A General Approach to Study the Reliability of Complex Systems

G. M. Repici, A. Sorniotti

In recent years new complex systems have been developed in the automotive field to increase safety and comfort. These systems integrate hardware and software to guarantee the best results in vehicle handling and make products competitive on the market.
However, the increase in technical details and the utilization and integration of these complicated systems require a high level of dynamic control system reliability. In order to improve this fundamental characteristic methods can be extracted from methods used in the aeronautical field to deal with reliability and these can be integrated into one simplified method for application in the automotive field.
Firstly, as a case study, we decided to analyse VDC (the Vehicle Dynamics Control system) by defining a possible approach to reliability techniques. A VDC Fault Tree Analysis represents the first step in this activity: FTA enables us to recognize the critical components in all possible working conditions of a car, including cranking, during 'key-on'-'key-off' phases, which is particularly critical for the electrical on-board system (because of voltage reduction).
By associating FA (Functional Analysis) and FTA results with a good FFA (Functional Failure Analysis), it is possible to define the best architecture for the general system to achieve the aim of a high reliability structure.
The paper will show some preliminary results from the application of this methodology, taken from various typical handling conditions from well established test procedures for vehicles.

Keywords: safety, systems reliability, fault tree analysis (FTA), functional analysis (FA), handling, vehicle dynamic control (VDC).

1 Introduction

Automobiles and land vehicles in general have seen a dramatic increase in complexity in recent years. Today's automobile presents a higher than ever, and increasing, number of value-added features, many of which are controlled by the vehicle's electrical and electronic (E/E) system. In fact, a vehicle today has approximately twice as many E/E functions as one produced just 10 years ago. This trend requires electrical system designs that provide both increased functionality and increased reliability. This inflation effect has been caused mainly by two factors: the first is rising demands from the consumer. This has not only manifested itself through the desire for better performance or comfort, but also stems from increased awareness of safety related issues and more protection for the occupants of the vehicle. The second factor has been the development of various electronic techniques and equipment. This technology has pushed the limits imposed by the on-board systems and, specifically, has allowed the implementation of many functions controlled by hardware and software systems on board.

It is common practice when buying a car nowadays to find under the hood and scattered throughout the vehicle kilometres and kilometres of cables and wires, multiple control boxes and an equally high number of sensors picking up a very wide range of physical parameters. On top of this, all the electronic systems on board a car are interfaced in some way or another with themechanical and hydraulic systems.

An example of typical functions now under the control or assistance of electronics is the control function. This affects the ride and the handling performance, above all else. When the driver makes a sudden manoeuvre, control is critical. It is just as essential in bad weather or on rough roads, especially on unpredictable road surfaces. Even under normal conditions, on straightroads and turns, or during braking and acceleration, control determines the ride and handling performance. Often, the level of control depends on the skill of the driver. The ride and handling technologies emerging in the industry help offer significantly more control for every driver in every situation, regardless of skill [1]. However, all this comes with a price tag. This is not only in terms of the final price for the user, but also in terms of increased design complexity that places heavier loads on the design engineers and extends the time to prototype and testing. This is a key point that has been taken as a key driver in our methodology. Later we will uncover how integrating the different analyses in an intelligent way can provide a way to develop preliminary estimates early in the development. In this context the complex system identified has to be intended as the ensemble of subsystems in a vehicle integrating different and advanced functions. To give a brief idea, the list of various state-of-the-art technologies applied might include: Higher- and multiple-voltage power generation and storage, Networked communications (multiplexing), Fiber-optic communications, Multi-drop wiring, Networked controllers with distributed computing, standard interfaces, and mechatronics (electronics integrated into switches, connectors, sensors, and actuators). Fig. 1 shows a generic vehicle encompassing a set of advanced circuitries and components.

Turning to the aerospace field, we can see how avionics [5] has been a relevant part of the development of an airplane since the late 1940s. It has since developed into a variety of lesser streams, covering the most various functions on an airplane: communications, navigations, control, etc. It still is at a level of complexity much higher than that of a car, but several system are comparable in terms of functions and criticalities. Since some of the electronics mounted on a vehicle oversee safety, and the development of some specific aspects can be derived from analogous activities from the aerospace industry. In particular we would like to point out here how evolution in avionics design has shifted with hardware miniaturization and the concomitant architectural integration strategies [2].

