

Analýza dopadu implementace normy (ISO 21434) do ASPICE procesu

Adéla Odstrčilová



Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Adéla Odstrčilová
Osobní číslo: A22139
Studijní program: B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia: Kombinovaná
Téma práce: Analýza dopadu implementace normy (ISO 21434) do ASPICE procesu
Téma práce anglicky: Impact Analysis of Implementing the ISO 21434 Standard in the ASPICE Process

Zásady pro vypracování

- Uveďte základní terminologii.
- Popište normu ISO 21434.
- Proveďte analýzu dopadu implementace normy ISO 21434.
- Na základě výsledků navrhněte opatření ke zmírnění dopadu implementace normy.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. ČSN ISO 21434. *Silniční vozidla – Kybernetické zabezpečení při vývoji*. Ženeva: Mezinárodní organizace pro normalizaci, 2021.
2. SMITH, JOHN. *Automotive Cybersecurity Engineering Handbook*. 1. vydání. New York: CyberTech Press, 2023. ISBN 978-1-2345-6789-0.
3. ČSN ISO 26262. *Silniční vozidla – Funkční bezpečnost*. 2. vydání. Ženeva: Mezinárodní organizace pro normalizaci, 2018.
4. UNECE. *Předpis č. 155 – Kybernetická bezpečnost a systém řízení kybernetické bezpečnosti*. Ženeva: Evropská hospodářská komise OSN, 2021.
5. UNECE. *Předpis č. 156 – Aktualizace softwaru a systém řízení aktualizací softwaru*. Ženeva: Evropská hospodářská komise OSN, 2021.

Vedoucí bakalářské práce: **Ing. Dora Kotková, PhD.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **23. listopadu 2024**

Termín odevzdání bakalářské práce: **2. června 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 23. listopadu 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Tato bakalářská práce zpracovává problematiku analýzy dopadu implementace normy ISO 21434 do procesního rámce ASPICE ve verzi 3.1 v oblasti automobilového průmyslu.

Hlavním cílem práce je identifikace klíčových oblastí, které proces ASPICE nepokrývá z pohledu kybernetické bezpečnosti a určení požadavků plynoucích z ISO 21434, které je nutné do procesů doplnit. Při výzkumu bude využito komparativní analýzy a analýzy dopadu k posouzení a řešení dané problematiky.

Výsledky ukazují, že integrace této normy je velmi komplexní aktivitou a vyžaduje úpravy v oblastech, jako je řízení rizik, bezpečnostní požadavky a také lidské zdroje či organizační struktura. Zjištění této práce poskytují užitečné informace pro společnosti v automobilovém průmyslu, které usilují o efektivní sladění obou standardů s cílem zvýšit celkovou kybernetickou bezpečnost vyvíjených systémů.

Klíčová slova: ISO 21434, ASPICE, kybernetická bezpečnost, analýza dopadu, automobilový průmysl, řízení rizik, bezpečnostní opatření

ABSTRACT

This bachelor's thesis addresses the impact analysis of implementing the ISO 21434 standard into the ASPICE 3.1 process framework within the automotive industry.

The main objective of the thesis is to identify key process areas not currently covered by ASPICE from the perspective of cybersecurity and to determine the requirements derived from ISO 21434 that need to be integrated. The research applies comparative analysis and impact assessment to evaluate and address the issue.

The findings indicate that integrating the standard is a highly complex activity requiring adjustments in areas such as risk management, security requirements, human resources, and organizational structure. The results of this work provide valuable insights for companies in the automotive industry aiming to effectively align both standards in order to enhance the overall cybersecurity of developed systems.

Keywords: ISO 21434, ASPICE, cybersecurity, impact analysis, automotive industry, risk management, security measures

„Any sufficiently advanced technology is indistinguishable from magic“ – Arthur C. Clarke

OBSAH

ÚVOD.....	13
I TEORETICKÁ ČÁST	14
1 ÚVOD DO PROBLEMATIKY	15
1.1 ROZDÍL MEZI KYBERBEZPEČNOSTÍ A FUNKČNÍ BEZPEČNOSTÍ.....	15
1.2 HROZBY SPOJENÉ S KYBERNETICKOU BEZPEČNOSTNÍ AUTOMOBILŮ.....	16
1.2.1 Kybernetické útoky	16
1.2.2 Útoky na komunikační systémy	17
1.3 POPTÁVKA PO ŘEŠENÍ PROBLEMATIKY	18
1.3.1 Rostoucí počet připojených vozidel.....	18
1.3.2 Tlak na automobilové výrobce.....	19
1.4 ZÁKONY A REGULACE	19
1.5 SHRUTÍ PRVNÍ KAPITOLY	22
2 ZÁKLADNÍ TERMINOLOGIE.....	23
2.1 OBECNÉ ZÁKLADNÍ POJMY	23
2.1.1 Aktivum.....	23
2.1.2 Hrozba	24
2.1.3 Zranitelnost	24
2.1.4 Riziko	25
2.1.5 Bezpečnostní opatření	25
2.1.6 Zmírňování rizik.....	25
2.1.7 Analýza dopadu.....	26
2.1.8 Řízení životního cyklu produktu.....	26
2.2 KOMPONENTY A TECHNOLOGIE VOZIDEL	27
2.2.1 Embedded systém.....	27
2.2.2 Firmware	28
2.2.3 Elektronická řídicí jednotka	28
2.2.4 Komunikační sběrnice CAN	29
2.2.5 Telematická jednotka	30
2.2.6 Bezdrátová aktualizace softwaru.....	30
2.3 METODY A POSTUPY V OBLASTI KYBERNETICKÉ BEZPEČNOSTI	30
2.3.1 Analýza hrozeb a hodnocení rizik.....	30
2.3.2 Správa zranitelností.....	31
2.3.3 Plán reakce na incidenty.....	31
2.4 KLÍČOVÉ POJMY A KONCEPTY V ASPICE PROCESU.....	31
2.4.1 Model referenčních procesů.....	31
2.4.2 Základní praktiky	31
2.4.3 Pracovní výstupy	32
2.4.4 Sledovatelnost požadavků.....	32
2.4.5 Stanovení úrovně způsobilosti	32
2.4.6 Úrovně způsobilosti	32

2.4.7	Přizpůsobení procesů.....	33
2.5	KLÍČOVÉ POJMY A KONCEPTY Z NORMY ISO 21434	34
2.5.1	Identifikace aktiv	34
2.5.2	Cíle kybernetické bezpečnosti	34
2.5.3	Scénáře hrozeb.....	34
2.5.4	Úroveň zajištění kybernetické bezpečnosti	34
2.5.5	Security-by-Design.....	35
2.5.6	Monitorování a záznamy	35
2.5.7	Zbytkové riziko	36
2.5.8	Systém řízení kybernetické bezpečnosti.....	36
2.6	SHRNUTÍ DRUHÉ KAPITOLY	36
3	PŘEHLED PROCESU ASPICE	37
3.1	HISTORIE	37
3.2	ÚČEL	38
3.3	V-MODEL	38
3.4	STRUKTURA.....	39
3.5	DÍLČÍ OBLASTI PROCESU	41
3.5.1	Vstupy jednotlivých procesů	42
3.5.2	Výstupy jednotlivých procesů	42
3.6	DOSTUPNÁ ROZŠÍŘENÍ	43
3.6.1	ASPICE for Hardware Engineering	43
3.6.2	ASPICE for Cybersecurity	44
3.7	SHRNUTÍ TŘETÍ KAPITOLY	45
4	POPIS NORMY ISO 21434	46
4.1	HISTORIE	46
4.2	ÚČEL	46
4.2.1	Odlišnosti od jiných standardů kybernetické bezpečnosti.....	46
4.3	STRUKTURA.....	47
4.4	ŽIVOTNÍ CYKLUS PRODUKTU	48
4.5	ROLE A ODPOVĚDNOSTI V RÁMCI NORMY	49
4.6	VZTAH K OSTATNÍM NORMÁM, VYHLÁŠKÁM A REGULACÍM	49
4.6.1	UNECE Předpis č. 155 a Předpis č.156	50
4.6.2	ISO 26262.....	50
4.6.3	ISO 27001	50
4.7	SHRNUTÍ ČTVRTÉ KAPITOLY	50
II	PRAKTICKÁ ČÁST	51
5	CÍL PRÁCE	52
6	KOMPARATIVNÍ ANALÝZA POŽADAVKŮ NORMY ISO 21434 A VÝCHOZÍHO STAVU PROCESU ASPICE.....	53

6.1	ANALÝZA VÝCHOZÍHO STAVU ASPICE	53
6.1.1	Nedostačující řešení problematiky	54
6.2	ANALÝZA POŽADAVKŮ ISO 21434	54
6.3	VÝSLEDEK KOMPARATIVNÍ ANALÝZY	56
6.4	SHRNUTÍ ŠESTÉ KAPITOLY	57
7	ANALÝZA DOPADU	59
7.1	NOVÉ ČINNOSTI A PROCESY VYŽADOVANÉ IMPLEMENTACÍ ISO 21434	59
7.2	DOPADY IMPLEMENTACE NA ORGANIZAČNÍ STRUKTURU A KOMPETENCE	60
7.3	DOPADY IMPLEMENTACE NA NÁSTROJE A TECHNICKÉ INFRASTRUKTURY	60
7.4	DOPADY IMPLEMENTACE NA VÝKONNOST, NÁKLADY A PLÁNOVÁNÍ PROJEKTŮ	61
7.5	VÝSLEDEK ANALÝZY DOPADU	63
7.6	VZTAH VÝSLEDKU ANALÝZY DOPADU S VÝSLEDKY KOMPARATIVNÍ ANALÝZY	65
7.7	SHRNUTÍ SEDMÉ KAPITOLY	65
8	DOPADY IMPLEMENTACE NA PROCES ASPICE	67
8.1	DOPADY NA PROCESNÍ OBLASTI	67
8.1.1	SYS.2 a SYS.3	67
8.1.2	SWE.1 až SWE.6	69
8.1.3	MAN.5	70
8.1.4	SUP.1, SUP.9 a SUP.10	71
8.2	DOPADY NA NÁSTROJE A TESTOVACÍ STRATEGIE	73
8.3	DOPADY NA LIDSKÉ ZDROJE A KOMPETENCE	74
8.4	PŘEHLED PŘÍČIN A NÁSLEDKŮ – ISHIKAWA DIAGRAM	75
8.5	SHRNUTÍ OSMÉ KAPITOLY	76
9	NÁVRH OPATŘENÍ PRO ZMÍRNĚNÍ DOPADŮ IMPLEMENTACE NORMY	78
9.1	OPATŘENÍ V OBLASTI PROCESŮ	78
9.2	OPATŘENÍ V OBLASTI LIDSKÝCH ZDROJŮ A KOMPETENCÍ	79
9.3	OPATŘENÍ V OBLASTI NÁSTROJŮ, TECHNOLOGICKÉ INFRASTRUKTURY A TECHNICKÉHO TESTOVÁNÍ	80
9.4	OPATŘENÍ V OBLASTI PROJEKTOVÉHO ŘÍZENÍ A PLÁNOVÁNÍ	81
9.5	SHRNUTÍ DEVÁTÉ KAPITOLY	81
	ZÁVĚR	83
	SEZNAM POUŽITÉ LITERATURY	85
	SEZNAM OBRÁZKŮ	90
	SEZNAM TABULEK	91

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	92
---	-----------

ÚVOD

S rostoucí digitalizací, automatizací a konektivitou moderních vozidel se kybernetická bezpečnost stává nedílnou součástí vývoje komponent automobilového průmyslu. Elektronické řídicí jednotky dnes umí komunikovat nejen mezi sebou, ale i s vnějším prostředím, což dává za vznik nové oblasti útoků. Výrobci automobilů a jejich dodavatelé tak čelí rostoucímu tlaku ze strany zákazníků, regulací i trhu na zavedení systematického řešení kybernetické bezpečnosti během celého životního cyklu produktu.

Na tuto potřebu reaguje norma ISO 21434, která poskytuje vhodný rámec pro identifikaci, hodnocení a zmírnění rizik v oblasti silničních vozidel. Aby však mohla být účinně zavedena do vývojových procesů, je nezbytné ji vhodně integrovat do již existujících struktur, které automobilový průmysl dlouhodobě používá, do procesu ASPICE (Automotive SPICE).

Norma ISO 21434 však výslovně neurčuje, které její požadavky mají být integrovány do struktury ASPICE, ani jak má být tato integrace provedena. Vzniká tak nejistota ohledně praktické aplikace normy – například které aktivity, výstupy nebo role odpovídají daným požadavkům na kybernetickou bezpečnost.

Cílem této bakalářské práce je provést analýzu dopadu implementace požadavků normy ISO 21434 do procesu ASPICE. Teoretická část práce se věnuje nejprve obecnému úvodu problematiky kybernetické bezpečnosti v automobilovém průmyslu, vysvětlení používané terminologie a přehledu základních komponent, které jsou z hlediska bezpečnosti relevantní. Dále jsou popsány klíčové pojmy a metodiky používané v ASPICE ve verzi 3.1 a ISO 21434. Samostatné kapitoly jsou pak věnovány podrobnému rozboru obou norem, jejich struktuře a cílům.

Praktická část je postavena na vlastním výzkumu zaměřeném na dopady implementace požadavků normy ISO 21434 do struktury procesu ASPICE. Výzkum je započat komparativní analýzou výchozího stavu ASPICE a nalezením konkrétních požadavků ISO 21434 s cílem identifikovat jejich oblast překryvu a rozporu. Na základě této analýzy je vytyčeno, které požadavky normy jsou již procesem pokryty, a které bude nutné nově implementovat. Na základě informací z komparativní analýzy je následně zpracována jejich analýza dopadu z hlediska vlivu na vývojový proces. Výsledkem je konkrétní zařazení požadavků do struktury ASPICE a doporučení ke zmírnění těchto dopadů z pohledu implementace a procesního řízení.

I TEORETICKÁ ČÁST

1 ÚVOD DO PROBLEMATIKY

S rapidním rozvojem digitálních technologií a automatizovaných systémů se automobilový průmysl ocitl uprostřed významné transformace. Moderní vozidla jsou spojena s větším a větším množstvím externích systémů a pokročilými technologiemi, jako je například autonomní řízení či komunikační systémy. Přestože doba digitalizace se nedá zastavit a dává nám spoustu možností, výhod a komfortu v našich vozidlech, přináší sebou bohužel také vznikající výzvy a hrozby. Je proto kritické řešit téma kybernetické bezpečnosti v tomto průmyslu.

Na začátku první kapitoly bakalářské práce budou objasněny rozdíly mezi pojmy kyberbezpečnost (cybersecurity) a funkční bezpečnost (functional safety), jelikož tyto pojmy se velmi často chybně zaměňují. Dále se bude věnovat přiblížení existující zranitelnosti a útokům, které je v dnešní době možné na vozidlech spáchat, včetně představení konkrétního známého případu kybernetického útoku. Díky existenci vzniklého ohrožení samozřejmě roste poptávka po řešení, která má hned několik motivujících faktorů, jež budou popsány v třetí části této kapitoly. V neposlední řadě budou zprehledněny i zákony a vyhlášky, které se řešením této problematiky zabývají.

1.1 Rozdíl mezi kyberbezpečností a funkční bezpečností

Nejprve je nezbytné vymezit rozdíl mezi kyberbezpečností a funkční bezpečností, neboť tyto pojmy jsou v odborné praxi často nesprávně zaměňovány. Pod pojmem *funkční bezpečnost* (definována normou **ISO 26262**) se skrývá identifikace a řízení rizik vyplývajících z technických chyb hardwaru nebo softwaru. Jejím cílem je zajistit, že i v případě selhání jedné části systému zůstane vozidlo bezpečné pro uživatele. Příkladem může být systém řízení stability (ESP), který musí zůstat funkční i při částečném selhání některého senzoru. Naproti tomu *kyberbezpečnost* se zabývá hrozbami, které pocházejí z vnějšího prostředí. Tyto hrozby zahrnují neoprávněný přístup k systémům vozidla, manipulaci s daty nebo jejich odcizení. Klíčovou normou v této oblasti je **ISO 21434**, která stanovuje požadavky na ochranu systémů proti kybernetickým útokům. [1] [2]

1.2 Hrozby spojené s kybernetickou bezpečností automobilů

„V oblasti automobilových systémů je kybernetický útok definován jako čin, kterým se útočník snaží narušit informace o vozidle nebo ovlivnit jeho schopnost dosahovat provozních, bezpečnostních či ochranných cílů.“ (Nasser, [3, str. 64-65])

1.2.1 Kybernetické útoky

Aktivní

- zahrnují zásahy do cílového systému, jako je například úprava, mazání, přidávání nebo blokování dat a funkcí. Útočníci, kteří napadají centrální elektronickou řídicí jednotku nebo síť vozidla, obvykle nepřikládají velký význam tomu, zda budou odhaleni. Nicméně v případě státem podporovaných útočníků nebo pokročilých hrozeb je častým cílem zamaskovat své stopy a prodloužit dobu, po kterou mohou exploit zneužívat. Mezi příklady se uvádí spoofing (metoda, kdy útočník předstírá jinou identitu, například falešnou IP adresu, e-mail nebo signál, aby zmátl systém nebo uživatele) či replay (útok spočívá v opakovaném přehrání zachycené komunikace mezi dvěma stranami útočníkem, aby získal neoprávněný přístup nebo narušil systém) [3]

Pasivní

- útoky se zaměřují na získávání informací o cílovém systému bez toho, aby útočník prozradil svou přítomnost. Tyto útoky, ať už cílené na IT síť nebo síť vozidla, obvykle spočívají v odposlechu či průzkumných aktivitách [3]

Je mnoho důvodů, proč ke kybernetickým útokům dochází. Mezi ty očividné patří:

- **Ukradení dat** (z důvodů finančního výtěku, osobních identifikačních údajů, pojištění, zjištění fyzické bezpečnosti vozidla, zjištění dat o vozidle jako takovém apod.)
- **Podvod**
- **Hacktivismus** [4]

Ale může k nim docházet i z jiných důvodů, mezi které se řadí:

- **Přepsání vozidla na jinou osobu**
- **Terorismus**

- Sabotáž
- Hackování „pro zábavu“
- Atd. [4]

Asi jedním z nejznámějších příkladů hrozeb je případ Jeep Cherokee z roku 2015. Charlie Miller a Chris Valasek pomocí internetově připojenému systému Uconnect předvedli, jak se na dálku dá ovládnout Jeep Cherokee. Nejednalo se o pouhé ovládání rádia, či zapínání a vypínání stěračů. Ale o naprostou kontrolu absolutně kritických funkcí vozidla, jako jsou především brzdy, volant či motor. Díky této události se strhla celosvětová debata o kybernetické bezpečnosti vozidel. [5]



Obrázek 1 Ukázka útoku Jeep Cherokee z roku 2015

(zdroj:[6])

1.2.2 Útoky na komunikační systémy

Přestože propojení moderních vozidel s okolním světem technologiemi, jako jsou Wi-Fi, Bluetooth či mobilní sítě, dávají uživatelům větší komfort a jednoduchost ovládání či přístupu k navigacím, otevírá to dveře (někdy doslova) pro další možnost pro útočníky.

Kybernetické hrozby spojené s těmito systémy mohou zahrnovat odposlech komunikace, manipulaci s daty nebo dokonce získání kontroly nad některými funkcemi vozidla. Jako příklad se uvádí využívání nezabezpečené Wi-Fi, ale asi jedno z největších

hrozeb představuje manipulace s OTA (over-the-air) aktualizacemi. Útočníci mohou mít přístup ke změně či kompletnímu nahrazení softwaru nahrávaného do auta. [7]

Podle předpisu Evropské unie UNECE Předpis č. 155 (2021) musí výrobci vozidel zajistit ochranu všech komunikačních systémů, včetně bezdrátových technologií, jako jsou Wi-Fi, Bluetooth nebo mobilní sítě, aby byla zajištěna integrita přenášených dat a zabráněno neoprávněnému přístupu. Tento přístup zahrnuje identifikaci a řízení rizik spojených s kybernetickými hrozbami, které mohou narušit funkčnost vozidla nebo ohrozit bezpečnost jeho uživatelů. [8]

1.3 Poptávka po řešení problematiky

Vzniká samozřejmě potřeba rizika a hrozby proaktivně řešit. Poptávka na řešení roste exponenciálně hned z několika důvodů. Prvním očividným je zvyšující se množství připojených moderních vozidel, což zvyšuje pravděpodobnost množství výskytu útoků.

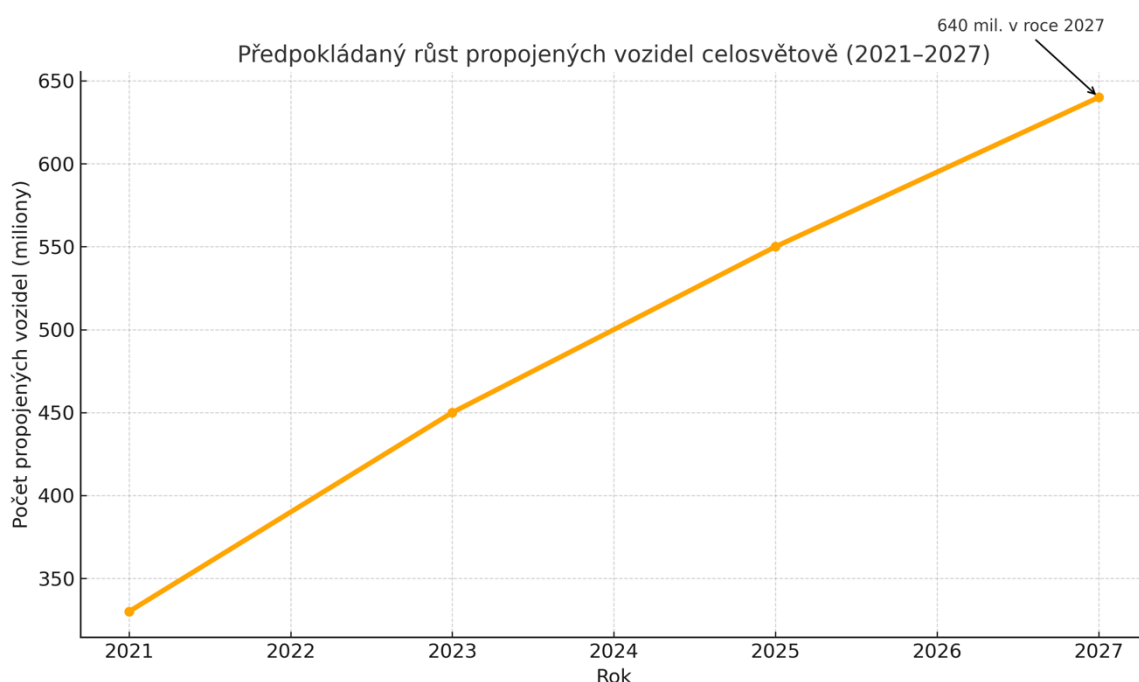
Výrobci jsou nuceni reagovat na stále přísnější požadavky nejen ze strany zákazníků, ale i regulačních orgánů. Například **UNECE Předpis č. 155** zavazuje výrobce k tomu, aby u všech nových modelů zavedli systémy řízení kybernetické bezpečnosti. To zahrnuje jak ochranu během samotného vývoje, tak i průběžné aktualizace softwaru, které zajišťují, že vozidlo zůstane chráněné i několik let po jeho výrobě. [8]

Norma **ISO 21434** (někdy také zmiňována pod názvem ISO/SAE 21434) pak zdůrazňuje, že kybernetická bezpečnost není jednorázová záležitost – musí být součástí každé fáze životního cyklu vozidla, od návrhu až po jeho likvidaci. [1]

Výsledkem kombinace těchto dvou skutečností je zvýšený tlak na výrobce, který je ještě umocněn také finančním tlakem. Kybernetické útoky mohou způsobit obrovské škody – nejen přímé náklady na opravy a ztráty dat, ale také poškození reputace značky.

