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 17.

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 17.

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 minél 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 szakaszában is fellelhetőek. Ez a kezdetekben, az 1930-as években, csak egy fedélzeti rádió volt. Később, az 1960-as évektől bővült a gyújtási rendszer elektronikai alapokra helyezésével. Napjainkban pedig már, a technológia és a félvezetők folyamatos fejlődésének köszönhetően, a járműelektronikai megoldások egyre több és több feladatot látnak 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 szervokormányok elektromos rásegítése is mind ilyen elektronikai rendszerek használatával történnek.

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

Az elmúlt 10-20 év technológiai fejlődése forradalmi változásokat hozott az autóiparban. Először megjelentek a hibrid, majd a teljesen elektromos hajtásláncú járművek. Részarányuk az eladásokban drasztikusan növekedett.Bizonyos adatok szerint évente akár 50%-kal is több került forgalomba. Ezek a fejlesztések elsősorban környezetvédelmi szempontok miatt történtek, a kőolaj és egyéb nem megújuló energiaforrástól való elszakadást szolgálják. Ennek a forradalomnak egyik nagy eredménye, ami dolgozatom témájához is kapcsolódik, az a tendencia, miszerint már a járművet működtető legkomplexebb mechanikai folyamatokat is villamossági alapokra terelték át.

A másik, szintén forradalminak nevezhető változás a fejlett vezetéstámogató rendszerek (ADAS, advanced driver assistance systems) területén jelentkezett. Egymásután jelentek meg újabb és újabb megoldások, melyek mára már teljes önvezetésre képes járműveket eredményezett. Ez bizonyos szempontból összefügg az előzővel, hiszen a komplex jármű folyamatok áttelerélését 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, hogy a jármű különböző komponensei akár különböző beszállítóktól is érkezhetnek, és mégis koordinált feladat végrehajtást képesek ellátni. Ezeknek a rendszereknek a feladata lehet egyrészről kényelmi (pl. tempomat, parkolás segítő, stb.) vagy biztonsági (pl. vonalkövetés, holttérfigyelő, fáradtságérzékelő, stb.).

Bár ezeknek a rendszereknek az ismertetése egy külön fejezetet is megérne, dolgozatom szempontjából az a fontos, hogy ezeknek a rendszereknek a jelenléte és az

elektronikai megoldások terjedése olyan kockázattal jár, amelynek kezelésére az autóipar és járműgyártás rugalmatlan struktúrái még viszonylag korlátozottan vannak felkészülve, ez pedig a kiberbiztonsági kockázatoknak a megjelenése.

A biztonsági kockázatok kezelése nem új dolog az autóiparban, hiszen az üzembiztonság már több mint egy évtizede szabványosítva (ISO 26262, 2011) működik. A kiberbiztonság még csak pár éve került szabványosításra (ISO 21434, 2021). Ez azt jelenti, hogy ezeknek a rendszereknek a kiberbiztonsági elemzése 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, már a 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. Az általános IT rendszereknél viszont ez is rendelkezik egy pár évtizedes múlttal. Itt jellemzően már kész integrált rendszereknek történik az elemzése, felmérik a támadó potenciális belépési pontjait, 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 monitorozást és az 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 Threat Analysis and Risk Assessment-nek, vagy röviden TARA-nak.

Dolgozatomban először egy olyan eljárást javaslok, amely az autóiparra már jellemző modellekből kiberbiztonsági elemzésre alkalmas modelleket készít. Ez az eljárás automatikusan származtatja a rendszermodellből a fenyegetésmodellt. Ezt követően 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 kiberbiztonság 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, ismertetve azok alkalmazhatóságát a dolgozatom célja elérésében. Ugyancsak taglalom a megközelítésükben lévő hiányosságokat.

A kiberbiztonsági analízis metodológiája a modellező eszköz alkotóelemeivel, azok működésével, valamint a használatuk bemutatásával foglalkozik.

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

Az *Esettanulmány* című fejezet az eljárás egy példán való bemutatása, az analízis végrehajtása, valamint az eredmények értelmezése.

Végül pedig az *Összegzés* alatt lesznek találhatóak az elért célok kiértékelése, alkalmazási lehetőségek és bővítési lehetőségek. A dolgozat az *Irodalomjegyzékkel* zárul, ahol a használt források találhatóak.

2. fejezet

Háttérismeretek

A célja ennek a fejezetnek, hogy összefoglaljam 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.

Az első fejezet tartalmazza a későbbiekben használt szakszavakat az elterjedt szakirodalmakban található leírások alapján.

Ezután következik az autóipari kiberbiztonság szabályozási környezete, azon belül is elsősorban az ISO/SAE 21434 szabvány, ami lefedi a terület alapvető irányelveit, valamint ad egy kezdetleges metodológiát a kiberbiztonsági kockázatelemzésre.

Ezt követi egy leírás az IT biztonság területén már ismert fenyegetésmodellezés technikákról és keretrendszerekről.

Végül pedig a munkám során alkalmazott eszközök és technológiák rövid ismertetése olvasható.

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, amely egy károkozást realizálnak
- **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 változatukban 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[7]). 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, és ennek megfelelően 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 termékek üzembiztonságának a kezelésére és elemzésére fókuszál.

A szabvány először a tervezési, fejlesztési, gyártási, üzemeltetési, karbantartási és kivezetési fázisokra 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 különböző menedzsment és organizációs szintekre, azonban ezek ismerete nem tartozik a témám látókörébe.

Dolgozatom kifejezetten a tervezési fázishoz tartozó kockázatelemzés végrehajtására vonatkozó követelményeket veszi alapul. A későbbi bemutatásuk során felfedezhető lesz, hogy a kockázatelemzés iteratív használatának szükségessége az életciklus különböző fázisaiban, azonban a termék üzemeltetési környezetére vonatkozó védelmet ebben a tervezési fázisban határozzuk meg. Ezzel elkerülve a magasabb költségű utólagos fejlesztéseket.

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, aminek az eredményeképp születnek meg, az egyes kockázatok kezelésére vonatkozó döntések, 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 teljesült 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 kockázatértékelésre

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 az azok kezeléséről szóló döntés.

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

A kockázatelemzés második lépése a **hatásértékelés**. Itt a célunk az egyes lehetséges károkozásokat és azok következményeit valamilyen keretrendszer mentén értékelni. Egy lehetőség, amit több szabvány is említ, az az SFOP alapú értékelés. Az SFOP négy dimenziót határoz meg amiben el kell végezni az értékelést. Ezek az üzembiztonsági hatás

(safety), gazdasági hatás (financial), üzemeltetési hatás (operational), valamint az adatvédelmi hatás (privacy).

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

A negyedik lépés a **támadási útvonal elemzés**. Az elemzés során 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, sok döntési jogosultságot helyez a folyamatot bevezető személyekre, emellett viszont magas szinten 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 javasolja.

2.3.1. CIA és AAA

Bár még nem is egy teljes fenyegetésmodellezési keretrendszer a CIA háromszög vagy CIA triád, mégis a legtöbb kiberbiztonsági elemzés az 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 előfordul ennek a modellnek a bővítése egyéb tulajdonságokkal, ilyenek a szoftverbiztonság esetén használt AAA modell elemei amelyek az egyediség (authenticity), engedélyezhetőség (authorizability), valamint az elszámoltathatóság (accountability).

Adott értéknek a tulajdonságait meghatározhatjuk az alábbi kérdések megválaszolásával:

- **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. Az én esetemben a CIA elegendő lesz, hiszen autóipari beágyazott rendszerekben a szoftver szinten azon tulajdonságok relevánsabbak. Az üzenet egyediségének hamisítása már az eredeti üzenet egyfajta sérülését vonja magával, ez a sértetlenség tulajdonság által már kezelve van. Az engedélyezhetőség pedig már bonyolultabb operációs rendszerek használatánál kerül elő, ami külön felhasználókat és hozzáféréseket tud definiálni. Ez bizonyos formában az autóiparban is fellelhető, de nem abban a komplexitásban mint Linux vagy Windows alapú rendszereknél. Az elszámoltathatóság szintén problémás mivel ennek a biztosítása, a beágyazott rendszerek limitált hardvererőforrásai miatt nem tud azzal a granularitással létezni, ahogy a hozzáférések számon lennének tartva IT rendszereknél.

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 hamisan érzékeli az információ küldőjének a kilétét
- **Tampering:** Valamilyen információ megváltoztatása
- **Repudiation:** Annak az állítása, hogy valamit nem te csináltál vagy nem is történt meg
- **Information disclosure:** Egy támadó képes hozzáférni olyan információhoz amire nincs jogosultsága
- **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.

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

Ezekből én mivel csak a CIA tulajdonságait használom, az én esetemben a Tampering, Disclosure és Denial fenyegetések lesznek a tulajdonságokból származtatva.