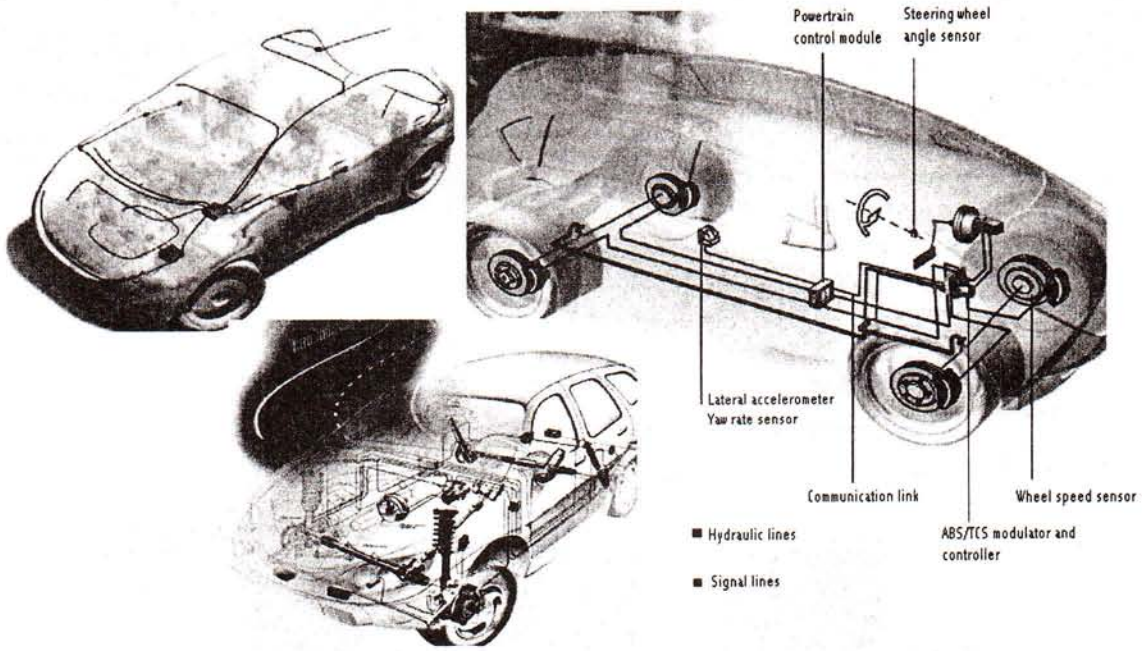

Fig. 1: Modern vehicle circuitry schematics (Courtesy of Delphi Automotive Systems)

In its basic form, an aircraft avionics system can be viewed as a large number of interconnected computers. Up to the 1980s there would be about ten computers, going up around 30 for bigger airplanes. The capabilities developed over recent years have allowed a switch from these so called federated architectures to a system integration approach. Basically, that functions can be mapped onto hardware as integrated computer nodes. The base line for an avionics architecture can be represented as in Fig. 2. This can be taken as a starting point for an analysis that will lead us to transition development methodologies aimed at taking the higher reliability levels achieved in aerospace into the automotive field.

Aside from the specific architecture, which is not under discussion in this work, we have recognized how some typical methodologies have been applied in, in a slightly different way the aerospace field than in the automotive field. In particular, well known analyses like FA (Functional Analysis), Fault Tree Analysis (FTA) and Failure Modes and Effect Analysis (FMEA) [9], have all been used extensively and have undergone improvements [6], [7]. Most significantly, however they are all inserted in a well structured methodology that allows results and trade information to be gathered from the very beginning, so that the overall results can be evaluated. A major advantage of this approach is the integration of all the analyses, both horizontally and as vertically over the different levels of definition from equipment up to system level. It is not necessary to recollect and reframe the results since the analysis are all interlaced among them and they are evolved from common standpoints.

At this point it is thus clear how this operational way can be exported to the automotive sector with great advantage in terms of development and overall reliability.