1.3.1 Rostoucí počet připojených vozidel

Počet připojených vozidel na světě se každoročně výrazně zvyšuje díky rychlému rozvoji digitálních technologií a rozvoji samotného automobilového průmyslu. Podle odhadů se očekává, že do roku 2027 bude na celém světě více než 640 milionů připojených vozidel, což podtrhuje jejich rostoucí význam v moderní mobilitě. [9]



Obrázek 2 Graf předpovězeného růstu počtu připojených vozidel po celém světě mezi lety 2021-2027

(zdroj:[9])

1.3.2 Tlak na automobilové výrobce

Automobiloví výrobci jsou pod tlakem nejen kvůli výše zmíněnému rostoucímu počtu připojených vozidel a nutnosti dodržovat požadavky regulačních předpisů. Čelí také vysokým nákladům spojeným s implementací bezpečnostních opatření, školením personálu a zaváděním nových technologií. [10]

Kromě toho musí investovat do systémů řízení kybernetické bezpečnosti a softwarových aktualizací, což může ovlivnit jejich konkurenceschopnost na trhu. Dalším tlakem je risk poškození pověsti značky. Zákazníci i regulační orgány očekávají, že moderní vozidla budou chráněna proti neoprávněným zásahům a že výrobci budou schopni rychle reagovat na případné hrozby. [11]

1.4 Zákony a regulace

Jak již bylo dříve zdůrazněno, automobilový průmysl je čím dál více ovlivňován požadavky na bezpečnost, které musí zohledňovat jak technické, tak právní aspekty. Pro zajištění bezpečnosti vozidel a jejich systémů byly zavedeny specifické normy a regulace, jež definují

postupy a pravidla pro vývoj, řízení a hodnocení kybernetické a funkční bezpečnosti. Tyto rámce umožňují výrobcům reagovat na hrozby a minimalizovat rizika, která přicházejí s rostoucími nároky na propojení a digitalizaci.

Mezinárodní normy a standardy

1. ISO 21434 Silniční vozidla – Kybernetické zabezpečení při vývoji
 - Poskytuje rámec pro řízení kybernetické bezpečnosti během celého životního cyklu vozidla: od návrhu, přes vývoj, až po výrobu a likvidaci.
 - Publikace: 2021.
 - Spojení s UNECE Předpisem č.155: Klíčová norma pro splnění požadavků pro kybernetickou bezpečnost. [1]
 - Tato norma bude podrobně popsána v pozdějších kapitolách.
2. ASPICE 3.1 (Automotive SPICE)
 - K hodnocení procesů v oblasti automobilového průmyslu se soustředěním na kvalitu vývoje.
 - Publikace: 2017. [12]
 - Celý dokument bude analyzován více v dalších částech práce.
3. ISO 26262: Silniční vozidla – Funkční bezpečnost
 - Poskytuje rámec pro identifikaci a řízení rizik spojených s funkčními chybami elektrických a elektronických systémů vozidel.
 - Publikace: 2011 (1. vydání), 2018 (2. vydání).
 - Spojení s kybernetickou bezpečností: Pomáhá zajistit, že funkční chyby nejsou zneužity kybernetickými útoky. [2]
4. ISO 24089 Silniční vozidla – Inženýrství aktualizací softwaru
 - Specifikuje požadavky na bezpečné aktualizace softwaru vozidel, OTA.
 - Publikace: 2023. [13]

Mezinárodní vyhlášky:

1. UNECE. Předpis č. 155 – Kybernetická bezpečnost a systém řízení kybernetické bezpečnosti (CSMS)
 - Zavádí povinnost implementace systémů řízení kybernetické bezpečnosti.
 - Hlavní milníky:
 - 2021 Q1: Přijetí vyhlášky.
 - 2022 Q3: Povinnost pro všechny nové typy vozidel.
 - 2024 Q3 (7. července 2024): Povinnost splnit požadavky ISO21434 pro všechna nová vozidla bez ohledu na typ. [8]
2. UNECE Předpis č. 156 – Aktualizace softwaru a systém řízení aktualizací softwaru. (SUMS)
 - Vyžaduje bezpečné řízení a monitorování aktualizací softwaru.
 - Hlavní milníky:
 - 2022 Q3: Povinnost pro nové typy vozidel.
 - 2024 Q3 (7. července): Povinnost plnění pro všechna nová vozidla bez ohledu na typ. [14]

Pro přehled časové osy klíčových milníků poslouží Tabulka 1:

Tabulka 1 Časová osa klíčových milníků

Datum	Událost
2011	Publikace první verze ISO 26262
2018	Publikace druhé verze ISO 26262
2021 Q1	Přijetí UNECE Předpisů č. 155 a č. 156
2021	Publikace ISO 21434
2022 Q3	Povinný soulad s Předpisy UNECE č. 155 a č. 156 pro nové typy vozidel
2023	Publikace ISO 24089
7. července 2024	Povinnost splnit požadavky UNECE Předpisů č. 155 a č. 156 a ISO/SAE 21434 pro všechna vozidla
2026	Očekává se další harmonizace norem a možná revize stávajících předpisů

(zdroj: [1], [2], [8], [12], [13], [14])

1.5 Shrnutí první kapitoly

Automobilový průmysl čelí významné transformaci způsobené digitálními technologiemi, které přinášejí jak výhody, tak nové výzvy. Funkční bezpečnost, definovaná normou ISO 26262, se zaměřuje na zvládání technických selhání, zatímco kyberbezpečnost v rámci automobilového průmyslu, definovaná normou ISO 21434, řeší možné externí hrozby a kybernetické útoky. Rozlišení těchto pojmů je klíčové pro pochopení problematiky a její správné implementace.

Kybernetická bezpečnost se stává klíčovým tématem, protože moderní vozidla jsou ohrožována útoky, které mohou ovlivnit jejich funkčnost, bezpečnost a ochranu uživatelských dat. Tyto útoky mají různé motivace, od krádeží dat po sabotáž, a jsou umožněny zranitelnostmi, jako jsou slabé šifrování nebo neaktuální systémy. Příkladem je případ Jeep Cherokee z roku 2015, který odstartoval globální debatu o zabezpečení vozidel.

Poptávka po řešení roste, což podtrhují normy jako již zmíněná ISO 21434 a regulace Evropské unie UNECE Předpis č. 155 a 156, které zavazují výrobce k zajištění implementace kybernetické bezpečnosti po celý životní cyklus vozidla.

2 ZÁKLADNÍ TERMINOLOGIE

Pro provedení analýzy dopadu implementace normy ISO 21434 do procesu ASPICE je klíčové jasně vymezit pojmy, které jsou společné pro oblast kybernetické bezpečnosti, softwarového inženýrství a procesního řízení v oblasti automobilovém průmyslu. Tato část poskytuje přehled základních termínů a konceptů, tvořící teoretický základ pro pochopení souvislostí mezi procesem ASPICE a normou ISO 21434. Definované pojmy zároveň zajišťují konzistenci a vysvětlení terminologie, jež bude používána v dalších částech práce.

Kapitola je rozdělena do logických celků od obecných základních pojmů až po pojmy specifické pro ASPICE proces a normu ISO 21434.

2.1 Obecné základní pojmy

Jako první je nutné vymezit základní obecné pojmy, jež se využívají i v jiných oblastech, než je kyberbezpečnost v automobilovém průmyslu. Jejich přehled však umožní lepší pochopení dalších oblastí terminologie, které na ně budou navazovat.

2.1.1 Aktivum

„Aktivum je cokoliv, co má pro organizaci hodnotu a co je třeba chránit.“ (KYBEZ, [5]). Může se jednat o data, systémy, technologie, procesy, ale i zaměstnance nebo dodavatele. Organizace by měly mít přehled o svých aktivech, protože právě na nich závisí její fungování a bezpečnost. Aby bylo možné aktiva efektivně spravovat a chránit, je nutné vést jejich evidenci. [15]

K aktivu je doporučeno přiřazení jasně určeného názvu, například konkrétní server, software nebo oddělení. Dále je potřeba znát jeho typ – může jít o hardware, software, personál nebo třeba know-how. Důležitým faktorem je také způsob likvidace aktiva, tedy co se s ním stane, až nastane jeho konec – například zda bude smazáno, fyzicky zničeno nebo jinak bezpečně odstraněno. Klíčovou roli zde hraje i osoba, která za aktivum odpovídá (tzv. garant), a jeho fyzické umístění. Užitečné je také zaznamenání vazby mezi aktivy, tedy jak spolu souvisejí a zda jedno závisí na druhém. [15]

Pro menší organizace může být dostatečné evidovat aktiva v jednoduché tabulce, větší organizace by měly zvážit propracovanější systémy, které umožňují lepší přehled a analýzu vzájemných vztahů mezi aktivy. [15]

2.1.2 Hrozba

Pod pojmem hrozba se rozumí jakákoli potenciální situace nebo činnost, která může ohrozit aktivum. V oblasti kybernetické bezpečnosti hrozby představují nebezpečí, která mohou vést k neoprávněnému přístupu, manipulaci s informacemi, odposlechu nebo dokonce k převzetí kontroly nad systémy. Mohou být způsobeny úmyslnými útoky, jako je hacking nebo šíření škodlivého softwaru, ale také neúmyslnými chybami, například lidským selháním či technickými poruchami. Z hlediska praxe jsou častější právě chyby neúmyslné. [16]

Hrozby lze rozdělit na přírodní (např. požáry nebo povodně), a technologické či lidské (např. selhání systémů nebo útoky vedené s cílem poškodit organizaci nebo získat přístup k citlivým informacím). Příkladem kybernetické hrozby je například útok typu phishing, kdy útočník manipuluje uživatele, aby mu poskytl své přihlašovací údaje, nebo spoofing, kdy se útočník vydává za někoho s jinou identitou. [16]

Hrozba se řadí mezi neodmyslitelnou součást analýzy rizik, protože společně se zranitelnostmi může způsobit vážné dopady na bezpečnost, funkčnost a důvěryhodnost systémů či softwaru. Z toho důvodu je důležité hrozby nejen identifikovat, ale také přijímat opatření, která jejich dopad minimalizují. [16]

2.1.3 Zranitelnost

Zranitelnost představuje slabinu v systému, softwaru, hardwaru nebo procesech, která může být zneužita hrozbou a způsobit tak narušení bezpečnosti, funkčnosti nebo důvěryhodnosti aktiv/dat. Jde o jakési „otevřené dveře“ či nedostatek ochrany, který útočníci mohou využít k neoprávněnému přístupu či manipulaci s daty. Zranitelnosti se mohou nabývat různých podob, od chyb v kódu, přes neaktuální software, až po slabé heslové zabezpečení či špatně nastavené šifrování. [16]

Jako příklad může sloužit systém s neaktuálním firmwarem, náchylný k útokům, které by mohly být snadno odvráceny, pokud by byl software pravidelně aktualizován. Podobně může být slabým článkem organizace nedostatečně vyškolený personál, který například klikne na škodlivý odkaz, nebo špatně zabezpečená síť, která umožní neoprávněný přístup. Pro zajímavost, i vyškolení zaměstnanci často naletí na škodlivé odkazy, i když jsou očividné. [16]

Zranitelnost jako taková nemusí nutně vést k problému, ale pokud se spojí s hrozbou, může mít vážné následky. Proto je zásadní zranitelnosti neustále vyhledávat, opravovat a

zařazovat opatření, která minimalizují riziko jejich zneužití. V moderních systémech, zejména těch propojených, je pravidelná kontrola a aktualizace klíčová pro systematické udržení bezpečnosti. [16]

2.1.4 Riziko

Riziko představuje možnost vzniku nežádoucí události, která může způsobit škody, ztráty nebo jiné negativní dopady. Skládá se z kombinace pravděpodobnosti, že k události dojde, a závažnosti důsledků, které by nastaly. V oblasti kybernetické bezpečnosti je riziko definováno jako pravděpodobnost, že konkrétní hrozba (např. kybernetický útok) využije existující dříve definovanou zranitelnost (např. slabé šifrování nebo neaktuální systém) a způsobí tím negativní důsledky (např. narušení funkčnosti nebo ztráta dat). Je možné riziko snižovat implementací bezpečnostních opatření, která slouží k minimalizaci zranitelnosti, omezují pravděpodobnost realizace hrozeb nebo zmírňují jejich dopady. [16]

2.1.5 Bezpečnostní opatření

Bezpečnostní opatření jsou strategie, nástroje a procesy určené k ochraně aktiv, jak bylo zmíněno v podkapitole výše. Zahrnují fyzická opatření (např. zámky nebo kamerové systémy), digitální opatření (např. dvoufaktorová autentizace), a kybernetická opatření (např. systémy prevence průniků kybernetických útoků). Klíčovou roli hrají také bezpečnostní opatření v cloudu, která chrání data a zátěže v cloudovém prostředí. Vzhledem k rostoucím kybernetickým hrozbám a přísným regulačním požadavkům (např. zákony o ochraně dat), je implementace bezpečnostních opatření nutná. Tyto nástroje pomáhají minimalizovat rizika útoků, chrání citlivá data a zajišťují, že organizace splňují právní a průmyslové standardy. [17]

2.1.6 Zmírňování rizik

Zmírňování rizik neboli mitigace rizik hraje klíčovou roli v procesu řízení rizik, která se zaměřuje na identifikaci, analýzu a implementaci opatření ke snížení pravděpodobnosti výskytu hrozeb nebo minimalizaci jejich dopadů. Tento proces začíná systematickým rozpoznáním potenciálních hrozeb, která mohou ovlivnit dosažení stanovených cílů. Následuje analýza těchto hrozeb, při níž se posuzují jejich možné důsledky a pravděpodobnost výskytu. Na základě výsledků analýzy se jednotlivá rizika vyhodnocují a stanovují se priority jejich řešení. Při samotném zmírňování dochází k výběru vhodných strategií, které mohou zahrnovat vyhnutí se riziku, snížení pravděpodobnosti, hrozby, sdílení

rizika například prostřednictvím pojištění, nebo vědomé přijetí rizika, pokud by náklady na jeho zmírnění byly vyšší než očekávané přínosy. Implementace těchto opatření musí být vyvážená, pro zaručení jejich efektivity a ekonomické přijatelnosti. Důležitou součástí zmírňování rizik je také jejich pravidelné monitorování a přehodnocování, aby se zajistilo, že přijatá opatření zůstávají aktuální a účinná i při změně podmínek. Aby bylo zmírňování rizik úspěšné, je nutné provozovat neustálou komunikaci a spolupráci mezi všemi zainteresovanými stranami. Tím je přispěno k udržení stability a bezpečnosti organizace. [18]

2.1.7 Analýza dopadu

Analýza dopadu, známá také pod anglickým termínem *impact analysis*, představuje systematický proces, sloužící k identifikaci a hodnocení možných pozitivních i negativních důsledků plánované změny nebo neočekávané události. Jejím hlavním cílem je pomoci organizacím konat informovaná rozhodnutí a připravit se na případné problémy, které by mohly vzniknout. Tento proces je klíčový zejména při řízení změn v podnicích, ať už jde o zavádění nových funkcí, reorganizaci procesů, nebo reakci na externí vlivy. [19]

Existují tři hlavní metody analýzy dopadu. **Analýza sledovatelnosti**, která se zaměřuje na odhalení vazeb mezi různými částmi produktu nebo systému, aby bylo zajištěno, že plánované změny nenaruší celkovou funkčnost produktu. Tato metoda je často využívána při vývoji softwaru. Další je **analýza závislostí**, která zkoumá, jak změna ovlivní celý systém, hlavně jeho vzájemné závislosti. Poslední, **experimentální analýza**, se opírá o minulá data a události, aby bylo možné předpovědět dopady budoucích změn a lépe se na ně připravit. [19]

Analýza dopadu je důležitá, protože pomáhá minimalizovat ztráty tím, že identifikuje rizika spojená se změnou a umožňuje firmám na ně reagovat. Podporuje také týmovou spolupráci, protože umožňuje všem zúčastněným pochopit dopady plánovaných změn a přispět k jejich hladké implementaci. Tento přístup zvyšuje efektivitu rozhodovacích procesů a přispívá k úspěšnému řízení změn v organizaci. [19]

V praktické části této práce bude využita analýza sledovatelnosti a analýza závislostí.

2.1.8 Řízení životního cyklu produktu

Řízení životního cyklu produktu je komplexní přístup k řízení všech fází života produktu od jeho počátečního návrhu až po likvidaci. Tento proces zahrnuje hned několik klíčových fází.

První fází je vývoj produktu, který začíná prvotním nápadem a jeho realizací do finální podoby. V této fázi dochází ke shromažďování nápadů, provádění změn a testování produktu u cílové skupiny. Důležité je zmínit, že v této době nejsou zatím žádné příjmy z prodeje. Druhá fáze představuje uvedení na trh, kdy se produkt začne prodávat. Tento krok obvykle zahrnuje vysoké výdaje na propagaci, reklamu či zavedení distribuční sítě. Správná cenotvorba je klíčová, protože první uživatelé jsou často ochotni platit vyšší cenu. Poté následuje fáze růstu, kdy prodeje začínají výrazně stoupat a společnost se zaměřuje na zvyšování tržního podílu. Rostoucí trh však přitahuje konkurenci, což vyžaduje zařízení odlišnosti produktu od ostatních (např. modifikací, patentem). Ve čtvrté fázi, nazývané zralost, produkt dosahuje vrcholu prodeje, avšak trh se postupně nasycuje a tempo růstu se stává pomalejším. Společnosti proto často snižují ceny, aby zůstaly konkurenceschopné, a zároveň hledají nové trhy nebo využití pro svůj produkt. Finální fází je úpadek, kdy prodeje začínají klesat vlivem technologického pokroku, změn v preferencích zákazníků nebo silnější konkurence. Firmy pak musí rozhodnout, zda produkt stáhnout z trhu, vylepšit nebo najít nové způsoby jeho využití. [20]

Efektivní řízení životního cyklu produktu dává firmám možnost optimalizovat náklady, zkrátit dobu uvedení na trh a zvyšovat konkurenceschopnost. Tento proces řízení zahrnuje propojenost procesů, technologií a lidí napříč celou organizací, což zlepšuje sdílení informací a spolupráci mezi jednotlivými částmi organizace. Je nutné tento přístup využít z důvodů efektivního řízení moderních produktů a jejich následný úspěch na trhu. [20]

2.2 Komponenty a technologie vozidel

Jelikož se práce bude zabývat problematikou týkající se automobilového průmyslu, je nutné definovat základní pojmy komponent a technologií vozidel.

2.2.1 Embedded systém

Embedded systém je specializovaný, z velké části dnes již plnohodnotný, počítačový systém a slouží k vykonání jedné nebo malého množství menších funkcí. V českém jazyce se tento termín překládá jako vbudovaný nebo vestavěný systém, ale tento překlad je poměrně nešikovný a v praxi se prakticky nepoužívá. Mikroprocesorem embedded systému bývá mikrokontroler (MCU), doplněný o operační paměť a užitečné periferie (např. AD/DA převodníky, ethernet řadiče, čítače a časovače). Používanými programovacími jazyky jsou

C či C++ a assembler pro oblasti funkční bezpečnosti, kdy je nutné být co nejbližší hardware. [21]

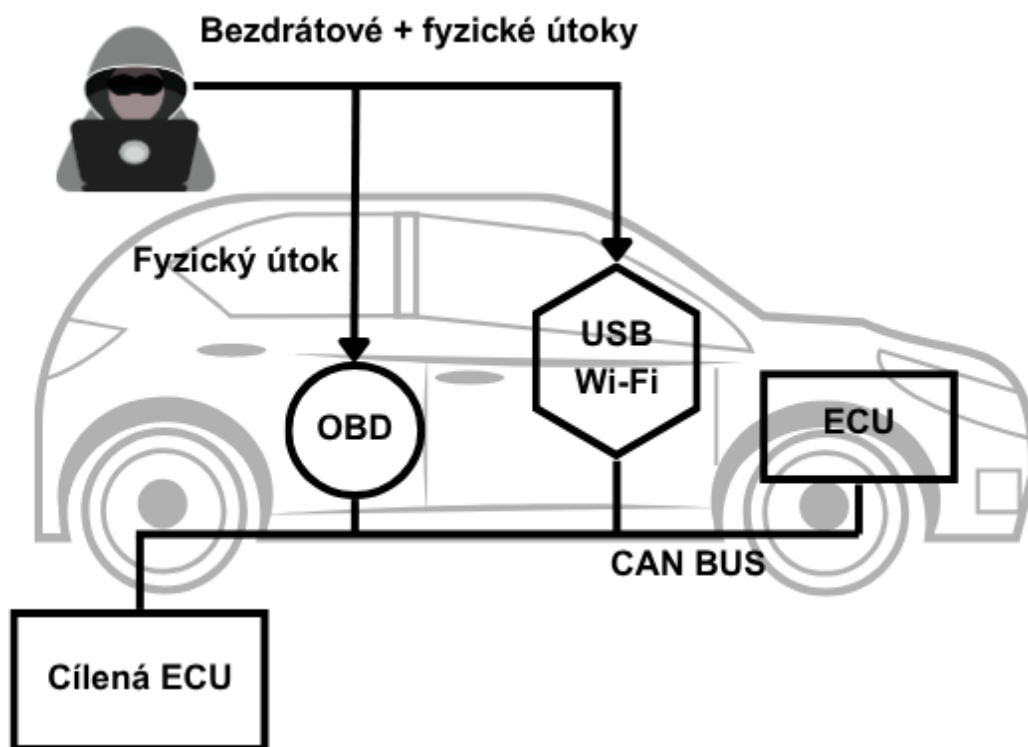
2.2.2 Firmware

Firmware představuje nízkourovňový software, který je uložený v paměti ROM (Read-Only Memory) nebo EPROM (Erasable Programmable Read-Only Memory) a často bývá součástí embedded systémů. Pojmem nízkourovňový se rozumí, že je velmi blízko hardwaru. Jeho úkolem je dávat instrukce hardwaru a určovat, jak má hardware fungovat. Umožňuje základní fungování zařízení a komunikaci mezi komponenty hardwaru a ostatními vrstvami softwaru. [22]

2.2.3 Elektronická řídicí jednotka

Elektronická řídicí jednotka, či zkráceně ECU (Electronic Control Unit), je klíčovou součástí moderních vozidel, která dohlíží na správnou funkci motoru. V automobilech obohacených o elektronické vstřikování paliva elektronická řídicí jednotka reguluje množství paliva vstupujícího do válců motoru, což následně optimalizuje směs paliva a vzduchu při kompresi. Tím dochází k maximalizaci výkonu vozidla a minimalizaci plýtvání palivem. [23]

Tato řídicí jednotka může být umístěna v různých částech vozidla, nejčastěji však bývá v motorovém prostoru nebo v přední části interiéru (např. v přihrádce spolujezdce či pod palubní deskou). Konkrétní umístění ECU je obvykle definováno v uživatelské příručce vozidla. Vzhledem k tomu, že ECU řídí mnoho funkcí moderních vozidel, její správná funkce je nezbytná pro celkový výkon a spolehlivost automobilu a řadí se mezi klíčová aktiva oblasti kybernetické bezpečnosti v automobilovém průmyslu. [23]



Obrázek 3 Příklad útoku na cílenou ECU

(zdroj: [3])

Obrázek 3 ilustruje, jak může útočník využít jedné elektrické řídicí jednotky k útoku na jinou pomocí jeho interní komunikační sběrnice CAN. Útočník může využít diagnostický port (OBD) k fyzickému útoku anebo využít bezdrátové připojení pomocí adaptéru (USB či WiFi). Cílem útoku je získání přístupu k vybrané (cílené) ECU a poté manipulovat s její funkcionalitou nebo sbírat data. [3]

2.2.4 Komunikační sběrnice CAN

Komunikační sběrnice CAN (Controller Area Network) představuje robustní a osvědčenou síťovou technologii, která se již více než 40 let používá v automobilovém průmyslu. Její otevřený standard umožňuje širokou dostupnost řadičů od různých výrobců, což poskytuje flexibilitu při výběru vhodných komponent pro konkrétní aplikace. Jejím hlavním cílem je zajištění komunikace mezi elektrickými řadičími jednotkami ve vozidle. Díky své dlouhé historii a otevřenosti je její implementace ve vozidlech nákladově efektivní. Topologie sběrnice, kterou CAN využívá, umožňuje snadné přidávání nebo odstraňování uzlů bez nutnosti změn v ostatních částech sítě. Existuje také sběrnice CAN s flexibilní datovou rychlostí (CAN FD), která má vyšší přenosovou rychlost a datovou kapacitu. V porovnání

klasická CAN sběrnice umožňuje přenos o délce až 8 byte, CAN FD umožňuje až 64 byte. Komunikace je tak rychlejší a efektivnější. [24]

2.2.5 Telematická jednotka

Dalším kritickým aktivem v oblasti vývoje v automobilovém průmyslu je telematická jednotka, zkráceně TCU (Telematics Control Unit). Je to komunikační jednotka, která umožňuje obousměrnou komunikaci mezi vozidlem a externí sítí pomocí bezdrátových modulů. Jejím cílem je zlepšení funkčnosti vozidla a pohodlí. Také poskytuje asistenci řízení. Díky instalaci TCU je umožněno provádění bezdrátové aktualizace systému. [25]

Zatímco ECU zajišťuje řízení konkrétních funkcí ve vozidle, TCU je nadstavbovou jednotkou, která čerpá informace z různých ECU a zajišťuje jejich komunikaci s okolním světem. [25]

2.2.6 Bezdrátová aktualizace softwaru

Bezdrátová aktualizace softwaru, zkráceně OTA, představuje formát aktualizace, která funguje na bezdrátové bázi a doručuje software, firmware nebo data do zařízení, jako jsou chytré telefony či IoT zařízení, prostřednictvím Wi-Fi nebo mobilní sítě. Tímto způsobem se dá také aktualizovat software vozidla a tento přístup má rostoucí popularitu u výrobců, jelikož umožňuje snadno udržovat zařízení aktuální bez potřeby fyzického připojení k počítači. OTA princip je využíván k instalaci nových verzí systémů, opravám chyb nebo ke konfiguraci zařízení a může být jak automatické, tak manuální. [26]

2.3 Metody a postupy v oblasti kybernetické bezpečnosti

Kybernetická bezpečnost má svou vlastní metodiku a postupy řešení, které se liší od ostatních. Má své vlastní požadavky na přístup k analýze hrozeb a hodnocení rizik i k reagování na kyberbezpečnostní incidenty.

