AKADEMIA GÓRNICZO-HUTNICZA IM. STANISŁAWA STASZICA W KRAKOWIE

DZIEDZINA NAUK INŻYNIERYJNO-TECHNICZNYCH

DYSCYPLINA AUTOMATYKA, ELEKTRONIKA, ELEKTROTECHNIKA
I TECHNOLOGIE KOSMICZNE

AUTOREFERAT ROZPRAWY DOKTORSKIEJ

Systemowa analiza bezpieczeństwa układów sterowania w pojazdach o wysokim stopniu automatyzacji jazdy

Autor: mgr inż. Piotr Piątek

Promotor rozprawy: dr hab. inż. Paweł Skruch, prof. AGH
Promotor pomocniczy: dr inż. Szczepan Moskwa

Praca wykonana: Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie,
Wydział Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej

Kraków, 2024

Streszczenie

Przemysł motoryzacyjny znajduje się obecnie w fazie rewolucyjnej transformacji. Jej charakter przejawia się wzrostem automatyzacji i intensywną wymianą dużych ilości danych. Zmiany te wymuszają poszukiwanie nowych sposobów projektowania systemów wbudowanych w pojazdach. Niniejsza praca podejmuje wyzwanie zintegrowania obecnie odizolowanych zagadnień technicznych, jakimi są bezpieczeństwo funkcjonalne oraz cyberbezpieczeństwo, proponując holistyczne podejście do rozwiązywania złożonych, interdyscyplinarnych wyzwań projektowych.

Separacja zagadnień bezpieczeństwa funkcjonalnego oraz cyberbezpieczeństwa prowadzi do błędnych decyzji projektowych, zwiększonego ryzyka awarii, obniżonego poziomu bezpieczeństwa oraz możliwości powstawania dodatkowych słabości systemów, które mogą skutkować cyberatakami. Jednym z przykładów takich zagrożeń jest zdalne przejęcie kontroli nad pojazdem, wyciek wrażliwych danych lub kradzieże. Poza wpływem na bezpieczeństwo, ma to również wpływ na aspekty finansowe, operacyjne czy też biznesowe. Jednym z najbardziej znanych przypadków potwierdzających te zagrożenia był skuteczny atak na pojazd marki Jeep w 2014 roku [1].

Zasady, na których opierają się bezpieczeństwo funkcjonalne oraz cyberbezpieczeńswo są głęboko współzależne. Zawiera się to w kluczowych aspektach analiz, jak identyfikacja ryzyka oraz słabości systemu czy wdrażanie działań zaradczych. Dlatego też naturalnym kierunkiem jest podejście mocno zintegrowane. Wspólne podejście umożliwia wykorzystanie jednolitych narzędzi oraz metodologii analiz. Pozwala to na bardziej efektywną identyfikację słabości systemów, co przyczynia się do zwiększenia poziomu bezpieczeństwa systemu, jego jakości, jak również sprzyja zwiększeniu efektywności projektowania, przy jednoczesnej redukcji nakładów pracy oraz przyspieszeniu procesu rozwoju produktu.

Próbując zwiększyć poziom współpracy między pozostającymi w odizolowaniu od siebie zagadnieniami bezpieczeństwa funkcjonalnego oraz cyberbezpieczeństwa w rozprawie podkreślono korzyści płynące z wykorzystania inżynierii systemów opartej na modelach (*a*ng.model-based systems engineering) jako narzędzia wspierającego. Takie podejście zwiększa skalowalność i praktyczność procesu projektowania w rzeczywistych środowiskach przemysłowych.

W pracy zdefiniowano proces *CyberSafety* (CySa) jako nowatorskie podejście projektowe integrujące bezpieczeństwo funkcjonalne i cyberbezpieczeństwo od najwcześniejszych etapów rozwoju produktu. Zdefiniowane rozwiązanie, oparte na dogłębnym przeglądzie literatury, analizie obecnie obowiązujących standardów, trendów rynkowych oraz konsultacjach z ekspertami branżowymi, poprawia działania zespołów projektowych. Proces ten zweryfikowano za pomocą zdefiniowanych wskaźników efektywności (*Key Performance Indicators – KPI*). Szczegółowa analiza studium przypadku systemu wspomagania jazdy autostra-

dowej (*Highway Pilot – HP*) wykazała znaczącą redukcję ryzyka oraz mniejsze nakłady pracy projektowej, co przełożyło się na poprawę jakości i zwiększenie poziomu bezpieczeństwa.

Rozszerzając standardowe analizy zagrożeń, zaproponowano nową metodę oceny ryzyka opartą o Ważony Współczynnik Bezpieczeństwa (Weighted Safety Score (WSS)). Podejście to integruje zagrożenia wynikające z zagadnień bezpieczeństwa funkcjonalnego oraz cyberbezpieczeństwa, uwzględniając współczynniki wagowe dostosowane do specyfiki różnych obszarów funkcjonalnych w architekturze pojazdu.

Wnioski z badań podkreślają potencjał do dalszej integracji obszarów technicznych w branży motoryzacyjnej uwzględniając nowe zagadnienia, jak bezpieczeństwo systemów wykorzystujących sztuczną inteligencję. Kluczowe znaczenie będzie miała kontynuacja współpracy z grupami standaryzacyjnymi, aby sprostać dynamicznie zmieniającym się wymaganiom bezpieczeństwa w pojazdach autonomicznych.

Spis treści

Streszczenie **ii**

Spis skrótów **v**

Autoreferat **1**

Wprowadzenie, hipotezy i cele pracy 1

Struktura Pracy 4

Najważniejsze osiągnięcia 4

Podsumowanie i wnioski 12

Bibliografia **15**

Spis skrótów

ADAS Advanced Driver Assistance System

ASIL Automotive Safety Integrity Level

BPMN Business Process Model and Notation

CySa CyberSafety

CySe Cybersecurity

DCI Design Complexity Index

DCR Design Compliance Rate

DCRR Design Change Request Rate

EE Electrical/Electronic

ERC Effort Reduction Coefficient

FuSa Functional Safety

HaSI Hazard Safety Indicator

HP Highway Pilot

IDS Intrusion Detection System

IEEE Institute of Electrical and Electronics Engineers

KPI Key Performance Indicators

MBSE Model-Based Systems Engineering

MSC Mitigation Strategy Completeness

RRL Residual Risk Level

SOTIF Safety of Intended Functionality

SSRC Security and Safety Requirement Coverage

SysML Systems modeling language

THA Threat and Hazard Analysis Efficiency

ThRS Threat Risk Score

WSS Weighted Safety Score

Autoreferat

Wprowadzenie, hipotezy i cele pracy

W obliczu czwartej rewolucji przemysłowej, charakteryzującej się zwiększoną automatyzacją i intensywną wymianą danych między urządzeniami, rośnie pilna potrzeba ochrony systemów przed zagrożeniami cybernetycznymi. Transformacyjny charakter tej zmiany obejmuje niemal wszystkie sektory gospodarki, a szczególnie wpływa na przemysł motoryzacyjny, który znajduje się w epicentrum tej technologicznej rewolucji.