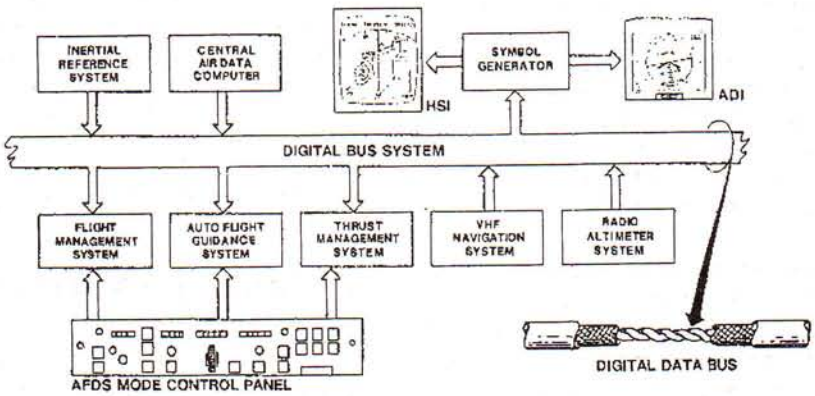

Fig. 2: Typical bus configuration for elementary on board avionics [3]

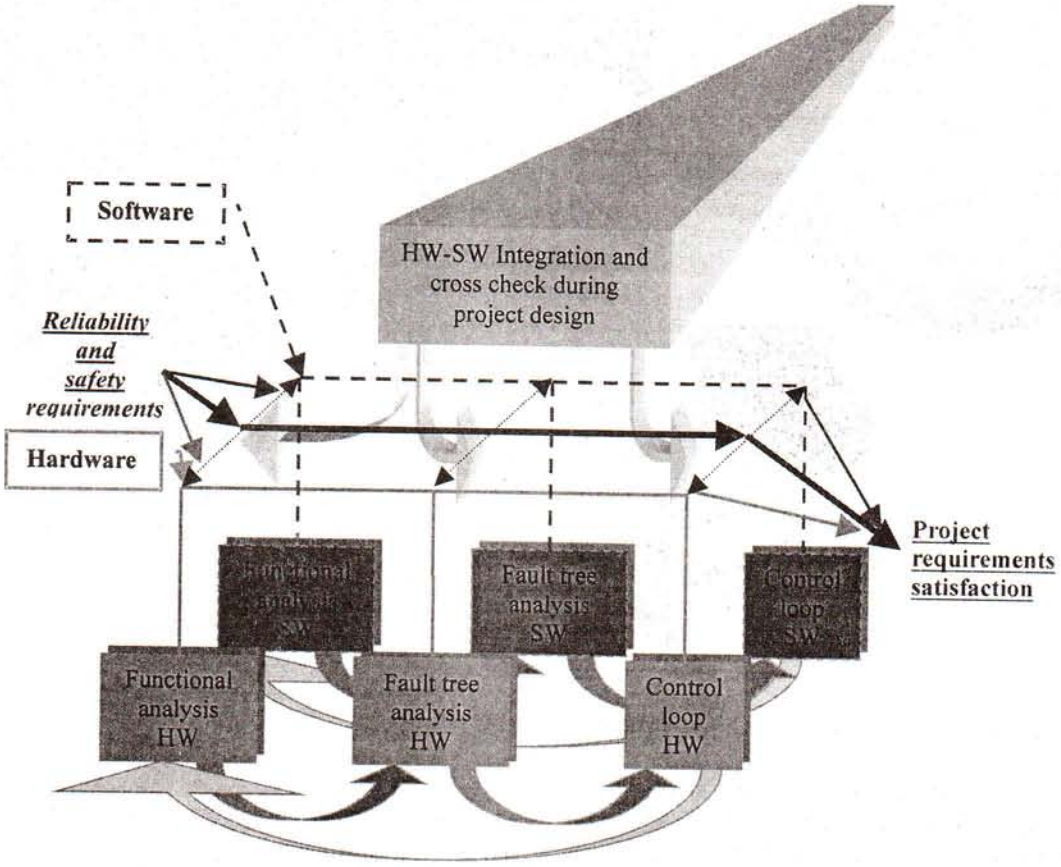

Fig. 3: Overall scheme, methodology

2 Study scheme

Starting from the background illustrated in the previous paragraph, we have identified the main target of our study as the definition of a general methodology to support, as an ancillary analysis, the development of the design of automotive systems complex. This will essentially be aimed at reaching a consistent level of reliability and safety. These are features intended for a generic system encompassing electro-mechanical components and containing consistent software functions. Our purpose has been to develop a true methodology. Though not as complex as others available in the literature [4], it will have the great advantage of being extremely lean and widely applicable. One of the main features is the possibility, which we intend to make use of, to apply it from the very beginning of the design, accompanying all the phases of the development of the project. Moreover, our intention has been to define in an objective way, the requirements necessary to develop all the related subsystems as well as the embedded software. All of the above will take into account the targets established at the beginning of the project.

