TOWARDS DRIVE-BY-WIRE AUTOMOBILES

Rolf Isermann

Institute of Automatic Control
Darmstadt University of Technology

Abstract:
The development of automotive systems shows an increasing integration of electronic sensors, microcomputers and actuators for single components, engine, drive-chain, suspensions and brakes. After considering electronic driver assisting systems such as ABS, TCS, ASR, ESP, BA the developments towards drive-by-wire systems with and without mechanical or hydraulic backup are considered. Drive-by-wire systems consist of an operating unit (steering wheel, braking pedal) with an electrical output, a haptic feedback to the driver, bus systems, microcomputers, power electronics, and electrical actuators. For their design safety integrity methods like reliability, fault tree, hazard analysis and risk classification are required. Different fault tolerance principles with various forms of redundancy are considered resulting in fail-operational, fail-silent and fail-safe systems. Fault-detection methods are discussed for use in low-cost components. This is followed by some principles for fault-tolerant design of sensors, actuators and communication. The contribution reviews and evaluates those methods and principles which have been developed in quite different areas and shows how they can be applied to low-cost automotive components and drive-by-wire systems.
A recently developed brake-by-wire system with electronic pedal and electrical brakes is then considered in more detail showing the design of the components and the overall architecture. An outlook then shows the further development of drive-by-wire systems.

Keywords: drive-by-wire, brake-by-wire, fault tolerance, fault detection, safety integrity, reliability, fault tree, hazard analysis, redundancy, fail-operational, fail-silent, d.c. motor, fault-tolerant sensors, fault-tolerant actuators.

1. INTRODUCTION

Automobiles and engines show an increasing integration with actuators, sensors, microelectronics and information processing. They develop to *mechatronic systems* which are characterized through the integration of components (hardware) and integration of signal-based functions (software), resulting in automatic functionality. Examples for first steps towards mechatronic systems for *automobiles* were digitally controlled combustion engines with fuel injection in 1979 and digitally controlled ABS (antilock brake systems) around 1978. Todays combustion engines are completely microcomputer controlled with e.g. five electrical, electro-hydraulic or electro-pneumatic actuators and few (two) measured output variables taking into account different operating phases, like start-up, warming-up, idling and normal operation. The only input from the driver is generated by the accelerating pedal and transferred to the throttle (s.i. engines) or the injection pump (diesel engines).

Drive-by-wire systems with mechanical backup

Since about 1986 the engine is increasingly manipulated by electronic pedal and electrically driven throttle or injection, (Kohlberg, 1985), (Gilz and Wokan, 1993), representing first *drive-by-wire components*. In this case a limp home function after electronic failure is possible, because the throttle

ISBN 972-98603-0-0

spring system provides a reduced engine speed, e.g. 1200 rpm. Hence, the system fails safe by the mechanics. Other mechatronic units within the power train were developed for the *automatic transmission* with hydraulic torque converter and microcomputer controlled gear shift.

Electronic driver assisting systems

The development of mechatronic systems for the engine and the drive chain was paralleled by driver assisting *electronic braking functions* like ABS (antilock braking system) (1978), TCS (traction-control systems) (1986), ESP (electronic stability control system), (van Zanten *et al.*, 1995) and BA (brake assistant) see e.g (Jurgen, 1999). In these cases the hydraulic pressure generated by the drivers brake pedal and pneumatic booster is modulated in order e.g. to control the slip of single wheels (ABS) or to control the drift angle of the vehicle by individual wheel braking (ESP). If the electronic control fails, the brake systems behave like a conventional purely hydraulic one.

Power steering was for a long time (since about 1945) realized by hydraulic supporting energy. *Electrical power steering* for light weight vehicles came on the market in 1996 not requiring special hydraulic circuits and auxiliary pumps anymore, (Connor, 1996). In all cases the direct mechanical linkage with the steering wheel and the driver action was retained.

Fly-by-wire systems

The development of fly-by-wire systems for aircraft can be used as reference for automotive drive-by-wire systems. Electronic analogue control systems with hydraulic actuators have been used in civil aircraft engines since about 1955, (Potocki de Montalk, 1993). The transonic Concorde 1963 was then the first aircraft where electronic-hydraulic control systems were used to fly the aircraft, from 1978 on with a sidestick and a mechanical backup. Digital control was then implemented 1981/1982 in the Boeing 757/767 and Airbus A310 to manipulate the slats, flaps and spoilers. The first completely fly-by-wire aircraft with digital computers for the primary flight control was the Airbus A320 in 1988, followed by the Airbus A340 in 1991, (Favre, 1994). In 1994 then Boeing came on the market with the fly-by-wire 777. The only mechanical backup are cable linkages from the cockpit to the rudder and trimmable horizontal stabilizers. A high degree of fault tolerance is obtained for the A330/340 by using e.g. five computers (2 different processors, diverse software with different software languages), double or triple sensors and actuators, 3 independent hydraulic systems with 8 pumps, 6 electric generators, 2 batteries. Automobiles have far less driving hours during their life time (about $5 \cdot 10^3$ to $3 \cdot 10^4$ hours) than aircraft (some 10^5 hours) and more possibilities to reach a safe state in short time. However, their numbers are much higher and drivers and maintenance not as professional as for aircraft. Therefore, the fault tolerance for drive-by-wire vehicles does not need to be quite as high as for aircraft.

Drive-by-wire without mechanical backup

The approaches taken for the successful fly-by-wire systems and the good experience with the automotive drive-by-wire systems with mechanical backup for the engine and drive chain and the electronic driver assistance systems for braking and power steering are now a basis for the development of complete drive-by-wire systems without mechanical backup for braking, steering and higher level driver assisting functions. The mechanical backup systems have the disadvantages that they are costly, heavy, passive safety-critical (steering column, brake pedal) and do not give enough freedom to use the potential of the electrical systems.

Drive-by-wire systems without mechanical backup generate electrical commands through the driver and transfer them to computer controlled electromechanical actuators with usually no fail-safe behaviour by mechanics, but with fault tolerant properties.

Higher level automotive control

A recent development of higher level control is ACC (adaptive cruise control), also called ICC (intelligent cruise control), where the vehicle either follows a preceding vehicle with distance measurement and control or follows a driver set reference value as for classical speed control, see e.g. (Germann and Isermann, 1995), (Fritz, 1996). In this case electrical commands have to be given to an electrical throttle or to the brake booster.

Several research automobiles exist with appropriate sensors of the road situation (e.g. cameras) and *computerized autopilots*, (Dickmanns, 1995), or for automatic driving in platoons, like pioneered in the Californian PATH program, (Stevens, 1996), (Tomizuka, 1997).

This short summary of recent developments shows, that from the viewpoints of increased active safety and automated driving there is a clear demand for *drive-by-wire systems* which include the powertrain, braking and steering. These systems are also called *x-by-wire systems* where x stands for the commanded action. Figure 1 shows the hazard severity of failures for different electronic (and electrical) driving systems, compare (Rieth, 1999*a*) and section 3. Hence, the hazard severity of drive-by-wire control systems for vehicles increases considerably.

ISBN 972-98603-0-0

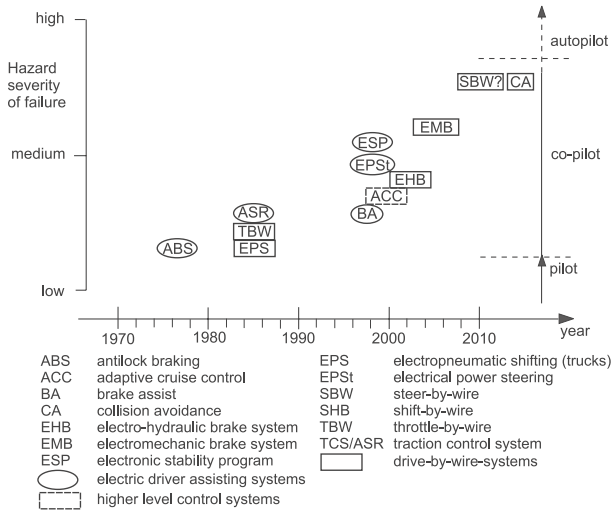

Fig. 1. Hazard severity of failures (qualitative) in electronic driver assisting systems, drive-by-wire systems and higher level control systems

2. DRIVE-BY-WIRE STRUCTURES WITH AND WITHOUT MECHANICAL BACKUP

The step from drive-by-wire systems with mechanical backup to those without mechanical backup or without fail-safe by mechanics is a large one because of the lower reliability and different fault behaviour of electronic and electrical components compared to mechanical components. Therefore, fault-tolerant electronic systems have to be incorporated to meet the high safety requirements.