Sektor motoryzacyjny nie tylko rozwija się w kierunku elektryfikacji pojazdów, lecz także intensywnie inwestuje w technologie autonomicznej jazdy. Inteligentne pojazdy obiecują poprawę bezpieczeństwa, efektywności transportu i komfortu użytkowania. Jednakże te zaawansowane systemy stają się coraz częściej celem cyberataków.

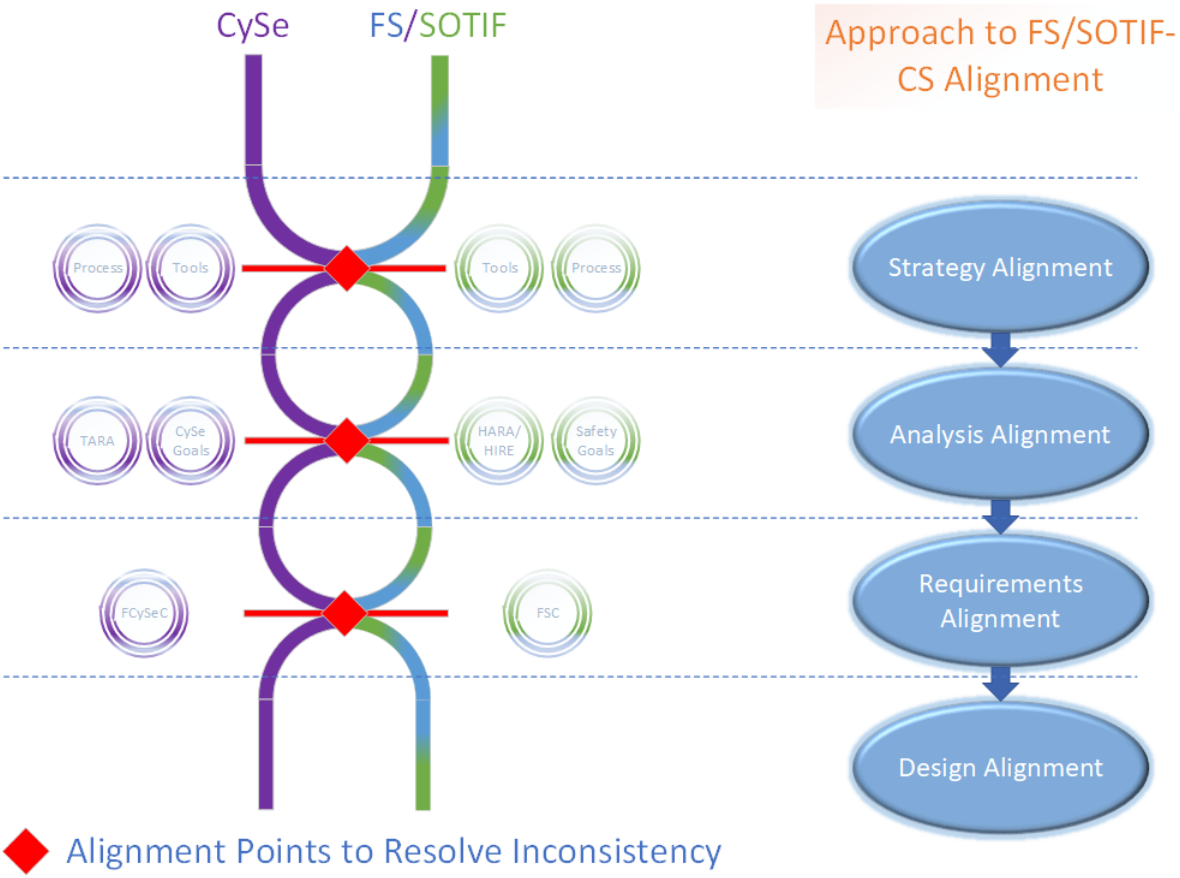
Obecnie obowiązujące normy ISO 26262-1:10:2018 [2] oraz ISO/PAS 21448 (SOTIF) [3] definiują ramy zapewnienia bezpieczeństwa funkcjonalnego i przeciwdziałania zagrożeniom wynikającym z ograniczeń funkcjonalnych systemów. Jednak te standardy nie uwzględniają wszystkich aspektów zagrożeń związanych z autonomią pojazdów. Cyberbezpieczeństwo, zdefiniowane w normie ISO/SAE 21434 [4], staje się kluczowym elementem ochrony przed złośliwymi atakami na systemy sterowania, łączność oraz dane pojazdów. Zintegrowanie wymagań bezpieczeństwa funkcjonalnego *(Functional Safety (FuSa))* i cyberbezpieczeństwa *(Cybersecurity (CySe))* jest nieodzowne, aby sprostać zagrożeniom współczesnych złożonych systemów.

Obecne podejścia traktują bezpieczeństwo funkcjonalne i cyberbezpieczeństwo jako odrębne obszary techniczne, co prowadzi do niespójności, zwiększonego ryzyka oraz nowych zagrożeń, takich jak zdalne przejęcie pojazdów czy wycieki danych [1, 5]. Przykładem tego jest atak cybernetyczny na pojazd marki Jeep, gdzie brak wystarczających zabezpieczeń uwzględnionych w architekturze systemu umożliwił zdalne przejęcie kontroli nad pojazdem [1]. Badania wskazują, że systemy ADAS są szczególnie podatne na ataki kontekstowe, które mogą generować zagrożenia z wysoką skutecznością [5–7].

Zwiększona łączność (ang. connectivity) pojazdów z siecią zewnętrzną znacząco rozszerza możliwości zdalnego przeprowadzania ataków cybernetycznych. Dostępne analizy pokazują, że liczba znanych słabości w systemach pojazdów stale rośnie [8], obejmując m.in. słabości oprogramowania związane z cyberbezpieczeństwiem czujników wykorzystywanych w autonomicznej jeździe [9]. W odpowiedzi producenci, tacy jak np. BMW, zaczęli proaktywnie ujawniać i eliminować słabości w swoich systemach [10].

W środowisku badawczym bezpieczeństwo funkcjonalne (FuSa) cechuje dojrzałość i bogate doświadczenie branżowe, podczas gdy cyberbezpieczeństwo (CySe) w motoryzacji jest stosunkowo młodą dziedziną, której rozwój przyspieszył wraz z publikacją normy ISO/SAE 21434 w 2021 roku.

