Model Driven Hardware-in-the-loop Fault Analysis of Railway Traction Systems

Jon del Olmo, Javier Poza, Fernando Garramiola
University of Mondragon, Faculty of Engineering
Loramendi 4, 20500 Mondragón, Spain
{jdelolmo,jpoza,fgarramiola}@mondragon.edu

Txomin Nieva, Leire Aldasoro
CAF Power and Automation
Poligono Katategi, 20271 Irura, Spain
{tnieva,laldasoro}@cafpower.com

***Abstract*—Classical Dependability Analysis techniques, such as Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis, have been used during the last decades to demonstrate the reliability, availability, maintainability and safety of industrial equipment. One of the main challenges that these techniques have to overcome is the complexity of current systems, in which more than one engineering domain is involved and many different subsystems interact. In order to facilitate the analysis of fault modes and their effects, some researches have proposed to use models as a tool to merge fault related information with structural and behavioural information. This kind of approach, also known as Model Based Analysis, pretends to develop extended models that can be shared by design and safety engineers. This paper is an example of Model Based Dependability Analysis and Fault Injection applied to a railway traction application. A Hardware-in-the-loop platform was built to inject faults in the model of the traction system and analyse the behaviour of the Traction Control Unit. As a case study, the effects of the faults in current sensors have been analysed. Phase current sensor faults were simulated and effects were identified using the platform. According to the preliminary FMEA and the experience of the technical support team, these faults are the most challenging ones in terms of detection and maintenance. The results show that a preliminary theoretical FMEA can be enhanced using the proposed model-based methodology.**

***Keywords*—Dependability, Faults, Hardware-in-the-loop, Model-driven development, Railway Traction, Variable Speed Drives.**

I. Introduction

For some years now, Dependability Analysis has been a key task in the design and manufacturing process of power electronic devices. In industries such as automotive, railway and aeronautics, the risks and the hazards that a system has to manage must be taken into account throughout the whole life-cycle. It is not enough to make a dependability analysis once the product is designed and validated with the sole purpose of getting a safety certificate. The assessment of the dependability of a system has to be performed as early as the requirement definition stage. Moreover, the increase in the interest for concepts such as reliability and maintainability is linked to the business model heavy machinery industries are developing. They do not only manufacture equipment, they also maintain, repair and refurbish it. Technical support is seen as a way to increase incomes in addition to equipment sales with limited warranties and subsequent parts supply [1]. As it was mentioned in [2], such a business model is making manufacturers explore new strategies in the field of maintenance. Their main objective is to reduce life cycle costs and maximise profits. In order to minimise life cycle costs, one research area has been the development of monitoring and diagnostic systems for maintenance tasks [1]–[3]. Another research area is related to the development of new dependability analysis methodologies [4], [5].

One of the problems that manufacturers have to face is that the team responsible for the dependability analysis might not know in detail the architecture or the behaviour of the system. Techniques such as Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) are used during the assessment, but they rely on informal models or on specification and requirement documents. Moreover, the quality of the analysis depends on the ability of the analyst to predict how the system will fail, and it often is very subjective [6], [7]. In [8] another two limitations are mentioned: the difficulty to represent the dynamic behaviour of the system and the lack of resources to handle complex systems and interrelated failures.

In this context, there have been some efforts to merge these two fields (product design and dependability) and develop new dependability analysis techniques. One of these techniques proposes to integrate analysis of faults and effects in the models used to design, develop, simulate and validate systems. The goal is to set a common framework for safety and design teams. Model Based Dependability Analysis benefits from the structural and dynamic description of the models to obtain more accurate results. Following this strategy, this paper presents a methodology for Failure Mode and Effects Analysis based on a Hardware-in-the-Loop (HIL) platform and fault injection. The goal of the study has been to analyse the behaviour under fault of the control and protection strategy executed in a railway Traction Control Unit (TCU). It will be shown that following the steps of this methodology qualitative and quantitative information can be obtained to improve the current dependability analysis.

