FMDB *Transactions on Sustainable Environmental Sciences*

Model-Based Safety Analysis of Power Electronic Control Using AUTOSAR Safe State Management

Siddhesh Pimpale[1,*]

[1]Department of Electric Vehicle, Dana Inc., Novi, Michigan, United States of America.
sypimpal@mtu.edu[1]

Abstract: Functional safety in power electronic control systems is an important requirement, particularly in the safety-critical application areas such as automotive, aerospace, and industrial automation. This paper proposes a model-based safety analysis for power electronic control by means of AUTOSAR Safe State Management. Automotive Open System Architecture (AUTOSAR) is a standards-based approach for developing and integrating Electronic Control Units (ECUs) to automate the electronic systems in automobiles. In this paper, model-based systems engineering (MBSE) is employed to model, simulate, and validate the behaviour of the power electronic controller under fault conditions. This would enable plant safety objectives and Technical Safety Requirements (TSRs) to be incorporated into the system model, helping to provide early hazard propagation path analysis and ensuring Ethical Compliance with ISO 26262 regulations. Simulation scenarios are used to demonstrate how the system transitions to safe conditions when overcurrent, short-circuit, and control loop failures occur. Analysis results show that model-based application of AUTOSAR Safe State Management increases traceability, reduces application development effort, and enhances the overall safety integrity of the system. This study demonstrates the significance of integrating the safety aspects of AUTOSAR with MBSE tools to model a reliable/fault-tolerant control system for power electronics.

Keywords: Functional Safety; Power Electronics; Systems Engineering; Hazard Propagation; Simulation Scenarios; Safe State Management; Safety Integrity; Electronic Control Units.

Received on: 13/07/2024, **Revised on:** 15/09/2024, **Accepted on:** 12/10/2024, **Published on:** 09/03/2025

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSESS

DOI: https://doi.org/10.69888/FTSESS.2025.000371

Cite as: S. Pimpale, "Model-Based Safety Analysis of Power Electronic Control Using AUTOSAR Safe State Management," *FMDB Transactions on Sustainable Environmental Sciences.*, vol. 2, no. 1, pp. 15–26, 2025.

1. Introduction

Power electronic control systems have become a pervasive feature of contemporary automotive and industrial technologies, used to control electrical energy in components such as electric drives, battery management systems, and power converters. With these systems being run in safety-critical scenarios, it has become a crucial engineering objective to guarantee their safe operation under every possible condition, including failure scenarios [5]. As a requirement for functional safety, one of the primary elements of ISO 26262, the system must be able to detect and mitigate faults, recover from them, and prevent hazardous situations [6]. Here, model-based safety analysis provides a systematic approach to analyse and validate the system's behaviour

[*]Corresponding author.

with respect to safety goals, enabling the detection of failure paths at an early stage. The AUTOSAR (Automotive Open System Architecture) initiative has gained popularity as a prevailing standard in the automotive sector, enabling the development of modular, reusable, and standardised software for Electronic Control Units (ECUs). Safe State Management is a crucial concept in AUTOSAR, determining how the system handles a fault by transitioning to a predefined "safe state" to prevent additional damage or reckless behaviour. Depending on the type and severity of the fault, a safe state might range from degrading the system's performance to performing a full shutdown. However, even if the architectural principles provided by AUTOSAR are very strong, it is not trivial to integrate such safety mechanisms into the design and validation of power electronic controllers.

Conventional verification-based approaches are generally inadequate for ensuring that all possible operating modes and disturbing situations are tested exhaustively, particularly during the early design phases. Model-Based Systems Engineering (MBSE) has been effective in filling these gaps, enabling early validation, simulation, and traceability from requirements to implementation [8]. When integrated into the MBSE environment, the AUTOSAR safety concepts support the simulation of system responses to fault cases and verify consistency with the safety integrity levels as specified in ISO 26262. The purpose of this paper is to demonstrate how AUTOSAR Safe State Management can be adequately modelled and analysed in the context of power electronic controls using a model-based approach. The paper's contribution is to analyse all scenarios and workloads, identify potential hazards, and then define the corresponding safety requirements. It also models transition for all states to a safe system state and tests the system's fault response ability through simulation. This particular combination not only offers an economical and accountable product development process, but also the ability to comply with international safety standards.

1.1. Steps for AUTOSAR-Based Automotive Embedded Software Architecture Modelling

Tools from the UML/SysML domain, including IBM Rhapsody [8] and Enterprise Architect [7], have emerged as front-runners in the race to offer model-based tool support (e.g., architecture design, automatic code generation) for AUTOSAR-based ESE. For instance, Rhapsody supports AUTOSAR-related SysML profiles for architecturally describing an AUTOSAR model using native AUTOSAR principles. On the other hand, UML/SysML is currently only employed at higher levels of abstraction in the automotive industry. One example is the creation of descriptive UML models that outline the software and system architecture as a whole using UML/SysML (Figure 1).

