintén már megtalálhatjuk az autóipari termékek életciklusának különválasztását fejlesztési, gyártási és gyártás utáni fázisokra, ami mutatja azt, hogy a kiberbiztonsági szempontból fontos figyelembe, venni, hogy az életciklus különböző szakaszain más-más fenyegetésekre lehet számítani, valamint ez alapján más követelmények is lesznek érvényesek a termékre.

A dokumentum a továbbiakban követelményeket határoz meg, hogy milyen folyamatokon kell keresztülmennie egy autóipari terméknek, ahhoz, hogy az a közúti használatra engedélyt kapjon.

2.2.2. ISO/SAE 21434

A másik, már technikaibb szintű, szintén 2021-es megjelenésű, irányadó szabvány az autóipari kiberbiztonsági mérnökségről szóló ISO/SAE 21434 "Road vehicles - Cybersecurity engineering". Ezt a szabványt közösen fejlesztette és adta ki 2021 augusztusában az International Standards Organization (ISO) és a Society of Automotive Engineers (SAE).

Ez a szabvány kezdett el követelményeket megfogalmazni az autóipari rendszerek (E/E) kiberbiztonsági kockázatkezelésének menetére, valamint a biztonság fejlesztésére és kezelésére. A felépítése emlékezetheti az olvasóját a már jóval ismertebb ISO 26262 "Road vehicles - Functional safety" szabványra, amely ugyanazon termékeknek az üzembiztonság kezelésére és elemzésére fókuszál.

Kezdésképpen a szabvány tervezési, fejlesztési, gyártási, üzemeltetési, karbantartási és kivezetési fázisaira fogalmaz meg követelményeket, valamint tartalmaz egy fenyegetés elemző és kockázat értékelő eljárást amelynek a Threat Analysis and Risk Assessment (TARA) nevet adták.

Továbbá tartalmaz más követelményeket a kiberbiztonsági elvárások kezelésére menedzsment és organizációs szintekre, azonban ezek ismerete nem tartozik a témám látókörébe.

Maga a téma kifejezetten a tervezési fázishoz tartozó kockázatelemzésnek a végrehajtására vonatkozó követelményeit veszi alapul. A később bemutatásuk során felfedezhető lesz, hogy nem elhanyagolható szüksége van a kockázatelemzés iteratív használatának eltérően az életciklus fázisaira, azonban a termék üzemeltetési környezetére vonatkozó védelmet ebben a fázisban határozzuk meg.

2.2.2.1. Követelmények a tervezési fázisra

A tervezési fázis egy autóipari termék életciklusában a kiindulópont. Az ebben a fázisban végzett kiberbiztonsági tevékenységek célja, hogy (i) definiálásra kerüljön az elemzendő termék, a környezete és interakciói, (ii) meghatározzák a kiberbiztonsági célokat és állításokat valamint, hogy (iii) elkészüljön a kiberbiztonsági terv.

A **termék definíciója** tartalmazza a termék határait, feladatait, valamint az előzetes architektúrát. Célunk itt az, hogy összegyűjtsük az elemzéshez szükséges információkat.

A **kiberbiztonsági célok és állítások** meghatározásához szükséges a TARA elvégzése, amelynek a kimenete, az egyes kockázatok kezelésére vonatkozó döntések lesznek, amelyek alapján eldönthetjük, hogy a kockázathoz egy célt vagy állítást kell megfogalmaznunk. A cél fogja meghatározni a magas-szintű követelményt amit a termék fejlesztése során figyelembe kell venni, míg az állítás azt határozza meg, hogy az adott kockázat mitigálása valamilyen okból már teljesül vagy a teljesülése szükségtelen.

Ezután készülhet el a **kiberbiztonsági terv**, amelyben az egyes mitigációkat határozzuk meg a célok elérésére, a célokat tovább finomítjuk követelményekké, majd azokat allokálhatjuk a termékre vagy egyes komponensekre.

2.2.2.2. Követelmények a fenyegetéselemzésre és kockátértékelésre

A TARA bemenete a termék definíció, és ez alapján lehet elvégezni a hét lépésből álló kockázatelemzési eljárást aminek a kimenete az egyes fenyegetések kockázati értékkel, valamint azok kezeléséről szóló döntés.

Az első lépése a kockázatelemzésnek az **érték azonosítás**. Ennek a lépésnek két célja van, az egyik, hogy a lehetséges *károkozásokat* azonosítja és annak segítségével az egyes *értékeket*, a másik pedig, hogy az értékekhez *kiberbiztonsági tulajdonságokat* rendelünk. A károkozások tartalmazhatják a kár körülírását, a releváns értékeket és a kapcsolatot a járműfunkcionalitás és a kedvezőtlen következményt. Az értékek azonosítására pedig használhatjuk továbbá a termékleírást, *fenyegetések* definiálását vagy már létező katalógusokat.

