

Approaching a SIL3-Compatible Failsafe Computer Control System in Safety-Critical Chassis Applications

Zheng-Yu Jiang, Jens Fiedler and Herbert Preis

Continental, Division Chassis & Safety, Chassis Components

Copyright © 2009 SAE International

ABSTRACT

The design of a cost-effective SIL3/ASILD-compliant failsafe computer control system is a great challenge because of the requirements of IEC 61508 and/or ISO CD 26262. In this paper the formal design methods in concept, space, time, and function domains are presented, which are used for the development of a failsafe chassis control system. We discuss the generic failsafe system architectures based on one-core and multi-core μ Cs in the framework of Markov's safety model, and associated safety metrics like DC, SFF, and PFH. The safety aspects require that, a safety-related system is validated by an adequate safety analysis method. For this purpose a new integrated FMEDA (iFMEDA) for the validation of a safety-related vehicle application system is briefly introduced. Finally, the use of safety concepts for failure monitoring in practice chassis applications and generic diversity algorithms is shown.

INTRODUCTION

Since the standards IEC 61508 and ISO CD 26262 have been introduced to the development processes of the automotive industry, the design of a cost-effective SIL3/ASILD-compliant (SIL: Safety Integrity Level /ASIL: Automotive Safety Integrity Level) failsafe computer control system for safety-critical chassis applications became a great challenge, which affects the whole product development process. New safety concepts are required and the rapid development in micro-electronic techniques provides now the opportunity to realize these novel safety technologies. Furthermore it opens a new way to fulfill the SIL3/ASILD challenges.

Continental has developed cutting-edge fail-safe and fail-tolerance technologies in a wide range of automotive products. For instance the Continental triple core is one of these contributions to build a safety-critical vehicle control system. In this paper the formal design methods for SIL3 compatible failsafe control systems, and the failsafe system architectures based on one-core and multi-core micro-controllers are presented. The shown methods are based on safety-critical chassis applications taken out of practice.

First, we discuss the SIL3/ASILD challenges, which are faced during the production of a failsafe computer control system in the context of concept, space, time and functional domains. To meet these challenges, the safety concept must involve the overall product development process in to which the functional safety development process has to be integrated.

It is assumed, that the respective systems have to be the SIL3 compliant as they are applied to safety-critical chassis systems. An example for such a system is a vehicle observer, an active steering system, an electric parking brake system or other OEM specific high level functions.

In this paper the generic failsafe system architectures based on one-core or multi-core μ Cs in the framework of Markov's safety model, and associated safety metrics like DC (Diagnostic Coverage), SFF (Safe Failure Fraction), and PFH (Probability of Failure per Hour) are discussed. In order to design a cost-effective product, the safety requirements have to be allocated to hardware and software by a HW&SW co-design in an optimal way. The system has to be validated by a safety analysis method, like FMEDA (Failure Mode Effect and

Diagnostic Analysis). Here a new integrated FMEDA (iFMEDA) will be briefly introduced. Additionally, the use of safety concepts for failure monitoring, and generic diversity algorithms, for example an arithmetic coding algorithm, are presented related to practice chassis applications.

THE 4-DOMAIN CHALLENGES

The safety challenges for approaching a SIL3 compatible failsafe computer control system can be classified into 4 domains (4-D) namely space, time, and concept, as well as function domains [1].

One important challenge in the space domain is, from the physical point of view, the system failure rate. For example for a SIL3 system it is required to have less than 10 FIT (Failures In Time, 1 FIT is one failure per 10^9 hours, about 114,000 years) according to IEC 61508. Since the failure rate of a system is the sum of the failure rates of all components or sub-systems, the requirement for the failure rate of such a component or sub-system may even be 1 FIT. In order to achieve this, redundant components or redundant sub-system(s) have to be introduced to a SIL3 compatible failsafe control system. But the product cost plays an important role in the decision-making of a redundant strategy in a highly competitive market. Particularly, the ECU (Electronic Control Unit) mechanic concept must be more robust, reliable, and safe to damp mechanical shocks and vibrations as well as EMI disturbances.