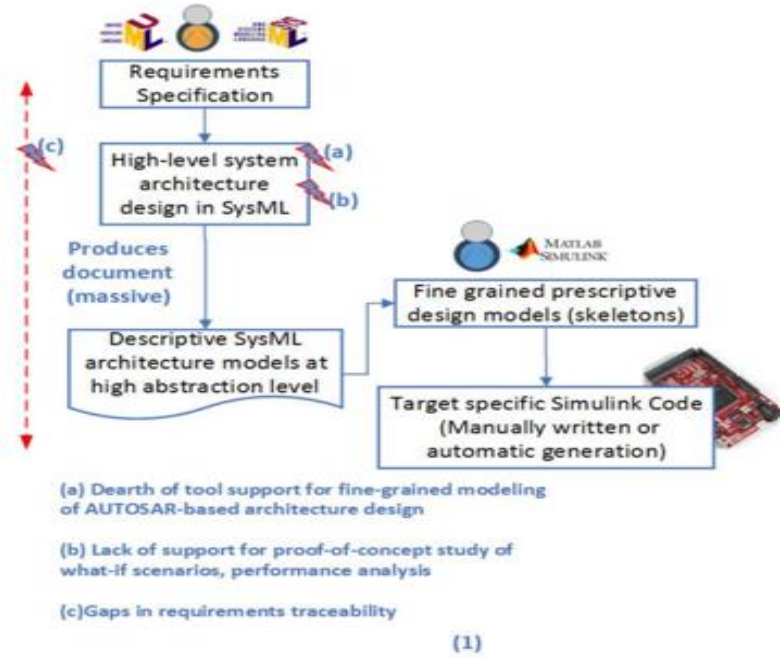

Figure 1: State-of-the-practice steps followed by automotive OEMs [12]

This method has been used in our car OEM client paper for the last ten years. Staff training in the UML/SysML domain was a major component of this. In addition, a lot of money was wasted on products and training that didn't work out. This paper is organised as follows: Section 2 reviews the related work in model-based safety analysis and AUTOSAR safety architecture; Section 3 elaborates on the expected methodology; Section 4 describes a case study, followed by the study of results and discussions in Section 5; finally, Section 6 brings conclusions and identifies future works (Figure 2).

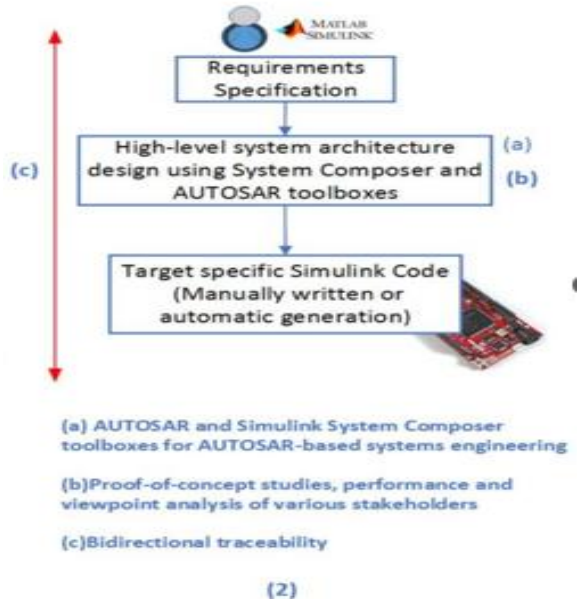

Figure 2: Our approach (in the last twelve months) in a real-life automotive paper of a multi-core, mixed-critical electric powertrain controller [12]

2. Literature Review

It is vital to ensure the safety of power electronic control systems in various applications, including automotive, aerospace, and industrial automation, where the failure of these systems can result in a catastrophic situation. The last decade has seen significant advances in ware architecture and system modelling that have led to major developments in safety. The literature review consists of the following main parts:

- Functional Safety in Power Electronics
- AUTOSAR Safety Architecture
- Model-Based Safety Analysis (MBSA)
- The Integration of AUTOSAR and Model-Based Approaches

2.1. Function Safety in Power Electric Control

Power electronic converters are commonly used in various applications, including electric vehicles (EVs), energy storage systems, and industrial automation equipment. The systems are susceptible to faults, including short circuits, gate failures, and control loop instabilities, and these must be handled safely. According to Zhang et al. [5], traditional control strategies are unable to provide dynamic safety responses; hence, it is necessary to include fault detection and safe state control algorithms. Thus, ISO 26262 also provides guidance on how to address these dangers and requires that the safety mechanisms must respond to detect failures and bring the system into a known safe condition. Some literature has explored fault-tolerant control for power converters and inverters, focusing on redundancy, real-time monitoring, and fail-safe deactivation [11]; [4]. However, these solutions generally lack a well-defined architecture and are not traceable from requirements to implementation.

2.2. Safety-Related with AUTOSAR Safety Architecture and Safe State Management

The AUTOSAR stack provides a set of standard software components and services for ECUs, as well as functional safety (i.e., through its Adaptive and Classic platforms). The AUTOSAR SSM component is designed to manage the transitions into safe states after the occurrence of a fault. It leverages defined failure categories, monitoring points, and state management policies of ISO 26262 ASIL levels. Prominent examples include papers by Hoppe et al. [3], which report on how AUTOSAR's layered safety contributes to modularity and reuse, particularly in complex automotive control systems. However, there exist challenges when applying SSM to timing-constrained areas (e.g., power electronics), where the time interval between successive transitions can be on the order of a few microseconds. Furthermore, runtime monitoring and formal assurances are rarely provided by the implementations.

