Electronics and Electrical Engineering

http://www.aimspress.com/journal/ElectrEng

AIMS Electronics and Electrical Engineering, 8(3): 370–379.
DOI: 10.3934/electreng.2024017
Received: 12 January 2024
Revised: 05 June 2024
Accepted: 26 June 2024
Published: 10 July 2024

Research article

Methodology of a hierarchical and automated failure analysis and its advantages

Levent Ergün*, Roman Müller Hainbach and Stefan Butzmann

Faculty of Electrical, Information and Media Engineering, Chair of measurement and sensor systems, University of Wuppertal, Rainer-Gruenter-Strasse 21, 42119 Wuppertal, Germany

* **Correspondence:** Email: erguen@uni-wuppertal.de; Tel: +49-(0)202-439-1891.

Abstract: Several industries, particularly the automotive sector, are increasingly incorporating more electronics into their products. As a result, these products are becoming more complex and difficult to analyze. This complexity poses a significant challenge for manufacturers in proving the functional safety of their products. Not only do random faults present risks, but component tolerances can also lead to unexpected safety hazards. Current methods are struggling to keep pace with these challenges. We have identified key issues with existing methods and introduce a new approach that leverages computer automation and a model-based framework to enhance the process. We explain how this new method not only improves upon existing practices but also introduces additional capabilities.
In this paper, we examine methods for proving the functional safety of electronic systems. We begin by identifying the challenges associated with current established methods. Next, we introduce our new approach, which relies heavily on computer assistance and offers novel techniques for conducting broader and more in-depth analyses of these systems. We then explain a new workflow that utilizes this approach. To illustrate its application, we provide a demonstrative example. Our conclusion summarizes our findings and results, and we share our thoughts on potential future developments.

Keywords: functional safety; automated safety analysis; hierarchical analysis; failure modes

1. Introduction and state of the art

The proportion of electronics in modern systems has significantly increased across almost all industrial sectors. This trend is particularly evident in the automotive industry, where electronic systems are increasingly used to enhance the safety of vehicle occupants, such as anti-lock braking systems and airbags. Similar scenarios are observed in medical technology, aviation, and other fields.

Random failures of individual components that were not accounted for during development and implementation, can dangerously impact the system. Therefore, proof of functional safety is essential,

especially for systems that could endanger human life if they fail.

Functional safety refers to the capability of an electrical, electronic, or programmable electronic system (E/E/PE systems) to enter and maintain a safe state in the event of accidental or systematic failures with hazardous effects [1]. Real systems always carry the residual risk of assuming a critical state at the end of their development [2]. However, the goal of functional safety is to minimize this residual risk.

Various standards underpin the development of safety-critical systems. IEC 61508 is the fundamental standard for E/E/PE systems. Different industries have specific safety verification requirements, leading to the development of industry-specific standards over the years.

To develop a functionally safe system, a hazard and risk analysis must be conducted in accordance with these standards. The basic standard outlines general criteria, metrics, and examples. Methods such as fault tree analysis (FTA), failure modes and effects analysis (FMEA), and failure modes, effects, and diagnostic analysis (FMEDA) are used to verify whether the developed system meets the relevant requirements.

However, the aforementioned tools (FMEDA, FTA) used for safety analyses are not automated. This limitation means that the vast number of possible fault combinations cannot be analyzed cost effectively. These methods largely rely on hypothetical reasoning and communication. Computer assistance often takes the form of spreadsheets used to store the results of this manual effort.

Given these challenges, it is necessary to enhance current methods with suitable extensions that align with technological advancements. This work aims to present an alternative methodological approach for the safety assessment of electronic systems. This method is designed to automatically predict the effects of failures of individual modules and components on the overall system. To reduce the number of potential simulation runs without losing information and thereby generate analysis results more quickly, a hierarchical analysis approach was chosen, which is further described later.