II. Dependability Analysis Techniques

A. Classical techniques

Among these methods, there are inductive and deductive techniques. On the one hand, deductive or top-down methodologies take an undesired event and deduce its causes using information related to the system behaviour. One of these techniques is the Fault Tree Analysis and it is a graphical representation of all the sequential or parallel faults that can

This work has been partially supported by the programs: Universidad Empresa (UE-2014-09) and Formación de Investigadores del Departamento de Educación, Universidades e Investigación from the Basque Government

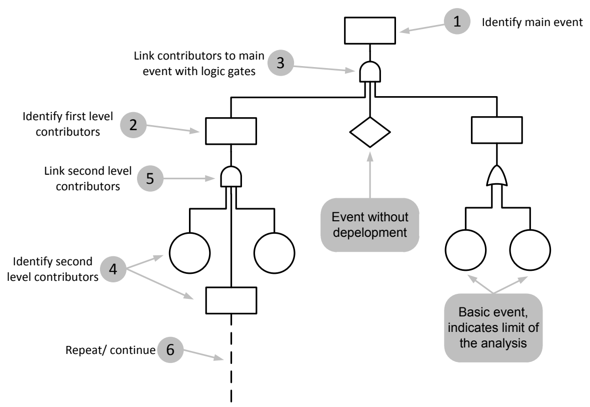
1
Identify main event
Link contributors to main event with logic gates
3
Identify first level contributors
2
Link second level contributors
5
Event without depelopment
Identify second level contributors
4
Basic event, indicates limit of the analysis
Repeat/ continue
6

Fig. 1. Fault tree structure and generation process

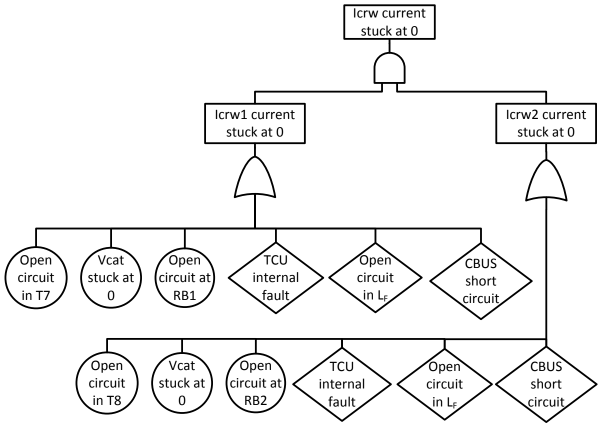

Fig. 2. Fault tree for two leg braking chopper

lead to an undesired event. The tree is generated for its top event following the process presented in figure 1, and it represents a unique fault mode, hence, one fault tree does not model all the possible faults present in a system. Once the main event is selected, first level contributors are identified and their link to the main event is represented using logic gates. In this way the tree states which combination of events leads to the top event. Several iterations are performed until basic events or events that can not be developed are found. Figure 2 shows an example Fault Tree for a two leg braking chopper of a railway traction system. In this case basic events are open circuits in the components of the chopper leg or a missing catenary voltage. There are also other events that are not developed, since they are considered as external failures that need to be studied further, such as the Traction Control Unit (TCU) internal failure.

On the other hand, inductive or bottom-up techniques, take a component, make a list of fault modes and try to identify systematically the effects of each mode in the component, the subsystem and the system. The best-known technique among these is the Failure Mode and Effects Analysis (FMEA). The result of this kind of analysis is a FMEA table (see table I). This methodology is defined as a systematic process to identify design and process faults before they happen with the aim of minimising the risks [9]. Fault modes are listed and classified depending on their probability of occurrence, severity and probability of detection. These three variables are used to calculate a Risk Priority Number (RPN) and to rank corrective action needs [10].

B. Model-Based techniques

Classical methods propose systematic strategies to analyse fault modes and their effects, but mainly depend on the quality of the information available for safety engineers. However, during the design stage only the normal behaviour of the system is modelled and there is little information about what could fail and which effects one should expect. Therefore, the result of a classical safety analysis might be superficial and might not help improve the design before it is tested.