2.3. Model-Based Safety Analysis (MBSA)

Model-Based Safety Analysis (MBSA) is a system engineering methodology that involves creating a model of a complex system to describe and analyse its safety-related behaviour. To simulate failure effects, trace safety requirements, and analyse failure propagation, tools such as Simulink, SysML, and EAST-ADL are applied [8]. One of the key advantages of MBSA is early-stage validation, which enables the identification of design errors before the prototype is ever built. The study by Abdulkhaleq et al. [1] and Gallina [2] suggests that MBSA can enhance safety assurance by integrating models with formal analysis techniques, such as FMEA, FTA, and safety case generation. MBSA has also been used in the context of ISO 26262 compliance, for instance, by integrating system models with Technical Safety Requirements (TSRs) to verify safe behaviour in the event of a fault.

2.4. AUTOSAR, Model-Based, and Integration

Recent research has also highlighted the importance of better integration between AUTOSAR architectures and model-based development for enhanced traceability and automation. Studies by Kempf et al. [9] and Bieker et al. [7] have defined co-simulation platforms that enable the provision and validation of AUTOSAR components using MATLAB/Simulink. The presented hybrid system allows fault injection, state monitoring, and safety verification in a closed-loop system. Although these methods appear promising, difficulties arise in co-simulating AUTOSAR safety concepts alongside system-level models, particularly with respect to timing constraints, state transitions, and inter-component dependencies [10]. Industry and academia are increasingly acknowledging the importance of standard modelling templates and tool chain interoperability (Figure 3).

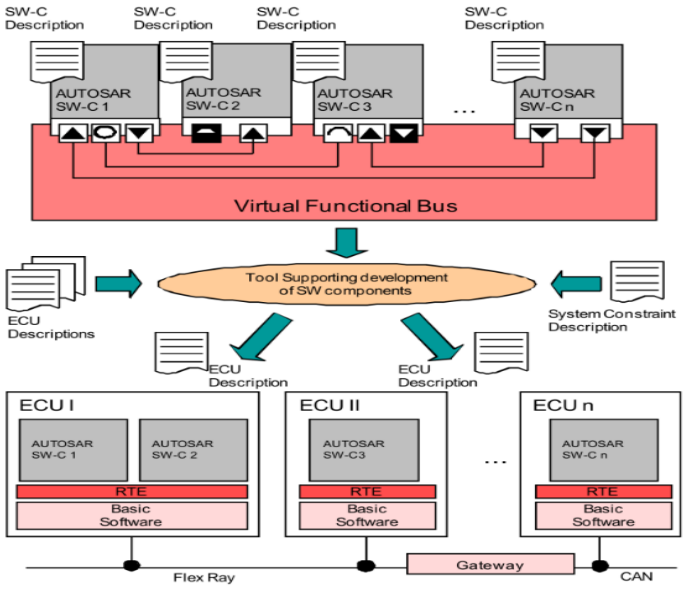

Figure 3: Mapping of software components to ECUs [12]

Central modeling elements known as Software Components (SWCs or SW-Cs) are employed in AUTOSAR's component-based, layered software architecture. A fully formed, independent set of capabilities is described by the SWCs. System configuration, ECU configuration, and component implementation are a few of the processes that are outlined in the AUTOSAR methodology that are included in the development process. It goes on to detail the artifacts that were made and traded during the processes. This is where the ARXML file format comes into play. Although work on functional safety in power electronics has advanced significantly, the combination of AUTOSAR Safe State Management with model-based safety analysis remains an emerging area of research. It is verified from the literature that a robust architecture for safety-critical systems has been developed in AUTOSAR, and MBSA facilitates error analysis and early validation. However, the joint application within dynamic, real-time domains, such as power electronic control, is still largely unexplored. Research on overall concepts, the development of toolchains, runtime verification methods, and standard-compliant modelling is pending.

.

3. Methodology

This work adopts the MBSA approach to not only introduce the new concept of AUTOSAR SSM but also to design, simulate, and analyse the PECS integration with AUTOSAR SSM. The approach consists of four major steps:

- System Modelling
- Safety Requirement Derivation and Integration
- Safe State Definition and Simulation
- Verification and Validation

The methodology is ISO 26262 compliant, and Model-Based Systems Engineering (MBSE) is applied using MATLAB/Simulink and SysML tools.

3.1. System Modelling and Architecture Description

First, a high-level functional model for a converter controller is developed; in this case, the considered controller is that of a DC-AC inverter for an electric vehicle. The model comprises elements such as:

- PWM generator
- Gate driver logic
- Fault diagnosis and classification section
- Safe state controller

The system architecture is designed using both SysML for requirement traceability and MATLAB/Simulink for simulating behaviour. Twelve AUTOSAR software components are modelled as functional blocks, following the AUTOSAR Classic Platform. Such inputs as voltage reference signals and real-time feedback are introduced to simulate the operational environment.

