Vysoká škola logistiky o.p.s.

Návrh rámce penetračního testování v oblasti robustnosti kybernetické ochrany autonomního systému vozidla

(Diplomová práce)

Přerov 2021 Bc. Marek Obršál, DiS.

Vysoká škola logistiky o.p.s.

Zadání diplomové práce

student	**Bc. Marek Obršál, DiS.**
studijní program	Logistika
obor	Logistika

Vedoucí Katedry magisterského studia Vám ve smyslu čl. 22 Studijního a zkušebního řádu Vysoké školy logistiky o.p.s. pro studium v navazujícím magisterském studijním programu určuje tuto diplomovou práci:

Název tématu: **Návrh rámce penetračního testování robustnosti kybernetické ochrany autonomního systému vozidla**

Cíl práce:

Zpracovat návrh rámce penetračního testování kybernetické bezpečnosti autonomního systému vozidel. Návrh zpracovat v souladu s relevantními bezpečnostními normami a pokyny souvisejícími s kybernetickou bezpečností.

Zásady pro vypracování:

Využijte teoretických východisek oboru logistika. Čerpejte z literatury doporučené vedoucím práce a při zpracování práce postupujte v souladu s pokyny VŠLG a doporučeními vedoucího práce. Části práce využívající neveřejné informace uveďte v samostatné příloze.

Diplomovou práci zpracujte v těchto bodech:

Úvod
1. Literární rešerše tématu testování kybernetické bezpečnosti autonomního systému vozidel (ASV)
2. Bezpečnostní normy spojené s kybernetickou bezpečností autonomních systémů vozidel
3. Návrh rámce penetračního testování kybernetické bezpečnosti ASV
4. Vyhodnocení návrhu rámce penetračního testování kybernetické bezpečnosti ASV

Závěr

Rozsah práce: 55 – 70 normostran textu

Seznam odborné literatury:

Kybernetická bezpečnost vozidiel [online]. ŠKODA AUTO a.s, 2020 [cit. 2020-11-04]. Dostupné z: https://www.skoda-auto.cz/sluzby/kyberneticka-bezpecnost

Národní ústav pro kybernetickou a informační bezpečnost [online]. Praha, 2020 [cit. 2020-11-04]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/poskytovane-sluzby/

SystemOnLine: Automobilový průmysl [online]. Brno: CCB [cit. 2020-10-10]. Dostupné z: https://www.systemonline.cz/automotive-it-pro-automobilovy-prumysl/

Certifikace kybernetické bezpečnosti vozidel [online]. TÜV NORD, 2020 [cit. 2020-11-04]. Dostupné z: https://www.tuv-nord.com/cz/cs/novinky/news-detail/article/nova-povinnost-certifikace-kyberneticke-bezpecnosti-a-bezpecnosti-aktualizace-softwaru-silnicnich-vozu-jako-podminka-homologace/

Vedoucí diplomové práce: prof. Mgr. Roman Jašek, Ph.D.

Datum zadání diplomové práce: 30. 10. 2020
Datum odevzdání diplomové práce: 13. 5. 2021

Přerov 30. 10. 2020

Ing. Blanka Kalupová, Ph.D.
vedoucí katedry

prof. Ing. Václav Cempírek, Ph.D.
rektor

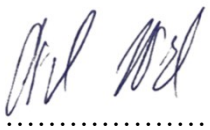
Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a že jsem ji vypracoval samostatně. Prohlašuji, že citace použitých pramenů je úplná a že jsem v práci neporušil autorská práva ve smyslu zákona č. 121/2000 Sb., o autorském právu, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

Prohlašuji, že jsem byl také seznámen s tím, že se na mou diplomovou práci plně vztahuje zákon č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména § 60 – školní dílo. Beru na vědomí, že Vysoká škola logistiky o.p.s. nezasahuje do mých autorských práv užitím mé diplomové práce pro pedagogické, vědecké a prezentační účely školy. Užiji-li svou diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat předtím o této skutečnosti prorektora pro vzdělávání Vysoké školy logistiky o.p.s.

Prohlašuji, že jsem byl poučen o tom, že diplomová práce je veřejná ve smyslu zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, zejména § 47b. Taktéž dávám souhlas Vysoké škole logistiky o.p.s. ke zpřístupnění mnou zpracované diplomové práce v její tištěné i elektronické verzi. Souhlasím s případným použitím této práce Vysokou školou logistiky o.p.s. pro pedagogické, vědecké a prezentační účely.

Prohlašuji, že odevzdaná tištěná verze diplomové práce, elektronická verze na odevzdaném optickém médiu a verze nahraná do informačního systému jsou totožné.

V Přerově, dne 13. 5. 2021 

…….

podpis

Poděkování

Rád bych poděkoval vedoucímu diplomové práce prof. Mgr. Romanu Jaškovi, Ph.D., za odbornou přípravu a metodologickou pomoc při zpracování mé práce. Dále bych chtěl poděkovat panu Ing. Karlu Jánskému a panu Ing. Jakubu Dvořákovi Ph.D., za všestrannou pomoc, množství cenných a inspirativních rad, podnětů, doporučení, připomínek a zároveň za velkou trpělivost s obdivuhodnou ochotou při konzultacích poskytnutých ke zpracování této práce.

Dále bych poděkoval rodině, za trpělivost, kterou se mnou měly a za velkou podporu.

Anotace

Cílem práce je návrh rámce penetračního testování kybernetické bezpečnosti autonomního systému vozidel. Návrh bude v souladu s relevantními bezpečnostními normami a pokyny souvisejícími s kybernetickou bezpečností (např. norma ISO/SAE 21434 o inženýringu kybernetické bezpečnosti pro silniční vozidla, SAE J3061 a ISO 24089 pro softwarové aktualizace).

Annotation

The aim of the work is to design a framework for penetration testing of cyber security of an autonomous vehicle system. The proposal will comply with relevant security standards and guidelines related to cyber security (eg ISO / SAE 21434 on cyber security engineering for road vehicles, SAE J3061 and ISO 24089 for software updates).

Klíčová slova

automotive, kybernetická bezpečnost, ISO, penetrační testy, autonomní vozidlo, EHK

Keywords

Automotive, cyber security, ISO, penetration test, Autonomous vehicle, UN ECE

Obsah

Úvod ... 9
1 Literární rešerše tématu testování kybernetické bezpečnosti ASV ... 12
1.1 Základní procesy vývoje ... 12
1.2 ISO 21434 ... 15
1.3 ISO 24089 ... 17
1.4 SAE J3061 ... 18
1.5 Předpis EHK 155 ... 27
1.6 Kybernetická bezpečnost v dalších oblastech ... 29
1.6.1 IEC62443 ... 29
1.6.2 ISO 27001 ... 29
1.7 Související normy ... 31
1.7.1 ISO 31000 ... 31
1.7.2 ISO 26262 FuSa ... 31
1.7.3 SOTIF ISO / PAS 21448 ... 32
1.7.4 ISO 12207 ... 32
1.7.5 EHK 156 ... 33
1.8 NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost ČR ... 33
2 Návrh rámce penetračního testování kybernetické bezpečnosti ASV ... 35
2.1 ALKS ... 35
2.2 TARA (Threat Analysis and Risk Assessment) ... 37
2.2.1 Potenciál útoku (Po) ... 37
2.2.1 Pravděpodobnost úspěšného útoku (Pr), ... 38
2.2.2 Výpočet potenciálu útoku: ... 38
2.2.3 Útočníci v oblasti automotive: [20] ... 39
2.2.4 Dopad konkrétních hrozeb I ... 44

2.2.5 Dopad útoku (MI) a výpočet ... 47
2.2.6 Tabulka modifikace dopadů na úrovně rizika ... 47
2.3 Rozbor TARA analýzy a možnosti užití penetračních testů. ... 48
2.3.1 Bezdrátová konektivita ... 49
2.3.2 Drátová konektivita ... 50
2.3.3 Kamera ... 51
2.3.4 Radar ... 52
2.3.5 Autorizace ... 52
2.3.6 Komunikace jednotek ... 52
2.3.7 Kryptografické technologie ... 53
2.3.8 Zřejmé útoky ... 53
2.3.9 Náročnější útoky ... 54
2.3.1 Další možnosti ... 54
3 Vyhodnocení návrhu rámce penetračního testování kybernetické bezpečnosti ASV ... 59
Závěr ... 63
Seznam zdrojů ... 64
Seznam grafických objektů ... 67
Seznam zkratek ... 68
Seznam příloh ... 70

Úvod

Kybernetická bezpečnost je jedním z nových pojmů ve všeobecném pojetí moderní doby. Jedná se o ochranu veškerých zařízení v IT oblasti proti vnějším zásahům s cílem poškodit nějakou vlastnost systému. Ochrana je zajišťována jak pro SW tak také pro HW. Hlavním úkolem kybernetické bezpečnosti je ochrana proti neoprávněným manipulacím, zajištění spolehlivosti, robustnosti a komplexnosti celého systému.

Kybernetická bezpečnost je nové odvětví, kterým se musí zabývat veškeré oblasti, a to nejen technického typu, ale i ty, které pracují s daty, nebo s nimi manipulují. Na základě postupného zavádění elektrifikace a automatizace se stále více spoléháme na systémy, které mohou mít své úskalí. Zavádění automatizace a digitalizace sebou nese nezbytnost zavádění informačních systémů. Veškerá odvětví se stávají komplexnějšími a systémově provázanými strukturami. Tento trend však sebou nese nezbytnost ochrany dat.

V současnosti se kybernetická bezpečnost zavádí postupnými procesy do všech odvětví. Veškeré témata týkající se kybernetické bezpečnosti jsou v dnešním světě potřebnou metodikou, jak ochránit citlivá data a zajistit komplexnost a robustnost dat, či komponentů nebo celků. Jednotlivá opatření se přijímají nejen na základech kybernetických útoků, které se odehrály, ale především jako prevence před případnými hrozbami. Samozřejmě se nedají veškeré útoky odhalit, ale i zde se kybernetická bezpečnost orientuje na možnosti pokusů o útok a jejich odhalení i při neúspěšnosti.

Nejprve je třeba vymezit, co je vlastně bezpečnost a co zahrnuje.

Bezpečnost je vlastnost prvku (např. informační systém), který je na určité úrovni chráněn proti ztrátám, nebo také stav ochrany. Bezpečnost informačních technologií zahrnuje ochranu důvěrnosti, integrity a dosažitelnosti při zpracování, úschově, distribuci a prezentaci informací.

Bezpečnost dat je bezpečnost aplikovaná na data. Zahrnuje například řízení přístupů, definování politik a procesů a zajištění integrity dat.

Bezpečnost informací je zachování (ochrana) důvěrnosti, integrity a dostupnosti informací. Bezpečnost informací / informačních systémů je uplatnění obecných bezpečnostních opatření a postupů sloužících:

a) K ochraně informací před jejich ztrátou nebo kompromitací (ztráta důvěrnosti, integrity, a dalších vlastností jako např. autentičnost, odpovědnost, nepopíratelnost a spolehlivost), případně k jejich zjištění a přijetí nápravných opatření.
b) K zachování dostupnosti informací a schopnosti s nimi pracovat v rozsahu přidělených oprávnění. Opatření INFOSEC zahrnují bezpečnost počítačů, přenosu, emisí a šifrovací bezpečnost a odhalování ohrožení skutečností a systémů a jeho předcházení. [1] Projekt INFOSEC se zabývá provedením průzkumu a analýz mezinárodních a národních norem v oblasti bezpečnosti informačních a komunikačních technologií a resortní legislativy z oblasti bezpečnosti informací. Dále tento projekt slouží za pomoci mezinárodních norem k zavádění ISMS zejména v rezortu Ministerstva obrany.

V současnosti jsou na vzestupu veškeré autonomní systémy, a to zejména v automotive odvětví. Vozidla s chytrými funkcemi, či dokonce s autonomními funkcemi se stávají čím dál více obětmi kybernetických útoků. V možnostech umožňující kybernetické útoky jsou vozidla ideálním terčem, jelikož se zavádí různé druhy komunikace, a to nejen ve vozidlech jako takových, ale zároveň vozidla mohou komunikovat mezi sebou a také s infrastrukturou. Dále zavádění vysokorychlostních připojení pro přenosy velkých objemů dat. Řeší se elektromobilita, kde je snaha o bezdrátové připojení a monitoringy. Zde všude bývají motivace k pokusům o útoky.

Autonomní vozidla jsou ideálním adeptem na implementaci umělé inteligence, jelikož zde je veliký investiční potenciál. Toto je také jeden z hlavních důvodů, proč se vozidla budou stávat častými obětmi kybernetických útoků.

Útok je pokus o neoprávněný vstup, manipulaci či jiný způsob vniknutí. Tyto útoky mají většinou své motivace pro pokusy o narušení bezpečnosti, nebo získání finančního prospěchu, např. zneužitím dat. SAE J3061 popisuje útok na systémovou kybernetickou bezpečnost, který vychází z inteligentního aktu, tj. Inteligentního aktu, který je záměrným pokusem (zejména ve smyslu metody nebo techniky) vyhnout se službám kybernetické bezpečnosti a porušit politiku kybernetické bezpečnosti systému.

Nejzákladnějšími otázkami u kybernetické bezpečnosti jsou **CO**, **PROČ**, a **JAK**.

Obr. 1 Co? Proč? Jak?

Zdroj: [2].

U otázky CO se představuje, co se má stát obětí kybernetického útoku. Nejčastěji jde o citlivá data, prvky, které nemají dostatečnou ochranu, databáze, atd.

Otázka PROČ má různé motivy útoků ať už se jedná o finanční motivy, tak se může jednat i o zranění či terorismus.

JAK, je otázka jak se může útočník dostat do systému, či kde jsou slabá místa prvků, a kde hrozí bezpečnostní incident.

Veškeré tyto parametry se zodpoví v následujících bodech. Dále se zde bude hovořit výhradně o kybernetické bezpečnosti autonomních vozidel a s tím spojené normy a veškerá opatření a doporučení, pokud nebude řečeno jinak.

Cílem práce je stanovit metodiku, podle které by se dala určit strategie, jak postupovat při schvalování kybernetické bezpečnosti pro autonomní vozidla a metodika pro volbu penetračních testů na jednotlivé parametry.

1 Literární rešerše tématu testování kybernetické bezpečnosti ASV

„Kybernetická bezpečnost vyjadřuje stav vozidel, ve kterém jsou silniční vozidla a jejich funkce chráněny před kybernetickými hrozbami pro elektrické nebo elektronické komponenty.“

Vozidla zpracovávají řadu různých typů dat a dokument definuje principy, které je třeba mít na zřeteli při ochraně informací před neoprávněným přístupem, změnou nebo vymazáním, a to jak při jejich ukládání, tak i při přenosu.

Zde je třeba zdůraznit také bezpečnost provozu „Bez ochrany není možná bezpečnost“. Patří sem ochrana komunikace, mezi které se především řadí V2V, V2I, a další. Zde se jedná o komunikace mezi vozidly a mezi infrastrukturou.

V následující části je třeba se zaměřit na normy, které jsou spojené s kybernetickou bezpečností, a to nejen v oblasti automotive, ale je třeba zmínit i další normy a nástroje související s touto problematikou. Spolu s těmito nástroji jdou ruku v ruce i další normy, které je třeba dodržovat.

Základním parametrem je také nastavení procesů, které se často řídí pomocí různých nástrojů. Výčet těchto nástrojů je zejména spojen s užitím V-modelu a správném nastavení procesů pomocí Best Practice.

Ohledně vývoje cílů kybernetické bezpečnosti je nutné klíčové použití Best Practice, což znamená nejlepší praxi, kde si firmy nechávají radit od odborníků, norem či standardů pro správné a optimální nastavení a metody řízení procesů.

1.1 Základní procesy vývoje

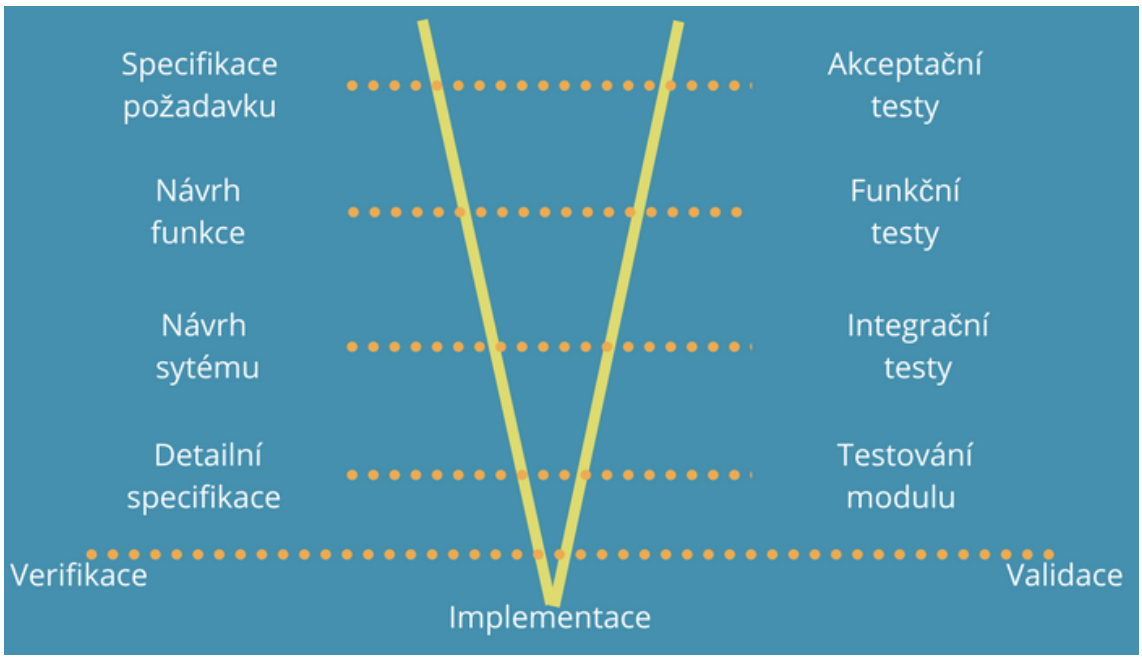
V-model je ideální nástroj, který se zaměřuje na důkladnou kontrolu a testování výrobku, který se již nachází v počátečních etapách návrhu. Testování je prováděno současně s odpovídající etapou vývoje. Vývoj probíhá za správných podmínek, a to zejména Validace a Verifikace.

