

Streamlining FMEDA Safety Evaluation in Hardware Design through Automation

Durgadevi Yenuganti*

Hima Bindu Anne**

Abstract

The research paper presents an automated method for evaluating FMEDA safety in hardware designs, specifically applied to an automotive Electronic Control Unit (ECU) used in advanced driver assistance systems (ADAS). The proposed method leverages MATLAB, Simulink, and exSILentia tools to streamline the FMEDA evaluation process, reducing time and effort while minimizing human error. The study demonstrates the practical application of the automated method, highlighting its efficiency, accuracy, and reliability. Key findings include the identification of critical failure modes, assessment of diagnostic coverage, and recommendations for design improvements. The automated method offers significant advantages over traditional manual methods, contributing to enhanced safety and reliability of hardware systems in safety-critical industries.

Copyright © 2024 International Journals of Multidisciplinary Research Academy. All rights reserved.

Keywords:

Automated FMEDA;
Hardware Safety;
Electronic Control Unit (ECU);
Advanced Driver Assistance
Systems;
Diagnostic Coverage.

Author correspondence:

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

1. Introduction

Failure Modes, Effects, and Diagnostic Analysis (FMEDA) is a critical methodology used in the evaluation of hardware safety, particularly in safety-critical industries such as automotive, aerospace, and medical devices. FMEDA extends the traditional Failure Modes and Effects Analysis (FMEA) by incorporating quantitative data on failure rates and diagnostic coverage, providing a more comprehensive assessment of system reliability and safety [1]. This methodology enables engineers to identify potential failure modes, analyze their effects on system performance, and evaluate the effectiveness of diagnostic mechanisms in detecting and mitigating these failures. The significance of FMEDA lies in its ability to provide detailed insights into the behavior of hardware components under fault conditions, thereby enhancing the overall safety and reliability of the system [2].

Despite its importance, traditional FMEDA evaluation methods face several challenges. One of the primary challenges is the manual and time-consuming nature of the process. Conducting a thorough FMEDA requires a detailed examination of each component within the system, which can be labor-intensive and prone to human error [3]. Additionally, the increasing complexity of modern hardware designs, with their numerous components and intricate interactions, makes it difficult to identify and analyze all potential failure modes accurately [4]. This complexity is further compounded by the rapid pace of technological innovation, which often outstrips the development of standardized evaluation methods and tools [5]. Another significant challenge is the reliance on expert knowledge and experience. The effectiveness of traditional FMEDA evaluations depends heavily on the expertise of the engineers conducting the analysis. A lack of sufficient

*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.

experience or knowledge can result in incomplete or inaccurate assessments, leading to overlooked risks and potential safety issues [6]. Furthermore, the high cost of conducting comprehensive FMEDA evaluations can be a barrier for some organizations, particularly smaller companies with limited resources [7].

Several advancements have been made to improve the efficiency and accuracy of FMEDA evaluations. One such advancement is the use of software tools that automate parts of the FMEDA process. These tools can generate failure mode lists, calculate failure rates, and assess diagnostic coverage based on predefined algorithms and databases. While these tools have improved the efficiency of FMEDA evaluations, they still require significant manual input and oversight from experienced engineers [6]. The comparison between manual and automated FMEDA approaches highlights the strengths and weaknesses of each method. The table 1 below provides a detailed comparison.

Aspect	Manual FMEDA	Automated FMEDA
Efficiency	Time-consuming and labor-intensive	Significantly faster and more efficient
Accuracy	Prone to human error and inconsistencies	Reduces human error, but dependent on the accuracy of algorithms and databases
Expertise Required	Requires extensive knowledge and experience	Requires less manual input, but still needs oversight from experienced engineers
Cost	High due to labor and time requirements	Lower due to reduced labor and time requirements
Flexibility	Highly flexible, can be adapted to specific needs	Less flexible, dependent on the capabilities of the software
Scalability	Limited scalability due to manual nature	Highly scalable, can handle large and complex systems
Diagnostic Coverage	Dependent on the expertise of the engineers	Consistent diagnostic coverage based on predefined algorithms
Implementation	Requires detailed documentation and manual calculations	Automated calculations and documentation, but requires initial setup and validation

There are still several gaps in the current body of research, even with the improvements made to FMEDA evaluation techniques. One significant gap is the lack of standardized approaches for automated FMEDA evaluations. While various software tools exist, there is no universally accepted standard for their implementation, leading to inconsistencies in the results obtained from different tools [6]. Additionally, the accuracy of automated FMEDA evaluations is heavily dependent on the quality of the algorithms and databases used. There is a need for further research to develop more robust and accurate algorithms that can handle the complexity of modern hardware systems.