For the time being the main developmental and test benchmarks come from the automotive industry. That is to that say some requirements have been extracted directly from the set of initial requirements and quality levels of the automotive industry. The purpose is to obtain significant reliability data well before the tests are launched, and in this way to identify the critical issues and act to correct them.

Fig. 3 shows the overall logic driving the study. The framework within which we have moved is given by the basic idea of integrating from the very beginning all the analyses and activities carried out, in parallel as much as possible, for both hardware and software [10]. It is essential that the developers of the software are fully aware of what is taking place on the hardware side, and vice versa. Running all the activities in parallel allows us to evaluate the impact on the different functions early in the project. As we can see from the figure, several cross checks are carried out during the development of the design. These are not intended as formal gates, but rather as check points for assessing the coherent development and exchange of information. The main drivers are the reliability and safety requirements. They are pursued all along, and each analysis is aimed at implementing , verifying then checking compliance with the target values. The analysis, as shown in Fig. 3, cascades from functional down to the control loop, through fault trees, and then back to reassess the progress, and integrate the results from downstream. The two plans, green and red for SW and HW, always move in tight parallel, maximizing the interchange.

3 Specific problem application

We now introduce the system we have chosen as a case study for the application of our methodology. Speaking in general terms, we can call Vehicle Dynamics Control System (VDC) a generic system aiming at increasing the level of safety during the operations of a common vehicle. The main func-

tion is to control the dynamic behaviour of the vehicle, intervening especially whenever the vehicle is approaching the limits of its usage envelope. As a first approach we see the action as being carried out by acting on the brakes and simultaneously controlling the torque produced by the engine.

Typically, a VDC includes functions related to the control of the braking actions (EBD), functions avoiding locking of brakes during the braking action (ABS), the traction control system (TCS), and a function controlling the release of torque in acceleration (ASR), and others. Each of the functions listed above encases several aspects and is carried out by processing various quantities. As an example we can point out here that an ABS function has to control the various degrees of longitudinal variation of attrition according to the different motion conditions. While making a turn, both longitudinal and lateral forces act on the vehicle, and also an additional function is called in, Cornering Brake Control (CBC), which takes into account the different load expressed by the internal and external wheels on the ground.

The VDC is a very complex system. It is normally made up of a number of electro-hydraulic-mechanical components. Typically we have up to twelve two-way valves coupled to the limiting components, pumps, and actuators. In order to better analyse this part of the system, a dedicated action has been devoted to modeling all the hydraulic components. This modeling is essential in order to advance the knowledge of the system and so move on from an a priori logic to a responsive system which acts according to the real vehicle-ground interaction and the conditions encountered while operating. Once again we would like to underline the importance of integrating the knowledge related to the software running the system with the physical definition of the system itself, especially the electro-hydraulic portion of it. From our point of view it is useless to investigate the physical functionalities of the system without a substantial verification of the data transmissions logics. Hence the use of several commercial software packages for testing the data buses and data interchange.

Assuming now that we want to develop a system similar to VDC, the first step is to think out the overall structure of the system. After all the main functions are identified and a thorough description has been made the next step is to start doing the preliminary design.

There are several ways of doing this; to maximizing the implementation of reliability and safety features from the very beginning [8], a potential development scheme is shown in Fig. 4.

The starting point is represented by a Functional analysis: a target function is defined, then a detailed representation of a breakdown of all the sub-functions. In this phase experts from different fields (mechanics, electronics, electrical, etc.) work together to evaluate every single function necessary to comply with the required target. when all functions are clearly identified, is possible to analyse the components implementing that function from both the hardware and software point of view.