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

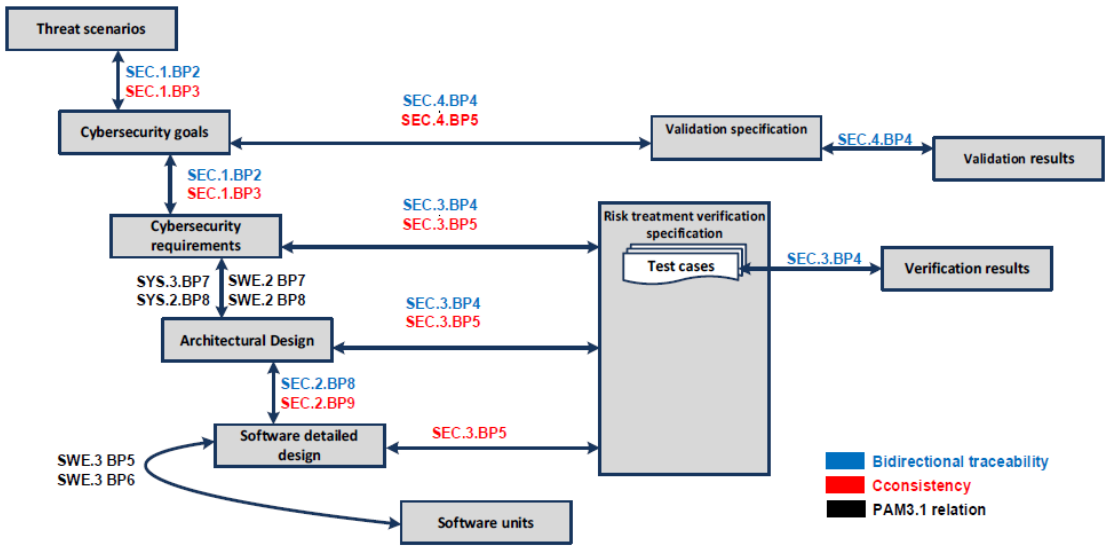
2.4. Autóipari rendszerek általános tervezése és modellezése

A diplomamunkám sajátossága abból adódik, hogy amíg az általános IT rendszereknek vagy azok egyes elemeinek az architektúrális tervezése kevésbé jellemző, addig a kiberfizikai rendszereknél, azon belül is a járműveknél, a rendszer komplexitása és az üzembiztonság kritikussága miatt, nagy hagyománya van ezeknek az átfogó dokumentálására már a tervezés kezdeti szakaszában.

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 célja a rendszerek specifikálása, a felépítésük leírása, vizualizálása és dokumentálása a fejlesztésben érdekelt minden résztvevő számára.

Az UML több diagram típust különböztet meg, azokat elsősorban két kategóriába sorolhatjuk, az egyik a strukturális a másik pedig a viselkedési diagramok. A strukturális diagramok közé tartozik a csomag, a komponens, az objektum, az osztály, a kompozit, a profil és a telepítési diagramok. A viselkedési diagramok közé pedig az aktivitás, az állapotgép, a használati eset, a kommunikációs, a szekvencia, és az időzítési diagramok.

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

A SysML az UML nyelvi elemei egy részhalmazának további nyelvi elemekkel bővített verziója. Ezeket a bővítéseket egy SysML profillal implementálják és elsősorban ezt a nyelvet használják a komplex hardver-szoftver rendszerek modellezésére.

Az én megoldásom az alap UML bővítéseképp tartalmaz egy kiberbiztonsági profilt, mivel a SysML bővítményei nem voltak elegendők az autóipari rendszerek kiberbiztonsági elemzésére, tervezésére. A termék leírására, valamint a kockázatelemzés érték és károkozás definíciós szakaszára egy használati eset (use case) és egy komponens (component) diagramot 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 keresztül.

Ebben az eszközben definiálok továbbá egy kiberbiztonsági profilt, ami bővítményeket tartalmaz a komponensekhez és a 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 támogatott, illetve mivel nincs szükség nagy komplexitású kódgenerálásra.

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, továbbá 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, majd a támadási fák inicializálását is.

2.5.5. Sirius

A Sirius egy nyílt forráskódú szoftverprojekt amelynek a célja, hogy könnyen lehessen grafikus felületeket létrehozni domén specifikus modellekhez Eclipse-ben.

Ez a keretrendszer volt használva a támadási fák megjelenítéséhez és azok szerkesztésére használt grafikus felület létrehozására.

3. fejezet

Kapcsolódó tanulmányok

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

A kutatómunkámat három témában végeztem, az első a fenyegetésmodellezés (threat modeling) területe volt. Ezen kutatásokon keresztül ismertem meg a fenyegetések felmérése során felmerülő problémákat, megoldásuknak módjait, azok lehetséges megjelenítését és modellezését.

A második téma az autóipari biztonsági elemzések területén készült munkák kutatása volt, hogy meg tudjam ismerni, hogy egy elemzés során milyen komponensekre és azoknak mely attribútumaira kell fókuszálni. Szintén megismertem olyan metodológiákat és best practice-eket, amelyeket az általam kidolgozott metodológiámban is fel tudtam használni.

A harmadik a legspecifikusabb téma azon kutatási eredmények megismerése, amelyek támadási fák (attack trees), illetve támadási gráfok (attack graphs) generálásáról szóltak.Ezek a publikációk az üzembiztonság területén elterjedt hibafa (fault tree) analízis eszközének adaptációi a kiberbiztonsági terület támogatására.

3.1. Fenyegetésmodellezés

Az első témába a Karahasanovic et al. [3] *"Adapting Threat Modelling Methods for the Automotive Industry"* című munkája illeszkedik. Ez két fenyegetésmodellezési keretrendszert mutat be. Az egyik az Intel-hez köthető TARA (Threat Agent Risk Assessment), ami nem összekeverendő az azonos rövidítéssel fémjelzett Threat Analysis and Risk Assessment metodológiával amit az ISO 21434 definiál. A másik pedig, a sokkal ismertebb Microsoft által fejlesztett STRIDE.

Az előbbi a grafikus modellezési technikák helyett egy könyvtárakon alapuló fenyegetés elemzést mutat be. Az elemzés során három könyvtárat használnak, egyik a lehetséges támadó ágenseket, másik az általuk véghezvihető támadásokat a harmadik pedig, a jellemző támadási felületeket gyűjti össze. Ezen könyvtárakból határoz meg egy olyan részhalmazt, ami az autóipari rendszerek ellen alkalmazható.

A második technika a támadó-centrikusság helyett inkább szoftver-centrikus irányt követi, ami egy fehér doboz vizsgálatot tesz lehetővé a rendszeren. Ez, a későbbiekben még előforduló Data Flow Diagramok használatára mutat be egy példát amelyben a szoftver komponensek közti kommunikációt modellezi és így tud egy támadási útvonalat végigkövetni.

Az előbbi technika gyengesége az, hogy csak magas szinten definiálja a fenyegetéseket, ami nem elégséges a védelmi mechanizmusok meghatározására. Utóbbi ezzel szemben alkalmas arra, viszont nem lehet vele rendszer szintű védelmet modellezni, valamint

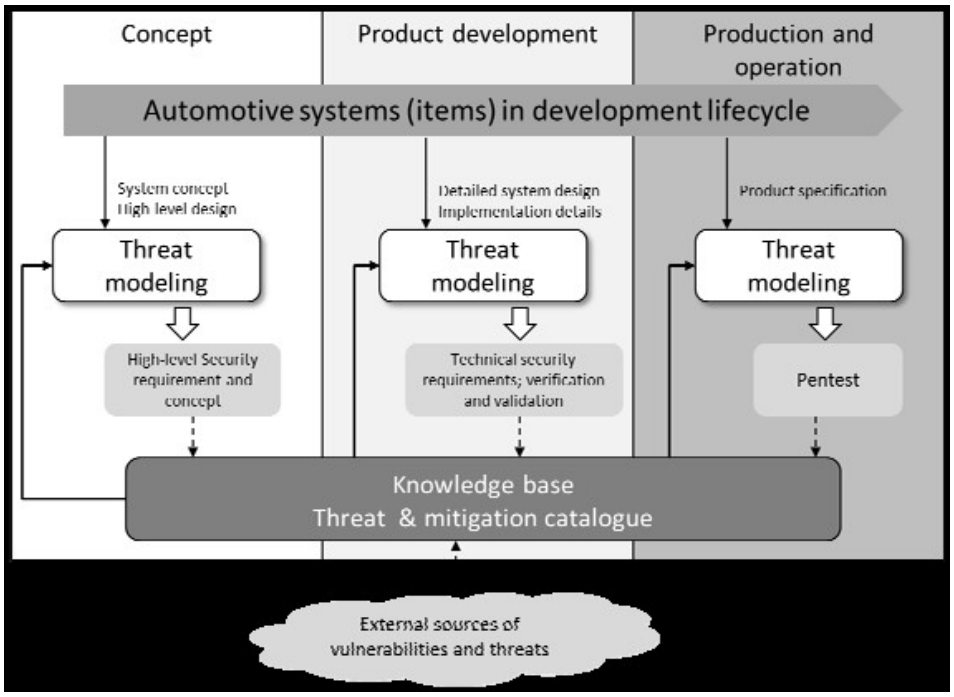
tervezési fázisban is nehezen alkalmazható.

Ma et al.[12] *"Threat Modeling for Automotive Security Analysis"* című munkája, a fenyegetésmodellezést egy sokkal gyakorlatiasabb módon közelíti meg, nem feltétlenül a technikai részekre koncentrál, hanem a termékfejlesztési életciklust és a már meglévő üzembiztonsági analíziseket is figyelembe veszi.

Helyesen fogalmazza meg jelzi a szükségét az elemzésszintekre bontásának, valamint hasonlóan az üzembiztonsághoz, egy funkcionális kiberbiztonsági tervnek, és egy termékspecifikációval kiegészített technikai kiberbiztonsági tervnek a szükségességét. Ezeket aztán lebontja és egyrészt a tervezési fázisban, magas szintű követelmények azonosításához, másrészt a rendszermodellt használva a termékfejlesztési szakasz bemeneteként, harmadrészt a gyártási fázisban használja.

