International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Innovative Approaches to Risk Identification in Connected and Autonomous Vehicles

Harshil Wadhwana , Dr. Megha Shah

PhD Research Scholar, Faculty of Management,
GLS university, Ahmedabad, Gujrat, India
Email ID - harshil.wadhwana93@gmail.com
Associate Professor, Faculty of Management,
GLS university, Ahmedabad, Gujrat, India
Email ID - megha.shah@glsuniversity.ac.in

***Abstract*—** Revolutionizing transportation networks globally, the emergence of Connected and Autonomous Vehicles (CAVs) brings about groundbreaking improvements to the automobile sector. Despite the advantages that CAVs may have, there are also complex issues with security, risk management, and safety that must be considered. This study explores new ways of looking at CAV-related concerns and how to deal with them. In order to account for the distinctive features of CAV technology, the research analyses current risk assessment approaches and suggests new frameworks. Autonomous functions, linked systems, cybersecurity vulnerabilities, human-machine interactions, and regulatory compliance are all aspects of risk that are examined in an ever-changing context. This research takes a multidisciplinary approach by combining findings from engineering, computer science, cybersecurity, and studies of regulations. The text delves into the complex relationship between technology progress and possible dangers, highlighting the importance of developing risk detection systems that can adapt to the constantly changing field of CAVs. The article also delves into cutting-edge risk detection models and technologies that use simulation approaches, machine learning algorithms, Bayesian networks, and probabilistic methodologies. It stresses the significance of anomaly detection, predictive modelling, and real-time data analysis in proactively finding and reducing hazards related to CAV operations. To show how these new ways of identifying risks work in practice, the study draws on case studies, empirical investigations, and industry standards. In order to guarantee the secure and dependable incorporation of CAV technologies into contemporary transportation networks, it also stresses the importance of stakeholders, regulatory agencies, industry participants, and academics working together to create strong risk management frameworks. Across the final analysis, this article adds to our knowledge of the changing risk picture in the field of autonomous and connected vehicles. It promotes the appropriate and safe integration of CAV technology into future transportation systems by providing useful insights and recommendations to help stakeholders anticipate, detect, and manage hazards.

Keywords— Automotive Industry, Connected and Autonomous Vehicles (CAVs), Risk Assessment, Safety, Supply Chain Vulnerabilities

I. INTRODUCTION

The introduction of connected and autonomous vehicles (CAVs) signals a paradigm shift in the landscape of the automotive industry, promising to bring about revolutionary improvements in terms of the efficiency, safety, and ease of transportation and transportation. Because they are outfitted with cutting-edge technology, these automobiles have the potential to revolutionize mobility systems, therefore redefining the method in which people travel and the way in which things are moved. On the other hand, the incorporation of autonomous driving and networking

into automobiles brings about a wide variety of dangerous situations that need for the implementation of effective risk management and detection procedures [1]. Within the scope of this study article, the primary objective is to investigate novel ways that may be utilized to recognize and mitigate the myriad of dangers that are intrinsic to the domain of CAVs. The traditional methods of risk assessment frequently have difficulty doing a complete job of capturing the dynamic and linked nature of the hazards that are posed by autonomous capabilities, networked systems, cybersecurity vulnerabilities, human-machine interactions, and developing regulatory environments.

In light of the tremendous advancements being made in the development and deployment of CAV technologies, it is becoming increasingly important to design risk detection frameworks that are adaptable and customized to the specific characteristics of these vehicles. This study aims to bridge the gap by analyzing the changing risk picture within the CAV domain [2]. It does so by taking into consideration a variety of views from engineering, computer science, cybersecurity, and regulatory research. In addition to this, it analyzes the most recent models and tools for risk detection, with a particular focus on the significance of utilizing cutting-edge techniques such as probabilistic methods, Bayesian networks, machine learning algorithms, and simulation approaches [3]. Real-time data analysis, anomaly identification, and predictive modeling are all made possible by these approaches, which also provide proactive steps to anticipate, identify, and reduce any dangers connected with CAV operations.