In practical terms the theoretical structure derived from the Functional Analysis becomes a physical structure in which we can see every single element making up the general system.

At this point, a Fault Tree Analysis can be applied to the obtained scheme and verified with a control loop if the requirements are satisfied in the case of failure of various components.

The control loop is basically a series of logical steps taken by the system engineer aimed at assessing the consequentiality of all the functions and the full satisfaction through the dedicated hardware. Since the procedure has not yet been formalized, check lists are being prepared in a generalized way and will be tested as more analyses are carried out on different subsystems.

It is important to underline that it is also possible to verify through the control loop whether all fundamental functions have been correctly identified during the functional analysis step. At the end of this process we have a general system architecture from the point of view of theoretical requirements and from the point of view of both physical hardware and software elements.

As the project design unfolds, thorough adherence to the scheme assures the safety and reliability allocations can be controlled in real time.

In particular, the fault tree analysis results (see Fig. 5) can be used to check the failure rate target of each component, and so it is out relatively easy to evaluate the trade offs and part substitutions to raise the overall system reliability.

Reliability data is nowadays widely used in every engineering field. MIL-HDBK 217 and RAC are two of the most widely used documents containing collections of failure rates and other data for various components. Several specific databases have also been built throughout the years to support design choices in the field of aerospace. In the automotive field these databases are not yet fully developed to the same extent.