Figure 2 shows the different stages for *brake systems* of passenger cars or light weight trucks. In the case of the *conventional hydraulic brake*, Figure 2a), the mechanical linkage between the pedal and the hydraulic main cylinder is paralleled by the power supporting pneumatic amplifier (booster). If the pneumatic amplifier fails, the mechanical linkage transfers the (larger) pedal force from the driver. The hydraulic cylinder acts on two independent hydraulic circuits in parallel. That means the brake system is fault-tolerant with regard to a failure of one of the two hydraulic circuits. Failures in the electronics of brake control systems as ABS bring the hydraulic actuators (e.g. magnetic valves) into a fail-safe status such that the hydraulic brake gets the pressure from the hydraulic main cylinder directly.

A first step towards brake-by-wire is the *electro-hydraulic brake* (EHB), Figure 2b), where the mechanical pedal has sensors for position and hydraulic pressure. Their signals are transferred to separated hydraulic pressure loops with proportional acting magnetic valves, manipulating hydraulic liquid flows from an accumulator/pump system to the wheel brakes. If the electronics fail the separation of the pedal to the wheel brakes is opened. Hence, a hydraulic back-up serves to fail safe as for conventional hydraulic brakes. Market introduction is expected for 2001.

The *electromechanical brake* (EMB) according to Figure 2c) does not contain hydraulics anymore. The pedal possesses sensors and its signals are sent to a central brake control computer and for redundancy also to the wheel brake controllers. The brake controllers act through power electronics to the electromotors of e.g. disc brakes. Because no mechanical or hydraulic connection does exist, a mechanical or hydraulic fail-safe is not possible. Hence, the complete electrical path must be build with fault tolerance.

Figure 3 shows a general signal flow diagram of a drive-by-wire system in more detail. The drivers operating unit (steering wheel, braking pedal) has a mechanical input (e.g. torque or force) and an electrical output (e.g. bus protocol). It contains sensors and switches for position and/or force, microelectronics and either a passive (spring-damper) or active (el. actuator) feedback to give the driver a haptic information (”pedal-feeling”) on the action. A bus connects to the brakes or steer control system. These consist of power electronics, electrical actuators, brake or steer mechanics, with sensors or reconstructed variables and a microcomputer for actuator control, brake or steer function control, supervision and different kind of management (e.g. fault tolerance with reconfiguration, optimization).

Each of the sensors, electronics, buses, power electronics, high power actuator and microcomputers has to be fault-tolerant with regard to at least one safety critical failure. Therefore, a *safety integrity analysis* and methods of *fault tolerance* are basic issues for drive-by-wire systems.

3. SAFETY INTEGRITY ANALYSIS METHODS

Drive-by-wire systems are safety-related systems. Therefore, all aspects of reliability, availability, maintainability and safety (RAMS) have to be considered because they are relevant for the responsibility of the manufacturers and the acceptability of customers. To meet safety requirements special procedures were developed in different technical disciplines like railway, aircraft, space, military and nuclear systems. These procedures are covered by the terms *system integrity* or *system dependability*.

The various kinds of safety requirements lead to different levels of integrity of safety-related systems, from lowest to highest requirements. In this context ”integrity” means more precisely ”safety integrity” with following definition:

Safety integrity is the probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time” (*IEC 61508*, 1997).

Safety and reliability are generally achieved by a combination of

ISBN 972-98603-0-0

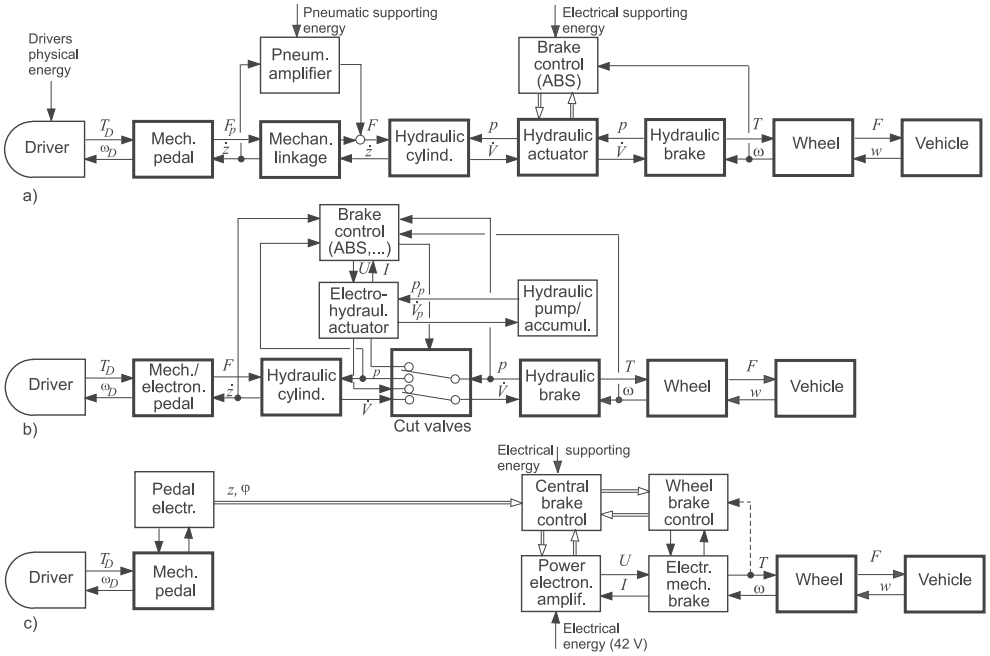

Fig. 2. Signal flow diagram for different brake systems of passenger cars (only 1 wheel considered)
a) Conventional hydraulic brake with pneumatic amplifier (booster) and electronic slip control (ABS)
b) Electro-hydraulic brake (EHB) with hydraulic backup
c) Electromechanical brake (EMB) without mechanical backup

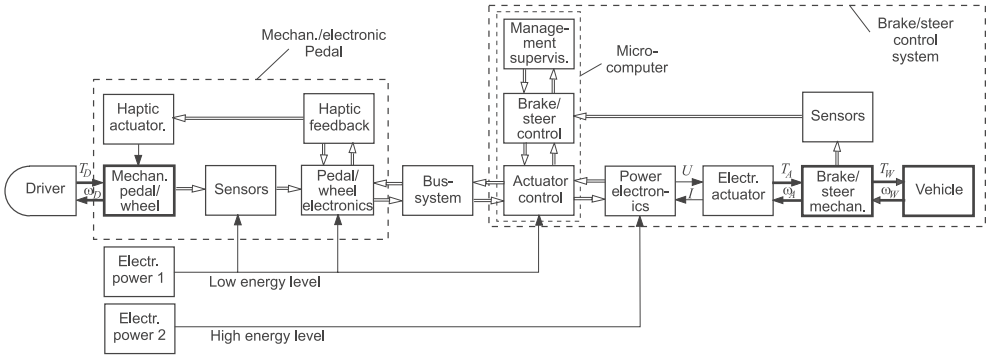

Fig. 3. Basic signal flow diagram of drive-by-wire systems

- fault avoidance,
- fault removal,
- fault tolerance,
- fault detection and diagnosis,
- automatic supervision and protection.

Fault avoidance and removal has to be mainly accomplished during the design and testing phase. For investigating the effect of faults on the reliability and safety during the design and also for type certification a range of analysis methods were developed.

They are mainly:

- reliability analysis
- event tree analysis (ETA) and fault tree analysis (FTA)
- failure mode and effects analysis (FMEA)
- hazard analysis (HA)
- risk classification.

For details see (Storey, 1996), (Reichart, 1998), (*IEC 61508, 1997)*.

These known methods can now be combined appropriately. Figure 4 shows an overall scheme. The FMEA identifies all components, failures, causes and effects. The single failures proceed to a FTA to determine the causes and their logic interconnections on a component level. The failure causes are then used to design the overall reliability. Remaining failures which cannot be avoided are then classified and determine the maintenance procedure.