The purpose of this paper is to give stakeholders with significant insights and guidance for predicting, detecting, and successfully managing risks in the rapidly developing field of autonomous vehicles by examining case studies, empirical analysis, and best practices in the industry. In addition, it highlights the significance of collaborative efforts among stakeholders, regulatory bodies, industry players, and academic institutions in order to develop comprehensive risk management frameworks that are conducive to the safe and reliable integration of autonomous vehicle technologies into future mobility systems [4].

II. RELATED WORKS

Risk managers should assess the CSR agenda for possibilities to apply risk management principles and tools to other areas of focus. The same risk management methods as risk assessment, control measure identification, and compliance audits may help CSR and CG [5]. We investigate different quantitative methods for supply chain risk management in this paper. It examines SCRM literature and how solutions compare to real-world implementations. This paper serves three purposes. We start by standardizing SCRM content categorization. Second, we hope this evaluation will assist researchers understand this crucial topic's mountain of literature. Third, we want to highlight the gap between theory and practice to inspire researchers to develop new supply chain disruption models [6]. Businesses now face more risk. Continuous risk assessment is required for enterprises. Risk modeling is challenging due to risk-event interdependencies and data scarcity. A constantly updated corporate risk assessment model is the paper's aim. A dual-sourcing supply chain disruption is examined in this article. The three-tiered supply chain is modeled using system dynamics. APIOBPCS and APVIOBPCS are being compared to see whether inventory replenishment policy performs better during interruptions [7]. The ISM diagraph shows how barriers are interrelated. Government support and manufacturing technology skills are the most essential elements, with minimal dependency and high driving power [8]. We focus on new kinds of NPD and their consequences on risk framing. In this study, we combine NPD and CAS from complexity theory. CAS helps explain emerging NPD categories. New NPD categories need a specific risk framing technique to manage risk due to their nature, emphasis, and product development process. A complete literature review of 354

2000–2016 publications using descriptive, thematic, and content analysis. Classifying hazards and recommending techniques to mitigate them have garnered attention. The research has focused on organizational responses to supply chain risks rather than theory. Study should continue in eleven primary areas [9]. This article shows how to create and implement a sustainable supply chain management framework utilizing two analytical phases. Our exchange measures include environmental effect, economic impact (costs and benefits), social impact, and risk, as well as penalties, intangible risk, and transaction costs (using balanced scorecard). The suggested technique uses math programming with three components and a parameter to find the optimal solution for a set of piece-wise equations. Verified and approved [10]. Managers may prioritize supply chain goals, pick the best supplier, and identify risk indicators and the impact of unwanted events and cause and effect relationships throughout the chain using AHP. This article focuses on using cognitive maps and Analytic Hierarchy Process to assess supply chain risk across product categories. Risk assessment for the auto supply chain: Automotive models are poorly understood. The automotive supply chain is complicated due to its multinational network and many multitier suppliers. Demand unpredictability is not the only automotive supply chain challenge that needs examination. Call-back risk and strong network design are examples [11]. Our analysis found the car sector important based on global, EU, and local output figures. Information affecting Hungary's position is most important. The results show that SMEs may decrease their OSR directly, through supplier integration, or by concentrating on buyer-supplier social capital. It is established that OSR hurts SMEs' operational performance and that supplier integration modulates the social capital-OSR relationship [12]. The survey sampled Iranian stock-listed or CBI-licensed banking organizations. This study measured ERM application with a new metric. Tobin's Q ratio and return on equity both measured organizational success. Tobin's Q ratio was positively and statistically significantly associated with ERM adoption, unlike ROE. The results show that ERM strategies affect long-term performance more than short-term success [13]. Risk assessment and threat analysis in the car sector are examined in this research. First, a new TARA method classification is proposed. We compared and evaluated methods. They then compared the performance of numerous popular TARA tools. Next, attack-defense mapping can help determine which mitigations are best for the system's vulnerabilities and threats. Finally, we discussed TARA's car sector expansion goals. Jiangsu's new energy vehicle sector was risk analyzed in July 2019 using the entropy weight-cloud model. The results showed that exogenous risk affected the sector more than endogenous risk and that industrial risk was greater than medium risk. Many corporate risk prevention strategies include improving the industry's internal risk resistance and soft environment [14]. This study was compared to others from other countries. We carefully analyzed the study's drawbacks and determined that worldwide comparative studies of small, medium, and large firms are urgently required. The natural way to improve the risk assessment system is to determine the causal relationship between non-compliance and its consequences across required levels. This employer will improve working conditions using its own resources, considering local production peculiarities, and aiming toward objectives. In addition, employees may be educated of regulatory mismatches and their health and safety effects [15]. Risk-based business excellence may satisfy customers more than technological leadership. Evaluate control techniques for permanent, low-risk categories.

