International Journal of Engineering & Scientific Research
Vol.12 Issue 10, October 2024
ISSN: 2347-6532 Impact Factor: 6.660
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Integrating Systems Theoretic Process Analysis (STPA) with Failure Mode and Effect Analysis (FMEA) for Risk Assessment in Road Vehicle Functional Safety

Durgadevi Yenuganti*
Hima Bindu Anne**

Abstract

The current research integrates Systems Theoretic Process Analysis (STPA) with Failure Mode and Effect Analysis (FMEA) to enhance risk assessment for road vehicle functional safety. Focusing on the Fuel Level Estimation and Display System (FLEDS), the study identifies unsafe control actions (UCAs) and failure modes, highlighting critical areas where system failures could lead to hazardous states. The integrated analysis combines the system-level hazard identification of STPA with the detailed component-level analysis of FMEA, providing a comprehensive risk assessment. The findings demonstrate that the integrated approach offers a more holistic view of potential risks, leading to more effective mitigation strategies. Despite some limitations, the integrated STPA-FMEA methodology proves to be a valuable tool for improving vehicle safety, with future research suggested to refine and expand its application.

Keywords:

Functional Safety;
STPA;
FMEA;
Risk Assessment;
Road Vehicle Systems.

Author correspondence:

DurgadeviYenuganti,
Masters in Computer science, Bachelors in Electronics and Communication Engineering,
Southeast Missouri state university, Cape Girardeau, Missouri,
Email: durgadeviyenuganti@gmail.com

1. Introduction

Functional safety in road vehicles is a critical aspect of automotive engineering, aimed at ensuring that electronic and electrical (E/E) systems operate correctly and safely under all conditions. The international standard ISO 26262 provides a framework for functional safety in road vehicles, defining the necessary requirements to mitigate risks associated with E/E system malfunctions [1]. This standard emphasizes the importance of identifying potential hazards and implementing measures to prevent or control these hazards, thereby reducing the risk of accidents and ensuring the safety of vehicle occupants and other road users [2].

The comprehensive guidelines are provided by ISO 26262; however, current risk assessment methods face several challenges. Traditional approaches such as Failure Mode and Effect Analysis (FMEA) often focus on component-level failures and may overlook system-level interactions and complex failure modes [3]. Additionally, FMEA can be time-consuming and may not adequately address the dynamic and interconnected nature of modern automotive systems [4]. On the other hand, Systems Theoretic Process Analysis (STPA) offers a broader perspective by considering system-level hazards and control actions, but it may lack the detailed failure mode analysis provided by FMEA [5]. The integration of these two methods could potentially address their individual limitations and provide a more comprehensive risk assessment framework.

*Continental Automotive components Pvt.Ltd,Southgate Tech Park, Hosur Rd, Electronic City, Bengaluru, Karnataka 560100, India
**Manager(ME),Medha servo drives Pvt.Ltd,Mallapur,Hyderabad-500076, India.

ISO 26262 is the international standard for functional safety in road vehicles, providing a comprehensive framework for ensuring the safety of electronic and electrical (E/E) systems. The standard covers the entire lifecycle of automotive systems, from concept phase through decommissioning, and emphasizes the importance of identifying and mitigating risks associated with system malfunctions [1]. ISO 26262 introduces the concept of Automotive Safety Integrity Levels (ASILs), which categorize the risk levels of potential hazards and guide the necessary safety measures [6]. The standard's systematic approach to risk assessment and management has become a key element in the development of safe automotive systems.

FMEA: FMEA is a structured approach used to identify potential failure modes within a system, assess their effects, and prioritize actions to mitigate risks. FMEA involves a detailed examination of each component and process to determine how failures can occur and what their consequences might be [3]. This method is widely used in various industries, including automotive, to enhance reliability and safety. FMEA's systematic nature allows for the identification of failure modes at the component level, making it a valuable tool for quality control and risk management [4]. However, its focus on individual components can sometimes overlook system-level interactions and complex failure scenarios.

