Abstract

The automotive industry is undergoing a revolutionary transformation with increased automation and data integration, necessitating a paradigm shift in the development of automotive electronic embedded systems. This dissertation addresses the critical need to integrate functional safety and cybersecurity in the design and implementation of highly automated control systems with mixed criticality in vehicles, presenting a holistic approach to solving complex, interdisciplinary, and cross-functional challenges.

Current approaches to analyzing automotive systems often treat safety and cybersecurity as separate domains, leading to increased errors, higher risks, reduced safety confidence, and the emergence of new hazards. This includes remote vehicle takeover, data leaks, vehicle thefts and break-ins, and issues related to service and business development, legal and regulatory compliance. A notable example of the risks involved is the famous "Jeep Hack", where cybersecurity vulnerabilities and insufficient isolation were exploited to remotely control the vehicle, underscoring the critical need for integrated safety and cybersecurity measures.

This dissertation highlights the imperative to analyze these aspects together, proposing a unified methodology that significantly reduces risks and improves system reliability. The integration is grounded in over ten years of industry experience, emphasizing deep technical knowledge in risk analysis and its impact on system design and architectural decisions, which are crucial for product commercialization.

There is a profound interplay between safety and cybersecurity, as both are based on the same fundamental principles. Commonalities such as risk identification, vulnerability analysis, and mitigation implementation exist in both domains. Therefore, a natural progression in the development of advanced systems is to analyze safety and cybersecurity together. Using extensive similarities and generic approaches allows the use of common tools and methodologies, contributing to more effective identification and resolution of potential threats. This coherence provides a unique opportunity to apply a unified approach, fostering greater synergy between domains, minimizing duplication of effort, and accelerating the product development process.

Furthermore, the dissertation underscores the benefits of integrating safety and cybersecurity through Model-Based Systems Engineering (MBSE) and joint engineering trends. The proposed reference organizational model is tailored for automotive Research and Development departments, promoting early collaborative development of safety and cybersecurity requirements. This integration ensures that the development process is both practical and scalable, addressing real-world applicability in industrial settings.

The research introduces the CyberSafety (CySa) process, a novel framework that combines safety and cybersecurity efforts from the earliest stages of product development. Using extensive literature reviews, standard analysis, and industry consultations, the CyberSafety process aims to effectively reduce risks,

propose technical solutions, and therefore increase the quality of the system. However, at the same time, optimize resource allocation, reduce time-to-market, and manage maintenance periods and associated risks effectively.

This approach is validated through a newly defined set of Key Performance Indicators (KPI)s as well as a detailed case study of a Highway Pilot (HP) system, which demonstrates a potential reduction in development effort by up to 66.5% and a significant decrease in related risks, thus improving overall quality and security of the product. In addition, a new robust risk scoring methodology, which extends stand-alone Cybersecurity (CySe) and Functional Safety (FuSa), the Weighted Safety Score (WSS) is proposed and evaluated. It takes into account both hazards and threats, with weight factors tailored to various automotive domains. The WSS provides a holistic view of the risk landscape of the system, supporting better informed decision making for risk mitigation and safety improvements.

Furthermore, the proposed solution extends CySe analysis into new domains, removing its traditional deep integration with the Electrical/Electronic (EE) vehicle architecture. Instead, it emphasizes abstracted system functional architecture elements, their interactions, use case data flows, and communication patterns. This abstraction facilitates the identification of risks independently from physical implementations, allowing early detection and mitigation of potential threats before finalizing physical architecture decisions and functional allocations.

The dissertation includes both theoretical and practical dimensions, applying the proposed methods to real active safety systems, specifically the HP, and promoting the innovative use of available toolchains. Through in-depth safety analysis, the research demonstrates a significant reduction in the risk and analysis effort.

The conclusions highlight the success of the CyberSafety process in improving system design decisions and reducing risks. Future work will focus on refining this process with newer tools and methodologies, expanding its applicability beyond the automotive industry, and integrating security patterns into existing cybersecurity standards. Ongoing collaboration with standardization working groups will be essential to keep up with the evolving landscape of autonomous vehicle safety and cybersecurity.

In essence, this dissertation provides a transformative approach to developing safe and secure systems for highly autonomous vehicles, redefining the future of automotive development through innovative risk analysis and comprehensive system integration.

Streszczenie

Przemysł motoryzacyjny przechodzi rewolucyjną transformację, wraz ze wzrostem automatyzacji i integracji danych, co wymaga zmiany paradygmatu w rozwoju elektronicznych systemów wbudowanych w pojazdach. Niniejsza rozprawa podejmuje krytyczną potrzebę integracji bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa w projektowaniu i wdrażaniu wysoko zautomatyzowanych systemów sterowania o mieszanej krytyczności w pojazdach, przedstawiając holistyczne podejście do rozwiązywania złożonych, interdyscyplinarnych i wielofunkcyjnych wyzwań.

Obecne podejścia do analizy systemów motoryzacyjnych często traktują bezpieczeństwo funkcjonalne i cyberbezpieczeństwo jako odrębne dziedziny, co prowadzi do wzrostu błędów, wyższego poziomu ryzyka, mniejszego bezpieczeństwa systemu oraz pojawienia się nowych zagrożeń. Obejmuje to przejęcia pojazdów na odległość, wycieki danych, kradzieże pojazdów i włamania oraz problemy związane z rozwojem usług i biznesu, zgodnością prawną i regulacyjną. Znanym przykładem tych zagrożeń jest słynny atak na Jeep'a, w którym wykorzystano luki w zabezpieczeniach cybernetycznych do zdalnego sterowania pojazdem, co podkreśla krytyczną potrzebę zintegrowanych środków bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa.