Rozwój bezpiecznych systemów wymaga nowego podejścia oraz zintegrowanego procesu obejmującego cały cykl życia systemu. Kluczowym elementem jest eliminacja izolacjonistycznego podejścia na rzecz ścisłej współpracy między zespołami inżynierskimi już na wczesnych etapach rozwoju produktu. Współpraca ta, wraz z kluczowymi punktami styku zilustrowanymi na rysunku 1, umożliwia wczesne wykrywanie wyzwań architektonicznych, i ryzyka. Jednocześnie przekłada się to później na redukcję kosztów oraz ograniczenie czasochłonnych modyfikacji w późniejszych fazach projektu.



Rysunek 1: Kluczowe punkty synchronizacji pomiędzy CySe a FuSa.

Zastosowanie metod inżynierii systemów opartych na modelach *(ang. Model-Based Systems Engineering (MBSE))* jako narzędzia wspierającego przyczynia się do poprawy skalowalności i praktyczności procesu projektowania w rzeczywistych środowiskach przemysłowych [11].

Zważywszy na zdefiniowany problem w postaci braku współpracy domeny CySe oraz FuSa, hipotezy rozprawy zostały zdefiniowane w następujący sposób:

- **Wczesna współpraca w zakresie zintegrowanego bezpieczeństwa i ochrony w całym cyklu życia produktu zapewni większą niezawodność i jakość wbudowanych systemów samochodowych o wysokiej autonomii, minimalizując ryzyko i zapewniając wysoką efektywność procesu projektowania.**

- **Nowatorski model rozwoju, który wyposaża firmy w kompleksowe narzędzia i metodologie do efektywnego zarządzania skomplikowanym projektowaniem złożonych systemów wbudowanych o wysokiej autonomii, przy jednoczesnej integracji bezpieczeństwa i ochrony w całym procesie, znacznie poprawi niezawodność systemu, skróci czas opracowywania i zwiększy ogólne bezpieczeństwo i ochronę pojazdu**.

Tym samym, głównym celem niniejszej rozprawy jest:

- **Sformułowanie praktycznego i możliwego do wdrożenia podejścia do projektowania i wdrażania zaawansowanych systemów sterowania w wysoce zautomatyzowanych pojazdach, mającego na celu poprawę niezawodności systemu, wspieranie synergii między zespołami programistycznymi, minimalizację powielania wysiłków i przyspieszenie ogólnego rozwoju;**

- **Zaproponowanie referencyjnego modelu i metodologii technicznej dostosowanej do wykorzystania w działach badawczo-rozwojowych firm motoryzacyjnych, koncentrującej się na zaawansowanych systemach sterowania w wysoce zautomatyzowanych pojazdach, integrującej bezpieczeństwo i ochronę w całym procesie rozwoju oraz usprawniającej współpracę i komunikację w zespołach**.

W rozprawie zaproponowano podejście oparte na płynnej integracji aspektów bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa. Głównym celem jest odpowiedź na pilną potrzebę synergii w tych obszarach w kontekście dynamicznie zmieniającego się środowiska motoryzacyjnego, ze szczególnym uwzględnieniem praktycznych zastosowań w rzeczywistych warunkach. Szczególny nacisk położono na praktyczną użyteczność proponowanych rozwiązań, w szczególności w firmach zaangażowanych w projektowanie i rozwój złożonych rozwiązań. Skuteczność opracowanego modelu procesu organizacyjnego została potwierdzona na rzeczywistym przykładzie, podkreślając praktyczne zastosowanie w projektowaniu i opracowywaniu złożonych rozwiązań w tych firmach.

Struktura Pracy

Rozprawa doktorska składa się z następujących części:

- Obszerny przegląd literatury oraz aktualnych technologii wykorzystywanych w branży motoryzacyjnej. Szczególny nacisk położono na publikacje z renomowanych baz danych, takich jak Scopus i Institute of Electrical and Electronics Engineers (IEEE) Xplore, które dostarczają aktualnych i zweryfikowanych informacji.
- Budowa modelu procesu CyberSafety wykorzystując Business Process Model and Notation (BPMN) oraz Systems modeling language (SysML) jako języki modelowania. Opracowanie wskaźników oceny efektywności procesu.
- Weryfikacja opracowanego procesu CyberSafety bazując na studium przypadku zaawansowanego systemu aktywnego bezpieczeństwa - Highway Pilot (HP).
- Podsumowanie osiągniętych rezultatów, głównych wkładów w dyscyplinę oraz branżę motoryzacyjną oraz rozważania dotyczące możliwych ulepszeń w przyszłości.
- Załączniki - w załączniku A zawarto pełny model procesu CyberSafety (CySa) z narzędzia Bizagi, zapewniający szczegółowy wgląd w jego strukturę i komponenty. Ponadto, w załączniku B, w oparciu o wyniki prac, przedstawiono analizę cyberbezpieczeństwa struktury Highway Pilot (HP) ADAS, oferując cenny wgląd w aspekty bezpieczeństwa i cyberbezpieczeństwa.

Najważniejsze osiągnięcia

W ramach realizacji celów pracy sformułowano nowe podejście projektowe łączące zagadnienia CySe oraz FuSa oraz wykazano, iż przyczynia się on do poprawy jakości projektowanego systemu poprzez podwyższenie jakości oraz minimalizację zagrożeń.

Podejście to ma na celu poprawę niezawodności systemów, usprawnienie współpracy między zespołami rozwojowymi, minimalizację powielania działań oraz przyspieszenie rozwoju. Realizacja tego celu była odpowiedzią na rosnącą potrzebę synergii pomiędzy bezpieczeństwem funkcjonalnym a cyberbezpieczeństwem w dynamicznie rozwijającym się przemyśle motoryzacyjnym.