STPA: STPA is a hazard analysis technique that extends beyond traditional methods by considering the interactions and control actions within a system. Developed as part of the Systems-Theoretic Accident Model and Processes (STAMP) framework, STPA identifies unsafe control actions that could lead to hazardous states [2]. This method is particularly useful for analyzing complex, software-intensive systems where traditional failure analysis methods may fall short. STPA's holistic approach allows for the identification of hazards that arise from system interactions, making it a powerful tool for ensuring functional safety in modern automotive systems [7].

Several studies have explored the integration of STPA and FMEA to leverage the strengths of both methods. For instance, combining STPA's system-level hazard identification with FMEA's detailed failure mode analysis can provide a more comprehensive risk assessment framework [8]. Research has shown that this integrated approach can enhance the identification of potential hazards and failure modes, leading to more effective risk mitigation strategies. One study demonstrated the application of this integrated method in the automotive industry, highlighting its potential to improve safety outcomes by addressing both component-level and system-level risks [9]. The integration of STPA and FMEA continues to evolve, with ongoing research aimed at refining the methodology and expanding its applications [10].

Table 1. The benefits of integrating the FMEA and STPA

Step	FMEA	STPA	Integrated Approach
System Definition	Define the system and its components.	Define the system, control structure, and interactions.	Combine detailed component definitions with control structure and interactions.
Hazard Identification	Identify potential failure modes for each component.	Identify unsafe control actions and hazards.	Use FMEA to identify failure modes and STPA to identify unsafe control actions and hazards.
Risk Analysis	Assess the severity, occurrence, and detection of each failure mode.	Analyze the causal factors leading to unsafe control actions.	Integrate severity, occurrence, and detection with causal analysis of unsafe control actions.
Risk Prioritization	Prioritize failure modes based on Risk Priority Number (RPN).	Prioritize hazards based on their potential impact.	Combine RPN with the impact of unsafe control actions for comprehensive prioritization.
Mitigation Strategies	Develop actions to mitigate high-priority failure modes.	Develop safety constraints to prevent unsafe control actions.	Integrate mitigation actions with safety constraints to address both failure modes and unsafe control actions.
Verification and Validation	Verify and validate the effectiveness of mitigation actions.	Verify and validate the effectiveness of safety constraints.	Conduct integrated verification and validation to ensure both mitigation actions and safety constraints are effective.
Documentation and Review	Document the FMEA process and results.	Document the STPA process and results.	Maintain comprehensive documentation combining FMEA and STPA results for thorough review.

The primary objective of this research is to integrate STPA with FMEA to enhance the risk assessment process for road vehicle functional safety. By combining the strengths of both methods, this integrated approach aims to provide a more holistic view of potential hazards and failure modes, thereby improving the identification and mitigation of risks. The details are presented in Table 1. This research will demonstrate the application of the integrated approach through a case study on a specific road vehicle system, highlighting the benefits and challenges of this methodology.

2. Research methodology

The current study employs a mixed-methods approach, integrating qualitative and quantitative techniques to enhance the risk assessment process for road vehicle functional safety. The research begins with a qualitative analysis using STPA to identify hazards and unsafe control actions. This is followed by a quantitative assessment using FMEA to identify failure modes and their effects. The integration of these methods aims to leverage the strengths of both approaches, providing a comprehensive view of potential risks and enabling the generation of actionable results.

Integration Framework: The integration framework combines the system-level hazard identification capabilities of STPA with the detailed failure mode analysis of FMEA. Initially, the system and its components are defined, followed by the identification of hazards and unsafe control actions through STPA. Subsequently, FMEA is applied to identify failure modes and their effects. The outputs of STPA feed into FMEA, and vice versa, ensuring a thorough risk assessment. This bidirectional flow allows for a holistic understanding of both system-level and component-level risks, facilitating the development of effective mitigation strategies.

STPA Steps: The STPA process begins with defining the purpose of the analysis and modeling the control structure of the system. This involves creating a control structure diagram to represent the system and its interactions. Next, unsafe control actions (UCAs) are identified, which are control actions that could lead to hazardous states. Finally, loss scenarios are analyzed to understand how UCAs could result in losses or accidents. This systematic approach ensures that all potential hazards are identified and analyzed comprehensively.