V- model začíná na levé straně Specifikacemi požadavku, jejich sepsáním a analýzou, pokračuje návrhem funkce a systému a detailním návrhem specifikace. Po těchto krocích

se dosáhne spodní části, která představuje implementaci jednotlivých modulů. Jakmile jsou moduly naprogramovány, proces pokračuje směrem vzhůru a tím vytváří typické písmeno „V“, které nám evokuje vztah mezi fázemi na stejných úrovních.

Pravá strana představuje testovací fáze modulů, integrační testování, funkční testování a akceptační testování. Po úspěšném akceptačním testování se projekt dostává do nekončící fáze provozu a údržby. Písmeno „V“ v názvu modelu představuje a připomíná opakovaně prováděné úkony verifikace a validace. Verifikace a validace zaujímá místo v každé fázi vývoje, kde se ověřují výstupy z každé fáze a snaží se tak zabránit, aby chyby procházely dále ve směru práce na projektu. Při verifikaci se kladou otázky: „ Je systém vytvořen správně? Tak, jak byl předem specifikován?“ Kontroluje se, zda systém odpovídá své specifikaci.

Při validaci se ověřuje, že to, co bylo vytvořeno, je skutečně to, co je požadováno [3].



Obr. 1.2 V-model

Zdroj: [4].

Validace ověřuje, zda produkt odpovídá předpokladům správnosti údajů a prověřování platnosti dokumentů při zadávání dat tak, aby zde nedocházelo k chybným zadáváním dat.

Verifikace je přezkoušení pravosti, potvrzení správnosti, ověřování a potvrzování pravdivosti dat proti zadání. U práce, kde jsou moduly vyvíjeny pomocí V-modelu, jsou

určeny různé metody a pojmy, které se implementují při práci na projektu pro optimalizaci a zvýšení úrovně pro výsledný produkt.

Související pojmy a metody:

- Benchmarking – Jedná se o porovnávání vybraných parametrů vůči referencím. Tuto strategii lze aplikovat na jakoukoli úroveň řízení.
- CAF - Základem tohoto pojmu je sebehodnocení, které pomáhá odhalit silná místa a přehled aktivit ke zlepšení výkonnosti
- EFQM Excellence Model – Hodnocení prováděné autorizovanými hodnotiteli
- Framework – Softwarová struktura
- ISO 9001 - Systém managementu kvality
- Model zralosti CMM – Hodnocení zralosti procesů v 6 stupních.

0 - Neexistující řízení: Neexistuje řízení procesů

1 - Počáteční (Initial): Realizace procesů adhoc (za určitým účelem)

2 - Opakované (Repeatable): Provádění základních opakovaných procesů

3 - Definovaná (Defined): Dokumentace procesů organizace

4 - Řízená (Managed): Procesy jsou řízeny a provádí se měření jejich výkonnosti pomocí ukazatelů výkonnosti

5 - Optimalizovaná (Optimized): Procesy trvale zlepšovány, zavedení inovačního cyklu na procesech a řízení. [5]

- Six Sigma – Průběžné zlepšování, orientace na potřeby zákazníků
- Standardy a normy - standardizace, kompatibilita a interoperabilita.

Související oblasti řízení:

- Řízení kvality (Quality Management) – Zlepšování a zefektivňování procesů vedoucí ke snížení nákladů a zvýšení produktivity.
- Řízení organizace (Organizational Management) – Nastavení systému řízení organizace (správa, operativní řízení, struktura).

V této části budou zmíněny normy, které souvisejí s kybernetickou bezpečností týkajících se především vozidel. Budou zde zmíněny i další normy, které se kybernetickou

bezpečností zabývají. Normy na rozdíl od EHK (řeší schválení) popisují, jak se má vyvíjet, a doporučují sady metod.

1.2 ISO 21434

Tato norma definuje kybernetickou bezpečnost, opatření a procesy v oblasti automotive. Zaměřuje se na celý vývojový proces a definuje terminologii, best practises, vyhodnocení, a mnoho dalšího. Jedná se o nadstavbu quality managementu a definuje se jako návod. Tato norma přebírá hodně z normy SAE J3061, která slouží spíše jako sada pokynů.

Tato norma se stále vyvíjí a předpisy EHK se na ní odvolávají. Aktuálně je využívaná jako hlavní norma.

Norma ISO 21434 obsahuje několik hlavních oblastí a to jsou:

- Celkové řízení kybernetické bezpečnosti

Celkové řízení rizik kybernetické bezpečnosti organizace je implementováno v souladu s ustanovením a platí ve všech jeho fázích. Cílem tohoto ustanovení je definovat politiku kybernetické bezpečnosti s pravidly a procesy, přidělit odpovědnosti a příslušné orgány, které jsou vyžadovány k provádění činností, zajišťování zdrojů a správy, interakce mezi procesy kybernetické bezpečnosti a souvisejícími procesy.

- Management kybernetické bezpečnosti závislý na projektu

V této části se norma zaměřuje na požadavky týkající se řízení činností rozvoje kybernetické bezpečnosti pro konkrétní projekt. Zahrnují se zde body, jako jsou zejména přiřazení odpovědností za kybernetickou bezpečnost, přizpůsobení aktivit, plánování, posouzení.

- Kontinuální činnosti v oblasti kybernetické bezpečnosti

Mohou být prováděny během všech fází životního cyklu a mohou být i mimo konkrétní projekt.

Monitorování vyvíjeného systému / systému / prvku / souboru systémů a komponent, aby se zabránilo známým problémům a řešení nových hrozeb. Může sloužit jako vstup pro činnosti v oblasti správy zranitelností a kybernetické bezpečnosti.

- Metody posouzení rizik

Účelem této kapitoly je popsat metody, které mohou organizace použít k určení rozsahu, v jakém scénář útoku může ovlivnit zúčastněné strany. Pro tento dokument je zúčastněná strana definována jako účastník silničního provozu.

V přístupu shora dolů **(deduktivní)** jsou cesty útoku odvozeny pro prvek/systém nebo pro komponent na základě znalostí o zranitelnostech v podobných systémech a komponentech. Přístup shora dolů je užitečný ve fázích koncepce a vývoje při implementaci aktuální položky nebo komponentu.

V přístupu zdola nahoru **(induktivní)** jsou útočné cesty vytvořeny pro položku nebo komponentu z kybernetické bezpečnosti zjištěná zranitelná místa. Každá akce na cestě útoku je založena na „zneužitelné slabosti“. Přístup zdola nahoru se nejčastěji používá, když je k dispozici implementace položky nebo komponentu, nebo když mají být potvrzeny hypotézy nebo model útoku.

- Vývoj produktu

Tato část popisuje v první části specifikaci kybernetické bezpečnosti a design architektury, který odpovídá levé části V-modelu.

V druhé části popis odpovídá pravé straně V- modelu, což popisuje integrační a ověřovací činnosti.

Další části ISO/SAE DIS 21434 popisují validaci kybernetické bezpečnosti, produkci, operaci a údržbu až po vyřazení z provozu. Jsou zde popsány příklady jednotlivých útoků a jejich hodnocení podle různých kritérií.

Definuje také stupně pro posouzení rizika, jako jsou příležitosti, znalosti komponentu, odbornost, zařízení použité pro útok, a času potřebného pro útok.

- Produkce produktu

Výroba zahrnuje výrobu, montáž a konfiguraci produktu nebo součásti. Plán kontroly výroby je vytvořen s cílem zajistit, aby byly na položku nebo komponentu použity požadavky na kybernetickou bezpečnost pro post-vývoj a aby bylo zajištěno, že položku nebo komponentu nelze během výroby zneužít a nelze přidat další chyby během výroby. Plán řízení výroby lze zahrnout jako součást celkového plánu výroby. Metody mohou zahrnovat ověření, kontrolu, nebo konfigurace a kalibrace.

a) Metody mohou být prováděny na úrovni komponent, aby poskytovaly jistotu a omezovaly testování na integrovaném zařízení.
b) Odebrání produkčního přístupu je nutné, jakmile je položka nebo komponenta vyrobena.
c) Popis ochranných opatření pro součásti zabraňující neoprávněné změně a ochranná opatření mohou zahrnovat fyzický přístup a logický přístup.
d) Fyzické opatření, které brání fyzickému přístupu na produkční servery obsahující software.
e) Logické opatření, které používá kryptografické techniky, a řízení přístupu.

1.3 ISO 24089

Tato norma se zabývá požadavky spojenými se softwarovými aktualizacemi. Norma přiřazuje odpovědnost za procesy vyžadované k bezpečné aktualizaci softwaru a poskytuje základní požadavky na správné provádění těchto procesů a vytváření aktualizací softwaru, které se používají bezpečně.

Aplikací procesů v této normě vede k:

- Aplikace aktualizací softwaru na vozidla bezpečným způsobem
- Zavedení jasných provozních procesů, včetně explicitního stanovení a plánování cílů, interních auditů, monitorování a měření procesů a zlepšení procesů
- Sdílené povědomí o bezpečnosti a kybernetické bezpečnosti mezi spřízněnými stranami
- Důvěryhodnost, že aktualizace softwaru jsou poskytovány na základě jasných a kontrolovaných procesů

Norma bude obsahovat tyto body:

- Organizační požadavky na aktualizaci softwaru
- Požadavky na úrovni projektu pro aktualizaci softwaru
- Požadavky na infrastrukturu
- Požadavky na vozidla a komponenty podporující aktualizaci softwaru
- Požadavky na vývoj aktualizace softwaru
- Požadavky na distribuci a provedení aktualizace softwaru.

Zejména v jedné své části popisuje příklad fáze životního cyklu vozidla a tomu odpovídající fáze infrastruktury pro návrh a vývoj softwarových aktualizací softwaru, vývoj vozidel a jejich komponentů podporujících softwarové aktualizace, vývoj balíčků aktualizací, až po operace s aktualizacemi softwaru.

1.4 SAE J3061

Norma SAE J3061 slouží především jako pokyny.

Od roku 2022 bude v EU povinné prokazování shody ve dvou nových oblastech popsaných v této normě: [6]

Systému managementu kybernetické bezpečnosti (CSMS)

Systém řízení kybernetické bezpečnosti (CSMS) znamená systematický přístup založený na rizicích, který definuje organizační procesy, odpovědnosti a správu za účelem řešení rizik spojených s kybernetickými hrozbami pro vozidla a jejich ochrany před kybernetickými útoky. [7]

Účelem CSMS je preventivně identifikovat a eliminovat kritické slabiny. Počet bodů vniknutí útočníků musí být od samého začátku udržován na co nejnižší úrovni. To je jediný způsob, jak omezit oblasti útoku a tím i riziko kybernetického útoku. Každá společnost se proto musí orientovat na osvědčené postupy pro efektivní kybernetickou bezpečnost. Tyto osvědčené postupy se primárně týkají zásad, které je třeba dodržovat při vývoji, výrobě, organizaci společnosti a přidělování odpovědností. [8]

Hlavními kritérii shody jsou momentálně vyvíjené dokumenty pracovní skupiny OSN pro kybernetickou bezpečnost a problematiku bezpečnosti bezdrátového přenosu dat (UN Task Force on Cyber Security and Over-the-Air issues), Hospodářské komise OSN pro Evropu (UN ECE) a Světového fóra UN ECE pro harmonizaci předpisů pro vozidla (WP.29).

Dosavadní návrh doporučení pro kybernetickou bezpečnost (Draft Recommendation on Cyber Security) definuje zásady pro řešení klíčových hrozeb a zranitelností identifikovaných za účelem zajištění bezpečnosti vozidla v případě kybernetických útoků. Je požadováno, aby byla kybernetická bezpečnost integrována do životního cyklu vozidla.

Aby bylo možné úspěšně zvládnout složitost všech rizik v oblasti kybernetické bezpečnosti vozidel, musí mít každá společnost v budoucnu CSMS. To zahrnuje jak organizační, tak technickou oblast společnosti nebo produktu. Zde je zahrnut proces vývoje produktu, výroba a veškeré servisní, údržbářské a opravné práce po uvedení komponentu nebo softwaru do provozu. Celý vývoj automobilového systému musí být pečlivě koordinován, aby vyhověl budoucím požadavkům na kybernetickou bezpečnost. Je proto důležité vytvořit správné rámcové podmínky v organizační i procesní struktuře společnosti a zahájit příslušná opatření. Certifikace podle WP.29/78 nebo podle norem ISO vytvoří regulační základ pro budoucí spolupráci mezi výrobci vozidel a poskytovateli služeb v automobilovém průmyslu.

Systému managementu aktualizace softwaru (SUMS)

Znamená systematický přístup definující organizační procesy a postupy pro splnění požadavků na dodávání aktualizací softwaru podle nařízení ECE/TRANS/WP.29/78.

Kybernetická bezpečnost dle ISO 21434 popisuje, jak by se měly softwarové změny řídit, aby bylo zajištěno, že jsou prováděny bezpečným způsobem prostřednictvím bezdrátové aktualizace, nebo jinými prostředky.

Vzhledem k tomu, že proces řízení a schvalování aktualizace softwaru po udělení počátečního typového schválení (homologace) a postup registrace vozidla se provádějí podle národních právních předpisů, budou některá doporučení ještě upravena právě legislativou jednotlivých zemí. Systémově adekvátním přístupem k dosažení shody s výše uvedenými doporučeními budou normy Mezinárodní organizace pro standardizaci ISO/SAE 21434 - Silniční vozidla - Kybernetická bezpečnost, respektive ISO 24089 - Silniční vozidla - Aktualizace softwaru. Ty stanoví jednoznačná kritéria, podle nichž bude možné obě oblasti auditovat a certifikovat.

Konference Evropské Hospodářské Komise z výboru pro vnitrozemskou dopravu vydávají návrhy na znění předpisů EHK pod označením ECE/TRANS/WP.29/2020/80 pro schvalování vozidel z hlediska Kybernetické bezpečnosti a systému řízení Kybernetické bezpečnosti. Případná certifikace podle ISO/SAE 21434 a ISO 24089. Tento předpis se zaměřuje na vozidla kategorie M a N případně O (pokud je vybaveno alespoň jednou řídící jednotkou). V tomto předpisu jsou stanoveny definice jako:

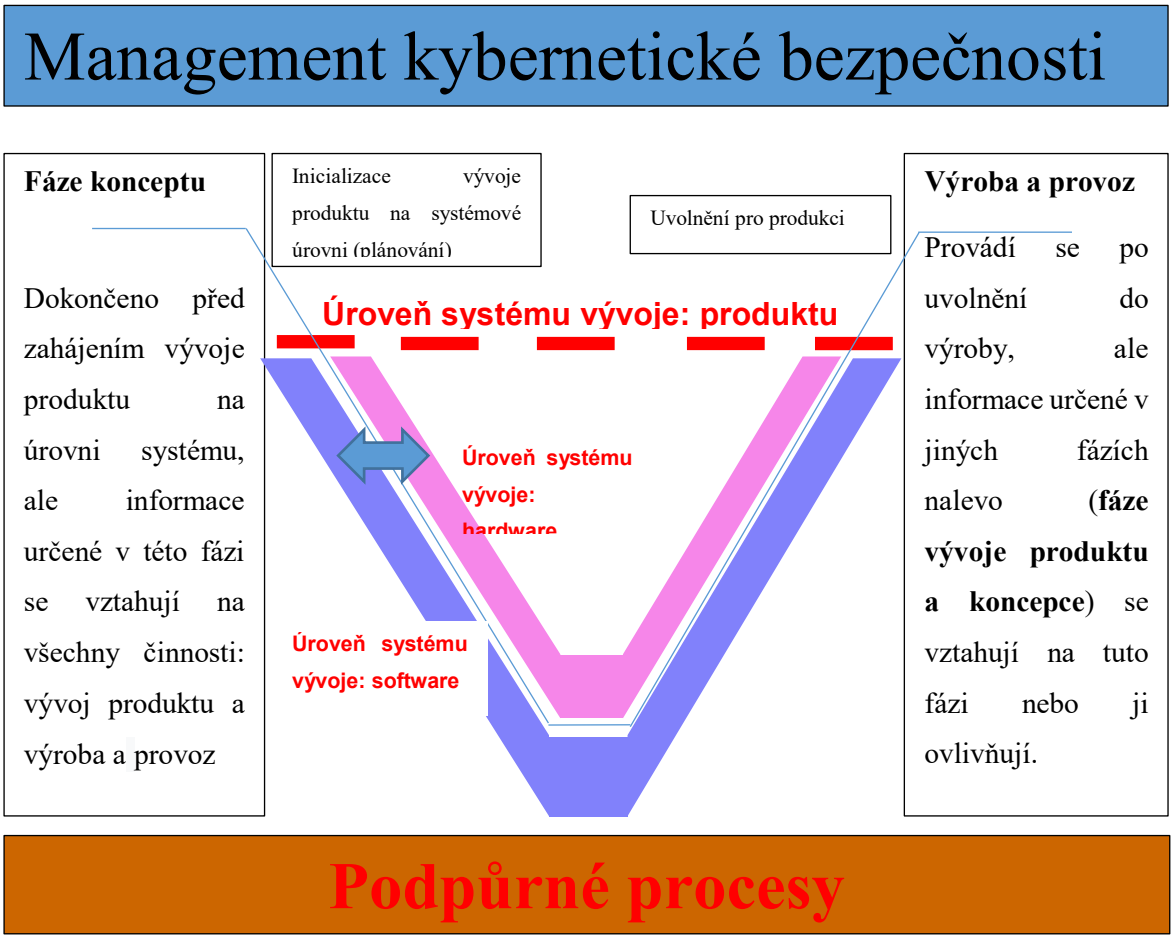
- *Zmírnění* – znamená opatření, které sníží riziko
- *Riziko* – potenciál pro zneužití zranitelnosti vozidla

- *Posouzení rizik* – proces hledání, rozpoznávání a popisování rizik
- *Hrozba* – potenciální příčina, která může vést k poškození systému
- *Zranitelnost* – slabina systému.