W wyniku przeprowadzonych prac osiągnięto następujące rezultaty:

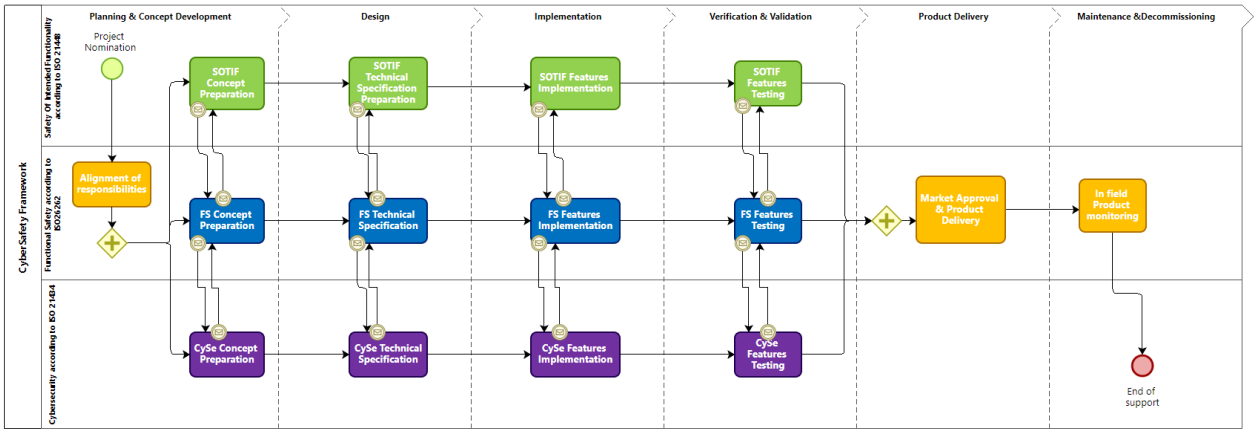
- **Opracowano model procesu CyberSafety *(CySa)* tj. zintegrowane podejście projektowe, unifikujące zagadnienia związane z bezpieczeństwem funkcjonalnych oraz cyberbezpieczeństwem,**
- **Bazując na doświadczeniu branżowym oraz przeglądzie dostępnych rozwiązań w literaturze, zdefiniowano wskaźniki procesu *(KPI)* wraz z ich akceptowalnymi wartościami, które użyto to weryfikacji zdefiniowanego podejścia *(CySa)*,**
- **Zdefiniowano wskaźnik efektywności *(ang. Effort Reduction Coeficient)*, weryfikujący nakłady pracy związane z analizą systemów,**

- **Zdefiniowano nowy proces oceny ryzyka oparty o Ważony współczynnik Bezpieczeństwa *(ang. Weighted Safety Score (WSS))*, dostosowany do specyfiki różnych obszarów funkcjonalnych w architekturze pojazdu. Dokonano analizy w oparciu o opracowany proces.**

- **Opracowany proces oraz wskaźniki zweryfikowano przeprowadzając analizę przypadku wg. procesu CyberSafety *(CySa)* dla systemu aktywnego wspomagania kierowcy.**

- **Przeprowadzona weryfikacja potwierdziła istotny spadek poziomu ryzyka, wzrost jakości projektowanego systemu przy jednoczesnym spadku nakładów pracy.**

Proces CyberSafety (CySa) został zaprojektowany w oparciu o istniejące standardy oraz ustrukturyzowany w celu uwzględnienia krytycznych interfejsów między procesami bezpieczeństwa funkcjonalnego oraz cyberbezpieczeństwa. Definiuje on również jasne role i obowiązki dla zespołów pracujących nad rozwojem produktu oraz podaje wspólne produkty pracy. Co ważne, proces ten wypełnia obecnie obowiązujące standardy motoryzacyjne. Dzięki użyciu języka BPMN oraz narzędzia Bizagi Modeller zdefiniowany proces można łatwo dostosować do specyficznych przepływów pracy w firmach motoryzacyjnych. Proces ten został przedstawiony na rysunku 2.



Rysunek 2: Ogólny schemat procesu CyberSafety . Kodowanie kolorami: Zielony - SOTIF, Niebieski - FuSa, Fioletowy - CySe, Żółty - Wspólne.

Znaczący nacisk położono na fazę projektowania w ramach procesu CySa, uznając jej kluczowe znaczenie w cyklu rozwoju produktu. Jednocześnie szczególną uwagę zwrócono na zarządzanie słabościami oprogramowania w fazie utrzymania produktu. Wynika to z wymagań związanych z procesem ciągłego monitorowania słabości oprogramowania, które są zwykle nakładane przez producentów samochodów zgodnie z regulacjami rynkowymi obowiązującymi w przemyśle motoryzacyjnym.

W świetle proponowanego podejścia CySa istnieje potrzeba zdefiniowania jasnych i reprezentatywnych wskaźników jakości tj. Key Performance Indicators, aby skutecznie mierzyć efektywność procesu. Ustanowienie właściwych i spójnych KPI służy kilku istotnym celom: zapewnieniu zgodności z przepisami, ułatwieniu zarządzania ryzykiem, ciągłego doskonalenia procesu i usprawnieniu komunikacji między interesariuszami.

Koncentrując się na fazie projektowania produktu, zdefiniowano następujące wskaźniki procesu Key Performance Indicators (KPI):

- Wskaźnik identyfikacji ryzyka bezpieczeństwa i ochrony (ang. Security And Safety Risk Identification Rate - SSRIR)
- Wskaźnik pokrycia oceny ryzyka (ang. Risk Assessment Coverage - RAC)
- Efektywność przeglądu projektu (ang. Design Review Effectivenes - DRE)
- Kompletność strategii łagodzenia skutków (ang. Mitigation Strategy Completeness - MSC)
- Wskaźnik zgodności projektu (ang. Design Compliance Rate - DCR)
- Poziom ryzyka rezydualnego (ang.Residual Risk Level - RRL)
- Pokrycie wymagań bezpieczeństwa i ochrony (ang. Security and Safety Requirement Coverage - SSRC)
- Wskaźnik złożoności projektu (ang. Design Complexity Index - DCI)
- Wskaźnik wniosków o zmianę projektu (ang.Design Change Request Rate - DCRR)

Wskaźnik identyfikacji ryzyka bezpieczeństwa i ochrony (SSRIR)

$$SSRIR = \frac{NumberofIdentifiedRisks}{TotalNumberofDesignElementsReviewed} \tag{1}$$

Zapewnia wczesną identyfikację potencjalnych zagrożeń. Wysoki wskaźnik SSRIR wskazuje na dokładny proces identyfikacji ryzyka. Akceptowalny wynik to 90% lub więcej, co sugeruje, że prawie wszystkie potencjalne zagrożenia zostały zidentyfikowane na etapie projektowania.

Wskaźnik pokrycia oceny ryzyka (RAC)

$$RAC = (\frac{NumberofAssessedRisks}{TotalNumberofIdentifiedRisks}) \times 100\% \tag{2}$$

Potwierdza dokładną ocenę ryzyka. Wszystkie zidentyfikowane ryzyka powinny zostać ocenione pod kątem wagi i prawdopodobieństwa. Akceptowalny wynik to 100%, wskazujący na kompleksowy zakres oceny ryzyka.

Efektywność przeglądu projektu (DRE)

$$DRE = (\frac{NumberofissuesIdentifiedinReviewes}{TotalNumberofIssues}) \times 100\% \tag{3}$$

Ocenia skuteczność przeglądów projektów. Skuteczne przeglądy projektów powinny identyfikować wysoki odsetek potencjalnych problemów. Akceptowalny wynik to 85% lub więcej, co wskazuje, że większość problemów jest wychwytywana podczas procesu przeglądu.