Ez a munka 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 diagramokat használ és modell alapon generál lehetséges fenyegetéseket.

Konklúzióként emeli ki az igényt, hogy a biztonsági analízis modellezési paradigmáit integrálni kell a rendszermodellezés paradigmáival, ezzel biztosítva, hogy az analízis a változások során napra kész maradjon. A termékfejlesztési fázisokat és kiberbiztonsági elemzéseket a 3.1 ábrán részletezik.



3.1. ábra. Fenyegetésmodellezés a termékfejlesztési életciklusokban[12]

Ehhez a területhez tartozik még Vivek et al.[10] *"Automotive system threat modelling"* című esettanulmánya, amelyben egy tetszőleges autóipari komponensre, a kiértékeléshez egy módosított STRIDE modellt használ, valamint a lehetséges fenyegetések feltárására az ISO 21434-ben definiált kockázatelemzés kezdeti lépéseit alkalmazza.

3.2. Kiberbiztonság és üzembiztonság kapcsolata

Ezzel a témával kapcsolatban Dantas et al. [11] *"Security engineering for ISO21434"* című munkája mutatja be, hogy a szabványosított kockázatelemzésre, hogyan lehet már meglévő technikákat alkalmazni, valamint, hogy a kockázatelemzés, hogyan illeszkedik be a már létező folyamatokba.

A dokumentum részletesen elemzi a kiberbiztonság szerepét az autóiparban, valamint a szoftverfrissítés fontosságát az esetleges sérülékenységek javításában. Szintén ki van emelve a folyamatok rendszeres és folyamatos auditálásának és kiértékelésének a szüksége. Ezekhez jelzi a lehetőséget különböző domén-specifikus nyelvek használatának lehetőségét és automatizálás integrálását, illetve modellellenőrző rendszerek bevezetését.

Van még szó az üzembiztonság területén alkalmazott FTA (Fault Tree Analysis) és FMEA (Failure Modes and Effects Analysis) technikák felhasználásáról a támadási útvonalak elemzésében, illetve idéz több más tanulmányt és keretrendszert amelyek szintén ezen alkalmazásokat ösztönzik.

Böhner et al.[5] *"Extending software architectures from safety to security"* című munkája az üzembiztonságra kidolgozott architektúrát terjeszti ki a kiberbiztonsági kockázatok kezelésére. Helyesen hívja fel a figyelmet arra, hogy a kiberbiztonsági elemzések alapjául használt CIA triádból kettő, az integritás (integrity) valamint a rendelkezésre állás (availability) az üzembiztonság területén már a véletlenszerű hibák esetére alkalmazva vannak.

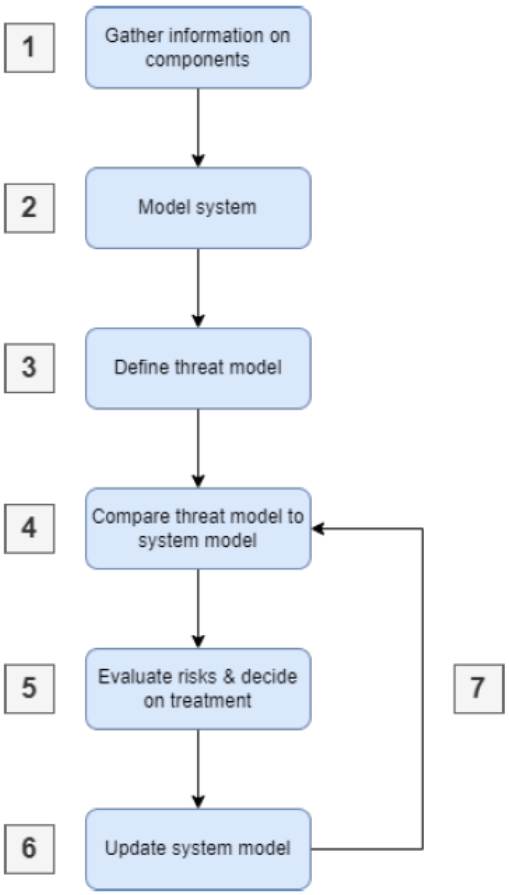
Említésre kerülnek még olyan megoldások, amelyek mind a két területen csökkentik a kockázatot. Ilyenek a memória particionálás illetve az üzenetek védelme a módosítás ellen. Bemutatja, hogy a kiberbiztonság esetén a szándékosan okozott hibákat kell figyelembe vennünk, ellentétben az üzembiztonság véletlenszerűen előforduló hibái helyett. A kockázat csökkentő intézkedések alkalmazása pedig szignifikánsan tudja mind a két fajta biztonság hatékony szolgáltatását.

Chulp et al.[9] *"ThreatGet: Toward automated attack tree analysis for automative cybersecurity"* című munkája 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. Az eszköz az ASPICE-szal ellentétben már vizsgálja a folyamat lépései közti feedback lehetőségét és egy külön modellt is használ kockázatelemzésre amelyet össze hasonlítana a meglévő rendszermodellel, ahogy az a 3.2 ábrán látható.

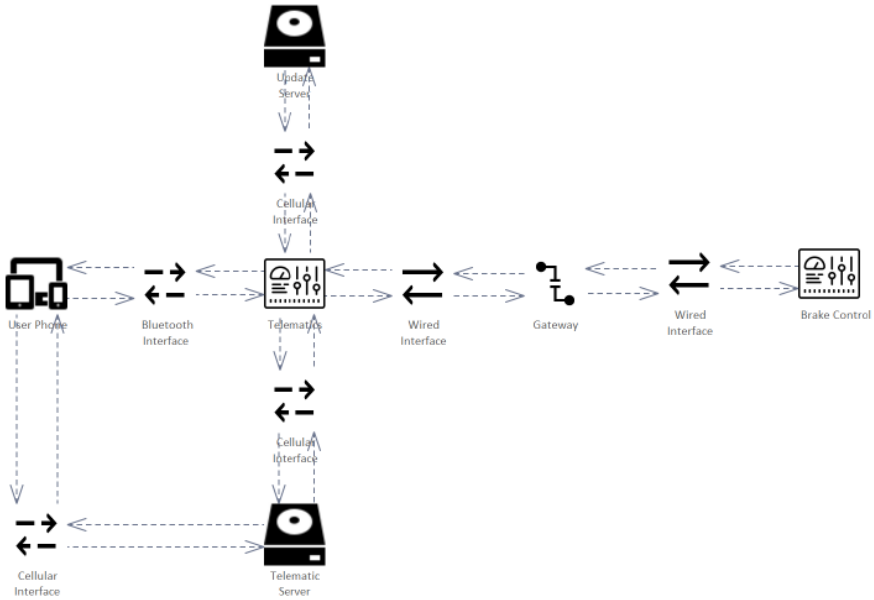
Ebben a munkában továbbá hasonlóan az én megoldásomhoz a STRIDE fenyegetésmodellezési keretrendszer valamint a CIA triád közös használata történik. Szintén érdemes kiemelni a fenyegetésmodellezésre jellemzően használt Data Flow diagram kiegészített formáját amelyet Extended Data Flow diagramnak neveznek. Ezzel egy részről kompozíciók modellezését teszik lehetővé, másrészről pedig értékek (asset) megjelenítéséről is gondoskodnak. Ez a modell már sokkal alkalmasabb komplex kiber-fizikai rendszerek elemzésére az általános Data Flow diagrammokkal szemben. Ez a diagram a 3.3 ábrán látható.

Ebben a kutatásban hangzik el először az automatizált támadási fa generálásának fogalma, valamint a tanulmány támadási gráfokat is definiál. 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.

Magukról a támadási fákról alkotott modell pedig a 3.4 ábra mutatja be. Ezen nehezen látható, hogy az Extended Data Flow diagramból (ami a 3.3 ábrán látható) lenne származtatva a modell, valamint a végeredmény egy absztrakt megfogalmazású és nem kifejezetten az egyes komponensekre irányuló támadásokat jelenít meg a támadás lépése-

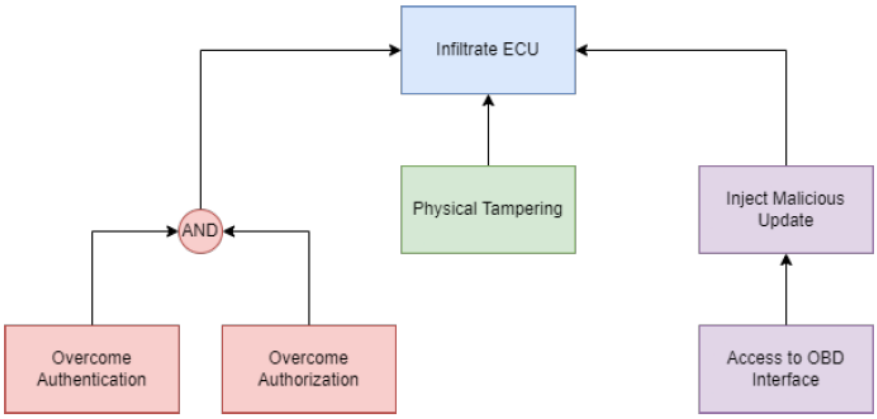


3.2. ábra. Fenyegetésmodellezés folyamata a tervezési fázisban[9]



3.3. ábra. Extended Data Flow diagram grafikus megjelenítése[9]

iként. Szintén a dependenciák is kevésbé használják ki a logikai kapuk nyújtotta felépítés lehetőségeit.



