HATARA: A Novel Approach by Fusion of HARA and TARA for System Safety and Security Analysis

Jherrod Thomas
Certified Functional Safety Expert, Tomco Service Group LLC
Jherrod.Thomas@tomcousa.com
The Lion of Functional Safety™

***Abstract*—The manuscript presents a thorough investigation into the HATARA framework, an innovative fusion of Hazard Analysis and Risk Assessment (HARA) with Threat Analysis and Risk Assessment (TARA), aimed at concurrently addressing the domains of safety and cybersecurity within automotive systems. This integrated approach is deemed imperative amidst the growing complexity and connectivity of contemporary vehicles, especially those that are autonomous and connected. The study elaborates on the procedural synergies and methodological convergences between the disciplines of safety and security, enabled through HATARA, to promote a comprehensive analytical paradigm. Through a series of illustrative case studies, the utility of this framework in improving risk mitigation strategies, optimizing development processes, and enhancing the resilience of automotive systems against a variety of threats is substantiated. Additionally, the paper recognizes the challenges inherent in deploying such an all-encompassing analysis framework, including the need for specialized knowledge and the complexities associated with harmonizing diverse analytical methodologies. The significance of this paper lies in its in-depth exposition of HATARA, providing a systematic methodology for the integration of safety and security risk assessments, thereby fulfilling a vital requirement for thorough, unified analyses amidst the advancement of automotive technologies. This research not only enriches the scholarly dialogue on automotive safety and security but also offers practical insights for industry practitioners, aimed at enhancing the reliability of future automotive innovations.**

***Index Terms*—ISO 26262, ISO 21434, HARA, TARA, HATARA Automotive Safety, Risk Assessment, Technological Integration, Hazard Analysis, Automotive Industry Standards**

I. Introduction

In the automotive sector, a profound shift is underway, underscored by technology's swift integration and progression within vehicular frameworks. This transition has engendered a heightened complexity in automotive architectures, chiefly due to the advent of connectivity and advanced functional features. While these developments augment the end-user experience, they concurrently pose novel challenges in the domain of system development [1], [2].

A pivotal facet of these emerging challenges is the simultaneous consideration of multiple quality attributes, explicitly focusing on functional safety and cybersecurity. In the automotive context, functional safety denotes the vehicle's ability to maintain safe operation even in system malfunctions [3]. Historically, this aspect has been integral to automotive design, underpinning the dependability and safety of vehicles [4].

Manuscript received February 03, 2024; revised February 06, 2024.

Concurrently, cybersecurity has risen to prominence as an attribute of equal significance in the era of interconnected vehicles. Automotive cybersecurity transcends traditional notions of data protection, encompassing the preservation of vehicular operational integrity and passenger safety [5]. As vehicular systems evolve towards more excellent connectivity and autonomy, the potential cyber threats increase, elevating the importance of cybersecurity in vehicular safety.

Integrating safety and security within automotive systems is not merely a juxtaposition of two distinct attributes but an intricate understanding and management of their mutual dependencies. Approaching these domains in isolation may result in scenarios where mitigating risk in one domain inadvertently heightens or neglects risks in the other [1]. Hence, an integrative strategy that contemplates safety and security in engineering and developing automotive systems is imperative [6].

This necessity for an integrated approach is particularly salient in the context of autonomous and semi-autonomous vehicles. These vehicles are reliant on sophisticated networks of sensors, control mechanisms, and data processing units, necessitating their reliable and secure operation to safeguard both functional safety and cybersecurity [3], [7].

The evolving dynamics of automotive systems, marked by increased connectivity and automation, call for a fundamental alteration in system development paradigms. This alteration should be oriented towards a comprehensive approach, prioritizing the concurrent and intertwined demands of functional safety and cybersecurity to ensure the robustness and resilience of vehicles in the contemporary, interconnected, and technologically advanced landscape [5].

A. Motivation and Objective

The impetus for amalgamating Hazard Analysis and Risk Assessment (HARA) with Threat Analysis and Risk Assessment (TARA) emanates from the progressively converging realms of safety and security in contemporary automotive systems. The distinction between safety and security risks is progressively diminishing within autonomous and connected vehicles. Safety risks, traditionally linked with vehicular system malfunctions, are now intricately connected with security risks, originating from the potentiality of malevolent cyber incursions [3].

This amalgamation's principal aim is to formulate an all-encompassing methodology, addressing both safety and secu-

rity risks under a singular framework. This unified approach is imperative for augmenting the robustness and resilience of automotive systems. As vehicles increasingly depend on electronic and software components and interface with external networks, the likelihood of safety hazards emerging from cybersecurity vulnerabilities intensifies [5]. Consequently, a methodology that concurrently considers both safety and security is indispensable.

An additional incentive for integrating HARA and TARA lies in the evolving spectrum of threats within the automotive sector. The progression of connected and autonomous vehicles heralds the emergence of unforeseen novel threats. These threats jeopardize vehicular data security and may culminate in physical detriment, underscoring the necessity of integrating safety and security evaluations [1], [8].

Moreover, this objective encompasses refining the development process by presenting a holistic perspective of the risk landscape. This comprehensive outlook facilitates the identification of intersecting areas between safety and security, thereby preventing redundant efforts and ensuring that mitigation strategies are harmoniously aligned [1].

In essence, the fusion of HARA and TARA is propelled by the necessity to adapt to the shifting risk milieu in the automotive industry, where the boundaries between safety and security are increasingly overlapping. The overarching ambition is to guarantee that modern vehicles are functionally safe and robustly fortified against the expanding array of cyber threats.

B. Significance of Comprehensive Safety and Security Analysis

The paramount importance of a thorough safety and security analysis in contemporary automotive systems is indisputable. An all-encompassing strategy is essential, as separate examinations of safety or security fail to adequately address the array of risks present in sophisticated, interlinked systems. The interrelationship between safety and security implies that a deficiency in one domain can substantially affect the other [1].

The convergence of operational and informational technologies in vehicular systems has ushered in novel vulnerabilities and threats. For example, connected vehicles are prone to cyber-attacks, which could jeopardize data integrity and the vehicle's physical functioning. This reality necessitates the inclusion of cybersecurity threats in the comprehensive safety risk assessment of vehicles [5].

Furthermore, as vehicles increasingly rely on advanced algorithms and electronic control systems for autonomous operation, the imperative for an integrated approach to safety and security becomes more pronounced. The reliability of these systems hinges not solely on their operational efficiency under standard conditions but also on their robustness against malicious intrusions and other security perils [3].

A holistic analysis guarantees that safety measures to mitigate specific risks do not unintentionally create new vulnerabilities. For instance, safety mechanisms designed to override driver control in particular scenarios must be impervious to cyber-attacks or unauthorized interference [1].

The amalgamation of safety and security analysis is crucial in confronting the entire risk spectrum of modern automotive systems. This integrated methodology is advantageous for identifying and mitigating risks and essential for sustaining consumer confidence and assuring the enduring success of automotive technologies [5].

C. Benefits and Challenges Associated with HATARA

The Integrated HATARA (Hazard Analysis and Threat Assessment Risk Analysis) Methodology presents numerous advantages and challenges in its application.

1) Advantages of the Integrated HATARA Methodology:

- Comprehensive Risk Assessment: The integrated HATARA framework allows for an extensive evaluation of risks, acknowledging the interactions between safety and security. This holistic perspective ensures that risks are appraised not in isolation but concerning their influence on the entire system [5].
- Increased Development Efficiency: The fusion of HARA and TARA streamlines the development process. This integration facilitates the concurrent consideration of safety and security, thereby diminishing the necessity for separate evaluations, leading to time and resource conservation [3].
- Enhanced System Dependability and Credibility: An integrated methodology augments the overall system's dependability. The system is fortified against a broad spectrum of potential failures and threats by concurrently addressing safety and security risks and elevating user confidence [1].

2) Challenges in Implementing the Integrated HATARA Methodology:

- Complexity in Methodological Alignment: The amalgamation of HARA and TARA necessitates synchronizing diverse methodologies and principles, a complex task. Each methodology encompasses distinct standards and procedures that require harmonization for efficacious integration [9].
- Requirement for Dual Domain Expertise: Executing an integrated approach demands expertise in both the safety and security domains. This dual proficiency is pivotal for effectively identifying and mitigating risks, yet it can be challenging to find within a single team or individual [10].
- Potential for Increased Initial Development Efforts: While the integrated approach may yield long-term efficiency gains, it may entail more intensive planning and analysis in the initial stages. Such augmented upfront efforts can pose challenges, especially regarding resource distribution and project scheduling [11].

The structure of the paper is methodically organized to facilitate a comprehensive understanding of its contents. Section II offers an in-depth background analysis, highlighting the pivotal aspects of ISO 26262 and ISO 21434 standards, delineating their differences, similarities, and the existing gaps between them. It elaborates on the significance of integrating these standards within the HATARA framework, addressing its relevance and the challenges it poses. Following this, Section

III details the HATARA methodology's proposed approach. Section IV applies this methodology to a case study focusing on Autonomous Vehicles (AVs) in both urban and highway settings, incorporating relevant research to support its implementation. A thorough discussion is presented in Section V, which critically examines the findings and implications of the study. The paper concludes with Section VI, which encapsulates the key conclusions drawn from the research, providing a closure to the discourse presented.