2.3.1 Analýza hrozeb a hodnocení rizik

Provedení analýzy posuzování rizik kybernetické bezpečnosti, zkráceně TARA (Threat Analysis and Risk Assessment), je systematický proces k řízení rizik kybernetické bezpečnosti, který se zaměřuje na identifikaci a hodnocení aktiv, hrozeb a rizik v systémech, zejména v oblasti automobilového průmyslu. Její definice pochází z normy ISO 21434. Nejprve je potřeba definovat systém, poté identifikovat aktiva, jejich důvěrnost, integritu a dostupnost. Poté jsou ve spojení s těmito aktivy analyzovány příslušné hrozby a přiřazena

jejich pravděpodobnost. Jako další fáze probíhá konkrétní dopad těchto hrozeb a stanovují se rizika, která budou vyžadovat bezpečnostní opatření. Více se TARA principu bude věnovat praktická část práce při detailní analýze požadavků vyplývajících z ISO 21434. [27]

2.3.2 Správa zranitelností

Správa zranitelností je také procesem, ovšem tento proces se zabývá identifikací, hodnocením a eliminací zranitelností v hardwaru či softwaru. Cílem procesu je odhalení slabín dříve, než může dojít k zneužití slabín útočníky. Součástí procesu je hodnocení rizik, stanovení priorit podle závažnosti, nápravu pomocí aktualizací či změn konfigurace, průběžné monitorování a opakované hodnocení. Díky efektivní správě zranitelností mohou organizace snížit riziko útoku a zajistit vyšší bezpečnost svých produktů. [28]

2.3.3 Plán reakce na incidenty

Plán reakce na incidenty je psaný dokument, který musí být formálně schválen vyšším managementem. V plánu musí být detailně popsáno, jak se chovat před, během a po incidentu, spolu s konkrétním seznamem rolí a odpovídajícím odpovědnostem v případě kybernetického útoku. Cílem plánu je minimalizovat dopad možného incidentu na organizaci a co nejrychlejší vrácení se k běžnému provozu. [29]

2.4 Klíčové pojmy a koncepty v ASPICE procesu

Procesní rámec ASPICE přináší svou vlastní terminologii, kterou používá a je nutné znát její přehled a význam pro lepší uchopení dalších částí práce.

2.4.1 Model referenčních procesů

ASPICE má svůj vlastní model referenčních procesů, který definuje dílčí procesy a jejich vzájemnou propojenost. Procesní rámec celkem 32 procesů a svou vlastní strukturu, která bude probírána více do hloubky během popisu normy ASPICE 3.1 v následující části práce. Každá oblast ASPICE je specifikována určitými základními praktikami a obsahuje specifické pracovní výstupy. [30]

2.4.2 Základní praktiky

Základní praktiky jsou konkrétní postupy, které organizace musí zavést, aby zajistila kvalitní a efektivní průběh vývojových procesů. Skládají se z klíčových aktivit (např. plánování a sledování procesů, řízení požadavků či řízení rizik). Plánování a sledování zajišťuje dobrou

organizovanost procesu a kontrolu nad jejich průběhem. Řízení požadavků zase pomáhá sledovat, zda všechny produkty splňují výsledné požadavky. Řízení rizik poté identifikuje a minimalizuje potenciální problémy. [30]

2.4.3 Pracovní výstupy

Pracovní výstupy jsou dokumenty a artefakty, které vznikají během jednotlivých procesů. Slouží jako důkaz o správném provedení a zajišťují sledovatelnost, propojenost a kvalitu. Běžné pracovní výstupy zahrnují dokumentaci požadavků, návrhy architektury, testovací plány a záznamy nebo zprávy o řízení rizik. Tyto výstupy umožňují pozorovat pokrok, identifikovat slabiny a zajistit shodu s průmyslovými standardy a regulačními požadavky, což přispívá k efektivnímu a kvalitnímu vývoji softwaru. [30]

2.4.4 Sledovatelnost požadavků

Sledovatelnost požadavků znamená schopnost propojit jednotlivé požadavky s každou fází vývoje produktu – a to od jejich zadání přes návrh, implementaci až po testování. Tím pomáhá zajistit, že každý požadavek byl správně pochopen, zpracován a ověřen. Umožňuje sledovat, jak se požadavky promítly do výsledného produktu, a rychle odhalit případné chyby nebo nesrovnalosti. Uspodňuje také řízení změn, jelikož je hned jasné, co bylo upraveno, proč a jak to ovlivnilo ostatní části projektu. [31]

Existuje celá škála nástrojů pro vytvoření, monitoring sledovatelnosti požadavků a jejich správu. Mezi nejvíc používané se řadí ELM7 nebo IBM DOORS, je i možnost udržovat požadavky v excelu, ovšem tento přístup není doporučován. [31]

2.4.5 Stanovení úrovně způsobilosti

Stanovení způsobilosti představuje proces, který hodnotí schopnost organizace efektivně realizovat specifické procesy při vývoji v oblasti automobilového průmyslu. Tato evaluace se provádí pomocí definovaných úrovní způsobilosti, které měří, jak dobře jsou procesy implementovány a jakých výsledků dosahují. Cílem je identifikace silných stránek a oblastí pro zlepšení. [32]

2.4.6 Úrovně způsobilosti

Automotive SPICE definuje šest úrovní schopností, které hodnotí zralost procesů v softwarovém vývoji v oblasti automobilového průmyslu. Hodnotí strukturu, řízení a optimalizaci procesů. Existuje 6 úrovní způsobilosti (0 až 5), dle zralosti a efektivity. Tyto

úrovně poskytují rámec pro organizace k posouzení a zlepšení jejich procesů vývoje softwaru, což vede k vyšší kvalitě produktů a lepší shodě s průmyslovými standardy. [32]

Tabulka 2 Přehled úrovní schopností v rámcovém procesu ASPICE

Úroveň	Pojmenování	Popis
0	Neúplné	Procesy nejsou implementovány nebo nejsou plně definovány, výsledky jsou nepředvídatelné.
1	Provedené	Základní procesy jsou zavedeny, ale postrádají formalizaci a dokumentaci. Práce je nekonzistentní.
2	Řízené	Procesy jsou plánovány, monitorovány a kontrolovány. Organizace sleduje výkon a řídí zdroje.
3	Ustálené	Procesy jsou dobře definovány a zdokumentovány, zajišťují konzistenci napříč projekty.
4	Předvídatelné	Procesy jsou kvantitativně měřeny a kontrolovány, výsledky lze spolehlivě předvídat.
5	Optimalizující	Organizace proaktivně vylepšuje procesy na základě zpětné vazby a metrik, zaměřuje se na inovace.

(zdroj: [32])

2.4.7 Přizpůsobení procesů

V rámci ASPICE je možné provést úpravu standardních procesů tak, aby odpovídaly specifickým požadavkům projektu nebo organizace. Termínově se jedná o přizpůsobení procesů, které zajišťuje, že procesy jsou efektivní, reflektují velikost týmu, složitost projektu nebo zákaznické potřeby, a zároveň splňují požadavky na kvalitu. Laicky by se dalo říci, že jsou „šité na míru“. Přizpůsobení procesů zahrnuje analýzu existujících postupů, identifikaci oblastí k úpravě a implementaci změn pro zvýšení efektivity a snížení rizik. Výsledkem je

procesní rámec přizpůsobený konkrétním podmínkám, který podporuje kvalitní a cílený vývoj softwaru. [12]

2.5 Klíčové pojmy a koncepty z normy ISO 21434

Norma ISO 21434 stanovuje rámec pro řízení kybernetické bezpečnosti v celém životním cyklu produktu. Pro správnou implementaci normy je zásadní pochopení základních pojmů a konceptů, které tvoří její teoretický i procesní základ.

2.5.1 Identifikace aktiv

Identifikace aktiv je proces, při kterém se určují a zaznamenávají klíčová aktiva systému, jejichž narušení by mohlo vést k nežádoucím následkům. Tento krok slouží jako vstup pro následnou analýzu hrozeb a rizik (TARA). Umožňuje stanovit, které části systému vyžadují zvýšenou ochranu. Správná identifikace aktiv zahrnuje pochopení funkcí jednotlivých komponent, jejich vzájemných vazeb a potenciálních zranitelností. Tento termín bude rozebrán více do hloubky během praktické části práce. [27]

2.5.2 Cíle kybernetické bezpečnosti

Cíle kybernetické bezpečnosti jsou specifické požadavky spojené s jedním nebo více scénáři hrozeb, které mají za úkol chránit systémy před potenciálními útoky. Stanovení těchto cílů je klíčové pro zajištění bezpečnosti a integrity funkcí vozidla. [27]

2.5.3 Scénáře hrozeb

Scénáře hrozeb představují potenciální situace, ve kterých mohou být aktiva systému vystavena potenciálním kybernetickým útokům. Tyto scénáře detailně popisují možné cesty útoku, včetně identifikace útočníka, jeho motivace, schopností a prostředků, které by mohl využít k dosažení svého cíle. V oblasti automobilové kybernetické bezpečnosti je tvorba scénářů hrozeb klíčová pro pochopení možných hrozeb či nežádoucích situací a následné implementace správných bezpečnostních opatření. [33]

2.5.4 Úroveň zajištění kybernetické bezpečnosti

Norma ISO 21434 definuje úrovně zajištění kybernetické bezpečnosti, které se určují po provedení dříve zmíněném provedení analýzy posuzování rizik kybernetické bezpečnosti. V praxi se často pro zjednodušení používá zkratka CAL (Cybersecurity Assurance Levels). Existují 4 úrovně zajištění, které jsou definované pomocí faktorů očekávaných během celého

životního cyklu vývoje. CAL1 představuje nejnižší úroveň kritičnosti a CAL4 nejvyšší. Úroveň je možné určit i podle dopadu a vektoru útoku. [1]

Tabulka 3 Určení CAL podle dopadu a vektoru útoku

		Vektor útoku			
		Fyzický	Místní	Přilehlý	Sít'ový
Dopad	Kritický	CAL2	CAL3	CAL4	CAL4
	Významný	CAL1	CAL2	CAL3	CAL4
	Mírný	CAL1	CAL1	CAL2	CAL3
	Zanedbatelný	není přiřazen	není přiřazen	není přiřazen	není přiřazen

(zdroj: [34])

Vektor útoku lze chápat jako způsob či cestu využívanou útočníky pro dosažení svých cílů, jako je například ilegální přístup k síti či systému. Motivace k využití je za účelem zisku, jak hmotného, tak nehmotného. Dle lokace mohou být vektory útoku fyzické, místní, přilehlé či síťové. Tento pojem je využíván i mimo oblast kybernetické bezpečnosti. [35]

2.5.5 Security-by-Design

Security-by-Design (žádný český ekvivalentní termín není v praxi používán) je bezpečnostní koncept při vývoji nejen v oblasti automobilového průmyslu. Primární myšlenkou tohoto přístupu je zbavit systém, software či hardware zranitelností a udělat jej odolný vůči kyberbezpečnostním útokům. Princip je založen na implementování bezpečnostních opatření a požadavků již od počátku místo jejich zařazení zpětně za provozu. [36]

2.5.6 Monitorování a záznamy

Monitorování a záznamy probíhají pomocí opakované detekce a reakce na aktuální či potenciální bezpečnostní incidenty. Jsou nedílnou částí normy ISO 21434 a slouží k zajištění bezpečnosti a funkčnosti vozidla během celého životního cyklu. [27]

2.5.7 Zbytkové riziko

I při důkladném plánování a implementaci správně definovaných bezpečnostních opatření mohou některé hrozby přetrvávat. Tomuto jevu se říká zbytkové riziko, které je potřeba minimalizovat na přijatelnou úroveň pomocí neustálého monitorování a úprav bezpečnostních opatření, aby zásadně neovlivňovalo bezpečnost vozidel a uživatelů. [37]

2.5.8 Systém řízení kybernetické bezpečnosti

Systém řízení kybernetické bezpečnosti je strukturovaný pracovní rámec, využívaný z důvodu systematické identifikace, zpracování a zmírňování rizik v kontextu kybernetické bezpečnosti. V praxi používá zkratka CSMS (Cybersecurity Management System), která se objevuje nejen v normě ISO 21434, ale i ve vyhlášce UNECE. Předpis č. 155 [1] [8]

Z právního hlediska v České republice se systémem řízení kybernetické bezpečnosti zabývá Vyhláška č.82/2018 Sb. [38]

2.6 Shrnutí druhé kapitoly

Tato kapitola se zaměřuje na klíčové pojmy a koncepty důležité pro uchopení souvislostí v oblasti automobilového průmyslu a mezi normami ASPICE a ISO 21434. Mezi hlavní základní pojmy se řadí aktivum, hrozba, zranitelnost a analýza dopadu. Aktivum představuje cokoli, co má pro organizaci hodnotu. Hrozba je aktivita, která ohrožuje aktivum a využívá přitom zranitelností aktiv. Analýza dopadu je systematický proces, který bude využit jako nástroj při zpracování praktické části práce. Elektrická řídící jednotka, její komunikační sběrnice CAN (popřípadě CAN FD), telematická jednotka a bezdrátová aktualizace jsou termíny objasňující komponenty a technologii vozidel.

Kapitola je zakončena výčtem termínů používaných v ASPICE a ISO 21434, které je nutné znát jak pro popis norem, tak pro jejich analýzu v navazujících částech.

3 PŘEHLED PROCESU ASPICE

Tato bakalářská práce se zabývá ASPICE verzí 3.1, vydanou dne 1. listopadu 2017, přestože existuje také novější verze 4.0, která byla vydána dne 29. listopadu 2023. Verze zvolena pro tuto bakalářskou práci byla vybrána z důvodu znalosti práce s procesem, novější verze 4.0 není mezi organizacemi zatím v praxi široce využívána.

Odůvodnění používání starší verze je hned několik. Verze 3.1 je zažitá, ověřená, a hlavně dává možnost auditovatelnosti. Organizace na ní mají postaveny veškeré interní směrnice, procesy, šablony i nástroje. Oproti tomu verze 4.0 je stále poměrně čerstvá a vyžaduje hlubokou analýzu k pochopení nových požadavků a řadu změn k implementaci a přináší rozšíření, které pro organizace prozatím nejsou prioritou. V automobilovém průmyslu je také běžné, že přechod na nové standardy probíhá postupně, aby byla zajištěna kompatibilita se stávajícími projekty a systémy a udržel se tak konzervativní přístup ke změnám. Dalším faktorem jsou dodavatelské řetězce a požadavky výrobců automobilů (OEM), které hrají klíčovou roli; OEM nepožadují okamžitý přechod na ASPICE 4.0 a tím pádem dodavatelé zatím preferují setrvání u předchozí verze. [39]

V současnosti je používání verze 4.0 pouze dobrovolné, ale v budoucích letech se dá očekávat povinnost přestupu na tuto verzi.

3.1 Historie

Historie procesního rámce sahá do počátku 90. let 20. století, kdy byla vyvinuta jako odnož rámce SPICE (Software Process Improvement and Capability Determination). Konkrétně tak bylo učiněno organizacemi ISO a IEC v roce 1993. Za vznik ASPICE, všech úprav a rozšíření je zodpovědný německý svaz automobilového průmyslu, známý pod zkratkou VDA (Verband der Automobilindustrie e.V.). [40]

Primárním cílem bylo vytvoření jednotného rámce pro hodnocení schopnosti organizací efektivně a spolehlivě dodávat softwarové produkty. Původní verze ASPICE, známá pod pojmem V-Model pro vývoj softwaru byla vydána v roce 2003. Jak z názvu vypovídá, byla tato verze založena na V-Modelu, což je model vývoje softwaru zdůrazňující důležitost testování a ověřování v celém životním cyklu vývoje softwaru. V-modelu bude věnována samostatná část této kapitoly. Od roku 2003 se Automotive SPICE stal široce uznávaným standardem v automobilovém průmyslu. [40]

3.2 Účel

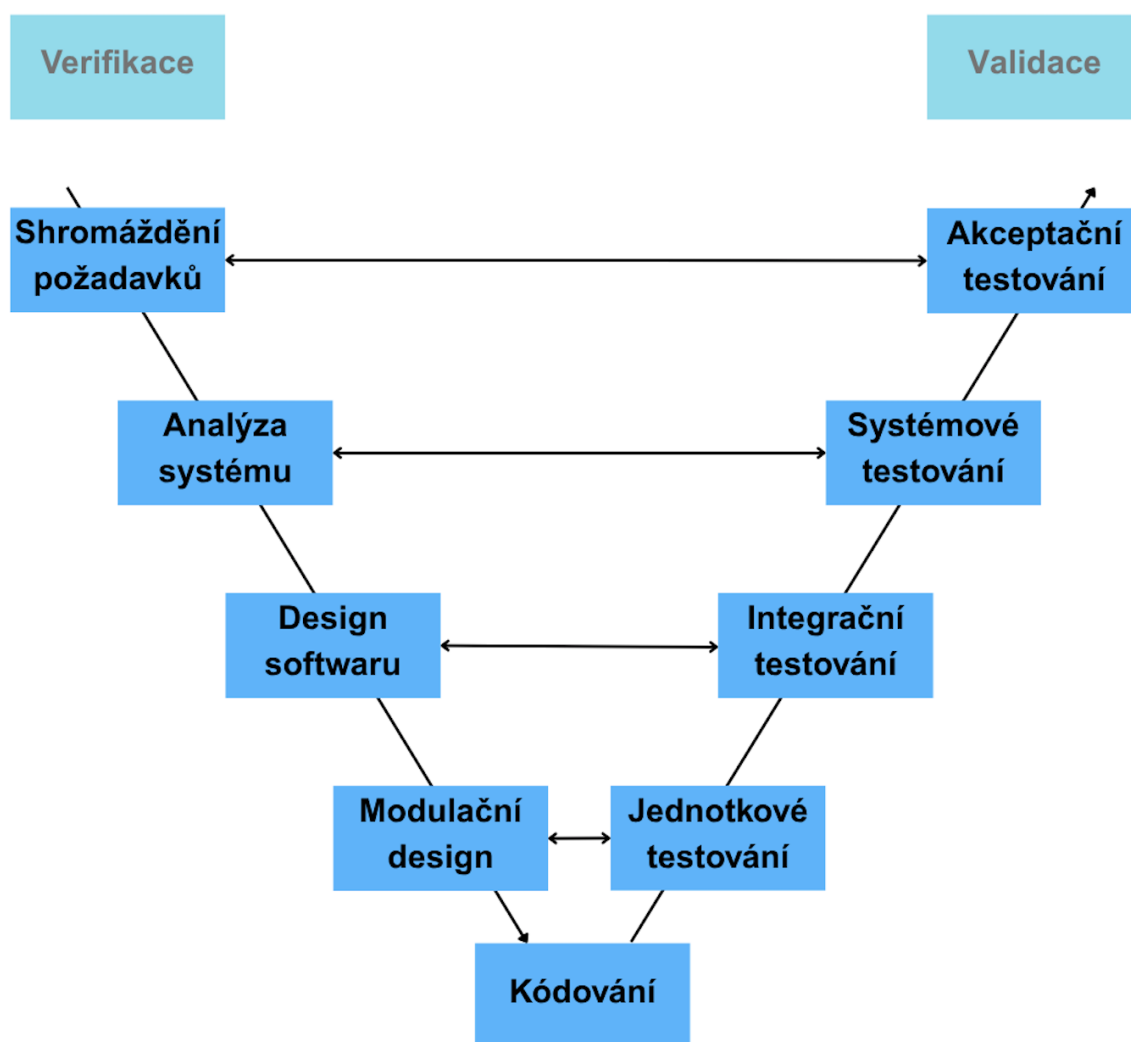
ASPICE slouží jako procesní referenční a hodnotící model, navržen speciálně pro automobilový průmysl. Jeho primárním účelem je poskytovat jednotný rámec pro hodnocení schopnosti organizací efektivně a spolehlivě vyvíjet embedded systémy. Díky tomu napomáhá k identifikaci slabin v procesech vývoje a podporuje jejich neustálé zlepšování. To automaticky vede ke zvýšení kvality produktů a spokojenosti zákazníků. ASPICE byl vyvinut v souladu s požadavky normy ISO/IEC 33004 (mezinárodní norma, zaměřená na hodnocení procesní způsobilosti) a skládá se ze sady indikátorů, které slouží k interpretaci záměru tohoto procesního referenčního modelu. Zmíněné indikátory jsou užitečné jak při hodnocení procesů, tak při implementaci programů na jejich zlepšování. Velkou výhodou ASPICE je soulad procesního rámce se dříve zmíněnou normou ISO 26262. [41]

3.3 V-Model

Jak již bylo dříve zmíněno v popisu historie ASPICE, tento procesní referenční model využívá k popisu životního cyklu vývoje embedded systémů V-model, který je v dnešní době standardem pro systematickou organizaci vývojových a testovacích činností v automobilovém průmyslu. V-Model graficky znázorňuje vztah mezi jednotlivými fázemi vývoje a odpovídajícími fázemi ověřování a validace. Levá strana písmene „V“ reprezentuje procesy související s návrhem a specifikací produktu, zatímco pravá strana zachycuje fáze testování a ověřování, odpovídající jednotlivým vývojovým krokům. [42]

Z praktického hlediska je výhoda V-Modelu v jeho důležitosti včasné detekce chyb a zajištění existence odpovídající testovací aktivity vůči každému definovanému požadavku. Díky tomu je možno se vyhnout vysokým nákladům pozdní detekce chyb a zajistit vysokou kvalitu produktu již ve fázi jeho vývoje. V praxi to znamená, že například systémové požadavky (SYS.2) jsou ověřovány systémovými akceptačními testy. [42]

Použití V-Modelu v ASPICE podporuje sledovatelnost a propojenost napříč celým životním cyklem produktu, což je klíčové pro plnění norem kvality a bezpečnosti. Zejména v kontextu automobilového průmyslu, kde jsou nároky na bezpečnost a spolehlivost extrémně vysoké. [42]