We suggest a molding facility with four diametric lines and Kunkel Wagner. The ductile manufacturing-focused CAE de fonds system may be updated by adding an in-house pattern and die shop with CAD/CAM, additional work plans, tasks, and control measures. The poll found that Indian retirees can invest a certain amount under the pension program. The study found that pension investment and capital market expansion boost national economic growth and pension investment returns. This boosts the stock market by encouraging pension fund investment [2]. From 2000 to 2021, automotive supply chain disruption risk management

publications increased from five to 105. This shows society and academia are prioritizing automotive supply chain disruption risk management studies. Determine significant books, authors, and research themes. The research found that long, sophisticated supply networks and company procedures made supply systems more susceptible. After susceptibility evaluations, experts may enhance supply networks by mitigating risks. This research helps establish a model for internal, regulated supply chain vulnerability factors.

III. TRADITIONAL RISK ASSESSMENT METHODS AND LIMITATIONS

Traditional risk assessment techniques, such as Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Hazard and Operability Studies (HAZOP), Event Tree Analysis (ETA), and Quantitative Risk Analysis (QRA), have been applied for a considerable amount of time in a variety of sectors with the purpose of identifying and managing risks. On the other hand, when similar methodologies are applied to the setting of connected and autonomous vehicles (CAVs), they are confronted with a number of restrictions. This is because of the particular complexity and uncertainties that are associated with this emergent technology.

Methods	Limitations
FMEA systematically examines potential failure modes within systems, processes, or designs and assesses their effects[16]	The intricate nature of CAVs, encompassing highly interconnected autonomous systems driven by artificial intelligence, may exceed the scope of FMEA. It might struggle to anticipate unforeseen scenarios or address uncertainties in AI decision-making on the road
FTA deconstructs complex systems into fault events to illustrate how they could lead to system failures	The complexities of CAVs, including software, hardware, sensors, and dynamic external factors, make it challenging to create exhaustive fault trees. FTA might not adequately account for evolving cyber threats or interactions between multiple failure modes
HAZOP systematically investigates deviations from intended operations to identify potential hazards	CAVs operate in diverse and evolving environments, making it difficult to predict and address all potential hazards through traditional HAZOP methods. It might overlook critical cybersecurity risks or issues related to human-machine interaction
ETA maps out sequences of events following an initiating event or hazard	The adaptability of CAVs presents challenges in accurately predicting and modelling event sequences. ETA might struggle to encompass uncertainties related to AI decision-making or external environmental factors influencing CAV operations
QRA quantifies risks using probability distributions and quantitative data	The lack of historical data for novel risks associated with CAVs hinders accurate quantitative analysis. QRA might face

	challenges in addressing uncertainties in AI-driven systems or dynamic cyber threats

It is important to note that although these conventional approaches to risk assessment have proven to be beneficial in a variety of sectors, their applicability to connected and autonomous vehicles (CAVs) has been found to be restricted due to the unprecedented complexity, uncertainty, and adaptability of autonomous and connected vehicle systems[17]. Consequently, this highlights the importance of developing novel risk detection frameworks that are specifically geared to handle the difficulties that are brought by CAV technologies to the industry.

There is a wide range of dangers that are posed by connected and autonomous vehicles, which include weaknesses in cybersecurity, worries about functional safety, ethical conundrums, legislative ambiguities, difficulties in human-machine interaction, concerns about data privacy, and infrastructural dependencies. The fact that CAVs are dependent on networked systems creates substantial cybersecurity vulnerabilities, which might possibly compromise the integrity of data and the operation of the autonomous vehicle. In addition to managing the intricacies of rules and liability frameworks, ensuring the dependability of autonomous systems and making ethical decisions is a difficulty that must be overcome [18]. For the safe and successful integration of autonomous vehicles, effective human-machine interaction, data privacy measures, and solid infrastructure are essential components. In order to avoid these multiple dangers, it is necessary for diverse sectors to collaborate and come up with novel solutions.