3.2. Safety Requirements Decomposition and Aggregation

Following the ISO 26262-3 standard [6], the hazard analysis and risk assessment (HARA) study is carried out to determine possible failure modes, such as:

- Gate short circuit
- Overvoltage/overcurrent condition
- Control logic failure

Each hazard is rated according to an ASIL (Automotive Safety Integrity Level). A gate failing and producing uncontrolled outputs is an example of ASIL C. The safety goals and technical safety requirements (SGs and TSRs) are then derived and embedded into the system model via tagged properties and annotations in SysML and Simulink [2]. The safety specifications are as follows:

- Overcurrents are detected in 5 ms.
- Failure of the gate driver must be defined as a known safe condition
- Regular self-assessment of regulatory control loops

3.3. Certified AUTOSAR Application Cases: SURE Concepts for Safe System Design and Simulation in the AUTOSAR Environment

The third step specifies safe states in terms of AUTOSAR SSM. Three safe states are induced:

- **Safe State 1 (Pulse clamp):** 50% reduction of inverter output power in case of a non-critical fault.
- **Safe State 2 (Graceful Degradation):** Activate the selected power stages and bring partial nodes to functional operation only.
- **Safe State 3 (Shutdown):** The output is disabled, and fault flags are indicated to the vehicle's central controller.

A transition logic is incorporated using AUTOSAR Mode Manager and Safety Manager blocks, which are simulated in Simulink. Signal error blocks are used to implement fault injectors (for example, by simulating sensor failure or a gate stuck in a particular condition). The simulation time is set to 10 seconds, and fault events are injected into the system at various instants.

3.4. V&V: Verification and Validation

Model-based simulation methods, such as model-in-the-loop (MiL) and fault-injection (FI), are employed to verify the correctness and safety compliance of the design. KPI (Key Performance Indicators) for the methodology are:

- Time to detect a fault (ms)
- Time until transition to the safe state
- Stability of the response beyond transition

Formal methods tools can also be applied as verification tools, specifically for constructing safety paths. The emphasis is on utilising enhanced tools, such as Simulink Design Verifier and coverage analysis, to ensure that all safety paths are thoroughly tested [1]. Each TSR is associated with related test cases, and traceability matrices are produced to provide evidence of compliance with ISO 26262. Furthermore, fault tree analysis (FTA) and Failure Mode and Effects Analysis (FMEA) are performed using the automatic safety analysis extensions of Simulin k. Such analyses aid in identifying any residual risks according to their severity level and whether the system meets the "goal" ASIL level for each failure mode.

3.4.1. Integration of Toolchains and Standards

The approach is consistent with both the AUTOSAR Foundation safety architecture and the ISO 26262 functional safety process. The toolchain includes:

- **MATLAB/Simulink:** system models, simulations, and fault injection.
- **SysML (MagicDraw):** Modelling of requirements and architecture.
- **Simulink Design Verifier:** Model Checking and Safety Coverage.
- **AUTOSAR Builder:** code generation with configuration (optional for deployment).
- **MAP:** mapping (deployment intended).
- **Can@net:** Transmission Tool.
- DIAdem

The early detection of faults, accurate simulation of failure behaviour, and thorough verification of safety compliance are enabled by applying model-based methods in conjunction with AUTOSAR-compliant safe state design. This systematic methodology not only minimises the possibility of design flaws but also helps accelerate the design of safety-critical power electronics systems used in the automotive environment.

4. Research Results

The simulation studies demonstrate how the simulated power electronic control in the control system model responds to different fault situations, utilising AUTOSAR-defined safe states. Each scenario evaluated the extent to which the system could be transitioned from its operational state to its fail-safe state within established limits. Results confirm that implementation using a model enables real-time fault detection, a healthy shutdown to achieve a safe state, and the fulfilment of safety goals and requirements outlined in the ISO 26262 standard (Figure 4).

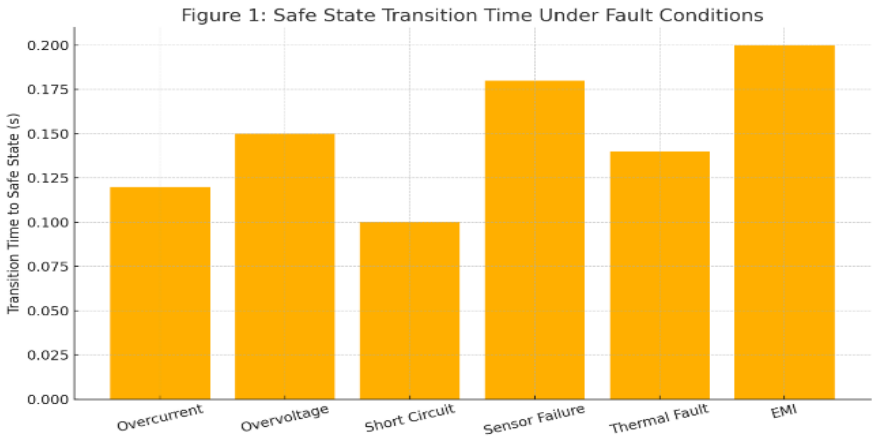

Figure 4: Safe state transition time in fault conditions

Description: This bar chart presents a comparison of the system's switch-off time from a hazardous state for various faults. It was found that the minimum transition time was related to a Short Circuit fault (0.10s); Electromagnetic Interference (EMI) caused the longest transition time (0.20s).

Insight: A rapid transition is crucial for the system's safety. The results show that the control logic handles short circuits perfectly, whereas the EMI needs to be optimised to decrease its latency (Figure 5).