II. Background

A. Concepts and Definitions of HARA and TARA

1) Hazard Analysis and Risk Assessment (HARA): HARA constitutes a critical methodology within the automotive sector, focusing on identifying and evaluating safety hazards that might inflict harm on individuals, property, or the environment. This structured approach, delineated in the ISO 26262 standard, pertains to creating safety-relevant systems involving electrical, electronic, and software components. The identified risks are categorized by their Automotive Safety Integrity Level (ASIL), which is determined based on factors such as Controllability, Severity, and Exposure [3].

2) Threat Analysis and Risk Assessment (TARA): TARA represents a process dedicated to pinpointing and assessing cybersecurity threats that may impair the functionality, integrity, or accessibility of a system or its data. Integral to the ISO/SAE 21434 standard, TARA focuses on the management and scrutiny of electrical systems in road vehicles from a cybersecurity standpoint [12]

3) ISO 26262: ISO 26262 stands as a pivotal international standard, focusing on the functional safety of electrical and electronic systems in road vehicles. This standard addresses the hazards posed by malfunctions within these systems. It offers comprehensive guidelines and stipulations for functional safety, encompassing an automotive safety lifecycle, vital safety aspects of the development process, Automotive Safety Integrity Levels (ASILs), and stipulations for the validation and confirmation measures [13].

4) ISO 21434: ISO 21434, an international standard dedicated to cybersecurity engineering in road vehicles, establishes guidelines and requirements for executing TARA. It plays a crucial role in ensuring that cybersecurity considerations are interwoven throughout the vehicle's lifecycle [14].

This emergent standard is designed to confront future challenges in automotive cybersecurity. It underpins the development of automotive cybersecurity engineering across various facets: risk assessment management, product development, operational maintenance, and process audit. Central to this standard is establishing uniform terminology and methodologies for risk assessment in the cybersecurity domain. It concentrates on the cybersecurity risks associated with the design and engineering of vehicular electronics. Table I represents the key features of both ISO 26262 and ISO 21434 standards.

5) Similarities between HARA and TARA:

- Both HARA and TARA employ methodical and structured methodologies.
- These approaches include identifying, analyzing, and mitigating risks.
- They necessitate documenting and reviewing results and procedures [17].

6) Differences between HARA and TARA:

- HARA concentrates on safety hazards that may cause physical injury or damage. In contrast, TARA is oriented towards cybersecurity threats that might result in loss of control, privacy intrusions, or data corruption.
- For risk assessment, HARA applies metrics such as severity and probability; contrastingly, TARA utilizes impact and likelihood as its metrics.
- They often differ in their respective sources, targets, and agents of risk [18].

7) Gaps and Limitations:

- Typically, HARA and TARA are conducted independently, which may lead to potential inconsistencies, duplications, or contradictions in their findings.
- There may be a need for more comprehensive coverage regarding the interactions and dependencies between safety and cybersecurity facets.
- HARA and TARA might need to sufficiently address the dynamic and changing nature of the operational environment and the threat landscape [19].

B. Purpose of the Integrated HATARA Framework

The rationale behind developing an integrated HATARA (Hazard Analysis and Threat Analysis Risk Assessment) framework stems from contemporary vehicles' escalating intricacy and interconnectivity. This framework addresses automotive systems' safety (HARA) and security (TARA) aspects. The fundamental objective of the HATARA framework is to refine and streamline the risk assessment process. Amalgamating HARA and TARA diminishes redundant efforts, thereby enhancing the efficiency and efficacy of risk management within the automotive industry [18]. HATARA also aims to guarantee uniformity and comprehensiveness in analysis outcomes. It recognizes and addresses the interdependencies between safety and security risks, ensuring that mitigation strategies for one domain do not inadvertently engender new risks in the other [20]. Table II illustrates the integration of features from both ISO 26262 and ISO 21434 standards, showcasing how they interrelate and support each other in the overarching framework.

Integrating ISO 26262 (focusing on functional safety) and ISO 21434 (concentrating on cybersecurity) involves a series of steps:

1) Understanding the Scope: Recognize that ISO 26262 deals with hazards arising from malfunctions in electronic and electrical systems in vehicles. At the same time, ISO 21434 is concerned with cybersecurity risks in designing and developing car electronics.
2) Leveraging Similarities: Both standards offer frameworks for the lifecycle of automotive electronic and electrical safety-related systems and adopt a risk-based approach for determining risk classes, along with validation and

TABLE I
KEY FEATURES OF ISO 26262 AND ISO 21434 [15], [16]

Key Features	ISO 26262	ISO 21434
Scope	Addresses potential hazards caused by malfunctions in electronic and electrical systems in vehicles	Addresses the cybersecurity risks inherent in the design and development of car electronics
Lifecycle Framework	Provides a framework for the entire lifecycle of automotive electronic and electrical safety-related systems	Provides a framework for the entire lifecycle of automotive electronic and electrical safety-related systems
Risk-Based Approach	Has a risk-based approach for determining risk classes	Has a risk-based approach for determining risk classes
Validation and Confirmation Measures	Provides requirements for validation and confirmation measures	Provides requirements for validation and confirmation measures
Functional Safety vs Cybersecurity	Focuses on functional safety	Focuses on cybersecurity
Gap Filling	-	Addresses the cybersecurity risks inherent in the design and development of car electronics
Detailed Guidelines and Requirements for Functional Safety	Provides a set of detailed guidelines and requirements for functional safety	-
Automotive Cybersecurity Engineering	-	Provides a framework for automotive cybersecurity engineering
Standard Terminology and Methods for Risk Assessment in the Field of Cybersecurity	-	Establishes a common terminology and methods for risk assessment in the field of cybersecurity

TABLE II
FEATURES OF INTEGRATED HATARA: FUSION OF ISO 26262 AND ISO 21434 [15], [16]

Key Features/Attributes	ISO 26262	ISO 21434	Integrated HATARA
Addresses potential hazards caused by malfunctions in electronic and electrical systems in vehicles	✓	×	Develop a unified safety policy that addresses both functional safety and cybersecurity risks
Addresses the cybersecurity risks inherent in the design and development of car electronics	×	✓	Develop a unified safety policy that addresses both functional safety and cybersecurity risks
Provides a framework for the entire lifecycle of automotive electronic and electrical safety-related systems	✓	✓	Implement a unified lifecycle framework that incorporates both safety and security considerations at each stage of the lifecycle
Has a risk-based approach for determining risk classes	✓	✓	Develop a unified risk assessment process that considers both safety and security risks
Provides requirements for validation and confirmation measures	✓	✓	Implement a unified validation and confirmation process that verifies safety and security requirements
Focuses on functional safety	✓	×	Ensure that both safety and security are considered in all activities
Focuses on cybersecurity	×	✓	Ensure that both safety and security are considered in all activities
Addresses the cybersecurity risks inherent in the design and development of car electronics	×	✓	Implement a process for identifying and addressing gaps in safety and security
Provides a set of detailed guidelines and requirements for functional safety	✓	×	Develop a unified set of guidelines and requirements addressing functional safety and cybersecurity
Provides a framework for automotive cybersecurity engineering	×	✓	Develop a unified set of guidelines and requirements addressing functional safety and cybersecurity
Establishes a common terminology and methods for risk assessment in the field of cybersecurity	×	✓	Establish a common terminology and methods for risk assessment in the field of both functional safety and cybersecurity

confirmation measures. These commonalities can be utilized to forge a unified approach.

3) Addressing Differences: Acknowledge that ISO 26262 is dedicated to functional safety, whereas ISO 21434 focuses on cybersecurity. These differences should be reconciled to afford equal importance to operational safety and cybersecurity.
4) Filling the Gaps: ISO 21434 complements ISO 26262 by addressing cybersecurity risks, a dimension not covered by ISO 26262. This complementary nature should be integral to the integration process.
5) Developing a Unified Approach: Formulate a cohesive strategy for functional safety and cybersecurity, understanding that cybersecurity is an extension of safety rather than an isolated discipline.
6) Continuous Improvement: Persistently enhance and update the integrated approach as both standards evolve and new challenges and risks emerge.

The objective is to ensure that automotive products and vehicles are compliant and ready for the market, balancing cybersecurity and functional safety. This endeavor requires an appreciation of the interconnectedness of these two standards, recognizing them as complementary facets of automotive systems' safety and security.

C. Overview and Contributions

The HATARA methodology is meticulously delineated showcasing its implementation in the case of an autonomous vehicle. This illustration is a practical testament to its applicability and effectiveness within the automotive sector. A

primary contribution of this study is introducing an innovative, all-encompassing method for amalgamating safety and security risk assessments. This approach fills the prevailing void in automotive system development, where safety and security have traditionally been addressed in isolation [21]. Furthermore, the study offers guidance and suggestions for future research endeavors, pointing towards potential avenues for advancing and refining integrated safety and security frameworks.