IV. INNOVATIVE APPROACHES TO RISK IDENTIFICATION IN CAVS

Formula-based approaches and model-based methods are the two categories that are used to classify TARA methods in this part where they are split. Tables, texts, and formulae are the primary components of formula-based approaches, which are utilized for the purpose of conducting threat analysis and risk assessment of the system [15]. The three categories of formula-based approaches are asset-based methods, vulnerability-based methods, and attacker-based methods. These categories are based on the varied problems that each type of method addresses when applied.

a. FORMULA-BASED METHODS

- *Asset-Based Methods*: asset-based approach is the most common type of TARA method in the automotive domain. ,is series of methods first identifies the final target asset under attack and then exhausts the attack paths and attack methods that can pose a threat to this target asset through the use of relevant experience and minds of security experts so that advance prevention can be carried out. The approach in question is also referred to as a "top-down" method. OCTAVE was initially made available in 1999 by CERT/CC, which stands for Computer Emergency Response Team/Coordination Center. It is now widely accepted that the OCTAVE approach is one of the most effective TARA methods in the world. ,,In order for the workforce of the organization to be able to take full ownership of the business's information security needs, the OCTAVE methodology is an approach that splits the assessment into three parts. During these phases, management concerns and technical issues are evaluated and debated.The OCTAVE technique defines itself as a methodology to assessment that takes into account assets, threats, and vulnerabilities all at the same time [19]. The results of the assessment may be used by managers to identify the OCTAVE technique, which is

defined by a combination of asset, threat, and vulnerability assessments. This facilitates the process of determining the OCTAVE method. The results of the assessment may also be used by managers to determine the order of importance for the risks that need to be addressed. Additionally, it takes into account the manner in which the computer infrastructure is utilized and the function that it plays in the accomplishment of the organization's business goals. OCTAVE is coordinated with the many technological features of computer infrastructure setup that are interconnected with one another. In addition to this, it makes it possible to have an approach that is adaptable, repeatable, and configurable, which can be tailored to meet the requirements of various businesses.

- *Vulnerability-Based Methods*: The vulnerability-based techniques are "bottom-up" TARA approaches, where the asset-based methods correspond to the vulnerability-based methods. When they begin with a vulnerability or weakness that has been discovered in a system, they proceed to investigate what additional larger vulnerabilities or failures the vulnerability may potentially trigger. The CVSS, which stands for the Common Vulnerability Scoring System, is an open standard that was developed by the industry to assist in determining the level of urgency and relevance of the needed response.One of the primary goals of the Common Vulnerability Scoring System (CVSS) is to assist in the establishment of a standard for assessing the severity of vulnerabilities. This will allow for the comparison of the severity of vulnerabilities and the determination of the importance of dealing with them [20]. The CVSS scores are derived from the results of measurements taken on a number of different dimensions, which are referred to as metrics. The CVSS consists of three different types of scores: base, temporal, and environmental meter. By extending the security features that are based on FMEA, FMVEA transforms it into a method that is used for both safety and security analysis. It is possible to examine how the quality characteristics of components fail using its failure modes, while threat modes are utilized in order to study how failing security attributes occur. It is possible to estimate the frequency of danger modes by recognizing threat agents, and the likelihood of the occurrence of threat modes is defined by the threat agents and vulnerabilities [21].