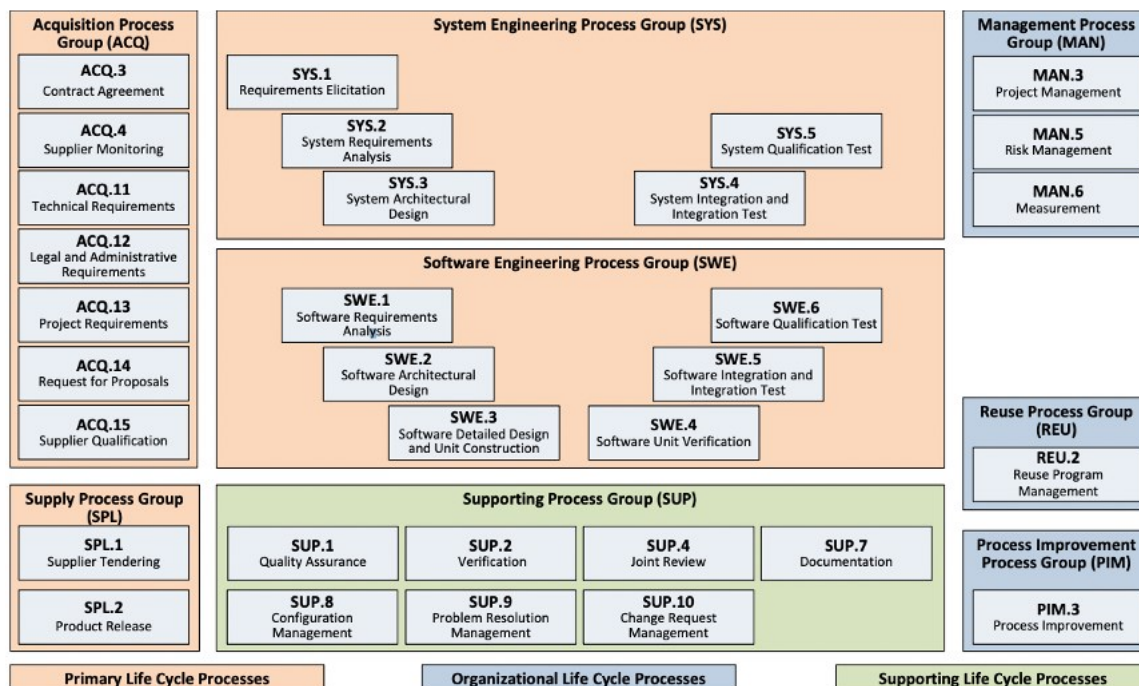


Obrázek 4 V-Model

(zdroj: [42])

3.4 Struktura

ASPICE obsahuje svou vlastní strukturu, která je navržena s účelem pokrytí celého životního cyklu vývoje embedded systémů. Dílčí procesy umožňují systematické hodnocení a zlepšování procesní zralosti v rámci organizace. Jedná se o jasně členěnou hierarchii procesů, která zajišťuje pokrytí všech klíčových oblastí (od analýzy požadavků až po řízení kvality a organizaci vývoje). Struktura byla vytvořena tak, aby byla přizpůsobitelná různým velikostem a projektům a potřebám organizací. Umožňuje tak systémový přístup při řízení vývojových aktivit, sledování kvality produktů i podporu neustálého zlepšování v souladu s požadavky trhu i legislativy. [12]



Obrázek 5 Struktura ASPICE ve verzi 3.1

(zdroj: [12])

Procesy ASPICE se dají rozdělit na 3 hlavní kategorie, dle zaměření:

- **Primární procesy životního cyklu produktu**

- na Obrázku 5 vyznačeny světle oranžovou barvou,
- procesy související přímo s vývojem a realizací embedded systémů,
- pokrývají veškeré činnosti od získání a analýzy požadavků, přes návrh systémové a softwarové architektury, implementaci a testování, až po systémovou integraci a validaci produktu. [12]

Primární procesy tvoří jádro vývojového procesu a patří zde skupiny pořizovací procesní (ACQ), procesů pro dodávku (SPL), systémových inženýrských procesů (SYS) a softwarových inženýrských procesů (SWE). [43]

- **Podpůrné procesy životního cyklu produktu**

- na Obrázku 5 vyznačeny světle zelenou barvou,
- poskytují metodologickou a organizační podporu hlavním vývojovým aktivitám,
- zaměřené například na zajištění kvality, řízení konfigurace, správu problémů a změn, míru efektivity procesů a podporu bezpečného řízení projektů. [12]

Skupina procesů pro podporu (SUP) zajišťuje kvalitu, řízení a zlepšování procesů. [41]

- **Organizační procesy životního cyklu produktu**

- na Obrázku 5 vyznačeny světle modrou barvou,
- procesy zaměřené na definici procesních standardů, správu lidských zdrojů, zajištění školení, sledování a zlepšování výkonnosti procesů napříč projekty,
- cílem je dlouhodobě podporovat zvyšování procesní vyspělosti a efektivity.[12]

Do této kategorie se řadí skupina manažerských procesů (MAN) a skupina pro zlepšování procesů (PIM), které se soustředí na definování, standardizaci a neustálé zlepšování vývojových procesů skrz celou organizaci. [43]

Každý proces je normou definován pomocí následujících prvků:

- **ID procesu** – například SUP.1
- **Jméno procesu** – konkrétní název procesu, například zajištění kvality
- **Účel procesu** – definice cíle a upřesnění, čeho má být procesem dosaženo
- **Vstup procesu** – často nepřímě odvozeny z výstupů přechozích procesů
- **Výstup procesu** – konkrétní výsledky potvrzující, že došlo ke splnění účelu procesu a konkrétní body, jak toho bylo docíleno
- **Základní praktiky** – doporučené činnosti k dosažení požadovaného výsledku procesu
- **Rozšířené praktiky** – doporučené činnosti zaměřené na zlepšování procesu
- **Atributy schopnosti procesu** – hodnotící kritéria úrovně zralosti a výše kvality procesu [12]

3.5 Dílčí oblasti procesu

Procesní rámec ASPICE 3.1 je konstruován z množství oblastí, aby bylo dosaženo komplexního pokrytí všech činností souvisejících s vývojem embedded systémů. Dílčí procesy jsou organizovány modulárně a tvoří základ pro hodnocení schopnosti organizace efektivně a kvalitně provést realizaci každé fáze životního cyklu produktu. Podrobné zaměření na správně definované vstupy a výstupy jednotlivých procesů je klíčové pro zajištění transparentnosti, sledovatelnosti a schopnosti neustálého zlepšování vývoje

produktu. Jak bylo definováno ve struktuře normy, jednotlivé procesy spadají do kategorie primární, podpůrné či organizační. [12]

3.5.1 Vstupy jednotlivých procesů

Pod pojmem vstupy se skrývají schválené výstupy jiných procesů, dokumenty či jiné informace, potřebné pro zahájení a úspěšné dokončení aktivit procesu. [12]

Příklady vstupů jednotlivých procesů:

- **SYS.2** – výstupy z procesu SYS.1, požadavky zákazníka, zákaznické smlouvy a zákaznické specifikace
- **SYS.3** – výstupy z procesu SYS.2, požadavky na systémovou architekturu
- **SWE.1** – výstupy z procesu SYS.2 a SYS.3, zákaznické požadavky na software
- **SWE.6** – výstupy z procesu SWE.1, specifikace testů pro kvalifikaci softwaru a softwarové komponenty k testování
- **MAN.5** – rizikové oblasti z přechozích analýz, projektové plány a záznamy o přechozích rizicích a jejich řešení,
- **SUP.10** – zaznamenané požadavky, stav předešlých změnových požadavků a analýzy dopadu změn [12]

3.5.2 Výstupy jednotlivých procesů

V porovnání se vstupy jsou výstupy jednotlivých procesů jasně definovány v normě ASPICE. Obsah výstupu musí jednoznačně splňovat účel daného procesu. [12]

Příklady vstupů jednotlivých procesů:

- **SYS.1** – navázání a udržování komunikace se zainteresovanými stranami, definování schválených požadavků zainteresovaných stran, zavedení mechanismu pro změnu definovaných požadavků dle potřeby zainteresovaných stran, zavedení mechanismu pro monitorování potřeb zainteresovaných stran, zajištění transparentnosti ohledně stavu požadavků a aktivní identifikace a řízení změn způsobených technickým vývojem a změněných potřeb zainteresovaných stran
- **SYS.2** – definování systémových požadavků, kategorizace a analyzování systémových požadavků pro zaručení jejich správnosti a ověřitelnosti, analýza dopadu systémových požadavků v operačním prostředí, definování prioritizace

implementace systémových požadavků, aktualizování systémových požadavků dle potřeby, zajištění konzistence a sledovatelnosti mezi systémovými požadavky a požadavky zainteresovaných osob, zhodnocení systémových požadavků z pohledu finančních nákladů, časového harmonogramu a technického dopadu a komunikace systémových požadavků všem dotčeným stranám

- **SWE.2** – definování softwarové architektury, alokace softwarových požadavků do prvků softwaru, definování propojenosti mezi všemi prvky softwaru, definování dynamického chování a požadavků na efektivitu systémových požadavků v rámci softwarových prvků, zajištění konzistence a sledovatelnosti mezi softwarovými požadavky a návrhem architektury softwaru a sdělení návrhu softwarové architektury všem dotčeným stranám
- **SUP.1** – vývoj, implementace a udržování strategie pro zajištění kvality, samostatné objektivní zajišťování kvality bez střetu zájmu, identifikace, zaznamenání, sledování, vyřešení a zabránění opakování neshod základních praktik, procesů či procesových aktivit, možnost eskalace neshod k předem definované úrovni managementu a zajištění vyřešení eskalace daným managementem
- **MAN.3** – definování rozsahu prací na projektu, zhodnocení realizace projektu dle dostupných zdrojů a omezení, provedení odhadu aktivit a potřebných zdrojů k dokončení práce na projektu, identifikace a monitorování propojenosti projektu s jinými projekty a částmi organizace, vývoj, implementace a udržování plánů pro dokončení projektu, monitorování a reportování průběhu projektu a provedení korespondujících aktivit při nesplnění cílů projektu [12]

3.6 Dostupná rozšíření

Norma ASPICE ve verzi 3.1 nabízí základní procesní rámec, který je možný podpořit implementací dostupných rozšíření. Tato rozšíření vznikla jako reakce na řešení specifické problematiky. Je možné je dělit na skupinu neoficiálních, kterým se říká „best practice“ (např. využívání agilních metodik při vývoji) a oficiálních, které existují pouze dvě. Jedno rozšíření se soustředí na hardware a druhé na řešení problematiky kybernetické bezpečnosti.

3.6.1 ASPICE for Hardware Engineering

Někdy také známé pod zkráceným výrazem HW-SPICE se zabývá oblastí vývoje hardwarových komponent embedded systémů. Vychází ze stejné metodiky jako původní

ASPICE, ale místo vývoje softwaru se soustředí na vývoj hardwaru s důrazem na vysokou kvalitu v každé životní fázi cyklu. Při implementaci tohoto rozšíření jsou firmy schopné zaručit kvalitu a sledovatelnost nejen u vývoje softwaru, ale také u vývoje hardwaru. [44]

HW-SPIICE nabízí následující rozšířené procesy:

- analýza hardwarových požadavků,
- sledovatelnost hardwarových požadavků,
- návrh hardwarové architektury,
- implementace hardwarových komponent,
- ověřování a validace v průběhu vývoje hardwaru. [44]

3.6.2 ASPICE for Cybersecurity

Německý svaz automobilového průmyslu se také rozhodl řešit aktuální problematiku kybernetické bezpečnosti a v srpnu roku 2021 přišel s rozšířením ASPICE for Cybersecurity. Rozšíření se skládá ze 122 stránek, logicky rozdělených na dvě části a celkově devět kapitol. [45]

Doplňuje základní oblasti o následující bezpečnostní aspekty:

- oblast **SYS.2** o systémovou identifikaci bezpečnostních požadavků a **SYS.3** zařazení bezpečnostních požadavků a bezpečnostních požadavků do návrhu architektury,
- oblast **SWE.1** až **SWE.6** o požadavky na navrhování, implementaci a testování softwarových komponent z pohledu kybernetické bezpečnosti,
- oblast **SUP.1** o posudek bezpečnostních vlastnostech produktu v rámci zajištění kvality, **SUP.8** o řízení bezpečnostních incidentů během celého životního cyklu produktu a **SUP.9** o bezpečnostní aspekty u řízení a právy konfigurace,
- oblast **MAN.5** o identifikaci kybernetických hrozeb a bezpečnostních slabín v rámci celkového řízení rizik. [45]

Dále definuje nově vzniklé oblasti, které nejsou součástí základního ASPICE. Jedná se o bezpečnostní procesy **SEC.1** až **SEC.7**, zaměřené na řízení bezpečnostních aktiv, analýzu hrozeb a návrh bezpečnostních opatření během celého životního cyklu produktu. [45]

Je důležité zmínit, že přestože rozšíření zní jako řešení problematiky této bakalářské práce, ve skutečnosti tomu tak není. Odůvodnění proč rozšíření není správným řešením se bude práce zabývat v praktické části, u analýzy výchozího stavu ASPICE.

3.7 Shrnutí třetí kapitoly

Třetí kapitola popisuje normu ASPICE verze 3.1, který je procesním referenčním a hodnotícím modelem v automobilovém průmyslu. Objasňuje její historii, účel a koncept V-Modelu. V rámci struktury jsou dílčí procesy děleny do 3 hlavních kategorií: primární, podpůrné a organizační. Každý proces obsahuje svoje ID, stručný popis, vstup, výstup, základní a rozšířené praktiky a atributy hodnotící schopnost procesu. Závěrem je kapitola doplněna o informace možného certifikovaného rozšíření základního rámce o HW-SPICE či ASPICE for Cybersecurity.

Z provedeného rozboru vyplývá, že norma ASPICE představuje komplexní a modulární rámec umožňující systematické hodnocení zlepšování a zvyšování kvality procesní zralosti organizací.

4 POPIS NORMY ISO 21434

Tato kapitola se věnuje podrobnému rozboru normy ISO 21434, která definuje požadavky na kybernetickou bezpečnost silničních vozidel. Norma řeší zvýšenou propojenost a komplexnost moderních vozidel, které závisí na softwarových a síťových systémech a přináší tím novou vlnu kyberbezpečnostních hrozeb a rizik. Definuje systematický a strukturovaný přístup pro identifikaci, zpracování a mírnění těchto rizik. [1]

4.1 Historie

Norma byla sice publikována v roce 2021, ale její kořeny sahají až do roku 2016, kdy ISO vytvořila technickou komisi s názvem ISO/TC 22/SC 32/WG 11. Původní záměr této pracovní skupiny bylo zajistit dostupné materiály, experty, organizace a základní praktiky zabývající se kybernetickou bezpečností v oblasti automobilového průmyslu a vytvořit podklady pro vznik nové normy. V roce 2018 pracovní skupina vydala ISO/SAE 21434 Inženýrství kybernetické bezpečnosti silničních vozidel, která byla předchůdcem nynější ISO 21434. [46]

Oficiálními autory normy jsou mezinárodní nezisková organizace ISO (International Organization for Standardization) a americká společnost SAE (Society of Automotive Engineers). Z toho vychází název ISO/SAE 21434, který byl zmíněn na začátku práce. Z hlediska praxe se však používá jen termín ISO 21434. [1]

4.2 Účel

Hlavním účelem normy je vytvořit komplexní metodický rámec, který umožní výrobcům vozidel systematicky řídit kybernetická rizika během celého životního cyklu vozidla. Norma se zaměřuje nejen na vývojové fáze, ale zahrnuje také výrobu, provoz, údržbu a princip nakládání s vozidly po ukončení jejich životnosti. Klade důraz na minimalizaci rizik spojených s útoky na vozidla, být v souladu s mezinárodními požadavky a tím zvýšit důvěrnost zákazníků a dotčených stran. [1]

4.2.1 Odlišnosti od jiných standardů kybernetické bezpečnosti

Existuje celá škála norem zabývajících se problematikou kybernetické bezpečnosti. Norma ISO 21434 se oproti ostatním liší těmito prvky:

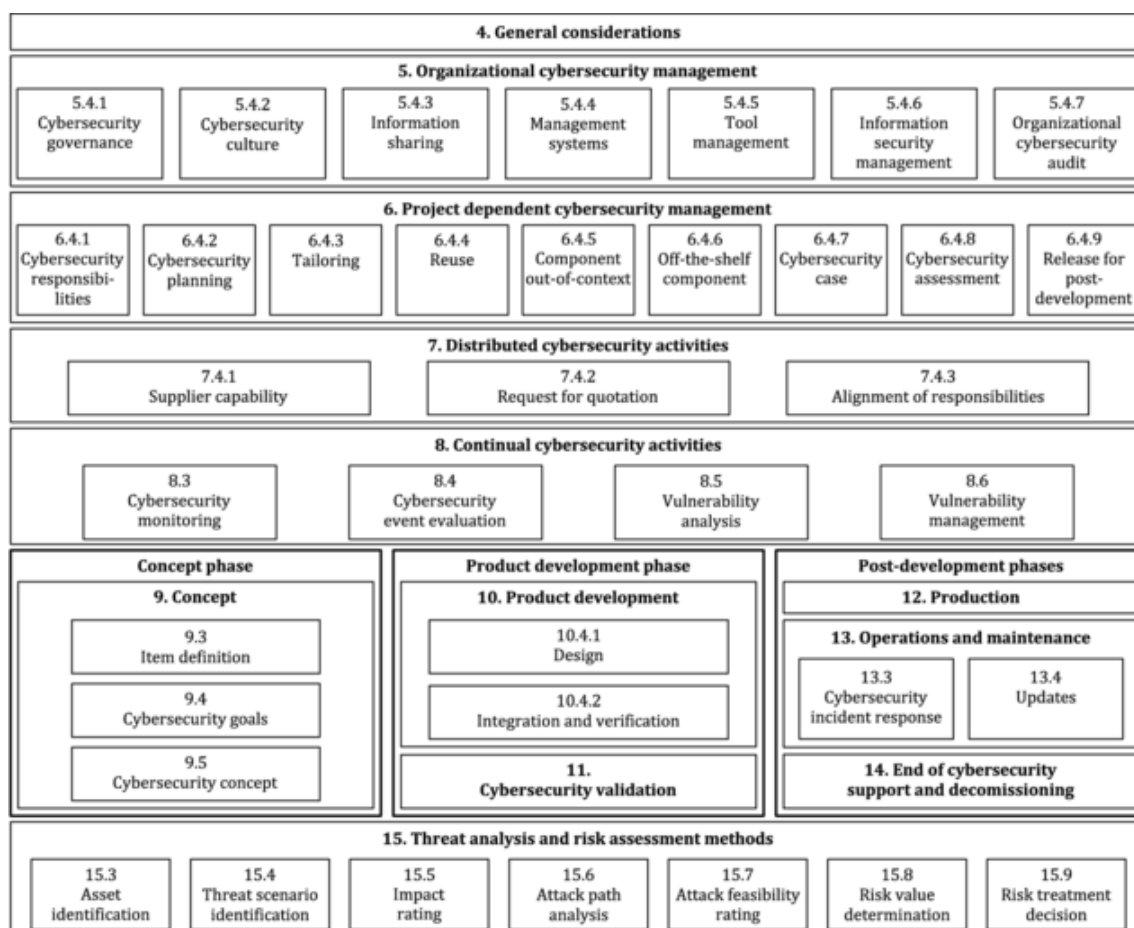
- důraz na integraci kybernetické bezpečnosti již od raných fází návrhu vozidla (Security-by-Design)

- nutnost specifikace bezpečnostních požadavků na jednotlivé komponenty vozidel
- stálé monitorování systému z hlediska možných rizik a zranitelností
- zohlednění specifických hrozeb týkajících se kybernetické bezpečnosti

Díky své soustředěnosti na konkrétní problematiku vyplnila norma díru na trhu, jelikož ostatní normy se automobilovou kybernetickou bezpečností zabývaly jen okrajově. [1]

4.3 Struktura

Samotný dokument je složen celkem z 15 částí a anexí A až F. Části jsou rozdělené do logicky navazujících kapitol. První část popisuje předmět normy, druhá normativní odkazy, třetí termíny a definice. Část čtvrtá až patnáctá se pak konkrétně věnuje problematice kybernetické bezpečnosti ve vozidlech, od obecných zásad až po metodiky TARA. Anexe doplňují normu o pomocné informativní přílohy, které však nejsou závazné. [1]

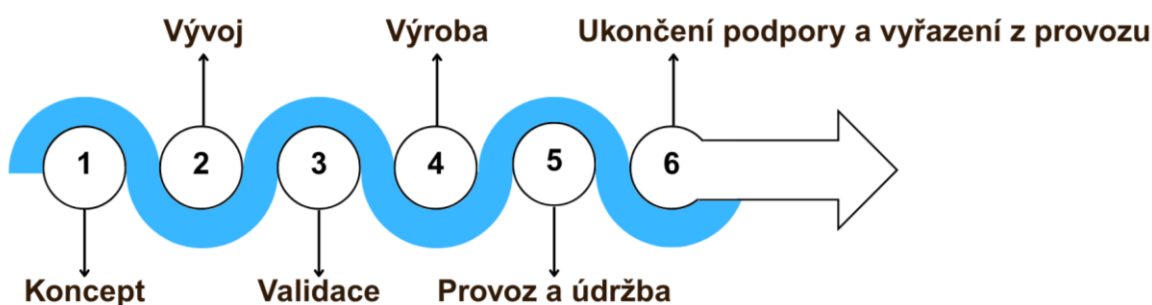


Obrázek 6 Struktura ISO 21434

(zdroj: [1])

4.4 Životní cyklus produktu

Norma ISO 21434 definuje svůj vlastní životní cyklus kybernetické bezpečnosti produktu. Cyklus začíná definicí nového systému či softwaru vozidla a končí vyřazením z provozu či likvidací. Na tomto principu si norma silně zakládá. [1]



Obrázek 7 Životní cyklus produktu dle ISO 21434

(zdroj: [1])

Fáze životního cyklu produktu jsou:

- **Fáze konceptu:** identifikace a vymezení bezpečnostních aktiv, provedení TARA, stanovení CAL a specifikace bezpečnostních cílů (v normě ISO 21434 obsah kapitoly 9)
- **Fáze vývoje produktu:** provedení návrhu a zařazení odpovídajících bezpečnostních opatření na úrovni architektury hardwaru, softwaru a systému (obsah kapitoly 10)
- **Fáze validace kybernetické bezpečnosti:** testování bezpečnostních opatření, schopnosti naplnění bezpečnostních cílů o ověřování účinnosti zmírňování rizik (v normě ISO 21434 obsah kapitoly 11)
- **Výrobní fáze:** kontrolování procesů použitých při výrobě pro zajištění integrity, dostupnosti a důvěrnosti produktu (v normě ISO 21434 obsah kapitoly 12)
- **Fáze provozu a údržby:** pozorování bezpečnostních aktiv a naplňování bezpečnostních cílů, monitorování, zaznamenávání a reagování na kyberbezpečnostní incidenty a kontrolování stavu zbytkového rizika (v normě ISO 21434 obsah kapitoly 13)

- **Fáze ukončení podpory a vyřazení z provozu:** bezpečné vyřazení s důrazem na likvidaci citlivých dat i komunikačního rozhraní (v normě ISO 21434 obsah kapitoly 14) [1]

4.5 Role a odpovědnosti v rámci normy

Definice rolí odpovědností v CSMS je klíčová pro zajištění bezpečnosti během celého životního cyklu produktu. [1]

Mezi tyto role a k nim odpovídající odpovědnosti se řadí:

- **Manažer kybernetické bezpečnosti** – určuje interní politiku kybernetické bezpečnosti organizace a zajišťuje soulad s relevantními zákony a vyhláškami kybernetické bezpečnosti
- **Produktový manažer kybernetické bezpečnosti** – ručí za začlenění kyberbezpečnosti do vývoje produktu a za soulad produktu s požadovanými kyberbezpečnostními standardy
- **Inženýr kybernetické bezpečnosti** – provádí TARA k identifikaci zranitelností a hrozeb, navrhuje a implementuje vhodná bezpečnostní opatření
- **Tým pro řešení bezpečnostních incidentů** – monitoruje, analyzuje a reaguje na bezpečnostní incidenty včetně jejich řešení a obnovu po incidentu
- **Manažer bezpečnosti dodavatelského řetězce** – kontroluje soulad dodavatelů a partnerů s požadovanými kyberbezpečnostními standardy [1]

Norma přináší řadu nových rolí, které vzájemnou propojeností umožňují efektivně řešit danou problematiku. Existuje řada dalších podpůrných rolí, například bezpečnostní tester, který se zabývá bezpečnostní strategií, bezpečnostními koncepty a samotným bezpečnostním testováním. [1]

Oblast bude detailněji pokryta a zařazena v praktické části bakalářské práce.