Mezi základní normy, jimiž se bude budoucí řízení kybernetické bezpečnosti řídit je SAE J3061_2016. Jedná se o normu kybernetické bezpečnosti pro kyber - fyzické systémy vozidla.

Definuje kompletní rámec procesu životního cyklu, který lze přizpůsobit a využít v rámci vývojových procesů každé organizace k začlenění kybernetické bezpečnosti do systémů kyber - fyzikálních vozidel od fáze konceptu přes výrobu, provoz, servis a vyřazení z provozu. [9]

V této normě se definuje mnoho důležitých aspektů, mezi které patří také management kybernetické bezpečnosti, který se dělí na fázi konceptu a výrobu a provoz, pod kterou spadá fáze vývoje produktu a koncepce.



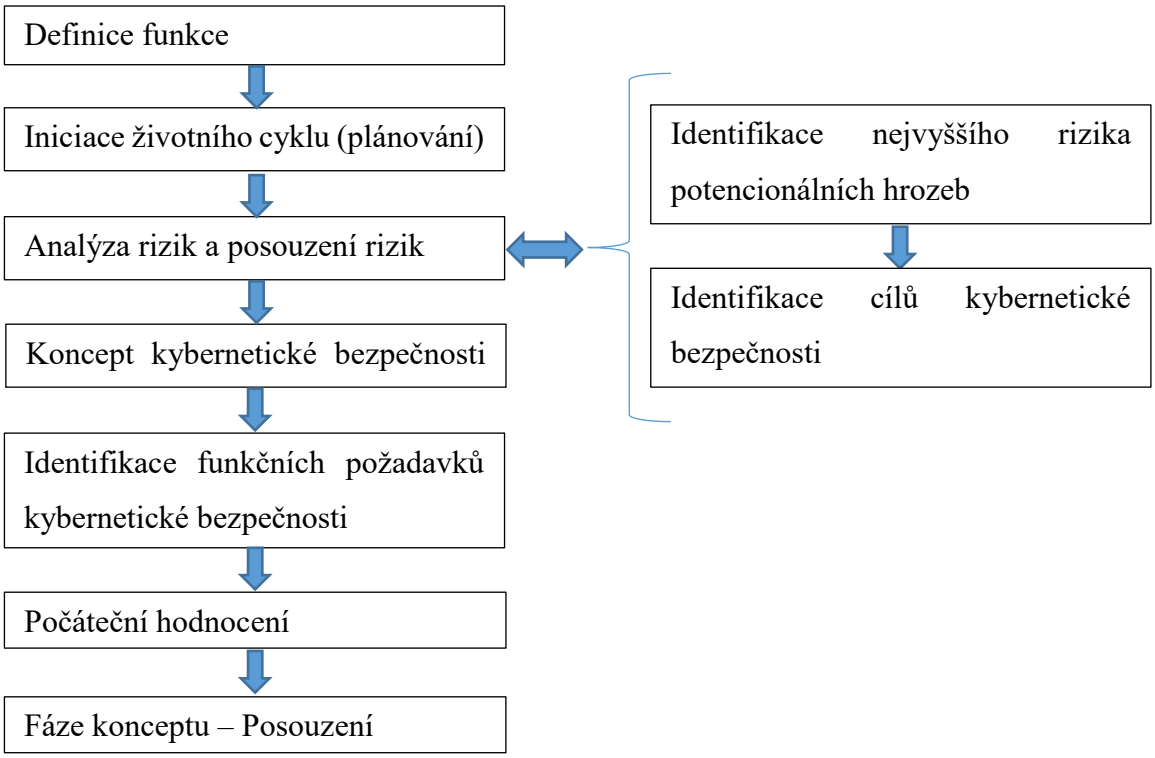
Obr. 1.3 Celkový rámec kybernetické bezpečnosti

Zdroj: [7] [SAE J3061str. 24].

Fáze konceptu

Ukazuje průběh aktivit během fáze konceptu. Dobře definovaný rozsah pomáhá propojit budoucí analytické činnosti, takže analýzy mohou být dokončeny efektivněji. Zahájení životního cyklu kybernetické bezpečnosti zahrnuje vývoj plánu programu kybernetické bezpečnosti, který popisuje činnosti, které mají být prováděny jako součást životního cyklu kybernetické bezpečnosti. Analýza a hodnocení hrozeb (TARA – Threat Analysis and Risk Assessment dle SAE J3061) se používá k identifikaci a hodnocení potenciálních hrozeb pro systém a k určení rizika spojeného s každou identifikovanou hrozbou. Výsledky této analýzy se zaměří na nejrizikovější kybernetické bezpečnostní hrozby. Cíle kybernetické bezpečnosti jsou určeny pro nejvyšší riziko potenciálních hrozeb. Na nejvyšší úrovni mohou být cíle kybernetické bezpečnosti inverzní k potenciální hrozbě; například pokud je potenciální hrozbou neoprávněné brzdění, může být cílem nejvyšší úrovně kybernetické bezpečnosti zabránit nebo snížit pravděpodobnost výskytu takového brzdění nebo zmírnit potenciální následky tohoto brzdění

Jakmile jsou cíle kybernetické bezpečnosti stanoveny pro nejvyšší úrovně hrozeb, může být vyvinut koncept kybernetické bezpečnosti, který popisuje strategii kybernetické bezpečnosti na vysoké úrovni pro tuto funkci. Na konci fáze konceptu může být provedeno předběžné posouzení kybernetické bezpečnosti k posouzení stavu, který je navržen pro tuto funkci.



Obr 1.4 Fáze konceptu – činnosti

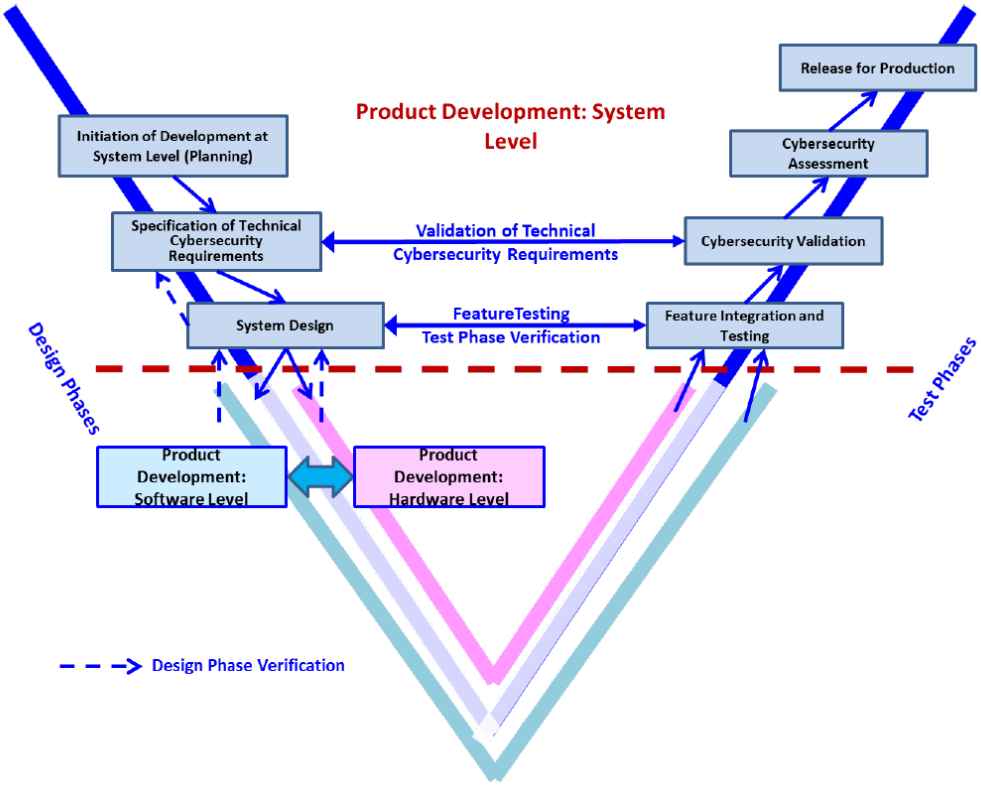
Zdroj: [9]

Fáze vývoje produktu

Tato fáze vývoje produktu zahrnuje vývoj produktu na úrovni systému, vývoj produktu na úrovni hardwaru a vývoj produktu na úrovni softwaru. Mezi jednotlivými fázemi vývoje dochází k iteracím mezi sebou.

Vývoj produktu na úrovni systému

Během vývoje produktu na systémové úrovni je koncepce kybernetické bezpečnosti vylepšena na technickou koncepci kybernetické bezpečnosti. Zde lze provést analýzu hrozeb na úrovni systému nebo analýzu zranitelnosti, pokud jsou k dispozici významné nové informace. Na úrovni systému se provádí validace a testování v testovacích fázích spodních úrovních V- modelu. Technické požadavky kybernetické bezpečnosti jsou poté odvozeny a upřesněny z požadavků vysoké úrovně kybernetické bezpečnosti a technické strategie kybernetické bezpečnosti.



Obr. 1.5 V diagram pro fázi vývoje na úrovni systému

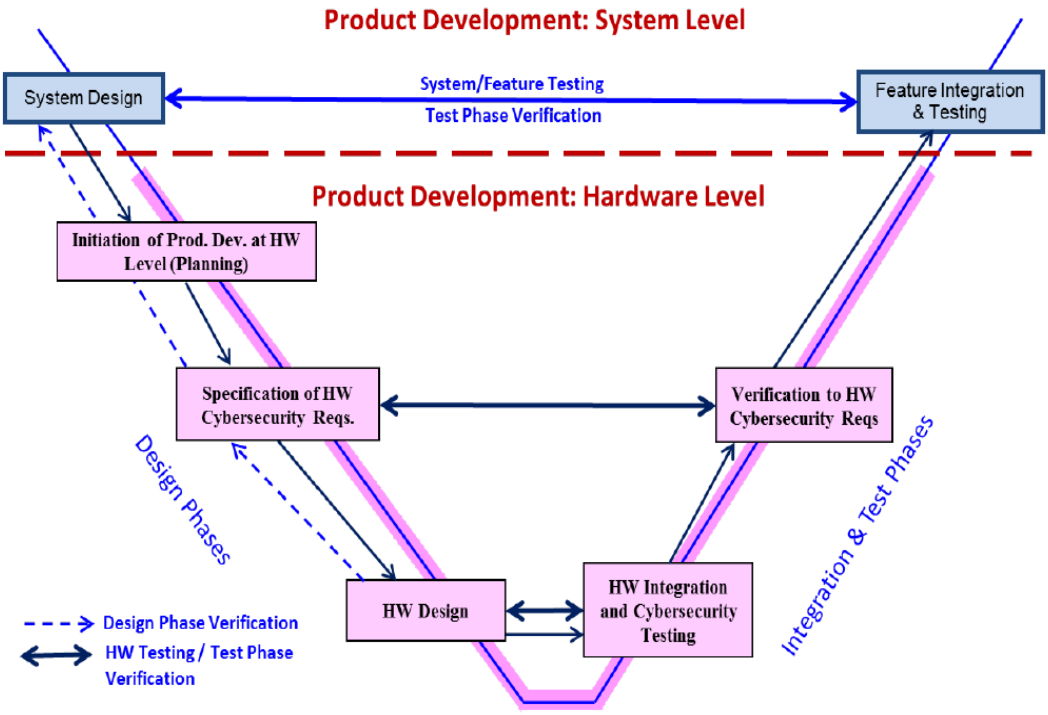
Zdroj: [9]

Kontext systému (dokument o hardwarovém / softwarovém rozhraní), který definuje rozhraní mezi hardwarem a softwarem systému, klíčovými datovými toky a ukládáním a zpracováním v systému. Pomocí kontextu systému se pak technické požadavky na kybernetickou bezpečnost na úrovni systému přidělí hardwaru a softwaru nebo oběma. Jakmile budou technické požadavky na kybernetickou bezpečnost přiděleny hardwaru, nebo softwaru, mohou začít aktivity na úrovni vývoje produktu:

Vývoj produktu na úrovni hardwaru

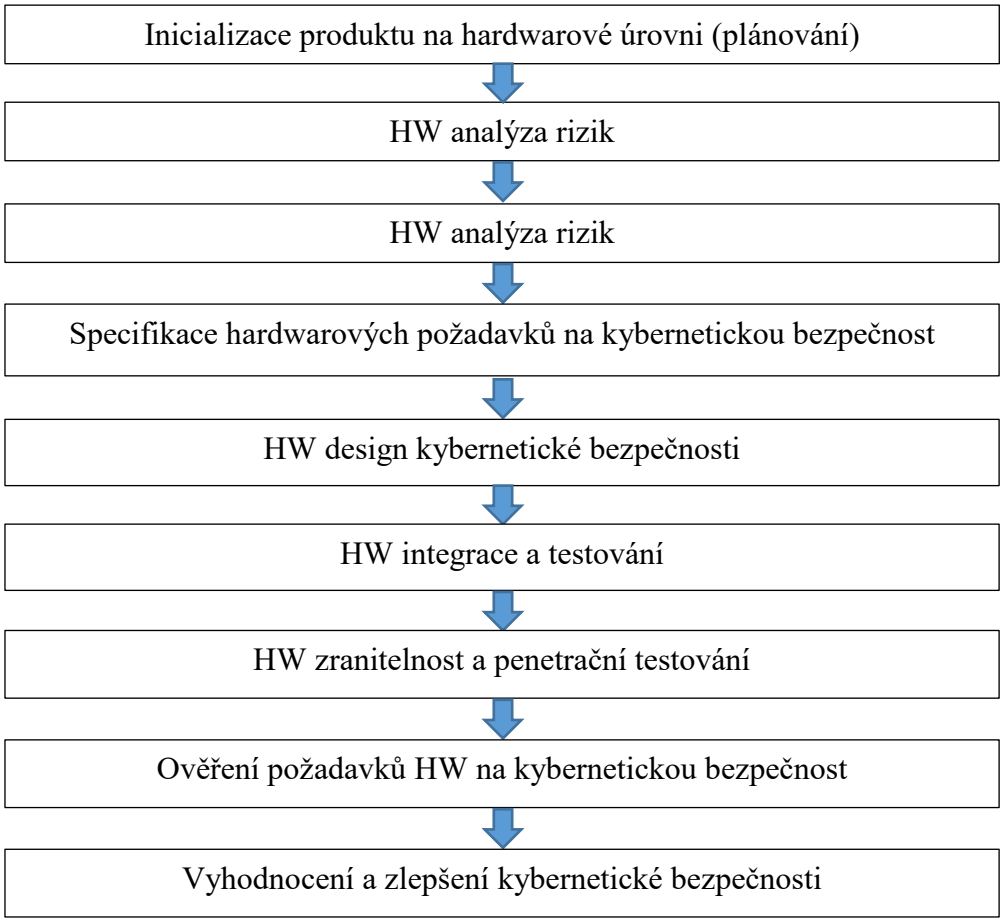
Hardwarové požadavky kybernetické bezpečnosti jsou specifikovány z požadavků kybernetické bezpečnosti přidělených hardwarů během vývoje na úrovni systému. Pokud je to možné, mohl by být v této fázi vylepšen koncept technické kybernetické bezpečnosti. Po návrhu hardwaru je provedena analýza zranitelností, která pomůže identifikovat potenciální rizika v návrhu a pomůže identifikovat řízení/ovládání/opatření kybernetické bezpečnosti k řešení potenciálních zranitelností. Po integraci a testování hardwaru lze na

návrh hardwaru použít testování zranitelnosti a penetrace. Poté se provede posouzení kybernetické bezpečnosti a upřesní se předběžné posouzení kybernetické bezpečnosti.



Obr. 1.6 V diagram fáze vývoje na úrovni hardwaru a jeho vztah k vývoji produktu na systémové úrovni

Zdroj: [9].