- *Attacker-Based Methods:* There is a form of threat analysis approach known as the attacker-based method, which examines the activities of attackers. It performs threat analysis and risk evaluation of the system by analysing the knowledge level of potential attackers, attack pathways, assault motivations, and the quantity of resources that are owned. This allows for the threat to be modelled and assessed from the perspective of the underlying cause of the attacked system. An upgraded security risk analysis framework for autonomous driving system-dedicated automobiles is known as SARA. This framework incorporates the opinions of security experts, new threat models, attack techniques, asset mappings, and attack tree definitions. In addition, the SARA establishes a new measure that takes into account the controllability of the driver or the automated driving system when calculating the risk value [22]. A comprehensive integration of safety management and model-based system engineering is achieved by SAM (Security Abstraction Model), which is characterized by an abstract representation of the fundamental concepts underlying automotive security modelling [23]. Agent Risk Assessment is a process that is carried out in six phases, and its objective is to identify the critical exposure of the connected automobile. There are three components that make up the Threat Agent Risk Assessment technique. These are the Threat Agent Library (TAL), the Methods and Objectives Library (MOL), and the Common Exposure Library (CEL). The approach of Threat Agent Risk Assessment is able to identify a list of potential assaults and rate these attacks according to the chance that they will occur . On

the other hand, the approach of the Great Agent Risk Assessment is very new, and there is essentially no documentation that supports it, with the exception of the very limited information that Intel Security has provided. There is also additional work that needs to be done in order to properly use this strategy inside the automobile sector. In the Bayesian Stackelberg game technique, the attack and defensive process is modelled as a Stackelberg game for network security. This game is of the Bayesian type, and it offers the best hybrid strategy for both the attacker and the Internet of Vehicle defence system. The latter offers the optimal deployment of the available security resources in the transportation infrastructure, with the goal of minimizing the impact of attacks and improving their detection. There are a number of different kinds of data corruption assaults that are taken into consideration, as shown by the probability distribution that is derived by the stringent risk assessment approach. When compared to a unified defensive architecture that does not take into account the kind or tactic of the attacker, this solution has the potential to lessen the effect of sophisticated persistent threats. This method has the potential to be incorporated into the designing process of the intrusion detection system for the Internet of Vehicles in order to enhance its robustness.

b. MODEL-BASED METHODS

- *Graph-Based Methods:* Nodes and directed edges are the means by which graph-based approaches are connected to one another. Methods that are based on graphs have the ability to articulate the direct mathematical quantitative link between each node module, which makes it easier to conduct quantitative threat analysis on the system. Spoofing (S), tampering (T), repudiation (R), information disclosure (I), denial of service (D), and elevation of privilege (E) are the components that make up the STRIDE paradigm. It has been demonstrated that the STRIDE approach is capable of identifying and analyzing the dangers that are present in the system, which may effectively lower the chance of the system being attacked. This method has been widely utilized in the information technology sector. Because of the remarkable impact it has, the STRIDE approach is increasingly being implemented in a variety of other domains. ,,An additional recommendation for the STRIDE approach may be found in the SAE J3061 rules, which pertain to the subject of vehicle information security. It was in 2012 that UcedaVelez devised a seven-stage threat analysis process that they termed PASTA (which stands for Process for Attack Simulation and Analysis). This method was developed in addition to the STRIDE method. Data flow diagrams are utilized by PASTA at the application decomposition layer of the architecture. ,,The LINDDUN technique, which stands for linkability, identifiability, nonrepudiation, detectability, disclosure of data, unawareness, and noncompliance, is a method that offers protection for the system's data security and privacy by means of a six-step examination . In order to assess and identify various kinds of dangers, it employs pieces of an iterative model that are taken from a data flow diagram. It is possible to extend the VAST approach, which stands for visual, agile, and simple threat, and its application may be extended to include large-scale threat model analysis.
- *Tree-Based Methods*: There is a possibility that tree-based approaches can both explain the hierarchical connection between nodes and reflect the affinity that exists between them. It is the attack tree model that is the most typical example of this sort of strategy. This model is able to explain the assault that the system is susceptible to and clearly indicate the attack path. The concept of attack tree analysis refers to a form of threat analysis that employs a tree as its structure. The overall structure of the attack tree in terms of its structure. The top event is used to define the attack target, and the nodes that are located below the attack target reflect all of the possible events that might result in

the attack target occurring. The "OR" gate and the "AND" gate are two types of gates that may be used to link the logical relationship between these occurrences. In order to undertake attack tree analysis, one can execute it in a top-down fashion, which means that one must first choose the ultimate attack target and then proceed to analyse all of the alternative assault paths in accordance with the attack target. Additionally, it is feasible to carry out the process in a bottom-up fashion, which entails first studying the potential attack surface and then analysing the potential vulnerabilities based on this observation [24]. On the other hand, when confronted with the task of threat analysis of big systems, the conventional attack tree analysis approach necessitates the manual building of a significant number of attack possibilities. It is unavoidable that attack vectors will be lost, and the likelihood of car systems being targeted will grow, both of which are situations that the original equipment manufacturers (OEMs) cannot tolerate. In response to this limitation of attack tree analysis, Salfer et al. [25] suggested a method for automatically generating attack forests for automobile networks in order to protect against software vulnerabilities.