FMEA Steps: FMEA starts with identifying potential failure modes for each component of the system. The effects of these failure modes are then determined, assessing their impact on the overall system. Each failure mode is assigned severity, occurrence, and detection ratings, which are multiplied to calculate the Risk Priority Number (RPN). This helps prioritize the risks based on their potential impact. Mitigation actions are then developed to reduce the RPN of high-priority failure modes, ensuring that the most critical risks are addressed effectively.

Integration Process: The integration process involves a seamless flow of information between STPA and FMEA. The hazards and unsafe control actions identified through STPA inform the identification of failure modes in FMEA. Conversely, the detailed failure mode analysis from FMEA helps refine the identification of UCAs and loss scenarios in STPA. This iterative process ensures that both system-level and component-level risks are comprehensively addressed, leading to a more robust risk assessment framework.

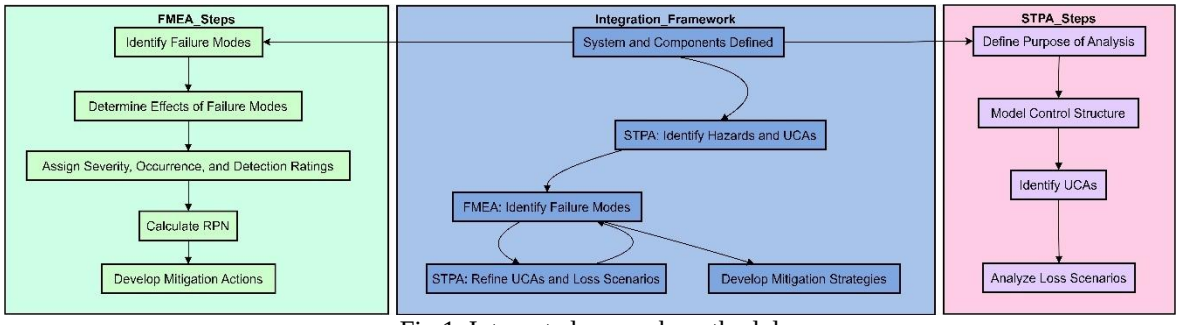

Fig 1. Integrated research methodology

Case Study Selection: To demonstrate the application of the integrated STPA-FMEA approach, a case study is conducted on the fuel level estimation and display system (FLEDS) of a road vehicle. This system is selected due to its complexity and critical role in vehicle safety. The FLEDS involves multiple components and interactions, making it an ideal candidate for applying the integrated methodology. The availability of sufficient data for detailed analysis further supports its selection. Through this case study, the effectiveness of the integrated approach in identifying and mitigating risks in road vehicle systems is illustrated.

3. Results and discussions

As mentioned in the section 2, the selected road vehicle system for this case study is the Fuel Level Estimation and Display System (FLEDS). This system is responsible for accurately estimating the fuel level in the vehicle's tank and displaying this information to the driver. The FLEDS consists of several components, including the fuel level sensor, the electronic control unit (ECU), the display unit, and the communication network that connects these components. Accurate fuel level estimation is critical for vehicle operation, as it informs the driver about the remaining fuel and helps prevent situations where the vehicle runs out of fuel unexpectedly.

Application of STPA: The application of STPA to the FLEDS involves several steps. First, the control structure of the system is modeled, including the interactions between the fuel level sensor, ECU, and display unit. Next, UCAs are identified. For example, a UCA might be the ECU sending incorrect fuel level data to the display unit, leading to a hazardous state where the driver is misinformed about the fuel level. The table 2 summarizes the identified UCAs and their potential hazards from the study.

Table 2. Summary of identified UCAs and their potential hazards

Control Action	Unsafe Control Action (UCA)	Potential Hazard
Fuel level sensor data transmission	Sensor sends incorrect data	Driver receives incorrect fuel level information
ECU data processing	ECU processes data incorrectly	Display shows incorrect fuel level
Display unit update	Display fails to update	Driver is unaware of actual fuel level

These findings indicate that incorrect data transmission from the fuel level sensor could misinform the driver about the remaining fuel, potentially causing the vehicle to run out of fuel unexpectedly. Similarly, incorrect data processing by the ECU or failure of the display unit to update could lead to hazardous situations where the driver is unaware of the actual fuel level. These UCAs emphasize the importance of accurate data transmission, processing, and display in ensuring the functional safety of the FLEDS.

