Advanced Materials Research *Online: 2011-05-31*
ISSN: 1662-8985, Vols. 255-260, pp 2179-2182
doi:10.4028/www.scientific.net/AMR.255-260.2179

Functional Safety Management in Microcontroller Design and Development Process: the Case of Safety-critical Vehicle Systems

Binghai Zhou[1,a] and Ziqing Zhai[2, b]

[1] School of Mechanical Engineering, Tongji University, Shanghai 201804, PR China

[2] School of Mechanical Engineering, Shanghai Jiaotong University, Shanghai 200240 PR China

[a]zbh719@sohu.com, [b]chingzhai@sjtu.edu.cn

Key words: Functional safety, Process management, Safety assessment, Microcontroller

Abstract. Safety is always the key issue in automotive industry. The adoption of hi-tech automotive applications requires not only the development of reliable electrical/electronic/programmable electronic (E/E/PE) systems and communication protocols, but also an evolution in functional safety process management. ISO/WD 26262, the adaption of IEC 61508 for road vehicles, provides guidelines and standardized measurements for functional safety. This paper discusses how automotive microcontroller suppliers can deal with this new challenge by integrating functional safety management into product design and development. An ISO/WD 26262-compliant functional safety management flow is proposed, with specifications on techniques of corresponding safety assessment.

Introduction

Historically, safety considerations have been issues of the utmost importance for automotive manufacturers and suppliers [1]. As hi-tech automotive applications begin to receive increasing research effort and public attention, reliability and safety concerns have also risen up. Meanwhile, it has become a consensus for automotive industry that reliability and safety of products is determined not only by the technical aspects of products, but also by the business processes in an organization realizing and operating these products [2]. ISO/WD 26262 requires clearly that both aspects should be taken into accounts for product's whole safety lifecycle. While facilitating the clarification of functions and responsibilities for car manufacturers and suppliers, this standard also brings new challenges for implementation where real situations differ from company to company. On the other side, vast growth is envisaged in automotive microcontrollers, the "brain" of various safety-critical vehicle systems. Some of the automotive microcontroller suppliers have already started to pursue compliance with ISO/WD 26262 in order to develop more reliable and customized products, thus to gain market initiative.

ISO/WD 26262

ISO/WD 26262 is the working draft of the international standard on functional safety for E/E/PE safety-related systems within road vehicles (classes M, N, O). It provides specifications on activities to be carried out in each stage of automotive safety lifecycle. It also offers an automotive risk-based approach for determining risk classes (Automotive Safety Integrity Level, ASIL) and corresponding safety requirements for items to achieve an acceptable ASIL [3].

Automotive safety lifecycle. According to ISO/WD 26262, functional safety is ensured through three phases in product safety lifecycle: concept phase, product development and product release [4].

In concept phase, hazard analysis and risk assessment should be conducted to determine the appropriate ASIL for every function, corresponding functional safety concepts should be developed.

In the phase of product design and development, technical safety requirements on architecture should firstly be specified, giving coherent answer to associated functional safety concepts. These technical safety concepts encompass the development of hardware and software. Their efficiency should be assessed for every safety goal during design process with respect to ASIL-based criteria.

Finally, in the phase of After SOP (start of production), appropriate measures should be implemented to ensure that production and operation would not deteriorated safety goals.

Challenges for the development of safety-related equipments. There are various rules and regulations existing for safety in today's automotive industry, which seriously hinder the development of automotive safety-related hi-tech systems. By normalizing functional safety management during automotive lifecycle, ISO/WD 26262 is able to provide a unified safety control framework for all participants in automotive industry, and will replace the majority of existing rules and regulations in a foreseeable future. Here we have identified three trends that will be brought by the establishment of ISO/WD 26262: (1) Function analysis, risk assessment and safety goal identification move towards early stage of product concept phase; (2) Intermediate verification activities take place within every phase; (3) Closer corporation between business, design, test and quality staffs.

As a result, safety-related activities should be rigorously integrated into early stage of product design and development, and this requires an adequate management flow to encompass all these activities.

Functional Safety Management Flow for Microcontroller Design and Development

Role of microcontroller. Microcontroller plays an indispensable role in hi-tech automotive applications such as by-wire systems and vehicle networks. As the core of information processing, microcontroller is safety-critical in such applications. A fault occurs in any part of the microcontroller can result in an unwanted accident if not detected and handled quickly and properly before the system goes wrong. As a consequence, safety requirements are generally very strict with microcontrollers on architecture and safety mechanisms with fault-tolerant characteristics.

The architecture design for microcontroller requires a profound understanding on fault tolerant mechanisms, and should be adequate to implement system fault tolerant strategy with the run of software. Regarding this specialty, we consider microcontroller as a system in concept phase, but hardware in product development.