3.4. ábra. Támadási fák grafikus megjelenítése[9]

3.3. Támadási fa generálás

Sowka et al.[8] *"A review on automatic generation of attack trees and its application to automative cybersecurity"* című publikációja különböző alkalmazásait értékelte az automatikus támadási fáknak az autóipari kiberbiztonság doménjében.

Az írás ad egy általános áttekintést a terület fontosságáról, a szabályozási környezet aktuális helyzetéről majd összehasonlította a különböző elérhető megoldásokat az adott problémára.

A Salfer et al.[6] *"Efficient attack forest construction for automative on-board networks"* című munkája által bemutatott módszer egy magas fokú modellezett megoldás alapján való támadási utak előállítását határozza meg.

Kifejezetten érdekes, ahogy felépíti a metamodelljét amiben definiál egy rendszer és egy támadó modellt 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] *"Cyber-security of connected vehicles: contributions to chance the risk analysis and security of in-vehicle communications"* 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 belépés szükségét, viszont kevesebb feltevést használ a támadások meghatározásánál.

Végül pedig Bryans et al.[2] *"A template-based method for the generation of attack trees"* 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.[9] 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.

4. fejezet

A kiberbiztonsági analízis metodológiája

A diplomamunkám legfontosabb része a metodológia előállítása volt. A metodológia az ami biztosítja azoknak a céloknak az elérését, hogy az analízis (i) teljes körű legyen, (ii) megismételhető legyen és (iii) már létező információkra építsen, azon túl, hogy az eredménye és használata minél átláthatóbb legyen a stakeholderek és az elemző mérnök számára is.

Ez a metodológia kapcsolja össze az autóiparra jellemző rendszermodelleket a fenyegetésmodellekkel. Ennek segítségére és támogatására készült el a kapcsolódó modellező eszköz és ennek az eredménye az egyik legfontosabb előállított értéke a kiberbiztonsági mérnök feladatkörnek.

Az említett fejezetben a példáimat egy tetszőleges személygépjármű kormányrendszerének az aktuációs (actuation: mozgásba hoz működtet) funkcionalitására készítettem el.

Az *Áttekintés* fejezet tartalmaz egy magas szintű végigvezetést a bemenetektől a kimenetig és a közte megtett lépésekről.

A *Termékleírás és fenyegetésmodell származtatása* mutatja be a kiindulómodell elkészítésének lépéseit valamint, hogy abból, hogyan állítjuk elő a fenyegetés modellt.

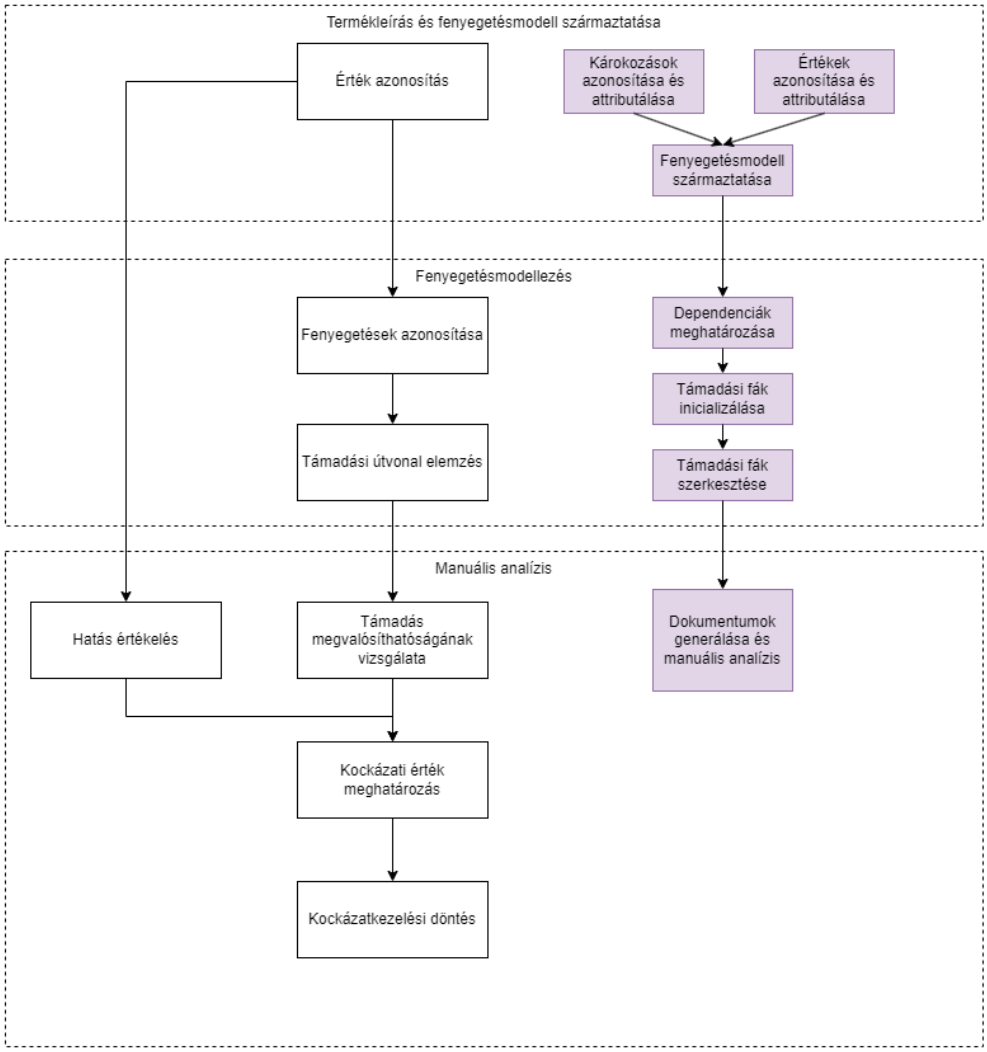
A *Fenyegetésmodellezés* fejezetben láthatóak a további lépések a fenyegetésmodell specifikálására, valamint be mutatja a fenyegetésmodellből előállított támadási fák konstrukcióját és annak szerkesztésének lépéseit.

A *Dokumentumok generálása és manuális analízis* fejezetben pedig találhatóak a szabvány által előírt output előállítása és az elemző eszköz használatát követő folyamatok.

4.1. Áttekintés

A metodológiám fő feladata a *Háttérismeretek* fejezetben található *Követelmények a fenyegetéselemzésre és kockázatértékelésre* részben leírtakat követve kialakítsam azt a lépéssorozatot amelyet az általam fejlesztett eszköz támogatásával végre lehet hajtani és el lehet jutni egy általános autóipari modellből a kockázatelemzés eredményéig.

A lépésekről egy áttekintés a 4.1 ábrán látható. Itt egyrészről a fehér hátterű négyzetekben az ISO 21434 által definiált lépések láthatóak amelyek bővebb leírása a *Háttérismeretek* részben található, lila hátterű négyzetekben pedig az ebben a fejezetben bemutatott lépések láthatóak. Így látható egy egyszerűbb áttekintés a két módszertan közti fedettségről.



4.1. ábra. Metodológia áttekintése

4.2. Termékleírás és fenyegetésmodell származtatása

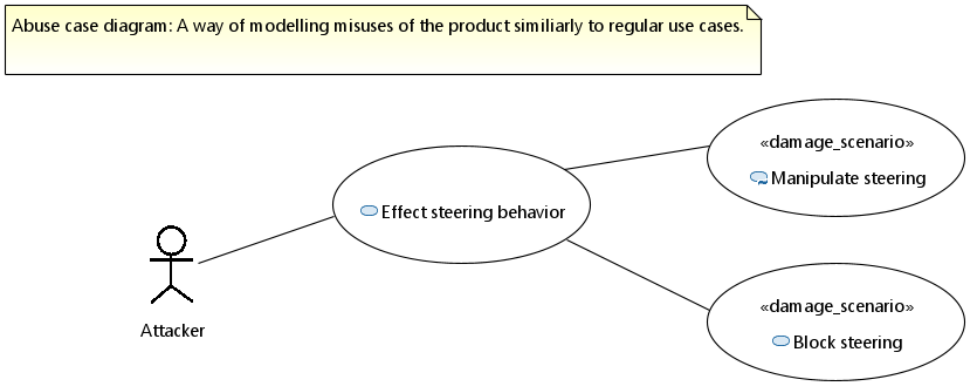
Ez a fejezet mutatja be az első lépéseit a kockázatelemzési folyamatnak. Itt lesz szükségünk a kiinduláskor rendelkezésünkre álló termékleírást (ami a rendszermodell egy részhalmaza) bővíteni kiberbiztonsági attribútumokkal majd abból származtatni egy olyan új modellt ami a kiberbiztonsági elemzésre alkalmas lesz.

Ehhez a rendszermodellünkben két diagram típusra lesz szükség. Az egyik a viselkedési diagramok közé sorolható használati eset (use case) diagram, a másik pedig egy strukturális kategóriába sorolható komponens diagram.