A második lépés a **hatásértékelés**. Itt a célunk az egyes lehetséges károkozásokat, valamilyen keretrendszer mentén értékelni azok következményeit. Egy lehetőség, amit több szabvány is említ az a SFOP alapú értékelés, ami négy dimenziót határoz meg amiben el

kell végezni az értékelést. Ezek pedig az üzembiztonsági hatás (safety), gazdasági hatás (financial), üzemeltetési hazás (operational), valamint az adatvédelmi hatás (privacy).

A harmadik lépés a **fenyegetések azonosítása**, amelyekhez hozzá kell rendelni a támadott *értéket*, annak a kompromittált *kiberbiztonsági tulajdonságát*, valamint a kompromitálás okát. A szabvány szerint ezek azonosítására lehet egyrészről csoportos, brainstorming alapú vagy szisztematikus, keretrendszerek által meghatározott módszereket is alkalmazni, utóbbi esetben javasolja valamilyen ismert fenyegetésmodellezési megközelítést használni. Néhány felsorolt példa ezekre az EVITA, TVRA, PASTA és a STRIDE.

A negyedik lépés a **támadási útvonal elemzés**, erre a szabvány szerint top-down vagy bottom-up megközelítést is használhatunk. Előbbi esetben támadási fákat, támadási gráfokat, utóbbi esetben már ismert sérülékenységekre alapulót.

Az ötödik lépés a **támadás megvalósíthatóságának vizsgálata**, ahol több már létező keretrendszert alkalmazhatunk az egyes támadási útvonalak kiértékelésére.

A hatodik lépés a **kockázatiérték meghatározás**. Itt egy egytől ötig terjedő skálán értékeljük a fenyegetési szcenáriókat a hatásértékek és a megvalósíthatósági értékek alapján.

A hetedik és egyben utolsó lépés pedig a **kockázatkezelési döntés**, amikor az egyes kockázatok kezeléséről hozhatunk döntést. A kockázatokat elkerülhetjük, csökkenthetjük, megoszthatjuk valamint megőrizhetjük.

Jól látható, hogy ezek a követelmények elég általánosak, sokat döntési jogosultságot helyez a folyamatot bevezető személyekre, emellett viszont magasszinten jól körülírt követhető lépéseket határoz meg amelyek megfelelnek más szabályozások feltételeinek és képes eljuttatni a mérnököt a konkrét megvalósítandó intézkedések meghatározásához.

2.3. Fenyegetésmodellezési keretrendszerek és módszerek

A fenyegetésmodellezés egy olyan folyamat, aminek segítségével azonosítani tudjuk a lehetséges fenyegetéseket, valamint segítenek azok értékelésében.

Ez a folyamat már viszonylag régóta elterjedt a kiberbiztonsági szakmában és támogató jellegű kapcsolatban áll a kockázatelemzésekkel. Amíg a fenyegetésmodellezés célja a fenyegetések meghatározása, a kockázatelemzés az ami segít nekünk a feltárt fenyegetések kezelésének priorizálásában vagy esetenként az egyes fenyegetések elhagyásában.

Tágabb értelemben akár a kockázatelemzést is vehetjük a fenyegetésmodellezés részének, azonban az ISO/SAE 21434 szabványban leírt folyamat is különválasztja azokat és a fenyegetésmodellezést kifejezetten a fenyegetések meghatározására hasznosítaná.

2.3.1. CIA és AAA

Habár talán még nem is egy teljes fenyegetésmodellezési keretrendszer a CIA háromszög vagy CIA triád, mégis a legtöbb kiberbiztonsági elemzés ezen betűszó által kifejezett modellt alkalmazza.

Már korábban beszéltünk kiberbiztonsági tulajdonságokról, itt a CIA által definiáltak használjuk, ezek a bizalmasság (confidentiality), sértetlenség (integrity) és elérhetőség (availability).

Szintén szokás még kibővíteni ezt a modellt egyéb tulajdonságokkal, ilyenek lehetnek a AAA modell elemei amelyek az egyediség (authenticity), engedélyezhetőség (authorizability), valamint az elszámoltathatóság (accountability).

Adott értéknek a tulajdonságait meghatározhatjuk az alábbi kérdések feltevésével:

- **Bizalmasság**: Harmadik fél szerezhet-e tudomást az értékről, annak tartalmáról?
- **Sértetlenség**: Az érték módosulása vezethet-e nem várt következményekhez?