2. Challenges with non-automated and non-hierarchical approaches

As already mentioned in the introduction, failure analysis is usually carried out manually with today's non-automated and non-hierarchical approaches. The number of failure combinations that need to be considered in this case for a complete analysis can be determined using the binomial coefficient in Equation 2.1. This is a combination without repetition, that is, k elements are selected from n objects without taking the order into account, whereby each object may only occur once in a combination.

$$\binom{n}{k} = \frac{n!}{(n-k)!\,k!} = \frac{n(n-1)\ldots(n-k+1)}{1\ldots(k-1)\,k} \tag{2.1}$$

For the dual-point-fault (DPF) analysis, the formula for the two-element subset can be simplified as in Eq 2.2. The DPF analysis can demonstrate whether two independent single faults can lead to a critical system state. In this case, the n refers to the number of components.

$$\binom{n}{2} = \frac{1}{2}\,n(n-1) \tag{2.2}$$

As each component has several failure modes, this influence is considered in Eq 2.3 with the factor F. For the two-element subset presented here, this factor is entered into the equation as a square.

$$\binom{n}{2} \cdot F^2 = \frac{1}{2} n(n-1) \cdot F^2 \tag{2.3}$$

In Eq 2.4, the number of single-point-fault simulations is also taken into account so that this equation can be used to determine the total number of single and dual-point-fault (SPF and DPF) combinations for a system.

$$\binom{n}{2} \cdot F^2 + nF = \frac{1}{2} n(n-1) \cdot F^2 + nF \tag{2.4}$$

If four failure modes are considered on average for each component in an electronic control unit (ECU) with 1,000 components, the calculation in Eq 2.5 results in a total of 7,996,000 failure combinations to be considered.

$$\begin{aligned} \binom{1000}{2} \cdot 4^2 + 1000 &= \frac{1}{2} 1000(1000-1) \cdot 4^2 + 1000 \cdot 4 \\ &= 7,996,000 \end{aligned} \tag{2.5}$$

This numerical example illustrates the rapid increase in the number of failure combinations to be considered, a phenomenon that is often referred to in technical literature as a "combinatorial explosion" [3]. Figure 1 shows the behavior with different average failure modes.

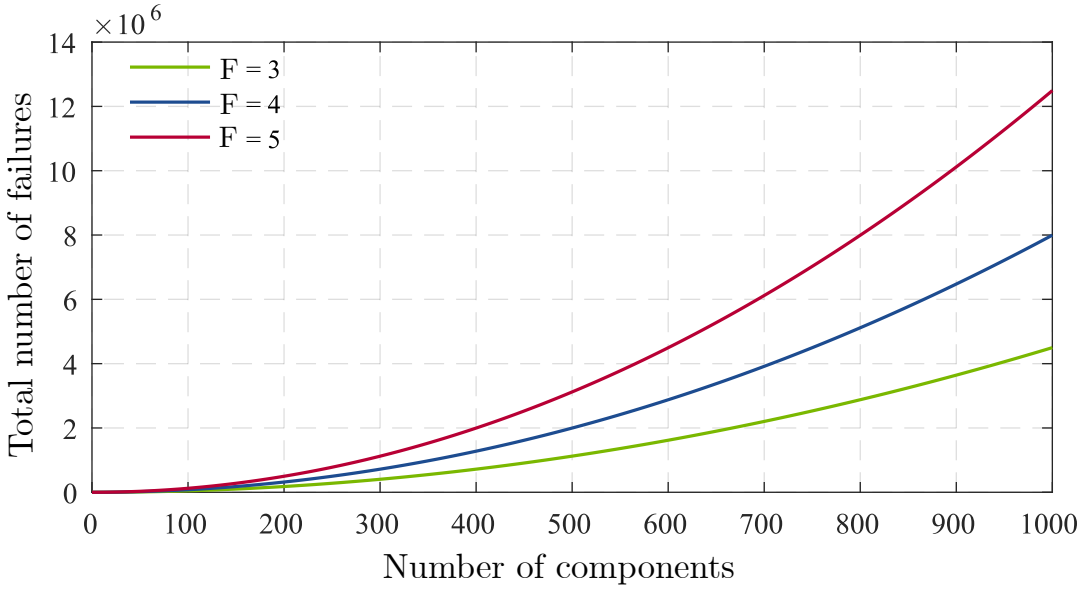

Figure 1. Effect of the combinatorial explosion on the number of total failure runs.

3. Model-based analysis and state of research

A key aspect of enabling computer-aided functional safety is the adoption of model-based design. The domain of modeling can vary. We have gathered experience with modeling in MATLAB/Simulink and SPICE, for which our approach has worked very well.