The second challenge domain is the time domain. The product development cycle must be as short as possible. The failure detection and reaction times and even the system's start-up time have to be as quick as possible. This is especially a challenge for distributed systems, which incorporate other vehicle ECUs. This makes the reduction in product cycle time more difficult, because the system design and integration will get more and more complex in a distributed development of a vehicle dynamic control system.

Since most vehicle chassis control systems are hard real-time computer control systems with multiple tasks running on, some non-functional safety requirements must also be considered for the design of a SIL3 compatible system. For instance, to avoid system timing failures at run-time, an effective method to perform the system schedulability and timing analysis must be applied [2] in order to make the system more predictable. However, this can be very difficult due to increasing complexity of software and hardware architectures.

The concept domain is the third domain. To meet the safety requirements of all the different standards (e.g.: international and region-specific), new safety technology and methods as well as new processes have to be applied or developed; and possible additional functional changes must be adapted to the products. For instance,

a more feasible concept for a generic chassis control system has to be developed in order to control a modern vehicle dynamics control system in the most optimal way.

The last domain is in the function domain. Regarding the specific requirements in safety functions, and various ways of human failure (e.g.: failure in driving behavior), the automotive application functions will be more and more complex, because an increasing number of mechanic functions are realized as software functions. Therefore, the software size and complexity is increasing dramatically. As a result, more and more parts of the software become safety-critical, and therefore the function verification and validation plays an important role in order to achieve the required functional safety level of the system

The other safety challenge in the function domain is the protected OS (Operating system). The protected OS is firstly required by OEMs. The two most interesting aspects of a protected OS is the protection of the application software as well as of the resource access. For the later one the software failure can be more intricate and subtle because a direct access of a safety critical resource [2] can damage a safety-related function.

It is certainly a large challenge to get feasible solutions to 4-D challenges. In the following sections the formal safety methods and the possibilities ways to achieve these challenges are discussed.

OVERALL SAFETY CONCEPTS

Since a vehicle control system has a great potential of hazards, the most important task for the safety concept is how to reduce the hazard risk to an acceptable level. In fact, the functional safety is a system topic. The procedure to establish a SIL-3 compatible failsafe ECU involves the complete product life-cycle, in which the functional safety process has to be integrated. In Continental AG the functional safety process has been established according to the IEC 61508. The resulting Continental functional safety development process has been successfully integrated into the CMMI3 product development process, and is adapted to each business division and business unit (refer to figure 1).

To meet the SIL3 challenge and approach a SIL3 compatible failsafe control device, following generic safety concepts must be considered in safety-related chassis system design.

MODULAR CONCEPT - The system components including sensor modules and the related software like the safety monitoring, and the model-based computations must be designed in modular re-configurable manner in order to meet different safety requirements from various vehicle control systems and to identify system faults like a HW component failure.

DIVERSITY CONCEPT - Diversity design has to be applied to avoid the systematic failures and common cause failure or common mode failure. Data diversity, design diversity must be applied to reduce the total probability of dangerous failures/hr (PFH).

MULTI-LEVEL MONITORING CONCEPT - The versatility failures in a computer control system can occur in different levels of hardware and software layers. A failure monitoring mechanism must be implemented to detect the different kinds of failures of a simple as well as of a sophisticated component.

TRACEABILITY CONCEPT - All product documents have to fulfill the traceability requirements. All errors discovered at run-time have to be recorded in a non-volatile memory, e.g.: EEPROM and the test procedures for diagnosis must be documented.

REDUNDANT DESIGN CONCEPT – In case the systems are designed redundantly, it is possible to detect and handle errors in particular ways. Redundancy can be realized by:

Information Redundancy: The information, like checksums, alive counters, signatures, and acknowledgement, can be added in the data processing for the sake of failure detection and correction.

Hardware Redundancy: System components can be duplicated in order to work parallel in a dual or triple modular way. Its purpose is to increase dependability (availability, reliability and safety) or to detect errors. It should be mentioned, that some sensor signals can be provided as virtual signals. This means, that a virtual sensor signal can be redundantly supplied by a model-based computing. For example, a redundant safety critical yaw rate can be calculated by using other independent sensor signals.