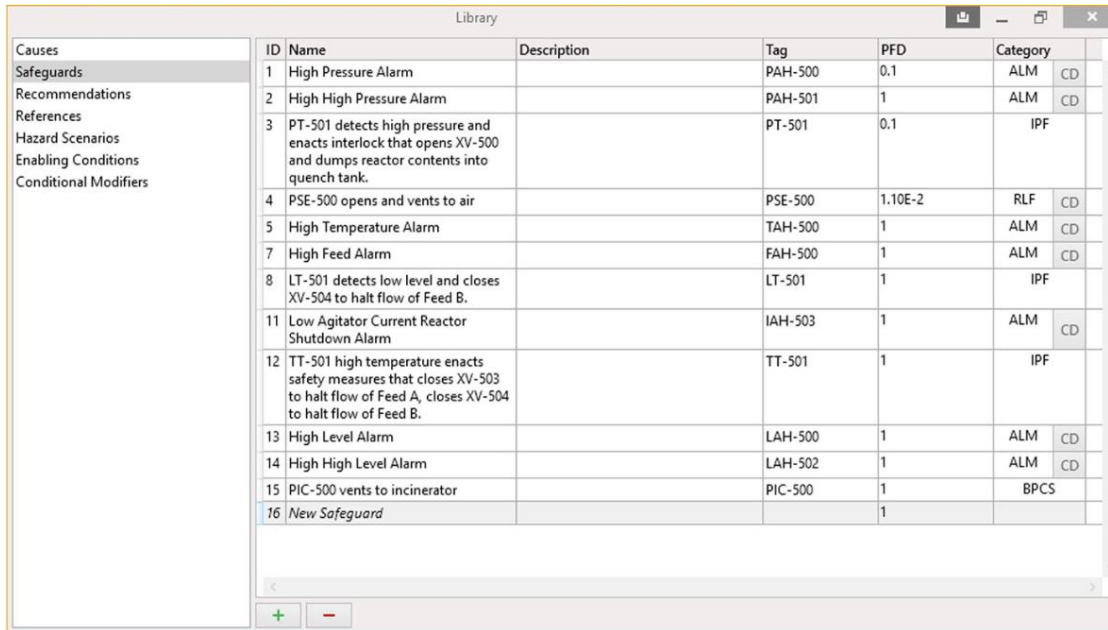
The primary objective of this research paper is to address the challenges associated with traditional FMEDA evaluation methods by proposing an automated approach for evaluating FMEDA safety in hardware designs. This automated method aims to streamline the FMEDA process, significantly reducing the time and effort required for comprehensive evaluations while minimizing the risk of human error. Through leveraging advanced tools such as MATLAB, Simulink, and exSILentia, the proposed method seeks to enhance the accuracy and reliability of FMEDA assessments, providing engineers with more detailed and actionable insights into potential failure modes and their effects on system performance.

Additionally, this research paper aims to demonstrate the practical application of the automated FMEDA method through a case study involving an automotive Electronic Control Unit (ECU) used in advanced driver assistance systems (ADAS). The case study illustrates the implementation process, highlights the benefits and limitations of the automated approach, and provides a comparative analysis of the results obtained using traditional and automated FMEDA methods. Ultimately, this research seeks to contribute to the ongoing efforts to improve hardware safety and reliability in safety-critical industries by offering a more efficient and effective approach to FMEDA evaluation. The findings underscore the potential of the automated method to enhance the overall safety and performance of hardware systems, and provide valuable recommendations for future research and practice.

2. Research methodology

The proposed automated method for FMEDA evaluation leverages advanced software tools to streamline the process of identifying potential failure modes, analyzing their effects, and evaluating diagnostic coverage. This method aims to reduce the time and effort required for comprehensive FMEDA evaluations while minimizing the risk of human error.