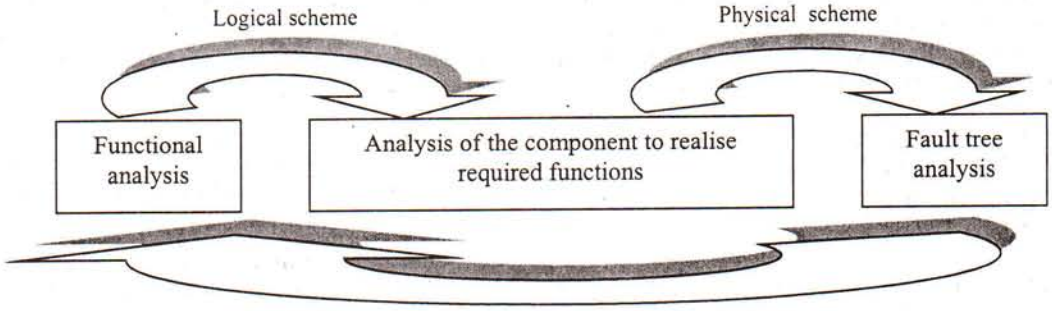

Fig. 4: Development scheme for a VDC-like system

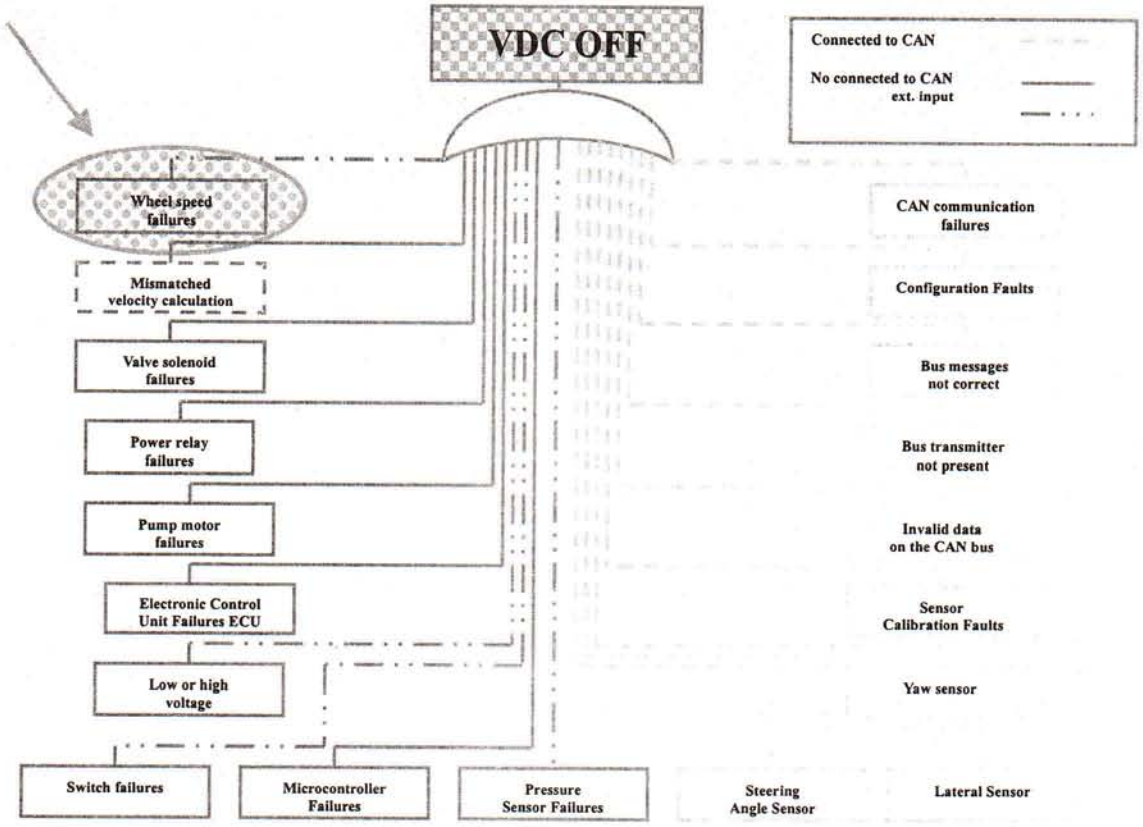

Fig. 5: VDC Fault Tree Analysis

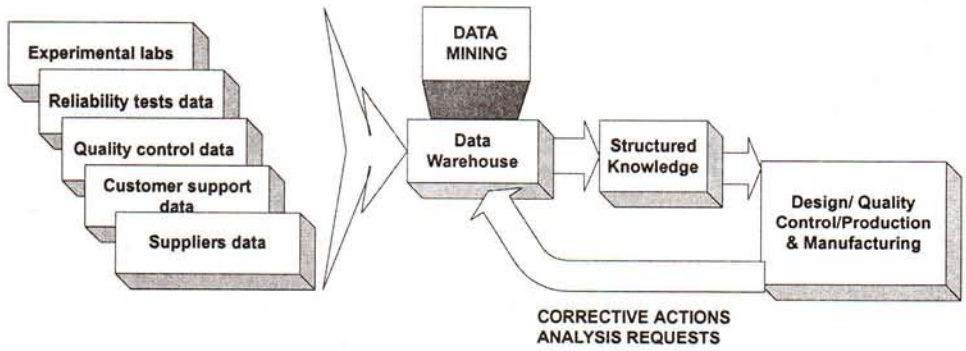

Fig. 6: Reliability data building and management philosophy

Fig. 6 shows a typical basic policy to enhance this situation. As an ancillary activity to this study the procedure shown has been partially implemented. In particular the work has been focused on increasing the data yield from subcontractors and suppliers. As far as we have seen till now, the data collection and management activities are carried out on the two different planes in two not completely compatible ways. It happens that the data relevant to the overall production is not necessarily the data that is sensitive to the equipment manufacturer. This causes biased collection, and subsequently data transmission.

Due to all of the above it is sometimes very hard to correctly evaluate the overall reliability of a complex system. In the course of the study an alternative strategy, coping with the lack of data, has been evaluated. Starting from the reliability data available, a corrective factor PM (Proceeding Mutation) is generated through a series of analyses aimed at coupling the aeronautical components (i.e., sensors) and the automotive components.

Through the correct application of this factor to aeronautical data, estimated values can be obtained for automotive elements and an approximate failure rate of these values can be calculated.

While the appropriate databases are being expanded and refined, a temporary collection of all the PM factors devised will be used and updated, constantly crossing the values with the results obtained from experimental tests.

4 Identification of the problem

Two main problems have been identified in the course of our work. They are diverse in nature, and can be solved immediately: firstly, there is the need to identify a methodology that will help, by means of graphical support, in correctly identifying the physical structure of the system being analysed. To this purpose we have looked at FA, which requires a functional description of the system, and FMEA, usually carried out to a more thorough level of detail and specific descriptions. Hence we will start out from the former, describe the main objectives that our system architecture has to comply with, and then move on to the latter to analyse the different components, their features and the potential failure modes. In doing this the two methodologies come together for whole and also work as a reciprocal verification.

