Automated model-based D-FMEA with partially unknown components' behaviors

Hadrien Tournaire, Florian Grigoleit

Automated model-based D-FMEA with partially unknown components' behaviors

Hadrien Tournaire
modelwise GmbH
Munich, Germany
0000-0003-1323-0561

Florian Grigoleit
modelwise GmbH
Munich, Germany
florian.grigoleit@modelwise.ai

***Abstract*— This paper presents a methodology that allows to automate the model-based generation of system FMEA for which some components' behaviors are not precisely known. Using simple assumptions on the relations that may exist between the input and output of such components, the deviation of the system from its nominal behavior brought by failure modes is inferred and used to identify the possible failure of its functions. The presented work is applied to an electromechanical system involving a controller whose exact behavior is assumed to be unknown.**

Keywords—qualitative reasoning, behavior deviations, FMEA automation

I. Introduction

Failure-mode-and-effects analysis (FMEA) is a well-established process [1] for ensuring that the safety requirements of a system are fulfilled. Although widely spread in the industry and mandatory for validating designs in automotive and aeronautics applications [2], FMEA remains a laborious task requiring time [3] and expensive highly qualified engineers. The need for computer aid to assist experts in the generation of FMEA has led to the development of several tools and methods. Although these tools often only provide support for the clerical aspects of FMEAs, powerful approaches to automatic or semi-automatic FMEA have been proposed [4]. Among these methods, the qualitative model-based approach has been used successfully, especially in the electronic fields, for instance [5, 6].

In the electronic domain however, it can be very difficult to obtain or develop models of some components, especially complex integrated circuits. Based on the assumed relationship between inputs and outputs of such components, we propose a methodology that allows generating FMEA, based on reasoning over the systems deviation from its nominal behavior. The proposed method consists of identifying the qualitative deviations induced by component failures and propagating these deviations through the whole system's variables to identify potential functions' failure. Components for which no model is available are referred to as black boxes. However, although the internal working of such components is unknown, the knowledge of their functions allows to infer the possible relationships between their input and output variables. Therefore, it is considered that the behavior of modeless components is only partially known. In the case of components for which qualitative models are available, the input and output relationships are determined using the evaluation of their correlations.

To illustrate the proposed method, let us consider a simple motor speed regulation system (see Figure 1) containing a controller for which no model is available. In this system, the controller regulates the motor's PWM signal to reach the desired motor speed relying on a measure of its actual value achieved by sensors. Besides this, the controller emits a signal indicating the status of the regulation.

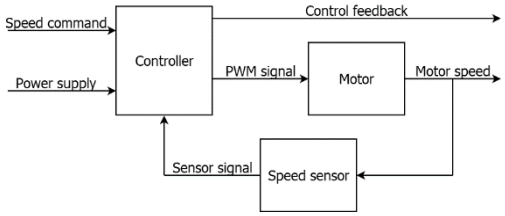

Fig. 1. Motor speed regulation system model

The motor speed regulation system is given 2 functions:

- **Motor speed regulation:** The system controls the motor speed to make it correspond to the speed command.
- **Controller feedback:** The system provides a feedback signal of the regulation status.

II. Black Box Components

In the proposed approach, we assume a system whose qualitative behavior is only partially known because of some black box components. The black box components of the system are present in the model (see Figure 1), their terminals are connected to the rest of the system but the exact relations between their inputs and output are unknown.

Let us consider a component whose behavior f is not exactly known but assumed to link inputs u to outputs y. For each output y_j of the component, it is possible to assume that it is influenced by input u_i via an unknown relation f_j so that:

$$y_j = f_j(u_1, \ldots, u_n) \tag{1}$$

The assumed relationships f_j of the controller inputs and outputs are represented in Figure 2 using colored (a color per relationship) arrows. Arrows highlight the causalities between the component's input and output expressed by relationships f_j.

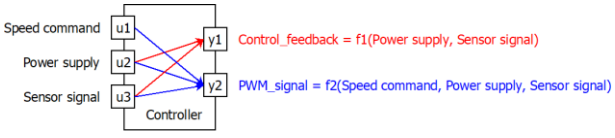

Fig. 2. Assumption of the relationship between a black box component's input and output variables.

The identification of the inputs, outputs, and their possible relationships are the only assumptions the present method requires on the black box components to achieve the FMEA of the system. In the worst case, when no relationship can be guessed, it is still possible to assume that every output y_j of a

component is influenced by all its inputs u_i. This assumption is however expected to generate very conservative FMEA results.

III. Failures induced deviations

Qualitative models can be represented as tables describing the values that output variables of a component can take for different input combinations. A simple qualitative model of the motor's behavior is presented in Table I, without and with a failure (winding failure). In this example, we assume that the failure "winding failure" changes the motor speed to a qualitative "not_regulated" value.

TABLE I. Motor's qualitative behavior: no failure and with winding failure

Motor input variable	**Motor output variable**	
PWM signal	***Motor speed (no failure)***	***Motor speed (winding failure)***
no_signal	zero	zero
regulation_signal	regulated	not_regulated

In Table I, one can see that the winding failure of the motor induces a deviation from the system's nominal behavior (i.e. when no failure mode is considered). Indeed, the motor's output (motor speed) is not "regulated" anymore but "not_regulated" when the input (PMW signal) has the value "regulation_signal".

Based on the qualitative behavior of each component with no failure, the relationships between input and output variables are established. Although in the presented motor example this causality is obvious it might not always be straightforward when considering numerous inputs and outputs. A simple but efficient solution for determining the input and output relationships of a qualitative model consists in evaluating the correlation coefficient (ρ) between these variables, therefore:

$$y_j = f_j(\ldots, u_i, \ldots) \text{ where } |\rho(y_j, u_i)| > 0 \quad (2)$$

IV. Deviations propagation

Once the input and output relationships are established for all the components of the system with no failure, the systems' variables' causalities are represented as a graph (see Figure 3).