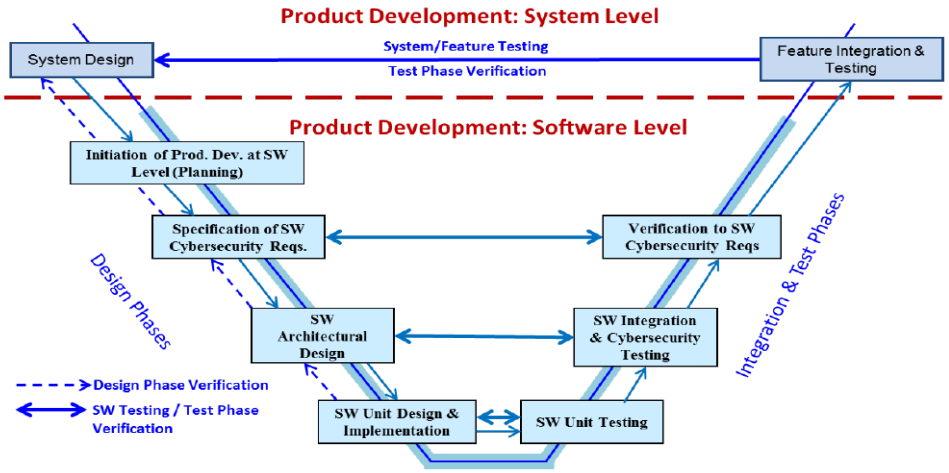


Obr. 1.7 Fáze vývoje na úrovni hardwaru

Zdroj: [9].

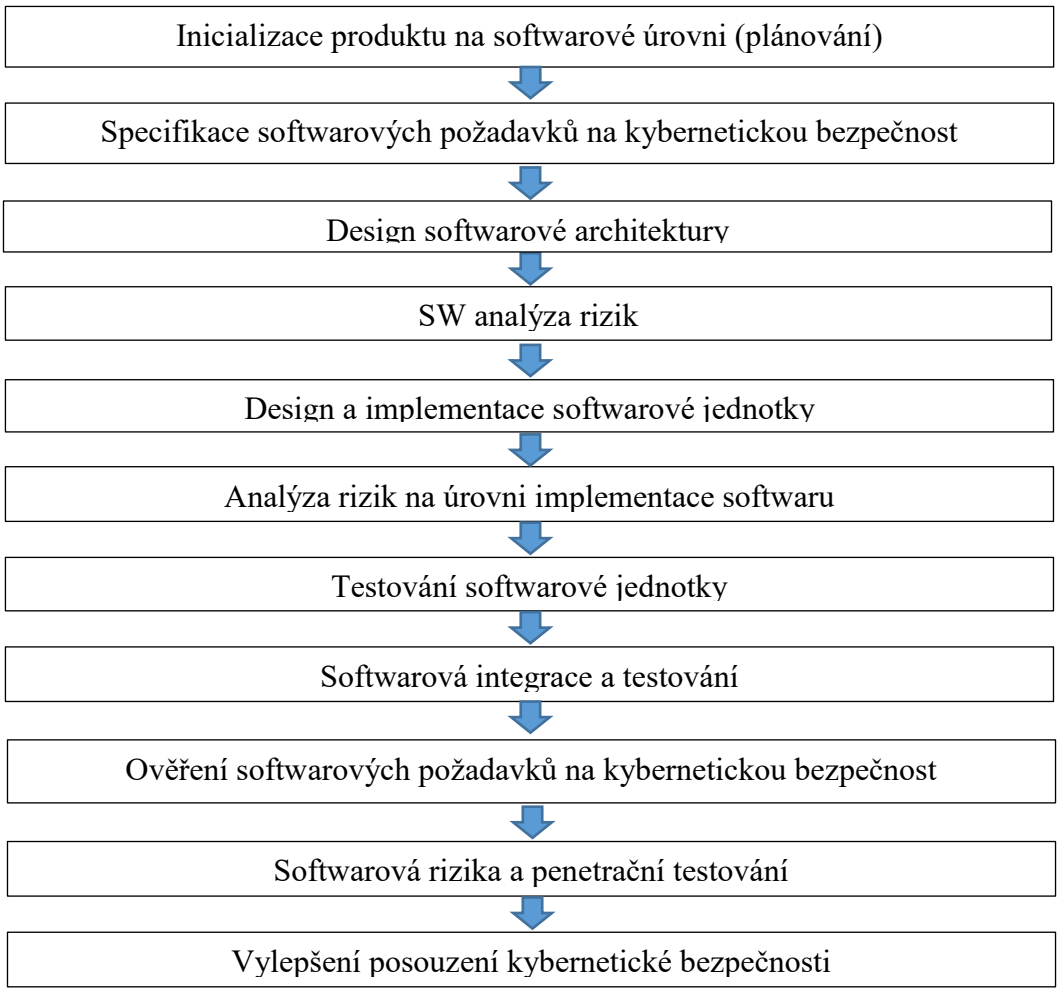
Vývoj produktu na úrovni softwaru

Softwarové požadavky kybernetické bezpečnosti jsou specifikovány z požadavků kybernetické bezpečnosti přidělených softwarů během vývoje na úrovni systému. Pokud je to možné, mohl by být v této fázi vylepšen koncept technické kybernetické bezpečnosti. Po provedení architektury softwarového návrhu lze provést analýzu rizik, která pomůže identifikovat potenciální rizika v této architektuře designu softwaru a pomůže identifikovat prvky kybernetické bezpečnosti k řešení potenciálních rizik. Po návrhu a implementaci softwarové jednotky lze aplikovat analýzu zranitelností na úrovni softwaru, testování softwarové jednotky a integraci testování softwaru. Po integraci softwaru jsou ověřeny požadavky na softwarovou kybernetickou bezpečnost a na softwaru lze provést testování zranitelnosti a penetrace. Poté se provede posouzení kybernetické bezpečnosti a upřesní se předchozí hodnocení kybernetické bezpečnosti.



Obr. 1.8 V diagram fáze vývoje na úrovni softwaru a jeho vztah k vývoji produktu na systémové úrovni

Zdroj: [9].



Obr. 1.9 Fáze vývoje na softwarové úrovni

Zdroj: [9].

Výroba, provoz a servis

Činnosti ve fázi produkce zahrnují plánování výroby s ohledem na všechny požadavky související s kybernetickou bezpečností, které mohou ovlivnit výrobní proces, včetně požadavků týkajících se zabezpečení konkrétních částí výrobního procesu. Požadavky na výrobu související s kybernetickou bezpečností mohou být zahrnuty do stávajícího plánu produkce. Tyto požadavky na kybernetickou bezpečnost systému mohou ovlivnit konkrétní proces, kterým bude software přenesen ve výrobním závodě na ECU.

Fáze provozu zahrnuje provoz i servis. Servis zahrnuje běžné činnosti údržby a opravy. Veškeré požadavky specifické pro kybernetickou bezpečnost během provozu by měly být zaznamenány v příslušných dokumentech. Pokud jde o služby, měly by být jakékoli činnosti údržby a opravy, které mají potenciál nepříznivě ovlivnit kybernetickou bezpečnost, identifikovány v dřívějších fázích životního cyklu a měly by být stanoveny příslušné postupy, jak udržovat kybernetickou bezpečnost během údržby a opravy jako například postupy údržby a opravy.

1.5 Předpis EHK 155

Tento předpis se týká zejména vozidel kategorie M a N (případně i O, pokud jsou tato vozidla vybavena alespoň jednou řídící jednotkou) s ohledem na kybernetickou bezpečnost. Návrh ECE/TRANS/WP.29/2020/79 ale později by z něho mělo vycházet právě nařízení EHK 155.

Tento předpis pojednává o schvalování ze stran schvalovacích orgánů pro ověření splňujících požadavků.

Nejen kontrolou dokladů je cílem prokázat nastavení procesů, doklady musí existovat, a musí s nimi být seznámeni pověření pracovníci a obhájit, že právě tyto dokumenty dokládají správně nastavené procesy:

a) Shromažďování a ověřování informací o prostředí dodavatelského řetězce, aby bylo prokazatelné, že rizika spojená s dodavateli jsou identifikována a řízena.

b) Dokumentace posuzování rizik během vývojové fáze a výsledky zkoušek a zmírnění za účelem posouzení rizik.

c) Zavádění opatření kybernetické bezpečnosti při navrhování typu vozidla.

d) Detekce možných útoků a reakce na tyto útoky.

e) Záznam pro umožnění detekce kybernetických útoků a poskytování jejich forenzních schopností (potenciálu) k umožnění analýzy kybernetických útoků a jejich pokusů. [10]

Schvalovací orgán (technická zkušebna) ověří zkouškou, zda výrobce vozidla provedl opatření, týkající se kybernetické bezpečnosti, které zdokumentoval.

Testování se zaměřuje, ale neomezuje na rizika, která jsou během hodnocení rizik hodnocena jako vysoká.

Výrobce vozidla musí identifikovat kritické prvky typu vozidla a provést vyčerpávající posouzení rizik pro typ vozidla a musí náležitě zacházet s identifikovanými riziky. Při posuzování rizik se musí brát v úvahu jednotlivé prvky typu vozidla a jejich vzájemné působení. Posouzení rizik dále musí brát v úvahu interakce s jakýmikoli externími systémy. Při posuzování rizik musí výrobce vozidla vzít v úvahu rizika spojená se všemi hrozbami, zavede vhodná a přiměřená opatření k zabezpečení dedikovaného prostředí typu vozidla pro ukládání a spouštění „aftermarket“ softwaru, služeb, aplikací nebo dat.

Výrobce vozidla provede před schválením typu vhodné a dostatečné testování, aby ověřil účinnost zavedených bezpečnostních opatření.

Analýza hrozeb rovněž zohlední možné dopady útoku. To může pomoci zjistit závažnost rizika a určit další rizika. Možné dopady útoku mohou zahrnovat:

a) Bezpečný provoz dotčeného vozidla
b) funkce vozidla přestanou fungovat
c) změněný software, změněný výkon
d) software změněný, ale bez provozních účinků
e) porušení integrity dat
f) porušení důvěrnosti údajů
g) ztráta dostupnosti údajů
h) jiné, včetně trestné činnosti.

DETA databáze

Návrh nového OSN předpisu o jednotných ustanoveních týkajících se schvalování vozidel s ohledem na kybernetickou bezpečnost a systém řízení kybernetické bezpečnosti uvádí, že po udělení schválení daného vozidla je nezbytně nutné nahrát schválení typu spolu s doplňující dokumentací do DETA databáze.

DETA je databáze pro výměnu dokumentace schválení typu. DETA je v rámci UNECE pod správou Německa a tato databáze byla spuštěna 18. března 2019.

Zpráva o zasedání 177. WP.29 poskytuje informace o přístupu k DETA. Uživatelé přistupující k DETA se zavazují zachovávat důvěrnost obsahu DETA. [11]

1.6 Kybernetická bezpečnost v dalších oblastech

1.6.1 IEC62443

Norma (2010 industrial and network) popisuje technické i procesní postupy průmyslové kybernetické bezpečnosti. Rozděluje průmysl na: provozovatele, integrátoři (poskytovatelé služeb pro integraci a údržbu) a výrobci. Jednotlivé role se řídí přístupem založeným na rizicích, aby předcházely a řídily bezpečnostní rizika ve svých činnostech.

1.6.2 ISO 27001

ISO27001 je norma, která se zaměřuje na porozumění organizaci, její činnosti a potřeby. Zkoumá prostředí, v němž organizace působí na vztahy se zainteresovanými stranami, jako jsou zákazníci, dodavatelé, veřejnost, zájmové skupiny. Jedná se především o systém managementu bezpečnosti informací tzv. ISMS a zavádění zlepšování ISMS na základech analýz a auditů v organizaci v souladu se systémy řízení kvality nebo bezpečnosti prostředí.

Samotná norma ISO / IEC 27000 obsahuje spoustu dalších řad, z nichž se zde uvedou pouze související normy s tématem kybernetické bezpečnosti.

- ISO 27000 - definuje pojmy a terminologický slovník pro všechny ostatní normy z této série.

- ISO 27001 (BS7799-2) - hlavní norma pro Systém řízení bezpečnosti informací (ISMS)
- ISO 27005 - norma byla publikována v červnu 2008 pod názvem Information technology - Security techniques - Information security risk management".
- ISO 27010 - Poskytuje doporučení pro řízení bezpečnosti informací při interní a mimo firemní komunikaci.
- ISO 27011 - Obsahuje doporučení a požadavky na řízení bezpečnosti informací v prostředí telekomunikačních operátorů.
- ISO 27032 - norma pod označením "Guidelines for cybersecurity" obsahuje bezpečnostní doporučení týkající se kyberprostoru.
- ISO 27033 - soubor norem poskytující doporučení pro implementaci protiopatření vztahujících se k bezpečnosti sítí.
- ISO 27034 - soubor norem poskytující doporučení pro bezpečnou tvorbu, implementaci a užívání aplikačního softwaru.
- ISO 27035 - "Information security incident management". Norma se věnuje řízení incidentů bezpečnosti informací.
- ISO 27038 - Norma obsahuje doporučení pro publikování digitálních dokumentů.
- ISO 27040 - Doporučení pro bezpečné ukládání dat.
- ISO 27100 – Norma poskytuje přehled kybernetické bezpečnosti a popis relevantních konceptů.
- ISO 27101 - Poskytuje doporučení pro vývoj rámce kybernetické bezpečnosti.
- ISO 27103 - Norma poskytuje doporučení jak použít existující standardy v rámci kybernetické bezpečnosti.
- ISO 27550 - norma pojednává o vytváření ICT systémů v zaměření na ochranu osobních údajů.
- ISO 27551 - norma by měla specifikovat požadavky pro autentizaci anonymních entit. [13]

1.7 Související normy

Další normy a nařízení, které jsou spojeny s kybernetickou bezpečností a jsou nedílnou součástí vývojových fází produktu, budou uvedeny v této kapitole.

1.7.1 ISO 31000

ISO 31000 (risk management guidelines) řízení rizik pro zvýšení efektivity firem. Tato norma popisuje, jak by organizace měly rozvíjet, implementovat a zlepšovat rámec, jehož účelem je integrace procesů pro řízení rizik do svého celkového vedení, strategie a plánování, managementu, procesů podávání hlášení, politik, hodnot a kultury.

ISO 33001 - Process assessment ISO33001(vyhodnocení V-modelu) - Jedná se o soubor norem popisující vývoj softwaru. Norma se věnuje terminologii hodnocení procesu, aplikaci hodnocení procesu pro hodnocení dosažení kvalitativních charakteristik procesu a aplikaci výsledků hodnocení procesu na řízení.

SAE J3101 - Hardware Protected Security for Ground Vehicles – Tato norma popisuje, jak je prostředí zabezpečené a chráněné hardwarem. Poskytuje platformu pro implementaci řízení přístupu pomocí zabezpečeného ověřování, autorizace a vynucování přístupu. Nedefinuje žádný konkrétní systém řízení přístupu, modely ani zásady.

Hlavní dva typy zapojení hardwarově chráněného bezpečnostního prostředí jsou plná kontrola a částečná kontrola. Při částečné kontrole je hardwarově chráněné bezpečnostní prostředí odpovědné za ověření a autorizaci přístupu, zatímco normální prostředí je odpovědné za uzamčení / odemknutí prostředku.

SPACE IEC 15504 - Účelem této normy je poskytnout schéma pro hodnocení schopnosti softwarových procesů a způsob jejich zlepšení. Schopnost procesu je definována jako charakterizace schopnosti procesu splnit současné, nebo předpokládané obchodní cíle.

1.7.2 ISO 26262 FuSa

Jedná se o normu Funkční bezpečnosti, která je často zmiňována, jako oblast, kde se dopady kybernetické bezpečnosti mohou výrazně projevit. Je také uváděna často v normách o kybernetické bezpečnosti.

Funkční bezpečnost má za cíl snížení rizika na společensky přijatelnou úroveň. Tato norma je zaměřená na snížení rizika zranění, nebo usmrcení osob způsobené nesprávnou funkcí elektronického systému v sériově vyráběném autě. Nejsou zde zahrnuty samotné funkce systému, hrozby jiné než selhání systému, škody na majetku a systémy v jiných než sériových vozech.

1.7.3 SOTIF ISO / PAS 21448

Norma se zaměřuje na minimalizaci rizika způsobeného nebezpečím, které vyplývá z nedostatečné činnosti zamýšlené funkce, resp. nesprávného použití této funkce.

Nedostatečná činnost funkce vyplývá především z limitů zvoleného technického řešení. Typickým příkladem jsou omezení jednotlivých typů senzorů v různých podmínkách (např. světelné podmínky, počasí, množství a chování objektů v okolí), případně omezení vyhodnocovacího procesu (např. nedostatečný výkon, nepřesný model).

Norma se aplikuje zejména na systémy ADAS a systémy odpovídající alespoň úrovni automatizace 1 nebo 2 podle standardu SAE J3016, založené na komplexních senzorech a vyhodnocovacích algoritmech, které zasahují do řízení vozidla podle okolní situace. Norma neslouží k rozšíření standardu ISO 26262, zabývá se další oblastí rizik, která jsou mimo rozsah standardu.

Cílem normy je popis procesu, jak pro komplexní funkce identifikovat scénáře, ve kterých se vozidlo může nacházet, vyhodnotit případné riziko a systematickým postupem během vývoje zapracovat taková technická (příp. jiná) opatření, aby se snížila pravděpodobnost těch scénářů, které jsou identifikovány jako nebezpečné. Součástí celého procesu je i ověření zvoleného řešení. [12]

1.7.4 ISO 12207

ISO 12207 SW development (sw life cycle) - Definuje standardní proces životního cyklu softwaru. Definuje rámec činností a úkoly, které je třeba provádět při dodávce, vývoji, provozu, údržbě a odstranění softwarového produktu nebo služby.