4.2.1. Károkozások azonosítása és attribútálása

A használati eset diagramot a továbbiakban nevezzük *kihasználási eset (abuse case)* diagramnak. Ez annyiban módosítja az eredeti diagram használatát, hogy amíg a szintaktikailag és szemantikailag ugyanaz, tartalmilag nem a felhasználó és rendszer közti kapcsolatokat keressük, hanem a támadó lehetséges motivációját és amit ténylegesen meg is tud tenni a rendszerrel.

A kihasználási esetek azonosításában már tudjuk használni a CIA triád alkalmazását is. A bemutatott eljárásban, veszünk egy funkcionalitást amit a vizsgált termék ellát és azt finomítjuk tovább az egyes kiberbiztonsági tulajdonságoknak a sérülése szerint. Egy példa a 4.2 ábrán látható.



4.2. ábra. Példa kihasználási eset diagramra

A példán jól látható, hogy amíg az "Effect steering behavior" tekinthető is lenne elvárt működésnek egy kormányrendszer esetén, addig amikor ez egy támadó lehetséges céljai közé tartozik akkor már nevezhető ez egy kihasználási esetnek. Ezt tudjuk tovább finomítani aszerint, hogy mely kiberbiztonsági tulajdonság sérülhet. Az eljárásban használt tulajdonságok a bizalmasság, sértetlenség és elérhetőség, ezek bővebben a *Háttérismeretek* fejezetben kerültek bemutatásra. A "Manipulate steering" esetében az aktuáció sértetlenségi attribútuma sérül, a "Block steering" esetén pedig az elérhetősége. Bizalmassági tulajdonsága nincsen az aktuációnak, hiszen ennek a működtetése kívülről nem igényel semmilyen személyes adatot, szellemi terméket vagy kriptográfiai információt.

Az ISO 21434 szerint mivel ez a kihasználási eset (i) összeköt egy funkcionalitást egy nem kívánt következménnyel, valamint ezáltal (ii) értékekhez lesz köthető, emiatt jelölhetjük ezt egy *károkozásnak* (damage scenario).

4.2.2. Értékek azonosítása és attributálása

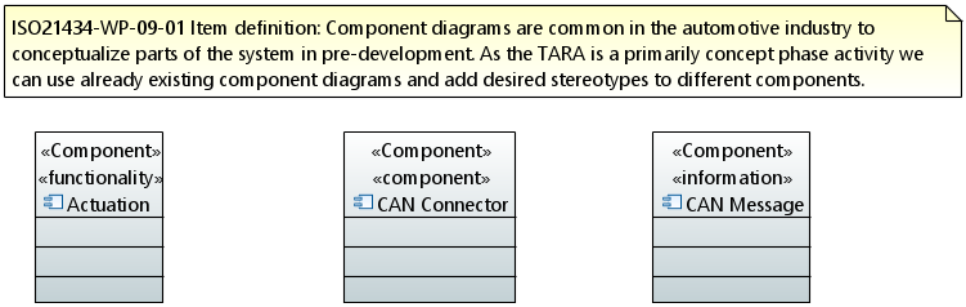
A komponens diagram lesz, az ISO 21434 megnevezése szerint, a termékleírás (item definition). Ennek célja, hogy meghatározzuk a (i) termék határait, (ii) a termék funkcionalitását, illetve a (iii) kezdeti architektúrát.

A termék határai, vagy kiberbiztonsági fogalommal támadási felületet (attack surface), a felvett HW komponensek formájában vagy a beérkező üzenetek (információk) formájában értékként vehetjük fel, a funkcionalitással egyetemben. Az előbbi kettő szintén analizálhatóak a kiberbiztonsági tulajdonságaik alapján (pl: bizalmas információt szállít-e egy CAN üzenet), a funkcionalitásnál erre nincsen szükség hiszen a károkozásokból származtatható lesz egy funkcionalitás védendő tulajdonsága.

A kezdeti architektúra abban az értelemben van figyelembe véve, hogy a termékleírás maga egy komplexebb rendszermodell esetre is alkalmazható, ahol a rendszermodell egyes komponenseit jelöljük fel az előbbi három sztereotípia egyikével.

Erre példa a 4.3 ábrán látható.

A termékleírásban látható, hogy az Actuation mint funkcionalitás jelenik meg, a CAN csatlakozó mint HW komponens, a buszon szállított és a csatlakozón beérkező CAN üzenetek pedig mint információ.



4.3. ábra. Példa termékleírásra

4.2.3. Fenyegetésmodell származtatása

Ebből a két diagram típusból, ami bármely autóipari termék rendszermodelljéhez könnyen integrálható, most már tudunk származtatni olyan modellt amely a fenyegetésmodellezési eljárásunkhoz szükséges. Ehhez nincsen másra szükségünk mint, hogy készítsünk egy kivonatot az elébb feljelölt információkból, amelyet aztán a fenyegetésmodellező eszközünk fel tud használni bemenetként.

Valamint fontos kiemelni az előző pontokban leírtak végrehajtásával egyben végrehajtottuk az ISO 21434 által leírt *Érték azonosítás* lépését is a kockázatelemzésnek.

4.3. Fenyegetésmodellezés

Már az előző fejezetben leírtak is fenyegetésmodellezésnek nevezhető, az még elsősorban a fenyegetésmodell előkészítését és a rendszermodellből való származtatását végezte el.

A következő fejezetben leírtak mutatják be magát a kiberbiztonsági analízisnek a menetét, aminek az eredménye a manuális analízisre alkalmas információk előállítása.

4.3.1. Dependenciák meghatározása

Első lépésként meg kell határoznunk a dependenciákat a károkozások, funkcionalitás és értékek között. Ezt egyszerűen megtehetjük, először a károkozásokat rendeljük hozzá egy-egy funkcionalitáshoz, majd pedig a funkcionalitásokhoz hozzárendeljük, hogy mely szoftveres információktól és mely hardver komponensektől függ.

Ennek a modellje a 4.4 ábrán látható.

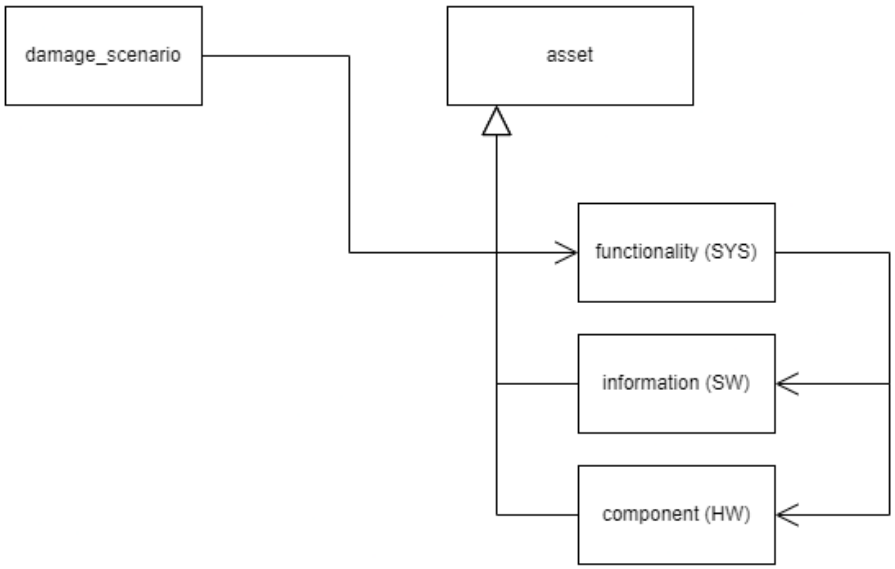
A korábbi példa esetében a két károkozásunk ("Manipulate steering", illetve "Block steering") az Actuation funkcionalitásnak a kártékony használatáról szólnak, ezzel már felvehető kapcsolat van a Károkozás és Funkcionalitás közt.

Ezután határozhatjuk meg a további dependenciákat, a funkcionalitás eléréséhez szükséges egyrészről egy CAN csatlakozóhoz való hozzáférés (ez történhet a CAN buszon keresztül más ECU-n keresztül, vagy állóhelyzetben, olyan kialakítás mellett akár egy saját eszköz csatlakoztatásával).

Másrészről pedig az aktuáció az alapján fog történni, hogy a kormányrendszer milyen üzeneteket kap a CAN buszról. Ilyen befolyásoló tényező lehet a jármű sebessége például.

4.3.2. Támadási fák inicializálása

A definiált következő lépése a szabványos kockázatelemzésnek a *Fenyegetések azonosítása* és a *Támadási útvonal elemzés*.



4.4. ábra. Károkozások, funkcionalitás és értékek összerendelése

Az előbbi elvégzésére a STRIDE keretrendszert fogom alkalmazni, amely az egyes fenyegetés típusokat rendeli a kiberbiztonsági tulajdonságokhoz, a keretrendszer bemutatása a *Háttérismeretek* fejezetben található.

Az utóbbinak pedig ezzel együtt el tudjuk végezni az előkészítését, ahol a generált fenyegetéseket a meghatározott dependenciák szerint rendezzük.

4.3.3. Támadási fák szerkesztése

A támadási fák olyan irányított aciklikus gráfok amelyekben minden páratlan szinten egy fenyegetés vagy pszeudo-fenyegetés található, minden páros szintjén pedig egy logikai kapu amely lehet *ÉS* vagy *VAGY* típusú. A gyökér fenyegetést nevezhetjük rendszerszintű fenyegetésnek, a levélben lévőeket pedig szoftver- vagy hardverszintű fenyegetésnek. Ezek közé pszeudo-fenyegetéseket helyezhetünk el, ezzel csoportosítva a szoftver- vagy hardverszintű fenyegetéseket.