Model-Based Analysis techniques have been proposed as a possible solution to this problem. This group of techniques uses models to characterise and simulate fault modes. They extend fault-free models to include faulty components and allow replicating the behaviour of the system under faulty conditions. Fault Injection or Model Checking is one of these methodologies [11]. The block diagram in Figure 3 describes Fault Injection. The main goal is to gather in one model the information from fault-free models and fault related data. On the one hand, design and validation engineers provide the methodology with formal models that describe accurately the behaviour of the system. On the other hand, safety analysts provide the fault injection approach with knowledge about failures and failure modes. The result is an extended model capable of replicating the faulty behaviour of the system, with the advantage that it takes into account operation modes and the dynamic behaviour. The extended model is simulated in an analysis platform, also known as Model Checker, to get new information about fault effects and check if the developed system complies with safety requirements.

The advantage of this method is that it allows reusing models used in the design and validation stages. Furthermore, the dynamic behaviour of the system can be analysed, including changes in control modes and corrective actions. Hence, thanks to fault injection, dependability analysis can take into account the interaction between different subsystems. Compared to classical techniques, Model Based Dependability Analysis provides more accurate results from a qualitative and quantitative point of view [6].

The work presented here is a practical example of Model Based Dependability Analysis and fault injection, applied to the field of railway traction and the generation of enhanced FMEAs. In this case, a Hardware-in-the-Loop platform is proposed as an analysis tool. The platform is composed by a commercial TCU and an OPAL-RT real time simulator with models implemented in Matlab/Simulink.

III. HIL PLATFORM DESCRIPTION

A. Hardware Description

Figure 4 shows the structure of the platform. It is divided into two main parts: the plant and the control.

TABLE I
FMEA FOR CURRENTS SENSOR IN RAILWAY TRACTION CONVERTER UNIT

Component	Mode of operation	Fault mode	Cause	Local effect	System effect	Train effect
Phase current sensor	Traction/Braking	Measurement bigger than real value	Component internal fault	False measurement	Inappropriate control. Overcurrent	Disabled traction unit
Phase current sensor fase	Traction/Braking	Measurement smaller than real value	Component internal fault	False measurement	Inappropriate control. Overcurrent	Disabled traction unit

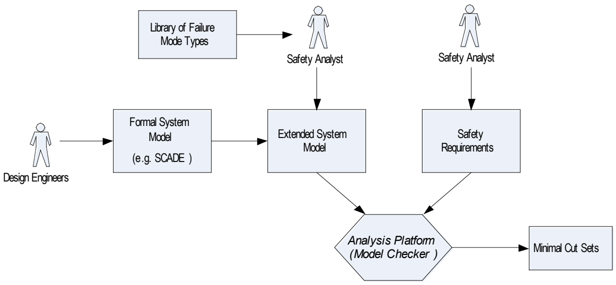

Fig. 3. Fault Injection Approach ([11])