Kompletność strategii łagodzenia skutków (MSC)

$$MSC = (\frac{NumberofRiskswithCompleteMitigationStrategies}{TotalNumberofIdentifiedRisks}) \times 100\% \tag{4}$$

Zapewnia, że wszystkie ryzyka mają strategie łagodzenia. Wszystkie zidentyfikowane ryzyka powinny mieć kompletne strategie mitygacji. Akceptowalny wynik to 100%, zapewniający, że każde ryzyko ma udokumentowany i wykonalny plan łagodzenia skutków.

Wskaźnik zgodności projektu (DCR)

$$DCR = (\frac{Numberof CompliantDesignElements}{TotalNumberof DesignedElements}) \times 100\% \tag{5}$$

Weryfikuje zgodność z normami Elementy projektu powinny być w pełni zgodne z odpowiednimi normami (ISO 26262, ISO 21434). Akceptowalny wynik to 100%, wskazujący na pełną zgodność.

Poziom ryzyka rezydualnego (RRL)

$$RRL = \frac{\sum ResidualRiskScore}{TotalNumberof Risks} \tag{6}$$

Mierzy skuteczność ograniczania ryzyka. Ryzyko rezydualne powinno zostać zminimalizowane po wdrożeniu strategii ograniczania ryzyka. Akceptowalny wynik jest niski, najlepiej między 0 a 20, co wskazuje na skuteczne ograniczanie ryzyka.

Pokrycie wymagań bezpieczeństwa i ochrony (SSRC)

$$SSRC = (\frac{Numberof ImplementedRequirements}{TotalNumberof Requirements}) \times 100\% \tag{7}$$

Zapewnia spełnienie wszystkich wymagań. Wszystkie wymagania dotyczące bezpieczeństwa i ochrony powinny zostać zaimplementowane w projekcie. Akceptowalny wynik to 100%, zapewniający pełne pokrycie wymagań.

Wskaźnik złożoności projektu (DCI)

$$DCI = (\frac{Numberof Interconnections}{TotalNumbercomponents}) \tag{8}$$

Zarządzanie złożonością projektu. Złożoność projektu powinna być łatwa do opanowania, aby uniknąć luk w zabezpieczeniach i bezpieczeństwie. Akceptowalny wynik to umiarkowany, wskazujący na zrównoważoną i możliwą do zarządzania złożoność.

Wskaźnik wniosków o zmianę projektu (DCRR)

$$DCRR = (\frac{Numberof DesignChangeRequests}{TotalNumberof DesignElements}) \tag{9}$$

Wartości docelowe dla proponowanych wskaźników przedstawiono w tabeli 1.

Podsumowanie wskaźników CySa dla studium przypadku systemu HP przedstawiono w tabeli 2. Zdefiniowanie interfejsów między CySe i FuSa umożliwia uwzględnienie wszystkich wspólnych elementów związanych z metodami projektowania i weryfikacji. W związku z tym wynik DCR może osiągnąć wartość 100%. Techniki łagodzenia skutków są niezwykle ważne, a dzięki zidentyfikowaniu nakładania się CySe i FuSa współczynnik MSC osiąga wartość 100%.

Ponieważ CySa został zaprojektowany zgodnie z normami ISO 21434, ISO 26262 i ISO 21448, wszystkie produkty pracy są brane pod uwagę, a zatem wynik DCRR można wykazać jako 100%. Zasadniczo ramy procesu CySa mają zastosowanie do każdej domeny pojazdu. Koncentrując się na domenie bezpieczeństwa,

Tabela 1: Opis wskaźników procesu CyberSafety wraz z wartościami docelowymi.

Wskaźnik	**Wartość docelowa**
Wskaźnik identyfikacji ryzyka bezpieczeństwa i ochrony (SSRIR)	$\geq 90\%$
Wskaźnik pokrycia oceny ryzyka (RAC)	100%
Efektywność przeglądu projektu (DRE)	$\geq 85\%$
Kompletność strategii łagodzenia skutków (MSC)	100%
Wskaźnik zgodności projektu (DCR)	100%
Poziom ryzyka rezydualnego (RRL)	Bardzo niski (0-20)
Pokrycie wymagań bezpieczeństwa i ochrony (SSRC)	100%
Wskaźnik złożoności projektu (DCI)	Średni (1-3)
Wskaźnik wniosków o zmianę projektu (DCRR)	$\leq 10\%$

czynniki ryzyka związane z bezpieczeństwem odgrywają największą rolę, a początkowy wynik wysokości ryzyka jest uważany za wysoki lub bardzo wysoki. W trakcie prac udowodniono, że po prawidłowym wskazaniu ryzyka i zapewnieniu odpowiednich kontroli i środków, RRL może zmniejszyć się, w najgorszym przypadku, do umiarkowanej wartości.

Dzięki wspólnym wysiłkom w domenach CySe i FuSa, wynik pokrycia wymagań, tj. SSRC, osiąga 100%. Podczas oceny przykładu HP z IDS jako proponowanym środkiem łagodzącym zarówno dla CySe, jak i FuSa, zakładany wskaźnik DCI może osiągnąć umiarkowaną wartość.

Wyniki THA i DCRR nie zostały dokładnie ocenione, ponieważ wymagają danych w czasie rzeczywistym w terenie. Niemniej jednak, postępując zgodnie z CySa, organizacje mogą spodziewać się niskiego wskaźnika DCRR, ponieważ wszystkie krytyczne kwestie projektowe zostały już uwzględnione na początku procesu projektowego.

Tabela 2: Opis wskaźników procesu cyberbezpieczeństwa wraz z ocenianymi wartościami w kontekście domeny bezpieczeństwa.

Wskaźnik	**Docelowa wartość**
Wskaźnik identyfikacji ryzyka w zakresie bezpieczeństwa i ochrony (SSRIR)	100%
Pokrycie oceny ryzyka (RAC)	100%
Skuteczność przeglądu projektu (DRE)	100%
Kompletność strategii łagodzenia skutków (MSC)	100%
Wskaźnik zgodności projektu (DCR)	100%
Poziom ryzyka rezydualnego (RRL)	Umiarkowany
Pokrycie wymagań bezpieczeństwa i ochrony (SSRC)	100%
Wskaźnik złożoności projektu (DCI)	Umiarkowany

Wprowadzenie procesu rozwoju CySa oznacza znaczącą zmianę w projektowaniu systemów motoryzacyjnych poprzez kompleksową identyfikację ryzyka na wczesnym etapie, a tym samym skuteczniejsze podejmowanie decyzji projektowych. Zdefiniowane wskaźniki KPI ułatwiają walidację procesu, zapewnia-

jąc, że ryzyka związane z CySe i FuSa są wspólnie analizowane i rozwiązywane, co prowadzi do lepszych wyników w zdefiniowanych metrykach. To zintegrowane podejście zapewnia, że wszystkie interfejsy między CySe i FuSa są zdefiniowane, wszystkie strategie łagodzenia są kompletne, a zgodność z normami ISO 21434, ISO 26262 i ISO 21448 jest osiągnięta. Rezultatem jest spójna i holistyczna struktura procesu inżynieryjnego, która może być stosowana przy projektowaniu różnych systemów pojazdów.