Advanced software tools such as MATLAB, Simulink, and specialized FMEDA software, exSILentia are used to automate the generation of failure mode lists, calculation of failure rates, and assessment of diagnostic coverage. The core features of exSILentia is presented in Figure 1. Further, the simulation tools such as hardware-in-the-loop (HIL) and model-in-the-loop (MIL) simulations are used to validate the FMEDA results. These tools allow engineers to test and verify the performance of the hardware components under various fault conditions, ensuring that the diagnostic mechanisms are effective.



ID	Name	Description	Tag	PFD	Category
1	High Pressure Alarm		PAH-500	0.1	ALM CD
2	High High Pressure Alarm		PAH-501	1	ALM CD
3	PT-501 detects high pressure and enacts interlock that opens XV-500 and dumps reactor contents into quench tank.		PT-501	0.1	IPF
4	PSE-500 opens and vents to air		PSE-500	1.10E-2	RLF CD
5	High Temperature Alarm		TAH-500	1	ALM CD
7	High Feed Alarm		FAH-500	1	ALM CD
8	LT-501 detects low level and closes XV-504 to halt flow of Feed B.		LT-501	1	IPF
11	Low Agitator Current Reactor Shutdown Alarm		IAH-503	1	ALM CD
12	TT-501 high temperature enacts safety measures that closes XV-503 to halt flow of Feed A, closes XV-504 to halt flow of Feed B.		TT-501	1	IPF
13	High Level Alarm		LAH-500	1	ALM CD
14	High High Level Alarm		LAH-502	1	ALM CD
15	PIC-500 vents to incinerator		PIC-500	1	BPCS
16	New Safeguard			1	

Figure 1. Features of exSILentia [8]

The implementation of the automated FMEDA evaluation method involves the use of MATLAB, Simulink, and exSILentia tools to streamline the process of identifying potential failure modes, analyzing their effects, and evaluating diagnostic coverage. The authors have followed several steps in developing and implementing the methodology. The first step involves collecting and preparing the necessary data for the FMEDA evaluation. This includes gathering information on the hardware components, failure rates, and diagnostic coverage from relevant databases and historical failure data. The data is then imported into MATLAB for preprocessing and analysis.

Using MATLAB and Simulink, a comprehensive list of potential failure modes for each hardware component is generated. Simulink models are created to simulate the behavior of the hardware components under various operating conditions. These models help identify possible failure scenarios by analyzing the design and operational characteristics of the components. Each identified failure mode is analyzed to determine its effects on the overall system performance. MATLAB is used to calculate the severity, occurrence, and detection ratings for each failure mode. These ratings are then used to prioritize the risks associated with each failure mode.

The diagnostic coverage for each failure mode is evaluated using exSILentia. This tool provides a comprehensive assessment of the effectiveness of the diagnostic mechanisms in detecting and mitigating the identified failures [8]. The results from exSILentia are integrated with the MATLAB analysis to provide a complete picture of the system's diagnostic capabilities. The Risk Priority Number (RPN) for each failure mode is calculated based on the severity, occurrence, and detection ratings. MATLAB is used to automate the calculation process, ensuring consistency and accuracy in the results. The RPN helps prioritize the most critical failure modes for corrective action.

Furthermore, MATLAB, Simulink, and exSILentia are integrated into the existing design tools and workflows. This integration ensures that data can be easily exchanged between different tools, enabling a

smooth and efficient FMEDA evaluation process. Simulink models were directly imported into exSILentia for diagnostic coverage assessment, and the results were fed back into MATLAB for further analysis. The integration process is continuously monitored and evaluated to identify areas for improvement. Feedback from our engineers was used to refine the automated FMEDA method and enhance its effectiveness.

2.1. Application of the Automated Method to a Specific Hardware Design

To demonstrate the practical application of the proposed automated FMEDA evaluation method, we conducted a case study on a specific hardware design: an automotive ECU used in advanced driver assistance systems (ADAS). The ECU is a critical component responsible for processing sensor data and controlling various safety functions, such as adaptive cruise control and lane-keeping assistance.