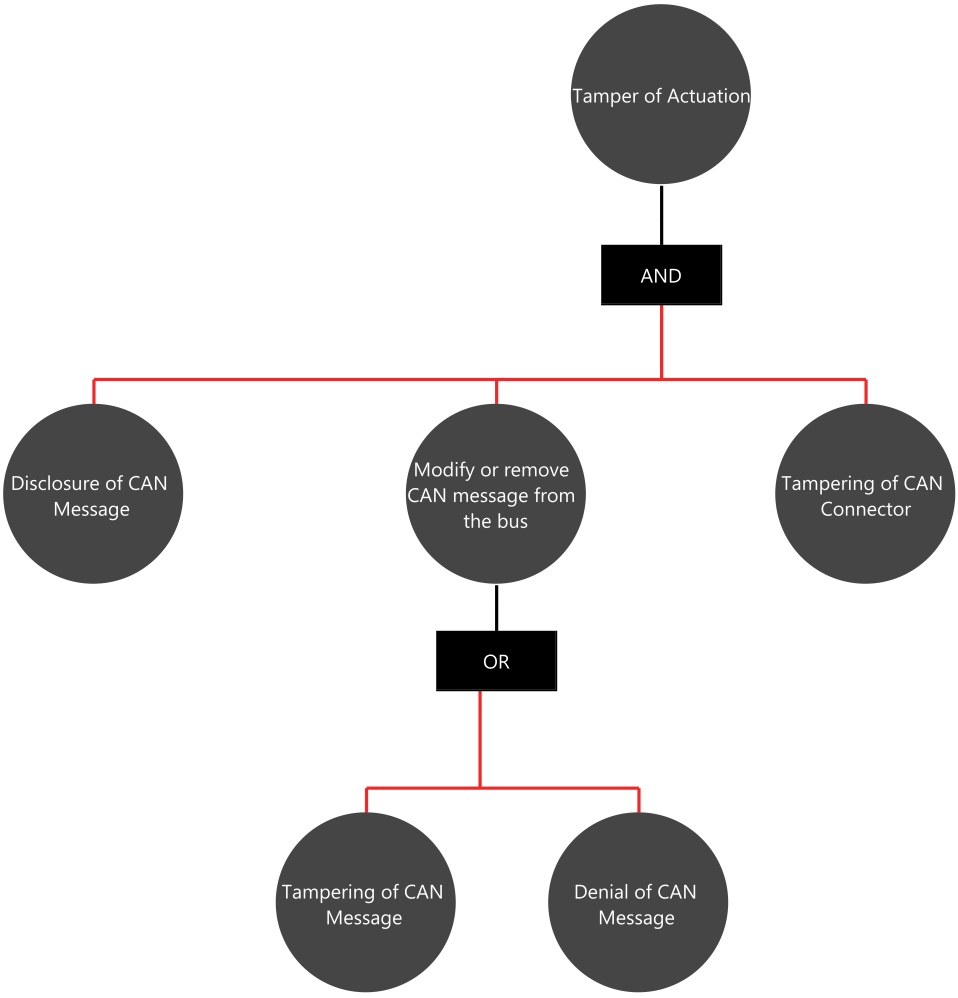
További korlátozás a gráffal szemben, hogy minden fenyegetésnek 0 vagy egy kapuja lehet mint gyermek elem, illetve egy kapunak 1 vagy több gyermek fenyegetése lehet. A fenyegetés felfele nulla vagy egy kapuhoz csatlakozhat (ez már következik a gráf aciklikusságából), a kapunak felfele pedig pontosan egy fenyegetése kell, hogy legyen. Ebből következik, hogy egy fenyegetés gyökérnek számít, ha nincs felette kapu, pszeudónak ha felette és alatta is van kapu, levélnek pedig, ha nincs alatta kapu.

Ezeknek a fáknak a konstrukcióját úgy végezzük el, hogy minden károkozáshoz egy támadási fát rendelünk, annak a gyökér eleme a hozzá rendelt funkcionalitás valamint a károkozásban sérült tulajdonság alapján meghatározott fenyegetés. A levél elemeket szintén a funkcionalitáshoz rendelt értékekből és azok tulajdonságaiból kaphatjuk meg.

Ezután adhatunk hozzá a fához kapukat és határozhatjuk meg az összefüggéseket a szoftver- és hardverszintű fenyegetések valamint a rendszerszintű fenyegetés között.

Egy példa erre a fejlesztett elemző eszközben a 4.5 ábrán láthatunk.

Itt látható, hogy a támadási végrehajtásához szükséges egyrésről a CAN üzenet tartalmának megismerése, ez alapján tud a támadó saját üzeneteket konstruálni, megtalálni a címezhető ECU-kat, stb.



4.5. ábra. Példa a támadási fára a "Manipulate steering" károkozáshoz

Másrészről szükséges a CAN csatlakozó ellen a Tampering, ami a sértetlenség tulajdonság sértése. Erre példa, hogy amennyiben módosítani akarjuk a kerekek állását, azt befolyásolhatjuk a CAN csatlakozó abban az esetben, ha van hozzáférésünk a CAN buszhoz amire az ECU csatlakoztatva van.

Utolsó sorban pedig a CAN üzenetnek módosíthatjuk a tartalmát vagy annak a továbbítását tudjuk blokkolni bizonyos esetekben, ezek közül bármelyik fenyegetés jelenléte a rendszerünkben okozhatja a rendszerszintű fenyegetés jelenlétét is.

Ennek a támadási fa konstrukciónak az elvégzése minden károkozásra elegendő ahhoz, hogy teljesítsük a *Támadási útvonal elemzés* lépését a szabványosított eljárásnak.

4.4. Dokumentumok generálása és manuális analízis

Jelenleg a fenyegetésmodellünk tartalmaz információt a rendszerre releváns károkozásokról, funkcionalitásról, értékekről, fenyegetésekről valamint a fákból származtatható a támadási útvonalakról.

Ennek a modellnek a segítségével fogunk tudni minden analízist amely pusztán a jellegéből fakadóan manuális analízisre szükséges.

Az egyik ilyen a hatás értékelés, ez a károkozások listázásával előállítható. A másik a támadás megvalósíthatóságnak a vizsgálata, amelyben a támadási útvonalak és támadási lépéseket kell kiértékelnünk a megvalósíthatóságuk szerint.

A támadási útvonal egy minimális halmaza a levéleseményeknek amelyeknek a teljesülése (rendszerben egy időben való jelenléte) vezet a gyökér esemény, vagy rendszerszintű fenyegetés jelenlétéhez. A támadási lépések az egyes levél események lesznek.

Példa a hatásérték analízisre a 4.1 táblázatban látható, a támadási megvalósíthatóság elemzésre pedig a 4.2 táblázatban.

A táblázat oszlopai a határérték analízis esetén az SFOP keretrendszert használják, a támadási megvalósíthatóságnál pedig az Attack Potential Based megközelítést.

Damage Scenario	Safety	Financial	Operational	Privacy	Impact
Manipulate steering					
Block steering					

4.1. táblázat. Generált hatásérték analízis dokumentum

Attack Paths	ET	SE	KoI	WoO	Eq	Attack Feasibility
Attack Path - Manipulate steering						
|-> Tampering of CAN Message						
|-> Tampering of CAN Connector						
|-> Disclosure of CAN Message						
Attack Path - Manipulate steering						
|-> Denial of CAN Message						
|-> Tampering of CAN Connector						
|-> Disclosure of CAN Message						

4.2. táblázat. Generált támadás megvalósíthatósági elemzés dokumentum

Ezek a táblázatok már alkalmasak a megfelelő szakértők bevonásával az elemzés elvégzésére. Ezen eredményéből már meghatározható a kockázati érték és a kockázatkezelési döntés a stakeholder-ek által.

5. fejezet

A kiberbiztonsági analízis megvalósítása

A következő fejezetnek a célja, hogy bemutassa az előző fejezetek által körülírt metodológia végrehajtását segítő fenyegetésmodellező eszközt, valamint a rendszermodellek származtatására készített szkriptet.

Az első alfejezetben látható egy áttekintés majd két fő részre osztva láthatóak a további alfejezetek. A két fő rész egyike a rendszerből kiberbiztonsági modell transzformálást mutatja be és az ezt segítő eszközöket. A másik pedig az EMF alapon implementált modellező eszközt amely a kiberbiztonsági modell alapján képes a manuális analízist támogatni dokumentumok generálásával valamint a támadási fák szerkesztésével.

5.1. Áttekintés

Egy áttekintése az elemző eszköz részeinek megtekinthető a 4.1 ábrán.

Itt először kiemelném a fenyegetésmodell és a rendszermodell közös halmazában lévő tartalmakat. Ez a rendszermodell egy Papyrus projekt formájában készült el. Tartalmazza a *Kihasználási eset diagramot* és a *Termékleírást*. Ezek tartalmazzák az értékeket, funkcionalitást és a lehetséges károkozásokat, amelyekből két dokumentum állítható majd elő, amelyek három ISO 21434 workproduct-ot fednek.