4.6 Vztah k ostatním normám, vyhláškám a regulacím

ISO 21434 není izolovaným dokumentem, ale součástí širšího ekosystému norem a vyhlášek a regulací v oblasti automobilového průmyslu a kybernetické bezpečnosti.

Její vztah k ostatním normám je popsán v následujících podkapitolách:

4.6.1 UNECE Předpis č. 155 a Předpis č.156

Splnění požadavků vyplývajících z těchto předpisů Evropské unie jsou zcela pokryty technickým základem normy ISO 21434. Projevuje se to například důrazem na existenci systému řízení kybernetické bezpečnosti a procesů řízení softwarových aktualizací (zde spadá OTA). [1] [8] [14]

4.6.2 ISO 26262

Jedná se o vzájemně se doplňující normy, kdy jejich společná implementace zaručuje bezpečné fungování systému i při selhání komponent a zároveň ochranu před kyberbezpečnostními útoky. Jedním z důvodů je možné využití zranitelnosti bezpečnostního aktiva a tím způsobit funkční selhání. Při kombinované integraci je zásadní zařadit požadavky obou norem již do návrhu systému. [1][2]

4.6.3 ISO 27001

ISO 27001 pokrývá problematiku managementu bezpečnosti informací a zaměřuje se na správu bezpečnosti informací v organizaci, principy řízení rizik a politik bezpečnosti. Tyto principy mohou být aplikovány i na automobilový sektor jako podpůrný rámec. [47]

4.7 Shrnutí čtvrté kapitoly

Kapitola se soustřeďuje na rozbor normy ISO 21434, která stanovuje požadavky na řízení kybernetické bezpečnosti v automobilovém průmyslu. Popisuje její původ vzniku, účel i rozdílnost oproti jiným normám s obdobnou problematikou.

Samotná struktura normy je velmi komplexní, jelikož se skládá z 15 kapitol a 6 anexí. Kapitola rozebírá také klíčové oblasti této normy, životní cyklus produktu, složeného z 6 fází a důležitosti určení rolí a odpovědností v rámci CSMS. Výklad doplňuje zmínka o vztahu s jinými normami a vyhláškami.

V této fázi práce jsou dostupné veškeré materiály pro zpracování problematiky tématu práce a provedení praktického výzkumu.

II PRAKTICKÁ ČÁST

5 CÍL PRÁCE

Cílem praktické části této bakalářské práce je provést výzkum pomocí analýzy dopadu k zjištění, jak implementace normy ISO 21434 do ASPICE verze 3.1 ovlivní určité oblasti softwarového a systémové vývoje v automobilovém průmyslu.

V první fázi výzkumu bude provedena takzvaná komparativní analýza mezi výchozím stavem ASPICE a požadavky ISO 21434, kde bude zmíněno i ASPICE rozšíření pro kybernetickou bezpečnost a zdůvodněno proč není vhodným a dostačujícím řešením problematiky. Výstupem komparativní analýzy budou specifické oblasti, které obsahují nedostatečné pokrytí vůči požadavkům ISO 21434. Tyto oblasti se následně stanou vstupem pro hlavní část výzkumu – analýzy dopadu. Analýza dopadu bude zkoumat, jaké nové aktivity, procesy a organizační změny bude potřeba provést. Také zde budou zkoumány případné potřeby nových nástrojů a s tím spojené dopady na náklady, výkonnost a plánování projektů, tak aby mohla norma ISO 21434 být úspěšně implementována. K zřehlednění celé problematiky doplní obě analýzy prvky vizualizace.

Ve třetí části výzkumu se z výsledků analýzy dopadu převedou dopady implementace zpět do ASPICE procesu. Bude se jednat o praktickou integraci požadavků ISO 21434 do konkrétních oblastí procesního rámce ASPICE a přiřazení hodnot a kritérií. Tuto část doplní Ishikawa diagram pro zřehlednění konkrétních dopadů implementace do procesu.

Poslední a závěrečná fáze výzkumu se bude zabývat návrhem opatření pro zmírnění dopadů, které implementace normy ISO 21434 způsobí. Stejně jako u analýzy dopadu a dopadu implementace do ASPICE procesu se bude návrh ošetření věnovat konkrétním oblastem pro zachování logického rozložení, doplněný o vizualizaci.

6 KOMPARATIVNÍ ANALÝZA POŽADAVKŮ NORMY ISO 21434 A VÝCHOZÍHO STAVU PROCESU ASPICE

Primárním cílem této kapitoly je porovnat rozsah pokrytí požadavků na kybernetickou bezpečnost v rámci normy Automotive SPICE verze 3.1 oproti požadavkům vyplývajících z normy ISO 21434. Během výzkumu pomocí komparativní analýzy bude soustředěna pozornost na identifikaci oblastí, kde se ASPICE a ISO 21434 plně shodují obsahem (jinými slovy vzniká překryv), a oblastí, které ASPICE nejsou z pohledu kybernetické bezpečnosti pokryty. Zjištěním mezer mezi procesem a normou vznikne podklad pro navazující a nejdůležitější část výzkumu – analýzu dopadu.

6.1 Analýza výchozího stavu ASPICE

Automotive SPICE verze 3.1 poskytuje vysoce propracovaný procesní rámec pro řízení vývoje softwarových a systémových komponent v automobilovém průmyslu. Na první pohled by se mohlo zdát, že je dostatečně komplexní. Po bližší inspekci z pohledu kybernetické bezpečnosti je jeho pokrytí však částečné. Jako první vstup pro vytvoření komparativní analýzy je potřeba zjistit, do jaké míry ASPICE pokrývá aspekty relevantní pro ochranu embedded systémů před kybernetickými hrozbami.

Prvním pozitivním aspektem z pohledu kybernetické bezpečnosti ASPICE ve verzi 3.1 je jeho systematický přístup pro řízení kvality vývoje a jeho procesů. To se projevuje nejen podporováním strukturovaného řízení požadavků, ale také návrhu, implementace, testování či správy konfigurace. Další oblasti ASPICE, které se do jisté míry zabývají kybernetickou bezpečností v automobilovém průmyslu jsou oblasti SYS.2, SYS.3, SWE.1 až SWE.6, MAN.5, SUP.1 a MAN.3.

Oblast SYS.2 (Systémová analýza požadavků) společně s oblastí SYS.3 (Systémový návrh požadavků) umožňují zaznamenání a začlenění bezpečnostních a kyberbezpečnostních požadavků, což je v souladu s ISO 21434 a tím vzniká možnost integrace požadavků, pokud jsou přesně definovány. V praxi však chybí specifikace, jak mají být požadavky identifikovány, analyzovány či jak se mají spravovat rizika související s hrozbami a zranitelnostmi.

Oblasti SWE.1 až SWE.6 (Softwarové procesy) poskytují rámec pro implementaci a testování komponent softwaru, což dává možnost zařadit ověřování kyberbezpečnostních funkcí do ověřovacích aktivit. Zde je stejná limitace jako u SYS.2 a SYS.3, znova je nutno,

aby požadavky byly přesně definované v dokumentaci. Oblasti SWE.1 až SWE.6 se také zaměřují převážně na funkční správnost a robustnost.

Oblasti MAN.5 (Řízení rizik) a SUP.1. (Zajištění kvality) zajišťují obecné mechanismy, které lze použít k identifikaci a mitigaci rizik a správu kvality. Záměr je sice směřován na rizika v širším úhlu pohledu a není zde zvláštní kategorizace přímo pro kyberbezpečnostní hrozby, ale z pohledu kybernetické bezpečnosti se jedná o částečný překryv.

Oblast SUP.1 se zároveň společně s MAN.3 zabývá celkovou dokumentací v rámci ASPICE 3.1 procesu a požaduje, aby všechny činnosti byly dokumentovány, kontrolovány a spravovány. Evidence v oblasti kybernetické bezpečnosti proces však konkrétně neurčuje, což ovšem nepředstavuje až tak velký problém.

Verifikace požadavků je pokryta v oblastech SWE. 4 až SWE.6, SYS.2 a SUP.1., kde je pokrytí úplné. Chybí zde pouze kategorizace pro kyberbezpečnostní a bezpečnostní požadavky.

6.1.1 Nedostačující řešení problematiky

Jak už bylo zmíněno v teoretické části práce, v roce 2021 vzniklo rozšíření základního ASPICE, které nese název ASPICE for Cybersecurity. I když rozšíření poskytuje doplňující podklady pro řešení kybernetické bezpečnosti, jeho implementace v praxi není rozšířená a není přímou součástí základního ASPICE 3.1. Největším nedostatkem je ovšem skutečnost, že ani toto rozšíření nepokrývá požadavky ISO 21434 na 100 % a je na této normě založen pouze částečně.

Z hlediska praxe je pro firmu i zákazníka nutné dodržovat proces ASPICE a zároveň plnění požadavků ISO 21434. I když rozšíření ASPICE for Cybersecurity byl dobrý pokus o řešení problematiky, není dostačující a z toho důvodu o něj není zájem.

6.2 Analýza požadavků ISO 21434

Norma ISO 21434 klade velký důraz na systematickou ochranu před kybernetickými hrozbami v oblasti automobilového průmyslu. A to od v rámci celého životního cyklu produktu, od úplného počátku práce až do zničení produktu.

Prvním důležitým a poměrně komplexním požadavkem je provedení analýzy posuzování rizik kybernetické bezpečnosti, které se v normě říká TARA. V první fázi je

zapotřebí stanovit všechna aktiva v systému (hardwarové komponenty, softwarové komponenty, datové toky, komunikační systémy apod.), které mohou čelit kybernetickým útokům. V praxi se jedná o vytvoření strukturovaného seznamu všech částí systému, nesmí se na nic zapomenout.

Vůči nalezeným aktivům je poté esenciální najít hrozby, jejich realizaci a zranitelnosti, jež by mohly aktivum ovlivnit a ohrozit. K této činnosti je zapotřebí znát nejen celou architekturu systému, ale také znalost aktuálních hrozeb v oblasti automobilové kybernetické bezpečnosti a schopnost používat metodiky, jako je například STRIDE. STRIDE metodika v sobě skrývá zkratku 6 typů hrozeb (S – Spoofing, T – Tampering, R – Repudiation, I – Information Disclosure, D – Denial of Service a E – Elevation of Privilege) a slouží k analýze hrozeb a zjištění zranitelností v rámci softwarových systémů.

Ke zjištěným hrozbám je následně nutné přiřadit jejich pravděpodobnost realizace a jejich potenciální dopad na bezpečnost vozidla. Dokončení TARA je vstupem pro určení úrovně zajištění kybernetické bezpečnosti, dříve zmíněnými úrovněmi CAL (1 až 4).

TARA také vytváří základ pro formulaci bezpečnostních cílů a zpřesnění bezpečnostních požadavků, což je další požadavek normy. Bezpečnostní cíle a požadavky musí být konkrétní, měřitelné a jednoznačně provázané s riziky, které mají mitigovat. V praxi to znamená vytvoření specifikací (systémových i softwarových), do nichž jsou poté zařazeny bezpečnostní a kyberbezpečnostní požadavky. Je kladen důraz i na návrh bezpečnostních konceptů. Bezpečnostní koncepty spojují více opatření pro chránění klíčových aktiv před vybranými útoky. Opatření musí být provedena nejen na úrovni architektury (např. oddělení kritických funkcí), ale také na úrovni implementace (např. autentizace, šifrování). Z hlediska praxe se jedná o začlenění kyberbezpečnostního testování do testovací strategie. Všechny zmíněné body tohoto odstavce musí být provedeny již v rané fázi vývoje.

Dalším důležitým požadavkem je zavedení procesů pro ověřování a validaci kybernetické bezpečnosti a kyberbezpečnostních požadavků.

Následujícím požadavkem normy je řízení bezpečnosti během provozu. Za nutné se považuje monitorování bezpečnostních stavů produktů během provozu, analyzování bezpečnostních incidentů a v případě potřeby rychlé reagování za pomoci aktualizace softwaru či zavedení nápravných opatření. Například schopnost provádění aktualizace OTA.

V oblasti organizační bezpečnosti je také požadavek, a to zavedení vnitřních pravidel a procesů pro správu bezpečnosti, vymezení odpovědností a zajištění průběžné správy a aktualizace bezpečnostní dokumentace. Z hlediska praxe se jedná o existenci bezpečnostních týmů a bezpečnostních rolí s kvalifikací a pochopením problematiky. Nutná je i integrace bezpečnostního řízení do všech organizačních oblastí, jsou-li relevantní.

Systematická dokumentace je v normě označená za velmi důležitou a musí obsahovat všechny aktivity spojené s kybernetickou bezpečností. Cílem správné dokumentace je schopnost dohledání zpětného rozhodnutí, být prostředkem pro auditovatelnost, a hlavně popisovat důkaz o plnění požadavků.

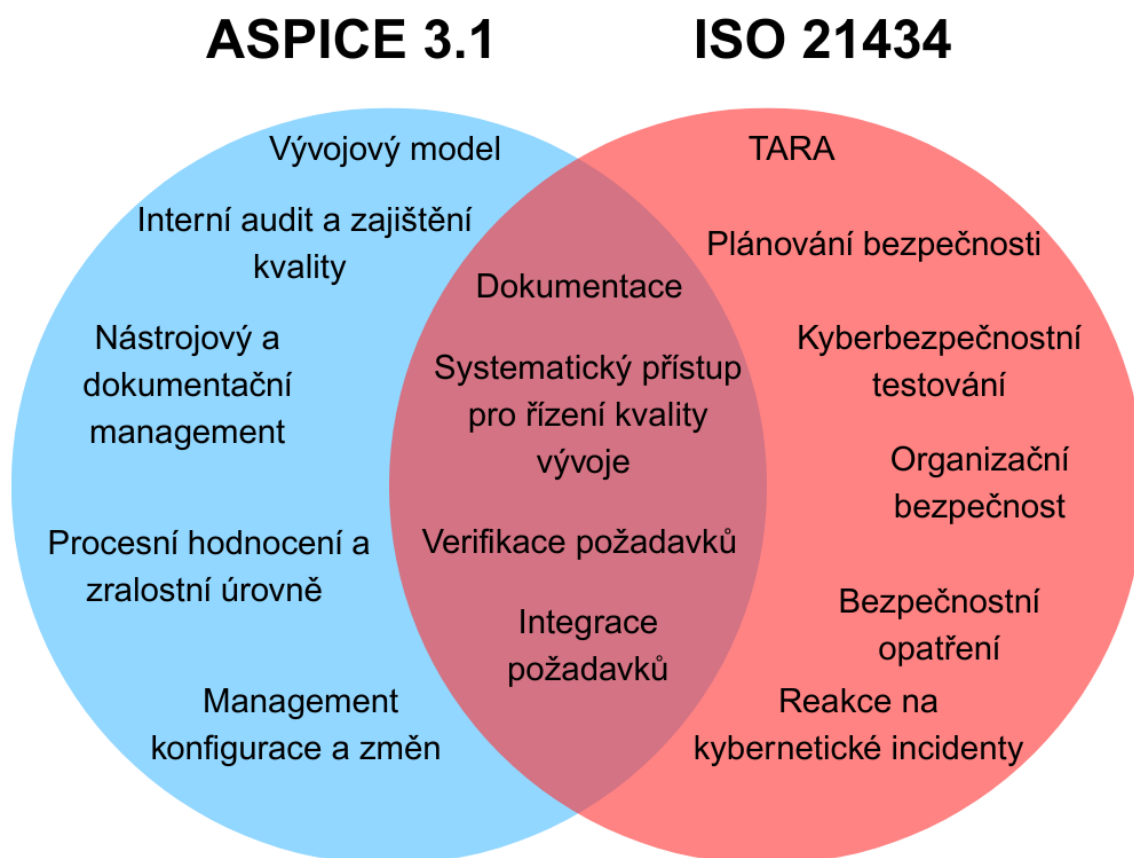
Z analýzy požadavků ISO 21434 vyplývá, že požaduje mnohem detailnější a systematictější přístup ke kybernetické bezpečnosti, než samostatný ASPICE ve verzi 3.1 nabízí.

6.3 Výsledek komparativní analýzy

Po zjištění výstupů z analýzy výchozího stavu ASPICE 3.1 a požadavků vyplývajících z ISO 21434 je nyní možné dokončit celkovou komparativní analýzu.

Tyto konkrétní oblasti bude z výsledku komparativní analýzy potřeba vyřešit:

- systematické analýzy hrozeb a zranitelností,
- hodnocení a správy kybernetických rizik,
- definice bezpečnostních opatření na základě kybernetických analýz,
- plánování bezpečnosti v provozní fázi produktu,
- bezpečnostního testování v testovací strategii,
- řízení a reakce na kybernetické incidenty,
- existence bezpečnostních týmů v organizaci,
- organizační bezpečnosti, školení a kompetence zaměstnanců.



Obrázek 8 Vennův diagram překrytí a nedostatků ASPICE 3.1 vůči požadavkům ISO 21434

(zdroj: vlastní)

Obrázek 8 znázorňuje, ve kterých oblastech dochází k překryvu a oproti tomu oblasti, jenž se bude práce věnovat v dalších částech. Ke znázornění byl použit Vennův diagram.

6.4 Shrnutí šesté kapitoly

V rámci šesté kapitoly byla provedena analýza výchozího stavu ASPICE ve verzi 3.1 a jeho pokrytí kybernetické bezpečnosti v automobilovém průmyslu a identifikace požadavků vyplývajících z normy ISO 21434.

Analýza výchozího stavu ASPICE prokázala, že je nabízen robustní rámec pro řízení vývojových procesů v rámci vývoje. V oblastech dokumentace, systematického přístupu pro řízení kvality vývoje a verifikace i integrace byl prokázán překryv. Avšak chybí například systematické provedení analýzy posuzování rizik kybernetické bezpečnosti.

Z analýzy požadavků ISO 21434 bylo potvrzeno, že norma požaduje systematictější a detailnější přístup ke kybernetické bezpečnosti během celého životního cyklu produktu.

Norma si zakládá primárně na identifikaci hrozeb a zranitelností, nutnosti kybernetického testování, bezpečnostním plánováním v rámci provozní fáze systému, organizační bezpečnosti, reakci na incidenty a definici bezpečnostních opatření v rané fázi produktu.

Porovnáním bylo dokázáno, že existují určité oblasti překryvu, zejména v řízení požadavků, systémovém přístupu a dokumentaci. Nicméně bude nutné provést implementaci nedostatečně pokrytých oblastí a zároveň rozšíření a úpravu stávajících procesů.

Výstup této komparativní analýzy bude sloužit jako základ pro analýzu dopadu, kterou se bude zabývat následující část práce.

7 ANALÝZA DOPADU

Na základě provedené komparativní analýzy, jež znázornila překryv a nedostatky výchozího stavu ASPICE 3.1 ve srovnání s požadavky z normy ISO 21434, je zřejmé, že proces je ve výchozím stavu nedostačující a bude zapotřebí rozšíření a úprava jeho dílčích procesů.

Tato kapitola se zabývá konkrétními kroky, které musí být dodrženy, aby došlo k souladu s normou ISO 21434. Dále se zabývá analýzou dopadu, které implementací těchto kroků vzniknou v oblastech samotné organizace, nástrojů, lidských zdrojů, řízení projektu a procesů.

Cílem této analýzy je zodpovězení na následující otázky:

- jaké nové činnosti a procesy bude nutné zavést,
- jaké změny v organizaci a kompetencích budou vyžadovány,
- jaké nové nástroje a metodiky bude potřeba integrovat,
- jaký bude očekávaný dopad na náklady, výkonnost a časové plánování projektů.

Na základě výsledku analýzy dopadu bude v další části zpracována analýza dopadu implementace zpět do procesu a jeho specifických oblastí.

7.1 Nové činnosti a procesy vyžadované implementací ISO 21434

Implementace normy ISO 21434 s sebou přináší řadu nových specifických činností, které se doposud v ASPICE 3.1 nenachází. Jedná se primárně o následující činnosti:

- zavedení nových procesů s cílem konkrétní identifikace a analýzy aktiv a s nimi spojených hrozeb a zranitelností,
- vytvoření procesu analýzy a hodnocení potenciálních rizik v oblasti kybernetické bezpečnosti a ohodnocení úrovně zabezpečení,
- definice a správa bezpečnostních opatření a cílů již od rané části životního cyklu produktu,
- vytvoření bezpečnostních konceptů, které musí být vnořeny přímo do návrhu systémové a softwarové architektury,
- zřízení kyberbezpečnostního plánu, jež bude obsahovat celkové pokrytí oblasti kyberbezpečnosti v organizaci a potvrzovat soulad s normou ISO 21434,

- zavedení procesu pro rozpoznání a reakce na kybernetické incidenty během provozu spolu s dodržením periodické aktualizace systému.

Zmíněné nově vytvořené procesy a činnosti musí být integrovány do současného vývojového modelu organizace a musí dojít k provázání mezi ostatními již existujícími procesy, jako jsou například správa konfigurace, řízení kvality či řízení změn.

7.2 Dopady implementace na organizační strukturu a kompetence

Z pohledu požadavků normy ISO 21434 nastane potřeba poměrně intenzivně zasáhnout do organizační struktury a zlepšení kompetence zaměstnanců.

Týká se zejména:

- zajištění existence bezpečnostních týmů a zajištění propojenosti s ostatními týmy, které se dotýkají či zabývají prací na produktu v jakékoliv části jeho životního cyklu,
- zavedení nových rolí zaměřených na kybernetickou bezpečnost ve výše zmíněných týmech (například bezpečnostní architekt, manažer bezpečnostních incidentů a rizik, specialista na bezpečnostní testování a metodiky),
- školení již zaměstnaných pracovníků v oblasti kybernetické bezpečnosti, analýzy rizik, bezpečnostní architektury a základního bezpečnostního testování,
- přiřazení odpovědností a rolí v rámci kybernetické bezpečnosti a CSMS,
- upravení interní politiky a zařazení řízení kybernetické bezpečnosti v projektovém řízení a celkovém vývoji produktu.

Je patrné, že zavedení změn organizační bezpečnosti bude vysoce nákladné jak časově, tak i finančně. A to z důvodů náboru nových kvalifikovaných zaměstnanců, adaptace současných zaměstnanců a přeuspořádání celé organizační struktury a interní politiky.

7.3 Dopady implementace na nástroje a technické infrastruktury

Naplnění požadavků dle normy ISO 21434 významně ovlivňuje používané nástroje ve vývoji produktu, testovací strategii, správu bezpečnostních požadavků a provozní bezpečnost.

Nejdůležitější je integrace nástrojů či softwaru pro modelaci hrozeb a analýzu útoků, sloužící k lepší vizualizaci potenciálních útoků a odhalení zranitelností u aktiv již v rané fázi

projektu. Příklady nástrojů jsou ThreadModeler, Microsoft Threat Tool či SecuriCAD. Nástroje musí být předem definované v dokumentaci a verifikované.