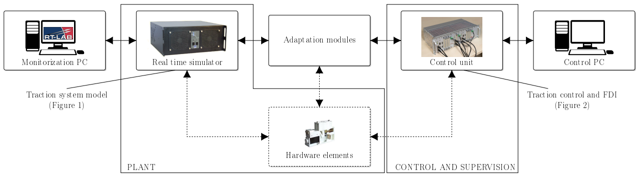

Fig. 4. HIL platform structure

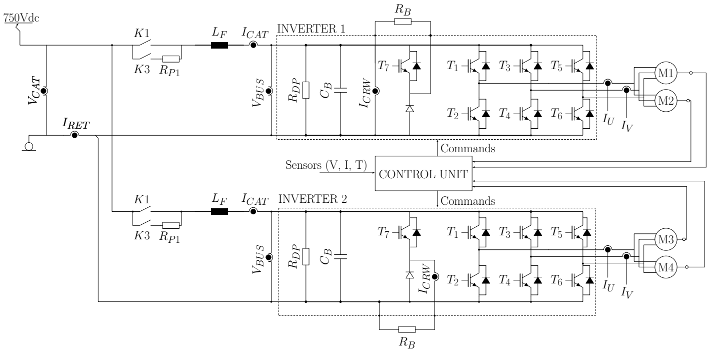

Fig. 5. Electric traction unit schematics

The traction converter unit is simulated in the OPAL-RT real time simulator. Its main characteristic is that models can be implemented in Matlab/Simulink, so there is no need for advanced programming skills. This feature is particularly useful when the model has to be modified constantly to inject different faults. It has several digital and analogue input/output cards to interact with external devices. In this case the external device is the TCU. The control and protection strategy is executed by the TCU and by the control computer. The TCU is a modular commercial electronic control unit developed by CAF Power&Automation for railway applications. The functionalities of the control software include the loading/unloading of the bus, the control of the inverter and the management of the protections and alarms. The control computer is used to send commands to the TCU and monitor its internal variables.

Moreover, there are several adaptation modules that convert the output signals of each device. The TCU is a fully functioning commercial control unit, so it is only prepared to work in a train. Therefore, adaptation modules are required to convert the simulator output signals to the voltage and current levels of the control unit and the other way around.

Finally, it is also considered the option to connect some real components (like sensors or circuit breakers) to the platform. This would facilitate the testing of worn out elements and the analysis of the effects in the performance of the control strategy.

B. Traction System Description and Modelling

For the study presented in this article, the reference system to be modelled was a tram traction unit developed by CAF Power&Automation. The main characteristics of the unit are shown in table II. It is a DC traction unit composed by two inverters that is capable of controlling four induction motors, two by each inverter. The topology can be seen in detail in figure 5.

TABLE II
TRACTION UNIT CHARACTERISTICS

Maximum power	500 kW
Output max. current	370A
Catenary voltage	750 Vdc
Suppy voltage range	500 - 900 Vdc
Output voltage	565 V_{rms} (V_{cat} = 750 V_{dc}) 680 V_{rms} (V_{cat} = 900 V_{dc})

A reduced model of the traction unit has been implemented. Only one of the inverters has been included for the sake of simplicity and computational cost. The input filter and the braking chopper have been built using the SymPowerSystems toolbox of Matlab/Simulink. The models of the inverter and the traction machine are analytical simplified models. The induction machine uses a two phase $\alpha\beta$ model and a simplified first order mechanical system as a load.

IV. HIL BASED FMEA ANALYSIS

With the aforementioned testing platform the process presented in figure 3 has been performed. The steps of the methodology to generate an advanced FMEA are described in the following lines.

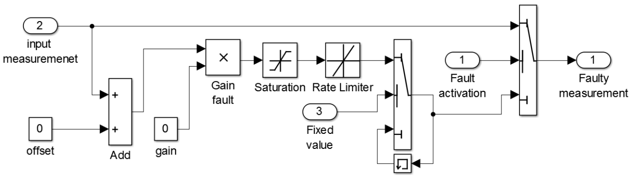

Fig. 6. Sensor fault injection block

A. Formal system modelling and simulation

The first step involves modelling and simulating the formal model. In this respect, this model-based strategy has the advantage that it shares the models already developed in the design stage. With a few changes, the real time simulator is able to replicate the behaviour of the traction converter unit. The TCU runs the control software and sends the commands for the circuit breakers and the IGBTs. As it was mentioned before it is a commercial equipment, so it runs the same code as in the real application.

B. Preliminary FMEA

To prioritize fault modes, a preliminary FMEA should be generated using descriptive documentation of the system and the knowledge of the technical support teams. In this case, since the TCU has been used in several projects during the last years, the FMEA has been enhanced including new information about fault modes and effects detected in real-life scenarios. Thus, it is considered as a good starting point for the real-time simulations in the HIL platform. If the equipment being tested is a prototype in its design and validation stage, there will be limited information about fault modes and effects. Therefore, the HIL based FMEA analysis will start from a theoretical FMEA.