1.7.5 EHK 156

Dále skupina GRVA vydává předpis ECE/TRANS/WP.29/2020/80, který se týká schvalování vozidel z hlediska aktualizací softwaru a systému správy aktualizací softwaru. A to vše s ohledem na kybernetickou bezpečnost a bezdrátovou komunikaci. Tento předpis by měl být platný pro všechna vozidla kategorií M, N, O, R, S a T, které umožňují aktualizaci softwaru.

Předpis o jednotných ustanoveních týkajících se schvalování vozidel s ohledem na aktualizace softwaru a systém správy aktualizací softwaru. Toto nařízení se týká všech motorových vozidel, které umožňují softwarové aktualizace.

Jsou zde popsány jednotlivé procesy ohledně softwarových aktualizací. Od požadavků na systém správy aktualizací, jako jsou dokumentace těchto aktualizací, přes identifikace aktualizací a jejich kompatibilita se systémem vozidla, až po provedení aktualizace.

V tomto předpisu se uvádí povinnost výrobce prokázat správné nastavení procesů. Postupovat v souladu s tímto předpisem a to jak s dokumentací, tak i s demonstrací například OTA aktualizacemi. [14]

1.8 NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost ČR

je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo. Vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Ředitel úřadu se též pravidelně účastní jednání Bezpečnostní rady státu (BRS) a je členem Výboru pro kybernetickou bezpečnost, který je stálým pracovním orgánem BRS pro koordinaci plánování opatření k zajišťování kybernetické bezpečnosti České republiky. [15]

Ústřední správní orgán pro:

- Kybernetickou bezpečnost
- ochrana utajovaných informací v oblasti informačních a komunikačních systémů
- kryptografická ochrana
- problematika služby PRS (Public Regulated Service) v rámci družicového systému Galileo
- vzdělávání.

2 Návrh rámce penetračního testování kybernetické bezpečnosti ASV

Tato část se zaměří na metodiku pro oblast působnosti z hlediska kybernetické bezpečnosti, a to systému ALKS. Systém ALKS aktuálně patří do kategorie L3, ale pro naše potřeby jej použijeme jako případ pro stanovení metodiky.

Pro tyto účely použijeme osobní automobil úrovně L4, na který bude z hlediska kybernetické bezpečnosti dle návrhu EHK 155 aplikovaný tento rámec/metodika. Výsledky a poznatky by měly sloužit pro případné testování v certifikačních laboratořích pro udělení schválení autonomních systémů kategorie L4, případně vyšší. Tato úroveň je zvolena, protože v této kategorii je stále vyžadována přítomnost řidiče, ačkoli se nevyžaduje jeho zásah a je to vyšší úroveň autonomity, než je aktuálně povolen legislativními omezeními, proto je třeba zohlednit možná rizika a sdílet mezi jednotlivými zkušebnami postupy pro ověření robustnosti a bezpečnosti.

Systém ALKS bude hodnocen pomocí TARA analýzy, kde budou zohledněny možné slabiny systému ALKS obecně.

Jelikož se jedná o rámec, bude obsah zjednodušen pro ukázku možného postupu. Hrozby, stejně tak i navrhovaná opatření společně s dalšími parametry, které budou příkladové pro postupné stanovení jednotlivých metodik ke konkrétním projektům.

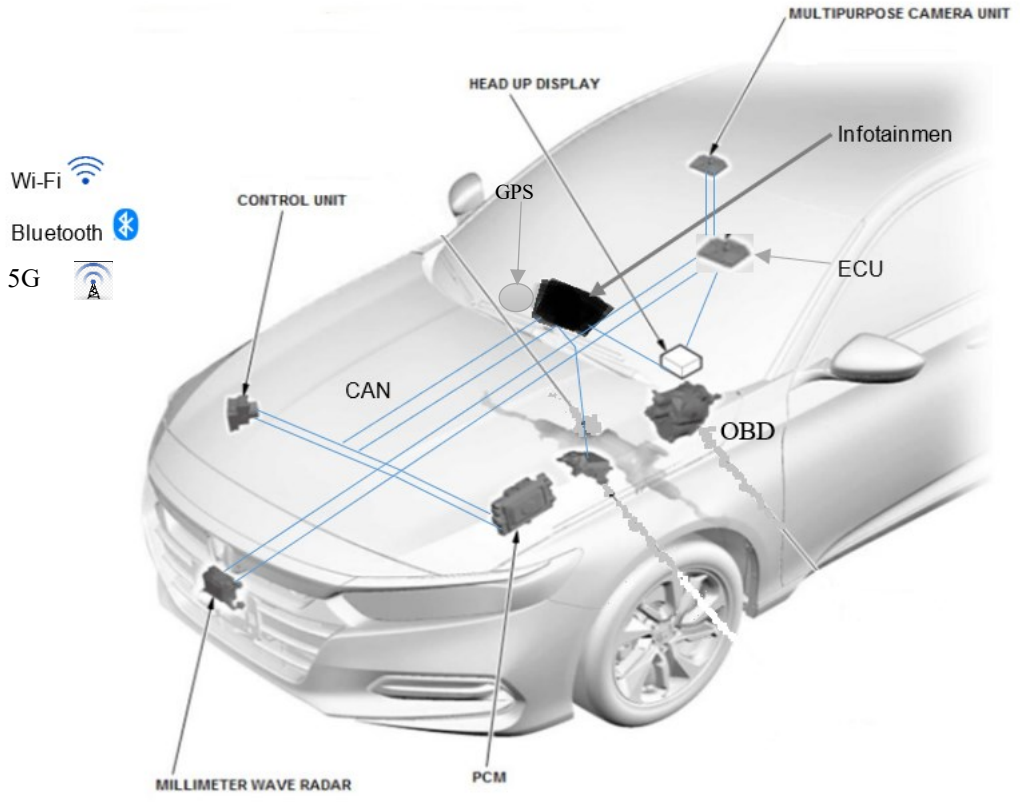
2.1 ALKS

ALKS je technologie vozidla navržená k dlouhodobému ovládání bočního tj. levého a pravého a podélného tedy rychleji nebo pomaleji pohybujícího se vozidla bez dalšího povelu zásahu řidiče. [16] Během této doby má ALKS primární kontrolu nad vozidlem a tak může provádět místo řidiče řidičské úkony. Pro tento případ bude systém využíván kombinací front kamery, radaru, případně lidaru pro zajištění správné funkčnosti. Tyto senzory společně kooperují a na základě zpráv ze všech senzorů systém rozhoduje, zda je aktuální situace příznivá v takové míře, aby systém mohl provést aktivaci.

Pro systém ALKS je připraven návrh ECE/TRANS/WP.29/2020/81, který je vydán jako EKH 157.

Aktuálně je systém ALKS definovaný pro úroveň autonomity L3 pro použití do sériově vyráběných vozidel. V případě, že budou systémové funkce posíleny, systém ALKS bude schopen samostatných úkonů, bez zásahu řidiče, a to na všech typech komunikací a za splnění všech bezpečnostních podmínek. Vozidlo musí být schopno fungovat jak v extravilánu (mimo obec), tak i v intravilánu (zastavěné území). Musí být bezpečné pro pasažéry i pro ostatní účastníky silničního provozu, a to za všech možných situací. Pro takové možnosti bude třeba více prvků, jako jsou například komunikace V2I a V2V pro kooperaci na pozemní komunikaci, snímání okolí, logické vyhodnocovací funkce, určení polohy na základě GPS, příp. mapových podkladů a mnoho dalších. Takto upravené vozidlo se systémem ALKS může dosáhnout úrovně L4.

Pro potřebu sestavení TARA analýzy je třeba určit strukturu vozidla (viz Obr. 2.10) s možnými prostředími, kde je potenciální riziko útoku či hrozí bezpečnostní incident. Jednotlivé komponenty jsou názorné a komunikace je zvolena jak bezdrátovými sítěmi typu Wi-Fi a Bluetooth, tak i komunikačními kanály mezi jednotkami pomocí CAN bus či OBD. Toto schéma ALKS systému je zvoleno jako příkladové.



Obr. 2.10 Schéma pro ALKS systém

Zdroj: [17].

2.2 TARA (Threat Analysis and Risk Assessment)

Tato metodika se opírá o TARA analýzu, která bude stěžejní pro doporučená opatření, případné penetrační testy k otestování bezpečnosti a následného doporučení potřebných opatření ke snížení rizika či zmírnění dopadů. V této analýze se zohlední známé možnosti, které by mohly vést k potenciální kybernetické hrozbě, nebo kde by mohlo dojít k útoku a následnému ovládnutí, zahlcení, nebo ovlivnění fungování ALKS funkce vozidla.

Pro sestavení TARA analýzy je třeba stanovit a zjednodušit jednotlivé parametry. Pro toto zjednodušení jsem se inspiroval ve článku, kde se popisuje toto zjednodušení na základech metod SAE J3061. [18]

EVITA metoda dle SAE J3061 je založena na konceptu potenciálu útoku použitém při hodnocení zabezpečení a zohledňuje útočníka i systém.

HEAVENS metoda dle SAE J3061 jsou různým parametrům přiřazeny různé váhy. Parametry popsané v Tab. 2.4. Dopad bezpečnostních a finančních parametrů může mít nejzávažnější důsledky pro zúčastněné strany, například cestující ve vozidle nemusí přežít, organizace mohou bankrotovat. Na druhé straně je dopad parametrů „Provozní“ a „Legislativní/Osobní“ na celkový dopad relativně nižší, pokud jde o bezpečnost a finanční škody. Různé úrovně bezpečnosti a odpovídající hodnoty pro odhad dopadu bezpečnosti jsou popsány níže.

Dle těchto metod se stanoví v několika bodech Potenciál útoku (**Po**). Hodnota určuje potenciál útoku a pravděpodobnost útoku a jejich modifikace pro získání parametrů ke specifikaci jednotlivých elementů.

2.2.1 Potenciál útoku (Po)

je funkcí odbornosti, zdrojů a možnosti přístupu k cíli a představuje obtížnost provedení útoku. Čtyři navržené faktory, z nichž každý má zvolenou stupnici od 0 (nejnižší potenciál útoku) po 3 (nejvyšší potenciál útoku),

- Vyžadují se odborné technické znalosti (**E**xpertise)
- Znalost návrhu a provozu cíle (**K**nowledge)
- IT hardware / software nebo jiné vybavení potřebné pro cílový útok (**Eq**uipment)
- Příležitosti (**Op**portunity)

Tab. 2.1 Potenciál útoků

Potenciál útoků **Po**			
Odbornost E	**Znalost cílů K**	**Vybavení Eq**	**Příležitosti Op**
E0 (Laik)	K0 (Veřejné)	Eq0 (Standartní)	Op0 (Neomezené)
E1(Pokročilý)	K1 (Omezené)	Eq1 (Specializované)	Op1 (Velké)
E2 (Expert)	K2 (Citlivé)	Eq2 (Zakázkové)	Op2 (Střední)
E3(Profesionál)	K3 (Kritické)	Eq3 (Zakázkové speciální)	Op3 (Malé)

Zdroj: [18 Controllability-aware TARA].

2.2.2 Pravděpodobnost úspěšného útoku (Pr),

jeho hodnocení je vyšší u útoků spojených s nižším potenciálem útoku, Po (Tab. 2.1), a u více útoků spojených s vyšším potenciálem útoku. Nejprve se vypočítá hodnota **Po**, jako součet faktorů dle rovnice viz kap. 2.2.2. Hodnota Po, je celé číslo v rozsahu [0, 12] se převede na celočíselnou hodnotu Pr, v rozsahu od 0 (Nepravděpodobná) do 4 (Vysoká pravděpodobnost).

2.2.3 Výpočet potenciálu útoku:

Potenciál útoku se vypočítá jako součet všech proměnných stanovených v Tab. 2.1, kde numerické označení za písmenem označuje jeho číselnou hodnotu, která se použije pro účely výpočtu a stanovení hodnoty Po – potenciálu útoku. [19]

$$\boldsymbol{Po = E + K + Eq + Op} \tag{2.1}$$

Tab. 2.2 Mapování potenciálu útoku k pravděpodobnosti útoku

Mapování potenciálu útoku k pravděpodobnosti	
Po rozsah	**Pr Hodnocení**
11 < Po (Základní)	Pr0 (Nepravděpodobná)
10 ≤ Po ≤ 11 (Základní vylepšený)	Pr1 (Velmi Nízká)
7 ≤ Po ≤ 9 (Mírný)	Pr2 (Nízká)
4 ≤ Po ≤ 6 (Vysoký)	Pr3 (Pravděpodobná)
0 ≤ Po ≤ 3 (Nejvyšší)	Pr4 (Vysoce pravděpodobná)

Zdroj: [18 Controllability-aware TARA].

Potenciál a jeho rozsah je určen na základech výpočtu, a na základě výsledku je stanovena míra pravděpodobnosti útoku. Vysvětlení parametru pravděpodobnost útoku je níže popsán.

Pravděpodobnost útoku Pr

Pr0 – Útok je nepravděpodobný a může k němu dojít jen ve zvláštních podmínkách.

Pr1 – Velmi nízká pravděpodobnost je ta, ke které dochází zřídkakdy.

Pr2 – Zde je pravděpodobnost nízká, avšak může nastat.

Pr3 – Pravděpodobný výskyt příležitostí je takový, kde útočník nemusí nijak zvlášť vyhledávat situace optimální pro útok.

Pr4 – Vysoce pravděpodobné jsou situace běžného provozu, kde k nim dochází všude a opakují se velice často. Může se jednat třeba o jízdu na dálnici, ve městě atd.

2.2.4 Útočníci v oblasti automotive: [20]

O kompromitaci vozidel mají zájem různé příklady typů útočníků s různými motivacemi:

Tab. 2.3 Popis útočníků a jejich možnosti

	Útočník	Odbornost E	Znalost K	Příležitost Op	Vybavení Eq	Motivace
	Tuner vlastník	E0-E1	K0-K1	Op0-Op1	Eq0-Eq1	Rozšíření a úprava funkčnosti vozidla
	Servis	E1-E3	K1-K3	Op0-Op2	Eq0-Eq2	Rozšíření a úprava funkčnosti nebo stavu (tachometr, palivoměr)
	Bezpečnostní výzkum	E0-E2	K0-K1	Op1-Op2	Eq1-Eq2	Výzkum (veřejný)
	Haktivista	E0-E1	K0-K2	Op2	Eq1	Publicistika
	Konkurent	E2-E3	K2-K3	Op2	Eq1-Eq3	Know-how, technický a technologický náskok (konkurenceschopnost)
	Kriminálník	E1-E2	K2	Op1-Op2	Eq0-Eq2	Finanční motivace, krádež, podvod
	Terorista	E2-E3	K2-K3	Op2-Op3	Eq2-Eq3	Kybernetická válka
	Mezinárodní útočník	E3	K3	Op3	Eq3	Špionáž, kybernetická válka, politické motivy

Zdroj: vlastní zpracování.

Jednotlivý útočníci jsou stanoveni na základech jejich motivací, a proto je i na ně podle toho nahlíženo. V další části budou vysvětleny jednotlivé parametry Tab. 2.1 pro pochopení metodiky stanovení jednotlivých údajů.

Pro parametr **odbornosti E** jsou použity tyto rozsahy:

- E0 Laik – jedná se o běžného uživatele
- E1 Pokročilý – tento typ je mírně znalý v dané problematice
- E2 Expert – jedná se o znalého člověka s možnými přístupy
- E3 Profesionál – člověk pracující či podílející se na vývoji s neomezenými možnostmi

Další parametr, jakým je **Znalost cílů K**

- K0 (Veřejné) – jedná se o informace, které nepodléhají žádnému utajení a jsou veřejně dostupné.
- K1 (Omezené) – tyto informace lze získat od znalých lidí a jsou omezeny pouze znalostí.
- K2 (Citlivé) – citlivá data podléhají utajení a je tudíž obtížné se k nim dostat. Takové informace lze získat od zasvěcených lidí.
- K3 (Kritické) – Tyto informace mají kritickou znalost a podléhají nejpřísnějším utajením a zabezpečením. Jedná se především o data, která jsou klíčová.

Parametr **Vybavení Eq**

- Eq0 (Standardní) – Zařízení tohoto typu jsou volně prodejná (USB, telefon)
- Eq1 (Specializované) – Mezi tyto druhy patří zařízení, které je odbornějšího typu, a jsou k němu zapotřebí znalosti.
- Eq2 (Zakázkové) – Toto zařízení je běžně nedostupné. Pro jeho získání jsou důležité znalosti a tato zařízení jsou nákladná na pořízení.
- Eq3 (Zakázkové speciální) – Speciální zařízení, které jsou vyrobené na zakázku a je tudíž velice obtížné si ho obstarat.

Parametr **Příležitosti Op**

- Op0 (Neomezené) – neomezené příležitosti jsou zde brány tak, že není třeba vyhledávat příležitost k útoku. Jedná se především o častý výskyt vozidel, parkoviště či osobní vlastnictví daného vozidla.
- Op1 (Velké) – Velké příležitosti se nabízejí útočníkovi například, když vozidlo přijede do servisu nebo když je veřejně dostupné.
- Op2 (Střední) – U těchto příležitostí se útok často odehrává například při průjezdu vozidel místem umožňujícím útok.

- Op3 (Malé) – Zde útočník připravuje útok dopředu a má velice omezenou šanci k provedení útoku. Může se jednat třeba o stav, kdy je vozidlo aktualizováno pomocí OTA.

Popis jednotlivých parametrů (viz Tab. 2.3 kapitola 2.2.3) si představíme, jako typy útočníků s jejich možnostmi, jak by mohly napadnout systém ALKS vozidla a jaké mají motivace k provedení útoku nebo pokusu o něj.