Podstawowy cel rozprawy, jakim było sformułowanie wysoce praktycznego i możliwego do wdrożenia podejścia do projektowania oraz wdrażania zaawansowanych systemów sterowania w wysoce zautomatyzowanych pojazdach, został osiągnięty i zweryfikowany. Walidacja ta została przeprowadzona poprzez proces oceny, realizowany w ramach powszechnie uznanego narzędzia Ansys Medini, w którym zaproponowano analizę międzyfunkcjonalną. Przykładem wybranym do tej oceny był system Highway Pilot, dobrany ze względu na jego rolę jako przedstawiciela wysoce zautomatyzowanej i złożonej funkcji bezpieczeństwa. Wybór ten był kluczowy, ponieważ wymagał kompleksowej oceny uwzględniającej zarówno aspekty bezpieczeństwa funkcjonalnego, jak i cyberbezpieczeństwa.

Proponowane rozwiązanie rozszerza analizę Cybersecurity (CySe) na nowe obszary, eliminując jej zwyczajową głęboką integrację z architekturą pojazdu Electrical/Electronic (EE). Zamiast tego koncentruje się na wyabstrahowanych funkcjonalnych komponentach architektonicznych systemu, ich relacjach, przepływach danych, przypadkach użycia i wzorcach komunikacji. Taka abstrakcja umożliwia identyfikację zagrożeń niezależnie od fizycznych implementacji, pozwalając na wczesne wykrywanie i łagodzenie możliwych problemów przed sfinalizowaniem fizycznych decyzji architektonicznych i alokacji funkcjonalnych.

Wyniki ewaluacji dostarczają przekonujących dowodów empirycznych na poparcie hipotezy badawczej. Rysunek 3 pokazuje znaczną redukcję zagrożeń dla cyberbezpieczeństwa i bezpieczeństwa (z bardzo wysokich do niskich) w przypadku analizowanego systemu Highway Pilot (HP). Co więcej, tabela 3 pokazuje znaczny spadek nakładów na rozwój, szczególnie w fazie projektowania systemu (do 60%), obliczonego zgodnie z zaproponowanym współczynnikiem redukcji wysiłku *Effort Reduction Coefficient (ERC)* według równania (10). Co ważne, redukcja nakładu pracy została osiągnięta przy jednoczesnym zachowaniu zgodności z ustalonymi standardami.

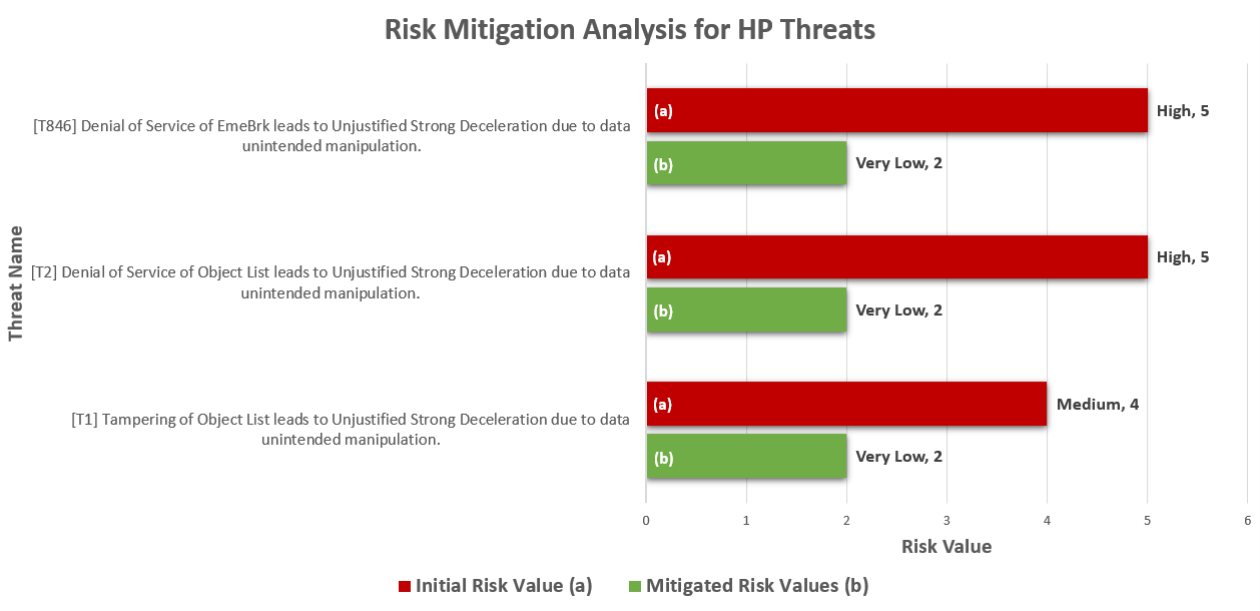
$$ERC = \frac{NOSI}{TNOSI} \times 100\% \tag{10}$$

gdzie:

ERC reprezentuje współczynnik redukcji wysiłku,

$NOSI$ oznacza liczbę elementów współużytkowanych,

$TNOSI$ to całkowita liczba elementów.



Rysunek 3: Analiza ograniczania ryzyka dla zagrożeń HP - (a) początkowe wartości ryzyka, (b) ryzyko złagodzone.

Tabela 3: Redukcja wysiłku analizy projektu produktu na podstawie funkcji HP.

Rodzaj produktu pracy	**Wskaźnik Efektywności (ERC)%**
Definicja przedmiotu analizy	100
Definicja scenariuszy ryzyka *	37.93
Definicja celów	38.46
Definicja wymagań	63.87
Podsumowanie	**66.50**

* Scenariusze zagrożeń i szkód są połączone w scenariusz ryzyka.