This preliminary analysis will help prioritize fault modes with the most severe effects. To this end, it is important to specify the active operation modes when the faults occur. For instance, the FMEA should state the following operation conditions:

- Traction unit in traction or breaking
- Flux and torque references
- Control mode
- Control strategy configuration

C. Extended Models

Once the fault-free model has been validated and the fault modes are selected, the model has to be extended to include the fault injection subsystems. Figure 6 shows the structure used to simulate sensor faults. In particular, this subsystem introduces among others gain, offset, noise and disconnection disturbances in the measured currents and voltages.

D. Fault injection and real time simulation

The next step in the generation of an advanced FMEA is the real time simulation of the system. The conditions specified in the preliminary FMEA should be replicated. Data about the behaviour of the system under faulty conditions is obtained from the simulations. In this case, as the TCU has some protection and fault management functionalities, its response capacity can be assessed.

E. Enhanced FMEA generation and TCU Validation

From the data obtained in the fault injection and real time simulation step, the FMEA can be modified to include the effects identified in the platform. Its use makes easier to quantify the effects of each fault mode in terms of torque and speed changes or harmonic components. Additionally, it should be taken into account that the control works in closed loop, so it always tries to compensate any disturbance in the system. This fact makes difficult to characterise the effects of a fault with only theoretical knowledge about the system. Real time simulations help performing this task.

The last step is the validation of the system with regard to the dependability requirements.

V. A CASE STUDY: SENSOR FAULT SIMULATIONS

In the following section a case study conducted to test the applicability of the methodology will be presented. Phase current sensor faults were simulated and effects were identified using the platform. According to the preliminary FMEA and the experience of the technical support team, these faults are the most challenging ones in terms of detection and maintenance. Current sensors are used to estimate flux and torque, so under faulty conditions the control strategy is misled and it sets the wrong operation point. Moreover, current sensor gain and offset faults appear in fault logs as overcurrents, since the control loop performance rapidly gets worse and the traction unit is forced to shut-down (see FMEA in table I).

A. Offset faults

An offset fault mode in the phase current measurements generates a sinusoidal oscillation in the electromagnetic torque of the motor. The frequency of the oscillation is equal to the frequency of the stator current. This phenomenon can be demonstrated performing the Park transformation to the stator three phase currents [12]. The oscillation is also found in the catenary current and the bus voltage. To see the effect of the fault with the closed loop control strategy, an offset of 100A was injected using the real time model at 600 rpm (20 Hz) and 660 Nm. Figure 7 shows the current in the model and the current measured by the control unit. When the fault is injected at t = 118.65 s, the measured current tends to increase suddenly. The control strategy compensates this changing the commands for the inverter to stabilise the system. This happens because it estimates that the torque of the machine is deviating from the reference value. Thus, as it can be seen in figure 7, the measured current maintains the amplitude it had before the fault. However, the real current is modified.

Figure 8 presents the reference, estimated and real torque. The control strategy commands the inverter to make the torque and flux estimates follow their references. It can be seen that after the fault is applied a new oscillating component

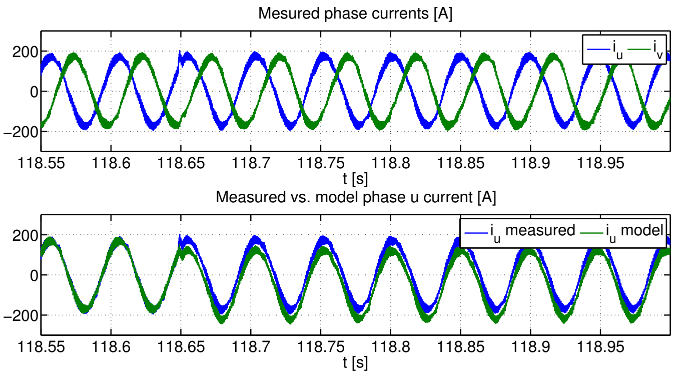

Fig. 7. Model current and measured current with 100 A offset (fault in t = 118.65 s)