Time Redundancy: The time redundancy can be realized by a double and re-execution of N-Version or N-Copy software in safety-related control system. It is certainly an effective safety measure to detect systematic and random failure of a safety-related control system.

FORMAL SAFETY DESIGN METHODS IN THE DEVELOPMENT PROCESS

In practice, the safety design methods for approaching a SIL3 compatible computer control system have to accommodate the safety development process. The most important safety design methods are risk analysis, FMEA (Failure Mode Effect Analysis), FMEDA, FTA (Failure Tree Analysis) and Markov modeling analysis.

The conceptual design phase is the starting point of the safety development process shown in figure 1. During this phase the system or subsystem under consideration has to be defined, including the system function description and system interfaces.

The hazard analysis is one important element in the second process phase. A hazard analysis and a system risk assessment must be performed in order to identify all possible potential hazards of the designed system. The risk analysis derives an inventory of all potential hazards of the system. Additionally their severity, probability of occurrence, and their controllability is estimated, and the associated risk is calculated by using a risk graph. In the hazard and risk assessment the vehicle operation state, the vehicle situations and state transitions have to be considered, for instance the vehicle starts, accelerates as well as vehicle brakes under different road and environment conditions. A worst-case scenario has to be considered for the final SIL level assessment. Like other safety documents the hazard analysis must be reviewed, and the hazards identified in the hazard analysis have to be taken into account by the safety concept.

There are several important subjects, which must be contained in the safety concept. First, the safety goals and the safe state have to be clearly defined in order to avoid the hazards or move a failure state to a safe state, respectively. More commonly, the safety requirements and safety measures to detect all potential failures have to be specified. Under these premises, the safety system architecture must be proposed in order to realize the related SIL level requirements.

In the third process phase, the safety requirement specification must be created. All functional safety requirements are allocated in hardware, software, and mechanical design. The safety requirements are documented in a traceable database together with other non-safety related system and software requirements. At the same time, a FMEA and if necessary a FTA have to be performed.

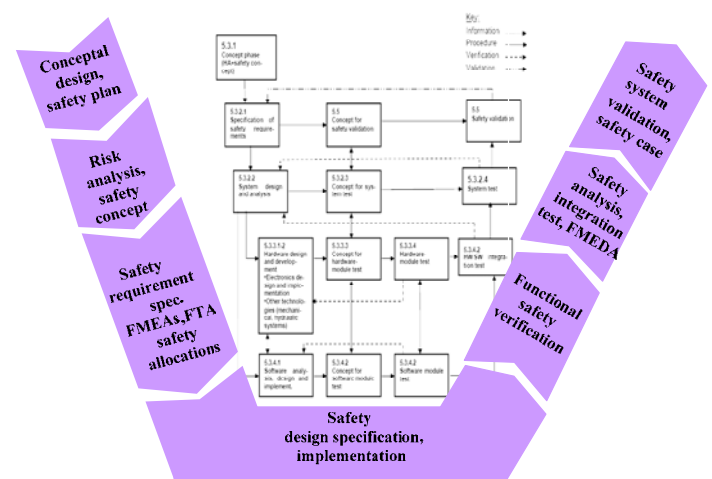


Figure 1: Continental product functional safety development process

The FMEA (Failure Model and Effect Analysis) is a method, which is used for the identification of potential failures or failure modes of the examined subject.

(system, subsystem, or software/hardware components). Furthermore by this method the according failure effects together with the criticality of this failure effects shall be discovered and classified. This method is also known as Failure Modes, Effects and Criticality Analysis. The failure modes, which are identified in the Hazard analysis and the safety concept, can be used for the FMEA. The necessary safety technologies namely the safety measures will be identified to control the potential failure and to lower the system risk to an acceptable level. The FMEA risk is calculated by (Risk Priority Number) = (Severity) x (Occurrence) x (Detection). It shall be noted, that the main benefits of performing a FMEA is to prevent faults (causes of failure) and thus weaknesses in the design, which might result in dangers or loss of the system, property or persons.