Based on the FMEA the hazard analysis extracts safety critical failures. Their presentation in a (reduced) fault tree determines the causes with logic interconnections, (Stölzl, 2000), i.e. dangerous faults leading to hazards. Based on this the safety system at lower levels can be designed. Remaining dangerous failures then undergo a risk classification and deter-

ISBN 972-98603-0-0

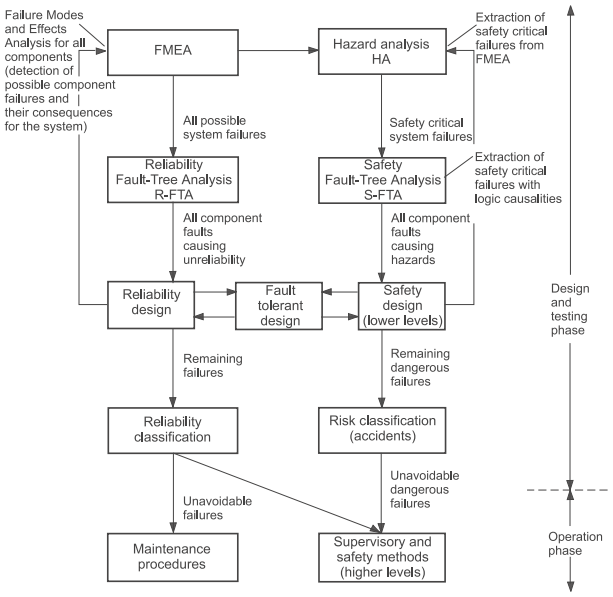

Fig. 4. Integrated design procedures for system reliability and safety to result in high system integrity

mine the supervision and safety methods to reduce the risk to an acceptable measure.

Herewith a hazard risk number

$$R = C \times F_H \times F_{OP}$$

can be used, where

- C: consequence (severity) of hazard
- F_H: frequency (probability) of hazard
- F_{OP}: frequency of operation state

compare (*IEC 61508, 1997)*, (*Prometheus*, 1998), (Reichart, 1998).

In general ways of fault tolerance have to be implemented at component and unit level to improve both, reliability and safety especially by reducing F_H. Figure 4 summarizes the integrated reliability and safety procedure *during the design and testing phases*.

The unavoidable failures have to be covered by maintenance and on-line supervision and safety methods *during operation,* including fault tolerance, protection and supervision with fault detection and diagnosis and appropriate safety actions. These methods are discussed in the following sections.

4. FAULT-TOLERANT DESIGN

After applying reliability and safety analysis methods during design and testing and also corresponding quality control methods during manufacturing, the development of certain faults and failures still cannot be avoided totally. Therefore, they should be tolerated by additional design efforts. Hence, high-integrity systems must have as much as possible the ability of *fault tolerance*. This means that faults are compensated in such a way that they do not lead to system failures. The most obvious way to reach this goal is *redundancy* in components, units or subsystems. However, the overall systems then become more complex and costly.

In this section various types of faults and fault-tolerant methods are reviewed briefly.

4.1 *Type of faults*

The design of high-integrity systems depends among others also on the type of faults which show a characteristic behaviour for the various components. They may be distinguished by their form, time behaviour and extent. The *form* can be either systematic or random. The *time behaviour* may be described by permanent, transient, intermittent, noise or drift, Figure 5. The extent of faults is either local or global and includes the size.

Fig. 5. Time behaviour of faults

Electronic hardware shows systematic faults if they originate in specification or design mistakes. Once in operation hardware components are mostly random with all kind of time behaviour. The faults or mistakes in *software* (bugs) are usually systematic, e.g. by wrong specification, coding, logics, calculation overflows, etc. They are in general not random like faults in hardware.

Failures of *mechanical systems* can be classified into the following failure mechanisms: distortion (buckling, deformation), fatigue and fracture (cycle fatigue, thermal fatigue), wear (abrasive, adhesive, cavitation), or corrosion (galvanic, chemical, biological), see e.g. (*Reliability Toolkit*, 1995). They may appear as drift like changes (wear, corrosion) or abruptly (distortion fracture) at any time or after stress. *Electrical systems* consist usually of a large number of components with various failure modes, like shortcuts, loose or broken connections, parameter changes, contact problems, contamination, EMC problems etc. Generally electrical faults appear more randomly than mechanical faults.

Sensors belong mainly to electrical systems and actuators to both, electrical and mechanical systems.

4.2 *Fault tolerance for components*

Fault-tolerance methods generally use *redundancy*. This means that in addition to the considered module one or more modules are connected, usually in parallel. These redundant modules are either *identical* or *diverse*. Such redundant schemes can be designed for hardware, software, information processing, mechanical and electrical components, like sensors, actuators, microcomputers, buses, power supplies, etc.

ISBN 972-98603-0-0

4.2.1. *Basic redundant structures.* There exist mainly two basic approaches for fault tolerance, static redundancy and dynamic redundancy. The corresponding configurations are first considered for *electronic hardware* and then for other components.

Figure 6a) shows a scheme for *static redundancy*. It uses three or more parallel modules which have the same input signal and are all active. Their outputs are connected to a voter who compares these signals and decides by majority which signal value is the correct one. If a triple modular redundant system is applied, and the fault in one of the modules generates a wrong output, this faulty module is masked (i.e. not taken into account) by the 2-out-of-3 voting. Hence, a single faulty module is tolerated without any effort for specific fault detection. n redundant modules can tolerate $(n-1)/2$ faults (n odd).

Dynamic redundancy needs less modules on cost of more information processing. A minimal configuration consists of two modules, Figure 6b) and c). One module is usually in operation and if it fails the standby or backup unit takes over. This requires a fault detection to observe if the operation modules become faulty. Simple fault-detection methods use the output signal only for e.g. consistency checking (range of the signal), comparison with redundant modules or use of information redundancy in computers like parity checking or watchdog timers. After fault detection it is the task of the reconfiguration to switch to the standby module and to remove the faulty one.

In the arrangement of Figure 6b) the standby module is continuously operating, called "*hot standby*". Then the transfer time is small on cost of operational aging (wear out) of the standby module.

Dynamic redundancy, where the standby system is out of function and does not wear, is shown in Figure 6c), called "*cold standby*". This arrangement needs two more switches at the input and more transfer time due to a start-up procedure. For both schemes the performance of the *fault detection* is essential.

Similar redundant schemes as for electronic hardware exist for *software fault tolerance*. Here, tolerance against mistakes in coding or errors of calculations is meant. The simplest form of a *static redundancy* is repeated running ($n \geq 3$) of the same software and majority voting for the result. However, this only helps for some transient faults. As software faults in general are systematic and not random, a duplication of the same software does not help. Therefore, the redundancy must include diversity of software, like other programming teams, other languages, or other compilers. With $n \geq 3$ diverse programs a multiple redundant system can be established followed by majority voting as Figure 6a). However, if only one processor is used calculation time is increased, and using n processors may be too costly.

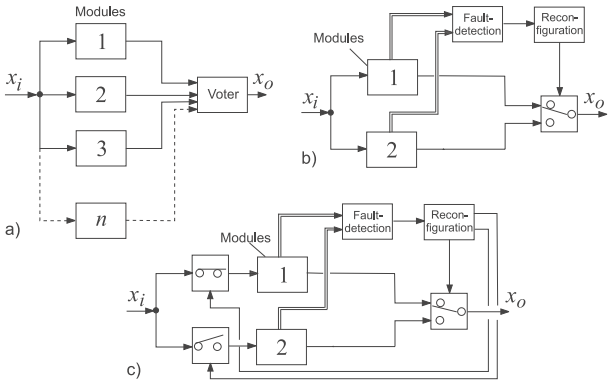

Fig. 6. Fault-tolerant schemes for electronic hardware
a) Static redundancy: multiple redundant modules with majority voting and fault masking, m out of n system (all modules are active)
b) Dynamic redundancy: Standby module which is continuously active, "hot standby"
c) Dynamic redundancy: Standby module that is inactive, "cold standby"

Dynamic redundancy by using standby software with diverse programs can be realized by using recovering blocks. This means that in addition to the main software module other diverse software modules exist, (Leveson, 1995), (Storey, 1996).

For digital computers (microcomputers) with only a requirement for fail-safe behaviour, a duplex configuration like Figure 7 can be applied. The output signals of two synchronized processors are compared in two comparators (software) which act on two switches of one of the outputs. It is useful if the miss of the output brings the system in safe-state. (This fail-safe system is e.g. used for ABS braking systems).

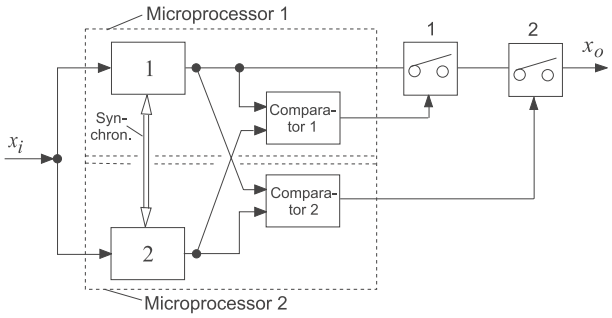

Fig. 7. Duplex computer system with dynamic redundancy as hot standby, fault detection with comparators and switch to (possibly) fail-safe. (Not fault tolerant).