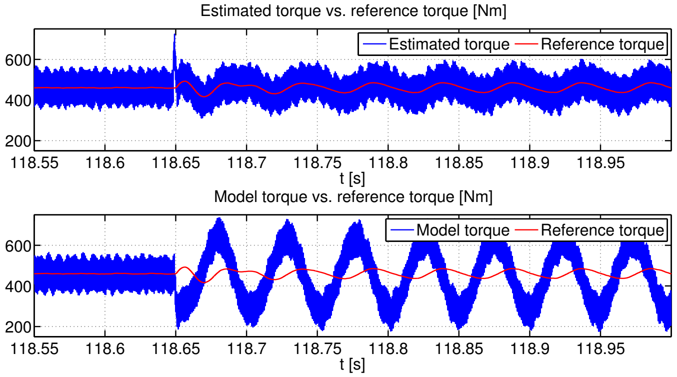

Fig. 8. Electromagnetic torque with 100 A offset (fault in t = 118.65 s)

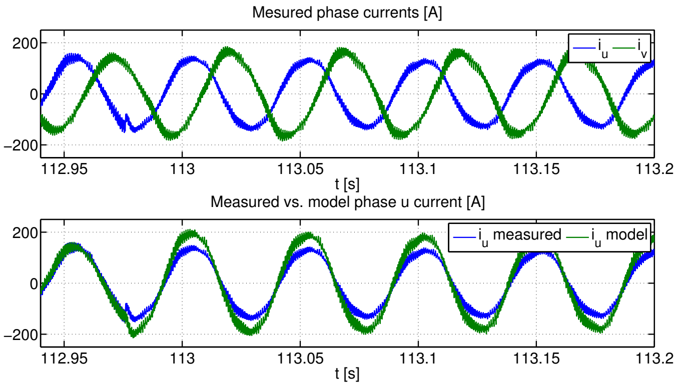

Fig. 9. Model current and measured current with 30% less measured current (fault in t = 112.98s)

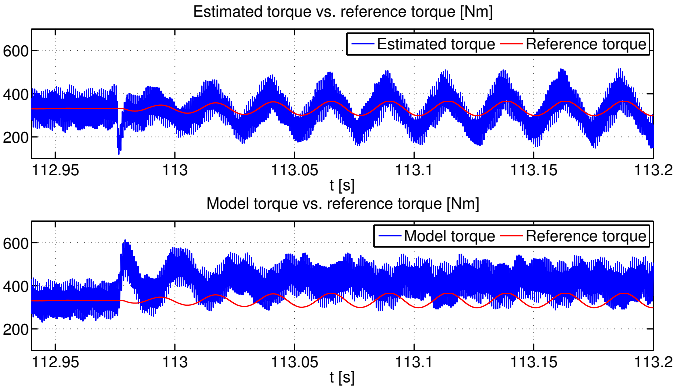

Fig. 10. Electromagnetic torque with 30% less measured current (fault in t = 112.98s)

appears in the torque. With a more detailed analysis, it can be concluded that its frequency is the same as the supply frequency of the machine. The average value of the torque is maintained in the reference point.

In conclusion, it can be said that the traction unit continues working even if there is an offset in the currents. The protection system does not activate any alarm, so the operation is still considered safe. Nevertheless, the normal operation of the unit is not guaranteed for large offset values, since torque oscillations could affect the overall performance and comfort of the train, to the point where the driver has to disable manually the traction unit.

B. Gain faults

As in offset faults, sensor gain faults generate oscillations in the torque of the traction machine. In this case, the frequency of this new component is equal to twice the supply frequency [12]. In addition, the torque is controlled above or below its reference value.

