A Simulation based Approach to Failsafe Systems in Automotive Design

ALDO SORNIOTTI, GIANFRANCESCO MARIA REPICI
Mechanical and Aerospace Engineering Departments
Politecnico di Torino
Corso Duca degli Abruzzi 24
10129 Torino
ITALY

Abstract: Nowadays, in the automotive field, a lot of new active systems have been put on the market; the most significant are the Electronic Stability Program, the Four Wheels Steering, the Air Springs and the Active Roll Control. In the next future also Steer-by-Wire and Brake-by-Wire will be sold. The most difficult and expensive task in designing these systems is to implement an efficacious failsafe and good recovery strategies, not to have dangerous consequences due to faults in the systems. The first step consists in understanding which can be all the possible faults and in evaluating their level of danger. This process, consisting in a fault injection, is fast and cheap if carried out through PC simulation, as shown in this paper. The second step consists in virtually implementing and verifying the effectiveness of the failsafe/recovery strategies. Bench tests and road tests will be limited to the last phase of the system development.

Key-words: Safety, Reliability, Fault injection technique, Virtual models.

1 Introduction
During last years, our research team was involved in the development of several control strategies for automotive active systems. The first approach to their design was always based on simulation; only in second approximation studies ([5], [8]), we built test benches to obtain experimental data. The paper firstly presents our vehicle models, then four case studies of virtual definition of failsafe mechanisms for active systems.

2 Vehicle models description
In these studies a functional vehicle model was used, having 10 Degrees-Of-Freedom (DOF), six for the car body (three rotational degrees and three translational degrees), and one, rotational, for each wheel. It was obtained through Lagrange equations; the different DOF are coupled. Non-linear suspensions characteristics were taken in account. Also camber/toe/kingpin/caster angles variations due to roll/pitch/bounce motions were considered, depending on suspensions kinematic characteristics. Also suspensions compliance, due to rubber elements deformation, was used as input data in the model. Tyres were simulated by using Pacejka equations [6]. The vehicle model was implemented in Matlab/Simulink®.

The actuation strategy of the different active systems was modelled in detail, by using a commercial devoted software, the AMESim® tool, capable of co-simulating together with Simulink®.

Figure 1: Suspensions kinematic characteristics were inserted in the vehicle model

3 First application: 4 Wheels Steering
The first case study was a Four Wheel Steering System, fully designed through simulation.

Its control strategy had to compensate lateral wind phenomena (Figures 2 and 3), very dangerous for common drivers at high vehicle speeds, and to reduce body yaw rate and sideslip angle oscillations during dynamic manoeuvres, like step steer or double step steer (Figure 4). The control algorithm was based on a yaw rate
feedback control, similar to that of a common ESP.

Figure 2: Lateral wind disturbance provokes a change in vehicle trajectory

![Figure 2](image)

According to the kind of vehicle, it is possible to tune the parameters with different targets. For example, the 4WS system of Figure 4 is characterized by different parameters in comparison those of the 4WS of Figure 3.

The hydraulic actuation of the system, modeled in AMESim®, consisted of a power generation system, located in the engine vane, and a rear steering system, with four 2/2 valves. The power generation pump was a typical steering system pump (8.5 cc/r), feeding an accumulator (2 litres) with a pressure transducer. The system was capable of idling the pump when possible, to reduce power dissipation. The maximum power required by the pump was 1 kW. The 2/2 valves, located near the linear actuator, were modulated by Pulse Width Modulation (PWM) techniques. Also friction phenomena in the actuator were considered in the model. Actuator response was excellent for frequencies until to 5 Hz.

Figure 3: Body yaw rate disturbance with and without 4WS

![Figure 3](image)

Fault injection campaigns were carried out on this system. Oil leakages due to faults at the hydraulic pipes are very dangerous since they provoke a free counter-phase steering of rear wheels, giving origin, in dynamic manoeuvres, to evident instability phenomena. To solve the problem, an electric brake was designed, actioned by the recovery algorithm.

Figure 4: Step steer manoeuvre with and without 4WS

![Figure 4](image)

Figure 5: AMESim® hydraulic circuit model

![Figure 5](image)

Figure 6: Failsafe analysis through simulation

Figure 6 is a simulation of a leakage (between the third and the fourth second) in the pipe connecting the actuator electro-valves to the tank. The tank was designed with an oil level sensor;
when oil level has a reduction, the failsafe algorithm sends an activation signal to the brake and the warning lamp lights on. Of course, rear wheels will remain locked in a non-straight position, but the driver can continue performing the manoeuvre in safe conditions. The car with the non-recovered system has consistent, innatural values of body sideslip angle. A lot of simulations for all the possible faults were rapidly performed, to detect the level of danger connected to each fault.

4 Second application: Air Springs
The second case-study was an Air Spring system for a high class passenger car, conceived to improve comfort and reduce understeer in semistationary manoeuvres. Also a self-leveling function was designed for the system.

![Air Springs scheme](image1)

Figure 7: Air Springs scheme

![Air Springs integration with helicoidal springs](image2)

Figure 8: Air Springs integration with helicoidal springs

Figures 7 and 8 are schemes of the configuration of commercial air springs, integrated with traditional helicoidal springs, similar to those modeled in this work. Also in this case each component was modeled in detail (Figure 9), including also pneumatic power generation system (it was chosen a commercial system by WABCO), formed by a pump, an air drier with an idling system (Figure 10) and a tank. In studying air springs, also vehicle unsprung masses were inserted in the vehicle model.

![Air Springs AMESim model](image3)

Figure 9: Air Springs AMESim model

![Air drier with filter and idling system](image4)

Figure 10: Air drier with filter and idling system
The designed recovery algorithm puts air springs at a low pressure level when a fault is detected (not to have excessive asymmetries during extreme dynamic manoeuvres); in this condition, vehicle sprung mass is supported only by helicoidal springs. In case of electrical problems due to the coils of the electro-valves, a failsafe algorithm based on electric signals was implemented.