Application of FMEA: FMEA is applied to the FLEDS to identify potential failure modes for each component and assess their effects. The analysis involves assigning severity, occurrence, and detection ratings to each failure mode, and calculating the RPN to prioritize risks. The table 3 presents a summary of the FMEA for the FLEDS.

Table 3. Summary of FMEA for the FLEDS

Component	Failure Mode	Effect	Severity	Occurrence	Detection	RPN
Fuel level sensor	Sensor failure	Incorrect fuel level data	9	3	4	108
ECU	Data processing error	Incorrect data sent to display	8	2	5	80
Display unit	Display failure	Incorrect fuel level shown	7	2	6	84

The highest RPN is associated with the fuel level sensor failure (RPN = 108), indicating that this failure mode has a significant impact on the system's safety. The high severity rating (9) reflects the critical nature of accurate fuel level data for vehicle operation. The occurrence and detection ratings suggest that while sensor failures are relatively infrequent (occurrence = 3), they are not easily detectable (detection = 4). This highlights the need for robust mitigation strategies, such as using multiple sensors for cross-verification, to address sensor failures effectively.

Integrated Analysis: The integrated analysis combines the findings from STPA and FMEA to provide a comprehensive risk assessment. The UCAs identified through STPA are used to inform the identification of failure modes in FMEA, ensuring that both system-level and component-level risks are addressed. For instance, the UCA of the ECU sending incorrect data is linked to the failure mode of data processing errors in

the FMEA. This integrated approach allows for a more thorough understanding of potential hazards and failure modes, facilitating the development of effective mitigation strategies. The table 4 summarizes the integrated risk assessment.

Table 4. Integrated risk assessment

UCA	Linked Failure Mode	Potential Hazard	RPN	Mitigation Strategy
ECU sends incorrect data	Data processing error	Incorrect fuel level shown	80	Implement redundancy in data processing
Sensor sends incorrect data	Sensor failure	Incorrect fuel level information	108	Use multiple sensors for cross-verification
Display fails to update	Display failure	Driver is unaware of actual fuel level	84	Regular maintenance and diagnostics

The proposed integrated analysis highlights the critical areas where risks need to be mitigated and provides a clear path for implementing safety measures. For example, implementing redundancy in data processing and using multiple sensors for cross-verification can significantly reduce the risk of incorrect fuel level information being displayed to the driver. Regular maintenance and diagnostics for the display unit can ensure that the driver is always aware of the actual fuel level.

Further, the integrated STPA-FMEA approach offers several advantages over using either method alone. By combining system-level hazard identification with detailed failure mode analysis, the integrated approach provides a more holistic view of potential risks. This ensures that both system interactions and individual component failures are considered, leading to more thorough risk identification and mitigation. The bidirectional flow of information between STPA and FMEA facilitates the development of more effective mitigation strategies, as seen in the proposed redundancy and cross-verification measures for the FLEDS. This comprehensive risk assessment framework enhances the overall safety of the road vehicle system by addressing both system-level and component-level risks.

Implications for Functional Safety: The findings from the integrated STPA-FMEA analysis have significant implications for the functional safety of road vehicles. By identifying UCAs and failure modes, the study highlights critical areas where the FLEDS could fail, potentially leading to hazardous situations. For instance, the identification of UCAs such as the ECU sending incorrect data underscores the importance of accurate data processing and transmission within the system. Similarly, the RPN associated with sensor failures indicates the need for robust sensor technologies and redundancy to ensure reliable fuel level estimation. These insights can guide the development of more effective safety measures, ultimately enhancing the overall safety of road vehicles.

Advantages of Integration: The integration of STPA and FMEA offers several key benefits over traditional risk assessment methods. Firstly, STPA's system-level perspective complements FMEA's detailed component-level analysis, providing a more comprehensive understanding of potential risks. This holistic approach ensures that both system interactions and individual component failures are considered, leading to more thorough risk identification and mitigation. For example, the integrated analysis revealed that UCAs identified through STPA could inform the identification of failure modes in FMEA, ensuring that no critical risks are overlooked. Additionally, the bidirectional flow of information between STPA and FMEA facilitates the development of more effective mitigation strategies, as seen in the proposed redundancy and cross-verification measures for the FLEDS.