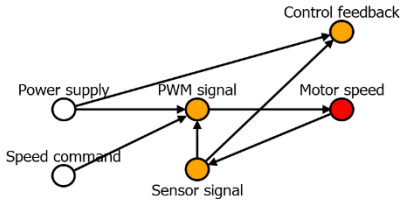

Fig. 3. Representation of the variables' deviation propagation using an oriented graph, the node directly impacted by the failure mode (Motor speed) is filled with red while the variables to which the deviation is assumed to propagate are filled in orange.

For all failure modes of interest which have to be considered in the FMEA, the deviated variables and the propagation of these deviations are estimated by browsing the variable causality graph. To do this, we assume that a deviation of a qualitative variable always induces a deviation of the variable it influences (hypothesis H1). In practice, this assumption is conservative and not always true, especially for non-linear systems. The deviation of the motor speed induced by the winding failure of the motor and its propagation is presented in Figure 3.

V. Effect identification

Browsing the graph of variable causalities allows us to conclude that a failure of the motor windings induces a change in the motor speed and the control feedback (see Figure 3). The main challenge now is to determine whether the identified deviations denote the failure of the system functions or not. Indeed, in the presence of winding failure, the deviation of the motor results in a failure of the motor speed regulation function. On the contrary, the deviation of the control feedback signal does not correspond to a failure of the system to communicate its status. In this case, the control feedback signal simply changes because the sensor measure changes due to a motor speed deviation.

The function's failure identification approach used in this work consists of considering that the system's functions have outputs, possible inputs, and never fail on the nominal system (hypothesis H2). Let us identify the inputs and outputs of the system's functions:

- For the motor speed regulation function, we consider the speed command as an input and the actual motor speed as an output.
- For the control feedback function, we consider the actual motor speed as an input and the emitted feedback signal as an output.

The failure of a function is then assumed for a given failure mode if it exists a simple directed path from one of the variables directly deviated by the failure mode, to one of the function's outputs, not passing by any of the function's inputs (hypothesis H3).

In the example, the motor's winding failure directly deviates the motor speed, therefore the motor speed regulation is failing. On the contrary, no path from the motor speed to the control feedback avoiding the sensor signal exists (see Figure 3), therefore it is concluded that the control feedback function is not failing.

TABLE II. FMEA of the motor control system

Component	**Failure**	**Effect on system's functions**
Controller	Functional error (Control feedback signal)	Control feedback failure
	Functional error (PWM signal)	Motor speed regulation failure
Motor	Winding failure	Motor speed regulation failure
Sensor	Measure error	Control feedback failure Motor speed regulation failure

It is important to note that the results proposed by the presented methodology are in practice very conservative. Indeed if we consider that the winding failure actually induce a change in the motor's dynamics it is in practice possible that the controller can stil manage to regulate the motor's speed. Despite of this, the abstraction layers brought by the proposed approach avoid the consideration of this and pessimistically predict the failure of the regulation function as shown in Table II.

VI. Conclusions and perspectives

The proposed method allows the generation of FMEAs, based on systems' models made of directed interconnected components. The knowledge or assumption of the possibly existing relation between inputs and outputs of components is used to predict how a failure may impact the different variables of a system and then which function of the system may fail. The presented approach has been developed with the aim to be integrated into computer programs to automate the generation of FMEA.

The main advantage of the proposed method is its capacity to overcome the lack of components' behaviors knowledge. The philosophy used in this development is to reproduce the mental reasoning that safety experts may rely on when facing components for which the evaluation of the exact behavior is too complex to achieve (for instance integrated circuits).

The components' input/output relationships can be saved and stored to form a library and then be reused in further projects. Furthermore, causality graphs (Figure 3) can be combined to assess the safety of larger systems. Considering that staying in a safe state is a function of the system, it seems possible to estimate whether the system can reach dangerous states and then assess the criticality of functions' failure.

Although the proposed method has been successfully applied to an academic use case, its main drawback is to be very conservative and therefore risk to provide results that are too pessimistic to be really pertinent. To better document this point and confirm the interest of the proposed method, its application on large industrial cases is now to be conducted.

References

[1] Struss, P.: Automated Failure-modes-and-effects Analysis of Embedded Software. In: 2nd International Workshop on Software Health Management, Palo Alto (2011).

[2] Fraracci, A.: Model-based Failure-modes-and-effects Analysis and its Application to Air-craft Subsystems. (2008).

[3] Struss. P, Fraracci. A.: Modeling Hydraulic Components for Automated FMEA of a Braking System. In: Proceedings of the Annual Conference of the Prognostics and Health Management Society, Fort (2014).

[4] Bieber, P., Bougnol, C., Castel, C., Kehren, J. H. C., Metge, S., Seguin, C.: Safety Assess-ment with Altarica. Springer US EBooks, pp 505–510, (2004).

[5] Picardi, C. Console, L. Berger, F. Breeman, J. Kanakis, T. Moelands, J. Collas, S. Arbare-tier, E. De Domenico, N. Girardelli, E. Dressler, O. Struss, P. Zilbermann, B.: AUTAS: a tool for supporting FMECA generation in aeronautic systems. In: European Conference on Artificial Intelligence, p 750–754, (2004).

[6] Price, C.: AutoSteve: Automated Electrical Design Analysis. In: European Conference on Artificial Intelligence, p 721-725, (2000).