- **Elérhetőség**: Az érték hiánya vezethet-e nem várt következményekhez?
- **Egyediség**: Kell-e az érték eredetét biztosítani felhasználása előtt?
- **Engedélyezhetőség**: Szükséges-e az adott értékhez való hozzáférés korlátozása?
- **Elszámoltathatóság**: Szükséges-e az adott értékhez való hozzáférések, módosulások visszakövethetősége?

A továbbiakban ezeket a modelleket fogom alkalmazni a kiberbiztonsági tulajdonságokként, azonban ezek módosíthatók, elhagyhatóak, cserélhetőek és bővíthetőek felhasználási környezetüktől függően.

2.3.2. STRIDE

A STRIDE egy modell, amely számítógépes kiberbiztonsági fenyegetések azonosítására lett kifejlesztve a Microsoft által 1999-ben. A nevét a hat fenyegetéstípusról kapta, ezek és a jelentésük:

- **Spoofing:** Megszemélyesítés, amikor a rendszer egy hamisan érzékeli a te kilétedet
- **Tampering:** Valamilyen információ megváltoztatása
- **Repudiation:** Annak az állítása, hogy valamit nem te csináltál vagy nem is történt meg
- **Information disclosure:** Egy támadó képes olyan információhoz való hozzáférésre amihez nincs felhatalmazva
- **Denial of Service:** Erőforrások túlterhelése miatt szolgáltatás elérhetetlenné tétele
- **Elevation of privilige:** Egy támadó képes olyan művelet elvégzésére amire nincs felhatalmazva

Ez első ránézésre egy jó lehetséges kategorizálást ad meg nekünk fenyegetésekhez, valamint kibővíthető ezek kapcsolata az azonosított értékekhez és kiberbiztonsági tulajdonságaikhoz. Tehát az egyes fenyegetés típusok egy bizonyos tulajdonság sérülését célozzák.

Spoofing	Egyediség (authenticity)
Tampering	Sértetlenség (integrity)
Repudiation	Letagadhatatlanság (non-repudiability)
Information disclosure	Bizalmasság (confidentiality)
Denial of Service	Elérhetőség (availability)
Elevation of privilige	Engedélyezhetőség (authorizatiability)

2.1. táblázat. Fenyegetések kapcsolata kiberbiztonsági tulajdonságokkal

Ebből jól látható, hogy az egyes értékekhez a tulajdonságaik alapján már azonosíthatjuk az azok kompromittálását célzó lehetséges fenyegetéseket.

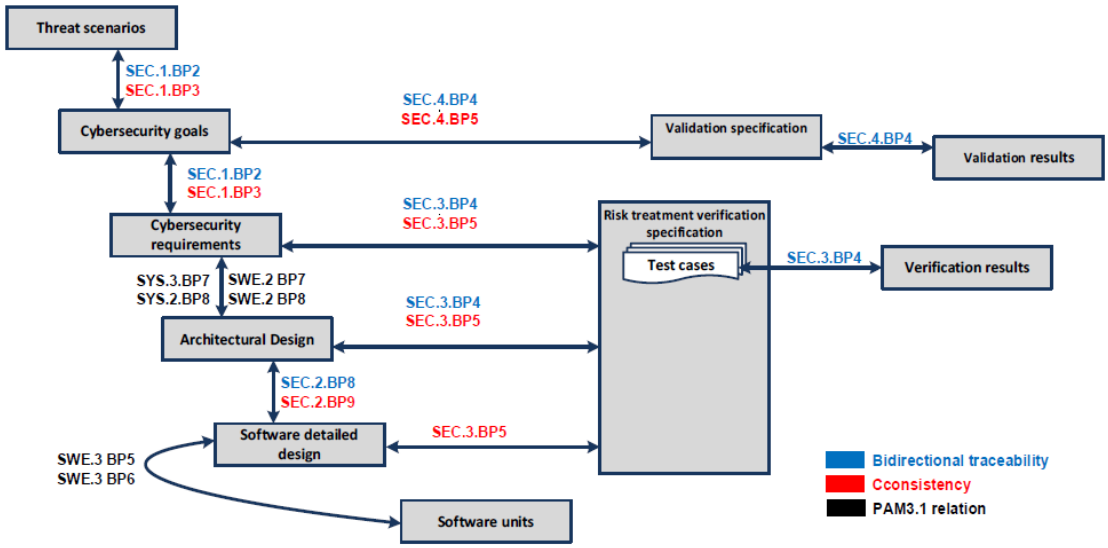
2.4. Autóipari rendszerek általános tervezése és modellezése

A diplomamunkám sajátossága abból adódik, hogy amíg az általános IT rendszerek architektúrális tervezésének jellemzően kisebb hagyománya van addig a kiber-fizikai rendszereknél, azon belül is a járműveknél, a rendszer komplexitása és üzembiztonság kritikussága miatt, mély hagyománya van ezeknek a rendszerekhez tartozó kezdeti tervdokumentumok készítésének.