Fault tolerance can also be designed for purely *mechanical* and *electrical systems*. Static redundancy is very often used in all kind of homogeneous and inhomogeneous materials (e.g. metals and fibers) and special mechanical constructions like e.g. lattice-structures, spoke-wheels, dual tyres or in electrical components with multiple wiring, multiple coil windings, multiple brushes for d.c. motors, multiple contacts for potentiometers. This quite natural built-in

ISBN 972-98603-0-0

fault tolerance is generally characterized by a parallel configuration, like in Figure 8a). However, the inputs and outputs are not signals but e.g. forces, electrical currents or energy flows and a voter does not exist. All elements operate in parallel and if one element fails (e.g. by breakage) the others take over a higher force or current, following the physical laws of compatibility or continuity. Hence, this is a kind of ”stressful degradation”.

Mechanical and electrical systems with *dynamic redundancy* as depicted in Figure 6b), c) can also be built. Mostly only cold standby is meaningful, Figure 8b). Fault detection of the operating unit may be based on measured outputs like position, speed, force, torque, pressure, flow, voltage or current. However, then only large failures like complete break down can be detected. To improve fault detection also the input signals and other intermediate signals should be available. Dynamic redundancy can mainly be applied for electro-mechanical systems.

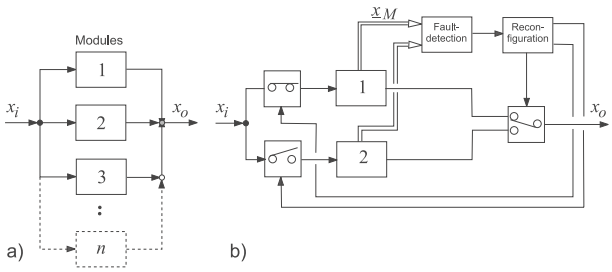

Fig. 8. Fault-tolerant schemes for electro-mechanical and mechatronic systems
a) Static redundancy for mechanical and electrical components: multiple redundant elements
b) Dynamic redundancy for electro-mechanical and mechatronic systems: standby module which is inactive, ”cold standby”. $\underline{x}_M$: measured input, output and intermediate signals

Fault tolerance with dynamic redundancy and cold standby is especially attractive for *mechatronic systems* where more measured signals and embedded computers are already available and therefore fault detection can be improved considerably by applying process-model-based approaches, see section 5. Table 1 summarizes the appropriate fault-tolerance methods for the case of electronic hardware.

4.2.2. *Redundant structures for drive-by-wire components.* Mainly because of costs, space and weight a suitable compromise between the degree of fault tolerance and the number of redundant components has to be found for automotive x-by-wire systems. Constrast to fly-by-wire systems only one single failure must be tolerated (presently) for hazardeous cases, (Schunck, 1999), mainly because a safe state can be reached easier and faster. This means that not for all components of drive-by-wire systems very stringent fault-tolerance requirements are needed. Following steps of degradation are distinguished:

- *Fail-operational* (FO): One failure is tolerated, i.e. the component stays operational after one failure. This is required if no safe state exists immediately after the component fails,
- *Fail-safe* (FS): After one (or several) failure(s) the component possesses directly a safe state (passive fail-safe, without external power) or is brought to a safe state by a special action (active fail-safe, with external power),
- *Fail-silent* (FSIL): After one (or several) failure(s) the component behaves quiet externally, i.e. stays passive by switching off and therefore does not influence other components in a wrong way.

For vehicles it is proposed to subdivide FO in ”long time” and ”short time”, (Reichart, 1998).

Considering these degradation steps for various components one has first to check if a safe state exists. For automobiles (usually) a safe state is stand still (or low speed) at a non hazardous place. For components of automobiles a fail-safe status is (usually) a mechanical backup (i.e. a mechanical or hydraulic linkage) for direct manipulation by the driver. Passive fail-safe is then reached e.g. after failure of electronics if independent on the electronics the vehicle comes to a stop, e.g. by a closing spring in the throttle or by actions of the driver via mechanical backup. However, if no mechanical backup exists after failure of electronics only an action by other electronics (switch to a still operating module) can bring the vehicle (in motion) to a safe-state, i.e. to reach a stop through active fail-safe. This requires the availability of electric power.

Generally a *graceful degradation* is envisaged, where less critical functions are dropped to maintain the more critical functions available, using priorities, (*IEC 61508, 1997)*. Table 1 shows degradation steps to fail-operational for different redundant structures of electronic hardware. As the fail-safe status depends on the controlled system and the kind of components it is not considered here.

For flight-control computers usually the quadruplex structure with dynamic redundancy (hot standby) is used, which leads to FO-FO-FS, such that 2 failures are tolerated and a third one allows the pilot to operate manually. If the fault tolerance has to cover only one fault to stay fail-operational (FO-F) a triplex system with static redundancy or a duplex system with dynamic redundancy is appropriate. If fail-safe can be reached after one failure (FS) a duplex system with two comparators is sufficient, Figure 7. However, if one fault has to be tolerated to continue fail-operational and after a next fault it is possible to switch to a fail-safe (FO-FS) either a triplex system with static redundancy or a duo-duplex system may be used, c.f. Figure 18. The duo-duplex system has the advantages of simpler failure detection and modularity.

ISBN 972-98603-0-0

Table 1. Fail behaviour of electronic hardware for different redundant structures. FO: fail-operational; F: fail; (FS: fail-safe not considered)

		Static redundancy		Dynamic redundancy		
Structure	Number of elements	Tolerated failures	Fail behaviour	Tolerated failures	Fail behaviour	Discrepency detection
Duplex	2	0	F	0 1	F FO-F	2 comparators fault detection
Triplex	3	1	FO-F	2	FO-FO-F	fault detection
Quadruplex	4	2	FO-FO-F	3	FO-FO-FO-F	fault detection
Duo-Duplex	4	1	FO-F	–	–	–

4.3 *Fault tolerance for control systems*

For automatically controlled systems the appearance of faults and failures in the actuators, the process and the sensors will usually effect the operating behaviour. With feedforward control generally all small or large faults influence the output variables and therefore more or less the operation.

If the system operates with feedback control small additive or multiplicative faults in the actuator or process are in general covered by the controller, because of usual robustness properties. This property is therefore a *passive controller fault-tolerance*. However, additive and gain sensor faults will immediately lead to deviations from the reference values. For large changes in actuators, process and sensors the dynamic control behaviour becomes either too sluggish or too less damped or even unstable. Then either a very robust control system or an *active fault-tolerant control system* is required to save the operation. In the last case it consists of fault-detection methods and a reconfiguration mechanisms which modifies the controller. Dependent on the kind of faults the reconfiguration may change the structure and/or parameters or the controller. This can also include the change to other manipulated variables or actuators or sensors, if available.

Examples are fault-tolerant flight control with reconfiguration to other control surfaces after failure of actuators or ailerons, elevators and rudders are given in (Rauch, 1995), (Chandler, 1997), (Patton, 1997), (Chen *et al.*, 1999). For failures in the satellite altitude control system see (Blanke *et al.*, 1997). Failures in heat exchangers are treated in (Ballé *et al.*, 1998) and fault-tolerant control for lateral vehicle control in (Suryanaryanan and Tomizuka, 2000).

5. FAULT DETECTION FOR SENSORS, ACTUATORS AND MECHATRONIC SERVO SYSTEMS

Fault-detection methods based on measured signals can be classified in

- *limit value checking* (thresholds) and *plausibility checks* (ranges) of single signals,
- *signal model-based methods* for single periodic or stochastic signals,
- *process model-based methods* for two and more related signals.

Figure 9 shows a scheme for these methods. For a description of the various methods it is referred to the literature, e.g. the special section in the (*IFAC Journal Control Engineering Practice*, 1996) or the books (Gertler, 1999), (Chen and Patton, 1999), (Isermann, 1994*b*).

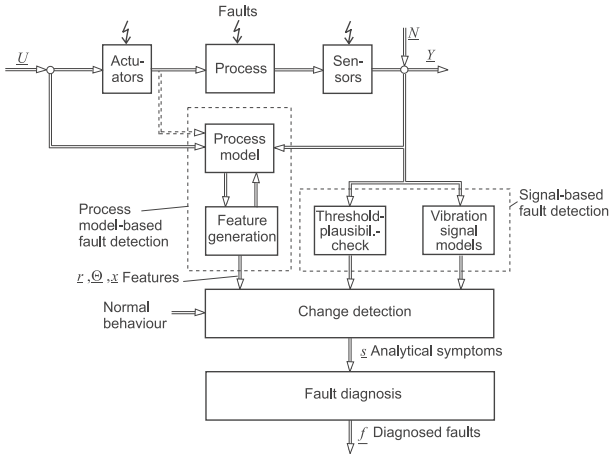

Fig. 9. General scheme of process model-based and signal-based fault detection

In order to obtain specific symptoms it is necessary to have more than one input and one output signal for parity equations or output observers. For parameter estimation one input and one output may be sufficient. Because of the various properties it is recommended to combine different methods in order to have a large fault detection coverage, (Isermann, 1994*a*), (Pfeufer, 1997).

