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

PHD FORUM SUBMISSION

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

***Abstract*—Recently, industrial evolution has been on the rising edge due to the Industry 4.0 phenomenon. The Industrial Cyber-Physical Systems (ICPSs) that compose smart factories are increasingly complex and interconnected among each other and humans. In such a context, functional safety is crucial for production, economic and legal reasons. Creating virtual models and behavioral simulations are powerful tools for ensuring the functional safety level required by these environments. Despite the complexity of creating these models, simulation is the key to the design of not only the main system but also the surrounding production environment. In order to analyze the system's behavior, multi-domain behavioral fault taxonomies have been produced and tested in simulation on different case studies. Fault injection and simulation methodology have been applied in the Verilog-AMS environment, as well as Simulink and SystemC. In addition, an exploration of the potential of game engines as simulators of physical systems is ongoing, due to the high accuracy at the graphics rendering level. The same fault models have also been useful for the development of Time-Sensitive Behavioral Contracts (TSBC) based fault detection mechanisms. Simulation models of the system under analysis enable the design and refinement of the contracts defined in the monitors. Future developments involve applying the same methodology to mixed-signal systems, thus including the system control part as well.**

***Index Terms*—Behavioral Simulation, Industry 4.0, Fault Modeling, Functional Safety**

I. Introduction

Considering nowadays industrial production scene, system simulation is crucial, whether for a system that is only a component of a larger system or for an entire production line. On the one hand, simple system simulation allows the designer to highlight the system's limits and to improve the concept before the deployment stage. On the other hand, fault simulation enables us to understand how and in which ways a system's faulty behaviors differ from nominal working conditions [1]. This knowledge allows the development of fault detection mechanisms and the optimization of machinery maintenance, making it potentially predictive. Other benefits come in terms of time and money: most of the refinements and adjustments that would occur on one or several prototypes would rather happen on the model. 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. In order to perform fault analysis, data sets representing the system's faulty behaviors 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. Moreover, building a system composed of many physical domains, including mechanical, electrical, and thermal, and simulating it correctly is challenging. 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.

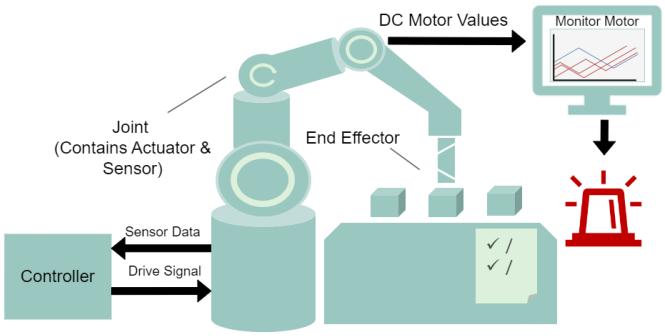

Fig. 1. Conceptual overview of the proposed methodology for the fault detection on a multidomain system.

One language chosen to implement this simulation setup is Verilog-AMS, which is a developing environment for systems belonging to different physical disciplines [2]. 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. However, industrial systems are not only composed of many physical domains but can also include digital components, which can be simulated together with the analog part. Although the construction of systems controlled by differential equations is straightforward in Verilog-AMS, the simulation of these components coupled with digital modules described in Verilog is onerous in computational terms. Therefore, to achieve fast mixed-signal simulation, the SystemC environment, with its analog extension SystemC-AMS, is currently being considered for future work of this PhD thesis. The goal is to have increasingly complex system models on which to apply the fault analysis proposed.

The main contributions of this work are:

1) The presentation of multidomain behavioral fault models obtained through the physical analogies among the electrical, mechanical, and thermal domains;
2) The testing and validation of such fault models on several models, coded in different simulation environments such as Verilog-AMS, Simulink, and SystemC-AMS;
3) Application of the proposed fault models to test a fault detection mechanism, which is composed by monitors based on TSBC (see Figure 1);
4) Exploring the capabilities of gaming engines for enhancing the effectiveness of the physics system's simulation.