2.4.1. V-modell

A V-modell egy szoftverfejlesztési folyamat amelyet az ASPICE szabvány adaptál az autóiparban. Lényegében arról szól, hogy a fejlesztés V alakban történik, ahol bal oldalt fentről lefele történik a tervezés és a fejlesztés, a jobb oldalon pedig minden lépéshez tartozik egy verifikációs vagy validációs lépés.

Nemrégiben kapott az ASPICE[1] szabvány egy kiegészítést a kiberbiztonsági mérnöki folyamatokhoz amelyeket részben az ISO 21434 is definiált. Ezekről egy összefoglaló a 2.1 ábrán látható.



2.1. ábra. Az ASPICE javaslata kiberbiztonsági folyamatokra[1]

Szintén érdemes itt megjegyezni, hogy az általam javasolt metodológia egyfajta visszacsatolást (feedback) tenne lehetővé az *Architectural design* és a *Threat scenarios* lépések közt. De erről később bővebben lesz szó.

2.4.2. UML és SysML

A komplex E/E architektúrák esetén, mint amilyenek az autóipari beágyazott rendszerek, jellemző valamilyen formában a rendszermodellek jelenléte és karbantartása a termék életciklusa alatt. Erre elsősorban a SysML (System Modeling Language) van használva, ami egy bővítése az UML-nek (Unified Modeling Language).

Az UML egy általános felhasználású grafikus modellezési nyelv amelynek a célja rendszerek modellezése, de használják gazdasági területeken vagy szoftver tervezésnél is.

Az UML több diagram típust különböztet meg, azokat elsősorban két kategóriába sorolhatjuk, az egyik a strukturális a másik pedig a viselkedési diagramok. Strukturálishoz tartoznak az osztály, komponens, kompozit és profil diagramok, a viselkedéshez pedig az aktivitás, szekvencia, interakció vagy use case (használati eset) diagramok.

Az UML szintén támogatja az egy adott doménre való szabását a modellezési nyelvnek, ezt profilok definiálásával lehet megtenni. A profilokra érdemes úgy gondolni mint egyfajta bővítmények, amelyeket bizonyos modell elemekre tudunk hozzászabni.

A SysML az UML nyelvi elemeinek egy részhalmazának egy további nyelvi elemekkel bővített verziója. Ezeket a bővítéseket egy SysML profillal implementálják és elsősorban ez a nyelv van használva komplex hardver-szoftver rendszerek modellezésére.

Az én megoldásom végül az alap UML-hez tartalmaz egy kiberbiztonsági profilt, mivel a SysML bővítményei nem voltak használva. A termék leírására valamint a kockázatelemzés érték és károkozás definíciós szakaszára egy használati eset (use case) és egy komponens (component) diagrammot használok.

2.5. Felhasznált eszközök

2.5.1. Papyrus

A Papyrus egy nyílt forráskódú UML 2 modellező eszköz. Ezt az eszközt fogom használni az értékek definiálására egy komponens diagramon valamint a károkozásokat egy használati eset diagramon.

Ebben az eszközben továbbá definiálok egy kiberbiztonsági profilt ami bővítményeket tartalmaz komponensekhez és használati esetekhez.

2.5.2. Acceleo

Az Acceleo egy nyílt forráskódú Model-2-Text (M2T) eszköz, amellyel a Papyrus-ban definiált modellekből fogom generálni a kiberbiztonsági elemző eszköz kiinduló modelljét. Más szóval ezzel az eszközzel származtatom a rendszermodellből a kiberbiztonsági modellt.

Azért eset a választásom erre az alkalmazásra az Xtend helyett, mivel az integrációja a Papyrus eszközzel sokkal jobban működik, illetve minimális komplexitású kódgenerálást fogok csak ezzel végezni.

2.5.3. Eclipse Modelling Framework

Az Eclipse Modelling Framework, vagy röviden EMF egy modellezési keretrendszer ami arra ad támogatást, hogy könnyen lehessen modellező eszközöket, majd ahhoz kódgenerátor alkalmazásokat fejleszteni.

Az EMF támogatja modellek definiálását, majd azokból automatikusan Java kódot származtat, ezzel elősegítve a modell könnyebb transzformációját, módosítását és abból való származtatást.

Az EMF szintén ad egy automatikusan generált kezelőfelületet a definiált modell szerkesztésére, tartalommal feltöltésére.