D. Importance and Challenges

1) In-Depth Evaluation of the Present Approaches: The research critically examines existing practices in automotive safety and security, underscoring the necessity of an integrated methodology in response to the dynamic evolution of automotive technologies and threats.

2) Recognition of Deficiencies in Current Strategies: It acknowledges the shortcomings of current methods, notably the absence of a cohesive framework that concurrently caters to safety and security aspects in automotive systems [22].

3) Innovations and Contributions Rendered by HATARA: The HATARA model introduces significant advancements in risk assessment practices by integrating safety and security analyses. This integrated approach not only bolsters risk management effectiveness but also aids in fostering more resilient automotive systems.

The integrated HATARA framework fulfills the critical need for a unified approach towards safety and security in the automotive industry. It surpasses existing methodologies and offers insightful perspectives for future innovations in this evolving field.

III. Methodology

A. Integrated HATARA Process

The HATARA Methodology represents an innovative approach that amalgamates Hazard Analysis and Risk Assessment (HARA) with Threat Analysis and Risk Assessment (TARA). This methodology is designed to conduct exhaustive safety and security analyses for systems, products, or processes in the automotive industry.

B. Steps of the HATARA Method

1) Defining System and Context: The initial phase involves determining the system's scope, goals, and limitations, encompassing its environment and operational scenarios [23].
2) Identification of Hazards and Threats: This step entails systematically identifying potential safety hazards and cybersecurity threats that might impact the system [24].
3) Risk Analysis: In this phase, the risks associated with the identified hazards and threats are evaluated, considering their severity, likelihood, and potential consequences [25].
4) Implementation of Mitigation Strategies: This involves developing and executing strategies to reduce or eliminate the identified risks [26].
5) Documentation and Monitoring: The process, outcomes, and actions implemented are thoroughly documented, with ongoing monitoring for new risks [27].
6) Review and Update: The risk assessment is periodically reviewed and updated to reflect any system or environment changes [17].

The HATARA Methodology thus provides a structured and comprehensive framework for addressing safety and security in the automotive sector, ensuring continuous improvement and adaptation to evolving risks.

C. Input and Output Tools and Benefits of the Integrated HATARA Process

1) Inputs: The process commences with gathering system specifications, operational scenarios, and relevant standards and regulations. These inputs form the foundational basis for the HATARA methodology.
2) Outputs: This methodology's outputs include identifying hazards and threats, thorough risk assessments, formulation of mitigation measures, and comprehensive analysis reports.
3) Tools Utilized in HATARA: A variety of tools can support the HATARA method. These tools encompass techniques for hazard and threat identification, risk assessment methodologies, and risk mitigation strategies.
4) Benefits of the HATARA Approach: The HATARA methodology addresses the limitations and gaps present in existing methods by providing a cohesive framework that simultaneously considers both safety and security aspects. It ensures that the analysis results are consistent and complete, thereby aiding in the decision-making and implementation processes in the development of automotive systems.

The integrated HATARA process significantly advances automotive safety and security. It presents a comprehensive and systematic approach to effectively managing modern vehicles' intricate and interconnected risks.

D. Integrated HATARA Process

1) Conceptual Framework:

- Development of a Unified Model: Creating a unified model is a critical step, integrating the principles of HARA and TARA to form a comprehensive framework. This model methodically covers safety hazards and cybersecurity threats in the automotive sector, ensuring a holistic approach to system risk management [28].
- Construction of a Flowchart: A flowchart that outlines the HATARA methodology's steps and interactions visually represents the sequence. It begins with identifying hazards and threats and culminates in implementing mitigation strategies [29].

2) Identification of Scope:

- Determining System Boundaries: Defining the system's boundaries for analysis is essential, encompassing an understanding of its operational environment and interactions with external factors [23].

Fig. 1. Process flow methodology implementation for Integrated HATARA Approach

- Criteria for Hazard and Threat Identification: Establishing specific criteria for hazard and threat identification is vital. This ensures the analysis is targeted and relevant and effectively identifies potential safety and security risks [30].

3) Data Collection:

- Gathering Data: Collecting pertinent data on potential hazards and threats involves consulting expert opinions, examining historical data, utilizing predictive models, and tapping into industry-specific knowledge bases [18].
- Utilizing Various Information Sources: Employing a range of sources, such as incident reports, simulation outcomes, and industry trends, is crucial for an exhaustive and accurate data collection process.

4) Risk Analysis:

- Severity and Likelihood Evaluation: The process involves a detailed assessment of the severity and likelihood of the identified hazards and threats. This evaluation can be conducted through quantitative tools like risk matrices or qualitative methods, including expert opinions [20].
- Employing Varied Risk Assessment Techniques: Using diverse risk assessment methods is instrumental in gauging the potential impacts of the identified risks on the automotive system.

5) Integration of Findings:

- Cross-referencing Hazards and Threats: Identifying potential overlaps or interdependencies between hazards and threats is vital, as this step is critical to a thorough risk assessment. This identification aids in comprehending the intricate relationship between safety and security risks [31].
- Prioritization of Risks: Post-integration, risks are prioritized based on the assessment outcomes, which directs the focus toward the most critical areas for mitigation strategies.

6) Mitigation Strategy Development:

- Formulating Comprehensive Strategies: The development of mitigation strategies encompasses considerations of system design, operational procedures, and emergency response plans, ensuring both safety and security risks are addressed [22].
- Maintaining a Balanced Approach: It is crucial to ensure that the mitigation strategies are balanced, safeguarding against compromising one system aspect (safety or security) for the other.

7) Documentation and Reporting: In the HATARA process, meticulous documentation and comprehensive reporting are pivotal for ensuring transparency and accountability across the risk assessment and mitigation stages.

- Process Documentation: Documenting each phase of the HATARA method is critical. This documentation details the methodologies employed, data gathered, decisions made, and the reasoning behind each decision. Such thorough documentation is instrumental in establishing a transparent, traceable record of the risk assessment and mitigation strategies, aiding in internal reviews and external audits [25].
- Reporting: The preparation of exhaustive reports is essential in summarizing the outcomes of the risk assessment and the implemented mitigation strategies. These reports should delineate the identified risks, their potential impacts, the measures taken for mitigation, and any remaining risks. They act as a critical communication medium

for stakeholders, offering insights into the efficacy of the risk management process [32].

8) Review and Continuous Improvement: The ethos of continuous improvement is integral to the HATARA process, ensuring the ongoing relevance and effectiveness of the risk assessment and mitigation strategies.

- Periodic Review Mechanisms: Instituting regular review mechanisms is crucial for maintaining the efficacy of the HATARA method. These reviews should evaluate the current risk landscape and the effectiveness of existing mitigation strategies and identify any necessary adjustments. Reviews should be conducted at predetermined intervals and respond to significant changes in the system or its operational context [33].
- Adaptation and Enhancement: The HATARA process should be adaptable and capable of integrating new information, emerging risks, and technological advancements. Continuous improvement efforts should refine risk assessment methodologies, update mitigation strategies, and bolster overall system resilience. This adaptive stance ensures that the HATARA process remains robust and efficacious amidst the evolving dynamics of automotive safety and security [34].

In essence, rigorous documentation and reporting play a crucial role in upholding the integrity and transparency of the HATARA process. Regular assessments and an ethos of continuous improvement are vital to ensure that the process stays aligned with contemporary safety and security standards in the automotive industry.

IV. Case Study: Autonomous Vehicle (AV) in Urban and Highway Environments

A. Defining System and Context

1) System Description: The Autonomous Vehicle (AV) being examined is an intricate ensemble of hardware and software geared for autonomous operation, eliminating the need for human driving input. It incorporates advanced technologies, including sensory apparatus like LIDAR, cameras, GPS, actuators, control systems, and communication modules. These elements synergize to facilitate autonomous navigation and decision-making in the AV [35].

2) Operational Context in Different Environments: In urban settings, the AV confronts complex maritime challenges such as managing intersections, pedestrian pathways, and diverse traffic conditions, necessitating sophisticated decision-making and environmental interpretation skills. Conversely, highway driving presents distinct challenges, including sustaining higher speeds, lane-keeping, and adapting to the driving behaviors of other vehicles. The AV must effectively interpret and respond to these multifaceted inputs to ensure safe functionality across these varied driving contexts [36].

The AV's proficiency in these environments hinges on its advanced sensory systems and intricate algorithms, which detect and respond aptly to many static and dynamic factors like vehicles, traffic signs, pedestrians, and diverse road conditions. In urban landscapes, the AV must navigate complex street designs, identify and react to pedestrian activities, and adjust to abrupt traffic variations. On highways, it faces challenges such as maintaining safe vehicular distances, executing lane shifts, and managing high-speed driving conditions.