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

II. Achieved Results

As mentioned before, the very first contribution was the presentation of multidomain behavioral taxonomies obtained through physical analogies. 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. So, by studying the resulting behaviors, it is possible to understand whether and what impact the injected faults have on the system. In [3] we formed a methodology to extend these analogies to fault models. The fault injection procedure is better illustrated in the article, explaining it step-by-step and with some examples. In [4] 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 last steps of this framework are included in [5], where we show the methodology can be applied to both to a Cyber-Physical System (CPS) and a Micro Electro Mechanical Systems (MEMS) as well. Later, the same methodology was also tested on an aircraft landing-gear system [6], modeled in Simulink: we simulated mechanical faulty behaviors using the taxonomy presented previously, mapping the behavioral fault models to actual failures of the system coming from the literature. 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 [7]. The main challenge was to replicate how the electrical, mechanical, and thermal domains affect each other, especially in the presence of faults. Then, we analyzed how, when coupled with fault models, an accurate model also expresses behaviors not directly related to the failed component or section [8].

Up to now, we have developed and tested methodologies related to the analysis of the behavior of physical systems. However, in the context of CPSs, the control part is equally important to the purely physical one. So, we built a virtual platform that included a digital controller and an analog MEMS sensor. The purpose was to investigate, after the injection of a fault model of the taxonomies, the possible propagation of a fault from the analog part to the digital component. The system was implemented entirely in Verilog-AMS and simulated in its entirety, also in the presence of mechanical and electrical faults. Through this case study, the importance of including behavioral faults simulation in the development phase of a smart system is shown [9], [10].

Recent works concern the construction of a fault detection system in the physical section of CPS. The fault taxonomies presented above have also been used to test the accuracy of the TSBCs in the monitors that check the system's behavior [11]. Finally, an investigation regarding the capabilities of a game engine as a physical systems simulator was presented: exploiting the rendering-level capabilities of a game engine to replicate an advanced level of physical simulation is an interesting topic from the perspective of safety analysis [12].

III. Future Works and Extensions

There are many future directions, but the main ones remain related to the extension and validation of the fault taxonomies presented. The development of increasingly complex multidomain models in industry enables testing and validation of the methodology and taxonomies. Regarding fault detection, we are working on extending the proposed methodology to digital control modules. The idea is to achieve an approach that aims not only at fault detection but also at predictive maintenance of CPSs. Finally, the simulation of systems in game engines wants to be extended and deepened, especially with regard to the interaction between the purely visual and simulative parts.

References

[1] *ISO 26262 – Road vehicles – Functional safety*, ISO, 2011.
[2] *Verilog-AMS Language Reference Manual*, Accelera Inc., 2014.
[3] 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.
[4] 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.
[5] F. Tosoni, N. Dall'Ora, E. Fraccaroli *et al.*, "Multidomain Fault Models Covering the Analog Side of a Smart or Cyber–Physical System," *IEEE Transactions on Computers*, vol. 73, no. 3, pp. 829–841, 2024.
[6] F. Biondani, N. Dall'Ora, F. Tosoni *et al.*, "Fault Injection for Synthetic Data Generation in Aircraft: A Simulation-Based Approach," in *2024 IEEE 22nd International Conference on Industrial Informatics (INDIN)*. IEEE, 2024.
[7] 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.
[8] 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.
[9] F. Tosoni, N. Dall'Ora, E. Fraccaroli *et al.*, "Assessing Robustness of Smart Systems via Multi-domain Analog Fault Simulation," in *2024 IEEE 30th International On-Line Testing Symposium (IOLTS)*. IEEE, 2024.
[10] F. Tosoni, N. Dall'Ora, E. Fraccaroli *et al.*, "Cross-domain Analog Fault Injection for Designing Robust Smart Systems," in *2024 27th Forum on specification & Design Languages (FDL)*. IEEE, 2024.
[11] F. Bruns, F. Tosoni, S. Mehlhop *et al.*, "Analyzing Fault Behaviors in Multi-Domain Systems with Contract-Based Monitors," in *2024 29th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2024.
[12] F. Tosoni, M. I. Amin, N. Dall'Ora *et al.*, "Exploring Multidomain Faults in Digital Twin: A Gaming Engine Perspective," in *2024 27th Forum on specification & Design Languages (FDL)*. IEEE, 2024.