Model-based analysis is already a systematic methodology in which models of electronic or mechatronic systems are used to enable a comprehensive analysis and detailed understanding of these systems. These models can include circuits, state machines, and other relevant components. The aim of this analysis is to evaluate the behavior of systems more accurately. This approach is crucial to ensure that the systems under development meet the specified requirements and achieve the intended performance goals. However, it is worth noting that the safety assessment based on these models is also usually carried out at this point by manual failure injection and is usually only performed for selected components.

In response to the existing research gap, numerous academic articles have been published concerning the advancement of model-based and automated safety verification [4–7]. However, it is important to highlight that these previous studies mainly concentrate on basic automation, often limiting their focus to simulation environments and providing only limited fault modeling capabilities. Despite the potential effectiveness of rudimentary automation for comprehensive safety analysis, its practical implementation within a reasonable timeframe is impeded by the combinatorial explosion inherent in more complex systems.

Against this backdrop, the primary goal is to minimize the number of simulations without loss of information, which at the same time significantly reduces the overall simulation time. To achieve this, we have extended the model-based automated failure analysis with a hierarchical approach. The hierarchical safety analysis is explained in more detail in the next section.

4. Automated and hierarchical safety analysis

This section introduces an alternative methodology for the safety verification of electronic systems. The proposed approach is characterized by a hierarchical and automated failure analysis that incorporates considerations of the equivalence of failure effects. This methodology is designed to enable the analysis of complex systems within a reasonable simulation timeframe.

4.1. General failure injection

The general relationships for error injection and the required data are shown in Figure 2. In addition to the model to be analyzed, the modeled failure modes are also required as input parameters. During the failure analysis, the failure-free model is first copied so that the respective failure mode and the manipulated model can be simulated. This process is carried out *i*-times according to the number of individual failure modes.

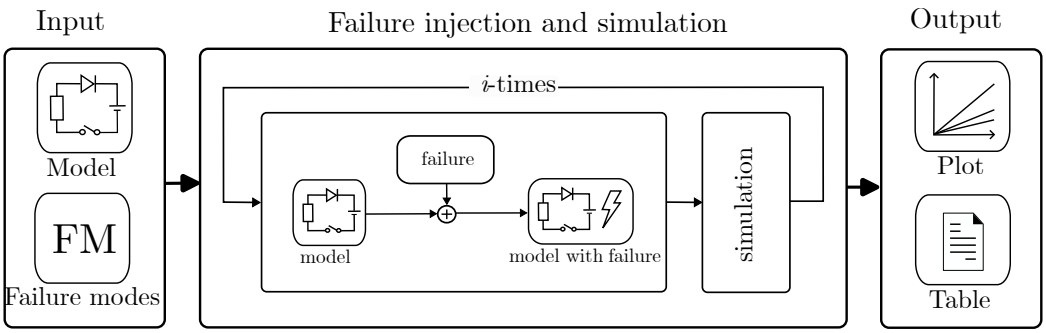

Figure 2. General failure injection.

4.2. Equality of the failure effect

Investigations as part of this work showed that different causes of failures in circuits can lead to identical failure effects. If the equality of the effects is considered during the failure analysis, the number of simulation runs and thus the total simulation time can be reduced.

Figure 3 illustrates the principle using a simple, minimal example: A voltage divider consisting of two equally sized resistors with a downstream impedance converter.

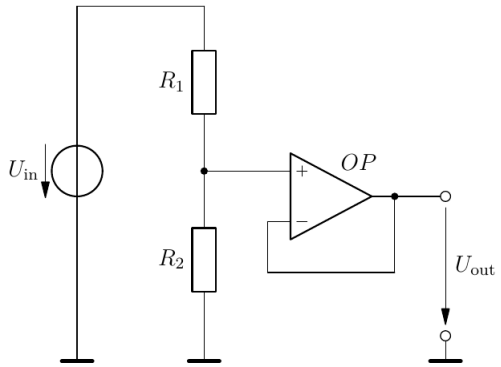

Figure 3. Test circuit.

The following failure modes were considered for the components in the failure analysis of this circuit:

Table 1. Components and failure modes considered in the analysis.