The capability of AVs in these scenarios is further enhanced by their learning and adaptability to new situations, an aspect that is continuously advancing with technological progress. Research in this field is centered on refining the precision and dependability of autonomous systems, bolstering their competence in dealing with the unpredictable dynamics of real-world driving environments.

B. Identifying Hazards and Threats in Autonomous Vehicles

1) HARA (Safety Hazards):

- Hazard 1: Software Malfunction Leading to Speed Variability: A prominent risk in Autonomous Vehicles (AVs) is unintended acceleration or deceleration due to software errors. Such malfunctions can cause unexpected speed changes, increasing the risk of loss of control and potential accidents. Given the intricacy of AV software systems, addressing this hazard is vital in the development phase [37].
- Hazard 2: Obstacle Detection System Failure: The risk of the vehicle's failure to accurately detect and react to obstacles, such as other vehicles, pedestrians, or roadblocks, is a concern. This could be due to sensor malfunctions or algorithmic errors. Ensuring the reliability of sensor fusion and algorithms is crucial in mitigating this risk [38].

2) TARA (Cybersecurity Threats):

- Threat 1: Unauthorized Access via Wireless Interfaces: A critical cybersecurity threat is the possibility of hackers gaining access to the vehicle's control systems through wireless networks. This unauthorized access could lead to manipulation of the vehicle's operations. Securing wireless interfaces is essential in mitigating this threat [12].
- Threat 2: Sensor Data Manipulation: This threat involves external entities tampering with the vehicle's sensor data, leading to inaccurate environmental perception and incorrect vehicular responses. Maintaining the integrity and authenticity of sensor data is crucial to counteract this threat [1].

The process of identifying these hazards and threats is crucial in the development and deployment of Autonomous Vehicles. It requires a thorough understanding of the vehicle's operational capabilities and potential cybersecurity vulnerabilities. Effectively addressing these risks is fundamental to ensuring the safety and security of AVs across various driving contexts.

C. Analyze Risks

1) HARA (Safety Risks):

- Risk Analysis for Unintended Acceleration: Severity: High. Malfunctions leading to unintended acceleration can result in serious injuries or fatalities due to unpredictable vehicle behavior, posing a substantial risk to passengers and other road users.

- Probability: Low, provided the vehicle incorporates sophisticated software design and has been subjected to extensive testing protocols to mitigate such risks [37].
- Risk Analysis for Obstacle Detection Failure: Severity: High. Inadequacies in obstacle detection increase collision risk, significantly elevating safety hazards.
- Probability: Medium. The likelihood of this risk depends on the sensors' dependability and performance under various environmental conditions [38].

2) TARA (Cybersecurity Risks):

- Risk Analysis for Unauthorized Access: Impact: High. Unauthorized access can compromise vehicle control and privacy breaches, adversely affecting passenger safety and data security.
- Likelihood: Medium. While basic cybersecurity measures can moderate this risk, vulnerabilities still pose a considerable concern [12].
- Risk Analysis for Sensor Data Manipulation: Impact: High. Tampering with sensor data can distort the vehicle's decision-making, leading to incorrect and potentially hazardous actions.
- Likelihood: Low. These attacks typically require advanced techniques and are less frequent, though ongoing vigilance is essential given the evolving nature of cybersecurity threats [1].

The risk analysis encompassing safety and cybersecurity is crucial for assuring Autonomous Vehicles' overall dependability and safety. This comprehensive analysis not only aids in prioritizing risk mitigation efforts but also steers the development process toward strengthening AVs' safety and security features.

D. Risk Mitigation Strategies

1) HARA (Safety Mitigations):

- Implementation of Redundant Systems: Introducing backup systems for critical functionalities such as acceleration and braking is crucial. These redundant systems act as a safety net, taking over control to maintain vehicle safety in case of a primary system failure, thus diminishing the likelihood of accidents caused by unintended speed changes [37].
- Adoption of Multi-Sensor Fusion Techniques: Employing an integration of data from diverse sensors, including LIDAR, cameras, and radar, significantly bolsters the reliability and precision of obstacle detection. This method amalgamates inputs from various sources, providing a more detailed and accurate understanding of the vehicle's surroundings, thereby improving its ability to detect and react to obstacles [38].

2) TARA (Cybersecurity Mitigations):

- Robust Encryption and Secure Authentication: Strengthening all wireless communications with robust encryption and secure authentication protocols is essential to thwart unauthorized access. This protection extends to vehicle-to-vehicle and vehicle-to-infrastructure communications, ensuring only authorized entities can interact with the vehicle's systems [12].
- Advanced Anomaly Detection Systems: Implementing sophisticated systems to identify and address abnormal patterns or manipulations in sensor data is critical. These systems are designed to detect and counteract data integrity threats, guaranteeing the vehicle's operations are based on accurate and reliable sensor inputs. Machine learning and artificial intelligence techniques are increasingly employed for such anomaly detection [39].

Integrating these mitigation strategies across both safety and cybersecurity realms is pivotal in assuring Autonomous Vehicles' overall safety and dependability. This holistic approach to risk mitigation is vital in tackling the multifaceted and dynamic array of threats and vulnerabilities that modern AVs encounter.

E. Document and Monitor

1) Documentation:

- Comprehensive Risk Reporting: Creating an in-depth report that encapsulates all identified risks is fundamental. This document should encompass detailed evaluations of each risk, including their severity, probability, or likelihood, and the mitigation strategies implemented for safety and cybersecurity concerns.
- This documentation is a critical resource for stakeholders, offering a transparent and detailed account of the decision-making process and the justification for each chosen mitigation approach. It's not just crucial for current comprehension and implementation but also serves as a foundation for future system modifications or updates. Including all pertinent details ensures the process's replicability and auditability [40].

2) Monitoring:

- Ongoing System Surveillance: Setting up a perpetual monitoring system is crucial to verify the efficacy of the applied risk mitigation measures. This should involve routine evaluations of the system's performance to confirm that the risk mitigation strategies are operating effectively and to pinpoint potential areas for enhancement.
- Incorporating updates in response to technological progress or emerging threats is essential to sustain the system's resilience against novel and evolving risks. Monitoring should be a continual element of the system's lifecycle, adapting to new challenges and upholding the highest levels of safety and security. This proactive stance ensures that the system remains robust and equipped to manage the evolving nature of safety and cybersecurity threats in the automotive industry [41].

In summary, documenting and monitoring are integral components of the risk management framework in Autonomous Vehicles. These processes ensure that all undertaken measures are meticulously recorded and assessed for their effectiveness, facilitating necessary adaptations and enhancements to boost the overall safety and security of the system.

F. Review and Update

The continuous evaluation and refinement of both Hazard Analysis and Risk Assessment (HARA) and Threat Analysis

and Risk Assessment (TARA) are essential aspects of the lifecycle of an autonomous vehicle (AV) system. Regular review and updates are fundamental to ensure that the system remains effective and adaptable to changes in its operational environment, technological progress, and new threats.

- Systematic Review Process: Conducting thorough and periodic reviews is necessary to completely reevaluate safety hazards and cybersecurity threats. This process should involve reassessing the severity, probability, and impact of identified risks and the efficiency of the existing mitigation strategies. Such reviews are critical to ensure that risk assessments and mitigation plans remain congruent with the current state of the AV system and its operational context [5].
- Commitment to Continuous Improvement: Embracing a continuous improvement approach is crucial for upholding the safety and security integrity of the AV system over time. This approach entails modifying and enhancing the HARA and TARA processes based on new insights, technological advancements, and operational feedback. It ensures that the AV system complies with the latest safety and security standards while being equipped to face future challenges and risks [11].

By integrating Hazard and Risk Assessment (HARA) with Threat and Risk Assessment (TARA), AV development teams can adopt a comprehensive approach to system safety and security. This unified method not only pinpoints potential safety hazards and cybersecurity threats but also facilitates the deployment of extensive mitigation strategies. The amalgamation of HARA and TARA results in a more resilient and robust design of the AV, effectively managing the complex risks associated with automated systems. This strategy is indispensable for developing AVs that are not only technologically sophisticated but also dependable and secure in various operational scenarios.

G. Exploration of Integrated Safety and Cybersecurity in Automotive Systems

The current study by Martin et al. entitled 'In Search of Synergies in a Multi-Concern Development Lifecycle: Safety and Cybersecurity' embarks on an analytical journey exploring the interconnectedness of functional safety and cybersecurity within automotive system development [42] . This investigation is anchored in a case study focusing on a crucial component of automated driving systems. This component is pivotal, aligning with two essential standards: ISO 26262, pertaining to safety, and ISO/SAE 21434, relating to cybersecurity. The study not only delves into the specifics of this component but also offers a broader perspective on the complex interplay between safety and cybersecurity in the automotive domain.

1) Comparative Analysis of Development Methodologies: At the heart of this research is a comparative examination of two distinct methodologies in the automotive system lifecycle. One is an integrative approach, considering safety and security concurrently, contrasting sharply with a traditional, sequential method treating these aspects separately. This comparative analysis highlights the intricate nature of automotive system development, where safety and security are closely intertwined.