Bezpečnostní testování musí být podchyceno dalšími novými nástroji pro tuto problematiku. Nástroje musí umožňovat řešit různé typy bezpečnostního testování jako je penetrační testování, provádění simulačních testů a testování odolnosti systému vůči kybernetickým útokům. Zavedením bezpečnostního testování a rozšířením testovacích nástrojů se bude muset upravit i testovací strategie, do níž bude nutné tuto novou oblast testování integrovat. Testovací strategie bude muset být rozšířena i o analýzu po provedeném simulovaném útoku. Pro vysvětlení, testovací strategie představuje plán testování v celém životním cyklu produktu a detailně popisuje každou fázi s informacemi co a na čem se bude testovat. Vše musí být důkladně zdokumentováno.

Provozní bezpečnost z pohledu ISO 21434 musí být doplněna o nástroje dávající schopnost monitorování bezpečnostního stavu produktu v provozu spolu s kontrolou řízení bezpečnostních incidentů, což je provázáno se dříve zmíněným procesem pro rozpoznání a reakcí na incidenty.

Na definování vhodných nástrojů pro splnění požadavků ISO 21434 navazuje zvolení vhodných hardwarových zařízení, aby bylo testování a splnění provozní bezpečnosti zajištěno. Samotná hardwarová zařízení musí být odolná vůči kybernetickým útokům a být vhodně zabezpečena a zálohována. Jako další prvek technické infrastruktury se zde objevují i bezpečnostní požadavky, které musí být jednoznačně definovány a kategorizovány. S tím se pojí i jejich dohledatelnost a spojení s k nim patřícími riziky.

Implementace zmíněných nových nástrojů a nutná úprava technické infrastruktury přinese další dopad na čas i finanční náklady. Samotný výběr softwarových nástrojů i hardwarového vybavení bude z velké míry záležet na preferencích a rozpočtu organizace. Úprava testovací strategie přináší nutnost úpravy interních procesů organizace, uzpůsobení metodik vývoje a testování. V této části výzkumu jde jasně vidět vzájemné propojení mezi všemi dopady a bez splnění jedné části nemůže být implementace kompletní.

7.4 Dopady implementace na výkonnost, náklady a plánování projektů

K dosažení správné implementace ISO 21434 je nutné podívat se blíže i na samotný projekt a dopady pokrytí požadavků normy v časovém plánování jeho realizace, výkonnosti a

nákladové struktury. Zařazení nových procesů a činností povede k zásadní změně v dosavadní organizaci práce a dojde i na zvýšení kapacitních nároků projektových týmů.

Jak již bylo zjištěno v předešlých fázích výzkumu, bude z hlediska plánování potřeba počítat se zpožděním v každé fázi vývoje produktu. Přidání nových činností, zařazení nových nutných bezpečnostních procesů, definic a zařazení bezpečnostních opatření vyžaduje značné množství času. Ovlivněn bude celý harmonogram, je nezbytné důkladně projít veškeré současné plány a doplnit milníky projektu o bezpečnostní aktivity. Při snaze si implementaci zjednodušit a vynechat nějaký proces či činnost hrozí riziko nedodržení bezpečnostní úrovně. Nejvíce časově náročná bude počáteční implementace, kde je potřeba počítat i s určitým vyhrazeným časovým oknem pro školení zaměstnanců a výběr kvalifikovaných odborníků. Mimo kvalifikace a školení je na počátku nutné brát v potaz, že bude mnohem složitější implementovat požadavky během již rozjetého projektu oproti projektu v rané fázi. Celkový dopad na časové plánování projektu silně ovlivní časové rozhraní vývoje, termíny dodávek i plánování zdrojů.

Výkonnost projektových procesů bude ovlivněna primárně přidáním k současným aktivitám vývoje nové činnosti se zaměřením na kybernetickou bezpečnost, návrhem bezpečnostních konceptů, úpravou testovací strategie i řízením bezpečnosti v provozní fázi projektu. Lze předpokládat zvýšení složitosti v oblasti projektového řízení a prodloužení celkového životního cyklu produktu.

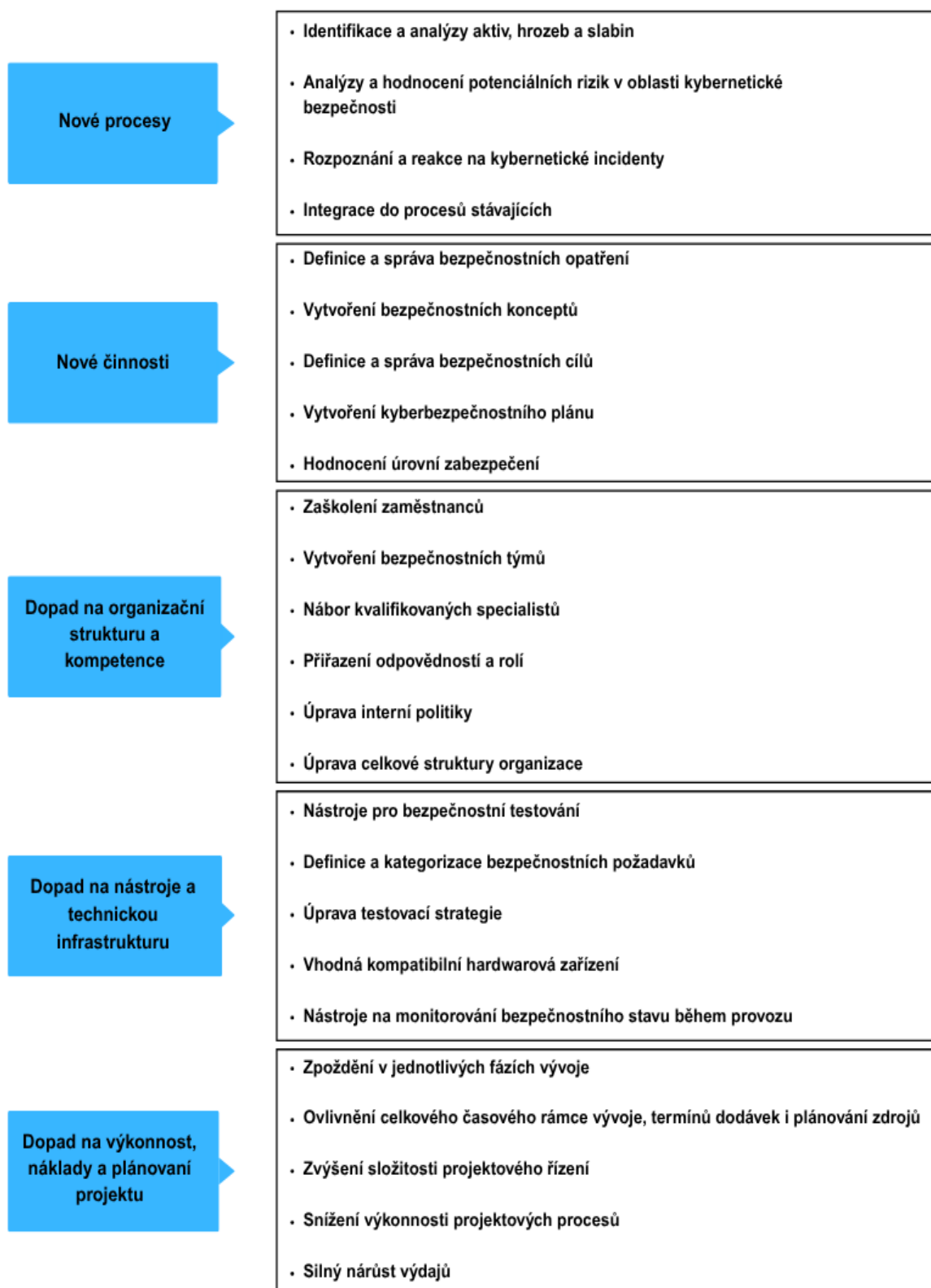
Nákladová náročnost bude rovněž významně ovlivněna. Implementace ISO 21434 představuje vysoké investice do nákupu a integraci nových softwarových nástrojů pro analýzu hrozeb, správu bezpečnostních požadavků a bezpečnostního testování. Další náklady vzniknou v oblasti školení zaměstnanců v oblasti kybernetické bezpečnosti, zařazením nových bezpečnostních týmů, úpravě organizace i náboru kvalifikovaných odborníků. Těmto kvalifikovaným osobám je samozřejmě potřeba posléze platit mzdu. Organizace také budou muset zvážit investici do certifikací či případně externích konzultací pro kontrolu kompletnosti implementace požadavků vyplývajících z ISO 21434. Zmíněné zpoždění harmonogramu projektu také zabere určité finanční prostředky.

Celkově implementace ISO 21434 přímo zasáhne do celkového plánování, výkonnosti a finančních prostředků projektu. Bude nezbytné počítat se zpožděním harmonogramu projektu, zvýšením komplexnosti řízení projektu i vyššími náklady. Tyto dopady je nutné brát v potaz již v raných fázích plánování projektu z důvodu efektivní implementace normy, pokud je to možné. Výzkumem došlo k potvrzení spojitosti mezi jednotlivými dopady.

7.5 Výsledek analýzy dopadu

Provedení analýzy dopadu ukázalo množství zasažených oblastí, jež bude potřeba upravit a rozšířit pro docílení splnění požadavků normy ISO 21434. Výzkum prokázal zásah do více klíčových oblastí organizace, jež bude nutno zařídit pro soulad procesu s normou ISO 21434. Oblasti a jejich dopady se vzájemně prolínají a dokazují komplexnost normy při jejím dodržení. Znázornění pomáhá lepšímu pochopení celkové problematiky a vytyčuje stěžejní kroky nutné k implementaci.

Zpřehlednění nově vzniklých činností, procesů a všech ostatních dopadů nutných k implementaci znázorňuje Obrázek 9.



Obrázek 9 Výsledek analýzy dopadu implementace normy ISO 21434

(zdroj: vlastní)

7.6 Vztah výsledku analýzy dopadu s výsledky komparativní analýzy

V této fázi výzkumu je žádoucí porovnání výsledků analýzy dopadu s výsledky komparativní analýzy, vstupy samotné analýzy dopadu. Obrázek 10 jednoznačně ilustruje spojitost mezi těmito výsledky a dokazuje plné pokrytí všech výstupů komparativní analýzy.



Obrázek 10 Propojení výsledků analýzy dopadu s výsledky komparativní analýzy

(zdroj: vlastní)

7.7 Shrnutí sedmé kapitoly

Sedmá kapitola se zabývala analýzou dopadu a zdůrazněním všech potřebných kroků pro správnou implementaci normy ISO 21434. Byla identifikována nutnost nejen vytvoření nových procesů a činností pro vyřešení problematiky týkající se oblasti kybernetické bezpečnosti, ale také nutnost integrace nových nástrojů a s nimi propojenými úpravami testovací strategie a technické infrastruktury. V průběhu výzkumu se ukázal nevyhnutelný

zásah do organizační struktury, interní politiky, znalostí kybernetické bezpečnosti současných zaměstnanců a žádoucí nábor kvalifikovaných pracovníků.

Všechny výše zmíněné body prokázaly dopad na výkonnost, časové plánování a náklady rozpočtu, se kterými se budou organizace muset potýkat k dodržení shody s normou ISO 21434. Pro zlepšení přehledu dopadové analýzy a také její provázanosti s výsledky komparativní analýzy pro zaručení úplnosti řešení problematiky byla kapitola doplněna o vizualizace.

Jednalo se o použití analýzy dopadu typu analýza závislostí, jelikož umožňuje identifikovat oblasti ovlivněné implementací normy ISO 21434 a určit, jaké změny bude nutné provést pro zajištění souladu s touto normou.

Výsledek analýzy dopadu bude použit v následující kapitole pro zařazení dopadu implementace do konkrétních oblastí procesu ASPICE 3.1.

8 DOPADY IMPLEMENTACE NA PROCES ASPICE

Po dokončení analýzy dopadu je další fází výzkumu zařadit nalezené oblasti implementace zpět do částí ASPICE verze 3.1. Nebude se jednat o pouhé doplnění jednotlivých činností, ale o nutné komplexní přehodnocení a úpravu stávajících procesů. Cílem této kapitoly je zařadit požadavky implementace do konkrétních oblastí ASPICE a provést analýzu jejich důsledků na oblasti procesu, lidských zdrojů a kompetencí, nástrojů, technologické infrastruktury a technického testování, ale i na samostatné projektové řízení a plánování. Dopady na tyto oblasti budou obohaceny o hodnoty a kritéria pro zlepšení viditelnosti dopadu implementace do procesu. Kapitola bude podpořena také vizualizací pomocí Ishikawa diagramu pro zprehlednění hlavních příčin a následků implementace ISO 21434.

Na začátek je nutné zmínit, že termínem týdný se rozumí člověkotýdný, nikoliv délka realizace v kalendářním času.

8.1 Dopady na procesní oblasti

Nejvýraznější dopady implementace ISO 21434 do procesu ASPICE 3.1 se objeví hned v několika klíčových oblastech procesu. Konkrétně se bude jednat o oblast SYS.2 (Analýza systémových požadavků), SYS.3 (Systémový návrh architektury) SWE.1 až SWE.6 (Vývojové procesy), MAN.5 (Řízení rizik), SUP.1 (Správa kvality), SUP.9 (Řízení konfigurace) a SUP.10 (Řízení změnových požadavků).

8.1.1 SYS.2 a SYS.3

Rozšíření stávajících procesů o identifikaci aktiv, hrozeb a zranitelností se bude týkat oblastí SYS.2 a SYS.3. Zde bude zapotřebí zařadit konkrétní kategorizaci a zpracování systémových bezpečnostních požadavků, včetně jejich provázanosti na systémové komponenty. Návrh systémové architektury bude muset obsahovat zohlednění principů bezpečnosti v návrhu (Security-by-Design). Součástí rozšíření systémové architektury je i analýza a definice bezpečnostních opatření a bezpečnostních cílů. Rozšíření představuje značný zásah do celkové systémové architektury produktu a analýzu všech aktiv z důvodu zařazení bezpečnostních požadavků do specifické kategorie. Časové rozhraní implementace do těchto oblastí procesu bude záležet na následujících kategoriích:

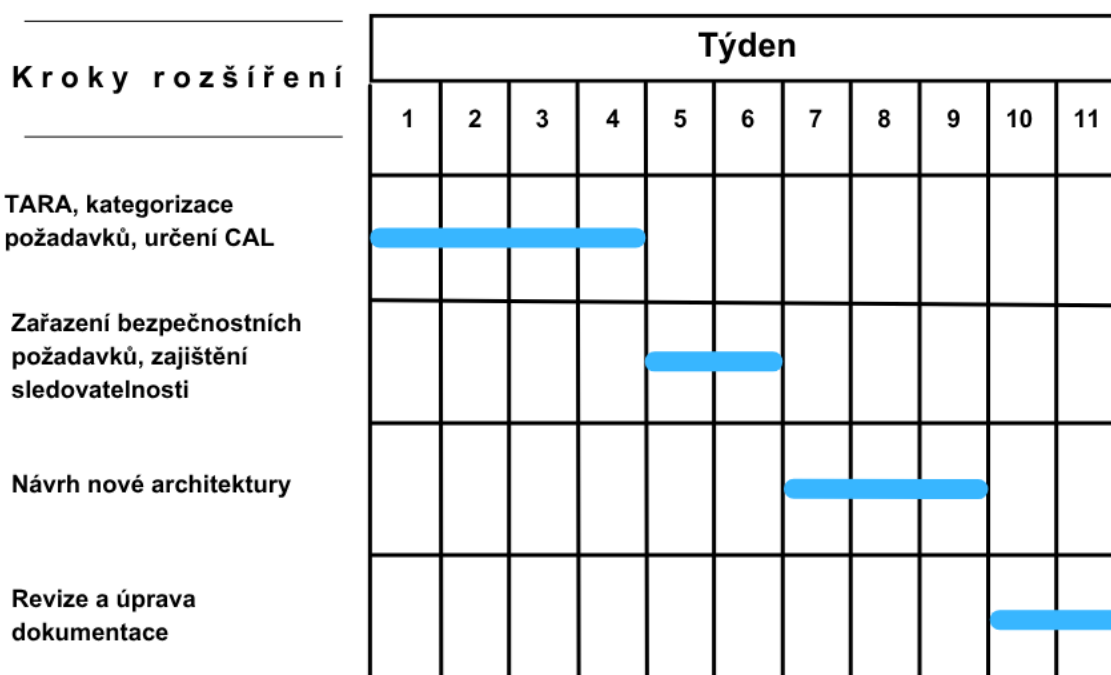
- komplikovanosti stávající architektury systémových komponent,
- množství analyzovaných aktiv a s nimi spojených hrozeb a zranitelností,

- délce vypracování analýzy hrozeb (TARA),
- úrovni požadovaného zabezpečení,
- velikosti samotného projektu,
- rychlosti správného vypracování nově vzniklé systémové architektury,
- návaznosti systémové architektury komponent na jiné komponenty.

Konkrétně se jedná o tento časový odhad:

- TARA, analýza a kategorizace bezpečnostních požadavků, určení úrovně zabezpečení (2–4 týdny),
- zařazení a sledovatelnost mezi požadavky, bezpečnostními požadavky a odpovídajícími hrozbami a zranitelnostmi (1–2 týdny),
- návrh nové systémové architektury (2-3 týdny),
- revize a úprava dokumentace (1–2 týdny).

U jednodušších menších až středních projektů se bude jednat o časové rozhraní cca 6 až 8 týdnů, zatímco u složitých komplexních větších projektů se bude organizace zabývat až 11 týdnů nutné práce.



Obrázek 11 Ganttův diagram rozšíření SYS.2 a SYS.3 u většího projektu

(zdroj: vlastní)

8.1.2 SWE.1 až SWE.6

Na systémové oblasti přímo navazují vývojové oblasti SWE.1 až SWE.6. Dle výsledků TARA musí být analyzovány a vytvořeny konkrétní softwarové bezpečnostní požadavky s jednoznačnou propojeností a návazností na bezpečnostní systémové požadavky. Softwarové bezpečnostní požadavky vyžadují kategorizaci z hlediska integrity, důvěrnosti a dostupnosti. Podobně jako u rozšíření systému musí dojít k přehodnocení stávající softwarové architektury a návrhu nové softwarové architektury i jednotlivých částí kódu, rozšířených o kategorizované softwarové bezpečnostní požadavky. Po dokončení softwarové architektury musí být do návrhu doplněny bezpečnostní mechanismy a směrnice pro psaní kódu. Vývojové oblasti se zabývají také tematikou bezpečnostního testování a nástrojů. Těm bude věnována pozornost zvlášť ve vlastní podkapitole. Obdobně jako u systémového rozšíření záleží doba vyřešení této problematiky na následujících kategoriích:

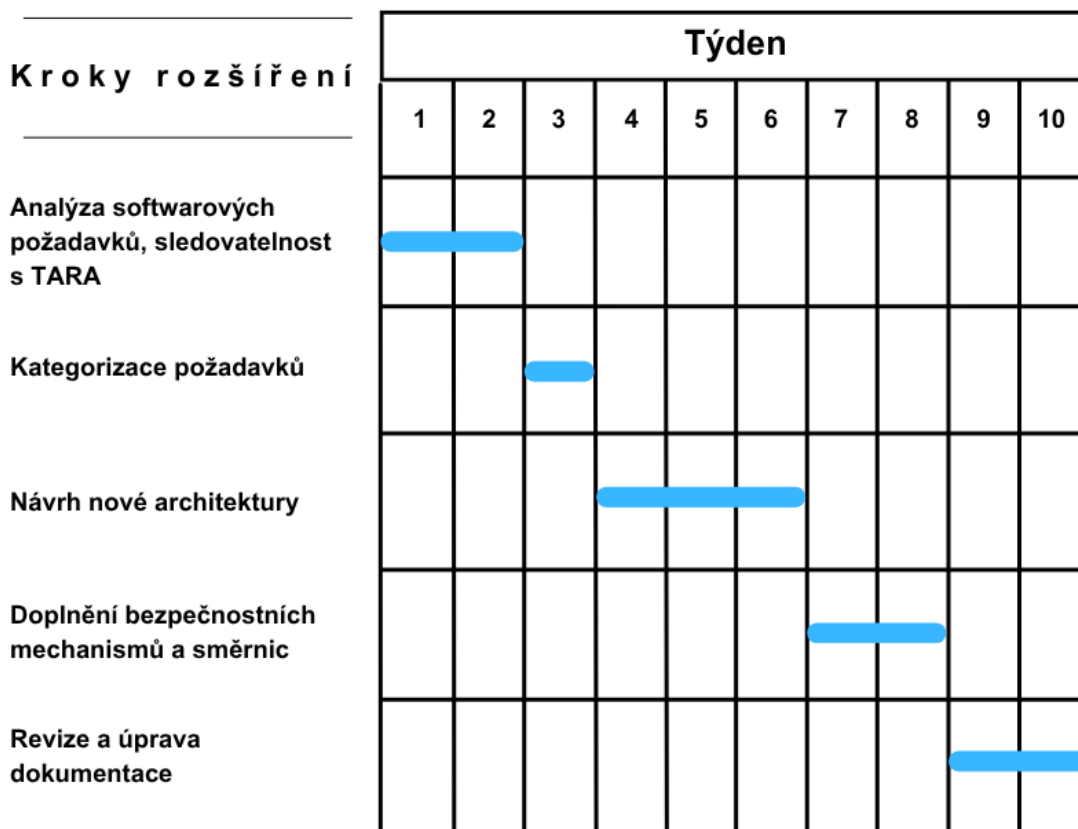
- komplexnosti zjištěných systémových bezpečnostních požadavků a nové systémové architektury,
- množství a složitosti identifikovaných softwarových požadavků,
- složitosti kategorizace dle integrity, důvěrnosti a dostupnosti,
- stavu a množství vazeb mezi základními softwarovými a bezpečnostními softwarovými požadavky,
- rychlosti zpracování rozšířené softwarové architektury dle systémové architektury,
- rychlosti zpracování a úpravy dokumentace.

Časový horizont expanze SWE.1 až SWE.6 pro soulad s ISO 21434 se pohybuje v těchto hodnotách:

- analýza softwarových bezpečnostních požadavků a jejich propojenost s TARA (1-2 týdny),
- kategorizace nových softwarových bezpečnostních požadavků z různých hledisek (0.5-1 týden),
- návrh softwarové architektury (2-3 týdny),
- doplnění softwarové architektury o bezpečnostní mechanismy a směrnice pro psaní kódu (1-2 týdny),

- revize a úprava dokumentace (1-2 týdny).

Tato fáze rozšíření zabere tedy při standardní složitosti softwaru zhruba 5.5 týdne práce oproti komplikovanému softwaru, jež bude potřebovat časovou investici 10 týdnů práce.