Niniejsza rozprawa podkreśla konieczność wspólnej analizy tych aspektów, proponując uwspólnioną metodologię, która znacząco redukuje ryzyka i poprawia niezawodność systemu. Integracja ta opiera się na ponad dziesięciu latach doświadczenia w branży, podkreślając głęboką wiedzę techniczną w zakresie analizy ryzyka oraz jej wpływ na projektowanie systemu i decyzje architektoniczne, które są kluczowe dla komercjalizacji produktu.

Istnieje głęboka interakcja między bezpieczeństwem funkcjonalnym a cyberbezpieczeństwem, ponieważ obie dziedziny opierają się na tych samych fundamentalnych zasadach. Wspólne elementy, takie jak identyfikacja ryzyka, analiza podatności i wdrażanie działań zaradczych, występują zarówno w bezpieczeństwie funkcjonalnym, jak i w cyberbezpieczeństwie. Dlatego naturalnym postępem w rozwoju zaawansowanych systemów jest wspólna analiza bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa. Wykorzystanie licznych podobieństw pozwala na stosowanie wspólnych narzędzi i metodologii, co przyczynia się do bardziej efektywnej identyfikacji i rozwiązywania potencjalnych zagrożeń. Ta spójność między bezpieczeństwem funkcjonalnym a cyberbezpieczeństwem stwarza unikalną okazję do zastosowania zjednoczonego podejścia, sprzyjając większej synergii między dziedzinami, minimalizując powielanie wysiłków i przyspieszając proces rozwoju produktu.

Ponadto, rozprawa podkreśla korzyści płynące z integracji bezpieczeństwa i cyberbezpieczeństwa poprzez inżynierię systemów opartą na modelach (ang. model-based systems engineering) oraz wspólne

trendy inżynierskie. Proponowany model organizacyjny jest dostosowany do działów badawczo-rozwojowych w motoryzacji, promując wczesne, wspólne opracowywanie wymagań dotyczących bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa. Ta integracja zapewnia, że proces rozwoju jest zarówno praktyczny, jak i skalowalny, odpowiadając na rzeczywiste zastosowania w środowiskach przemysłowych.

Badania wprowadzają proces CyberSafety, nowatorskie ramy, które łączą wysiłki w zakresie bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa od najwcześniejszych etapów rozwoju produktu. Wykorzystując obszerne przeglądy literatury, analizy standardów i konsultacje branżowe, proces CyberSafety ma na celu optymalizację alokacji zasobów, skrócenie czasu wprowadzenia na rynek oraz skuteczne zarządzanie okresami utrzymania i związanymi z nimi ryzykami. Podejście to zostało zweryfikowane za pomocą nowo zdefiniowanego zestawu wskaźników efektywności, a także szczegółowego studium przypadku systemu Pilota Autostradowego (ang.Highway Pilot), które wykazało potencjalne zmniejszenie nakładu pracy na rozwój nawet o 66,5% i znaczny spadek powiązanego ryzyka, poprawiając w ten sposób ogólną jakość i bezpieczeństwo produktu. Ponadto zaproponowano i zbadano nową, solidną metodologię oceny ryzyka, która rozszerza samodzielne analizy ryzyk bezpeczeństwa funkcjonalnego oraz cyberbezpieczeństwa tj. Ważony Współczynnik Bezpieczeństwa (ang. Weighted Safety Score (WSS)). Uwzględnia on zarówno zagrożenia, jak i niebezpieczeństwa, ze współczynnikami wagi dostosowanymi do różnych dziedzin motoryzacji. WSS zapewnia całościowy obraz ryzyka związanego z systemem, wspierając podejmowanie bardziej świadomych decyzji w zakresie ograniczania ryzyka i poprawy bezpieczeństwa.

Rozprawa obejmuje zarówno teoretyczne, jak i praktyczne wymiary, stosując proponowane metody do rzeczywistych systemów aktywnego bezpieczeństwa, w szczególności autostradowego wspomagania kierowcy, i promując innowacyjne wykorzystanie dostępnych narzędzi. Poprzez dogłębną analizę bezpieczeństwa, badania wykazują znaczną redukcję ryzyka i nakładu pracy analitycznego.

Wnioski podkreślają sukces procesu CyberSafety w poprawie decyzji projektowych systemów i redukcji ryzyk. Przyszłe prace będą koncentrować się na udoskonalaniu tego procesu za pomocą nowszych narzędzi i metodologii, rozszerzając jego zastosowanie poza branżę motoryzacyjną i integrując wzorce bezpieczeństwa z istniejącymi standardami cyberbezpieczeństwa. Ciągła współpraca z grupami standaryzacyjnymi będzie niezbędna, aby nadążyć za ewoluującym krajobrazem bezpieczeństwa i cyberbezpieczeństwa pojazdów autonomicznych.

W istocie, niniejsza rozprawa dostarcza transformacyjnego podejścia do rozwoju bezpiecznych i zabezpieczonych systemów dla wysoko autonomicznych pojazdów, redefiniując przyszłość rozwoju motoryzacji poprzez innowacyjną analizę ryzyka i kompleksową integrację systemów.