Component	**Failure mode**
Resistor	Open, Short
	Drift 50 %, Drift 200 %
OpAmp	Output stuck-high, Output stuck-low
	Input (+) stuck-high, Input (+) stuck-low
	Input (-) stuck-high, Input (-) stuck-low

Considering these failure modes alongside three components, Equation 2.4 yields approximately 80 combinations of single and dual-point faults. The green curve depicted in Figure 4 illustrates the input-to-output signal during DC analysis unaffected by failures. Conversely, the red curves represent variations resulting from diverse failure injections.

As can be seen in Figure 4, the 80 failure injections performed result in a total of seven different failure effects, which can be summarized accordingly in seven failure behavior groups. The first group contains the majority of failures. These are failures that lead to a stuck-low failure on the output side. This failure can be caused if, for example, R_2 becomes low impedance, or the output of the OP is connected to ground.

In order to examine the effect of the equality of failure effects in different circuits with an increasing number of components, various circuits from practice were examined in this work, and the hierarchical failure analysis was derived from the findings.

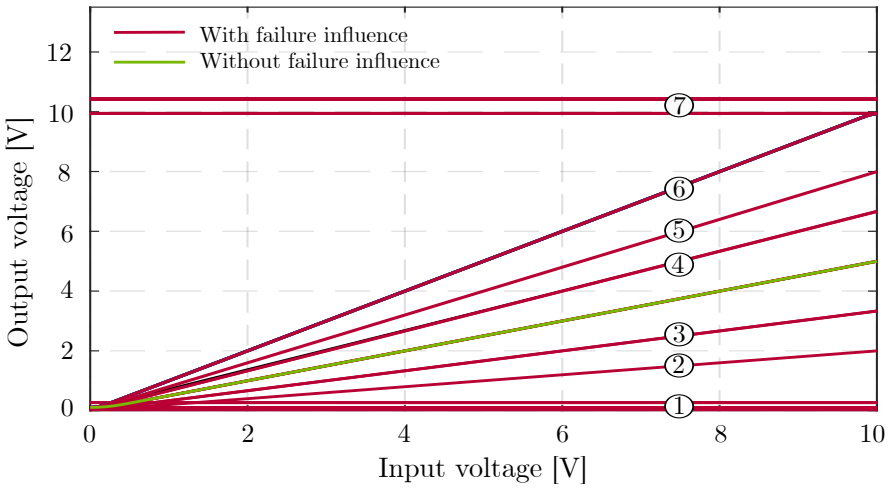

Figure 4. Result of the failure analysis of the voltage divider with impedance converter (80 failure combinations).

4.3. Hierarchical failure analysis

In the following section, the hierarchical failure analysis developed to reduce the number of simulation runs is explained using an example model. The system shown in Figure 5 comprises a measurement circuit (sensors), a microcontroller, and a control circuit (actuators), which together represent the system level.

In this example, the circuits consist of 15 and 13 components. The microcontroller is assumed to be ideal in this simplified representation. When analyzing the system without a hierarchical failure analysis, all failure combinations would have to be considered directly at the system level. With 28 components and an average number of five failure modes, this would result in 9,590 SPF and DPF combinations.

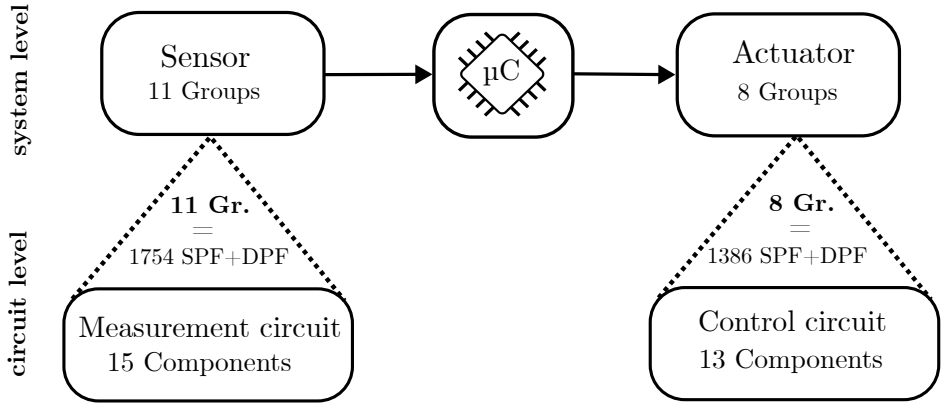

Figure 5. More detailed presentation of the development levels, failure behavior groups, and breakdown of possible subsystems.