Some application cases of fault detection and diagnosis are:

1) on-line-testing in manufacturing (quality control),
2) on-line-testing during service,
3) on-line, real-time supervision during operation (on-board).

1) and 2) require generally a detailed fault diagnosis with classification or inference methods and can be applied if the computational expense is not very limited. However, for 3) fault-detection capability usually is sufficient if used for fault-tolerant systems. Then a fault diagnosis is not necessarily required. However,

ISBN 972-98603-0-0

diagnosis capability is advantageous for general on-line supervision. Especially for on-board applications in automobiles the allowable computations are very limited, which restricts the fault detection to methods with less computations on microcomputers, see (Moseler *et al.*, 1999). Furtheron it is required that the fault-detection methods are transparent and easy to understand, function reliably for the different operating conditions, use only few measured signals and need only low effort for modeling. Also maintenance effort and easy transfer to modified components are important issues.

6. FAULT-TOLERANT COMPONENTS FOR DRIVE-BY-WIRE SYSTEMS

The discussion on high-integrity systems and drive-by-wire systems shows that a comprehensive overall fault tolerance can be obtained by fault-tolerant components and fault-tolerant control. This means to design:

- fault-tolerant sensors,
- fault-tolerant actuators,
- fault-tolerant process parts,
- fault-tolerant computers,
- fault-tolerant communication (bus systems)
- fault-tolerant control algorithms.

Examples for components with multiple redundancy are known for aircraft, space and nuclear power systems. However, *lower cost components with built-in fault tolerance* have only to be developed. In the following some examples from the automotive area are given, added by examples from other fields.

6.1 *Fault-tolerant sensors*

A fault-tolerant sensor configuration should be at least fail-operational (FO) for one sensor fault. This can be obtained by applying *hardware redundancy* with the same type of sensors or by *analytical redundancy* with different sensors and process models.

6.1.1. *Hardware sensor redundancy.* Sensor systems with static redundancy are realized for example with a triplex system and a voter, Figure 10a). A configuration with dynamic redundancy needs at least two sensors and a fault detection for each sensor, Figure 10b). Usually only hot standby is feasible. Another less powerful possibility is plausibility checks for two sensors, also by using signal models (e.g. variance), to select the more plausible one, Figure 10c).

The fault detection can be performed by *self-tests*, e.g. by applying a known measurement value to the sensor. Another way are *self validating sensors*, (Henry and Clarke, 1993), (Clarke, 1995), where the sensor, transducer, and a microprocessor form an integrated,

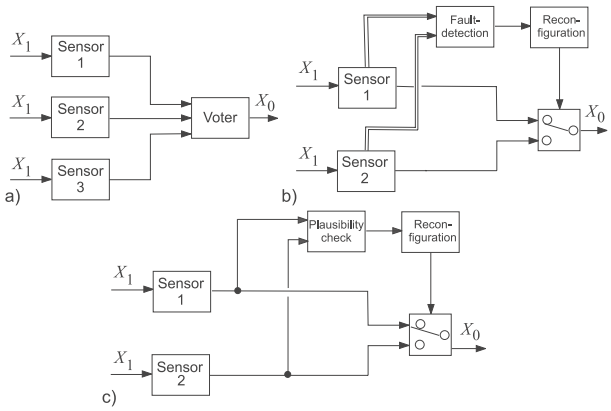

Fig. 10. Fault-tolerant sensors with hardware redundancy
a) Triplex system with static redundancy and hot standby
b) Duplex system with dynamic redundancy
c) Duplex system with dynamic redundancy, hot standby and plausibility checks

decentralized unit with self-diagnostic capability. The self-diagnosis takes place within the sensor or transducer and uses several internal measurements. The output consists of the sensors best estimate of the measurement and a validity status, like good, suspect, impaired, bad and critical.

6.1.2. *Analytical sensor redundancy.* As a simple example a process with one input and *one main output* y_1 and an auxiliary output y_2 is considered, Figure 11. Assuming the process input signal u is not available but two output signals y_1 and y_2, which both depend on u, one of the signals, e.g. $\hat{y}_1$ can be reconstructed and used as redundant signal , if process models G_{M1} and G_{M2} are known and considerable disturbances do not appear (ideal cases), Figure 11a).

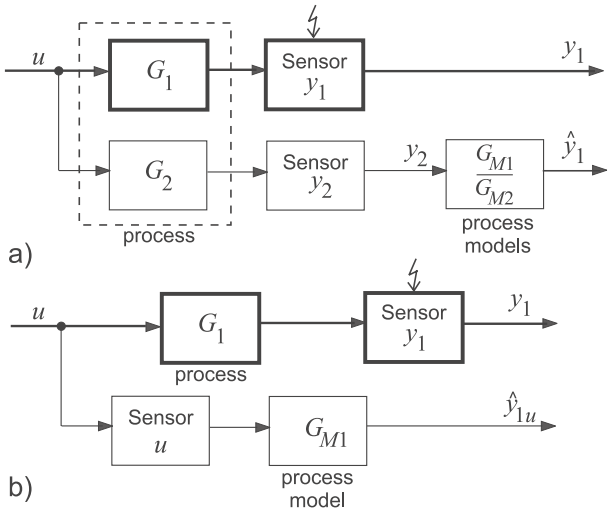

Fig. 11. Sensor fault tolerance for one output signal y_1 (main sensor) through analytical redundancy by process models (basic schemes)
a) Two measured outputs, no measured input
b) One measured input and one measured output

ISBN 972-98603-0-0

For a process with only one output sensor y_1 and one input sensor u the output $\hat{y}_1$ can be reconstructed if the process model G_{M1} is known, Figure 11b). In both cases the relationship between the signals of the process are used and expressed in the form of *analytical models*.

To obtain one usable fault-tolerant measurement value y_{1FT} at least three different values for y, e.g. the measured one and two reconstructed ones must be available. This can be obtained by combining the schemes of Figure 11a) and b) as shown in Figure 12a). A sensor fault y_1 is then detected and masked by a majority voter and either $\hat{y}_1$ or $\hat{y}_{1u}$ is used as a replacement dependent on a further decision. (Also single sensor faults in y_2 or u are tolerated with this scheme).

One example for this combined analytical redundancy is the yaw rate sensor for the ESP, where additionally the steering wheel angle as input is used to reconstruct the yaw rate through a vehicle model as in Figure 11b), and the lateral acceleration and the wheel speed difference of the right and left wheel (no slip) are used to reconstruct the yaw rate according to Figure 11a), (van Zanten *et al.*, 1999).

A more general sensor fault-tolerant system can be designed if *two output sensors* and one input sensor yield measurements of same quality. Then by a scheme as shown in Figure 12b) three residuals can be generated and by a decision logic fault-tolerant outputs can be obtained in the case of single faults of any of the 3 sensors. The residuals are generated based on parity equations. In this case also state observers can be used for residual generation, compare e.g. the dedicated observers by (Clark, 1989). (Note that all schemes assume ideal cases. For the realizibility constraints and additional filters have to be considered).

If possible, a faulty sensor should be fail-silent, i.e. should be switched off. However, this needs additional switches which lower the reliability. For both hardware and analytical sensor redundancy without fault detection for individual sensors at least three measurements must be available to make one sensor fail-operational. However, if the sensor (system) has in-built fault detection (integrated self-test or self-validating) two measurements are enough and a scheme like Figure 10b) can be applied. (This means that my methods of fault detection one element can be saved).

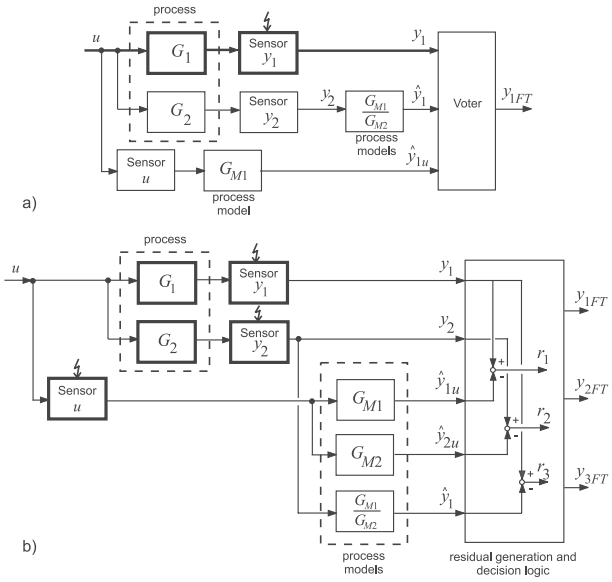

Fig. 12. Fault-tolerant sensors with combined analytical redundancy for two measured outputs and one measured input through (analytical) process models
a) y_1 is main measurement, y_2, u are auxiliary measurements (combination of Fig. 11a) and b))
b) y_1, y_2 and u are measurements of same quality (parity equation approach)

6.2 *Fault-tolerant actuators*

Actuators generally consist of different parts: input transformer, actuation converter, actuation transformer and actuation element (e.g. a set of d.c. amplifier, d.c. motor, gear and valve, Figure 13a). The actuation converter converts one energy (e.g. electrical or pneumatic) into another energy (e.g. mechanical or hydraulic). Available measurements are frequently the input signal U_i, the manipulated variable U_0 and an intermediate signal U_3.