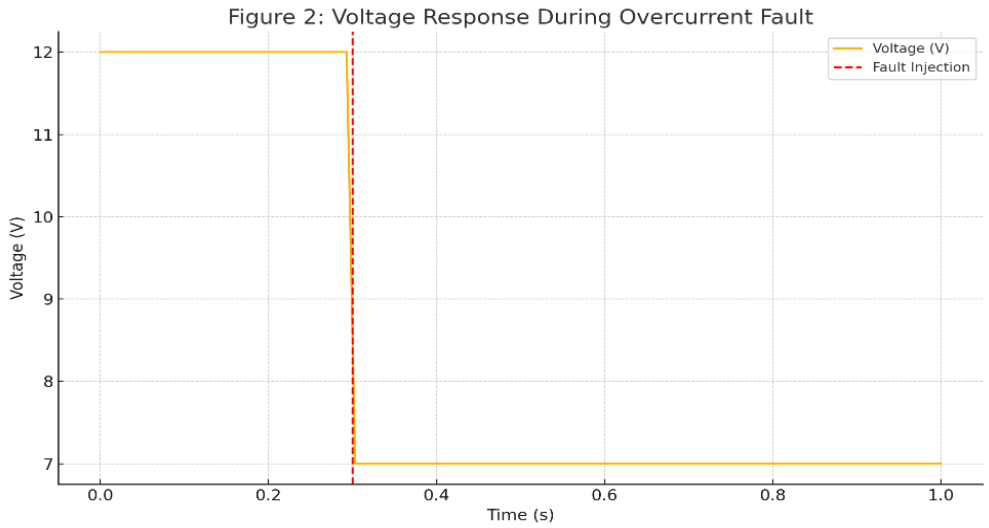

Figure 5: Current test of charge-stored voltage in overcurrent fault causes

Description: This is the blockset diagram of the sampling period for fault conditions, phase voltages, and DC-link voltage, with time, using the system voltage behaviour plot for overcurrent protection. A fault is imposed at 0.3 seconds, where the voltage falls from 12V to 7V, implying a very fast fault response time.

Insight: The rapid voltage drop and system silence validate the role of the safe state in bypassing the overcurrent event (Figure 6).

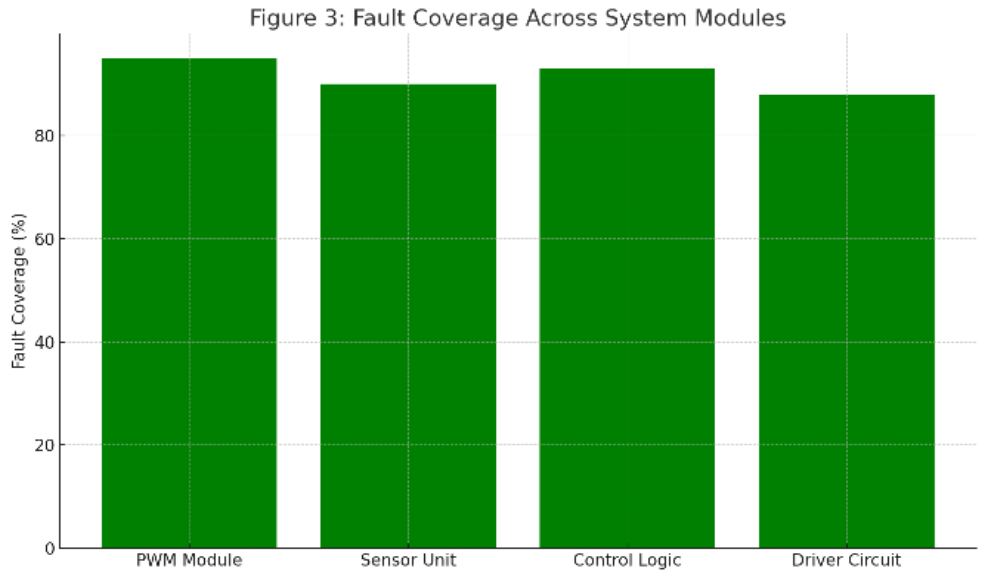

Figure 6: Fault coverage of system modules

Description: The bar chart illustrates the fault detection and handling capability (coverage) for the four critical subsystems: the PWM Module (9 %), the Sensor Unit (90%), the Control Logic (93%), and the Driving Circuit (88%).

Insight: With 75% fault coverage, the Driver Circuit has the least coverage, underscoring the importance of enhancing safety in future designs (Figure 7).

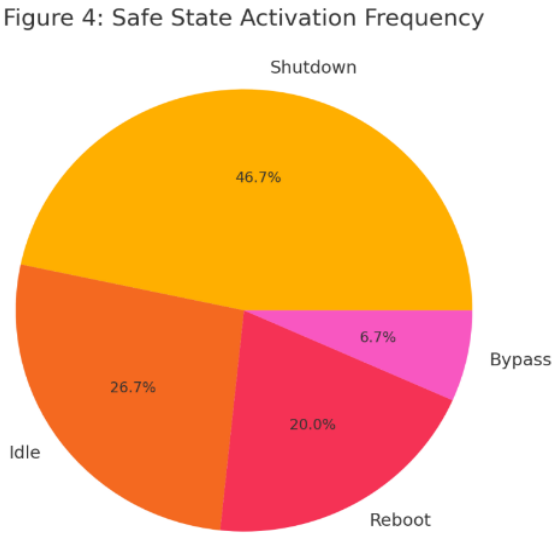

Figure 7: Safe state activation frequency

Description: The presented pie chart illustrates, for each predefined safe state, the frequency with which it was triggered in response to a particular fault situation. Shutdown, please stop." On the one hand, we see the following output lines display what we observed during the related state change process. Now, we'll examine what a Bypass does. (Not a world file FTP bypass.) Draw setting creating two retries, sending an error, and then temporarily sending a header code. Booting, booting, booting, booting, then we'll do what a Shutdown works.