Adresując zidentyfikowane braki we wspólnej analizie ryzyka dla FuSa oraz CySe, zaproponowano wieloaspektową metodę oceny, która łączy oba te aspekty. W tym celu zdefiniowano parametry Hazard Safety Indicator (HaSI) oraz Threat Risk Score (ThRS). Hazard Safety Indicator (HaSI) jest obliczany na podstawie wyniku Automotive Safety Integrity Level (ASIL), biorąc pod uwagę dotkliwość, narażenie i możliwość kontroli zagrożenia, podczas gdy Threat Risk Score (ThRS) ocenia wpływ, prawdopodobieństwo wystąpienia oraz wykrywalność. Te dwa parametry stanowią podstawę Weighted Safety Score (WSS), przy obliczaniu którego brane są pod uwagę wartości wagowe odpowiadające różnym obszarom funkcjonalnym w architekturze pojazdu. Weighted Safety Score (WSS) zapewnia całościowy obraz ryzyka związanego z sys-

temem, wspierając podejmowanie bardziej świadomych decyzji w zakresie ograniczania ryzyka i poprawy bezpieczeństwa. Zakresy punktacji WSS zostały przedstawione w tabeli 4. W ramach studium przypadku HP, przeanalizowano zagrożenia CySe oraz FuSa gdzie obliczono wskaźnik WSS przed i po zastosowaniu środka mitygującego w postaci systemu wykrywania intruzów tj. Intrusion Detection System (IDS). Wyniki analiz zostały przedstawione w tabeli 5.

Tabela 4: Zakresy WSS i ich interpretacja.

Zakres WSS	**Poziom ryzyka**	**Interpretacja**
0-20	Bardzo niskie ryzyko	System jest uważany za bardzo bezpieczny. Wymagane są minimalne lub żadne dodatkowe środki bezpieczeństwa. Zalecane jest ciągłe monitorowanie.
21-40	Niskie ryzyko	System charakteryzuje się niskim poziomem ryzyka. Podstawowe środki bezpieczeństwa i ochrony zostały wdrożone i są odpowiednie. Konieczne mogą być regularne przeglądy i drobne usprawnienia.
41-60	Umiarkowane ryzyko	System charakteryzuje się umiarkowanym poziomem ryzyka. Należy rozważyć zastosowanie dodatkowych środków bezpieczeństwa i ochrony. Konieczne jest regularne monitorowanie i przeprowadzanie okresowych ocen bezpieczeństwa.
61-80	Wysokie ryzyko	System charakteryzuje się wysokim poziomem ryzyka. Wymagana jest znaczna poprawa bezpieczeństwa i ochrony. Niezbędne jest wzmocnione monitorowanie i częste przeglądy bezpieczeństwa i ochrony.
81-100	Bardzo wysokie ryzyko	System jest uważany za bardzo niebezpieczny. Niezbędne są natychmiastowe i szeroko zakrojone środki bezpieczeństwa. Wymagane jest ciągłe i intensywne monitorowanie.

Tabela 5: Znormalizowany ważony współczynnik bezpieczeństwa przed i po zastosowaniu systemu wykrywania intruzów.

Zagrożenie FuSa	Zagrożenie CySe	Znormalizowany WSS przed włączeniem IDS	Znormalizowany WSS po włączeniu IDS
H1	T1	81.4	59.5
H1	T2	83.2	56.9
H1	T3	77.32	56.5
H2	T1	36.8	14.9
H2	T2	38.7	12.3
H2	T3	32.7	11.9
H3	T1	45.7	23.8
H3	T2	47.6	21.2
H3	T3	41.6	20.8

Podsumowanie i wnioski

Rosnąca złożoność systemów motoryzacyjnych, wynikająca między innymi z automatyzacji i potrzeby komunikacji (ang. connectivity), ujawniła słabości oprogramowania, które mają wpływ na z cyberbezpieczeństwo systemu. Niniejsza rozprawa wypełnia istotną lukę między zagadnieniami bezpieczeństwa funkcjonalnego a cyberbezpieczeństwem proponując holistyczne podejście do analizy i zarządzania ryzykiem w wysoce zautomatyzowanych systemach motoryzacyjnych;

Integracja analizy cyberbezpieczeństwa i bezpieczeństwa

Łącząc oceny Cybersecurity (CySe) i Functional Safety (FuSa) w ujednolicone ramy analizy ryzyka, niniejsza rozprawa przedstawia kompleksowe podejście do łagodzenia przypadkowych awarii i złośliwych ataków. Ta zintegrowana perspektywa znacznie poprawia ogólne bezpieczeństwo ruchu drogowego, zmniejszając prawdopodobieństwo wypadków spowodowanych awariami technicznymi i cyberatakami. Integracja analiz w tych dwóch obszarach uwzględnia funkcjonowanie komponentów elektronicznych w systemach motoryzacyjnych i oprogramowaniu, których specyfika projektowa i operacyjna była dotychczas analizowana oddzielnie w każdym z obszarów. Jednak wzajemna współzależność zagrożeń w tych obszarach sugeruje przyjęcie zintegrowanego podejścia.

Naświetlenie zależności technicznych i ich wpływu na ryzyko

Praca doktorska podkreśla krytyczną rolę zależności technicznych w kontekście połączonego systemu pojazdów o wysokim stopniu automatyzacji. Analizując potencjalny wpływ tych zależności na system CySe i FuSa, w tym kluczowe elementy elektroniki samochodowej i oprogramowania, badanie to dostarcza cennych informacji do projektowania odpornych systemów samochodowych.

Rozwój nowatorskich, elastycznych i kwantyfikowalnych ram analizy ryzyka

Wprowadzono elastyczne i skalowalne ramy analizy ryzyka, dostosowane do zmieniającego się krajobrazu branży motoryzacyjnej, przy jednoczesnym przestrzeganiu standardów branżowych. Ramy te umożli-

wiają skuteczną identyfikację, ocenę i ograniczanie ryzyka w całym cyklu życia produktu. Ocena wykazała znaczne zmniejszenie zarówno zagrożeń dla bezpieczeństwa, jak i cyberbezpieczeństwa, podkreślając ich skuteczność w zwiększaniu niezawodności i bezpieczeństwa systemu.

Koncentracja na wczesnym ograniczaniu ryzyka i proaktywnej kulturze bezpieczeństwa

Proponowana metoda nadaje priorytet wczesnej identyfikacji i ograniczaniu ryzyka, wspierając proaktywną kulturę bezpieczeństwa w organizacjach motoryzacyjnych. Zajmując się potencjalnymi słabymi punktami na wczesnym etapie procesu rozwoju, podejście to poprawia jakość produktu i zwiększa ogólną odporność systemu.