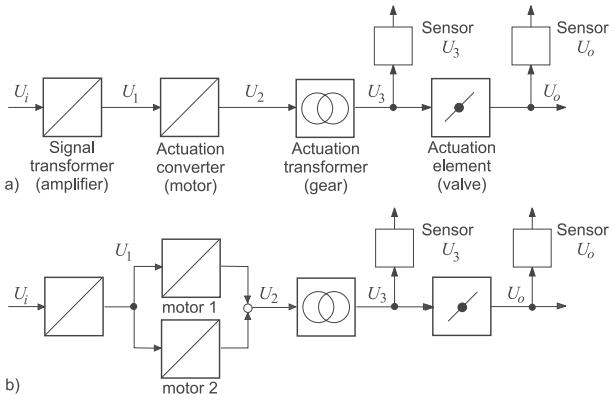

Fig. 13. Fault-tolerant actuator
a) Common actuator
b) Actuator with duplex drive

Fault-tolerant actuators can be designed by using *multiple complete actuators* in parallel, either with static redundancy or dynamic redundancy with cold or hot standby, Figure 6. One example for static redundancy are hydraulic actuators for fly-by-wire aircraft where at least two independent actuators operate with two independent hydraulic energy circuits.

Another possibility is to limit the redundancy to *parts of the actuator* which have the lowest reliability. Figure 13 shows a scheme where the actuation converter (motor) is split into separate parallel parts. Examples with static redundancy are two servo valves for hy-

ISBN 972-98603-0-0

draulic actuators, (Oehler *et al.*, 1997) or three windings of an electrical motor (including power electronics), (Krautstrunk and Mutschler, 1999). Within electromotor driven throttles for s.i. engines only the slipper is doubled to make the potentiometer position sensor static redundant.

One example for dynamic redundancy with cold standby is the cabin pressure flap actuator in aircraft, where two independent d.c. motors exist and act on one planetary gear, (Moseler *et al.*, 1999).

As cost and weight generally are higher than for sensors, actuators with fail-operational duplex configuration are to be preferred. Then either static redundant structures, where both parts operate continuously, Figure 6a) or dynamic redundant structures with hot standby Figure 6b) and Figure 8b) or cold standby, Figure 6c) can be chosen. For dynamic redundancy fault-detection methods of the actuator parts are required, (Isermann and Raab, 1993). One goal should always be that the faulty part of the actuator fails silent, i.e. has no influence on the redundant parts.

6.3 *Fault-tolerant communication*

Drive-by-wire systems require also a fault-tolerant communication system between several electronic control units, sensors and actuators (nodes). This can be realized by a multiple bus system which has to cover hard real-time requirements. At least a dual bus system with two independent buses and independent power supplies must be realized. Both buses are then connected to all nodes, where several of them are also at least dual. Hence, a multiple access distributed real-time system results.

The CAN-Bus (Controller-Area Network) was developed in 1983 for automobiles as a serial bus system with high reliability of data transfer and high flexibility and extendibility. It is an *event-triggered* and therefore *asynchronous bus* with highest priority access, indicated by the nodes identifier. (CSMA/CA: carrier sense multiple access collision avoidance protocol). Usually only soft real-time requirements can be satisfied because the time behaviour depends on the nodes. This means that a precise time-behaviour cannot be guaranteed.

Time-triggered bus systems like the TTP (time triggered protocol) seem to be more suitable for the hard real-time requirements of drive-by-wire systems with sampling times around some ms, (Heiner and Thurner, 1998). The nodes obtain certain time slots for their access to the bus (TDMA: time division multiple access) and therefore a deterministic behaviour. All nodes are designed to be fail-silent. This means that all subsystems have to detect their faults in value and also in time and to switch into a passive state. Means to guarantee the exchange between fail-silent components are e.g.: composability, periodic data transfer, fast fault detection, global clock synchronization. For more details see (Kopetz, 1997), (X-by-wire, 1998), (Poledna and Kroiss, 1999), (Heiner and Thurner, 1998).

As these fault-tolerant components for automobiles are in development it will be interesting to observe their realizations. This may also have an effect on industrial automatic control in general.

7. AN EXAMPLE FOR A BRAKE-BY-WIRE SYSTEM

A brake-by-wire system without mechanical backup is described as an example for the development of fault tolerance and supervising functions of a drive-by-wire system. The shown version is a prototype electrical brake system of Continental Teves, Frankfurt, Germany, which was developed in recent years, partially in cooperation with the authors, (Schwarz *et al.*, 1998), (Stölzl *et al.*, 1998), see also (Balz *et al.*, 1996) and (Rieth, 1999*b*).

The brake-by-wire system consists of 4 electromechanical wheel brake modules with local microcomputers, an electromechanical brake pedal module, a duplex communication bus system and a central brake management computer, Figure 14.

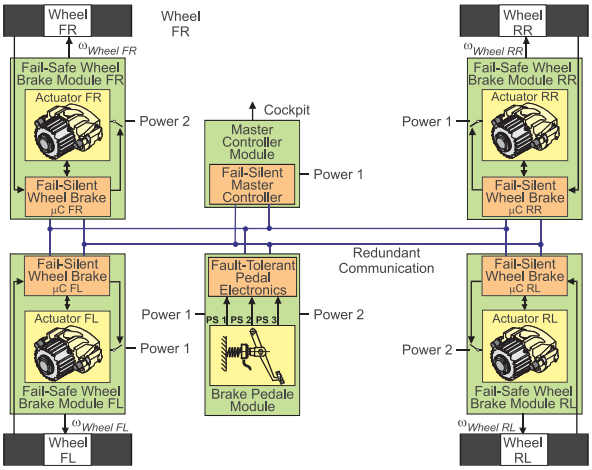

Fig. 14. Brake-by-wire architecture

The chosen overall structure is the result of a FMEA and hazard-analysis. Fault tolerance with duplex systems is implemented for the wheel brake controllers, the bus communication, the brake management computer and the power supply. However, the brake pedal contains internally higher redundancy because of its central function.

7.1 *Electromechanical brake (EMB)*

The design of the electromechanical wheel brake is driven by the demand for high electromechanical efficiency, minimized space, lightweight construction and robustness against rough environmental conditions.

ISBN 972-98603-0-0

Figure 15 shows the basic construction, (Schwarz *et al.*, 1998).

Fig. 15. Prototype of an electomechanically actuated wheel brake by Continental Teves

A generalized four pole model of the EMB is depicted in Figure 16. The current is controlled by power electronics. The d.c. motors torque is converted by the spindle gear into a friction force at the disk which then results in a braking force dependent on the tire-road characteristics. To compensate for the large parameter variations (and changing efficiency) in the whole EMB a closed loop control of the clamping force or brake torque is used in a cascaded loop system, with current and speed controllers as slave controllers. However, this requires special sensors. As an alternative the clamping force or the braking torque can be reconstructed by measuring only voltage, current and position of the d.c. motor, using adaptive dynamic models of the EMB, (Schwarz, 1999).

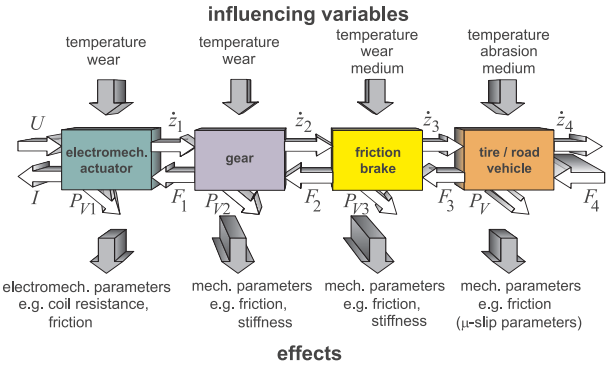

Fig. 16. Generalized four-pole models of an electromechanical disk brake
U, I: voltage, current; P_{v_i}: power losses
$\dot{z}, F$: speed, force or torque

The corresponding control and other algorithms, as e.g. parameter estimation, clamping force reconstruction and clearance-contact point detection are implemented in the brake module microcomputer-system. This is designed as a duplex system connected to the control brake management computer and the brake pedal via a duplex CAN-bus system.