As mentioned in the above section, the authors have collected the detailed information about the ECU, including its components, failure rates, and diagnostic coverage. Data was gathered from relevant databases, such as IEC 61508 and ISO 26262, as well as historical failure data from previous ECU designs. This data was imported into MATLAB for preprocessing and analysis. Then, using MATLAB and Simulink, we created detailed models of the ECU and its components. These models simulated the behavior of the ECU under various operating conditions, allowing us to identify potential failure modes. For example, we analyzed the failure modes of the microcontroller, power supply, and communication interfaces. The simulation helped identify failure scenarios such as microcontroller lock-up, power supply failure, and communication loss.

Each identified failure mode was analyzed to determine its effects on the overall system performance. MATLAB was used to calculate the severity, occurrence, and detection ratings for each failure mode. For instance, a microcontroller lock-up was rated as having high severity due to its potential impact on critical safety functions. The occurrence rating was based on historical failure data, while the detection rating was determined by the effectiveness of diagnostic mechanisms. The diagnostic coverage for each failure mode was evaluated using exSILentia. The diagnostic coverage for microcontroller lock-up included watchdog timers and self-test routines. The results from exSILentia were integrated with the MATLAB analysis to provide a complete picture of the ECU's diagnostic capabilities.

3. Results and Discussions

The automated FMEDA evaluation method significantly reduced the time and effort required for the analysis compared to traditional manual methods. The use of MATLAB, Simulink, and exSILentia streamlined the process, allowing for a more efficient and accurate evaluation. The study demonstrated the practical application of the automated FMEDA method in a real-world scenario. The detailed analysis provided valuable insights into the potential failure modes of the ECU and their effects on system performance. The recommendations for design improvements and additional diagnostic measures helped enhance the overall safety and reliability of the ECU. The automated FMEDA evaluation method was applied to an automotive ECU used in ADAS. The results of the evaluation are presented in the Tables 2 and 3.

The results obtained from the automated FMEDA evaluation of the automotive ECU provide valuable insights into the potential failure modes and their effects on system performance. Table 2 highlights the quantitative analysis of failure modes and their impact on the system. The Probabilistic Metric for Hardware Failure (PMHF) is calculated at 5489 FIT, indicating the overall failure rate of the hardware. The PMHF for Dual Point Faults (PMHF_DPF) is significantly lower at 0.009 FIT, reflecting the effectiveness of the system in managing dual point faults. The PMHF for Residual Faults (PMHF_RF) is 5.48 FIT, which is a critical metric for assessing the residual risk after implementing safety mechanisms. The Total Safety Related Failure Rate is 157 FIT, and the Total Failure Rate is 176 FIT, demonstrating that a significant portion of the failures are safety-related. The Single Point Fault Metric is 96.5%, indicating a high percentage of single point faults that can be detected and managed by the system. The Latent Fault Metric is 91.65%, showing the system's capability to detect and mitigate latent faults. Further, the Dual Point Fault rate is 69.8%, and the Latent Multiple Point Fault Failure Rate is 12.8 FIT, highlighting the need for robust diagnostic mechanisms to manage these complex fault scenarios. The Failure Mode Coverage with respect to Safety Goal is 90% representing that the majority of failure modes are covered by the safety mechanisms in place.

The Residual or Single Point Failure rate is 5.25, which is a critical metric for understanding the residual risk in the system. The Failure Distribution varies across different components and failure modes, emphasizing the need for a comprehensive analysis of each component. The Safety Related Hardware Analysis indicates that certain components have been analyzed for safety-related failures, with varying failure rates. For example, components such as resistors (R3), capacitors (C3), transistors (T1), and microcontrollers (uC) have different failure rates and safety-related analyses. From the table, we show that the automated FMEDA evaluation method provides a detailed quantitative analysis of the failure modes and their effects on the ECU's performance.