Establishment of the functional safety management flow. Generally, the standard presents a framework, which deals in a systematic manner with all the activities necessary to achieve the safety requirements. However, every application of a given standard is different because of differences in project details [5]. Here, we conclude three principles from previous discussions with automotive microcontroller designers: (1) Focus on product conception and development; (2) Focus mainly on hardware development, but also include system level approach on the scale of microcontroller; (3) Provide a fast, easy and clear understanding for all related working staffs.

Based on these guidelines, the functional safety management flow (shown in the left part of Fig. 1) is established with several rounds of careful study on ISO/WD 26262 and the real business practices in today's automotive microcontroller producers. The right part of Fig.1 presents the original phase model for the development of a hardware safety-related item in ISO/WD 26262 [6]. The grey dash lines link the equivalent phases in both models to each other, demonstrating the conformity of the proposed flow to ISO/WD 26262.

Based on the framework of hardware development given by ISO/WD 26262 [6], this new model also employs some activities from other chapters of the international standard including overall management, system level development and support processes into different steps to ensure plausibility and soundness of the proposed management flow.

Instructions on the implementation. Requirements attached to the proposed management flow are summarized from relevant ISO/WD 26262 chapters, and can be classified into five categories: (1) Quality and managements requirements; (2) Safety requirements; (3) Design and architecture requirements; (4) Techniques and methods requirements; (5) Test and assessment requirements. The list below briefly describes the activities that will be carried out in each step of this management flow. Function units which should participate in the step are identified in the corresponding parenthesis: (1) *Define item and its major functions to be performed*: Identify potentially hazardous driving situations,

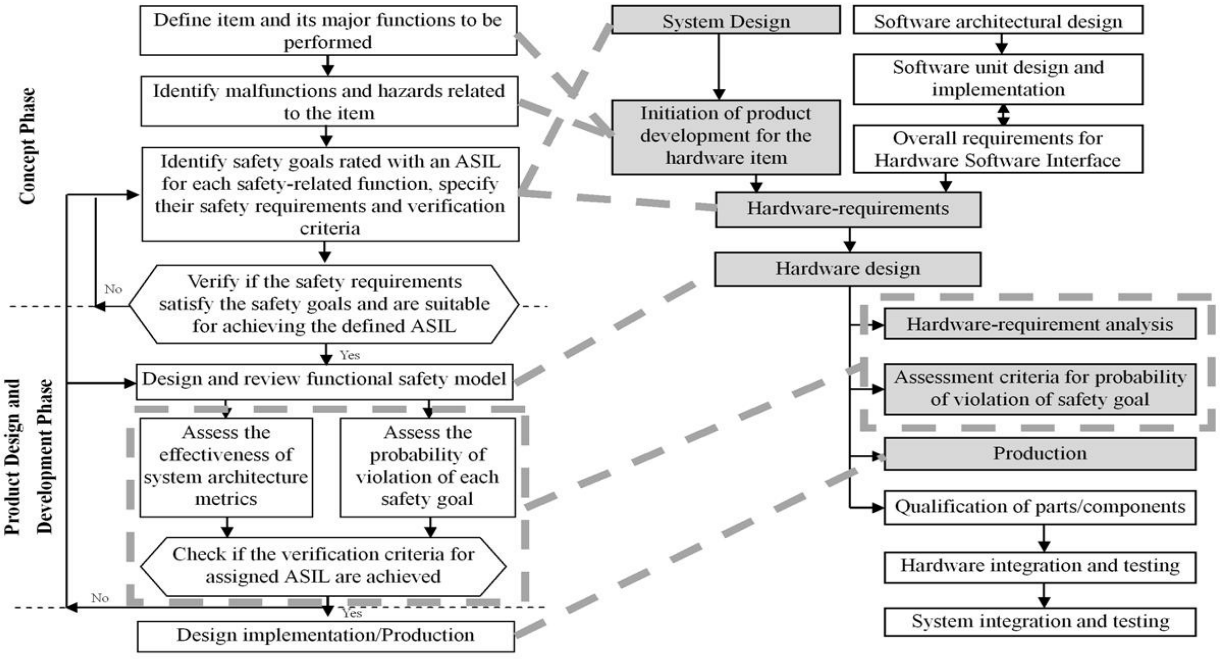

Fig. 1 Functional safety management flow and its comparison to ISO/WD 26262 phase model for the development of a hardware safety-related item