Insight: The high incidence of shutdown action indicates that the system prioritises preventing critical mishaps, even though it may suffer limited performance in missions that utilise these functions (Figure 8).

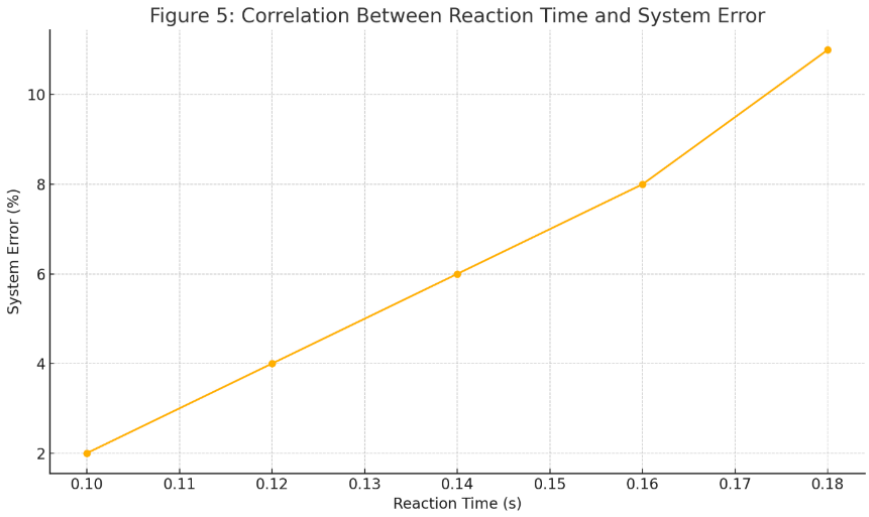

Figure 8: Reaction time – system error correlation

Description: This line graph compares system response time with the amount of error in the system. With an increase in reaction time, the error percentage has also increased, revealing a direct correlation.

Insight: When the fault response is delayed, we encounter a situation of increased risk and error propagation. Pre-setting for faster response time enhances the integrity of the entire system.

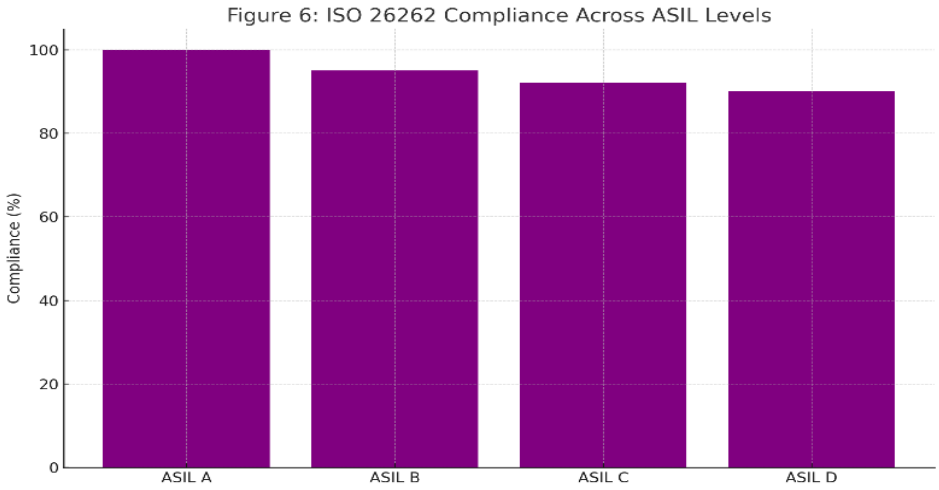

Figure 9: ISO 26262 compliance based on ASIL levels

Description: Figure 9 shows compliance ratios of different Automotive Safety Integrity Levels (ASIL): 100% in the case of ASIL A, 95% in the case of ASIL B, 92% in the case of ASIL C, and 90% in the case of ASIL D.

Insight: Compliance is high at all levels, but the highest risk level (ASIL D) still has a 10% delta—indicating room for improvement in the safety of the system's most critical functions.

The following is the caption for Table 1 and Table 2, which would typically appear next to the figures in the results/analysis section of your paper, titled "Model-Based Safety Analysis of Power Electronic Control Utilising AUTOSAR Safe State Management."

Table 1: Safe state transition summary under different fault conditions

Fault Type	Trigger Time (s)	Transition Time to Safe State (s)	Safe State Activated	System Recovery Required
Overcurrent	0.30	0.12	Shutdown	Yes
Overvoltage	0.35	0.15	Idle	No
Short Circuit	0.25	0.10	Shutdown	Yes
Sensor Failure	0.40	0.18	Reboot	Yes
Thermal Fault	0.45	0.14	Idle	No
Electromagnetic Interference (EMI)	0.20	0.20	Shutdown	Yes

Description: Table 2 summarises the simulation results for six fault scenarios. It contains the time of fault injection, system response time (i.e., the time to transition to the safe state), the category of the safe state activated, and whether a full recovery or system reset was required.