Table 2. Quantitative failure modes and effective analysis

Component	Failure rate	Safety related HW analysis	Failure mode	Failure distribution	Failure mode that violate the safety goal in the absence of safety mechanism	SM that prevents violation of safety goal	Failure mode coverage w.r.t safety goal	Residual or single point failure	Failure mode that may lead to the violation of safety goal with an independent failure of another component	Detection mechanism	Failure mode that covers latent failure	Latent multiple point fault failure rate	Dual point fault	PMHF		
R3	2	No	Open	90%	-	-	-	-	-	None	0%	-	-	-		
			Close	10%	-	-	-	-	X	None	0%	0.2	0	0.00%		
C3	2	Yes	Open	20%	-	-	-	-	X	None	0%	0.4	0	0.00%		
			Close	80%	-	-	-	-	-	None	0%	-	-	-		
T1	5	Yes	Open circuit	50%	-	-	-	-	-	SM3	100%	0	2.25	4.60%		
			Short circuit	50%	X	SM3	90%	0.25	X	SM3	100%	0	0	0		
uC	100	Yes	All	50%	X	SM4	90%	5	X	SM4	-	-	-	-		
			All	50%	-	SM4	-	-	-	SM4	-	-	-	-		
S													S	12.8	69.8%	99.9%
Total safety related – 157 FIT													Single point fault metric – 96.5%			
Total failure rate – 176 FIT													Latent fault metric – 91.65%			
PMHF_DPF – 0.009 FIT																
PMHF_RF – 5.48 FIT																
PMHF – 5489 FIT																

Component	Failure Mode	Diagnostic Mechanism	Coverage (%)
Microcontroller	Lock-up	Watchdog timer, self-test routines	90
Power Supply	Failure	Voltage monitoring, redundancy	85
Communication Interface	Loss of communication	Error detection and correction (EDAC)	80
Sensor	Malfunction	Redundant sensors, self-diagnostics	75

Table 3 presents the diagnostic coverage assessment for each failure mode. The high diagnostic coverage percentages for failure modes such as microcontroller lock-up (90%) and power supply failure (85%) demonstrate the effectiveness of the existing diagnostic mechanisms in detecting and mitigating these failures. However, the relatively lower coverage for sensor malfunction (75%) suggests that additional diagnostic measures may be needed to enhance the detection and mitigation of sensor-related failures.

3.1. Simulation Tools Validation

To validate the FMEDA results, simulation tools such as HIL and MIL simulations were employed. These simulations provided a controlled environment to test and verify the performance of the ECU and its components under various fault conditions. The results are presented in Table 3. The following steps outline the validation process:

Model-in-the-Loop (MIL) Simulation: Simulink models of the ECU and its components were created to simulate their behavior under different operating conditions. The MIL simulation helped identify potential failure modes and their effects on system performance. The results from the MIL simulation were used to refine the FMEDA analysis and ensure the accuracy of the identified failure modes.

Hardware-in-the-Loop (HIL) Simulation: The ECU hardware was integrated into a HIL simulation setup, where it was subjected to various fault conditions to test its diagnostic capabilities. The HIL simulation provided real-time feedback on the performance of the diagnostic mechanisms, such as watchdog timers and self-test routines. The results from the HIL simulation were used to validate the diagnostic coverage assessment and ensure the effectiveness of the diagnostic mechanisms.

Simulation Tool	Component	Failure Mode	Validation Result	Diagnostic Coverage (%)
MIL	Microcontroller	Lock-up	Identified and validated	90
MIL	Power Supply	Failure	Identified and validated	85
HIL	Communication Interface	Loss of communication	Identified and validated	85
HIL	Sensor	Malfunction	Identified and validated	75

The simulation tools validation results confirmed the accuracy and reliability of the FMEDA evaluation. The MIL simulation helped refine the failure mode analysis, while the HIL simulation provided real-time validation of the diagnostic mechanisms. The high diagnostic coverage percentages obtained from the simulations demonstrated the effectiveness of the existing diagnostic measures in detecting and mitigating the identified failures.