V. CONCLUSION

An examination and comparison of the TARA approaches utilized in the automobile industry has been carried out in this survey. All of the approaches have been categorized in order to facilitate researchers' ability to acquire a comprehensive and speedy understanding of the TARA topic. Ways to assess the TARA methods that have been published in the literature are also presented. A number of TARA tools that are often utilized have been presented, and a comparison of the performance of these tools has been made. Additionally, a concept known as attack-defense mapping has been presented. This idea focuses on how to match the proper mitigation measures after discovering threats and vulnerabilities. The notion serves as a theoretical foundation for TARA, which in turn makes the entire process more adaptable and persuasive. Following the classification of the attack-defense mapping strategies into five distinct groups, we proceeded to study and contrast these individual approaches. Additionally, the future directions of advances in TARA for the automotive domain are taken into consideration and explored.

VI. REFERENCES

[1]V. Garg, V. Singh, Y. K. Jain, and P. Sharma, “A Quantitative Analysis of Microfinance Credit Facilities for MSMEs and their Impact on Liquidating Poverty in Delhi-NCR Region : With Special Reference to AU Small Finance Bank,” vol. 3, no. 2, pp. 2224–2235, 2023.

[2]M. V. Kapitonov, “Evaluation and Analysis of Risks in Automotive Industry,” *Transportation Research Procedia*, vol. 61, pp. 556–560, 2022, doi: 10.1016/j.trpro.2022.01.090.

[3]F. Luo, Y. Jiang, Z. Zhang, Y. Ren, and S. Hou, “Threat Analysis and Risk Assessment for Connected Vehicles: A Survey,” *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/1263820.

[4]M. J. Ligarski, B. Rożałowska, and K. Kalinowski, “A study of the human factor in industry 4.0 based on the automotive industry,” *Energies (Basel)*, vol. 14, no. 20, pp. 1–20, 2021, doi: 10.3390/en14206833.

[5]K. Words, "Risk assessment of India automotive enterprises using Bayesian networks," *Risk assessment of India automotive enterprises using Bayesian networks Abstract:*, 2009.

[6]E. Bayer and G. O. Bustad, *Introducing Risk Management Process to a Manufacturing Industry*. 2012. [Online]. Available: http://kth.diva-portal.org/smash/get/diva2:606971/FULLTEXT01

[7]D. Dominic, S. Chhawri, R. M. Eustice, D. Ma, and A. Weimerskirch, "Risk assessment for cooperative automated driving," *CPS-SPC 2016 - Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and PrivaCy, co-located with CCS 2016*, pp. 47–58, 2016, doi: 10.1145/2994487.2994499.

[8]G. Dwivedi, S. K. Srivastava, and R. K. Srivastava, *Analysis of barriers to implement additive manufacturing technology in the Indian automotive sector*, vol. 47, no. 10. 2017. doi: 10.1108/IJPDLM-07-2017-0222.

[9]V. K. Dubey, J. P. Chavas, and D. Veeramani, "Analytical framework for sustainable supply-chain contract management," *Int J Prod Econ*, vol. 200, pp. 240–261, 2018, doi: 10.1016/j.ijpe.2018.03.003.

[10] L. Mirboroon and H. Razavi, "A Case Study of Risk Management of Automotive Industry Projects Using RFMEA Method," *Mapta Journal of Mechanical and Industrial Engineering (MJMIE)*, vol. 4, no. 1, pp. 42–50, 2020, doi: 10.33544/mjmie.v4i1.132.

[11] A. Meena, S. Dhir, and Sushil, "An analysis of growth-accelerating factors for the Indian automotive industry using modified TISM," *International Journal of Productivity and Performance Management*, vol. 70, no. 6, pp. 1361–1392, 2021, doi: 10.1108/IJPPM-01-2019-0047.