Promocja perspektywy inżynierii systemów w celu zwiększenia bezpieczeństwa i ochrony

Badania przeprowadzone w ramach pracy doktorskiej opowiadają się za podejściem inżynierii systemów do rozwoju motoryzacji, podkreślając współzależności między bezpieczeństwem i cyberbezpieczeństwem. Traktując CySe i FuSa jako integralne elementy systemu, praca ta promuje współpracę między zespołami inżynierów i ułatwia rozwój bezpieczniejszych i bardziej niezawodnych pojazdów. Proponowane podejście jest komplementarne z zakresem dyscypliny naukowej automatyki, elektrotechniki, elektroniki i technologii kosmicznych, które obejmują wzajemnie powiązane obszary.

Ustalenie jasnych celów i mierzalnych wyników

Rozprawa doktorska przedstawia ustrukturyzowane podejście do definiowania jasnych celów bezpieczeństwa i ochrony oraz koncepcji technicznych, umożliwiając skuteczne zarządzanie ryzykiem i ocenę wydajności. Poprzez dostosowanie działań ograniczających ryzyko do ogólnych celów systemu, praca ta przyczynia się do rozwoju systemów motoryzacyjnych, które spełniają najwyższe standardy bezpieczeństwa i ochrony.

Doskonalenie metodologii analizy ryzyka

Praca wprowadza nowatorskie techniki analizy ryzyka, które są dostosowane do złożoności wysoce zautomatyzowanych pojazdów. Odnosząc się do wielowymiarowego charakteru ryzyka związanego z motoryzacją, praca ta stanowi podstawę dla przyszłych postępów w ocenie i zarządzaniu ryzykiem.

Zdefiniowanie wskaźników efektywności zaproponowanego procesu

W ramach rozprawy doktorskiej, bazując na dostępnych publikacjach naukowych, zgromadzonej wiedzy teoretycznej oraz praktycznym doświadczeniu zdobytym w branży, zaproponowano autorskie wskaźniki jakości. Wskaźniki te zostały opracowane w celu precyzyjnego określenia efektywności zaproponowanego procesu CySa, umożliwiając jego ocenę pod kątem spełniania kluczowych wymagań bezpieczeństwa oraz zgodności z założeniami badawczymi i potrzebami praktycznymi w dynamicznie rozwijającym się środowisku motoryzacyjnym.

Niniejsza rozprawa doktorska wnosi znaczący wkład w dziedziny automatyki, elektroniki, elektrotechniki i technologii kosmicznych, zajmując się krytyczną interakcją między bezpieczeństwem a cyberbezpieczeństwem w wysoce zautomatyzowanych systemach pojazdów o znaczeniu krytycznym. Zaproponowane ramy stanowią podstawę dla rozwoju bezpieczniejszych i bardziej niezawodnych systemów w obliczu rosnącej złożoności i łączności. W pojazdach, w których rośnie rola elektroniki i elementów sterujących komponentami mechanicznymi, autonomiczna jazda będzie zależeć przede wszystkim od niezawodnego działania systemów elektronicznych i oprogramowania, a nie od mechanicznych aspektów działania pojazdu. Dlatego

zapewnienie bezpieczeństwa i cyberbezpieczeństwa tych systemów ma kluczowe znaczenie dla przyszłości autonomicznego transportu.

Przyszłe kierunki badań

W pełni autonomiczne pojazdy, w których kierowca jest całkowicie odsunięty od procesu prowadzenia, pozostają odległą koncepcją. Ich realizacja wymaga opracowania całego ekosystemu, który obejmuje nie tylko same pojazdy, ale także kompleksową infrastrukturę drogową oraz solidną, wysokiej jakości łączność bezprzewodową. Wymagania te stanowią poważne wyzwanie, zwłaszcza na obszarach poza centrami miast, gdzie budowa takiej infrastruktury może być szczególnie trudna.

Jedną z największych przeszkód w przejściu do w pełni autonomicznych systemów jest faza pośrednia. Faza ta obejmuje współistnienie w pełni autonomicznych i pół-autonomicznych pojazdów na drogach. W tym okresie wyeliminowanie czynnika ludzkiego, który często przyczynia się do wypadków, okazuje się trudnym zadaniem. Ta koegzystencja rodzi pytania o to, w jaki sposób ludzcy kierowcy wchodzą w interakcje z pojazdami autonomicznymi oraz jakie są potencjalne zagrożenia dla bezpieczeństwa związane z tą złożoną dynamiką.

Pomimo znacznej odległości w czasie, jaka dzieli nas od osiągnięcia świata „zero wypadków", w którym czynnik ludzki jest całkowicie wyeliminowany, konieczne jest, abyśmy pilnie wytyczyli właściwy kurs i pracowali nad standaryzacją rozwiązań. Jest to szczególnie ważne, biorąc pod uwagę rosnącą popularność połączonych pojazdów, które są bardzo narażone na cyberzagrożenia.

Bibliografia

[1] Charlie Miller and Chris Valasek. Hackers remotely kill a jeep on the highway - with me in it, 2014. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [Accessed: Dec2023].

[2] ISO Central Secretary. Road vehicles — functional safety. Standard ISO 26262:2018, International Organization for Standardization, Geneva, CH, 2018.

[3] ISO Central Secretary. Road vehicles — safety of the intended functionality. Standard ISO 21448:2019, International Organization for Standardization, Geneva, CH, 2019.

[4] ISO Central Secretary. Road vehicles — cybersecurity engineering. Standard ISO 21434:2021, International Organization for Standardization, Geneva, CH, 2021.

[5] Xugui Zhou, Anna Schmedding, Haotian Ren, Lishan Yang, Philip Schowitz, Evgenia Smirni, and Homa Alemzadeh. Strategic safety-critical attacks against an advanced driver assistance system. In *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 79–87, 2022.

[6] KEEN Security LAB. Car hacking research: Remote attack tesla motors, 2016. https://www.youtube.com/watch?v=c1XyhReNcHY&ab_channel=KeenSecurityLab [Accessed: May2024].

[7] Kyounggon Kim, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, and Huy Kang Kim. Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers and Security*, 103:102150, 2021.

[8] Upstream Security Ltd. Smart mobility cyber attacks repository, 2024. https://www.upstream.auto/research/automotive-cybersecurity/ [Accessed: May2024].

[9] Jonathan Petit, Bas Stotelaar, Michael Feiri, and Frank Kargi. Remote attacks on automated vehicles sensors: Experiments on camera and lidar, 2015. https://api.semanticscholar.org/CorpusID:39608826 [Accessed: Dec2023].

[10] KEEN Security LAB. Experimental security assessment of bmw cars: A summary report, 2019. https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf [Accessed: Dec2023].

[11] Piotr Piatek, Piotr Mydlowski, Aleksander Buczacki, and Szczepan Moskwa. Concept of Using the MBSE Approach to Integrate Security Patterns in Safety-Related Projects for the Automotive Industry. *IEEE Transactions on Intelligent Transportation Systems*, 25(11):15477–15492, November 2024.