Tuner/Vlastník – Tohoto útočníka si lze představit jako vlastníka vozidla, který si chce své auto upravit. Nejedná se o kybernetický útok s velkým rozsahem a s potenciálem usmrtit, ale spíše o jednotlivce zaměřené na jednotlivá vozidla, proto je na ně nahlíženo z pohledu odbornosti, jako na rozmezí E0-E1. Tomuto rozsahu také odpovídají ostatní rozsahy, jako jsou dostupné vybavení, které je závislé na znalostech, které se dají veřejně zjistit a zařízení cenově dostupná a snadno ovladatelná.

Příležitosti jsou velké, jelikož vlastník má k dispozici své auto neustále, a proto se může pokoušet o zásah do systémů velice často. Často se jedná o úpravy výkonu či aktivace komfortních funkcí přes OBD, jelikož tyto informace jsou často veřejně dostupné. Tito útočníci mohou zkoušet jednotlivé porty a jejich rychlosti s cílem najít kombinaci, jenž by jim umožnila vstup do komunikace a manipulaci s daty.

Servis – Tento případ si lze představit z více úhlů pohledu. Jednak z pohledu cíleného útoku servisu s cílem poškodit, nebo vyřadit vozidlo, nebo na žádost klienta. Co se týká odbornosti a vybavení servisů, tak bývají velice dobře informováni citlivými daty a informacemi a vybaveny zakázkovým vybavením pro možnosti úkonů na vozidle. Takto vybavený servis lze považovat za velké riziko, protože výrobce musí poskytovat informace a vybavení pro zajištění možností oprav vozidel a svých systémů. Sdílení know-how zajišťuje více kompetencí, ale také bezpečnostní rizika. Servis, který se rozhodne provést útok s úmyslem poškodit systém, může do vozidla vniknout několika způsoby, ať už přes OBD, nebo přímo pomocí komunikačních portů, případně pomocí vložení nějakého zařízení do vozidla s připojením na komunikaci kupříkladu pro sledování GPS pozice, která je využívána ALKS systémem, nebo zneužití e-callu. Jelikož se jedná v tomto případě o zásah neoprávněný, majitel vozidla nemá možnost tento zásah poznat. V opačném případě, kdy zásah požaduje zákazník, může servis

provádět různé úpravy systému, a proto je třeba i na tyto útoky brát zřetel a k tomu optimalizovat možnosti upozornění na zásah do továrního nastavení.

Bezpečnostní výzkum – Jedná se o útoky spíše za účelem odhalení jejich principů a slabin. Zde jsou využívány praktické zkušenosti za použití zakázkových a specializovaných zařízení. Může se jednat o samotný bezpečnostní výzkum, který si zadal výrobce pro možnosti odhalení nedostatků od nezávislé organizace pro následné přizpůsobení systému. Útoky jsou cílené většinou se širokou škálou možnosti průniku pro otestování co nejvíce možností.

Haktivista – Tento typ útočníka je známý spíše pro útoky za účelem jejich zveřejnění a možného poškození výrobce. Zde se může jednat o útoky na funkční prvky systému. Útoky jsou prováděny stylem pokus-omyl, takže není zapotřebí specializovaného ani zakázkového zařízení pro možnosti útoku. Haktivista má spíše omezené možnosti pro své útoky a jedná se o konkrétní vozidlo, takže cílem je poškodit jedno vozidlo a na těchto základech informovat veřejnost s dopadem na výrobce a zvýšení nedůvěryhodnosti v tyto systémy.

Konkurent – Konkurent se snaží odhalit veškerý technický a technologický náskok ostatních a zvýšit tak svojí výhodu na trhu. Jedná se o velice znalé útočníky s dostatečnými prostředky, a to jak v oblasti zařízení, tak i informací. Útoky jsou nejčastěji prováděny na systém jako takový. Není zde záměr poškodit systém, nebo zranit. Jedná se o cílené poslouchání komunikací, fungování, sestavení struktury dat, vyhodnocování a rozhodovací funkce. Po těchto útocích se útočník v tomto případě konkurenční firma snaží zamaskovat veškeré své možné pokusy o proniknutí či poslouchání. Při úspěšném útoku jsou odhalena citlivá data a to může mít fatální následky v oblasti know – how a s tím spojená finanční ztráta v oblasti konkurenceschopnosti.

Kriminálník – Jde o člověka relativně znalého se znalostmi citlivých dat a možností zakázkových zařízení. Většinou se jedná o zloděje s cílem ukrást vozidlo případně

poškodit vozidlo s úmyslem zabít. V praxi se útoky odehrávají často. V drtivé většině se jedná o nabourání do systému imobilizéru, případně chytání plovoucího kódu u klíčů aut. Tyto útoky mají za následek odcizení vozidla, nebo jeho vykradení. Útočníci mohou používat jak běžně dostupná zařízení, která nejsou nijak specializovaná ani zakázková, tak si mohou pomáhat i zakázkovými přístroji.

Terorista – Tento typ útočníka má motivaci jednoznačně usmrtit. Útoky bývají cíleny na velké množství vozidel tak, aby došlo k hromadným ztrátám, a to jak na straně vozidel, tak zejména na straně lidských životů. Využívají přitom specializované nástroje pro možnosti vedení kybernetických válek.

Mezinárodní útočník – Motivy těchto útoků bývají v globálních měřítkách. Jednat se může o špionáže, kde je monitorován pohyb vozidel, ochromení infrastruktury jako celku, vedení kybernetických mezinárodních válek. K dispozici pro tyto útoky jsou veškeré informace se zakázkovými zařízeními a podporou velkých možností k provedení útoku. Pokud bude útok dostatečně masivní, nelze se proti němu úspěšně bránit.

2.2.5 Dopad konkrétních hrozeb I

Dopad hrozeb je odhadem očekávané ztráty pro různé strany, když je bezpečnostní incident úspěšný. Úspěšným incidentem se tady rozumí očekávané možnosti ztrát, poškození, atp. na základech jednotlivých údajů uvedených v Tab. 2.3 a popisy pro každý parametr a jejich hodnoty.

Zde jsou použity čtyři faktory, kde jsou stanoveny parametry jako Závažnost (**Severity**), Provozní (**Operational**), Finanční (**Financial**) a Ochrana soukromí / Legislativní (**Privacy**). Tabulka 2.2 uvádí jejich úrovně dopadů, zařazených do pěti úrovní od 0 (žádná) do 4 (kritická).

Tab. 2.4 Dopad Útoků I

Dopad útoků **I**			
Závažnost (S)	**Provozní (O)**	**Finanční (F)**	**Legislativní/Osobní (P)**
S0	O0	F0	P0
S1	O1	F1	P1
S2	O2	F2	P2
S3	O3	F3	P3
S4	O4	F4	P4

Zdroj: [18 Controllability-aware TARA].

Závažnost S

- S0 – Dopad útoků s hodnocením 0 patří mezi drobnější závažnosti. Například sem spadají závažnostní dopady, které neohrozí funkcionalitu ani bezpečnost ale pouze omezení dostupností některých funkcí jako jsou třeba delší odezvy při připojení.
- S1 – Závažnosti mají za následky znepřístupnění některých funkcí tak, že nejsou uživateli k dispozici. Například znemožnění zapnutí tempomatu.
- S2 – Závažnost dopadů třídy 2 jsou dopady středních hodnot, kdy je možné kupříkladu zjistit nefunkčnost některých funkcí.
- S3 – Tyto závažnosti jsou kritické a mohou vést k znepřístupnění funkcí zajišťující chod vozidla a tím způsobit smrt.
- S4 – nejvíce závažné jsou ty, které přímo směřují k úmyslům usmrtit ve více vozidlech.

Provozní O

- O0 – Tyto dopady nemají téměř žádný vliv na provoz vozidla. Stejně jako u závažnosti se jedná pouze o delší odezvy, atp.
- O1 – Drobné dopady, které nemají přímý vliv na ovladatelnost vozidla.

- O2 – Provozní dopad této kategorie má vliv většinou na jednu nebo pár funkcí které mají přímý vliv na funkčnost autonomního vozidla. Například se jedná o znepřístupnění funkce ALKS, kde jí nelze aktivovat.
- O3 – Provozní dopady, které ovládají základní bezpečnostní a ovládací funkce vozidla.
- O4 – Tyto dopady mají konkrétní cíle a většinou se jedná o ovládnutí vozidla v celé jeho šířce.

Finanční F

- F0 – Dopady finanční jsou minimální spíše žádné.
- F1 – Finanční dopad hodnoty 1 jsou většinou drobné a jedná se vyřešení například updatu pro zpřístupnění konektivity.
- F2 - Drobnější nehody, nebo poškození vozidla a jeho funkcí.
- F3 – Zde jsou dopady většinou materiální při autonehodách.
- F4 – Obrovské finanční dopady. Jedná se o finančně nejnáročnější dopady a může dojít až k bankrotu firmy, rozsáhlé ztráty trhů, apod..

Osobní/Legislativní P

- P0 – Dle J3061 zde nedochází k porušení soukromí nebo legislativních předpisů
- P1 – Jedná se kupříkladu o porušení soukromí konkrétního účastníka, případně o porušení právních předpisů bez finančních následků
- P2 – Zde dochází ke ztrátám osobnějších dat souvisejících například s GDPR jako je ztráta, nebo předstírání jiné identity a porušení legislativních předpisů za účelem finančního poškození
- P3 – Ztráta integrity dat přímo vedoucí ke ztrátám finančním, data ohledně vozidla a jeho zabezpečení
- P4 – Tyto ztráty jsou nejvážnější a přímo ohrožují nejen zabezpečení vozidla, ale dochází k úniku citlivých dat výrobce, nebo skupiny uživatelů a následnému přímému ohrožení podniku (ztráta důvěry, pověsti, ztráta know-how, …). Patří sem také legislativní dopady s porušováním nařízení a legislativy.

2.2.6 Dopad útoku (MI) a výpočet

$$\boldsymbol{MI = 3 * S + F + 2 * O + P} \tag{2.2}$$

zachycuje ztrátu pro dané parametry. Jeho hodnota se počítá jako součet čtyř I faktorů (definovaných v Tab. 2.4). Pro závažnostní a provozní dopadové faktory byly nastaveny vyšší váhy, jelikož tyto parametry mají vyšší prioritu.

Výsledné MI má celočíselnou hodnotu v rozsahu [0, 28] a představuje dopad útoku. Hodnota dopadu útoků **MI** je dále podle hodnoty rozsahu modifikována na parametr **MIx,** kde x je rozsahem úrovní od MI0, který má hodnotu dopadu (**Žádný)** až po MI4 kde je hodnota dopadu (**Kritický)**.

Tab. 2.5 Dopady útoků (modifikace)

Modifikace dopadů útoků		
Modifikovaná hodnota dopadu	**Hodnocení**	**Dopad**
$0 \leq MI \leq 4$	MI0	Žádný
$4 < MI \leq 9$	MI1	Nízký
$9 < MI \leq 18$	MI2	Střední
$18 < MI \leq 28$	MI3	Vysoký
$24 < MI \leq 28$	MI4	Kritický

Zdroj: [18 Controllability-aware TARA].

2.2.7 Tabulka stanovení na úrovně rizika

Kombinací pěti možných hodnot pravděpodobnosti útoku (Pr) s pěti možnými hodnotami modifikovaného dopadu (MI) je riziko spojené s útokem (R) také klasifikováno do pěti úrovní, a to „QM“ (Quality Management), kterou je označena nejnižší úroveň rizika, a tudíž by měla být eliminována již zavedenými procesy, a nejvyšší hodnota je označena Kritická.

Tab. 2.6 Dopad útoků a modifikace dopadů

Modifikace dopadů + úrovně rizika						
Hodnota rizika (R)		**Pravděpodobnost útoku**				
		Pr0	**Pr1**	**Pr2**	**Pr3**	**Pr4**
Modifikovaná hodnota dopadu (MI)	**MI0**	QM	QM	QM	QM	Nízká
	MI1	QM	Nízká	Nízká	Nízká	Střední
	MI2	QM	Nízká	Střední	Střední	Vysoká
	MI3	QM	Nízká	Střední	Vysoká	Vysoká
	MI4	Nízká	Střední	Vysoká	Vysoká	Kritická

Zdroj: [18 Controllability-aware TARA].

V této tabulce je zobrazení dopadů a pravděpodobnost útoku.

Veškeré hodnoty a tabulky jsou navrženy dle SAE J3061 společně s normou ISO 21434 pro kybernetickou bezpečnost. Jednotlivé útoky a hrozby jsou uvedeny dle předchozích zkušeností a znalostí dané problematiky a jsou doplněny o parametry uvedené v návrhu normy ECE/TRANS/WP.29/2020/79 (EHK 155).

Jelikož bývají tyto analýzy sestavovány týmy odborníků ze všech možných oblastí, mají tudíž tito odborníci široký rozhled a zkušenosti, takže mohou objektivněji posoudit možná rizika s jejich dopady tudíž je třeba pro potřeby této metodiky zvolit přísnější měřítko.

Veškeré parametry v TARA analýze jsou voleny vzhledem k dostupnosti informací a vlastních zkušeností. Tyto parametry jsou voleny a posuzovány s přísnějším hodnocením tak, aby mohla být zajištěna větší robustnost a ochrana.

2.3 Rozbor TARA analýzy a možnosti užití penetračních testů.

Parametry v TARA analýze se zvolily tak, aby byl zastoupen každý parametr pro názornost. V obecném měřítku platí, že čím více parametrů a jejich třídění je zvoleno či sestaveno, tím spíše se dá každý jednotlivý útok, problém, nebo incident zahrnout do středního rizika.

V TARA analýze je zvoleno příkladových 20 ID odrážejících jednotlivé druhy útoků se všemi parametry, jež jsou výše zmíněné. Každý parametr byl uvážlivě volen s ohledem na zvolenou strukturu vozidla. Jednotlivé systémy jsou porovnány v závislosti

na uvedených parametrech a na útok je nahlíženo dle popisu útoku buď jako na útok na samostatnou jednotku, nebo jako na komplex jednotlivých prvků či komunikační kanály.

V obecném měřítku platí, že opatření, které se nevyzkouší, nefunguje, nicméně z hlediska normy se každé opatření vyzkoušet musí a to dokonce několikrát - v průběhu zadání formou verifikace - ověření specifikace na různých úrovních a po implementaci opět v rámci postupné verifikace a nakonec v rámci validace.

Proto se rozdělí tyto útoky na skupiny a dále k těmto skupinám budou přiřazeny skupiny penetračních testů:

2.3.1 Bezdrátová konektivita

Jelikož drtivá většina útoků se odehrává za použití komunikačních kanálů, jako jsou Wi-Fi, Bluetooth a 5G, je nutné rozebrat si tyto útoky a zvolit vhodné penetrační testy.

Ohledně konektivity je důležité zohlednění, v jaké konfiguraci dochází k útokům. Pokud se jedná o autonomní vozidlo, které jede v autonomním režimu a je aktuálně v plné konektivitě tak, že je připojené k 5G, Bluetooth, Wi-Fi, GPS, … či kombinacím těchto konektivit, je důležité nasazení penetračních testů s využitím těchto konektivit a jejich kombinací v pokusech o prolomení.

Jednalo by se například o test útoku Denial of service, kde by se pomocí penetračních testů prostřednictvím 5G sítě pokoušelo znepřístupnit funkce. Poté by se testoval tento útok pomocí Wi-Fi, či jiných možných konektivit podle možností systému, samozřejmě v závislosti na průběžných výsledcích testů. Testování pomocí připojení více jednotek a prolomení či zahlcení systému. Pokusy o jednoduchá prolomení komunikace pomocí aplikací běžně dostupných na webu.

Další sady testů lze aplikovat na konektivitu Bluetooth. Může se útočit pomocí různých operačních systémů připojených přes rozhraní Bluetooth. Pokusy se provádí také pomocí různých verzí. Testy s cílem zmatení ovládání případně zahlcení pomocí připojování zařízení a zkoušky vícenásobného připojení, popřípadě připojení více jednotek a testování prioritizace připojených jednotek.

Mezi opatření pro takové útoky může být třeba nepřijmout verzi SW aktualizace na základě CRC nebo jména souboru.

Při zjištění útoku na konektivitu uvedení autentizace jiným kanálem (SMS, e-mail), v kritickém případě použít pomocí e-call, dispečink.

Pokud dojde u Wi-Fi k rozpoznání zpoždění komunikace na základě odezvy, vozidlo musí dle EHK 155 mít zajištěný proces k monitorování útoku, ale nemusí informovat o této skutečnosti vlastníka. Dle EHK 155 není třeba informovat vlastníka, ale z hlediska bezpečnosti by bylo dobré zavedení tohoto informování.

GPS jednotku lze otestovat pomocí penetračních testů, jako jsou překrytí výhledu GPS lokátoru. Zarušení GPS respektive signálu GNSS (označení pro každý satelitní systém, který se používá pro přesné určení geografické polohy uživatele kdekoli na zemi), který bude rušen pomocí jiného radaru, nebo zdroje signálu, přerušení komunikace se satelity, odpojení lokátoru. Podstrčení nesprávného času, či jiného časového pásma, přehrání mapových podkladů, zmatení pomocí určení aktuální polohy vozidla (vozidlo se zobrazuje ve špatném směru). Záměna lokalizační jednotky za jinou (silnější, slabší), připojení nahrávací jednotky k lokátoru GPS pro posílání a mapování aktuální polohy.