[12] Y. Wang, Y. Wang, H. Qin, H. Ji, Y. Zhang, and J. Wang, "A Systematic Risk Assessment Framework of Automotive Cybersecurity," *Automotive Innovation*, vol. 4, no. 3, pp. 253–261, 2021, doi: 10.1007/s42154-021-00140-6.

[13] Y. Cao, Y. Bian, R. Wang, and L. Wang, "Research on the Risk Assessment of New Energy Automobile Industry Based on Entropy Weight-Cloud Model in China's Jiangsu Province," *Math Probl Eng*, vol. 2021, 2021, doi: 10.1155/2021/4714681.

[14] A. Tyagi and A. Singh, "The Pension Fund Investments Role in Financing and Enabling Global Development in Indian Market," vol. 13, no. 5, pp. 1125–1132, 2023.

[15] K. Huang, J. Wang, and J. Zhang, "Automotive Supply Chain Disruption Risk Management: A Visualization Analysis Based on Bibliometric," *Processes*, vol. 11, no. 3, pp. 1–25, 2023, doi: 10.3390/pr11030710.

[16] D. Singh-Ackbarali and R. Maharaj, "Perceptions of Street Food Safety among Select Groups of the Female Population in Trinidad," *Online International Journal of Food Science*, vol. 5, no. July 2018, pp. 1–13, 2016.

[17] S. Zhu, "Scholarship at UWindsor Scholarship at UWindsor Electronic Theses and Dissertations Theses, Dissertations, and Major Papers SUPPLY CHAIN RISK MANAGEMENT IN AUTOMOTIVE INDUSTRY SUPPLY CHAIN RISK MANAGEMENT IN AUTOMOTIVE INDUSTRY," 2018, [Online]. Available: https://scholar.uwindsor.ca/etd/7611

[18] N. H. Sarmin, M. A. El-Sanfaz, and S. M. S. Omer, "Groups and graphs in probability theory," *AIP Conf Proc*, vol. 1750, no. 2016, 2016, doi: 10.1063/1.4954600.

[19] N. A. Choudhary, S. Singh, T. Schoenherr, and M. Ramkumar, "Risk assessment in supply chains: a state-of-the-art review of methodologies and their applications," *Ann Oper Res*, vol. 322, no. 2, pp. 565–607, 2023, doi: 10.1007/s10479-022-04700-9.

[20] N. Yoga Irsyadillah and S. Dadang, "a Literature Review of Supply Chain Risk Management in Automotive Industry," *Journal of Modern Manufacturing Systems and Technology*, vol. 4, no. 2, pp. 12–22, 2020, doi: 10.15282/jmmst.v4i2.5020.

[21] C. Schmittner, Z. Ma, and P. Smith, "FMVEA for safety and security analysis of intelligent and cooperative vehicles," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8696 LNCS, pp. 282–288, 2014, doi: 10.1007/978-3-319-10557-4_31.

[22] J. P. Monteuuis, A. Boudguiga, J. Zhang, H. Labiod, A. Servel, and P. Urien, "SarA: Security automotive risk analysis method," *CPSS 2018 - Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, Co-located with ASIA CCS 2018*, pp. 3–14, 2018, doi: 10.1145/3198458.3198465.

[23] M. Zoppelt and R. Tavakoli Kolagari, *SAM: A Security Abstraction Model for Automotive Software Systems*, vol. 11552 LNCS. Springer International Publishing, 2019. doi: 10.1007/978-3-030-16874-2_5.

[24] D. Ren, S. Du, and H. Zhu, "A novel attack tree based risk assessment approach for location privacy preservation in the VANETs," *IEEE International Conference on Communications*, no. 61003218, pp. 11–15, 2011, doi: 10.1109/icc.2011.5962947.

[25] P. Chowdhury, K. H. Lau, and S. Pittayachawan, "Operational supply risk mitigation of SME and its impact on operational performance: A social capital perspective," *International Journal of Operations and Production Management*, vol. 39, no. 4, pp. 478–502, 2019, doi: 10.1108/IJOPM-09-2017-0561.