When the gain is less than one, the control strategy estimates less torque and tends to control the inverter to supply more current. In that way it compensates the virtual loss of electromagnetic torque that sees due to the fault. Figure 9 shows measured and model currents at 600 rpm and 300 Nm for a sensor gain of 0.7 (the sensor measures 30 % less current). In the upper graph the amplitude difference between phase u and phase v current measurements can be seen. In the lower graph it is shown that the measured current decreases at t = 112.98s. The control loop immediately compensates the change increasing the current to maintain the flux and torque estimations. Hence, the measured current in phase u has the amplitude it had before the fault.

Another effect of the fault is that the real torque is controlled above its reference. When the fault is applied, the estimated torque deviates from the command, so the control strategy asks

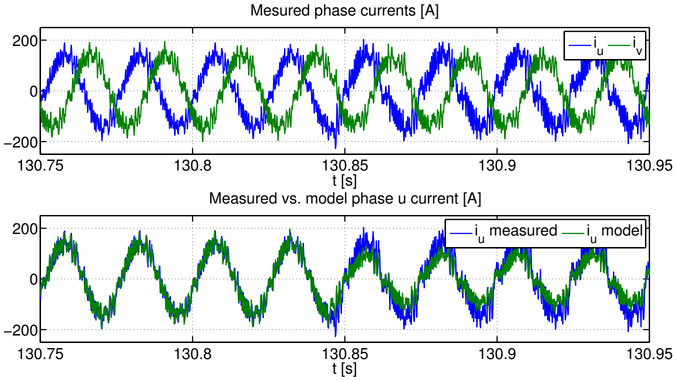

Fig. 11. Model current and measured current with 50% more measured current (fault in t = 130.85s)

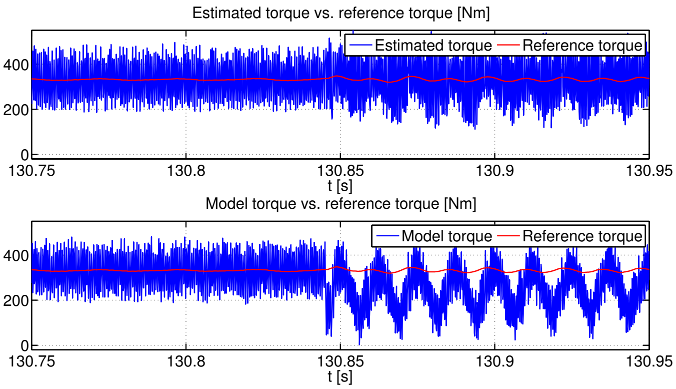

Fig. 12. Electromagnetic torque with 50% more measured current (fault in t = 130.85s)

for more stator current. The estimated torque goes back to the previous value but the real torque increases (see figure 10).

When the gain is more than one, the effect is the opposite one. As it is shown in figure 11, at time instant 130.85s, the measured current's amplitude increases. To compensate the change in the flux and torque estimations, the current in the stator is decreased by the inverter. Therefore, the real torque is controlled below its reference value (see figure 12). A gain error has a double effect in the control of the traction system. On the one hand, it generates an oscillation in the torque with apparently no consequences in the performance of the simulated traction unit. As it has been said before, depending on the magnitude of the fault, it could provoke overcurrents or comfort issues, especially if it is an abrupt fault.

On the other hand, the electromagnetic torque is not correctly controlled. This could affect the overall operation of a traction unit, since nowadays this kind of traction units are part of a distributed traction system with more than one converter unit. If one of those units is generating more or less torque than the command, the rest would need to be reconfigured to maintain the reference speed.

C. Information for enhanced FMEA

From the simulation results presented in previous sections, information for an enhanced FMEA can be obtained. From the qualitative point of view, the FMEA presented in table I only stated that overcurrents would occur and that the control would be inadequate in case of a current sensor measuring more or less than the real value. Considering the results from the HIL platform, the inappropriate control can be defined as the torque being controlled below or above the reference value. Moreover, an oscillation and its frequency were identified. From the quantitative point of view, a gain error value can be linked with a torque deviation. For example, in the case shown in figure 12, it can be seen that the real torque is 100 Nm below the reference value.