7.2 *Electromechanical brake pedal*

The drivers input to the pedal is measured by a proper combination of position (and force) sensors. The measured analogue signals are then transferred to microcontrollers. After some signal processing the brake pedal information is given to the CAN-bus system.

Because the pedal represents a central part in the brake system its design must be fault-tolerant with a high degree. Therefore, an integrated FMEA and hazard analysis as summarized in Figure 4 was applied to the pedal unit. As major hazards of the EMB were determined, (Stölzl *et al.*, 1998), (Stölzl, 2000):

1) no braking after brake command from the driver,
2) braking without brake command from the driver,
3) braking with wrong deceleration,
4) one-sided braking,
5) braking with unacceptable time delay.

From this investigation following recommendations were received:

- overdimensioned pedal mechanics,
- fault-tolerant pedal electronics,
- fault-tolerant touchless pedal sensors,
- two independent power supplies,
- two independent plug connectors for communication,
- two separate boxes with sufficient protection (EMC) and cooling,
- avoidance of common-mode failures.

The most sensitive parts like electronics and sensors were found to have triple or quadruple modular redundancy.

Figure 17 shows the design of the resulting overall structure. It represents a fault-tolerant and distributed real-time system which consists of three different kinds of modules: one brake pedal module, one central controller module, and four wheel brake modules.

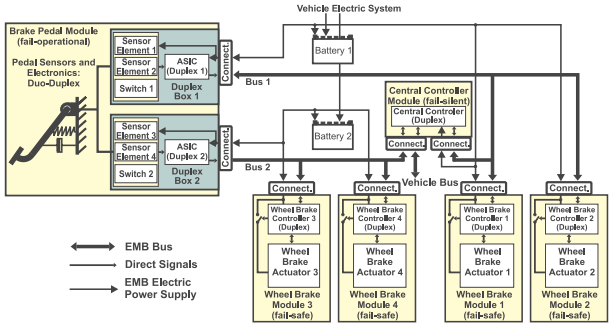

Fig. 17. Scheme of the fault-tolerant electromechanical brake system

The real-time communication system and the power system have a dynamic redundancy with hot standby. The pedal module has to be fail-operational after one failure in the sensors or electronics or plug connections.

ISBN 972-98603-0-0

The higher level brake functions as ABS, TCS, ESP und the master supervision functionality of the brake-by-wire system is mainly implemented in the integrated software of the fail-silent central controller module. The wheel brake modules can detect whether the brake management controller is working correctly or has transferred to a silent state after a failure in this unit has occurred.

Figure 18 shows the electronic hardware architecture of the pedal module. To obtain the fail-operational behaviour one triplex system or a duo-duplex system are alternatives. The duo-duplex system was chosen because it is easier to realize and can be brought in two different housings. Each sensor duplex unit contains two diverse angle sensor elements, thus four sensor signals are used to identify the driver's brake demand and to supervise the brake pedal module. Electronic hardware or sensor failures are detected within a duplex unit with a redundant voter which compares two ASIC outputs (including their two sensor signals). If the outputs differ too much a fault is assumed and one duplex unit is switched off (fails silent).

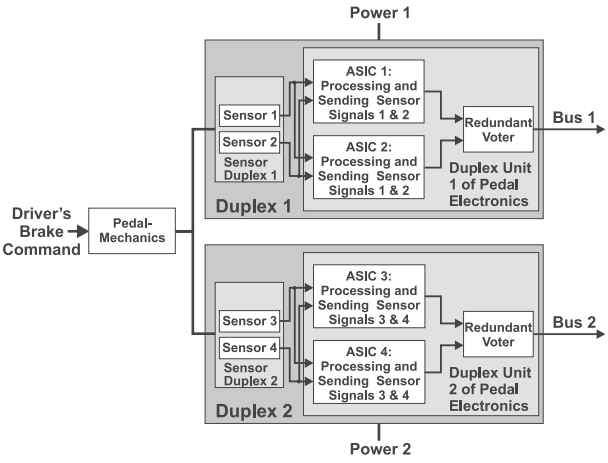

Fig. 18. Duo-Duplex architecture for the pedal module

A further task of the central controller module is to detect and locate pedal sensor failures for the case that the 4 ASICS and 2 buses work correctly. Here a model-based fault detection with parity equations is implemented. Figure 19 shows as example a brake pedal sensor configuration with three different pedal sensors and three residuals. The pedal sensors may be one angle sensor, one travel sensor and one force sensor. The residuals are the difference from one sensor signal and the reconstructed value from another sensor through an analytical pedal model.

When using four brake pedal sensors, this method is expanded to calculate six residuals, (Stölzl, 2000).

8. CONCLUSION AND OUTLOOK

Reliability and safety are of major importance for the introduction of drive-by-wire systems. The required

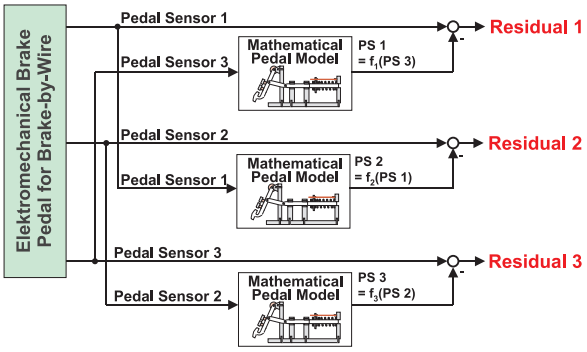

Fig. 19. Sensor fault detection with parity equations for three different sensors signals

high safety integrity needs *fault tolerance* of all electronic and electro-mechanical components, units and subsystems with regard to failures in electronic hardware, software, electrical and mechanical parts. Fault-tolerant properties can mainly be obtained by static or dynamic *redundancy*, last with cold or hot standby, leading to systems which are fail-operational for at least one failure. *Fault detection* is a basic issue for fault-tolerant systems with redundant modules. However, presently only computationally simple and reliable methods can be used, due to reasons of software reliability and testability and the limitations of small microcontrollers. Compared to static redundancy the use of fault-detection methods for dynamic redundancy saves at least one module.

An engineering challenge is the design of mass produced fault-tolerant sensors, actuators, microcomputers and bus communication systems with hard real-time requirements for reasonable low cost. Especially attractive are components with *built-in redundancy* for mass production. Since several years throttle-by-wire, shift-by-wire and electronic driver assisting systems have proven to be highly reliable and safe. Drive-by-wire systems with higher hazard severity for failures are presently developed. It is expected that the *electro-hydraulic brake* comes on the market in 2001 and the *electro-mechanical brake* about 4 years later. *Steer-by-wire* will take longer, because of the higher hazard severity and the missing inherent fault-tolerance possibilities through one pair of wheels. The development of drive-by-wire systems therefore will proceed in steps to gain experience with highly reliable and fault-tolerant sensors, microcomputers and electro-mechanical components, or in other words how to build *extremely safe mechatronic systems*.

ACKNOWLEDGEMENT: The author appreciates the good cooperation with Continental Teves, Frankfurt, during the development of the brake-by-wire system described in section 7 and the former research associates at IAT Dr. R. Schwarz and Dr. S. Stölzl. We are indebted to the support of research projects on fault diagnosis of actuators, hydraulic brakes and vehicles through Deutsche Forschungsgemeinschaft (DFG), Bonn, and Deutsche Forschungsgesellschaft

ISBN 972-98603-0-0

für die Anwendung der Mikroelektronik e.V. (DFAM), Frankfurt.

9. REFERENCES

Ballé, P., M. Fischer, D. Füssel, O. Nelles and R. Isermann (1998). 'Integrated control, diagnosis and reconfiguration of a heat exchanger'. *IEEE Control Systems* **18**(3), 52–63.

Balz, J., K. Bill, J. Böhm, P. Scheerer and M. Semsch (1996). 'Konzept für eine elektromechanische Fahrzeugbremse'. *Automobiltechnische Zeitschrift* **98**(6), 328–333.

Blanke, M., R. Izadi-Zamanabadhi, S. A. Bogh and C. P. Lunau (1997). 'Fault-tolerant control systems - a holostic view'. *Control Engineering Practice* **5**(5), 693–702.

Chandler, P. R. (1997). *Reconfigurable flight control at Wright laboratory*. Vol. III, AGARD advisory report 360, Aerospace 2020. Neuilly-sur-Seine, France.