Obrázek 12 Ganttův diagram rozšíření SWE.1 až SWE.6 v případě složitějšího softwaru

(zdroj: vlastní)

8.1.3 MAN.5

Další oblastí ASPICE 3.1 je MAN.5, která se bude týkat rozšíření o bezpečnostní rizika, vyhodnocování pravděpodobností a dopadů hrozeb a plánování mitigací rizika. Důležitou změnou oproti původnímu stavu je přidání samotného toku pro řízení kybernetických rizik do současné obecné správy projektových rizik. Nutné bude myslet i na opakované přehodnocení rizik v provozní fázi. Bude záležet na kritériích:

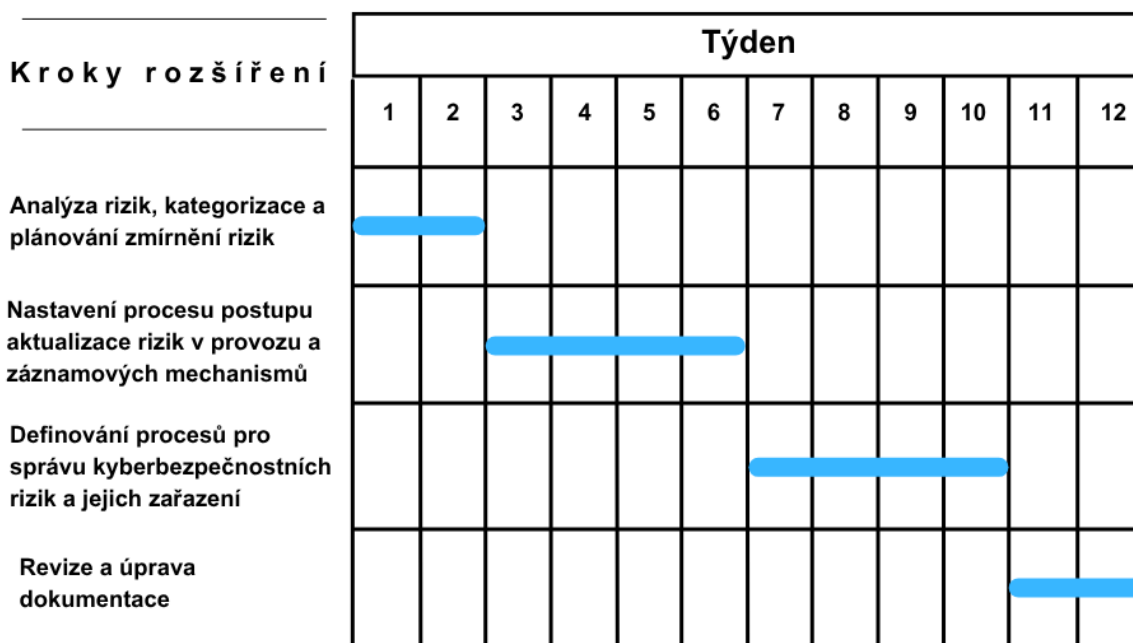
- množství analyzovaných rizik a jejich kategorizaci do skupiny bezpečnostních,
- rychlosti vyhodnocení dopadů, pravděpodobností a hrozeb,
- náročnosti plánování mitigací rizika,

- složitosti obecné správy projektových rizik a možnostech včlenění nového specifického toku pro kybernetické rizika.

V časovém měřítku se jedná o tyto konkrétní hodnoty:

- analýza rizik a kategorizace, plánování mitigací rizik (1-2 týdny),
- definování procesu pro správu zvláště kategorizovaných rizik v oblasti kybernetické bezpečnosti a zařazení do obecné správy projektových rizik (3-4 týdny),
- nastavení procesu postupu aktualizace rizik v provozu a záznamových mechanismů (2-3 týdny),
- revize, úprava a vytvoření dokumentace, například risk management plánu (2-3 týdny).

U menších projektů s nižším množstvím hrozeb, rizik a zranitelností bude zapotřebí časová investice zhruba 8 týdnů, u komplexnějších větších projektů dokonce až 12 týdnů.



Obrázek 13 Ganttův diagram rozšíření MAN.5 u větších projektů

(zdroj: vlastní)

8.1.4 SUP.1, SUP.9 a SUP.10

Přestože se tyto oblasti nezabývají přímo vývojem bezpečnosti funkcí, bude ale i tak nutná implementace nových prvků do stávajících procesů. Tyto oblasti budou muset nově pokrýt podporu kybernetické bezpečnosti v celém životním cyklu produktu. V rámci SUP.1 se bude

jednat o doplnění požadavků pro správnou kontrolu kvality produktu z úhlu kybernetické bezpečnosti a umožnění provádění auditů kyberbezpečnostních opatření. Kritéria ovlivňující zásah do SUP.1 jsou:

- stav momentálního procesu kvality,
- existence postupu pro ověřování aktivit spojených s kyberbezpečností (například kontrola TARA),
- rychlost úpravy dokumentů.

Při rozšíření nemá tato oblast tak vysoké nároky, jedná se o řád 1-2 týdnů a nezávisí na velikosti či složitosti projektu.

SUP.9 požaduje přiřazení procesu s možností identifikace, kategorizace a řešení incidentů a zranitelností v rámci kybernetické bezpečnosti. Incidenty i zranitelnosti požadují zařazení do konkrétní kategorie problémů a k nim odpovídající prioritě. Kritéria ovlivňující implementaci rozšíření jsou:

- stav současné identifikace, kategorizace a řešení obecných incidentů,
- možnosti kategorizace problémů,
- stav současných pracovních postupů pro řízení incidentů,
- náročnost propojení mezi incidentem a k němu odpovídajícím opatřením.

Časová investice je znovu v rozmezí 1-2 týdnů, jelikož definice nových kategorií incidentů či úprava procesu není zdaleka tak komplikovaná, jako zásah do systémové či softwarové architektury.

SUP.10 bude požadovat doplnění řízení změn o bezpečnostní analýzu dopadu každé navržené změny. Bude žádoucí u jakékoliv změny provést analýzu a posoudit, zda se změna týká právě kybernetické bezpečnosti. Pokud je změna relevantní této problematice, bude se muset opakovat ovlivněná část TARA a popřípadě i iniciace aktualizace požadavků. Pracovní postupy se musí rozšířit o schvalování kyberbezpečnostních změn i propojení těchto změn s hrozbou a implementovanými bezpečnostními opatřeními. Tato celková úprava oblasti SUP.10 se bude pohybovat v časovém rozmezí 1-2 týdnů a projektová velikost či komplexnost zde nehrají znatelnou roli.

Oblasti SUP.1, SUP.9 a SUP.10 je možné řešit paralelně. Výzkumem také vyšlo najevo, že zavedení procesu pro rozpoznání a reakce na kybernetické incidenty během provozu spolu

s dodržáním periodické aktualizace systému spadá do oblastí SUP.1 a SUP.10, ale také částí do oblasti MAN.5. Opět se potvrzuje provázanost mezi všemi oblastmi procesu a skutečnost, že změna jedné oblasti má vliv na stav jiné oblasti.

8.2 Dopady na nástroje a testovací strategii

Implementace normy ISO 21434 do ASPICE 3.1 v oblasti nových nástrojů, technologické infrastruktury, bezpečnostního testování, testovací strategie i tvoření bezpečnostních konceptů se dotýká konkrétně oblastí SWE.4 až SWE.6, SYS.4, SYS.5, MAN.3 a SUP.1.

Nutné bude zařazení nových specializovaných nástrojů pro analýzu aktiv, hrozeb a zranitelností, správu bezpečnostních požadavků, bezpečnostní testování či řízení bezpečnostních incidentů. Výběr vhodných softwarových nástrojů bude záležet na:

- množství uživatelů,
- velikosti firmy,
- typu licence.

V rámci pravidelných ročních investic se nástroje pro analýzu aktiv, hrozeb a zranitelností pohybují přibližně kolem 300 000 – 1 200 000 Kč, nástroje pro správu bezpečnostních požadavků v rozmezí 250 000 – 2 000 000 Kč, nástroje pro bezpečnostní testování zhruba 200 000 – 900 000 Kč a nástroje pro řízení bezpečnostních incidentů okolo 150 000 – 600 000 Kč. Celková investice za nástroje se tedy pohybuje mezi 1–4 miliony Kč. Důležitá je zde připomínka, že je nutné mít kompatibilní hardwarové vybavení, což může přinést další finanční náklady.

Aby byl proces ASPICE 3.1 v souladu s ISO 21434, musí být upravena i testovací strategie. Stávající funkční testy musí být doplněny o bezpečnostní testy (simulační testy, penetrační testy apod.) pro ověření odolnosti produktu vůči kyberbezpečnostním útokům. V testovací strategii budou muset být definovány nově zařazené nástroje, upravené testovací specifikace (jak se pozná, že testování bylo úspěšné), metodika plánování a provádění testů v každé fázi životního cyklu produktu a zajištění schopnosti rychlé reakce při zjištění zranitelnosti testováním. V praxi se často testovací strategii říká laicky „kuchařka“. V raných fázích projektu bude muset být vytvořen i bezpečnostní koncept, který také spadá do oblasti bezpečnostního testování. Výsledky bezpečnostních testů musí být uchovány, spravovány a zálohovány, jelikož budou sloužit jako podklad pro proces správy kvality a konfigurace.

8.3 Dopady na lidské zdroje a kompetence

Implementace ISO 21434 do ASPICE 3.1 přinese značné nároky nejen na znalosti a školení současných zaměstnanců, ale také na nábor nových odborníků se specializací v oblasti kybernetické bezpečnosti a analýz rizik.

Množství nových kvalifikovaných zaměstnanců bude záležet na velikosti organizace, současné úrovni kompetence v oblasti kybernetické bezpečnosti a množství projektů v organizaci. Přesné množství a obsazení rolí bude záležet na organizaci, její preferenci a hlavně rozpočtu.

Organizace bude povinna přesně definovat odpovědnosti vůči každé roli v oblasti kybernetické bezpečnosti. Všechny aktivity týkající se kybernetické bezpečnosti v organizaci, včetně definovaných rolí a zodpovědností musí být zaznamenány v kyberbezpečnostním plánu. Tento plán je odpovědností manažera a architekta kybernetické bezpečnosti v projektu či organizaci. Všechny nové role musí být integrovány do stávající organizační struktury společnosti.

Tabulka 4 ilustruje minimální počet zaměstnanců se specializací v kybernetické bezpečnosti, které bude muset organizace nabrat pro soulad s ISO 21434.

Tabulka 4 Odhad minimálního počtu nových zaměstnanců

Velikost firmy	Odhad minimálního počtu nových zaměstnanců pro splnění implementace ISO 21434 v rámci ASPICE 3.1
Malá (do 50 zaměstnanců)	1 až 2
Střední (od 50 do 200 zaměstnanců)	3 až 5
Velká (více než 200 zaměstnanců)	5 až 12+

(zdroj: vlastní)

Tito odborníci poté budou moci poskytnout každému zaměstnanci výklad ISO 21434 pro pochopení konceptu a základů problematiky kybernetické bezpečnosti v automobilovém

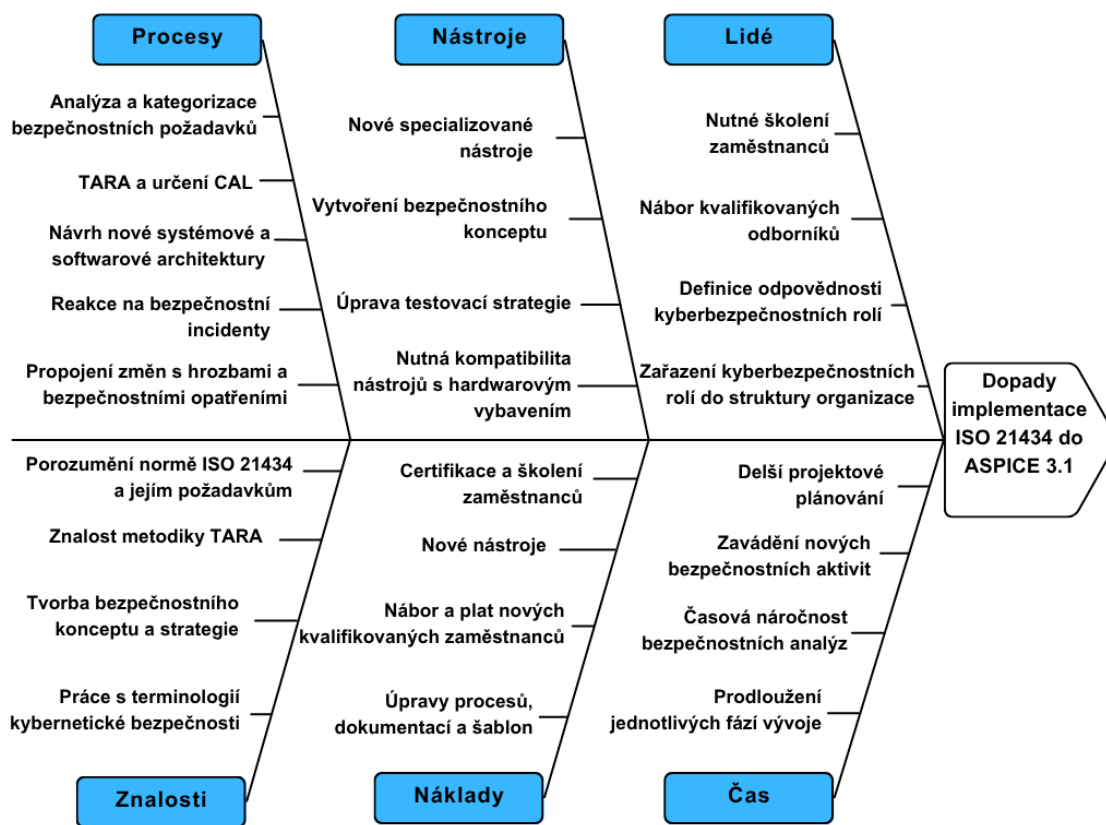
průmyslu. U určitých zaměstnanců je doporučeno podstoupení procesu certifikace u ověřené certifikované společnosti, v závislosti na rolích.

Pro manažery, vývojáře, testery a inženýry kvality bude stačit základní certifikace (například Automotive Cybersecurity Level 1 od TÜV SÜD, který trvá 2 dny a dává účastníkovi přehled terminologie ISO 21434 a znalost právních a regulačních požadavků v automobilové kybernetické bezpečnosti.) Pracovníci kybernetické bezpečnosti, interní auditoři, bezpečnostní manažeři a ostatní role zabývající se kybernetickou bezpečností více do hloubky mají za povinnost účastnit se také zmíněného školení, ovšem budou muset podstoupit i nástavbové školení. Příkladem se může uvést Automotive Cybersecurity Level 2 od zmíněné certifikační autority TÜV SÜD, trvající 2 dny. Toto školení se zabývá pokročilou znalostí kybernetické bezpečnosti dle ISO 21434.

Název školení není překládán, jelikož se přesný překlad nepoužívá a organizace většinou trvají na průběhu certifikace v anglickém jazyce. Pro představu, školení Level 1 se finančně pohybuje okolo 50 000 Kč na osobu a Level 2 okolo 42 000 Kč na osobu. Cena se může měnit v závislosti na regionu a brzké registraci. Součástí ceny školení je i poskytnutí samotné certifikace v případě splnění závěrečné zkoušky.

8.4 Přehled příčin a následků – Ishikawa diagram

Z důvodu zpřehlednění a utřídění hlavních ovlivněných oblastí, jež budou ovlivněny implementací ISO 21434, je ve výzkumu využit diagram příčin a následků, také zvaný jako Ishikawa diagram. Cílem tohoto diagramu je ilustrování vazeb mezi hlavními příčinami (procesy, nástroje, lidé, znalosti, náklady, čas) a příčin z nich vyplývajících.



Obrázek 14 Ishikawa diagram příčin a následků implementace požadavků ISO 21434 do ASPICE 3.1

(zdroj: vlastní)

8.5 Shrnutí osmé kapitoly

Osmá kapitola se soustředila na předposlední část výzkumu, a to na dopady implementace normy ISO 21434 do konkrétních částí procesu ASPICE 3.1. Pro zlepšení přehlednosti poměrně odborné tematiky byly využity tři Ganttovy diagramy v části zkoumající dopady na proces, tabulka při tématice dopadu na lidské zdroje a kompetence a v neposlední řadě Ishikawa diagram pro shrnutí všech hlavních dopadů.

Konkrétně byla provedena analýza sledovatelnosti k mapování požadavků ISO 21434 na konkrétní oblasti procesu dle ASPICE.

Výzkum potvrdil, že nelze požadavky ISO 21434 pouze volně doplnit do procesu ASPICE 3.1. Upravena musí být řada procesních oblastí pro zajištění souladu s normou, pozměněna a rozšířena organizační struktura i upraven celkový přístup testování v celém životním cyklu produktu. Tuto problematiku bude řešit následující část výzkumu ohledně návrhů opatření pro zmírnění dopadu implementace normy.

Tabulka 5 Odhad zdrojů a nákladů na implementaci ISO 21434

Typ projektu	Člověkotýdny	Investice bez školení a náboru	Školení (odhad)	Celková investice se školením a nábořem
Menší	22,5	1 000 000 Kč	100 000 - 150 000 Kč	~1,6–2 mil. Kč
Střední	30	2 500 000 Kč	150 000 - 300 000 Kč	~3,5–4,5 mil. Kč
Větší	39	4 000 000 Kč	250 000 - 600 000 Kč	~5,5–7 mil. Kč

(zdroj: vlastní)

Odhad nákladů na školení vychází z předpokladu účasti různých typových rolí na školeních certifikační autority TÜV SÜD. Pro menší projekty byl kalkulován s účastí 2–3 osob, pro střední projekty 3–5 osob a pro větší projekty 5–10 osob.

Tabulka 6 Přepočet člověkotýdnů na reálný kalendářní čas podle počtu pracovníků

Typ projektu	Člověkotýdny	Počet pracovních hodin	1 osoba	2 osoby	3 osoby
Menší	22,5	900 h	22,5 týdnů → 5,2 měsíce	11,25 týdnů → 5,2 měsíce	7,5 týdnů → 5,2 měsíce
Střední	30	1 200 h	30 týdnů → 7,0 měsíce	15 týdnů → 3,5 měsíce	10 týdnů → 2,3 měsíce
Větší	39	1 560 h	39 týdnů → 9,1 měsíce	19,5 týdnů → 4,5 měsíce	13 týdnů → 3 měsíce

(zdroj: vlastní)

Skutečná časová náročnost implementace bude záviset na počtu zapojených osob, jejich kvalifikaci, zkušenostech a možnostech paralelního zpracování úkolů. Vysoce kvalifikovaný tým může práci zvládnout rychleji, zatímco méně zkušený tým může realizaci výrazně prodloužit. Uvedené hodnoty slouží jako orientační model.

9 NÁVRH OPATŘENÍ PRO ZMÍRNĚNÍ DOPADŮ IMPLEMENTACE NORMY

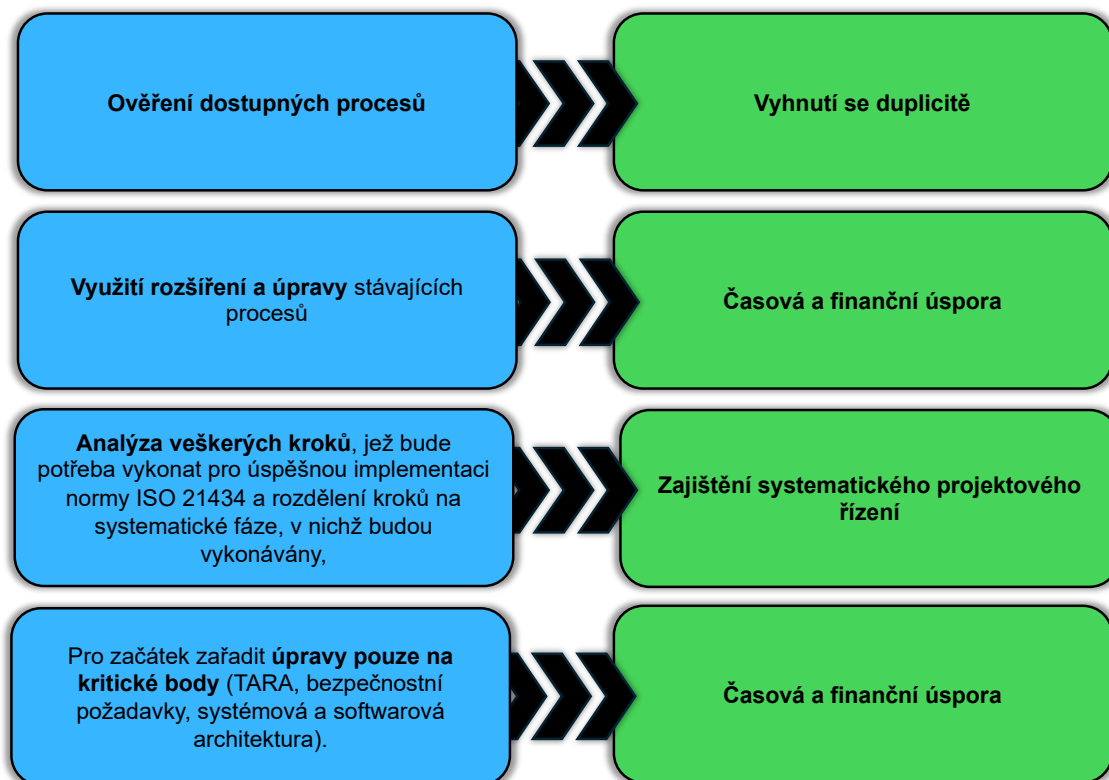
Z výsledků provedené analýzy dopadu implementace požadavků normy ISO 21434 do rámce ASPICE 3.1 jednoznačně vyplývá, že bez zavedení cílených opatření by mohlo dojít k neudržitelnému nárůstu nákladů, prodloužení cyklů v rámci vývoje, snížení efektivity a v extrémním případě dokonce i k bankrotu organizace.

Proto je cílem této kapitoly navržení konkrétních opatření, která umožní tyto dopady do určité míry minimalizovat a zajistit hladký přechod na soulad s normou ISO 21434. Tato část je finální částí výzkumu pro uzavření logického celku řešené problematiky.

9.1 Opatření v oblasti procesů

Implementace normy ISO 21434 do ASPICE 3.1 zasahuje do různých oblastí procesů poměrně intenzivně. Pro zmírnění dopadu kyberbezpečnostních požadavků je nutné dodržení systematického postupu při úpravě stávajících procesů vývoje.

Doporučení:



Obrázek 15 Doporučení opatření v oblasti procesů

(zdroj: vlastní)

Zařazení vyjmenovaných doporučení umožní minimalizaci potřebných změn a zachování efektivity vývojových projektů.

9.2 Opatření v oblasti lidských zdrojů a kompetencí

Zařízení souladu s ISO 21434 v oblasti lidských zdrojů a kompetencí zaměstnanců přináší pro organizaci poměrně vysoké náklady, jak už finanční, tak také časové. Znalosti problematiky kybernetické bezpečnosti totiž ovlivňují rychlost výkonu samotného projektu, správné dodržení postupů při testování, správné používání nově zařazených nástrojů, bezchybné konání analýzy stávajících procesů apod. Jednoduše řečeno, jedná se o stavební kámen veškeré implementace ISO 21434 do ASPICE 3.1. Důležité je dodržení následujících doporučení pro hladký postup implementace normy:



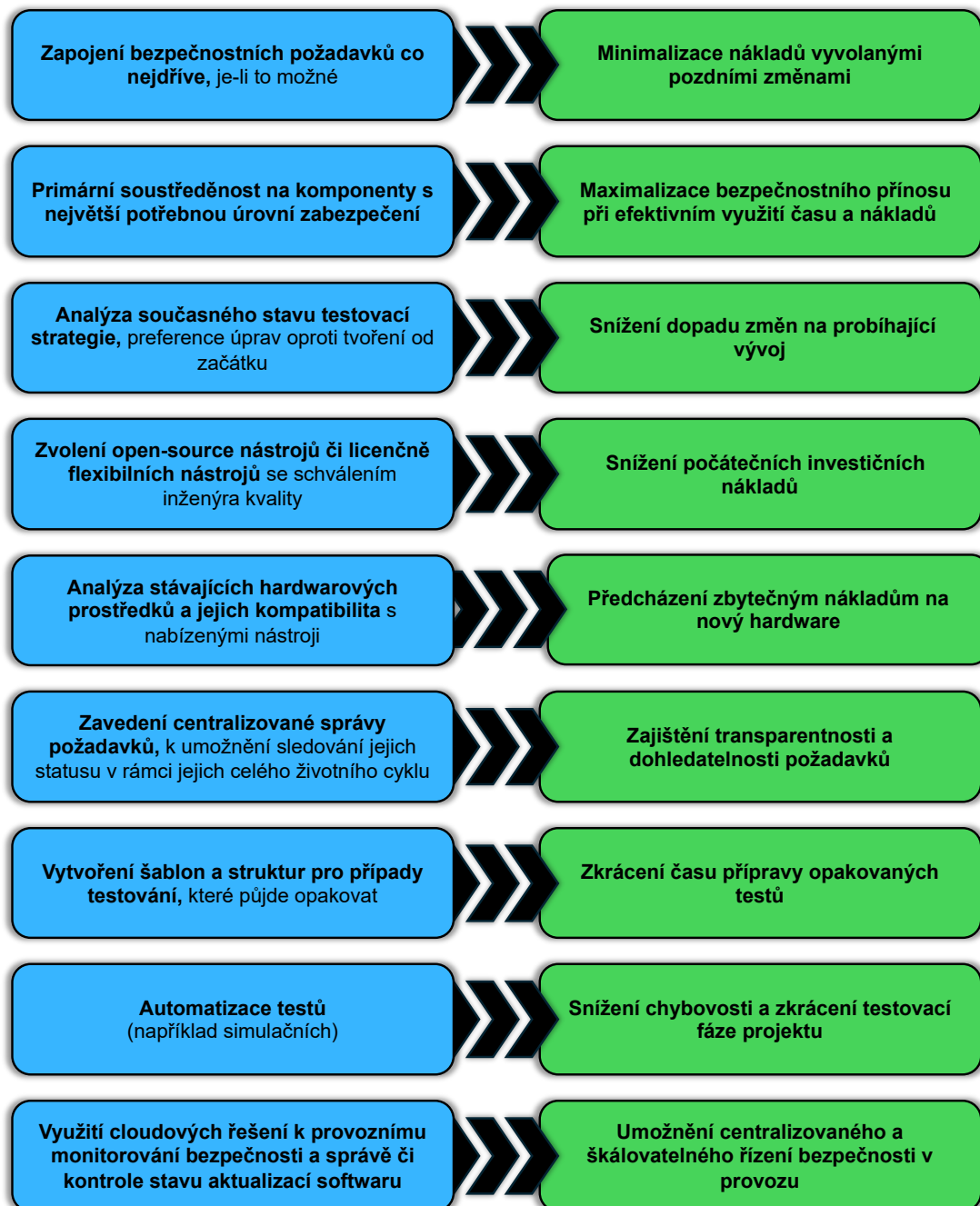
Obrázek 16 Opatření v oblasti lidských zdrojů a kompetencí

(zdroj: vlastní)

Investice do vzdělávání a rozvoje lidských zdrojů je opravdu klíčová a nutná pro udržitelnou implementaci požadavků normy ISO 21434.