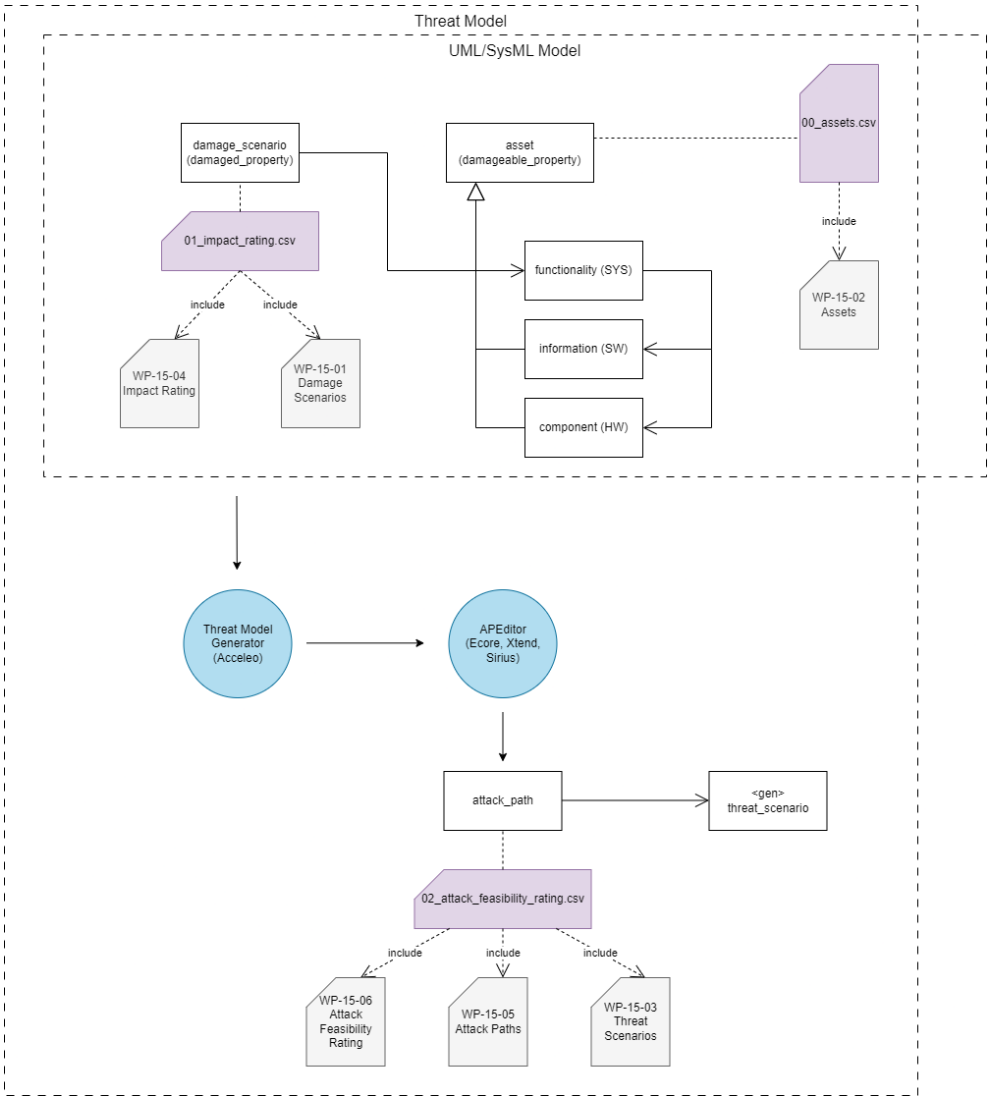
A következő elem a Threat Model Generator ami egy Acceleo script a Papyrus modellező eszközhöz integrálva és a cybersecurity profil alapján állít elő egy kezdeti modell fájlt amelyet a fenyegetésmodellező eszközzel fogunk tudni megnyitni.

A fenyegetésmodellező eszköz az APEditor (Attack Path Editor) amelyben lehetőségünk van a termékleírás és kihasználási diagram tartalmai közti dependenciák meghatározására, valamint támadási fák és fenyegetések automatikus származtatására.

A támadási fák elkészítése után fogjuk tudni a modellből származtatni a támadás megvalósíthatóság értékelés dokumentumot ami további három ISO 21434 workproductot fed le.

5.2. Kiberbiztonsági modell származtatása

A kiberbiztonsági modell származtatása egy fontos lépése a kockázatelemzési folyamatnak. Előkészíti a fenyegetésmodellünket illetve teremt egyfajta nyomon követhetőséget a rendszermodell és a kiberbiztonsági modell között.

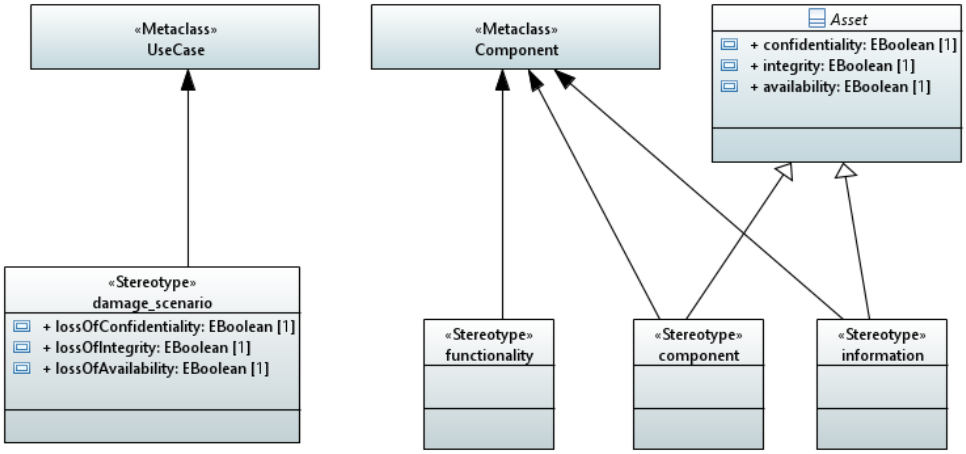


5.1. ábra. Megvalósítás áttekintése

5.2.1. Kiberbiztonsági profil

A profilban négy sztereotípia került meghatározásra. Egyrészről a UseCase UML metaosztályát bővíti a damage_scenario sztereotípia amellyel a károkozásokat tudjuk jelölni. A károkozásokhoz fel lett véve attribútumként, hogy azt mely kiberbiztonsági tulajdonság sérülése okozta.

A Component UML metaosztályt bővíti a functionality, component illetve az information sztereotípia. Itt a functionality jelenti a rendszerszintű funkcionalitást, ennek nincsenek az UML profilban attribútumai mivel azokat majd a kapcsolódó károkozások alapján fogjuk tudni meghatározni az elemzés későbbi fázisában. A component jelzi a HW komponenseket (pl. csatlakozó, modulok, áramkörök), az information pedig a SW szintű információkat (pl. szoftver, kriptográfiai adatok, üzenetek). Az utóbbi kettő az Asset (*érték*) absztrakt osztályból van származtatva, ebből öröklik a kiberbiztonsági tulajdonságaikat.

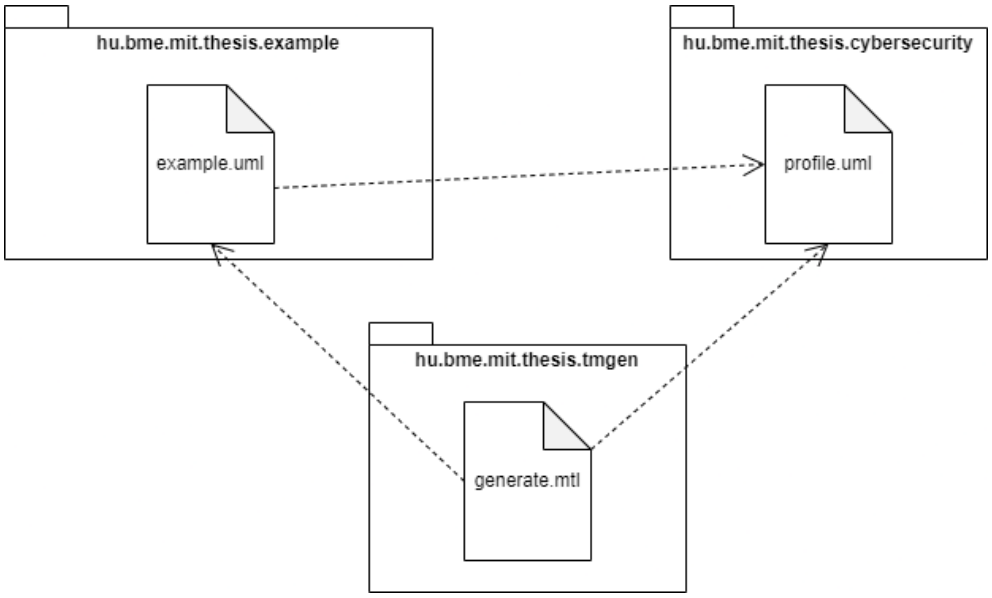


5.2. ábra. Kiberbiztonsági profil (UML)

5.2.2. Fenyegetésmodell generátor

A fenyegetésmodell generátor egy Acceleo nyelven írt szkript, amelynek a feladata a Papyrus-ban szerkesztett .uml fájloknak a beolvasása és a tartalmuk alapján egy .apeditor fájlnak a generálása, amelyet a fenyegetésmodellező eszközben lehet tovább szerkeszteni.