Ezt a keretrendszert használtam a kiberbiztonsági elemző eszköz metamodelljének definiálására, valamint az eszköz kezelő felülete is a generált szerkesztő felületre épül.

2.5.4. Xtend

Az Xtend egy Java alapú programozási nyelv amelyet elsősorban kódgenerálási célokra lehet használni.

Ezt a nyelvet használtam arra, hogy elkészítsem először a modellből való generálását a szabványos dokumentumoknak, valamint a támadási fák inicializálását is ebben készítettem.

2.5.5. Sirius

3. fejezet

Kapcsolódó tanulmányok

Ennek a fejezetnek a célja, hogy összefoglaljam a diplomamunkámhoz előzetesen elvégzett kutatómunka során megismert tanulmányok eredményeit, problémáit, valamint a lehetséges alkalmazásukat az én feladatomhoz.

A kutatómunkámat először a fenyegetésmodellezés (threat modeling) területen született tanulmányok olvasásával kezdtem, amelyek segítettek megismerni a fenyegetések felmérése során felmerülő problémákat és megoldásuknak módjait.

Ezek után az autóipari biztonsági elemzések területén végzett munkák segítettek abban, hogy megismerjem milyen komponenseket és azoknak mely attribútumai lesznek használhatóak egy elemzés során.

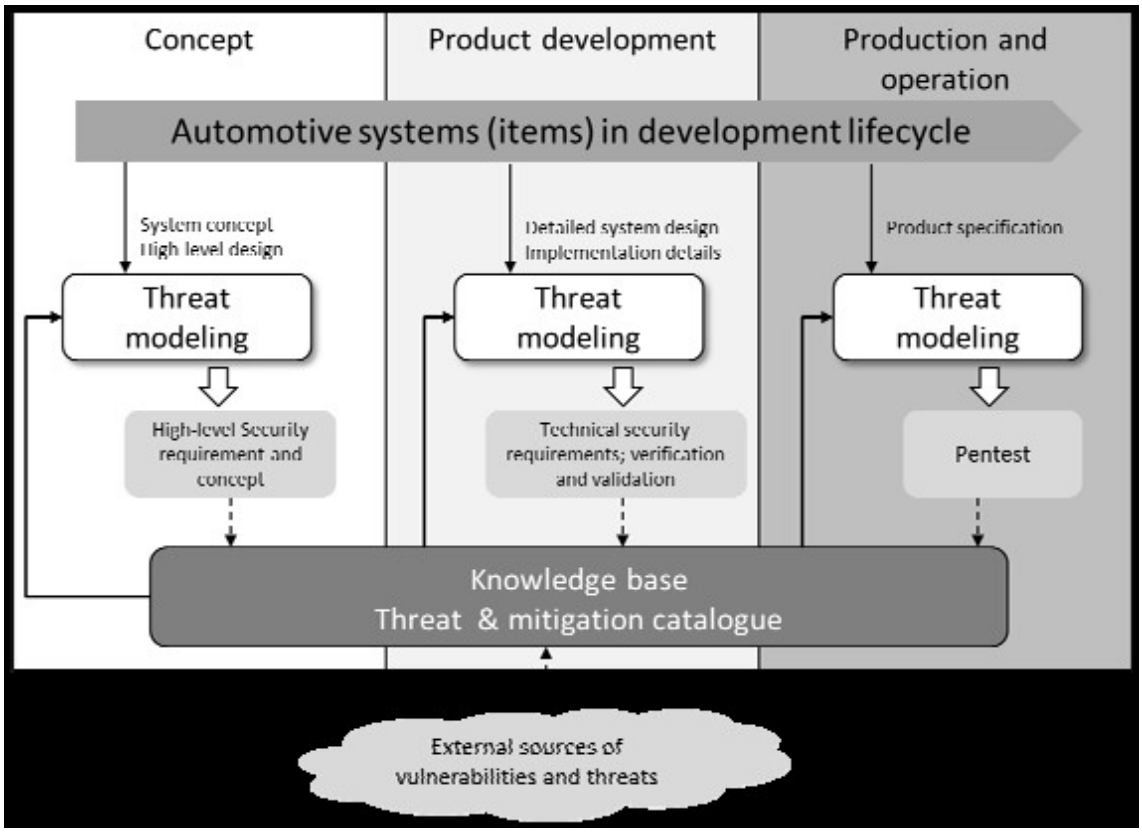
Végül pedig megismertem a már meglévő kutatásokat amelyek támadási fák (attack trees) generálásáról szólnak, ezek az üzembiztonság területén elterjedt hibafa (fault tree) analízis eszközének adaptációja a kiberbiztonsági terület támogatására.