and determine an appropriate ASIL of each situation by applying the classification criteria given in ISO/WD 26262. (2) *Identify malfunctions and hazards relate to the item*: Examine each safety-related function separately and determine the functional blocks to be used to carry out this function, then determine and evaluate the impact of every failure mode of every identified functional block by risk assessment. (3) *Identify safety goals rated with an ASIL for each safety-related function, specify their safety requirements and verification criteria*: define safety goals to ensure the performance of every safety-related function. Every safety goal shall be formulated for each hazardous event evaluated in the risk assessment, and appropriate ASIL should be assigned to all safety goals. (4) *Verify if the safety requirements satisfy the safety goals and are suitable for achieving the defined ASIL*: Verify if functional safety requirements can satisfy the safety goals and are suitable for achieving the defined ASIL, if not, iteration between steps in concept phase is needed, which includes either rework on item definition or functional safety requirements or even both. (5) *Design and review functional safety model* : Conduct architecture design, and check the complete and correct detailing and implementation of the microcontroller requirements specification into design. Classify all potential faults that might endanger the fulfillment of ASIL. (6) *Safety assessment*: ISO/WD 26262 proposes two options for safety assessment: The performance of system architecture (by system architecture metrics) and the performance on assigned safety functions (by probability of violation of each safety goal). (7) *Check if the verification criteria assigned to each ASIL are achieved*: verify if the results obtained in safety assessment can meet the target values given in ISO/WD 26262 on the assigned ASIL, if not, iteration of previous steps should be done until all requirements are satisfied.

In addition, main outputs of every step (e.g. project safety plan, design reviews, testing and analysis results) should be documented along product conception, design and development processes.

Integration of Safety Assessment and Functional Safety Management Flow

The proposed model provides a functional safety management flow that can be followed in microcontroller design and development process, while techniques for safety assessment should be substantiated to enable the implementation of the whole process. The same as IEC 61508, ISO/WD 26262 does not prescribe specific techniques to be used on verification of the achieved safety, but only gives general guidelines and recommendations. To provide microcontroller suppliers with reliable and readily-applicable tools, we have selected corresponding techniques for important assessment/verification steps by required inputs and available safety analysis techniques.

FMEA (Failure Mode and Effects Analysis) is an inductive analysis which examines all component failures and evaluates the effects of these failures on the entire systems [7]. FMEA has long been a traditional safety practice in automotive industry. Abundant failure information exists for various products. However, traditional FMEAs are rather component- based than function-based. To comply to ISO/WD 26262, a safety function-oriented FMEA can be set up to analyze component failure modes in regard with the safety function it shall perform. Moreover, the identified failure modes can be classified into different types of fault according to the criteria proposed in ISO/WD 26262 (with expert reviews) to facilitate further safety analysis on system architecture metrics.

FTA (Fault Tree Analysis) is selected to conduct quantitative approach on the probability of violation of safety goal because of its wide recognition, efficient semantics and easy adaptability with FMEA. Various commercial software is available to conduct FTA, some even embedded with other related methods and can perform more sophisticated calculations. Appropriate assumptions must be made considering system independencies and data constancy, etc.

Finally the difficulty, as well as the state of art in quantitative safety assessment on microcontroller is attached to the determination of diagnostic coverage of safety-mechanisms facing the occurrence of fault. A popular and fast approach on fault coverage estimation is VHDL. This is an off-line simulation where the whole system could be modeled by MATLAB/Simulink. With the injection of fault-generating code, fault-specific detection probabilities could be obtained. However, the results is only reliable for combinational circuits but not for sequential circuits, while both types of circuits are indispensable in a microcontroller. Although numerous mathematical models have been built up to solve this problem, no easy solution could be obtained concerning the complexity and diversity of system structure and context. There is still a long way to go before a basic agreement is reached, and before that, diagnostic coverage can only be roughly estimated.

Conclusion

This paper presents an approach on the integration of functional safety management into automotive microcontroller design and development process, whose originality lies in its orientation on safety function and safety mechanisms, its conformity with ISO/WD 26262. Although industry barriers which may hinder the corporation on safer products between car manufacturers and suppliers still exist, and technological limitations are still vast in fault-tolerant systems and safety analysis methods, this paper provides valuable instructions on the approach towards a more efficient, economical, as well as more customer-favored functional safety management for automotive hardware suppliers, which if applied, can greatly contribute to the enhancement of enterprise's safety culture.

Acknowledgements

This work is supported by National Natural Science Foundation of China (No. 71071115).

References

[1] C. Mondragon, A. Mondragon and E. Mondragon: Inter. J. Pro. Eco. Vol.118 (2009) p.473.

[2] A. Brombacher: Reliability Engineering and System Safety Vol. 66 (1999), p.109-120.

[3] ISO/WD 26262 Introduction, 2001.

[4] ISO/WD 26262-2 Management of functional safety, 2001.

[5] P. Chung, L. Cheung and C. Machin: Knowledge-Based Systems Vol. 21 (2008), p.332.

[6] ISO/WD 26262-5 Product Design and Development: Hardware Level, 2001

[7] J. Rouvroy, E. van den Bliek: Reliability Engineering and Safety Systems Vol.75 (2002), p.289.