Limitations: Despite its advantages, the integrated STPA-FMEA approach has some limitations. One potential limitation is the increased complexity and time required to perform the integrated analysis compared to using either method alone. The need to model the system's control structure, identify UCAs, and conduct a detailed failure mode analysis can be resource-intensive. Additionally, the effectiveness of the integrated approach depends on the accuracy and completeness of the data used in the analysis. Incomplete or inaccurate data could lead to incorrect risk assessments and mitigation strategies. Furthermore, while the integrated approach provides a comprehensive risk assessment, it may still not capture all possible failure modes and hazards, particularly in highly complex systems.

4. Conclusions

The current research aimed to enhance the risk assessment process for road vehicle functional safety by integrating STPA with FMEA. The study focused on the FLEDS as a case study to demonstrate the application and benefits of the integrated approach.The findings from STPA identified several UCAs that could lead to hazardous states, such as incorrect data transmission from the fuel level sensor and data processing errors by the ECU. These UCAs highlighted critical areas where the system's control actions could fail, potentially leading to safety issues.The FMEA analysis identified several failure modes for the components of the FLEDS, with the highest RPN associated with sensor failures. This indicated the significant impact of sensor failures on the system's safety and underscored the need for robust mitigation strategies.

The integrated analysis combined the findings from STPA and FMEA, providing a comprehensive risk assessment. The UCAs identified through STPA informed the identification of failure modes in FMEA, ensuring that both system-level and component-level risks were addressed. This bidirectional flow of information facilitated the development of effective mitigation strategies, such as implementing redundancy in data processing and using multiple sensors for cross-verification.The integrated STPA-FMEA approach offers several advantages over traditional risk assessment methods. By combining system-level hazard identification with detailed failure mode analysis, this approach provides a more holistic view of potential risks. This leads to more thorough risk identification and mitigation, enhancing the overall safety of road vehicle systems.Despite its advantages, the integrated approach has some limitations, including increased complexity and resource requirements. Future research could focus on developing automated tools to streamline the integration process and exploring the application of the integrated approach to other critical vehicle systems.

In brief, the integrated STPA-FMEA approach is a valuable tool for improving the functional safety of road vehicles. The findings from this study demonstrate the effectiveness of this methodology in identifying and mitigating risks, providing a robust framework for enhancing vehicle safety. Future research can build on these findings to further refine the methodology and expand its application to other automotive systems.

References

[1] ISO. (2018). ISO 26262: Road vehicles – Functional safety. International Organization for Standardization.
[2] Leveson, N. G. (2011). Engineering a safer world: Systems thinking applied to safety. MIT Press.
[3] Stamatis, D. H. (2003). Failure mode and effect analysis: FMEA from theory to execution. ASQ Quality Press.
[4] Ericson, C. A. (2015). Hazard analysis techniques for system safety. John Wiley & Sons.
[5] Thomas, J. P., & Leveson, N. G. (2011). Performing hazard analysis on complex, software- and hardware-intensive systems. MIT Press.
[6] Gheraibia, Y., Kabir, S., Djafri, K., & Krimou, H. (2018). An overview of the approaches for automotive safety integrity levels allocation. Journal of Failure Analysis and Prevention, 18(3), 707-720.
[7] Young, W., & Leveson, N. (2014). An integrated approach to safety and security based on systems theory. Communications of the ACM, 57(2), 31-35.
[8] Yang X, Zhu Y, Zhou T, Xu S, Zhang W, Zhou X, Meng X. Integrating Software FMEA and STPA to Develop a Bayesian Network-Based Software Risk Model for Autonomous Ships. *Journal of Marine Science and Engineering*. 2024; 12(1):4.
[9] Chen L, Jiao J, Zhao T. A Novel Hazard Analysis and Risk Assessment Approach for Road Vehicle Functional Safety through Integrating STPA with FMEA. *Applied Sciences*. 2020; 10(21):7400.
[10] Yang X, Zhu Y, Zhou T, Xu S, Zhang W, Zhou X, Meng X. Integrating Software FMEA and STPA to Develop a Bayesian Network-Based Software Risk Model for Autonomous Ships. *Journal of Marine Science and Engineering*. 2024; 12(1):4.