2) Insights from the Integrative Approach: Empirical findings highlight the integrative approach's benefits, notably in robust analysis and efficient reuse of testing resources. However, it reveals that the amalgamation of safety and security, especially in design and protective measures, has not fully matured. This gap indicates the partial integration of these domains in practical applications.

3) Positioning Component in Automated Driving: A Case Study: The study focuses on an embedded electronic system in the automotive sector, particularly a positioning component crucial for automated driving. Adherence to ISO 26262 and ISO/SAE 21434 is paramount. The study compares segregated and integrative development methodologies, revealing the integrative approach's superiority in verification and validation but noting its limited application in design phases.

4) Separate vs. Integrative Development Strategies: The traditional separate approach treats safety and security as isolated domains, while the integrative approach promotes concurrent consideration. This research section delves into the strengths and weaknesses of both strategies in automotive system development, highlighting the integrative approach's efficiency in verification and validation, yet its limited overlap in design phases.

5) The Multi-Concern Development Lifecycle: An Overview: This part introduces the Multi-Concern Development Lifecycle, guiding the creation of automotive systems with dual compliance to safety and security standards. Figure 2 depicts the life cycle processes for standard functionality, augmented with additional functional safety and cybersecurity activities.

The lifecycle comprises several phases:

- Concept Phase: Defining system requirements, including safety and security objectives, identifying the positioning component's functionality, and outlining hazards and threats.
- System Design Phase: Developing the system architecture to meet requirements, translating safety and security goals into technical specifications, with minimal overlap at this stage.
- Hardware/Software Design Phase: Detailing system design into hardware and software components, marked by limited safety-security interplay.
- Implementation Phase: Constructing the designs with often independent safety and security measures.
- Verification Phase: Testing the system for compliance, with the integrative approach showing superior effectiveness.
- Validation Phase: Validating the system against initial objectives, where the integrative method ensures comprehensive validation.
- Operation Phase: Continuous monitoring post-deployment, potentially revisiting previous phases for issue resolution.

6) Integrated Verification and Validation: In the realm of verification and validation, as expounded in this treatise, particularly on the right flank of the V-model, the scope

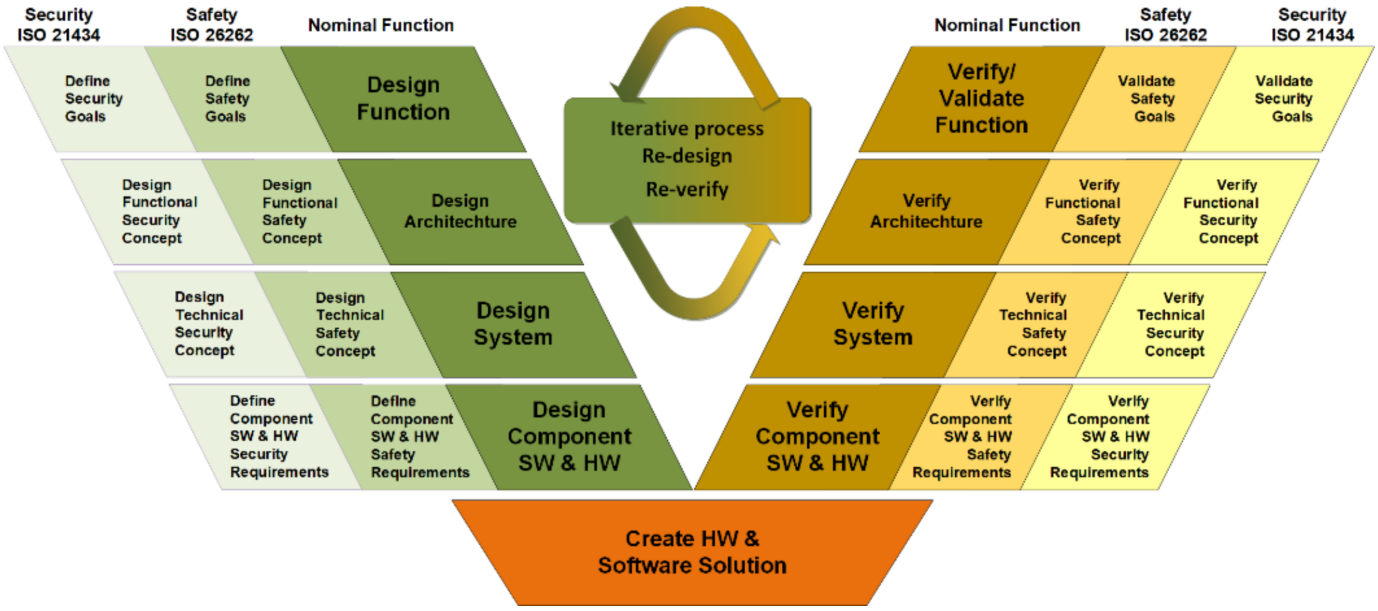

Fig. 2. Integration of Automotive Safety (ISO 26262) and Security (ISO/SAE 21434) in Co-engineering Approach [42]

for synergistic approaches is significantly amplified. This is particularly true for the use case under scrutiny. The synergies in question predominantly pertain to testing environments and methodologies employed for dual aspects. A pivotal observation is that the majority of testing mandated by prevailing standards is not exclusively oriented toward safety or cybersecurity. Instead, it is directed at ensuring overarching product quality. The primary divergence lies in the necessity to test specific safety or security mechanisms, which are ancillary to the nominal functioning of the product. Nevertheless, the methodologies for testing these mechanisms frequently overlap with those used for standard procedures.

Three principal domains that stand to gain from integrated engineering strategies have been identified on the right side of the composite development lifecycle. These domains encompass the testing environments, the objectives of each test within these environments, and the methodologies utilized to achieve these objectives, as depicted in Figure 3. The varying maturity stages of the implementation are examined using model-in-the-loop (MIL), software-in-the-loop (SIL), and hardware-in-the-loop (HIL) approaches.

As delineated in Figure 3, the test environments correspond to distinct levels of integration: component level (test environment 1), system/subsystem level (test environment 2), and complete vehicle level (test environments 3 and 4). These environments offer substantial advantages in terms of reusability across different testing criteria, namely nominal function, security, and safety. This reusability represents a significant benefit over creating, maintaining, and operating separate testing infrastructures. Furthermore, these environments are conducive to regression testing, essential for continuous deployment, and critical for maintaining security standards. Additionally, they facilitate back-to-back testing in scenarios employing model-driven development. Figure 3 further elucidates the objectives of these tests, which can be categorized as follows:

- Assurance of Specification Implementation Accuracy
- Robustness
- Consistency and Correct Implementation of Interfaces
- Functional Performance, Precision, and Timing
- Effectiveness of Mechanisms

These categories aim to identify systematic faults at various integration levels. In the context of the case study addressed in this paper, all the test objectives, barring the effectiveness of mechanisms, exhibit substantial overlap across the different concerns. This aspect dramatically facilitates the process of co-verification for both test environments and objectives. It is noteworthy, however, that the overlap in the "effectiveness of mechanisms" category is contingent upon factors such as tester competence and the nature of the mechanisms employed. Prior research indicates that safety mechanisms can positively and negatively affect system security. Parallel findings are reported regarding the influence of security mechanisms on system safety. Consequently, even in the domain of "effectiveness of mechanisms," the degree of overlap can be enhanced by elevating the proficiency of testers and selecting mechanisms that simultaneously bolster safety and security, wherever feasible.

The paper concludes by underlining the integrative approach's efficacy in reducing oversight risks and enhancing system assurance. However, it acknowledges the limited intersection of safety and security in design and countermeasures. This highlights the need for a nuanced approach recognizing their distinct yet interconnected nature in automotive system development.

V. Discussion

A. Strengths of HATARA

1) Comprehensive and Integrated Approach: HATARA distinguishes itself as an all-encompassing and integrated method that concurrently addresses safety and cybersecurity aspects of systems, products, or processes. By amalgamating Hazard