Instead, the two sub-circuits (measurement and control) are simulated separately at the circuit level. A detailed view of this is shown in Figure 5. The failure analysis of the measurement circuit leads to

1,754 SPF and DPF combinations at the circuit level. By considering the equality of failure effects, these failure combinations can be grouped into 11 failure behavior groups. In the failure analysis of the control circuit with 13 components, the resulting 1,386 SPF and DPF combinations can be assigned to eight failure behavior groups.

In this approach, a semi-automated method is used for grouping, in which similarly behaving curves at the circuit level are summarized on the basis of a similarity analysis and transferred to the system level. Finally, the overall analysis is carried out at the system level. The main difference is that only 20 failure behavior groups have to be combined at the system level, so a total of 190 SPF and DPF combinations exist.

To mathematically determine the resulting SPF and DPF combinations, Equation 2.4 can be simplified to $F = 1$. The reason that $F = 1$ applies is that each failure behavior group represents only one failure mode by definition. Furthermore, the n in Eq 4.1 does not stand for the number of components as before but for the number of failure behavior groups. This results in the following relationship ($n = 19$, $F = 1$):

$$\binom{n}{2} \cdot F^2 + nF = \frac{1}{2}\,19(19-1) + 19 = 190 \tag{4.1}$$

By initially considering the circuits in isolation at the circuit level and then transferring the few failure behavior groups to the system level, the number of runs for a holistic analysis of the overall system can be significantly reduced. The total number of combinations results from the sum of the failure combinations at the system and circuit levels (here: 190 + 1,754 + 1,386 = 3,330). In the example chosen here, with only a few components, the failure combinations could be reduced from 9,590 to 3,330. This corresponds to a reduction of approximately 65 %.

5. Results and discussion

The methodology developed was illustrated using three selected real control units from industrial partners. The failure modes considered can be found in Tables 2 and 3.

The analysis carried out showed that with the help of the automated and hierarchical safety analysis, the modeled systems could be considered with significantly fewer simulation runs. Table 4 summarizes the number of failure combinations for the investigated ECUs. The table represents both the total number of failure combinations (combinations at circuit and system level) when using the hierarchical failure analysis and the number of failure combinations when using the non-hierarchical failure analysis.

The applications demonstrate that hierarchical failure analysis can significantly reduce the number of failure combinations. In the specific case of the three examined systems, this approach led to an average reduction of approximately 91% in failure combinations. This corresponds to a reduction in overall analysis time by 91%, which is a major advantage of the approach.

Table 2. Components and failure modes considered in the analysis (Part 1).

Components	Failure modes	Components	Failure modes
Resistor	Open, Short	Bipolar Transistor	C-open, B-open
	Drift 50%		E-open, BC-short
	Drift 200%		BE-short, CE-short
Capacitor	Open, Short	MOSFET	D-open, G-open
	Drift 50%		S-open, GD-short
	Drift 200%		GS-short, DS-short
Inductor	Open, Short		
	Drift 50%		
	Drift 200%		
Diode	Open, Short		
	Reverse leakage 10x		
Z-Diode	Open, Short		
	Reverse leakage 10x		
	Pos. change in voltage by 20% and 50%		
	Neg. change in voltage by 20% and 50%		

Table 3. Components and failure modes considered in the analysis (Part 2).

Components	Failure modes
Optocoupler	Open (Inputs and Outputs)
	Short (Inputs and Outputs)
	Decrease in current transmission by 10%
	Increase in current transmission by 50%
OpAmp	Output stuck-high, Output stuck-low
	Input (+) stuck-high, Input (+) stuck-low
	Input (-) stuck-high, Input (-) stuck-low
Comparator	Output stuck-high, Output stuck-low
	Input (+) stuck-high, Input (+) stuck-low
	Input (-) stuck-high, Input (-) stuck-low
logic gate	Inputs stuck-high, Inputs stuck-low
	Output stuck-high, Output stuck-low
GPIO	Stuck-high, Stuck-low
MUX	Channel-stuck, Channel-swap
Relay	Always open
	Always short
ADC	Bit-stuck-high, Bit-stuck-low
	Gain-error, Offset-error
	Missing-codes

Table 4. Representation of the numbers of failure runs/combinations that are considered in a non-hierarchical analysis and which must be considered in the hierarchical analysis.