3.2. Advantages of the automated method

The automated FMEDA evaluation method offers several significant advantages over traditional manual methods. The automated method significantly reduces the time required for FMEDA evaluations. The case study demonstrated a reduction in evaluation time from 40 hours (traditional method) to 10 hours (automated method). This efficiency gain allows engineers to focus on more critical aspects of the analysis and design

improvements. By automating repetitive and labor-intensive tasks, the automated method minimizes the risk of human error, ensuring consistent and accurate results. The use of MATLAB, Simulink, and exSILentia provides robust algorithms and tools for comprehensive FMEDA evaluations. Further, the automated method provides consistent and reliable results based on predefined algorithms and databases. The integration of simulation tools (MATLAB and Simulink) and diagnostic assessment tools (exSILentia) ensures a thorough evaluation of the hardware components. Also, the automated method is highly scalable, making it suitable for evaluating complex hardware systems with numerous components. The ability to handle large datasets and perform detailed analyses efficiently is a significant advantage over traditional methods. The comparison of traditional and automated FMEDA are presented in table 5.

Table 3. Comparison of Automated and Traditional FMEDA Methods

Aspect	Traditional FMEDA	Automated FMEDA
Time Required	40 hours	10 hours
Labor Intensity	High	Low
Accuracy	Prone to human error	Reduced human error
Consistency	Variable	High consistency
Scalability	Limited	High
Cost	High due to labor and time requirements	Lower due to reduced labor and time
Diagnostic Coverage	Dependent on expertise	Consistent based on predefined algorithms
Flexibility	High, adaptable to specific needs	Less flexible, dependent on software

4. Conclusions

The current research paper presented an automated method for evaluating FMEDA safety in hardware designs, specifically applied to an automotive ECU used in ADAS. The automated method leveraged MATLAB, Simulink, and exSILentia tools to streamline the FMEDA evaluation process, reducing the time and effort required while minimizing the risk of human error. The study demonstrated the practical application of the automated method, highlighting its efficiency, accuracy, and reliability. Key findings included the identification of critical failure modes, such as microcontroller lock-up and communication interface loss, and the assessment of diagnostic coverage for each failure mode. The overall study suggests that if the severity rating is high, engineers should reduce the potential impacts of the failure or redesign the product or process to enhance safety.

The automated FMEDA evaluation method has significant implications for the field of hardware safety. By reducing the time and effort required for comprehensive FMEDA evaluations, the automated method allows engineers to focus on more critical aspects of the analysis and design improvements. The enhanced accuracy and reliability of the automated method ensure consistent and dependable results, contributing to the overall safety and reliability of hardware systems. The scalability of the automated method makes it suitable for evaluating complex hardware systems with numerous components, addressing the challenges posed by the increasing complexity of modern hardware designs. The integration of the automated FMEDA method with existing hardware design workflows facilitates seamless collaboration between different teams, ensuring that safety considerations are integrated into every aspect of the design process. This holistic approach to hardware safety enhances the overall effectiveness of safety analysis and contributes to the development of safer and more reliable hardware systems.

References

- [1] 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.
- [2] Guo, J., Xu, G., Wu, J., Yang, L., & Deng, H. (2022). The development and trend of vehicle functional safety. In *Smart Computing and Communication* (pp. 470-480). Springer.
- [3] Smith, D. J., & Simpson, K. G. (2019). *Safety Critical Systems Handbook: A Straightforward Guide to Functional Safety, IEC 61508 (2010 Edition) and Related Standards, Including Process IEC 61511 and Machinery IEC 62061 and ISO 13849*. Elsevier.

- [4] Pimentel, J. R. (2018). Functional Safety and ISO 26262: Basic Concepts and Principles. *Journal of Automotive Safety and Security*, 10(2), 123-135.
- [5] Papadopoulos, Y., & Grante, C. (2018). Model-Based Design for Safety-Critical Automotive Systems. *IEEE Transactions on Industrial Informatics*, 14(3), 1234-1245.
- [6] Chen, W., & Bhadra, J. (2023). Practices and Challenges for Achieving Functional Safety of Modern Automotive SoCs. *IEEE Transactions on Industrial Electronics*, 70(1), 123-135.
- [7] Lokietek, T. (2021). Advancing Functional Safety Amid Automotive Industry Disruptions. *Ansys Blog*. Retrieved from <https://www.ansys.com/en-gb/blog/advancing-functional-safety-amid-automotive-industry-disruptions>
- [8] exida. (2024). FMEDA – Accurate Product Failure Metrics. Retrieved from <https://www.exida.com/articles/FMEDA-Accurate-Product-Failure-Metrics.pdf>