A complement method to FMEA can be the FTA (Fault Tree Analysis). The FTA synthesizes data from the FMEA and takes into account the combination of causes, which lead to hazards (identified during the hazard and risk assessment). It is a top-down approach for the failure analysis, which starts with an undesirable event called a *top event*. Then it determines how this top event can be caused by individual or combined lower level failures or events, rather than identifying potential hazards in the FMEA. The fault tree is a graphical model of parallel or sequential combinations of faults in different levels, which contribute to the top event. Unlike the FMEA, the FTA can be used for a quantitative analysis, for instance, the probability of the failure rate of the top-level event can be calculated by finding minimal cut sets.

At the beginning of the fourth phase in the functional safety development process, the safety design specification is worked out, and their implementation in product hardware and software, and mechanic as well can be followed as required. At the same time, the related test concepts and specifications shall be completed.

A most time-consumed phase is the fifth phase, namely the verification phase for safety-critical modules and units. The system units, components, and subsystems design implementation are verified by a tool supported test versus the requirement specifications.

One important issue in sixth phase is the safety system analysis, where the FMEDA (Failure Mode Effects and Diagnostic Analysis) is performed in order to verify whether the system fulfills the required safety integrity level or not. FMEDA provides a systematic analysis to obtain a product-level failure rates, failure modes and diagnostic coverage. In FMEDA, all component functionality, their failure modes and their impact on product function, as well as their diagnostic ability is considered. The main benefits are the quantitative evaluation of the safety integrity metrics, the identification of unacceptable failure modes, and finding the potential improvements of the system design. IEC61508 recognize the FMEDA method to verify

whether safety integrity level is achieved in a particular automotive application system. The two used safety integrity metrics are the safe failure fraction (SFF) and the diagnostic coverage (DC). The FMEDA is discussed in more detail in next section.

During the final stage, the safety system verification must be carried out, where the system shall be tested against the system safety requirements. The system can be verified in real environment e.g.: in a test vehicle or a HiL (Hardware in the Loop) test environment, where the safety case is developed to provide a convincing and valid argument that a system is adequately safe for a given application in a given environment [3].

SAFETY MONITORING METHODS AND CONCEPTS

The key aspect of the functional safety in computer control system is minimizing the risk of hazards to an acceptable level. One important method is the safety monitoring method and concept in cooperating with underlying hardware SIL3 compatible platform. For this purpose, some generic monitoring methods and concepts are developed.

FOUR KINDS OF SAFETY MONITORING METHODS

For the realization of SIL3 compatible ECUs, four kinds of monitoring methods can be applied, namely basic monitoring, active tests, comparative tests and model-based monitoring. These four monitoring methods are involved in a multi-level safety monitoring concept. The basic monitoring consists of self tests in sensors, actuators, ASIC application chips, and micro-controller components. Whereas the active tests are interactive between a main micro-controller and independent units like an ASIC chip or diverse slave micro-controllers. Besides, the active tests can also be issued by external requirement to a micro-controller, a smart sensor or an intelligent actuator. A relative complex test method is the comparative test or voter, in which redundant hardware and/or diversity software are applied. In general, an external independent comparator has higher capability for failure detection as an internal comparator. By using vehicle dynamic model-based monitoring, most dormant failures can be revealed and hence improve the availability, reliability, and safety.

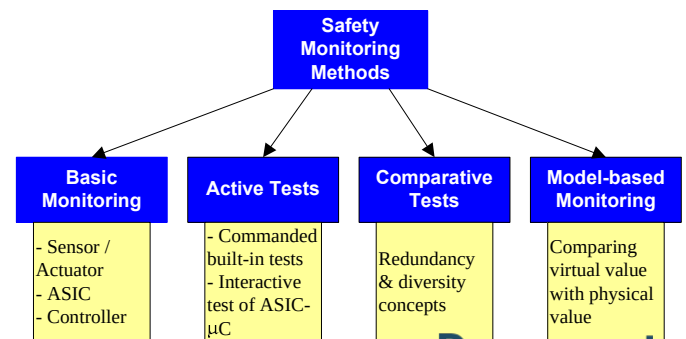


Figure 2: Four kinds of safety monitoring methods