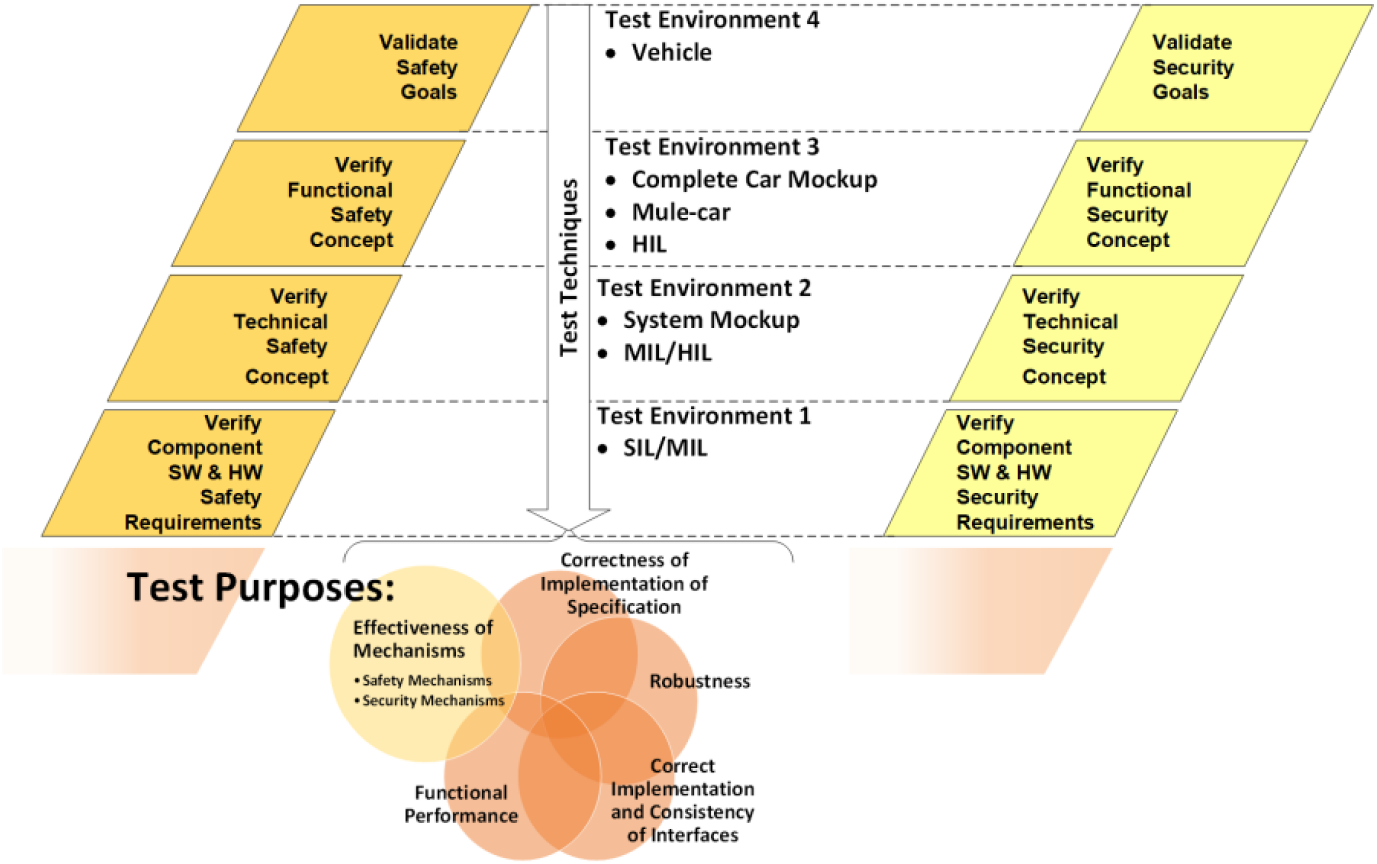

Fig. 3. Overview of Testing Techniques and Objectives Across Various Integration Levels and Environments [42]

Analysis and Risk Assessment (HARA) with Threat Analysis and Risk Assessment (TARA), HATARA offers a holistic perspective on potential hazards and threats, a critical aspect in the realm of complex systems such as Autonomous Vehicles (AVs) [43].

2) Enhancement of Mitigation Strategies: The fusion of safety and cybersecurity within the HATARA framework significantly aids in identifying and implementing robust mitigation strategies. This integrated approach ensures comprehensive consideration and handling of all potential risks, bolstering the overall safety and security of the system [44].

3) Efficiency in the Analysis Process: HATARA enhances the efficiency and coherence of the risk analysis process by reducing redundant and inconsistent efforts. Integrating HARA and TARA eliminates the need to conduct separate assessments, streamlining the process. This integrated methodology ensures that safety and security are viewed in isolation and as interrelated components of a unified framework [10].

The efficacy of the HATARA method lies in its capacity to deliver a comprehensive and integrated analysis of both safety and cybersecurity risks. By addressing these elements concurrently, HATARA empowers the development of systems, particularly in complex domains like autonomous vehicles, to be technologically sophisticated and resilient against a wide range of inherent risks. Such an approach is imperative for ensuring modern automated systems are safe, secure, and reliable.

B. Weaknesses of HATARA

1) Complexity and Requirement for Specialized Expertise: The intricate nature of HATARA and the need for high-level expertise present significant challenges. Implementing this integrated approach, which encompasses safety and cybersecurity, requires collaboration among diverse experts such as engineers, cybersecurity specialists, and safety professionals. This complexity necessitates specialized knowledge and expertise, which can be a hurdle for some organizations [43].

2) Potential for Trade-offs and Conflicts: The merging of safety and cybersecurity objectives within HATARA may lead to potential trade-offs or conflicts, especially concerning performance, cost, and usability. Achieving a balance between these sometimes competing objectives can be challenging, as enhancements in one aspect might entail compromises in another [10].

3) Limitations in Applicability: HATARA may not universally apply across all systems, products, or processes. Its suitability is contingent on the particular traits and needs of the system in question. In simpler systems or those with minimal integration between safety and cybersecurity, the complexity entailed in HATARA may not be warranted [45].

The identified weaknesses of HATARA underscore the necessity of meticulous consideration and strategic planning

in its adoption. Although it provides extensive advantages, the intricacy of HATARA and the potential for trade-offs and conflicts call for a reasonable and well-considered approach to ensure its effective application in appropriate systems.

C. Implications and Challenges of HATARA

1) Impact on System Development and Operation: HATARA significantly influences the development and operation of systems, especially those encompassing safety and cybersecurity. It necessitates a precise definition of the system and context to ensure a thorough understanding and address of all potential hazards and threats. Meticulous identification and assessment of hazards and threats are imperative for managing risks in complex systems like Autonomous Vehicles (AVs) [43].

2) Consistency and Effectiveness in Risk Mitigation: The consistent and effective implementation and monitoring of mitigation strategies are vital aspects of HATARA. It contributes to the streamlining of these processes. It ensures that safety and cybersecurity measures are well-integrated, continually monitored, and updated in response to changes in operational environments and technological advancements [10].

3) Challenges Associated with HATARA:

- Data and Information Quality: The effectiveness of HATARA is contingent on the availability and quality of data and information. Accurate and current data are essential for precise risk assessments, particularly in dynamic settings such as those encountered by AVs [45].
- Integration and Compatibility of Tools and Methods: Integrating diverse tools and methodologies required for HATARA poses challenges, especially in complex systems that demand various safety and security measures [44].
- Stakeholder Communication and Alignment: Another significant challenge is to achieve alignment and effective communication among various stakeholders, including safety engineers, cybersecurity experts, system designers, and operational personnel. This involves reconciling differing perspectives and objectives [46].

The implications and challenges of HATARA underscore the necessity for extensive planning, coordination, and collaboration among all parties involved in systems with integrated safety and cybersecurity features. Despite these challenges, HATARA is crucial in ensuring complex systems' comprehensive safety and security, particularly in fields where safety and security are deeply interconnected, such as in developing autonomous vehicles.

D. Suggestions for Future Work and Improvement of HATARA

1) Development of a Standardized Framework: Future initiatives in HATARA should focus on creating and validating a standardized, adaptable framework. This would entail establishing a universally applicable methodology, especially in safety-critical fields like automotive and aerospace. A standardized approach would promote more comprehensive implementation and ensure uniformity in HATARA's application across different systems, products, or processes [43].

2) Evaluation and Benchmarking: It is essential to evaluate and compare HATARA with other existing and emerging methodologies to gauge its efficacy and efficiency. Benchmarking HATARA against conventional risk assessment methods will highlight its strengths and pinpoint areas for enhancement, offering insights into its advantages over current practices [44].

3) Incorporation of Emerging Technologies: Integrating cutting-edge technologies and techniques, such as artificial intelligence, machine learning, and advanced analytics, could significantly augment HATARA's efficiency and effectiveness. These technologies hold promise for automating segments of the risk assessment process and providing more advanced analysis capabilities [47].

4) Conducting Case Studies and Empirical Research: Undertaking more case studies and gathering empirical evidence is crucial to illustrate HATARA's practical benefits and constraints. Applying HATARA in varied contexts and documenting its influence on system safety and security will offer valuable insights. Such case studies are instrumental in providing feedback and guidelines for the ongoing refinement and optimization of the HATARA process [48].

Future research and enhancements in HATARA are imperative for its continued development and efficacy in addressing the growing complexity of safety and cybersecurity challenges in contemporary systems. By focusing on these critical areas, HATARA can be further refined and adapted to meet the diverse requirements of various industries and applications.

VI. Conclusion

The article introduces HATARA, a novel methodology integrating Hazard Analysis and Risk Assessment (HARA) with Threat Analysis and Risk Assessment (TARA) for automotive systems. This integrated approach aims to enhance the identification, evaluation, and mitigation of safety and security risks, promoting a more comprehensive understanding of potential hazards and threats. It underscores the importance of addressing both safety and security in a unified framework to ensure the development of robust automotive systems. The methodology is presented as a step forward in managing the complexity of modern vehicle systems, highlighting its potential to improve system resilience against diverse risks. The detailed case study is delineates a comprehensive overview and implementation of the proposed HATARA approach.