The second main point we stated is that all too often the analyses from the software and hardware components are carried out separately. In this way the data gathered from the two sides, even though formally correct and complete, are not structurally integrated, and so information regarding the interactions is lost.

To repair this fault a method [4] has been developed, called Hierarchically performed Hazard Origin and Propagation Studies or Hip-Hops. These techniques are founded on the principle that all the existing methodologies function well, but need a higher degree of integration to suitably fit the most modern complex systems. The work evolves through integrating of several analyses, with the main purpose of maximizing the automation of the procedures through the development of appropriate tools and software.

5 Fault injection techniques

In order to achieve a more complete reliability analysis, it is deemed useful to analyse system reactions to hardware and software failures. The technique explained in this work, through fault injections, has proven to be cost effective and capable of providing valuable results. Using software tools like Amesim or Matlab Simulink, it is possible to develop software models to obtain a very close simulation of real events without the use of prototypes; in particular, it is possible to simulate the mathematical logic (Simulink) and physical elements (Amesim) of a generic electro-mechanical system. Analysing the mathematical equation and the logic which control the phenomena (Fig. 7 shows the traction control logic), it is possible to simulate a failure in the virtual model, using results from FTA and FA to isolate the most critical components.

In this way we can study the behaviour of the system in critical conditions and evaluate whether the general response is sufficient to guarantee the minimum safety value. In addition to this, using simulation techniques starting from hardware and software integrated FTA and FA analysis a large number of results can be obtained in a short period of time, and the correctnessof the project design can be evaluated before the construction of the physical system (i.e., the first prototypes). Fig. 8 shows the Simulink implemented scheme for fault injection. As an example in order to better understand the process, we can take a failure in the data transmission system. After injecting a generic or specific error in the transmission protocol, or the hardware implementing it, we evaluate the consequences, comparing the actual output with

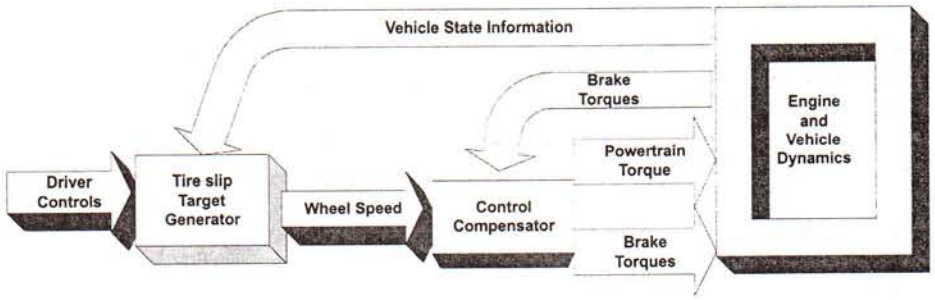

Fig. 7: Traction Control System operational logic

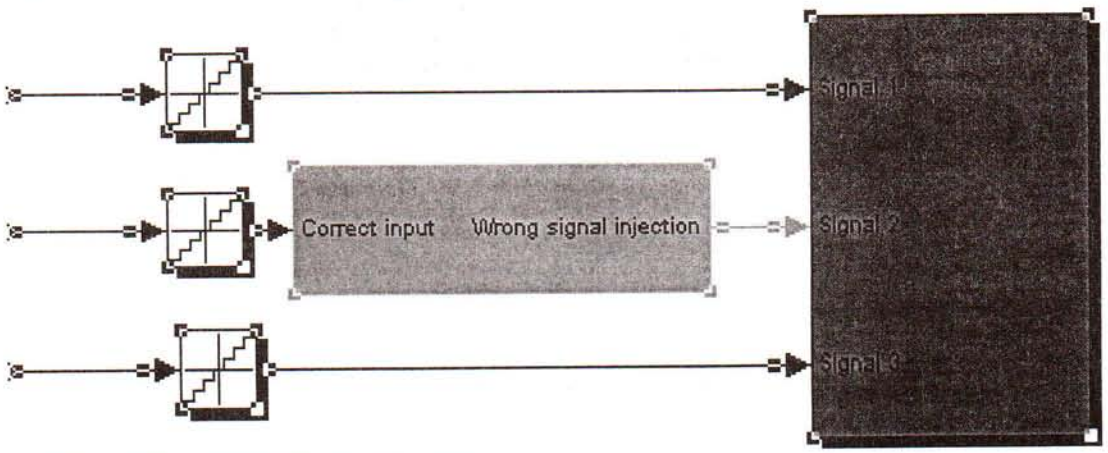

Fig. 8: Simulink scheme for fault injection techniques

the set of expected values. The consequences, both over a short period and over a long period are then evaluated. A wrong signal can be either a lack of information or a set of inconsistent bits. A preliminary result of this analysis is the establishment of the so-called safe operational time. This represents the minimum elapsed time during which the system, thanks to its robust design and reliability, can still operate within the safety limits. Later the analysis provides data about the period of latency and the reboot of the system.

6 Conclusion and recommendations

Our work has presented the preliminary results and the overall methodological approach to the problem of designing reliability and safety in automotive systems since the very beginning of the development. None of the component analyses used are brand new or innovative in themselves. That was not the purpose of the work. Nevertheless, the overall approach has been viewed as innovative and valuable in the automotive world, where interconnections between the different analyses and also between software and hardware, functional and physical analysis, are still partially lacking, at least in comparison with the aerospace environment. We have also seen how other researchers, all of them producing outstanding and valuable results, have travelled this road. What is different in this structured method is the leaner approach, aiming at applying just the minimum analysis required at the right time in the development, avoiding massive efforts for preliminary design. We have also highlighted how to let the software and hardware sides talk together right from the beginning in order to ensure that the development of the functions is correctly transformed into code and the hardware implementation evolves at the same pace.

The fault injection technique has also proven its effectiveness in supporting the assessment of the system performance in the earlier design phases. The key point is to accurately select the events to generate and support the simulations adequately, especially for those failures not easily reproducible on track.

The main advantage of applying this methodology is that is avoid common pitfalls and mistakes, especially in the earliest phases of the design, without overburdening the system with cumbersome procedures.

Acknowledgments

The authors wish to gratefully thank Prof. Paolo Maggiore for his support and invaluable help provided throughout the research work, and for reviewing this paper. He is a well known expert in the field of aerospace systems reliability analysis and design.

References

[1] Delphi Automotive Systems *Ride and Handling Systems* USA, Delphi, 2000.

[2] Newport, J. R.: *Avionics Systems Design.* CRC Press, 1994.

[3] Henderson, M. F.: *Aircraft Instruments and Avionics.* Jeppesen Sanderson Training Products Inc., 1993.

[4] Papadopoulos, Y., McDermid, J., Sasse, R., Heiner, G.: *Analysis and Synthesis of the Behaviour of Complex Programmable Electronic Systems in Conditions of Failure.* Reliability Engineering and Systems Safety 71, 2001, p. 229–247.

[5] Helfrick, A.: *Principles of Avionics.* 2nd Edition, Avionics Communication Inc., 2002.

[6] Chiesa, S.: *Affidabilità, Sicurezza e Manutenzione nel Progetto dei Sistemi.* Torino, CLUT, 1988.

[7] Galetto, F.: *Affidabilità. Vol. 1 Teoria e metodi di calcolo.* Torino CLEUP Editore, 1981.

[8] Society of Automotive Engineers, *ARP-4761: Aerospace Recommended Practice: Guidelines and Methods for Conducting Safety Assessment Process on Civil Airborne Systems and Equipment.* 12th edition, SAE, USA, 1996.

[9] Palady, P.: *Failure Modes and Effect Analysis.* PT Publications, USA, 1995.

[10] Crow, K.: *Value Analysis and Function Analysis System Technique.* USA, DRM Associates.

Ing. Gianfrancesco Maria Repici
phone: +39 011 564 6858
fax: +39 011 564 6899
e-mail: gianfrancesco.repici@polito.it

Department of Aeronautical and Space Engineering

Ing. Aldo Sorniotti
phone: +39 011 564 6915
fax: +39 011 564 6999
e-mail: aldo.sorniotti@polito.it

Department of Mechanical Engineering

Politecnico di Torino
Corso Duca degli Abruzzi, 24
10129 Torino, Italy