Faulty Behaviors Simulation in Industrial Cyber-Physical Systems for Safety Analysis

Francesco Tosoni
Department of Engineering for Innovation Medicine – University of Verona (Italy)
francesco.tosoni@univr.it

***Abstract*—In recent years, the industrial world has been progressing more and more thanks to the Industry 4.0 phenomena. The Industrial Cyber-Physical Systems (ICPSs) that compose smart factories are increasingly complex and interconnected. A key feature in such environments is the synchronization of these systems with each other and humans. In this context, functional security is crucial for production, economic and legal reasons. Modeling and simulation of ICPSs are critical processes to ensure the functional safety needed in these types of factories. However, building a model of the system under analysis is a complicated task, also because of the multiplicity of physical domains composing an ICPS. The tool adopted to realize such models is Verilog-AMS, as it allows one to create both multi-domain analog systems and mixed-signal models, and then to simulate such designs to study their behavior. A new methodology for modeling faults belonging to different domains by exploiting the capabilities of Verilog-AMS has been realized. The simulation of faulty systems allows for studying the effects of a single fault on the whole system. In particular, new mechanical and thermal fault models have been modeled through the physical analogies between these domains and the electrical domain. Moreover, automatic tools for injecting the identified fault models into simulable models have been created.**

***Index Terms*—Digital Twin, Industry 4.0, Fault Modeling, Functional Safety**

I. Introduction

In today's industrial environment, the simulation of a system is critically important, whether for a system that is only a component of a larger system or for an entire production line. Fault simulation enables us to understand how and in which ways a system's faulty behaviors differ from nominal working conditions [1]. This knowledge, not only allows optimization of machinery maintenance, making it also potentially predictive, but also enables structural improvement of the system already at the design stage. In fact, if the simulative model is built before the real system, preliminary studies can be performed to highlight critical issues and potential faults to which the system may be vulnerable. Furthermore, the maintenance process can be improved by predicting the occurrence of a fault and thus taking action before encountering serious safety and/or monetary problems [2]. In order to perform fault analysis, data sets representing faulty behaviors of the system are needed for comparison with nominal ones. This data cannot be obtained by voluntarily breaking the actual system, causing useless monetary losses, but they can be retrieved by the simulation of the system through a virtual model. Constructing such a holistic representation of a Cyber-Physical System (CPS), called the "digital twin", is an interesting and

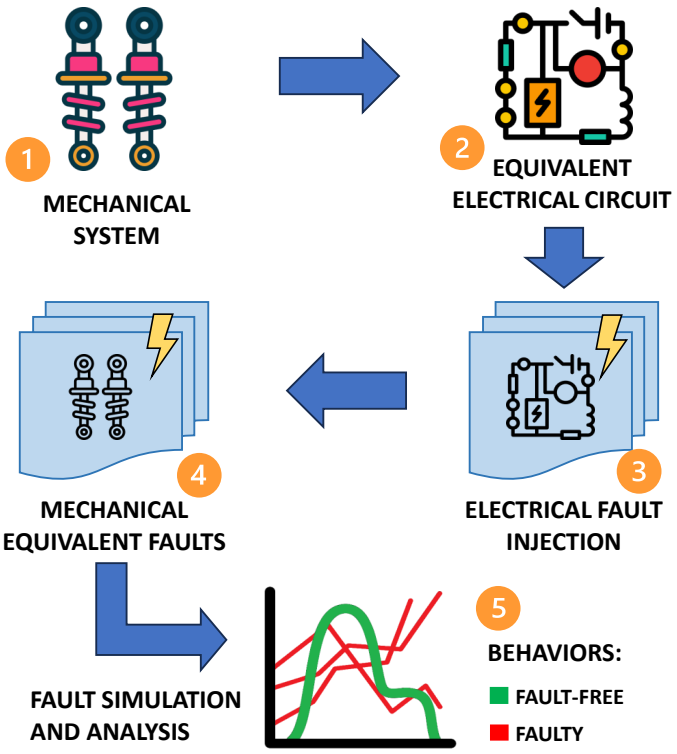

Fig. 1. Conceptual overview of the proposed methodology for a mechanical system.

open research problem. Moreover, building a system composed of many physical domains, including mechanical, electrical and thermal, and simulating it correctly is challenging. Building the model of the system and simulating it by injecting faults belonging to several physical domains can help ensure specific levels of functional safety of the system. This kind of simulation can provide us with the faulty data series needed to perform not only safety analysis but also to achieve the optimization processes discussed above.

The language that was chosen to implement this methodology is Verilog-AMS, which is a developing environment for systems belonging to different physical disciplines [3]. In this environment, modeling the behaviors of analog multi-domain systems is very simple: we only need to specify the differential equations of the system we want to describe. Although the model creation phase can be complex, especially if the differential equations need to be defined, the fault injection phase is simple. A fault is injected just by modifying an

existing differential equation or adding a new one in the code. Another advantage of Verilog-AMS is that it allows the cyber part of an ICPS to be implemented and simulated as well, enabling the creation of mixed-signal models. This thesis aims to demonstrate how Verilog-AMS can be an ideal modeling environment for building digital twins of ICPS of different sizes and performing fault analysis on such descriptions. These virtual systems are not only composed of many physical domains but can also include digital components, which are simulated together with the analog part.