To prevent dangerous inconveniences due to pneumatic leakages, four (one for each air spring) safety valves (Figure 11 and 12) were designed and virtually tested. They are located between the air tank and the electro-valves devoted to the modulation of the pressure level in the air springs. They remain open only if the pressure difference between ports 1 and 3 (Figure 12) does not exceed a pre-defined value.

In this case, an endstop sensor sends a signal to the CPU, which switches the air springs warning lamp and activates a recovery also for all the other air springs.

Figures 13 and 14 are about the same extreme step steer manoeuvre, simulated in high adherence conditions, with a fault consisting in an air leakage to an air spring. The two curves are about the same physical system, with and without a failsafe control in the CPU. The big asymmetry between left/right side of the car, due to the undetected fault, provokes a loss of control in the car without failsafe. The vehicle equipped with the failsafe algorithm has not evident problems from the point of view of body yaw rate; it only manifests an increase of roll angle values (however, for other kinds of vehicles, like SUVs, they could give origin to rollover phenomena).

Also in this case-study simulation was fundamental to quantify the danger of each fault.

5 Third application: Active Roll Control

One of the most interesting automotive active systems is, without any doubt, Active Roll Control (ARC).

It consists in pre-charging, through hydraulic actuators, the front and rear torsion springs. The
same pre-charge actuation (obtainable through a single channel system) on front/rear bars can improve vehicle behaviour from the point of view of roll angle values. A differentiated pre-charge actuation on front/rear springs (obtainable through a double channel system) permits also a consistent improvement from the point of view of body yaw rate and under/oversteer. In particular, a pre-charge of front bar provokes understeer and a pre-charge of rear bar provokes oversteer. Differently from air springs, this improvement is consistent also in dynamic conditions, due to the hydraulic actuation, which guarantees high actuation frequencies. At the moment, recent BMWs are equipped by such a system, consisting of rotative actuators on the torsion springs.

Our research team designed, through simulation, a linear actuation (Figure 15) for a double channel ARC [7]. It should be suitable also for middle-low size car, due to the reduced costs. The same methodology of the other case-studies was applied: a detailed model was built and control strategies were implemented. Two main kinds of faults were tested through simulation: fluid losses and valves locking phenomena.

Figure 16 is about a locking phenomenon (dashed line) of the front linear actuator due to an electric fault of the valves connecting the actuator to the pump and the tank. Oil cannot reach or go out of the hydraulic chambers: as a consequence, actuator displacement remains constant. In this case, there is not need of a recovery system, since rear active bar standard control algorithm (it is a feedback control on body yaw rate) automatically tends to compensate the fault at the front bar. The effect is not consistent from the point of view of vehicle dynamics. Of course, the same procedure was carried for faults at all the possible components, including valves, pipes, sensors, etc...

Many of these faults, like a fluid leakage during a step steer manoeuvre, could not be reproduced through road tests, due to safety reasons.

Due to the excellent results obtained through simulation with this system, we started building, in the laboratory of the Department of Mechanics of Politecnico di Torino, a rear ARC test bench (scheme of Figure 17). It permits to reproduce the roll behaviour of a car body, considering different heights of the roll centre. In a first phase, it will be used to obtain the frequency response of the linear actuation, at fixed values of body roll angle. Secondly, it will be subjected to a complete Hardware-In-the-Loop (HIL), by dynamically changing, through a hydraulic actuation system, the roll angle, according to a vehicle model running in real time on a PC. Devoted force sensors will measure the reactions between the torsion spring and the attachments to the car body, which will be transmitted to the vehicle model.

6 Fourth application: Electronic Stability Program

Electronic Stability Program is the most famous automotive active system, based on braking system interventions, independently of driver effort on the pedal. Our research group built also a test bench to experimentally verify the simulation results [8]. Politecnico di Torino ESP strategy is mainly based on a body yaw rate controller, comparing, instant by instant, the measured body yaw rate with the reference body yaw rate.

Figures 18 and 19 are examples of faults of ESP body yaw rate sensor, injected in the first instants of a step steer manoeuvre. The sensor output is kept constant at the last useful value. In both cases, the undetected fault creates a condition of great danger. In fact, if the sensor has a fault when the steering wheel has not been turned yet, during the step steer the reference body yaw rate reaches
consistent values, since it depends on steering wheel angle. ESP brakes the wheels internal to the bend, making the car oversteer. Typical failsafe algorithms [5] deactivate body yaw rate control (from the ‘On’ condition it passes to an ‘Off’ condition) when a fault is detected. Deactivation is based on the comparison between the measured value of body yaw rate [1] and an estimation by using the signals from the other sensors of the car. This process has to be repeated for each sensor of the system, to correctly identify the fault and the recovery strategy. Commercial ESP deactivate Antilock Braking System (ABS) and Electronic Brake Distribution (EBD) very rarely (on the contrary of body yaw rate control), only when several faults have manifested. The several comparisons performed by the diagnostic algorithm of the CPU can be summarized in complex flow charts [9], like that of Figure 20.

![Graph](image)

*Figure 18: Extreme step steer manoeuvre, gas released, low adherence conditions*

7 Conclusion
The paper demonstrates that the same simulation based methodology can be used to successfully conceive failsafe/recovery strategies of different automotive active systems. Several case studies were presented; for two of them, prototypes were experimentally tested too.

In any case, after simulation it is necessary to carry on tests on devoted benches and then on the vehicle, to complete a robust design process of the failsafe mechanism.

![Graph](image)

*Figure 20: Example of a failsafe flow chart for an active brake system*

References: