AutoTechnology
International Magazine for Engineering, Production and Management

Safe and Reliable – or Just Complex?

by Konrad Slanec, Methode Electronics Malta

Offprint
from AutoTechnology 6/2002 · Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Wiesbaden

Safe and Reliable – or Just Complex?

by Konrad Slanec, Methode Electronics Malta

The role and features of the brake pedal controls in electromechanical brake systems. The move towards the electromechanical brake (EMB) represents a breakthrough in brake system technology.

Safety was ensured by the high reliability of components and by simply adding redundant features

Historically, a driver's feeling of safe vehicle control was always linked to the reliability of mechanical components. As vehicle performance has continuously improved, the demand to apply higher forces for vehicle control has also increased. Year after year, new mechanical, hydraulic and electronic devices and systems have been invented to increasingly support the driver in better controlling the vehicle. Safety was ensured by the high reliability of components and by simply adding redundant features, which have continuously increased the complexity of the systems used.

Driver-to-Car Interface

The move towards the electromechanical brake (EMB) represents a breakthrough in brake system technology. The driver's wish to apply the brakes is detected by sensors monitoring the brake pedal movement. The electric signal containing the pedal position information is transferred to the redundant brake masters, which control the actuators on the brake calipers by wire only. Since this system does not incorporate any mechanical fallback system and the system fail-safe mode does not exist, new safety architectures are under development [1, 2, 3].

The brake pedal unit for an EMB system, Figure 1, is being provided with new functions, which can be classified into two categories:

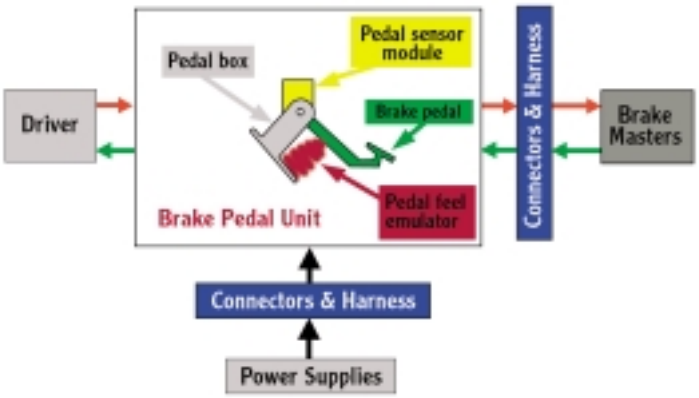

Figure 1: System interfaces of the Brake Pedal Unit for EMB.

- Transmission of the driver's wish to actuate the brake to the brake masters
- Generation of pedal feel and feedback from the brake system to the driver.

Here, we would like to focus on some safety and reliability aspects of the generation and transmission of the pedal position information to the brake masters. Nevertheless, the generation of the system feedback to the driver is also considered as a safety-critical function of a brake pedal unit for an EMB system[4].

Brake Pedal Position Sensing

At first sight, brake pedal position sensing looks easy. There are many solutions for sensing the position of the accelerator pedal used for electronic engine control by wire. Why can´t these be easily adopted for EMB systems?

First of all, the concepts of such sensor units are based on fail-safe requirements which are sufficient for engine control by wire. The EMB system, however, requires fail-silent / fail-operational features. This means that, if a single fault occurs at any time, the system must remain operational and tolerate this fault.

Secondly, a small signal drift at the accelerator pedal rest position – for example, due to mechanical wear or ageing of electronic components – can be classified from the engine control point of view as not safety-critical. For the EMB, such signal drift may have catastrophic consequences, such as driving the car

- *Loss of brake*
  Brake cannot be activated
- *Reduced deceleration*
  Braking distance increases
- *Unwanted increased deceleration*
  Deceleration increases at low pedal travel
- *Undesired sudden braking*
  Unwanted abrupt braking applied to vehicle
- *Undesired constant braking*
  Brakes are constantly activated whilst vehicle is moving
- *Retarded braking*
  Greater pedal travel needed to activate brake

Figure 2: Hazards and effects due to failures of the Brake Pedal Unit for EMB.

with unintentionally applied brakes.

Thirdly, the signal evaluation and diagnostics for the current accelerator pedal sensors are performed in the engine control module. In order to fulfil the redundancy requirements for the EMB, the system complexity will drastically increase if the same strategy is used.

Design Approach

The biggest challenge for the design is to consider not only the above-mentioned safety requirements but also to ensure high reliability and to propose a commercially feasible solution. This can be achieved by an iterative design approach using combined hazard analysis techniques and FMEA [5, 6].

The first step is to identify the hazards. Figure 2 shows the hazards and the related effects for the brake pedal sensor unit for an EMB system. The design concept should start by first considering one sensor and checking the risk. If necessary, hazard controls have to be implemented for the next iteration. This process should continue until the remaining risks are classified as low [7]. In parallel, during each iteration stage, the reliability and the costs have to be reviewed.

Methode's Brake Pedal Sensor Unit

The brake pedal sensor unit for an EMB system under development at Methode Electronics Malta is a stand-alone unit. This means that the unit provides and processes the required information with sufficient redundancy. All information is passed to the brake masters by a fault-tolerant bus system (TTP/C or Flexray) on two independent channels.

The safety strategy is based on the following:

- Comprehensive self-diagnosis
- Dynamic redundancy
- Combined design redundancy and design diversity
- Galvanic decoupling of redundant elements
- Multiple independent power supplies with sufficient buffers
- Adaptive learning system for dynamic pedal rest position detection
- Data communication using a time-triggered, fault-tolerant bus system.

The availability of comprehensive self-diagnosis enables the application of dynamic redundancy, which helps to reduce the number of precise redundant position sensors to two. This has a positive effect since it reduces the complexity and the costs, as well as increasing the reliability with regard to static redundancy. The two accurate angular position sensors are eddy current sensors with an accuracy of < 0.1°. In addition, analytical redundancy is partially implemented by introducing a data-matching factor. Two microcontrollers condition the signals and transmit data to the brake masters.

Dynamic redundancy

One rough Hall-sensor encoder is used to prevent common cause failures through design diversification. In addition, a rough evaluation of the two main signals is performed.

Galvanic decoupling of redundant elements, three independent power supplies (and three independent connectors for series production parts) and different program codes in each microcontroller, contribute further to the prevention of common cause failures.

An adaptive learning system is already being developed for the dynamic detection of the pedal rest position of conventional brake and clutch systems. The dynamic recognition and update of the pedal rest position is essential for avoiding some hazards.

For the prototypes only, data communication to the brake masters is implemented via a CAN to TTP/C adapter by two independent node-to-node CAN bus channels. The CAN message on each channel contains the following information:

- Pedal position Sensor 1
- Pedal position Sensor 2
- Pedal velocity Sensor 1

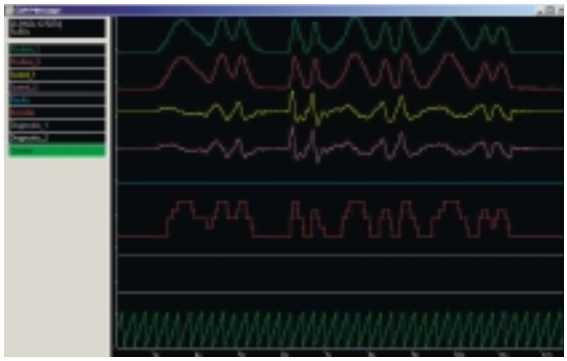

Figure 3: Screen-shot of CAN messages on one channel.

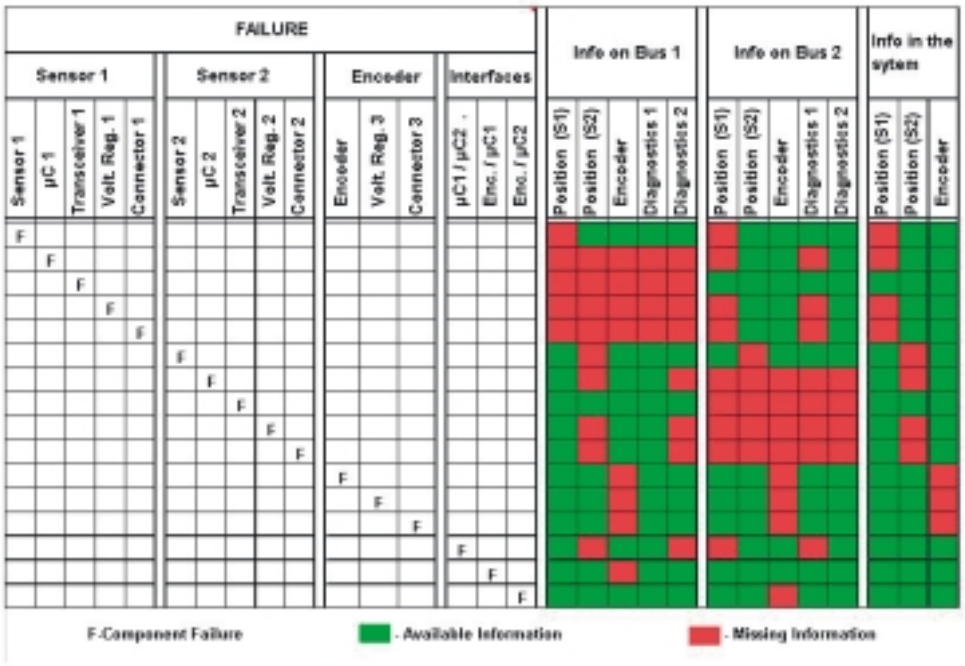

Figure 4:
Fail-silent / fail-operational matrix.

Two sources of information

- Pedal velocity Sensor 2
- Pedal position Encoder
- Data matching factor
- Diagnostics µC 1
- Diagnostics µC 2
- Synchronization counter for the microcontrollers.

Figure 3 shows a screen-shot of the above CAN messages.

Figure 5:
Prototype of the Brake Pedal Unit for EMB. The pedal sensor module and a passive pedal feel emulator are assembled in a pedal box, which is in series production at AUDI.

Fail-Silent / Fail-Operative Matrix

The matrix shown in Figure 4 demonstrates the required fail-silent / fail-operational capability for a single fault. If one component or link within the sensor unit fails, certain information will not be available on one or both bus channels. In this case, the brake system still has at least two sources of information on the pedal position. It is assumed that the chosen bus system must be fault-tolerant.

Current Status

A prototype of the pedal sensor unit is shown in Figure 5. The unit is assembled in a pedal box which is currently in series production at Audi. The pedalfeel emulated by mechanical springs is only passive. For the prototypes only, one industrial connector is used instead of three independent connectors.

Validation testing of the sensor unit performance using hardware-in-the-loop simulation techniques, shows that the concept which is based on dynamic redundancy, meets the safety requirements without compromising theoretical reliability and commercial feasibility.

Acknowledgment

We would like to thank Dr. Thierry Mingers, TTTech Computertechnik GmbH, Pfaffenhofen, for supporting this project.

[1] Kopetz, H.; Thurner, T.: TTP – A new approach to solving the interoperability problem of independently developed ECUs, SAE (1998) Paper 981107

[2] Dilger, E.; Führer, Th.; Müller, B.; Poledna, S: The X-By-Wire Concept: Time-triggered information exchange and fail silence support by new system services, SAE (1998) Paper 98-PC124

[3] Belschner, R.; Hedenetz, B.; Heni, A.; Nell, J.; Willimowski, P.; Kopetz, H.: Trockenes Brake-By-Wire mit fehlertolerantem TTP/C Kommunikationssystem, VDI - Berichte Nr. 1415, 1998

[4] Bill, K.H.; Leber, M.; Becker, H.; Breuer, B.: Forschungswerkzeug zur Untersuchung der Schnittstelle Fahrer / Bremspedal, ATZ Automobiltechnische Zeitschrift 101 (1999) 2

[5] Stölzl, S.; Isermann, R.; Rieth, P.; Nell, J.: Methodik zur Erarbeitung von Überwachungsverfahren für sicherheitskritische verteilte Echtzeitsysteme, GMA - Kongreß 1998, Ludwigsburg

[6] Isermann, R.: Fault tolerant components for Drive-By-Wire Systems, VDI - Berichte Nr. 1646, 2001, Pg. 739 ff

[7] Federal Aviation Administration, U.S. Department of Transportation, System safety handbook, Chapter 3: Principles of system safety, 30. December 2000, Pg. 3-9