The proposed flow is shown in Figure 1, and described in detail:

1) At the top left corner, the system under analysis has been modeled in Verilog-AMS through differential and algebraic equations that describe its dynamics;
2) The same system has been translated into an electrical network via physical analogies. The electrical circuit has been described in Verilog-AMS code to be simulated to ease the next step;
3) The injection of analog electrical faults into the analogous electrical network allows the formalization of new non-electrical fault models, extending the analogy;
4) The obtained faulty behaviors can be used to perform fault analysis, fault propagation, fault detection and predictive maintenance techniques;
5) Tools for the automatic injection of the derived fault have been designed.

The report is structured as follows: Section II depicts an overview of the results already achieved. Then, Section III proposes future extensions and research directions for this Ph.D. thesis.

II. Achieved Results

The methodology briefly presented in the previous section is depicted in Figure 1. In the example, the flow is applied to the mechanical domain only for simplicity. The mechanical domain was the first to be addressed for the development of this methodology, even by previous works [4], [5]. Starting from a mechanical system, it is possible to translate the same system into an equivalent electrical network. According to the physical analogies between the electrical and mechanical domains, the behaviors of the two systems are equivalent, since they use the same differential equations. In [6] we formed a methodology to extend these analogies to fault models. Specifically, as shown in Figure 1 (center right), once the equivalent electrical network is obtained, the electrical fault models are applied once at a time to the equivalent electrical circuit. By studying the resulting behaviors, it is possible to understand whether and what impact the injected faults have on the system. The fault injection procedure is better illustrated in the article, explaining it step-by-step and with some examples. In [7] we presented a new mechanical taxonomy derived from this analogy-based analysis. Moreover, an analysis of mechanical faults at the physical level was also presented, mapping behavioral-level faults to physical ones. The flow presented so far has been designed and implemented for the mechanical domain, but it has been extended to the thermal domain as well. The aim is to include more and more domains to achieve a richer and more complete fault analysis. In our recent work [8], we studied how the methodology presented applies also to the thermal domain. The main challenge was to replicate how the electrical, mechanical and thermal domains affect each other, especially in the presence of faults. The goal is to build digital twins of increasingly complex systems: the more accurate a model is, the more faithful it is to its actual implementation. In particular, when coupled with failure models, an accurate model also expresses behaviors not directly related to the failed component or section [9].

The creation of automatic tools for injecting analog fault models into Verilog-AMS modules is an open research point. Taking a fault-free module as input, the designed tool injects the differential equations of the desired faults into the code branches. As output, we will have several modules, each with a different fault injected, depending on the fault pattern and location. Automating the process of injecting all possible fault models into all possible locations speeds up the subsequent analysis process.

III. Future Works and Extensions

One of the next steps in the near future is to improve and extend the proposed methodology by considering additional aspects of the production line and more sophisticated models. Another key aspect is the inclusion of the digital components of the systems into the simulation models. This approach would lead to a mixed-signal, multi-domain simulation: safety analysis would be much more accurate with such types of digital twins. The methodology will be validated on a real production machine that is present in the *ICE Laboratory* located in Verona, Italy. The laboratory is equipped with the state of practice machinery, which is compliant with Industry 4.0 standards. Verifying the analogies approach on more complex designs and extending the fault taxonomies in another key future development.

References

[1] *ISO 26262 – Road vehicles – Functional safety*, ISO, 2011.
[2] S. Centomo, N. Dall'Ora, and F. Fummi, "The Design of a Digital-Twin for Predictive Maintenance," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1, 2020, pp. 1781–1788.
[3] *Verilog-AMS Language Reference Manual*, Accelera Inc., 2014.
[4] N. Dall'Ora, S. Vinco, and F. Fummi, "Functionality and Fault Modeling of a DC Motor with Verilog-AMS," in *2020 IEEE 18th International Conference on Industrial Informatics (INDIN)*, vol. 1, 2020, pp. 35–40.
[5] N. Dall'Ora, E. Fraccaroli, S. Vinco *et al.*, "Multi-Discipline Fault Modeling with Verilog-AMS," in *2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*. IEEE, 2021, pp. 237–243.
[6] N. Dall'Ora, F. Tosoni, E. Fraccaroli *et al.*, "Inferring Mechanical Fault Models from the Electrical Domain," in *2022 5th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*. IEEE, 2022.
[7] F. Tosoni, N. Dall'Ora, E. Fraccaroli *et al.*, "A Framework for Modeling and Concurrently Simulating Mechanical and Electrical Faults in Verilog-AMS," in *2022 25th Forum on specification & Design Languages (FDL)*. IEEE, 2022.
[8] F. Tosoni, N. Dall'Ora, E. Fraccaroli *et al.*, "Thermal digital twin of a multi-domain system for discovering mechanical faulty behaviors," in *2023 IEEE 21st International Conference on Industrial Informatics (INDIN)*. IEEE, 2023.
[9] F. Tosoni, N. Dall'Ora, E. Fraccaroli *et al.*, "The challenges of coupling digital-twins with multiple classes of faults," in *2022 IEEE 23rd Latin American Test Symposium (LATS)*, 2022, pp. 1–6.