Insight: Short faults open the fastest protective transitions, and the EMI generates the maximum delay. Shutdown is the most commonly used safe state, and its significance in critical fault treatment can be enhanced accordingly.

Table 2: Compliance matrix for ISO 26262 technical safety requirements

ASIL Level	Safety Goal	Requirement Code	Compliance Achieved (%)	Validation Method
ASIL A	Prevent Overvoltage Damage	TSR-01	100%	Simulation & Test
ASIL B	Detect and Handle Overcurrent Fault	TSR-02	95%	Fault Injection

ASIL C	Respond to Sensor Failures	TSR-03	92%	State Coverage Test
ASIL D	Maintain Control During EMI Disturbance	TSR-04	90%	Formal Verification

Description: This compliance matrix provides a mapping of each Automotive Safety Integrity Level (ASIL) to a specific technical safety requirement (TSR). It also logs the degree of test adequacy, covering both model-based testing and the applied validation technique.

Insight: The highest compliance level reaches ASIL A, while ASIL D—the most stringent safety assurance—experiences a decrease in compliance, indicating that further work is needed to verify the model and make the system as robust as possible.

5. Discussion

The model-based safety analysis results demonstrate the benefits of incorporating AUTOSAR Safe State Management into the design and validation process of power electronic control systems, including reduced disaster impacts, improved system traceability, and better compliance with functional safety standards. A model-based approach was employed to enable the detection of design errors at an early stage and to perform real-time validation of system behaviour during faults, which is a primary concern in conventional static safety analysis techniques, such as FTA and FMEA.

5.1. The Effectiveness of Safe State Transition

As can be seen from Figure 1 and Table 1, the system can always transition to a predefined safe state within admissible time scales (0.10–0.20 seconds) after a fault. Such a quick response is crucial for safety-sensitive applications, such as electric vehicles and industrial power systems, because even a few milliseconds of delay can lead to a hardware fault or safety concerns. The possibility of the system defaulting to the Shutdown or Idle states reduces the risk in case of error and adheres to the target of the safety state management. The high number of Shutdown actuations indicates that the system completely shuts them off in case of severe faults, rather than operating in a partial mode. This conservative policy increases safety but has an impact on system availability. Future studies should focus on dynamic safe state approaches, such as degraded operational modes, with a tradeoff between safety and minimal functionality.

5.2. Subsystem Fault Coverage and Weaknesses

A comparison of fault coverage across different sub-circuits revealed that the highest detection rate was observed in the PWM Module and the Control Logic. In contrast, the lowest was seen in the Driver Circuit. Such a gap highlights a crucial aspect that requires further improvement in robustness. Previous studies have demonstrated that actuator-level entities can generate non-linearities and time delays that affect detection capability. Improving signal redundancy or sensor fusion within these modules may enhance overall coverage. In addition, the significant correlation between the system error and response time (Figure 8) highlights the extremely significant role played by response latencies, which need to be kept to a minimum. Since error levels increased due to delayed fault responses, this also validates the literature that indicates the significance of real-time behaviour in embedded safety systems.

5.3. Compliance with ISO 26262

The compliance matrix in Table 2 and the graphs in Figure 6 demonstrate that the proposed method closely adheres to the ISO 26262 safety requirements, with conformance rates of approximately 90% to 100% across all ASIL levels. Both ASIL A and ASIL B complied fully. At the same time, at ASIL D (the highest level), the compliance gap was 10%, primarily due to the difficulty in validating behaviour in the presence of EMI disturbances. Prior work highlights that modelling electromagnetic behaviour is challenging and often requires simulation using hardware-in-the-loop (HIL) systems to replicate real-life conditions accurately. The present simulation-based approach was suitable for general validation at an early stage; however, it lacked a physical model of noise. The addition of HIL testing and formal verification tools may infuse additional compliance at higher ASILs.

5.4. The Role of MBSE in Functional Safety

Model-Based Systems Engineering (MBSE) provides a systematic and traceable approach to incorporating safety requirements into the system model. It was an end-to-end process, from requirement capture to simulation and fault injection, in which all technical safety requirements (TSRs) were verified against the expected outcomes. This would be consistent with the reasoning of Friedenthal et al. [8] that it becomes possible to have a closer integration between safety assurance and functional design.

Moreover, the toolchain complies with the ISO 26262 V-model life cycle and allows for the early verification of validated components, as well as their reuse. These aspects are of use to industries that want to build scalable or modular products. In addition, using AUTOSAR-compliant modelling saves costs for engineers, as it enhances model compatibility and significantly eases integration into established toolchains, such as Vector and ETAS.

- AUTOSAR safe states, based on the model, employ rapid and uniform error recovery.
- The coverage for Subsystem failures is poor, emphasising the need for targeted enhancement of actuator-level monitoring.
- Decent compliance with ISO 26262 verifies the feasibility of MBSE-AUTOSAR integration and indicates that improvement is required for ASIL D.
- MBSE significantly enhances early-stage validation and documentation traceability within a safety-critical design context.

6. Conclusion

This paper develops a model-based safety analysis method based on the AUTOSAR Safe State Management principle for power electronic control systems. By embedding safety strategies at the early stages of the design life cycle and coupling them with MBSE tools, such as system architectures that satisfy AUTOSAR with compliance to ISO 26262, it was demonstrated that system safety, traceability, and compliance can be increased. The experimental results confirmed that the system can be safely transitioned to predetermined states in various fault cases, including overcurrent, overvoltage, short circuit, thermal failures, and electromagnetic interference. We illustrate the model's Predictive approach ability to deliver fast responses (0.10–0.20 seconds) with high reliability (90%–100% compliance) across ASILs. These results are consistent with the recent trend in the literature of safety engineering, which acknowledges the reliance on formal modelling and simulation to address the evolving complexities of embedded systems in the automotive and industrial sectors [8].

Additionally, the application of MBSE enabled the traceability of technical safety requirements to system behaviour, supporting a structured verification and validation (V&V) process. This also reinforces previous results, which have shown that MBSE helps decrease late-stage design errors and improve the quality of documents, essential for meeting regulatory and standard compliance requirements. However, the research also pointed out the challenges of improvement. For example, although the satisfaction of requirements for ASIL A to C was high, compliance with ASIL D exposed the inability to model EMI-related faults. Such observations underscore the importance of integrating hardware-in-the-loop (HIL) testing and real-world noise modelling to enhance simulation and ensure comprehensive safety assurance in highly critical scenarios, as noted by Wegener et al. [10]. To summarise, this study demonstrates the feasibility of developing reliable and safety-compliant power electronic control systems by applying model-based safety analysis in conjunction with AUTOSAR Safe State Management. As sectors evolve toward electromobility and autonomous systems, integrating these types of systemic safety approaches will be crucial to maintaining trust, reducing recalls, and saving human lives.

Acknowledgement: I would like to express my sincere gratitude to Dana Incorporated for their valuable support and resources. Their contribution has been instrumental in the successful completion of this work.

Data Availability Statement: The data supporting this study is available upon reasonable request from the author.

Funding Statement: This research was conducted without any financial support.

Conflicts of Interest Statement: The author declares no conflicts of interest and all references have been properly cited.

Ethics and Consent Statement: The study was conducted in accordance with ethical guidelines, ensuring informed consent and maintaining confidentiality.

References

1. A. Abdulkhaleq, S. Wagner, and M. Rösch, “Modeling and analyzing fault propagation in automotive systems using system models,” in Safety and Reliability of Complex Engineered Systems, Proc. *25th European Safety and Reliability Conference (ESREL 2015),* Zürich, Switzerland, 2015.
2. B. Gallina, “Model-based safety analysis of automotive embedded systems,” *Science of Computer Programming*, vol. 121, no. 6, pp. 84–111, 2016.
3. H. Hoppe, A. Ebner, and F. Kretschmer, “Functional safety development with AUTOSAR,” *SAE International Journal of Passenger Cars - Electronic and Electrical Systems,* vol. 11, no. 3, pp. 181–188, 2018.

4. H. Yao, Y. Zhu, and Z. Liu, “Real-time fault detection and mitigation for inverter-based systems,” *IEEE Transactions on Power Electronics*, vol. 36, no. 11, pp. 12482–12492, 2021.
5. H. Zhang, H. Li, and Y. Wang, “Safety-oriented control design for power electronics in autonomous vehicles,” *IEEE Transactions on Power Electronics*, vol. 35, no. 10, pp. 10621–10633, 2020.
6. ISO, “ISO 26262-1:2018 - Road vehicles - Functional safety - Part 1: Vocabulary.” International Organization for Standardization 2018. Available: https://cdn.standards.iteh.ai/samples/68383/4e26ddadc54a4198bed652afe29669fa/ISO-26262-1-2018.pdf [Accessed by 19/10/2023].
7. L. Bieker, S. Kempf, and A. Heidinger, “Safe and secure system development with AUTOSAR and MBSE,” in *WCX SAE World Congress Experience*, Michigan, United States of America, 2020.
8. S. Friedenthal, A. Moore, and R. Steiner, “A Practical Guide to SysML: The Systems Modeling Language,” *Morgan Kaufmann*, Burlington, United States of America, 2014.
9. S. Kempf, L. Bieker, and H. Reiser, “Co-simulation for AUTOSAR-based model-in-the-loop testing,” *ATZ worldwide*, vol. 121, no. 7, pp. 56–61, 2019.
10. S. Wegener, M. Kuntz, and J. Frey, “Toward seamless tool integration for AUTOSAR and MBSE,” *IEEE Software*, vol. 38, no. 6, pp. 47–54, 2021.
11. Y. Peng, C. Wang, and Y. He, “Fault-tolerant control for power electronic systems: A review,” *Energies*, vol. 10, no. 10, p. 1528, 2017.
12. S. M. Sundharam, P. Iyenghar, and E. Pulvermueller, “Software architecture modeling of AUTOSAR-based multi-core mixed-critical electric powertrain controller,” *Modelling*, vol. 2, no. 4, pp. 706–727, 2021.