3.1. Fenyegetésmodellezés

Az első témába illő kutatás a Karahasanovic et al.[3] kutatása volt "Adapting Threat Modelling Methods for the Automotive Industry" címmel. Ez két fenyegetésmodellezési keretrendszert mutat be, egyik az Intel-hez köthető TARA (Threat Agent Risk Assessment), ami nem összekeverendő az azonos rövidítéssel fémjelzett Threat Analysis and Risk Assessment metodológiával. Másik pedig a sokkal ismertebb Microsoft által fejlesztett STRIDE. Az előbbi a grafikus modellezési technikák helyett egy könyvtárakon alapuló fenyegetés elemzést mutat be, ahol három könyvtárat használnak, egyik a lehetséges támadó ágenseket, másik az általuk véghezvihető támadásokat a harmadik pedig a jellemző támadási felületeket gyűjti. A kutatás ezen könyvtárakból határoz meg egy részhalmazt ami az autóipari rendszerek ellen alkalmazható. Utóbbi technika már a támadó-centrikusság helyett inkább szoftver-centrikus, ami egy fehér doboz vizsgálatot tesz lehetővé a rendszeren. Ez a későbbiekben még előforduló Data Flow Diagrammok használatára mutat be egy példát amelyben a szoftver komponensek közti kommunikációt modellezi és tud egy támadási útvonalat végigkövetni. Az előbbi technika gyengesége az, hogy csak magasszinten definiálja a fenyegetéseket ami nem elégséges a védelmi mechanizmusok meghatározására. Utóbbi ezzel szemben alkalmas arra, viszont nem lehet vele rendszer szintű védelmet modellezni.

Ezután olvastam el Ma et al.[12] kutatását "Threat Modeling for Automotive Security Analysis" címmel, amelyik a fenyegetésmodellezést egy sokkal gyakorlatibb módon közelíti meg, nem feltétlenül a technikai részekre koncentrál, hanem a termékfejlesztési életciklust és a már meglévő üzembiztonsági analíziseket is figyelembe veszi. Helyesen jelzi a szükségét az analízis szintekre bontásának, hasonlóan az üzembiztonsághoz, azonosítja az igényét egy funkcionális kiberbiztonsági tervnek valamint egy technikai kiberbiztonsági

tervnek, kiegészítve egy termékspecifikációval. Ezeknek a jelenlétét pedig lebontja az elsőt a tervezési fázisban, magasszintű követelmények azonosításához, a másodikat a termékfejlesztési szakaszhoz, bemenetként a rendszermodellt használva, a specifikációt pedig a gyártási fázisban való használattal. A kutatás tartalmaz még egy esettanulmányt amely egy jármű utasterének a biztonsági analízisén vezet végig, a Microsoft Threat Modelling Tool használatával, ami a STRIDE keretrendszerre épít, data flow diagrammokat használ és modell alapon generál lehetséges fenyegetéseket. Konklúzióként emeli ki az igényt, hogy a biztonsági analízis modellezési paradigmáit, valahogyan integrálni szeretnék a rendszermodellezés paradigmáival, ezzel biztosítva, hogy az analízis a változások során napra kész maradjon. A termékfejlesztési fázisok és kiberbiztonsági elemzéseket a 3.1 ábrán részletezik.



3.1. ábra. Fenyegetésmodellezés a termékfejlesztési életciklusokban[12]

Ezen a területen még egy kutatást [10] vizsgáltam meg ami egy esettanulmány volt egy tetszőleges autóipari komponensre, kiértékeléshez egy módosított STRIDE modellt használt, valamint az ISO 21434-ben definiált kockázatelemzés kezdeti lépéseit amelyek a lehetséges fenyegetések feltárására vannak alkalmazva.

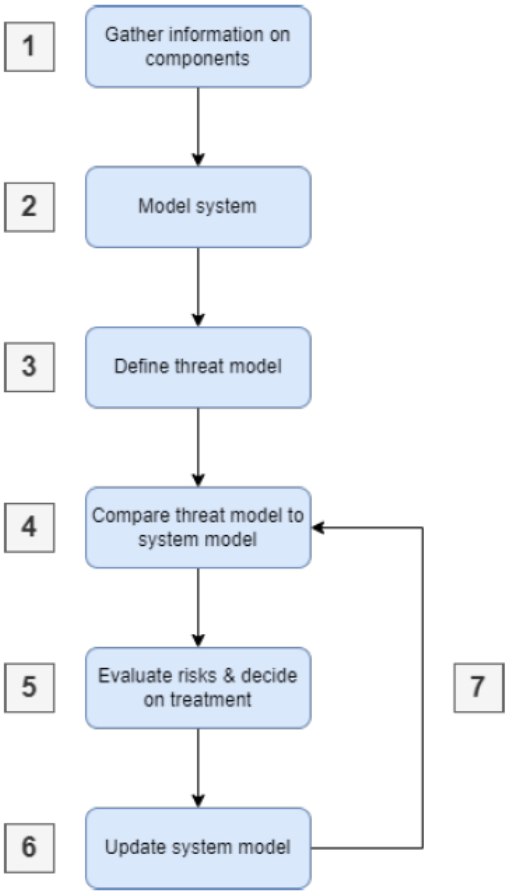
3.2. Kiberbiztonság és üzembiztonság kapcsolata