A projekt felépítése és a dependenciák a 5.3 ábrán láthatóak.



5.3. ábra. Threat Model Generator dependenciái

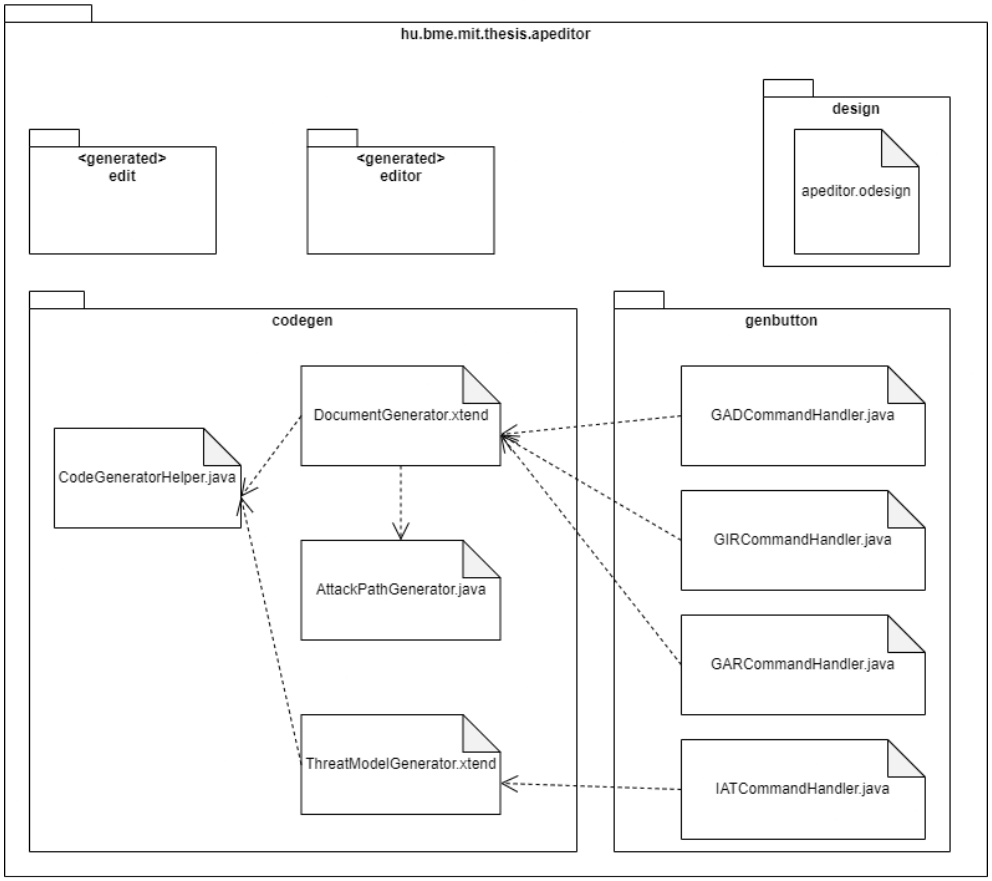
A **hu.bme.mit.thesis.example** projekt tartalmazza a kihasználási eset diagramot és a termékleírást, valamint applikálja a **hu.bme.mit.thesis.cybersecurity** projektben definiált kiberbiztonsági profil sztereotípiáit.

A **hu.bme.mit.thesis.tmgen** tartalmazza a **generate.mtl** fájlt ami egy Acceleo nyelven írt Model-To-Text generátor. Ez fogja előállítani a projekt *generated* mappájába az **example.apeditor** fájlt, amelyet át lehet majd másolni a fenyegetésmodellező eszköz *runtime* környezetében létrehozott projektekbe.

5.3. Fenyegetésmodellező eszköz

A fenyegetésmodellező eszköz teszi lehetővé a károkozások, funkcionalitások és értékek közti dependencia beállítását, a támadási fák szerkesztését, illetve a szabványos dokumentumok generálását.

Ennek a projektnek az áttekintése a 5.4 ábrán látható.



5.4. ábra. APEditor projekt felépítése és dependenciái

A **hu.bme.mit.thesis.apeditor** projektben található az *apeditor.ecore* fájl ami a metamodellt tartalmazza, illetve az Eclipse Modelling Framework által generált fájlokat.

A **hu.bme.mit.thesis.apeditor.edit** illetve a **hu.bme.mit.thesis.apeditor.editor** projektek szintén az EMF által lettek generálva, ezek adják meg a modell szerkesztő felületének az alapjait.

A **hu.bme.mit.thesis.apeditor.design** tartalmaz egy Sirius keretrendszert használó *apeditor.odesign* fájlt amely a támadási fáknak a grafikus megjelenítését és szerkesztő felületét írja le.

A **hu.bme.mit.thesis.apeditor.genbutton** tartalmazza a plugin.xml-t amelyben az APEditor felhasználói felületén megjelenítendő gombok vannak leírva, valamint a gombok megnyomásával futtatott .java fájl is itt kerül összelinkelésre. A négy .java fájl a különböző funkcionalitását definiálják.

- **GADCommandHandler.java** Asset Definition workproduct generálását viszi végbe a **hu.bme.mit.thesis.apeditor.codegen** projektben definiált funkcionalitás aktiválásával

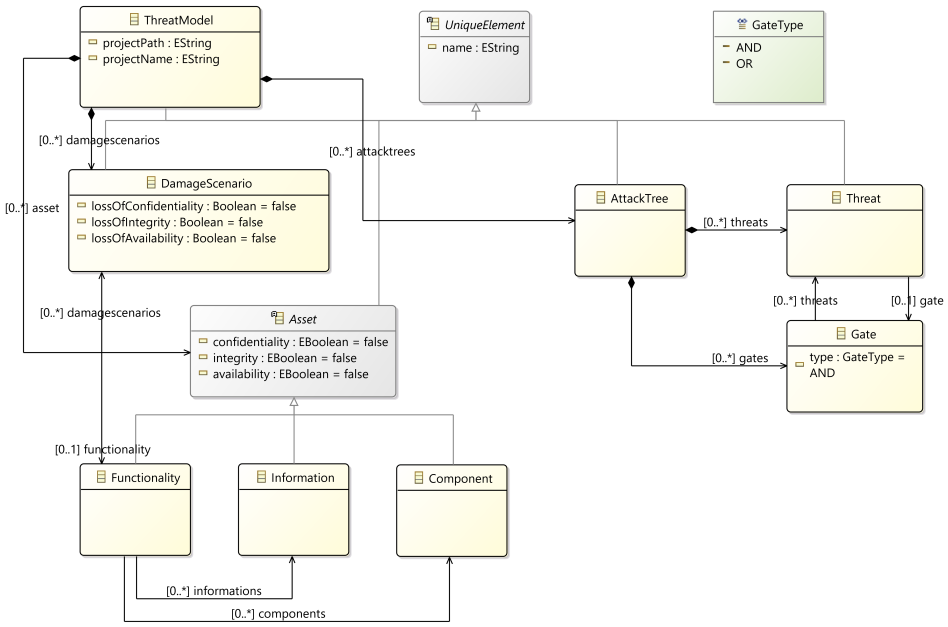
- **GIRCommandHandler.java** Impact Rating workproduct generálását viszi véghez a **hu.bme.mit.thesis.apeditor.codegen** projektben definiált funkcionalitás aktiválásával
- **GARCommandHandler.java** Attack Feasibility Rating workproduct generálását viszi véghez a **hu.bme.mit.thesis.apeditor.codegen** projektben definiált funkcionalitás aktiválásával
- **IATCommandHandler.java** Inicializálja a támadási fákat az **hu.bme.mit.thesis.apeditor.codegen** projektben definiált funkcionalitás aktiválásával

Végül az **hu.bme.mit.thesis.apeditor.codegen** tartalmazza a kódgeneráláshoz szükséges osztályokat és függvényeket. Itt egyrészről a *DocumentGenerator.xtend* fájl tartalmazza azokat az Xtend-ben megírt függvényeket, amelyek a szabványos workproduct-ok előállításához szükségesek, másrészről az Attack Feasibility Rating generálásakor, használja az *AttackPathGenerator.java* függvényeit amelyek a támadási fákat fejti ki támadási útvonalakká amelyek támadási lépésekből állnak.

Az *ThreatModelGenerator.xtend* a modellből generálja le a támadási fák kezdeti állapotát és aztán azokat írja bele a modellfájlba. Ezzel bővítve a szerkesztett modellt.

Mindkét Xtend fájl a *CodeGeneratorHelper.java* fájlt használja még a fájlba író és fájlt olvasó műveletek elvégzésére.

5.3.1. Metamodel



5.5. ábra. apeditor.ecore fájlban definiált metamodell

5.3.2. Fenyegetésmodell szerkesztő felület

5.3.3. Támadási fák inicializálása

5.3.4. Támadási fa szerkesztő felület

5.3.5. Dokumentum generátor

6. fejezet

Esettanulmány

7. fejezet

Összegzés

Irodalomjegyzék

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

[2] Nguyen H. N. Sabaliauskaite G. Shaikh S. Zhou F. Bryans J., Liew L. S.: A template-based method for the generation of attack trees, 2020.

[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] Claudia Eckert Martin Salfer, Hendrik Schweppe: Efficient attack forest construction for automotive on-board networks, 2014.

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

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

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

[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.