Pro GNSS platí, že slouží jako časová synchronizace, zajišťující jednotný čas pro všechny prvky v dopravním systému. I když je to tak, není jednoduché provedení testů na tento druh bezdrátového připojení, jelikož vozidla nikdy nespoléhají pouze na určení polohy, ale současně se snaží rozpoznat objekty a věci kolem sebe a na ty reagovat.

Na tuto problematiku lze aplikovat testy pomocí deaktivace veškerých ostatních senzorů a pomocí nejrůznějších „překážek“ (vozidel, …) zmást systém, jelikož se rozhoduje pouze na základě těchto objektů a vzdáleností k nim. „*Vozidlo, které se rozhoduje pouze na základě svých relativních polohových informací „vidí“ překážky ve svém okolí a zná vzdálenosti k nim, nebude mít možnost projet úsekem nebo včas reagovat na překážky, které přímo „nevidí“(mohou být několik vozidel před ním)“*. [21 str. 24]

2.3.2 Drátová konektivita

Použití například u konektivity s možností připojení síťového kabelu. Penetrační testy se sadami různých kabelů. Různě poškozené kabely, různé varianty kabelů (stíněné, nestíněné), pokusy o propojení nekompatibilních kabelů.

U dalších drátových konektivit se lze zaměřit na OBD připojení a zde se pokoušet různými „hlavami“ neboli jednotkami pokusit prolomit CAN-Bus komunikaci a posílat zprávy do komunikace. Penetrační sada testů může také obsahovat fyzické rozebrání

konektoru a přímé propojení na dráty. Použití dalších vhodných gateway jednotek k propojení komunikací a pokusy o získání dat, odesílání dat, …

Při připojení USB jednotky (možnost připojení do infotainmentu, kde lze ovládat spuštění či deaktivaci ALKS) lze aplikovat testy s cílem softwarových updatů, které nemusí být autorizované, ale ani škodlivé. Jde o testy robustnosti a odolnosti proti neautorizovaným aktualizacím a při nesplnění podmínek pro možnost aktualizací. U těchto testů s může jednat také o pokusy penetrace aktualizací například za jízdy, případně při používání cílené funkce, která se má aktualizovat. Připojování médií, které nejsou podporovány aktuální konfigurací (velikost USB flash disku, připojení externího disku, použití USB 2.0 a USB 3.0). Používání spustitelných souborů, různé druhy virů, či nesmyslně dlouhé názvy nebo adresáře.

Další sadou jsou pokusy o deformaci aktualizací a poškození v průběhu. Odpojování a připojování médií s daty pro aktualizaci, mazání knihoven s daty z nové aktualizace, nahrazování těchto souborů, pokusy o instalaci nižších verzí apod.

2.3.3 Kamera

Nedílnou součástí systému ALKS ve vozidle je i kamera. Tato kamera se může stát cílem kybernetického útoku, a proto je třeba aplikovat sady penetračních testů. Jednotlivé sady by měly obsahovat možnosti ke snížení účinnosti, či zmatení této kamery.

Testy mohou probíhat formou zasvícení kamery infra - laserem o různé intenzitě i barevné škále. Použití dezorientačního dopravního značení ke zmatení kamery. V tomto případě lze také aplikovat testování na downgradování softwaru kamery. Fyzické odpojení kamery a pokusy o výměnu kamery samotné za neautorizovanou, případně pokusy o zapojení terminačních odporů, nebo vložení jednotky na čtení a odesílání dat mezi kameru a její zapojení. Mohou se také vyzkoušet penetrační testy, které jsou zdánlivě jednoduché, ale mohou mít fatální dopady. Mezi tyto jednoduché testy patří zejména oslepení kamery a jejího výhledu. Znečištění čočky kamery, snížení viditelnosti přidáním sluneční clony na sklo vozidla.

Tyto útoky lze zmírnit pomocí mapových podkladů a jejich dat. Pro použití dbát na jejich časté a ověřené aktualizace. Tyto mapové podklady a data také musí podléhat vhodnému testování.

2.3.4 Radar

U radaru je testování penetračních testů obtížnější, avšak jsou zde parametry testů, které umožňují variabilitu testů. Dle druhu radaru se lze zaměřit na jeho frekvenci. Pokud se jedná o Short - range radar, jeho optimální frekvence je 24GHz do vzdálenosti zhruba 30m, ale pokud se jedná o Long - range radar, jeho frekvence využívá rozmezí 76-81GHz, kde jeho dosahy jsou okolo 150m.

Podle druhu radaru se dají použít penetrační testy s pokusy o zarušení odrazivosti na základech vysílání po stejné frekvenci, a pokusy se změnami zarušovací frekvence.

2.3.5 Autorizace

Nesmí se zapomínat také na lidský faktor, který stojí za každým incidentem, jelikož je to právě lidské selhání, které umožňuje bezpečnostní incident. V případech úmyslných, kdy je vědomě umožněn, nebo proveden útok, tak i v případech neúmyslných, jako jsou třeba případy zneužití oprávněných a zasvěcených osob, či únik informací při změně vlastníka vozidla.

Na tyto útoky lze užít penetrační testy s variabilitou měnění identit pro užívání funkcí ve vozidle a pokusy o získání dat předchozí identity. Penetrace pomocí malwarových souborů nahrávaných pomocí médií. Vkládání nepodporovaných formátů a pokusy o jejich spuštění a tím způsobené narušení jednotek.

Úspěšnou obranou na tyto útoky by mělo být víceprvkové ověřování, ochrana jednotlivých dat od vývoje po after - market, kontrola dokumentace ohledně zajištění bezpečnosti přenosu dat a ověřování oprávnění oprávněných lidí, a dalších podobných testů a auditů dokumentací.

Možnost opatření pomocí řízeného přístupu osob, zákaz použití osobního vybavení (USB flash disky, atp.), osobních prohlídek (omezení pohybu po fabrice na výrobní lince, průchod přes brány) samozřejmě s informovaným souhlasem všech zúčastněných.

2.3.6 Komunikace jednotek

Při reverse inženýringu dochází k zneužití dat pro možnost kopírování a získání technického náskoku konkurenční firmou.

Zde se může použít gateway pro možnost propuštění a získání dat z komunikace. Změna jednotlivých prvků systému. Získání a dešifrování jednotlivých zpráv při komunikaci

mezi jednotkami. Získání softwarové a hardwarové struktury. Přímé propojení komunikačních kanálů s možností čtení. Využití komerčních firem pro možnosti nahrávání zpráv.

Je třeba chránit ECU jednotky a jejich komunikace pomocí šifrování a ověřování dat s autentizacemi. Ochrana databází k dekódování zpráv a signálů.

2.3.7 Kryptografické technologie

Používání kryptografických technologií sebou nese velké riziko, které je zohledňováno nejčastěji u většiny jednotek a přístupů. Na tyto technologie pamatuje nejen norma ISO/SAE 21434, ale i výrobci samotní. Při pokusech kybernetických útočníků jsou kryptografické technologie častým terčem, proto je nezbytnou nutností udělat vše pro nepropustnost těchto technologií, a to jak za pomoci penetračních testů, kde lze provádět opakované pokusy o průlom až po neustálou aktualizaci těchto technologií.

Útoky metodou Sybil, kdy se útočník vydává za více identit naráz. Tato metoda může poskytnout nepravé informace a zapříčinit tak směrování zpráv a tím umožnit útok.

Pro použití penetračních testů musejí být prioritou pokusy o detekování zašifrovaných souborů, extrahování šifrovacích klíčů a hesel z paměti.

Pro ochranu kryptografických technologií je nejdůležitější neustálá kontrola a inovace zejména kryptografických klíčů. Tyto klíče se musejí udržovat neustále aktualizované a stále držet v patrnosti jejich inovace. Další nezbytným faktorem těchto klíčů je jejich složitost a zde platí, že čím složitější tyto klíče budou, tím se více zvýší jejich ochrana a možnost jejich použití.

2.3.8 Zřejmé útoky

Zohledňují se zde útoky, které jsou považovány za zřejmé a samozřejmé. Mezi tyto útoky patří nejčastěji zachytávání informací, rušení signálů, škodlivý SW na USB připojený do portů, …

Penetračními testy se ověří, zda ve vozidle nejsou žádné volné porty, a to ani fyzické porty, které by umožňovaly přístup do systému, nebo jednotek. Zamezení fyzických portů zejména pro produkční verze.

Veškeré konektory, a to především konektory na senzorech jako na radaru a kameře. Tyto vstupy musí být specializované či zakázkové a jejich připojení chráněno šifrováním

na nejvyšších úrovních případně udělat vstupy pouze virtuální a jejich přístup šifrovat a chránit zabezpečovacím vícenásobným ověřováním.

2.3.9 Náročnější útoky

Tyto útoky jsou málo pravděpodobné, avšak musí se s nimi také počítat. U těchto útoků se zaměřuje útočník cíleně na vzdálenou manipulaci s daty, případně na úpravu SW či jejich aktualizací, a to zejména pomocí OTA aktualizací. Jedná se o globální útoky cílené na větší množství vozidel a tudíž k velkému potenciálu útoku.

Jedná se především o útoky s cílem ovládnout vozidla, nebo jejich části. Další útoky jsou snaha o ovlivnění dat při přenosu mezi jednotkami, nebo senzory. Patří sem také narušení V2X komunikací.

Proto se penetrační testy v této části musí zaměřit na tyto parametry a pokus o jejich ovládnutí nebo změnu. Penetrační testy pro tyto účely jsou náročné a vyžadují veškeré možné informace a specializované nástroje pro možnosti prolomení.

Ochrana těchto dat je maximální prioritou výrobců pro zajištění integrity a robustnosti dat a systémů. Pokud by nebyla tato data dostatečně chráněna, nemohla by být ani zajištěna ochrana vozidel, a to nejen v autonomním režimu, ale například i při aktivaci do tohoto režimu. Jejich ochrana proti manipulaci s aktualizacemi lze podmínit platnou autorizací, případně podmínkou přihlášení a monitoringem po celou dobu manipulace až do úspěšného odhlášení. Dalším opatřením je zamezení dalšího pohybu vozidel při manipulaci s těmito daty viz kapitola 1.7.5 EHK156. V praxi to znamená, že aktualizace či servisní zásahy do citlivých dat se smějí provádět pouze při vypnutém motoru a statickém vozidle, nebo při zjištění s narušením bezpečnosti nouzové odstavení za podmínek bezpečných pro provoz.

2.3.10 Další možnosti

Patří sem především záměna jednotek, rušení signálu dálkových ovladačů, pokusy o připojení se na OBD pomocí neoriginálních diagnostik, … U těchto variant je důležitým faktorem jejich uvedení ve vyčerpávající TARA analýze. Pokud jsou tyto útoky zmíněny, je třeba se zaměřit i na ně a ověřit, zda výrobce pamatuje i na ně.

Poté by mělo být riziko úspěšného útoku minimalizováno ve větší míře. Je důležité také tyto „samozřejmé“ možnosti útoků otestovat při procesu schvalování. S ohledem

na vyjádření certifikační laboratoře vzhledem ke struktuře, dokumentace a TARA analýze.

Popisy oblastí možných útoků a užití penetračních testů a související metody ke zmírnění zranitelnosti nebo útoku jsou uvedeny v následující přehledové tabulce. Zde je uveden rámec výčtu parametrů, na jejichž základě lze vytvářet přehledné tabulky pro užití penetračních testů pro další použití. Tento návrh slouží jako přehled oblastí a na ně aplikovatelné penetrační testy.

Tab. 2.7 Návrh rámce volby penetračních testů

Oblast útoku	**Penetrační testy**	**Zmírnění**
Bezdrátová komunikace	Denial of service – znepřístupnění funkcí	Možné odmítnutí funkce
	Pokusy o prolomení systému	Autorizace a vícenásobné ověřování
	Zmatení ovládání případně zahlcení pomocí připojování zařízení a vícenásobné připojení popřípadě připojení více jednotek	Znemožnění připojení více jednotek
	Testy s připojením různých operačních systémů a různých verzí	Zajištění SW kompatibility
	Testy na podstrčení SW při aktualizaci	Nepřijmout verzi SW aktualizace na základě CRC nebo jména souboru
	Záměny lokalizačních jednotek	Ověřování jednotlivých jednotek a znemožnění záměny bez autorizace
	Zarušování GPS lokátoru	Ověřování na základě více impulzů
	Fyzické překrývání lokátorů	
	Podstrčení a změny času u GNSS	
	Záměny prioritizací signálů u jednotlivých konektivit	Prioritizace přímo související s funkčností systému

	Prolomení SW ochrany pomocí běžně dostupných aplikací na webu	Autorizace a vícenásobné ověřování
Drátová konektivita	Připojování pomocí různých kabelů a různých stavů (poškození, kompatibility, stínění)	Znemožnění připojení, kompatibilita pouze podporovaných kabelů
	Připojování neautorizovaných hlav pro OBD	Podpora servisních jednotek, šifrování komunikačních kanálů a zpráv
	Posílání a poslouchání zpráv v CAN-Bus	Šifrování zpráv, autorizace komunikace
	Připojování USB jednotek o různých velikostí a rychlostí připojení	Odmítnutí nekompatibilních jednotek
	Používání spustitelných souborů, různé druhy virů	Ověřování formátů a obsahů. Separace od hlavních komunikačních kanálů
	Nesmyslně dlouhé názvy nebo adresáře	
Senzory	Zasvícení laserem	Ověřování na základech referenčních dat a
	Zmatení pomocí podstrčení objektů	
	Použití znečištění výhledu senzorů	

	Přidávání sluneční clony	pomocí mapových podkladů a dat
	Zarušení odrazivosti pomocí různých frekvencí a frekvenčních rozsahů	
	Záměny senzorů	
	Vícenásobné odpojování kamery	Odolnost jednotky, případně deaktivace senzoru
Autorizace	Variabilita měnění identit	Více prvkové ověřování, ochrana jednotlivých dat. Zajištění přenosu dat a oprávnění pro použití dat
	Vkládání nepodporovaných formátů	
Kryptografická technologie	Opakované pokusy o prolomení	Kontrola a inovace kryptografických klíčů a jejich složitost
	Detekování zašifrovaných souborů	
	Extrahování šifrovacích klíčů a hesel z paměti	
	Útok metodou Sybil	Pro ukládání klíčů musí být použity bezpečnostní kontroly kryptografických klíčů
	Chyby v zabezpečení při vývoji	Testování při vývoji na známé chyby
	Útoky na směrování dat	Zavedení hardwarových bezpečnostních modulů
Další možnosti útoků	Ověřování volných virtuálních a fyzických portů	Dodržování bezpečnostních postupů při vývoji a výrobě. Testování všech dostupných portů

	Manipulace s daty při OTA SW aktualizaci	Autorizace, statické vozidlo po celou dobu SW aktualizace
	Narušení V2X komunikace	Robustnost sítě V2X
	Ovlivnění dat při přenosu mezi jednotkami, nebo senzory	Detekování útoku,
	Rušení signálu dálkových ovladačů	Používání různých frekvencí
	Ilegální/neautorizované změny elektronického ID vozidla	Šifrování, autorizace
	Vymazání dat z vozidla	Ochrana citlivých dat proti smazání, zálohování
	Získání dat z vozidla při změnách uživatele	Automatické odhlášení související s kompletním smazáním a uvedením do základního nastavení
	Pokusy o získání autorského nebo patentovaného softwaru ze systémů vozidla, jako jsou pirátství/odcizení softwaru	Ochrana systémových dat kódu, použití bezpečnostních kontrol
	Manipulace s údaji pro zfalšování jízdních údajů vozidla (stáčení km, rychlost vozidla, omezovače)	Korelace signálů z různých retenčních signálů a jednotek
	Únik informací neúmyslným sdílením dat chyby správce, ukládání dat na servery	Použití bezpečnostních kontrol na back-end systémy

Zdroj: vlastní zpracování.

3 Vyhodnocení návrhu rámce penetračního testování kybernetické bezpečnosti ASV

Při postupu u hodnocení robustnosti systému ALKS je třeba mít kompletní dokumentaci s podrobným popisem HW a SW struktury pro orientaci v komunikaci. Dále je třeba podrobný popis celého systému, dle kterého se dá zjistit, v jakém stavu se daná konfigurace zařízení nachází a do jakých stavů může přejít, aby se vyloučila chybná funkčnost. S touto dokumentací je třeba důkladně se seznámit a vyjasnit případné nejasnosti. Výrobce musí také komunikovat se zkušebnou, a to jak před, tak i v průběhu posuzování. Během provádění penetračních testů může být zástupce ze strany dodavatele přítomen, za předpokladu že budou splněny veškeré bezpečnostní opatření, aby nedošlo k narušení či ovlivnění testů a zároveň byla zkušebna schopna zajistit bezpečnost.

Z dat vyplývajících z předchozích šetření a rozboru je třeba zohlednit veškerá rizika uvedená v TARA analýze a podle nich by měla každá zkušebna volit ideální postup, kde zohlední jednotlivé parametry a jejich možné slabiny a zvolit optimální výběr jednotlivých vzorků k penetračním testům dle možností. Zde je třeba přihlédnout i k možnostem, které dle evropských norem ukládá případným žadatelům o schválení. Dodat potřebné komponenty (SW, HW, …) pro provedení penetračních testů dle dokumentace a popisu.

Zkušebna musí disponovat dostatečně proškoleným personálem, který se dopředu seznámí podrobně s veškerou dokumentací k danému schvalovacímu procesu.

Tito lidé musí mít veškeré informace, jak systém funguje, a možnost přístupů ke všem komponentům, a to jak na straně uživatele, tak i na straně vývojáře a možnost provádět penetrační testy.