Ezzel a témával kapcsolatban Dantas et al. [11] kutatását vizsgáltam meg annak területén, hogy a szabványosított kockázatelemzésre, hogyan lehet már meglévő technikákat alkalmazni valamint, hogy a kockázatelemzés, hogyan illeszkedik be már létező folyamatokba. A dokumentum részletesen elemzi a kiberbiztonság fontosságát az autóiparban, valamint a szoftverfrissítés jelenlétét mint fontos eszközt esetleges sérülékenységek javításában. Szintén elemezve van a rendszeres és folyamatos auditálása és kiértékelése ezeknek a folyamatoknak. Ezekhez jelzi a lehetőséget különböző domain-specifikus nyelvek használatának

lehetőségét és automatizálás integrálását, illetve modellellenőrző rendszerek bevezetését. Van még szó az üzembiztonság területén alkalmazott FTA és FMEA analízisek technikájának felhasználásáról a támadási útvonalak elemzésében, illetve idéz több más tanulmányt és keretrendszert amelyek szintén ezen alkalmazásokat ösztönzik.

Szintén olvastam Bohner et al.[5] kutatását amely az üzembiztonsági architektúrát terjesztené ki a kiberbiztonsági kockázatok kezelésére. Helyesen hívja fel a figyelmet arra, hogy a kiberbiztonságban használt CIA triádból kettő, az integritás (integrity) valamint a rendelkezésre állás (availability) az üzembiztonság területén is alkalmazva vannak. Említésre kerülnek itt a memória particionálás mint ami mint a két területen csökkentik a kockázatot, az üzenetek védelmét módosítás ellen, valamint összességében a kiberbiztonság mint részhalmaza az üzembiztonságnak ahol a véletlenszerűen előforduló hibák helyett a szándékosan okozott hibákat kell figyelembe vennünk. A kockázat csökkentő intézkedések alkalmazása pedig szignifikánsan tudja mind a két biztonság hatékony szolgáltatását.

Még ami ide tartozna az Chulp et al.[8] kutatása ami egy ThreatGet nevezetű kiberbiztonsági kockázatelemző eszköz működési elvét mutatja be amely a bécsi egyetemen készült. Ez az eszköz gyakorlatiasan írja le a tervezési fázisban elvégzendő kockázatelemzés menetét, ebben már az ASPICE-szal ellentétben láthatunk feedback alkalmazását a folyamat lépései közt, azonban az én célommal ellentétben ez egy külön modellt használ kockázatelemzésre amelyet össze kell hasonlítani majd a meglévő rendszermodellel, ahogy az a 3.2 ábrán látható.



3.2. ábra. Fenyegetésmodellezés folyamata a tervezési fázisban[8]

Chulp et al.[8] kutatásában továbbá hasonlóan az én munkámhoz a STRIDE fenyegetésmodellezési keretrendszert valamint a CIA attribútumait használják. Szintén érdemes kiemelni a fenyegetésmodellezésre jellemzően használt Data Flow Diagram kiegészített for-

máját amelyet Extended Data Flow Diagramnak neveznek, ebben egy részről kompozíciók modellezését teszik lehetővé, másrészről pedig értékek (asset) megjelenítéséről is gondoskodtak. Ebben a kutatásban hangzik el először az automatizált támadási fa generálásának fogalma, valamint a tanulmány támadási gráfokat is definiál. A kutatás jól használja fel az Extended Data Flow Diagram rendszermodelljét támadási fák és gráfok generálására amelyekből támadási utakat vezet le amelyek alkalmasak lesznek valódi kockázatok meghatározására.

3.3. Támadási fa generálás

Elsőnek Sowka et al.[7] publikációját olvastam amelyben különböző alkalmazásait értékelte az automatikus támadási fáknak az autóipari kiberbiztonság doménjében. Az írás adott egy általános áttekintést a terület fontosságáról, a szabályozási környezet aktuális helyzetéről majd összehasonlította a különböző elérhető megoldásokat az adott problémára. Ezekből választottam én is további kutatásokat amelyeket érdemes lehet átolvasni.