Chen, J. and R. J. Patton (1999). *Robust model-based fault diagnosis for dynamic systems*. Kluwer Academic Publishers. Boston, MA, USA.

Chen, J., R. J. Patton and Z. Chen (1999). 'Active fault-tolerant flight control systems design using the linear matrix inequality method'. *Transactions Institute of Measurement and Control* **21**(2/3), 77–84.

Clark, R. N. (1989). State estimation schemes for instrument fault detection. In R. Patton, J. Chen and R. N. Clark (Eds.). 'Fault diagnosis in dynamic systems'. Prentice Hall. New York, NY, USA.

Clarke, D. W. (1995). 'Sensor, actuator, and loop validation'. *IEE Control Systems* **15**(August), 39–45.

Connor, B. (1996). 'Elektrische Lenkhilfen für Pkw als Alternative zu hydraulischen und elektrischen Systemen'. *Automobiltechnische Zeitschrift* **98**(7/8), 406–410.

Dickmanns, E. D. (1995). Road vehicle eyes for high precision navigation. In Linkwitz (Ed.). 'High precision navigation'. Dümmler Verlag. Bonn, Germany. pp. 329–336.

Favre, C. (1994). 'Fly-by-wire commercial aircraft: the airbus experience'. *International Journal of Control* **59**(1), 139–157.

Fritz, H. (1996). 'Modellgestützte neuronale Geschwindigkeitsregelung von Kraftfahrzeugen'. *Automatisierungstechnik* **44**(5), 252–257.

Germann, S. and R. Isermann (1995). Nonlinear distance and cruise control for passenger cars. In 'First IFAC-Workshop on Advances in Automotive Control'. pp. 203–208.

Gertler, J. J. (1999). *Fault detection and diagnosis om engineering systems*. Marcel Dekker. New York, NY, USA.

Gilz, G. and A. Wokan (1993). 'Elektronisches Gaspedal für Nutzfahrzeuge'. *Automobiltechnische Zeitschrift* **95**(2), 80–88.

Heiner, G. and T. Thurner (1998). Time-triggered architecture for safety-related distributed real-time systems in transportation systems. In 'Fault-Tolerant Computing (FTCD 28)'. Munich, Germany.

Henry, M. P. and D. W. Clarke (1993). 'The self-validating sensor: rationale, definitions, and examples'. *Control Engineering Practice* **1**(2), 585–610.

IEC 61508 (1997). Normenentwurf IEC 61508, Part 1-7. Functional Safety of E/ E/ PES: (complex) Electrical/ (complex) Electronic/ Programmable Electronic Systems. Version 4.0.

IFAC Journal Control Engineering Practice (1996). Special Section on Supervision, Fault Detection and Diagnosis of Technical Processes. (Tutorial Workshop IFAC Congress 1996), Vol. 5 (5), 637-719.

Isermann, R. (1994*a*). Integration of fault detection and diagnosis methods. In 'IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS)'. Espoo, Finland.

Isermann, R. and U. Raab (1993). 'Intelligent actuators - ways to autonomous actuating systems'. *Automatica* **29**(5), 1315–1331.

Isermann, R. (Ed.) (1994*b*). *Überwachung und Fehlerdiagnose*. VDI-Verlag. Düsseldorf, Germany.

Jurgen, R. K. (Ed.) (1999). *Electronic braking, traction, and stability control. SAE: PT-76*. Warrendale, PA, USA.

Kohlberg, G. (1985). 'Elektronische Motorsteuerung für Kraftfahrzeuge'. *Motortechnische Zeitschrift*.

Kopetz, H. (1997). *Real-time systems*. Kluwer. Boston, MA, USA.

Krautstrunk, A. and P. Mutschler (1999). Remedial strategy for a permanent magnet synchronous motor drive. In 'Proceedings of EPE99'. Lausanne, Switzerland.

Leveson, N. (1995). *Safeware. System safety and computer*. Addison-Wesley Publishing Company. Reading, MA, USA.

Moseler, O., T. Heller and R. Isermann (1999). Model-based fault detection for an actuator driven by a brushless dc motor. In '14th IFAC World Congress'. Vol. P. Beijing, China. pp. 193–198.

Oehler, R., A. Schoenhoff and M. Schreiber (1997). Online model-based fault detection and diagnosis for a smart aircraft actuator. In 'IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS)'. Vol. 2. Kingston upon Hull. pp. 591–596.

Patton, R. J. (1997). Fault-tolerant control: the 1997 situation. In '"IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS)'. Vol. 2. Kingston Upon Hull, UK. pp. 1033–1055.

Pfeufer, T. (1997). 'Application of model-based fault detection and diagnosis to the quality assurance

ISBN 972-98603-0-0

of an automotiv actuator'. *Control Engineering Practice* **5**(5), 703–708.

Poledna, S. and G. Kroiss (1999). 'TTD: Drive-by-wire in greifbarer Nähe'. *Elektronik* (14), 36–43.

Potocki de Montalk, J. P. (1993). 'Computer software in civil aircraft'. *Mircoproc. Mircosystems* **17**(1), 17–23.

Prometheus (1998). Report on recommended practice of safety and reliability engineerng of future automotive system. Germany.

Rauch, H. E. (1995). 'Autonomous control reconfiguration'. *IEEE Control Systems Magazine* **15**(6), 37–48.

Reichart, G. (1998). 'Sichere Elektronik im Kraftfahrzeug'. *Automatisierungstechnik* **46**(2), 78–83.

Reliability Toolkit (1995). Commercial Practices Edition.Rome Laboratory and Reliability Analysis Center. Rome, NY, USA.

Rieth, P. (1999*a*). Elektronische Fahrerassistenz. In 'VDA-Technischer Kongress'. Frankfurt, Germany.

Rieth, P. (1999*b*). Technologie im Wandel: X-by-wire. In 'Neue Elektronikkonzepte in der Automobilindustrie. Institute for International Research (IIR)'. Stuttgart, Germany.

Schunck, E. (1999). Das Sicherheitskonzept einer elektrohydraulischen Bremse. In 'VDA Technischer Kongress'. Frankfurt, Germany.

Schwarz, R. (1999). *Rekonstruktion der Bremskraft bei Fahrzeugen mit elektromechanisch betätigten Radbremsen*. Fortschr.-Ber. VDI Reihe 12 Nr. 393. VDI Verlag. Düsseldorf, Germany.

Schwarz, R., R. Isermann, J. Böhm, J. Nell and P. Rieth (1998). Modeling and control of an electromechanical disk brake. In 'SAE Technical Paper Series'. Vol. SP-1339.

Stevens, W. B. (1996). The automated highway system program: a progress report. In '13th World Congress of IFAC'. Vol. plenary and index. San Francisco, CA, USA. pp. 25–33.

Stölzl, S. (2000). *Fehlertolerante Pedaleinheit für ein elektromechanisches Bremssystem (brake-by-wire)*. Fortschr.-Ber. VDI Reihe 12, VDI-Verlag. Düsseldorf, Germany.

Stölzl, S., R. Schwarz, R. Isermann, J. Böhm, J. Nell and P. Rieth (1998). Control and supervision of an electromechanical brake system. In 'FISITA World Automotive Congress, The Second Century of the Automobile'. Paris, France.

Storey, N. (1996). *Safety-critical computer systems*. Addison Wesley Longman Ltd.. Essex, UK.

Suryanaryanan, S. and M. Tomizuka (2000). Fault-tolerant lateral control of automated vehicles based on simultaneous stabilization. In '1st IFAC Conference on Mechatronics Systems'. Darmstadt, Germany.

Tomizuka, M. (1997). Automated highway systems - an intelligent transportation system for the next century. In 'Proceedings of the IEEE/ASME International Conference on Advanced Intelligent Mechatronics '97'. Tokyo, Japan.

van Zanten, A. T., R. Erhardt and G. Pfaff (1995). VDC. The vehicle dynamics control system of Bosch. In 'SAE Technical Paper Series'. number 950759.

van Zanten, A. T., R. Erhardt, H. Schramm and G. Pfaff (1999). Die Fahrdynamik-Regelung ESP vom Pkw zum Nkw. In M. Bargende and J. Wiedemann (Eds.). '3. Stuttgarter Symposium Kraftfahrwesen und Verbrennungsmotoren'. expert verlag. Renningen-Malmsheim, Germany. pp. 801–814.

X-by-wire (1998). Safety related fault-tolerant systems in vehicles. Final report of EU Project Brite-EuRam III, 3.B.5, 3.B.6, Prog. No. BE 95/1329. Contract No: BRPR-CT95-0032.

ISBN 972-98603-0-0