This approach marks notable progress in the domains of safety and security engineering. HATARA extends beyond conventional methods by concurrently addressing both safety hazards and cybersecurity threats. It explores the complex interplay between these areas, ensuring an all-encompassing analysis. Central to HATARA is its integrated framework, which supports informed decision-making. This framework is critical in formulating robust risk mitigation strategies that address safety and security issues, improving the clarity and effectiveness of the risk assessment process. HATARA's dual emphasis on safety and security enables more precise identification and mitigation of risks. This is especially important in systems where the overlap of safety and security is significant, and overlooking one could introduce substantial risks.

HATARA contributes significantly to advancing safety and security engineering, merging these two critical fields into a unified risk assessment approach and establishing new standards for integrated methodologies. HATARA's utility spans multiple sectors, demonstrating its versatility. In the automotive industry, it ensures the integrity of sophisticated vehicular systems. For aerospace, it offers protection for intricate flight control mechanisms. The healthcare field can apply HATARA to secure delicate medical devices and systems, highlighting its wide-ranging applicability.

HATARA approach represents a significant leap forward in merging safety and security evaluations. Its comprehensive, unified strategy and its potential for widespread application across different sectors underscore its importance as a foundational element in advancing safety and security protocols industry-wide.

REFERENCES

[1] F. Luo, Y. Jiang, Z. Zhang, Y. Ren, and S. Hou, "Threat Analysis and Risk Assessment for Connected Vehicles: A Survey," *Secur. Commun. Networks*, vol. 2021, pp. 12 638 201–126 382 019, 2021. [Online]. Available: https://consensus.app/papers/threat-analysis-risk-assessment-connected-vehicles-luo/f18ce79fa9bd59b480b9d3c094e20aba/

[2] Y. Tian, J. Li, and X. Huang, "Integrated risk analysis of function safety and cyber security on I&C system of HTP-PM with STPA-SafeSec," in *International conference on nuclear engineering*, vol. 86397. American Society of Mechanical Engineers, 2022, p. V005T05A057.

[3] A. Barreto and Z. Bachir, "SAHARA: SIMULATION AIDED HAZARD ANALYSIS AND RISK ASSESSMENT METHODOLOGY," *WIT transactions on engineering sciences*, vol. 129, pp. 41–53, 2020. [Online]. Available: https://consensus.app/papers/sahara-simulation-aided-hazard-analysis-risk-assessment-barreto/dda0cbcd701457e49ba617277b789906/

[4] E.-Y. Kang and S. Hacks, "Safety & Security Analysis of a Manufacturing System using Formal Verification and Attack-Simulation," in *2023 12th Mediterranean Conference on Embedded Computing (MECO)*. IEEE, 2023, pp. 1–8. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10154960/

[5] M. Khatun, M. Glass, and R. Jung, "An Approach of Scenario-Based Threat Analysis and Risk Assessment Over-the-Air updates for an Autonomous Vehicle," *2021 7th International Conference on Automation, Robotics and Applications (ICARA)*, pp. 122–127, 2021. [Online]. Available: https://consensus.app/papers/approach-scenariobased-threat-analysis-risk-assessment-khatun/896cedf347ba5e91a4112b0e5d1f4f58/

[6] T. Witte, R. Groner, A. Raschke, M. Tichy, I. Pekaric, and M. Felderer, "Towards model co-evolution across self-adaptation steps for combined safety and security analysis," in *Proceedings of the 17th Symposium on Software Engineering for Adaptive and Self-Managing Systems*. Pittsburgh Pennsylvania: ACM, May 2022, pp. 106–112. [Online]. Available: https://dl.acm.org/doi/10.1145/3524844.3528062

[7] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner, "SAHARA: A security-aware hazard and risk analysis method," in *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Mar. 2015, pp. 621–624, iSSN: 1558-1101. [Online]. Available: https://ieeexplore.ieee.org/document/7092463

[8] A. Bolovinou, U.-I. Atmaca, A. T. Sheik, O. Ur-Rehman, G. Wallraf, and A. Amditis, "TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems," in *2019 IEEE Intelligent Vehicles Symposium (IV)*, Jun. 2019, pp. 8–13, iSSN: 2642-7214. [Online]. Available: https://ieeexplore.ieee.org/document/8813999

[9] P. Bhosale, W. Kastner, and T. Sauter, "Automating Safety and Security Risk Assessment in Industrial Control Systems: Challenges and Constraints," *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1–4, 2022. [Online]. Available: https://consensus.app/papers/automating-safety-security-risk-assessment-industrial-bhosale/cad0a8ad055853b2890cbdc2cb503238/

[10] A. Cormier and C. Ng, "Integrating cybersecurity in hazard and risk analyses," *Journal of Loss Prevention in The Process Industries*, vol. 64, 2020. [Online]. Available: https://consensus.app/papers/integrating-cybersecurity-hazard-risk-analyses-cormier/a290a2965c6156c5ad39f49fd0494ce8/

[11] A. Patel and P. Liggesmeyer, "Machine Learning Based Dynamic Risk Assessment for Autonomous Vehicles," *2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC)*, pp. 73–77, 2021. [Online]. Available: https://consensus.app/papers/machine-learning-based-dynamic-risk-assessment-patel/96fe81813ae052d291b3bd646ebed182/

[12] Y. Kawanishi, H. Nishihara, H. Yoshida, H. Yamamoto, and H. Inoue, "A Study on Threat Analysis and Risk Assessment Based on the "Asset Container" Method and CWSS," *IEEE Access*, vol. 11, pp. 18 148–18 156, 2023. [Online]. Available: https://consensus.app/papers/study-threat-analysis-risk-assessment-based-asset-kawanishi/51cdf0a07a5f5aa4a567283269535517/

[13] P. Mydlowski and S. Moskwa, "New approach to functional safety work products for advanced automotive projects," *2022 26th International Conference on Methods and Models in Automation and Robotics (MMAR)*, pp. 342–345, 2022. [Online]. Available: https://consensus.app/papers/approach-safety-work-products-advanced-projects-mydlowski/0d7f4b9a795f52b9821062db5b294208/

[14] G. Costantino, M. Vincenzi, and I. Matteucci, "In-Depth Exploration of ISO/SAE 21434 and Its Correlations with Existing Standards," *IEEE Communications Standards Magazine*, vol. 6, pp. 84–92, 2022. [Online]. Available: https://consensus.app/papers/indepth-exploration-isosae-21434-correlations-existing-costantino/cfe9a03e0aa750bab9546f3d112e49d0/

[15] I. ISO, "26262: 2018: Road vehicles—Functional safety," *British Standards Institute*, vol. 12, 2018.

[16] ISO/SAE, "ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering," *ISO*. [Online]. Available: https://www.iso.org/standard/70918.html

[17] D. Püllen, N. Anagnostopoulos, T. Arul, and S. Katzenbeisser, "Safety Meets Security: Using IEC 62443 for a Highly Automated Road Vehicle," pp. 325–340, 2020. [Online]. Available: https://consensus.app/papers/safety-meets-security-using-62443-highly-automated-road-p%C3%BCllen/9dfe73d13d675ad0a2c300ef1e0d782a/

[18] J. Dobaj, D. Ekert, J. Stolfa, S. Stolfa, G. Macher, and R. Messnarz, "Cybersecurity Threat Analysis, Risk Assessment and Design Patterns for Automotive Networked Embedded Systems: A Case Study," *J. Univers. Comput. Sci.*, vol. 27, pp. 830–849, 2021. [Online]. Available: https://consensus.app/papers/cybersecurity-threat-analysis-risk-assessment-design-dobaj/d9594060fb4a5fc383115089f8983eb5/

[19] M. Ebrahimi, C. Striessnig, J. C. Triginer, and C. Schmittner, "Identification and Verification of Attack-Tree Threat Models in Connected Vehicles," *ArXiv*, vol. abs/2212.14435, 2022. [Online]. Available: https://consensus.app/papers/identification-verification-attacktree-threat-models-ebrahimi/5d258b61258c566eacaef753eb0d90a0/

[20] T. K. Hema, "Integrated Automotive Software Quality Management System in compliance with Automotive SPICE, ISO 26262, ISO 21448 and ISO 21434 Standards," *International Journal of Scientific and Research Publications (IJSRP)*, 2022. [Online]. Available: https://consensus.app/papers/integrated-automotive-software-quality-management-hema/1c9c8af78fd55302a3c121724a1786f3/

[21] G. Macher, E. Armengaud, C. Kreiner, E. Brenner, C. Schmittner, Z. Ma, H. Martin, and M. Krammer, "Integration of Security in the Development Lifecycle of Dependable Automotive CPS," *Research Anthology on Artificial Intelligence Applications in Security*, 2021. [Online]. Available: https://consensus.app/papers/integration-security-development-lifecycle-dependable-macher/932a6d7ffd6255dfb0f7b42b9519614b/