9.3 Opatření v oblasti nástrojů, technologické infrastruktury a technického testování

Oblast technického testování, technologické infrastruktury a plánování obecně vyšla ve výzkumu analýzy dopadu implementace ISO 21434 do ASPICE ve verzi 3.1 jako vysoce nákladná položka. Pro limitaci dopadů normy a snížení počátečních nákladů přichází v potaz tato doporučení:



Obrázek 17 Opatření nástrojů, technologické infrastruktury a technického testování

(zdroj: vlastní)

Zavedením zmíněných opatření dojde k poklesu počátečních nákladů a zvýšení přehlednost manipulace s bezpečnostními požadavky. Pro organizace je nutné zasahovat do oblasti nástrojů a technologické infrastruktury postupně.

9.4 Opatření v oblasti projektového řízení a plánování

V neposlední řadě je potřeba zmínit také opatření pro zmírnění dopadu implementace normy ISO 21434 do ASPICE 3.1 z hlediska projektového plánování a řízení.

Doporučení:



Obrázek 18 Opatření v oblasti projektového řízení a plánování

(zdroj: vlastní)

Při dodržení proaktivních doporučení v rámci projektu bude umožněno včasné odhalení rizik a minimalizace zpoždění.

9.5 Shrnutí deváté kapitoly

Devátá kapitola pojednávala o představení souboru proaktivních opatření při implementaci normy ISO 21434 do ASPICE ve verzi 3.1. Tato opatření slouží k pomoci organizacím implementovat normu správně, ale postupně.

Hlavním důležitým zjištěným opatřením je postupná integrace bezpečnostních aktivit do aktivit současných, soustředěnost na školení a kompetence zaměstnanců, vhodná a postupná volba nástrojů a včlenění soustředěnosti na kybernetickou bezpečnost do projektového plánování a řízení.

Přijetím vyjmenovaných opatření lze dosáhnout minimalizace negativních dopadů implementace a zároveň posílení celkové odolnosti organizace vůči kybernetickým hrozbám.

ZÁVĚR

Tato bakalářská práce se zabývala analýzou dopadu implementace normy ISO 21434 do procesu ASPICE. Cílem bylo provést výzkum k identifikaci překryvů mezi oběma normami, stanovení požadavků nutných k implementaci a následnému posouzení dopadů těchto změn na vývojový proces.

Práce byla rozložena na část teoretickou, skládající se ze čtyř kapitol a část praktickou o pěti kapitolách. Části i kapitoly práce na sebe navazují a vytváří logický celek.

V první kapitole byl představen kontext kybernetické bezpečnosti v automobilovém průmyslu, který se vyvíjí v reakci na rostoucí digitální propojenost vozidel, tlak na automobilové výrobce a nově vznikající rizika spojená s moderními technologiemi a automatizací.

Druhá kapitola se zabývala představením základní terminologie a přiblížením komponent, které jsou z hlediska bezpečnosti aktuální. Také byly definovány klíčové pojmy a metodiky vycházející z norem ASPICE a ISO 21434.

Třetí kapitola byla věnována samotnému rozboru ASPICE ve verzi 3.1, jeho historii, účelu, struktuře, dílčím procesům a dostupným certifikovaným rozšířením.

Ve čtvrté kapitole byl obdobným způsobem analyzován obsah normy ISO 21434. Pozornost byla věnována také její historii, struktuře a účelu, ale také životnímu cyklu produktu a jeho fázím, spolu s definicí rolí a odpovědností v systému řízení kybernetické bezpečnosti.

V praktické části práce byla nejprve provedena komparativní analýza pokrytí požadavků na kybernetickou bezpečnost mezi normou ASPICE 3.1 a ISO 21434. Výzkum ukázal, že ačkoli ASPICE poskytuje solidní rámec pro řízení vývoje systémů a softwaru, jeho schopnost pokrýt specifické požadavky kybernetické bezpečnosti je pouze částečná. Byly identifikovány oblasti překryvu (zejména v řízení požadavků, dokumentaci a ověřování), ale také osm klíčových oblastí, v nichž ASPICE nedosahuje potřebné úrovně pokrytí, a které bude nutné pro zajištění souladu rozšířit nebo upravit.

Na tuto analýzu navázala sedmá kapitola, která se věnovala dopadům implementace těchto chybějících požadavků do praxe. Analýza dopadu se zaměřila na rozsah nových činností, nutné organizační změny, nové nástroje a technickou infrastrukturu, ale i dopady na časové plánování, náklady a výkonnost projektových týmů. Zjištěno bylo, že správná

implementace ISO 21434 vyžaduje vytvoření specifických procesů, úpravu softwarové a systémové architektury, doplnění testovací strategie o bezpečnostní testování a zavedení reakčních mechanismů na kybernetické incidenty. Organizace bude muset nově zajistit odpovídající kvalifikaci zaměstnanců a rozšířit stávající týmy o odborníky na kybernetickou bezpečnost. V závislosti na velikosti firmy se jedná o 1 až 12 nových pracovníků.

Z hlediska časové a finanční náročnosti byl výzkumem zjištěn rozsah zátěže mezi 22,5 a 39 člověkotýdny, což odpovídá 5,2 až 9,1 měsícům čistého času práce jednoho pracovníka. Celkové náklady na implementaci včetně školení a náboru se pohybují v rozmezí 1,6 až 7 milionů korun, dle velikosti projektu. Významnou složku těchto nákladů tvoří školení, přičemž cena za účast jednoho pracovníka na certifikovaných kurzech ISO 21434 od TÜV SÜD může dosáhnout až 92 000 Kč.

Devátá kapitola se zaměřila na návrh opatření, která by umožnila zmírnit negativní dopady implementace zjištěné v předchozí fázi. Bylo navrženo celkem dvacet tři konkrétních opatření ve čtyřech oblastech – procesů, lidských zdrojů a kompetencí, nástrojů, technické infrastruktury a bezpečnostního testování a projektového řízení a plánování. Výzkum prokázal, že bez cíleného přístupu může být implementace ISO 21434 pro organizaci extrémně náročná až neudržitelná. Nejdůležitější doporučení jsou systematické vzdělávání zaměstnanců, definice nových bezpečnostních rolí, vytvoření bezpečnostního plánu a integrace bezpečnostních činností do projektového harmonogramu již od rané fáze vývoje. Tato opatření tvoří základ pro efektivní, dlouhodobě udržitelnou implementaci normy bez zásadního narušení běžného chodu organizace.

Výsledkem práce je přehledný návrh implementace identifikovaných požadavků normy ISO 21434 do ASPICE procesu. Ten může sloužit jako podklad pro vývojové týmy či samotné organizace zabývající se řízením kybernetické bezpečnosti v automobilovém průmyslu.

SEZNAM POUŽITÉ LITERATURY

- [1] ČSN ISO 21434. *Silniční vozidla – Kybernetické zabezpečení při vývoji*. Ženeva: Mezinárodní organizace pro normalizaci, 2021.
- [2] ČSN ISO 26262. *Silniční vozidla – Funkční bezpečnost*. 2. vydání. Ženeva: Mezinárodní organizace pro normalizaci, 2018.
- [3] NASSER, Ahmad MK. *Automotive Cybersecurity Engineering Handbook*. 1. vyd. Birmingham: Packt Publishing, 2023. ISBN 978-1-80107-653-1.
- [4] SCHMEKEN, Holger. *Kybernetická bezpečnost v automobilovém průmyslu: nové povinné předpisy*. Online. DQS Global, 2024. Dostupné z: <https://www.dqsglobal.com/cs-cz/vzdelavani/blog/kyberneticka-bezpecnost-v-automobilovem-prumyslu-nove-povinne-predpisy>. [cit. 2025-12-09].
- [5] GREENBERG, Andy. *Hackers Remotely Kill a Jeep on the Highway—With Me in It*. Online, Wired, 2015. Dostupné z: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>. [cit. 2024-12-09].
- [6] WIRED. Jeep hack – redakční fotografie [online]. In: GREENBERG, Andy. *After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix*. WIRED, 24. července 2015 [cit. 2024-12-09]. Dostupné z: <https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix>
- [7] LI, Beibei, HU, Wei, DA, Lemei, WU, Yibing, WANG, Xinxin, LI, Yiwei, YUAN, Chaoxuan. *Over-the-air upgrading for enhancing security of intelligent connected vehicles: a survey*. Online, *Artificial Intelligence Review*. 2024. Dostupné z: <https://link.springer.com/article/10.1007/s10462-024-10968-z>. [cit. 2024-12-09].
- [8] UNECE. *Předpis č. 155 – Kybernetická bezpečnost a systém řízení kybernetické bezpečnosti*. Ženeva: Evropská hospodářská komise OSN, 2021
- [9] VDA. *Automotive SPICE® for Cybersecurity: Part I: Process Reference and Assessment Model for Cybersecurity Engineering. Part II: Rating Guidelines on Process Performance (Level 1) for Cybersecurity Engineering*. 1. vyd. Frankfurt nad Mohanem: VDA QMC, 2021. ISBN 978-3-86490-360-1.
- [10] TÜV SÜD. *Revoluce v oblasti kybernetické bezpečnosti: Nové požadavky a výzvy pro automobilový průmysl*. TÜV SÜD, 2024. Dostupné z:

- [cz/tisk-a-media/2024/rijen/revoluce-v-oblasti-kyberneticke-bezpecnosti](https://tisk-a-media/2024/rijen/revoluce-v-oblasti-kyberneticke-bezpecnosti) [cit. 2025-12-13].
- [11] WOJNAR, Bohdan. Kybernetická bezpečnost v automobilovém průmyslu – vždy online. Online. DSM, 2020. Dostupné z: <https://dsm.tate.cz/cs/2020/dsm-4-2020/zdarma-4-2020/uvodnik-kyberneticka-bezpecnost-v-automobilovem-prumyslu-vzdy-online>. [cit. 2024-12-13].
- [12] AUTOMOTIVE SPICE. *Process Assessment / Reference Model*. Version 3.1. Kolín nad Rýnem: VDA QMC and Automotive SIG, 2017.
- [13] ISO 24089:2023. *Silniční vozidla – Inženýrství aktualizací softwaru*. Ženeva: Mezinárodní organizace pro normalizaci, 2023.
- [14] UNECE. *Předpis č. 156 – Aktualizace softwaru a systém řízení aktualizací softwaru*. Ženeva: Evropská hospodářská komise OSN, 2021.
- [15] KYBEZ. *Analýza bezpečnosti #2: Co jsou aktiva a jak je evidovat?* Online. Dostupné z: <https://kybez.cz/analyza-bezpecnosti-2-co-jsou-aktiva-a-jak-je-evidovat/>. [cit. 2025-01-05].
- [16] SANDS s.r.o. *Vysvětlení zranitelností, hrozeb a rizik*. Online. Dostupné z: <https://www.sands.cz/vysvetleni-zranitelnosti-hrozeb-a-rizik/>. [cit. 2025-01-05].
- [17] STUDYSMARTER. *Security Measures: Definition & Techniques*. Online Dostupné z: <https://www.studysmarter.co.uk/explanations/hospitality-and-tourism/safety-and-security-in-tourism/security-measures/> [cit. 2025-01-05].
- [18] IBM. *What is Risk Mitigation?* Online. 2024. Dostupné z: <https://www.ibm.com/think/topics/risk-mitigation> [cit. 2025-01-05].
- [19] MASTERCLASS. *Impact Analysis*. Online. Dostupné z: <https://www.masterclass.com/articles/impact-analysis>. [cit. 2025-01-05].
- [20] NĚMEC, Marek. *Metodika hodnocení procesní vyspělosti v automobilovém průmyslu*. Online, Diplomová práce. Praha: České vysoké učení technické v Praze, 2008. Dostupné z: https://stc.fs.cvut.cz/history/2008/sbornik/Papers/DP/Nemec_Marek_12138.pdf. [cit. 2025-01-05].

- [21] VOLNÝ, Petr. *Úvod do embedded systémů*. Online. DPS Elektronika od A do Z, 2022. Dostupné z: <https://www.dps-az.cz/clanky/id:6173/uvod-do-embedded-systemu> [cit. 2025-01-08].
- [22] DELL Technologies. *Použití dostupných nástrojů ke kontrole aktuální verze firmwaru hardwarových zařízení*. Online. Dostupné z: <https://www.dell.com/support/kbdoc/cscz/000134797/pou%C5%BEit%C3%AD-dostupn%C3%BDch-n%C3%A1stroj%C5%AF-ke-kontrol%C3%A1ln%C3%AD-verze-firmwaru-hardwarov%C3%BDch-za%C5%99%C3%ADzen%C3%AD> [cit. 2025-01-08].
- [23] ALLEN, James. *What is an ECU in a car?* Online. 2022. Dostupné z: <https://www.carwow.co.uk/guides/glossary/what-is-an-ecu-in-a-car#gref>. [cit. 2025-01-08].
- [24] INTREPID CONTROL SYSTEMS, Inc. *CAN / CAN FD*. Online. Intrepid Control Systems. Dostupné z: <https://intrepidcs.com/applications/can-can-fd/>. [cit. 2025-01-10].
- [25] PANASONIC. *TCU (Telematics Control Unit) – Technical Explanation*. Online. Dostupné z: <https://industrial.panasonic.com/ww/ds/ss/technical/b19> [cit. 2025-01-10].
- [26] MIXON, Erica a STEELE, Colin. *OTA update (over-the-air update)* Online .TechTarget. Dostupné z: <https://www.techtarget.com/searchmobilecomputing/definition/OTA-update-over-the-air-update> [cit. 2025-01-10].
- [27] Synopsys. *ISO/SAE 21434 for Automotive Cybersecurity*. Online. Synopsys. Dostupné z: <https://www.synopsys.com/designware-ip/technical-bulletin/iso-sae-21434-automotive-cybersecurity.html>. [cit. 2025-01-15].
- [28] IBM. *What is Vulnerability Management?* Online. IBM, 2022. Dostupné z: <https://www.ibm.com/think/topics/vulnerability-management>. [cit. 2025-01-15].
- [29] CISA. *Incident Response Plan Basics*. Online. Cybersecurity and Infrastructure Security Agency. Dostupné z: https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf [cit. 2025-01-16].
- [30] MathWorks. *Automotive SPICE (A-SPICE)*. Online. Dostupné z: <https://in.mathworks.com/discovery/automotive-spice.html> [cit. 2025-01-17].

- [31] SODIUSWILLERT. *Traceability Standards & Regulations in the Automotive Industry*. Online. Dostupné z: <https://www.sodiuswillert.com/en/blog/traceability-standards-regulations-in-the-automotive-industry> [cit. 2025-01-17].
- [32] CONFLUENT. *ASPICE (Automotive SPICE)*. Online. Confluent. Dostupné z: <https://www.confluent.io/learn/aspice/> [cit. 2025-01-17].
- [33] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti*. Online. Brno: NÚKIB, 2022. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Prvodce%20zenm%20aktiv%20a%20rizik%20dle%20vyhlky%20o%20kybernetick%20bezpenosti.pdf [cit. 2025-02-15].
- [34] OBERTI, Franco; SANCHEZ, Ernesto; SAVINO, Alessandro; PARISI, Filippo a DI CARLO, Stefano. *CAL determination based on impact and attack vector parameters table extracted by ISO/SAE-21434*. Online. In: *PSP Framework: A novel risk assessment method in compliance with ISO/SAE-21434*. ResearchGate, květen 2023. Dostupné z: https://www.researchgate.net/figure/CAL-determination-based-on-impact-and-attack-vector-parameters-table-extracted-by_fig3_370633490 [cit. 2025-02-15].
- [35] FORTINET. *Attack Vector*. Online. Dostupné z: <https://www.fortinet.com/resources/cyberglossary/attack-vector> [cit. 2025-02-15].
- [36] TECHTARGET. *Security by design*. Online. Dostupné z: <https://www.techtarget.com/whatis/definition/security-by-design> [cit. 2025-02-15].
- [37] TAYLLORCOX. *Zbytkové riziko* [online]. Dostupné z: <https://www.tx.cz/slovník/business-continuity/zbytkove-riziko> [cit. 2025-05-20].
- [38] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*. Online. 21. května 2018. Dostupné z: <https://www.zakonyprolidi.cz/cs/2018-82> [cit. 2025-02-20].
- [39] ARNOWSKI, M. *Automotive SPICE*. Online. 19. října 2015. Dostupné z: <https://www.plays-in-business.com/automotivespice/> [cit. 2025-02-20].

- [40] Visure Solutions. *ASPICE 101: What is Automotive SPICE (ASPICE)?* Online. Dostupné z: <https://visuresolutions.com/blog/automotive/aspice/>. [cit. 2025-02-20].
- [41] GEEKSFORGEES. *Software Engineering | SDLC V-Mode*. Online. 9. dubna 2025. Dostupné z: <https://www.geeksforgeeks.org/software-engineering-sdlc-v-model/> [cit. 2025-03-15].
- [42] ZAMBROWSKI, Michał. *ASPICE 4.0: Challenges and Opportunities*. Online. Spyrosoft, 2024. Dostupné z: <https://spyro-soft.com/blog/automotive/aspice-4-0-challenges-and-opportunities> [cit. 2025-03-15].
- [43] SKRČENÝ, Vlastimil; MICHALIČKA, Tomáš. *Automotive SPICE*. Online. Praha: Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky, 2015. Semestrální práce ke kurzu 4IT421 Zlepšování procesů budování IS. Dostupné z: https://spicenter.vse.cz/wp-content/uploads/2018/08/semestralni_prace/15_02/AutomotiveSPICE_Skrdeny_Michalicka.pdf [cit. 2025-03-15].
- [44] INTACS. *Automotive SPICE for Hardware Engineering: Process Assessment Model – Version 1.0*. Online. November 2019. Dostupné z: https://www.intacs.info/images/uploads/intacs_HW_Engineering_PRM_PAM_v1.0.pdf [cit. 2025-03-15].
- [45] VDA QMC. *Automotive SPICE® for Cybersecurity. Process Assessment Model (PAM) – Version 1.0*. Berlin: Verband der Automobilindustrie, 2021. 117 s. ISBN 978-3-86506-664-6.
- [46] KEYSIGHT Technologies. *ISO 21434: Safeguarding the Future of Automotive Security* Online. 10. června 2024. Dostupné z: <https://www.keysight.com/blogs/en/tech/nwvs/2024/06/10/iso-21434-safeguarding-the-future-of-automotive-security> [cit. 2025-03-28].
- [47] ISO/IEC. *ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements*. Ženeva: International Organization for Standardization, 2013.

SEZNAM OBRÁZKŮ

Obrázek 1 Ukázka útoku Jeep Cherokee z roku 2015	17
Obrázek 2 Graf předpovězeného růstu počtu připojených vozidel po celém světě mezi lety 2021-2027	19
Obrázek 3 Příklad útoku na cílenou ECU	29
Obrázek 4 V-Model.....	39
Obrázek 5 Struktura ASPICE ve verzi 3.1	40
Obrázek 6 Struktura ISO 21434.....	47
Obrázek 7 Životní cyklus produktu dle ISO 21434	48
Obrázek 8 Vennův diagram překrytí a nedostatků ASPICE 3.1 vůči požadavkům ISO 21434.....	57
Obrázek 9 Výsledek analýzy dopadu implementace normy ISO 21434.....	64
Obrázek 10 Propojení výsledků analýzy dopadu s výsledky komparativní analýzy	65
Obrázek 11 Ganttův diagram rozšíření SYS.2 a SYS.3 u většího projektu.....	68
Obrázek 12 Ganttův diagram rozšíření SWE.1 až SWE.6 v případě složitějšího softwaru.....	70
Obrázek 13 Ganttův diagram rozšíření MAN.5 u větších projektů	71
Obrázek 14 Ishikawa diagram příčin a následků implementace požadavků ISO 21434 do ASPICE 3.1	76
Obrázek 15 Doporučení opatření v oblasti procesů	78
Obrázek 16 Opatření v oblasti lidských zdrojů a kompetencí	79
Obrázek 17 Opatření nástrojů, technologické infrastruktury a technického testování	80
Obrázek 18 Opatření v oblasti projektového řízení a plánování.....	81

SEZNAM TABULEK

Tabulka 1 Časová osa klíčových milníků.....	21
Tabulka 2 Přehled úrovní schopností v rámcovém procesu SPIICE	33
Tabulka 3 Určení CAL podle dopadu a vektoru útoku.....	35
Tabulka 4 Odhad minimálního počtu nových zaměstnanců.....	74
Tabulka 5 Odhad zdrojů a nákladů na implementaci ISO 21434	77
Tabulka 6 Přepočet člověkotýdnů na reálný kalendářní čas podle počtu pracovníků.....	77

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACQ	Acquisition Process Group
AD/DA	Analogově – digitální/ Digitálně – analogový
Apod	A podobně
ASPICE	Automotive SPICE
ATD	A tak dále
CAL	Cybersecurity Assurance Level
CAN	Controller Area Network
CAN FD	Controller Area Network – Flexible Data-rate
CSMS	Cybersecurity Management Systém
ECU	Eletronic Control Unit
EPROM	Erasable Programmable Read-Only Memory
ESP	Eletronic Stability Program
HW-SPICE	ASPICE for Hardware Engineering
IEC	International Electrotechnical Commission
ID	Identifier
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
MAN	Management Process Group
MCU	Microcontroller Unit
Např	Například
OBD	On-Board Diagnostics
OEM	Original Equipment Manufacturer
OTA	Over-The-Air

PIM	Process Improvement Process Group
Q	Quartal
REU	Reuse Process Group
ROM	Read-Only Memory
SAE	Society of Automotive Engineers
SC	Subcommitee
SEC	Security Engineering Process Group
SPICE	Software Process Improvement and Capability dEtermination
SPL	Supply Process Group
STR	Strana
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
SUMS	Software Update Management System
SUP	Supporting Process Group
SYS	System Engineering Process Group
SWE	Software Engineering Process Group
TARA	Threat Analysis and Risk Assessment
TC	Technical Committee
TCU	Telematic Control Unit
TZV	Tak zvaný
UNECE	United Nations Economic Commission for Europe
USB	Universal Serial Bus
VDA	Verband der Automobilindustrie
Wi-Fi	Wireless Fidelity
WG	Working Group