VI. Conclusion

In this article a methodology to generate advanced FMEA analysis has been presented. The main objective of the strategy is to reuse the models developed during design and validation stages to improve previous dependability analysis results. The main advantage of this approach is that the HIL platform allows testing the performance and behaviour of the system under faults. More detailed qualitative and quantitative information about fault modes can be obtained in this way. It is worth mentioning that using a HIL platform, with the same TCU (HW&SW) than in the real application, exactly the real dynamic behaviour of the control and the protection system can be tested. In addition, the methodology has been used to assess the effects and enhance the dependability analysis related to phase current sensor faults in a railway traction application. It has been shown how a systematic process including real time simulations can improve theoretical studies. Moreover, fault indicators that will help in the design of new diagnosis and maintenance strategies were identified. The platform has demonstrated itself to be a powerful tool and it should be used in the validation process of TCUs, not only to test control strategies (as it is common nowadays), but also to analyse systematically the behaviour of the control system under faulty conditions.

References

[1] A. Varma and N. Roddy, "ICARUS: design and deployment of a case-based reasoning system for locomotive diagnostics," *Engineering Applications of Artificial Intelligence*, vol. 12, no. 6, pp. 681–690, 1999.

[2] M. Farnsworth and T. Tomiyama, "Capturing, classification and concept generation for automated maintenance tasks," *CIRP Annals - Manufacturing Technology*, pp. 8–11, apr 2014.

[3] J. Gandibleux, "Contribution to embedded monitoring/diagnosis architectures dependability assesment. Application to the railway transport," Theses, Université de Valenciennes et du Hainaut-Cambresis, 2013.

[4] Y. Papadopoulos, D. Parker, and C. Grante, "A Method and Tool Support for Model-based Semi-automated Failure Modes and Effects Analysis of Engineering Designs," *Ninth Australian Workshop on Safety-Related Programmable Systems (SCS 2004)*, vol. 47, pp. 89–95, 2004. [Online]. Available: http://crpit.com/confpapers/CRPITV47Papadopoulos.pdf

[5] F. Mhenni, N. Nguyen, and J.-y. Choley, "SafeSysE : A Safety Analysis Integration in Systems Engineering Approach," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–12, 2016.

[6] A. Joshi and M. P. E. Heimdahl, "Model-based safety analysis of simulink models using SCADE design verifier," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3688 LNCS, pp. 122–135, 2005.

[7] L. Grunske, K. Winter, N. Ytapanage, S. Zafar, and P. A. Lindsay, "Experience with fault injection experiments for FMEA," *Software - Practice and Experience*, vol. 41, pp. 1231–1258, 2011.

[8] J. I. Aizpurua and E. Muxika, "Model-Based Design of Dependable Systems : Limitations and Evolution of Analysis and Verification Approaches," *International Journal on Advances in Security*, vol. 6, no. 1, pp. 12–31, 2013.

[9] T. I. M. C. Association, *Failure Modes & Effects Analyses (FMEAs)*. The International Marine Contractors Association, 2002, no. April.

[10] Sematech, "Failure Mode and Effects Analysis (FMEA): A Guide for Continuous Improvement for the Semiconductor Equipment Industry," p. 27, 1992. [Online]. Available: http://www.sematech.org/docubase/document/0963beng.pdf

[11] O. Lisagor, D. J. Pumfrey, and J. a. Mcdermid, "Towards a Practicable Process for Automated Safety Analysis," *24th International System Safety Conference (ISSC)*, pp. 596–607, 2006.

[12] D.-W. C. D.-W. Chung and S.-K. S. S.-K. Sul, "Analysis and compensation of current measurement error in vector-controlled AC motor drives," *IEEE Transactions on Industry Applications*, vol. 34, no. 2, 1998.