Toto testování je třeba provádět v bezpečném prostoru. Zejména testování jednotlivých komponent v laboratorním prostředí, ale také fyzicky na uzavřeném polygonu, pokud je možné simulovat útok v tomto prostředí. V opačném případě je třeba využít laboratorních podmínek.

Pro potřeby penetračních testů na úrovni schvalování není nezbytně nutné brát v potaz jen rizika s nejvyšší mírou rizika, ale objektivně vybrat kombinaci těch, která jsou četnější, snadná, … Ideálně zahrnout všechny možné incidenty a průřezově zvolit komponenty dle TARA analýzy.

Takže pokud u některého komponentu, nebo softwaru hrozí maximální riziko s fatálními následky, ale jeho uskutečnění je obtížné a pravděpodobnost takového útoku je nízká, nemusí se nutně testovat. Pokud však komponenta disponuje vysokou pravděpodobností útoku, ale následky nejsou fatální, je tato komponenta vhodná k provedení penetračních testů.

Úkolem penetračních testů je ověřit integritu a robustnost systému a v případě úspěšného útoku při penetračním testování dostatečně posoudit riziko a následky útoku a podrobně vše zapsat a zdokumentovat.

Sestavení parametrů pro volbu těchto testů slouží vzorová tabulka 2.7, kde je příkladový výčet oblastí možných útoků a k nim vybrané penetrační testy, a jako součást této tabulky jsou návrhy na snížení rizika.

Poté je povinností této autority neprodleně (Nejpozději však do 14 dnů od provedení a vyhodnocení testů) vše zapsat v angličtině a nasdílet do DETA databáze pro další případné autority či další možnosti schvalování. Tyto úkony je třeba provádět s předešlými ověřeními, a to zejména s platnými přihlašovacími údaji do DETA.

Penetrační testování musí být zejména účelné a cílené, aby nedocházelo k ovlivnění dalších komponent v případě testování komplexnějších komponent, nebo soustav.

Co se týká penetračního testování na polygonu, kde může být testovaným komponentem auto jako komplex, je nezbytnou nutností v dostatečné míře zohlednit možné následky a jim přizpůsobit testovací podmínky, možné únikové zóny, zajistit bezpečnost pro testovací tým i případné okolí.

Pokud laboratoř zjistí při schvalovacím procesu na základech DETA databáze, odborných zkušenostech, výsledcích penetračních testů nedostatky či opomenutí důležitých parametrů v TARA analýze, nebo slabé místo, kde hrozí bezpečnostní incident, je třeba vše zdokumentovat a zanést do výsledného protokolu. V takovém případě musí výrobce

nedostatky odstranit a v případě přidání, nebo změny systémů musí vše zohlednit v TARA analýze a přizpůsobit tomu odpovídajícím způsobem parametry a robustnost k minimalizaci rizika. Poté může být opět vozidlo podrobeno zkouškám pro získání homologace.

V protokolu musí být veškeré parametry, které odpovídají nejnovějším standardům dle norem. Veškerý použitý SW, HW, i další pomůcky, které byly využity při testování, jsou zaneseny v tomto dokumentu. A jsou zde uvedeny všechna jména lidí, kteří se na testování podíleli.

Kybernetická bezpečnost má jako hlavní cíl zabránění útoku, nebo jeho rozpoznání a informování o něm. Kybernetická bezpečnost se zaobírá hrozbami, identifikuje je a na základě těchto parametrů přijme dostatečné opatření a tato opatření je třeba dostatečně otestovat pomocí penetračních testů pro minimalizování rizika. Kybernetická bezpečnost, Funkční bezpečnost a SOTIF neslouží k 100% neproniknutelnosti a ochraně, ale slouží k minimalizaci rizika a zmírnění dopadů.

Pro volby penetračních testů na základech TARA analýz je nezbytné dostatečné porozumění aktuální problematice, orientace v aktuálních předpisech a optimální výběr komponent pro otestování.

V těchto případech je také nezbytné, aby TARA analýza poskytnutá dodavatelem byla vyčerpávající a byly zohledněny veškeré možné bezpečnostní incidenty, které by mohli nastat. U takto vytvořené analýzy je třeba, aby se sešli odborníci a nahlíželi na ní jak subjektivně, tak i komplexně. Je nanejvýš důležité správné posouzení ze strany zkušebny, která bezpečnostní rizika jsou natolik závažná, případně četná, aby se na ně daly aplikovat penetrační testy a ověřila se odolnost zkoumaného sytému, nebo vozidla pro případné schválení. Testování nemusí být nutně vyčerpávající jak pro zkušební laboratoř, tak i pro dodavatele, ale musí být účelné a cílené s jasným úkolem, a to prověřit připravenost a robustnost systému či vozidla.

Po otestování se musí zhodnotit stav a výsledky posoudit dostatečně objektivně ke stanovení výsledků, zda vozidlo splnilo požadavky na kybernetickou bezpečnost dle aktuálních předpisů na kybernetickou bezpečnost autonomního vozidla a je tak způsobilé a bezpečné pro provoz. Zde je také třeba popsat, jak dodavatel u popisu hrozeb

a slabin systému a komponent zohlednil hrozby a k tomu přijal bezpečnostní opatření ke snížení rizika a dopadů v případě úspěšnosti útoku.

Je maximálně důležité být při každém procesu vnímavý k detailům a zvažovat veškeré možnosti, a to zranitelnosti, příležitosti tak i dostatečná opatření.

Riziko tzv. Potěmkinových vesnic je aktuálním trendem, a to zejména, protože dopad bezpečnostních požadavků v kombinaci s nedostatkem lidských a finančních zdrojů způsobují, že povinné subjekty se pod tíhou rizika spojeného s udělením sankcí ze stran regulací snaží za každou cenu projít auditním řízením. Jinými slovy, potenciální sankce či jiná ekonomická ztráta spojená s nesouladem s normou či standardem se stává pro organizaci rizikem v kritické úrovni, jež je třeba v ideálním případě eliminovat. [22]

Závěr

Na začátku této práce byly zadány normy s kybernetickou bezpečností autonomních systémů vozidel a tato část je popsána v kapitole 1 této práce v tématu Literární rešerše tématu testování kybernetické bezpečnosti ASV. Zde je popis norem zabývajících se kybernetickou bezpečností spolu s výčtem norem, které se zabývají kybernetickou bezpečností mimo oblast autonomních vozidel a také výčet norem, které jsou nezbytné pro zavedení kybernetické bezpečnosti.

Návrh rámce penetračního testování kybernetické bezpečnosti ASV je popsán v kapitole 2, kde je pomocí norem o kybernetické bezpečnosti aplikován návrh rámce penetračního testování autonomního systému vozidel, který je aplikován na systém ALKS a jeho možné části popsané v kapitole 2.1.

Vyhodnocení návrhu rámce penetračního testování kybernetické bezpečnosti ASV viz kapitola 3 je výsledkem návrhu penetračních testů, na jejichž základě jsou přijata opatření ke snížení rizika a dopadu útoku, nebo informování o možném útoku ať už byl úspěšný či nikoli.

Seznam zdrojů

[1] JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[2] Co? Proč? Jak? [online]. 2021 [cit. 2021-02-28] Dostupné z: Intranet https://www.tuvsud.com/cs-cz.

[3] KOHÚT, Radek. *Implementace V-modelu v Rational Team Concertu* [online]. Brno: MU, 2021 [cit. 2021-01-12] Dostupné z: https://is.muni.cz/th/dwj9y/DP_Radek_Kohut.pdf.

[4] Metody vývoje aplikací. Watefall, V-model, Inkremetální model. [Červenec 2016] [Obr. 1] V-model [online]. 2021 [cit. 2021-02-22]. Dostupné z: https://blog.iquest.cz/2017/07/metody-vyvoje-aplikaci-waterfall-v.html.

[5] Řízení kvality (Quality management) [online]. Management mania, 2018, 13. 4. 2018 [cit. 2021-02-22] Dostupné z: https://managementmania.com/cs/rizeni-kvality.

[6] TÜV NORD Nová povinnost certifikace kybernetické bezpečnosti [online]. TÜV NORD GROUP [cit. 2021-02-20] Dostupné z: https://www.tuv-nord.com/cz/cs/novinky/news-detail/article/nova-povinnost-certifikace-kyberneticke-bezpecnosti-a-bezpecnosti-aktualizace-softwarusilnicnich-vozu-jako-podminka-homologace/.

[7] TÜV SÜD CZECH s.r.o. [online]. 2021 [cit. 2021-01-20] Dostupné z: Intranet ECE/trans/wp.29/2020/79, nařízení OSN o jednotných ustanoveních pro schvalování vozidel z hlediska kybernetické bezpečnosti a jejich systémů řízení kybernetické bezpečnosti 2020-08-06.

[8] Automotive cyber security management system magility [online]. Magility, 2020 [cit. 2021-02-18] Dostupné z: https://www.magility.com/en/cyber-security-management-system-2/.

[9] Standard SAE J3061_2016 [Normen-Download-Beuth-TÜV Süd AG Verlag-KdNr.7031496-ID.DAKD0I3GALYRYYX7E7VESQJT.4-2019-05-27 16:48:18] Dostupné z: TÜV SÜD Germany GmbH intranet.

[10] TÜV SÜD CZECH s.r.o. elektronická knihovna - Návrh předpisu ECE/TRANS/WP.29/2020/79 - Návrh nového OSN předpisu o jednotných ustanoveních týkajících se schvalování vozidel s ohledem na kybernetickou bezpečnost a systém řízení kybernetické bezpečnosti EHK 155 [online]. 2021 [cit. 2021-04-12] Dostupné z: Intranet Elektronická knihovna TÜV SÜD Czech s.r.o. (tuv-sud.cz).

[11] DETA databáze [online]. UNECE, 2021 [cit. 2021-02-02] Dostupné z: https://unece.org/data-sharing.

[12] SOTIF - ISO/PAS 21448:2019 (en) Road vehicles — Safety of the intended functionality [online]. ISO [2019] [cit. 2021-02-27]. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso:pas:21448:ed-1:v1:en.

[13] Řada norem ISO 2700 [2019], [online]. ISO [cit. 2020-11-27]. Dostupné z: Intranet Elektronická knihovna TÜV SÜD Czech s.r.o. (tuv-sud.cz).

[14] EHK 156 Návrh nového OSN předpisu o jednotných ustanoveních týkajících se schvalování vozidel s ohledem na aktualizace softwaru a systém správy aktualizací softwaru. [31.7.2020] [online]. EHK/OSN [cit. 2020-12-15] Dostupné z: Elektronická knihovna TÜV SÜD Czech s.r.o. (tuv-sud.cz) EHK 156 ECE/TRANS/WP.29/2020/80.

[15] Jaroslav Šmíd, NÚKIB [online]. Prezentace Jaroslav Šmíd [cit. 2021-01-21] Národní úřad pro kybernetickou a informační bezpečnost a jeho role - O NÚKIB. Dostupné z: https://nukib.cz.

[16] TÜV SÜD CZECH s.r.o. elektronická knihovna - Návrh předpisu ECE/TRANS/WP.29/2020/81 – ALKS <EHK 157 [11.4.2020] [online]. EHK/OSN [2020-03-12] Dostupné z: Intranet Elektronická knihovna TÜV SÜD Czech s.r.o. (tuv-sud.cz).

[17] Honda ADAS system [14.12.2017] [online]. [2020-01-21] Honda sensing, Dostupné z: https://www.civicx.com/forum/attachments/guild21_12-14-2017_ adaspresentation-pdf.194102/.

[18] Anastasia Bolovinou, a kol., 2019 TARA +: Controllability-aware TARA for L3 Automated Driving Systems [únor 2017] [online]. [cit. 2021-02-23], Dostupné z: https://www.researchgate.net/publication/333520940_TARA_Controllability-aware_ Threat_Analysis_and_Risk_Assessment_for_L3_Automated_Driving_Systems.

[19] SAE J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, SAE standard, 2016 [online]. SAE International 2016 [cit. 2021-02-12] Dostupné z: https://www.sae.org/standards/content/j3061_201601/.

[20] TÜV SÜD AG Germany Mobility HAD | Automotive Cybersecurity Fundations | v0.1 | Cybersecurity Fundamentals; Dr. Mattias Wachs [Senior Expert Automotive Security Technology] [2020] [cit. 2020-11-10] Dostupné z: Intranet TÜV SÜD GmbH Germany.

[21] Ministerstvo dopravy. Akční plán autonomního řízení 2019 Praha [online]. Ministerstvo dopravy, 2019 [cit. 2021-03-06] Dostupné z: https://amsp.cz/wp-content/uploads/2019/02/Ak%C4%8Dn%C3%AD-pl%C3%A1n-autonomn%C3%ADho-%C5%99%C3%ADzen%C3%AD-ma_KORNB8UGXNR8.pdf.

[22] Radek Švadlenka 12/2020, Soulad s normou nemusí znamenat bezpečnost [online]. [cit. 2021-02-23] Dostupné z: https://www.systemonline.cz/it-security/soulad-s-normou-nemusi-znamenat-bezpecnost.htm.

Seznam grafických objektů

Seznam obrázků

Obr. 1 Co? Proč? Jak?.....11

Obr. 1.2 V-model.....13

Obr. 1.3 Celkový rámec procesu kybernetické bezpečnosti.....20

Obr. 1.4 Fáze konceptu činnosti.....22

Obr. 1.5 V-diagram pro fázi vývoje na úrovni systému.....23

Obr 1.6 V-diagram fáze vývoje na úrovni hardwaru a jeho vztah k vývoji produktu na systémové úrovni.....24

Obr. 1.7 Fáze vývoje na úrovni hardwaru.....25

Obr. 1.8 V-diagram na úrovni softwaru a jeho vztah k vývoji produktu na systémové úrovni.....26

Obr. 1.9 Fáze vývoje na softwarové úrovni.....26

Obr. 2.10 Schéma pro ALKS systém.....36

Seznam tabulek

Tab. 2.1 Potenciál útoků.....38

Tab. 2.2 Mapování potenciálu útoku k pravděpodobnosti.....39

Tab. 2.3 Popis útočníků a jejich možnosti.....40

Tab. 2.4 Dopad útoků I.....45

Tab. 2.5 Dopady útoků (modifikace).....47

Tab. 2.6 Dopad útoků a modifikace dopadů.....48

Tab. 2.7 Návrh rámce volby penetračních testů.....55-58

Seznam zkratek

ALKS	Automated Lane Keeping System - Automatický systém udržování v jízdním pruhu
ASV	Autonomní systém vozidla
BRS	Bezpečnostní rada státu
CAF	Common Assessment Framework – Běžné posouzení vývoje
CAN	Controller Area Network – Kontrolní komunikační sběrnice
CMM	Capability Maturity Model - Model zralosti schopností
CRC	Cyclic redundancy check – Kontrola opakované redundance
CSMS	Cyber Security Management System – Management kybernetické bezpečnosti
CySe	Cyber Security - Kybernetická bezpečnost
DETA	Database for the Exchange of Type Approval documentation – Databáze pro výměnu schvalovací dokumentace
EFQM	European Foundation of Quality Management – Evropská nadace pro řízení kvality
EHK	Evropská Hospodářská Komise
FuSa	Functional Safety - Funkční bezpečnost
GDPR	General Data Protection Regulation – Obecné nařízení o ochraně údajů
GNSS	Global Navigation Satellite System - Globální družicový systém
HW	Hardware
INFOSEC	Informační bezpečnost v komunikačních a informačních systémech resortu Ministerstva obrany
ISMS	Information Security Management System – Systém řízení bezpečnosti informací
ISO	International Organization for Standardization – Mezinárodní organizace pro normalizaci

IT	Informační technologie
NÚKIB	Národní úřad pro Kybernetickou Bezpečnost
OBD	On-board diagnostics – Palubní diagnostika
OTA	Over the Air – Bezdrátově (vzduchem)
PRS	Public Regulated Service – Veřejná regulovaná služba
SOP	Start of Production – Začátek produkce
SOTIF	Safety Of The Intended Functionality – Bezpečnost zamýšlené funkce
SW	Software
TARA	Threat Assessment and Remediation Analysis (Threat Analysis and Risk Assessment dle J3061) – Posouzení hrozeb a analýza rizik
V2I	Vehicle to Infrastructure – Vozidlo a infrastruktura (komunikace)
V2V	Vehicle to Vehicle – Vozidlo s vozidlem (komunikace)

Seznam příloh

Příloha A Tara analýza

Příloha A

TARA analýza

Autor	**Bc. Marek Obršál DiS.**
Název DP	**Návrh rámce penetračního testování v oblasti robustnosti kybernetické ochrany autonomního systému vozidla**
Studijní obor	**LRDP**
Rok obhajoby DP	**2021**
Počet stran	55
Počet příloh	1
Vedoucí DP	**prof. Mgr. Roman Jašek, Ph.D.**
Anotace	Cílem práce je návrh rámce penetračního testování kybernetické bezpečnosti autonomního systému vozidel. Návrh bude v souladu s relevantními bezpečnostními normami a pokyny souvisejícími s kybernetickou bezpečností (např. norma ISO/SAE 21434 o inženýringu kybernetické bezpečnosti pro silniční vozidla, SAE J3061 a ISO 24089 pro softwarové aktualizace).
Klíčová slova	automotive, kybernetická bezpečnost, ISO, penetrační testy, autonomní vozidlo, EHK
Místo uložení	ITC (knihovna) Vysoké školy logistiky v Přerově
Signatura	