Salfer et al.[2] által bemutatott módszer egy magas fokú modellezett megoldás alapján való támadási utak előállítását határozza meg. Kifejezetten érdekes, ahogy felépíti a metamodelljét egy rendszer és egy támadó modellnek is. A rendszermodell meghatározza az elektronikus vezérlő egységeket, szoftvereket, kommunikációs hálózatokat és értékeket (*asset*), a támadó modell pedig tartalmazza a tudást, motivációt, amelyek aztán a támadások megvalósíthatóságának értékelésében játszanak szerepet. Szintén elemzi ezeknek a támadási utaknak az alkalmazását a rendszer kiberbiztonsági (penetrációs) tesztelésénél és jól ismeri fel, hogy ez egy magasszintű white-box tesztelésben lehetne felhasználható.

Karray et al.[4] kutatása sokban épít az előző bekezdésben említettre, azonban itt nem lehet egy explicit támadómodellről beszélni. A rendszermodell használ bizonyos tulajdonságokat amelyek jelzik a támadó szükséges tudását vagy belépési szükségét, viszont kevesebb feltevést használ a támadások meghatározásánál. A gráf trnaszformáció valamint a rendszermodell még alkalmas lehet a saját munkámhoz.

Végül pedig Bryans et al.[9] kutatását néztem meg amely kombinálja a modell alapú valamint a könyvtár alapú automatizált generálást, azaz a modell és template alapú támadási fa generálást. A Chulp et al.[8] kritikája alapján is ez volt kiemelve mint legérettebb megoldás, valamint ez is az egyik legfiatalabb. A támadó modell helyett előredefiniált támadási mintákat használ fel, amelyek segítségével rekurzívan tud a fa leveleiből kifejteni komplexebb támadásokat egyfajta bottom-up megközelítésben. A rendszermodell szemben a template-ekkel sokkal egyszerűbb, nem különít el ECU funkcionalitást vagy értékeket, emiatt ez a része nem lesz használható a munkám során, viszont ez teszi lehetővé teszteléskor a black-box megközelítést, valamint akár teszt kódok és eszközök integrációjával is lehetne használni deszkriptív template-ek esetén. Célom az, hogy ezt a fajta kombinált megközelítést alkalmazzam erősebben rendszermodellezett megközelítéssel és egyszerűsítettebb template-ekkel.

4. fejezet

A kiberbiztonsági analízis metodológiája

4.1. Áttekintés

4.2. Termékleírás és fenyegetésmodell származtatása

4.3. Fenyegetésmodellezés

4.3.1. Károkozások attributálása

4.3.2. Értékek attributálása és dependenciák meghatározása

4.4. Támadási fák inicializálása és szerkesztése

4.5. Dokumentumok generálása és manuális analízis

5. fejezet

A kiberbiztonsági analízis megvalósítása

5.1. Kiberbiztonsági modell származtatása

5.1.1. Kiberbiztonsági profil

5.1.2. Fenyegetésmodell generátor

5.2. Fenyegetésmodellező eszköz

5.2.1. Metamodel

5.2.2. Fenyegetésmodell szerkesztő felület

5.2.3. Támadási fák inicializálása

5.2.4. Támadási fa szerkesztő felület

5.2.5. Dokumentum generátor

6. fejezet

Esettanulmány

7. fejezet

Összegzés

Irodalomjegyzék

[1] ASPICE: Automotive spice® for cybersecurity process reference and assessment model, 2021.

[2] Efficient attack forest construction for automotive on-board networks, 2014.

[3] Almgren M. Karahasanovic A., Kleberger P.: Adapting threat modeling methods for the automotive industry, 2017.

[4] Khaled Karray: Cyber-security of connected vehicles : contributions to enhance the risk analysis and security of in-vehicle communications, 2020.

[5] Alexander Much Martin Böhner, Alexander Mattausch: Extending software architectures from safety to security, 2015.

[6] United Nations: Un regulation no. 155 - cyber security and cyber security management system, 2021.

[7] A review on automatic generation of attack trees and its application to automotive cybersecurity, 2023.

[8] Christoph Schmittner Sebastian Chlup, Korbinian Christl: Threatget: Towards automated attack tree analysis for automotive cybersecurity, 2022.

[9] A template-based method for the generation of attack trees, 2020.

[10] Tanvi Tirthani Yashodhan Vivek: Automotive system threat modeling, 2022.

[11] Dr. Vivek Nigam Yuri Gil Dantas, Dr. Harald Ruess: Security engineering for iso21434, 2020.

[12] C. Schmittner Z. Ma: Threat modeling for automotive security analysis, 2016.