Control unit	Number of components	Non-hierarchical approach (Failure runs)	Hierarchical approach (Failure runs)
Gas burner	114	103,512	9,372
Home storage	133	140,980	12,224
Heat pump	172	235,984	18,956

6. Conclusions and future possibilities

This paper presented a methodology for the automated safety verification of electronic systems. Initially, we identified the weaknesses of currently employed methods to highlight areas for improvement.

Moreover, it was determined that the increasing complexity of systems results in an unmanageable number of potential failure combinations, which cannot be addressed by today's manual methods due to the combinatorial explosion. Although rudimentary automated failure injection could theoretically allow for comprehensive safety assessment, it is impractical due to the high computational demands.

We found that circuits with different fault causes often exhibit similar fault effects. These effects can be grouped into fault behavior categories. The hierarchical analysis approach we introduced allows this knowledge to be applied effectively to complex systems.

Finally, we validated our automated safety verification methodology using three different control units from various industries. Notably, hierarchical failure analysis reduced the number of failure combinations and the overall computing time by approximately 91%.

There are numerous ways to enhance modeling capabilities for more accurate prediction results. These capabilities could include thermal modeling for conducting safe-operating-area (SOA) analysis, known as smoke analysis, during safety simulation. The outcomes of this analysis can be used to implement fault sequence analysis, where the model considers the damage from operating outside the SOA and accurately predicts the probable chain reaction of faults.

Another opportunity lies in fault modeling, which can be improved with stochastic variations. This approach combines failure analysis with tolerance analysis and applies it to failure models.

Additionally, we plan to use the results from tolerance analysis to identify sensitivity hot spots in the design. These insights could be invaluable for optimizing component selection and reducing costs in the final stages of development.

Author contributions

Levent Ergün: Investigation, Writing – original draft, Writing – review & editing; Roman Müller-Hainbach: Writing – review & editing, Resources; Stefan Butzmann: Project administration, Supervision. All authors have read and agreed to the published version of the manuscript.

Use of AI tools declaration

The authors declare they have not used artificial intelligence (AI) tools in the creation of this article.

Conflict of interest

The authors declare that there are no conflicts of interest in this paper.

References

1. DIN EN 61508 (2002) *Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme*, VDE-Verlag.
2. Löw P, Pabst R, Petry E (2011) *Funktionale Sicherheit in der Praxis: Anwendung von DIN EN 61508 und ISO/DIS 26262 bei der Entwicklung von Serienprodukten*, dpunkt. verlag, Heidelberg.
3. Behrends E, Gritzmann P, Ziegler GM (2018) *π und Co.: Kaleidoskop der Mathematik*, Springer Berlin Heidelberg, Berlin. https://doi.org/10.1007/978-3-662-67495-6
4. Pill I, Rubil I, Wotawa F, Nica M (2016) SIMULTATE: A Toolset for Fault Injection and Mutation Testing of Simulink Models. *IEEE Ninth International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, 168–173. https://doi.org/10.1109/ICSTW.2016.21
5. Fabarisov T, Mamaev I, Morozov A, Janschek K (2021) Model-based Fault Injection Experiments for the Safety Analysis of Exoskeleton System, *The 30th European Safety and Reliability Conference and The 15th Probalilistic Safety Assessment and Management Conference*. https://doi.org/10.3850/978-981-14-8593-0_5770-cd
6. Bartocci E, Mariani L, Ničković D, Yadav D (2022) FIM: Fault Injection and Mutation for Simulink. *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, 1716–1720. https://doi.org/10.1145/3540250.3558932
7. Saraoğlu M, Morozov A, Söylemez M, Janschek K (2017) ErrorSim: A tool for error propagation analysis of simulink models. *Computer Safety, Reliability, and Security: 36th International Conference, SAFECOMP 2017, Trento, Italy, September 13-15, 2017, Proceedings 36*, 245–254. Springer International Publishing. https://doi.org/10.1007/978-3-319-66266-4_16

AIMS Press