[22] A. Buczacki and P. Piatek, "Proposal for an Integrated Framework for Electronic Control Unit Design in the Automotive Industry," *Energies*, 2021. [Online]. Available: https://consensus.app/papers/proposal-integrated-framework-electronic-control-unit-buczacki/d3f99daf95665145adbea8b8c77577c5/

[23] M. Quamara, G. Pedroza, and B. Hamid, "Facilitating Safety and Security Co-design and Formal Analysis in Multi-layered System Modeling," *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, pp. 1–8, 2022. [Online]. Available: https://consensus.app/papers/facilitating-safety-security-codesign-formal-analysis-quamara/8142352c42145d19854a5926f5469008/

[24] M. Fockel, D. Schubert, R. Trentinaglia, H. Schulz, and W. Kirmair, "Semi-automatic Integrated Safety and Security Analysis for Automotive Systems," pp. 147–154, 2022. [Online]. Available: https://consensus.app/papers/integrated-safety-security-analysis-automotive-systems-fockel/ef9b1ae4d0ef5fd187666ee12d981a34/

[25] M. Saulaiman, M. Kozlovszky, Csilling, A. Bánáti, and A. Benhamida, "Overview of Attack Graph Generation For Automotive Systems," *2022 IEEE 10th Jubilee International Conference on Computational Cybernetics and Cyber-Medical Systems (ICCC)*, pp. 000 135–000 142, 2022. [Online]. Available: https://consensus.app/papers/overview-attack-graph-generation-automotive-systems-saulaiman/20a33f04f676527490f9bac8103e0ee4/

[26] A. Cimatti, S. Corfini, L. Cristoforetti, M. Natale, A. Griggio, S. Puri, and S. Tonetta, "A comprehensive framework for the analysis of automotive systems," *Proceedings of the 25th International Conference on Model Driven Engineering Languages and Systems*, 2022. [Online]. Available: https://consensus.app/papers/framework-analysis-systems-cimatti/1693fa8841ef54b89a6ed9666165d6ce/

[27] I. Koley, S. Dey, D. Mukhopadhyay, S. K. Singh, L. Lokesh, and S. V. Ghotgalkar, "CAD support for Security and Robustness Analysis of Safety-Critical Automotive Software," *ACM Transactions on Cyber-Physical Systems*, 2022. [Online]. Available: https://consensus.app/papers/support-security-robustness-analysis-safetycritical-koley/1cdead2b56f75f5e9d15e4c0ce3d5fb4/

[28] G. Gondhalekar, B. Ashreeth, G. R. Thellaputta, D. Venkataramireddy, M. Sumithra, and N. Karyemsetty, "A Safety Assessment Model for Automotive Embedded Systems Networks," in *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)*, Oct. 2022, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/9972628

[29] T. Syamsundararao, B. Samatha, P. K. Pinjala, and N. Karyemsetty, "A Model for the Safety Risk Evaluation of Connected Car Network," *Review of Computer Engineering Research*, 2022. [Online]. Available: https://consensus.app/papers/model-safety-risk-evaluation-connected-network-syamsundararao/c1e9ce59bac651df84ec5b660145bc5e/

[30] T. Brandt and T. Tamisier, "The future connected car – safely developed thanks to UNECE WP.29?" in *21. Internationales stuttgarter symposium*, M. Bargende, H.-C. Reuss, and A. Wagner, Eds. Wiesbaden: Springer Fachmedien Wiesbaden, 2021, pp. 461–473.

[31] Török and Z. Pethő, "Introducing safety and security co-engineering related research orientations in the field of automotive security," *Periodica Polytechnica Transportation Engineering*, vol. 48, pp. 349–356, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:225372819

[32] M. Hamad and V. Prevelakis, "SAVTA: A hybrid vehicular threat model: Overview and case study," *Information-an International Interdisciplinary Journal*, vol. 11, no. 5, 2020, number: 273. [Online]. Available: https://www.mdpi.com/2078-2489/11/5/273

[33] M. Khosravi-Farmad and A. Ghaemi-Bafghi, "Bayesian Decision Network-Based Security Risk Management Framework," *Journal of Network and Systems Management*, vol. 28, no. 4, pp. 1794–1819, Oct. 2020. [Online]. Available: https://doi.org/10.1007/s10922-020-09558-5

[34] M. Roy, N. Deb, A. Cortesi, R. Chaki, and N. Chaki, "CARO: A Conflict-Aware Requirement Ordering Tool for DevOps," in *2021 IEEE 29th International Requirements Engineering Conference (RE)*, Sep. 2021, pp. 442–443, iSSN: 2332-6441. [Online]. Available: https://ieeexplore.ieee.org/document/9604702

[35] A. Severino, S. Curto, S. Barberi, F. Arena, and G. Pau, "Autonomous Vehicles: An Analysis Both on Their Distinctiveness and the Potential Impact on Urban Transport Systems," *Applied Sciences*, vol. 11, 2021. [Online]. Available: https://consensus.app/papers/vehicles-analysis-both-their-distinctiveness-potential-severino/2966c1b1fde35bd9b5c5475cee5f02e8/

[36] L. Claussmann, M. Revilloud, D. Gruyer, and S. Glaser, "A review of motion planning for highway autonomous driving," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 5, pp. 1826–1848, 2020.

[37] J. Sini and M. Violante, "A simulation-based methodology for aiding advanced driver assistance systems hazard analysis and risk assessment," *Microelectronics Reliability*, vol. 109, 2020. [Online]. Available: https://consensus.app/papers/simulationbased-methodology-aiding-advanced-assistance-sini/1d866f71fe505197b8ef431954394def/

[38] X. Xia, W. Xi, H. Li, and Y. Wang, "Application and comparison of STPA and functional safety analysis in ACC system," in *Sixth international conference on electromechanical control technology and transportation (ICECTT 2021)*, Q. Zeng, Ed., vol. 12081. SPIE / International Society for Optics and Photonics, 2022, p. 120813X. [Online]. Available: https://doi.org/10.1117/12.2623891

[39] C. Kyrkou, A. Papachristodoulou, A. Kloukiniotis, A. Papandreou, A. Lalos, K. Moustakas, and T. Theocharides, "Towards Artificial-Intelligence-Based Cybersecurity for Robustifying Automated Driving Systems Against Camera Sensor Attacks," in *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Jul. 2020, pp. 476–481, iSSN: 2159-3477. [Online]. Available: https://ieeexplore.ieee.org/document/9154906

[40] P. Piatek, "Incident Management Process Model for Automotive CyberSafety Systems Using the Business Process Model and Notation," in *2022 26th International Conference on Methods and Models in Automation and Robotics (MMAR)*, Aug. 2022, pp. 232–237. [Online]. Available: https://ieeexplore.ieee.org/document/9874288

[41] V. K. Kukkala, S. V. Thiruloga, and S. Pasricha, "Roadmap for cybersecurity in autonomous vehicles," *IEEE Consumer Electronics Magazine*, vol. 11, no. 6, pp. 13–23, 2022.

[42] M. Skoglund, F. Warg, and B. Sangchoolie, "In search of synergies in a multi-concern development lifecycle: Safety and cybersecurity," in *Computer safety, reliability, and security*, B. Gallina, A. Skavhaug, E. Schoitsch, and F. Bitsch, Eds. Cham: Springer International Publishing, 2018, pp. 302–313.

[43] K. T. Kosmowski, E. Piesik, J. Piesik, and M. Śliwiński, "Integrated functional safety and cybersecurity evaluation in a framework for business continuity management," *Energies*, vol. 15, no. 10, 2022, number: 3610. [Online]. Available: https://www.mdpi.com/1996-1073/15/10/3610

[44] G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey," *Future Internet*, vol. 12, no. 4, p. 65, Apr. 2020, number: 4 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: https://www.mdpi.com/1999-5903/12/4/65

[45] A. A. Ganin, P. Quach, M. Panwar, Z. A. Collier, J. M. Keisler, D. Marchese, and I. Linkov, "Multicriteria decision framework for cybersecurity risk assessment and management," *Risk Analysis*, vol. 40, no. 1, pp. 183–199, 2020, tex.eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/risa.12891. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.12891

[46] D. Ashenden, "The future human and behavioural challenges of cybersecurity," in *The oxford handbook of cyber security*. Oxford University Press, Nov. 2021, tex.eprint: https://academic.oup.com/book/0/chapter/352568229/chapter-ag-pdf/55148369/book_41360_section_352568229.ag.pdf. [Online]. Available: https://doi.org/10.1093/oxfordhb/9780198800682.013.48

[47] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," *IEEE access : practical innovations, open solutions*, vol. 8, pp. 23 817–23 837, 2020.

[48] Z. Belkhamza, "Cybersecurity in Digital Transformation applications: Analysis of Past Research and Future Directions," *International Conference on Cyber Warfare and Security*, vol. 18, no. 1, pp. 19–24, Feb. 2023, number: 1. [Online]. Available: https://papers.academic-conferences.org/index.php/iccws/article/view/1005