2013 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE)
2013 International Conference on Materials and Reliability (ICMR)
2013 International Conference on Maintenance Engineering (ICME)

Research Trends In Automotive Functional Safety

Azianti Ismail
Faculty of Mechanical Engineering
Universiti Teknologi MARA
Shah Alam, Malaysia
azianti106@salam.uitm.edu.my

Won Jung
Dept. of Industrial and Management Engineering
Daegu University
Gyeongsan, South Korea

Abstract— **In recent years, most of the modern automobiles are equipped with embedded electronic systems which include lots of Electronic Controller Units (ECUs), electronic sensors, signals, bus systems and coding. Due to the complex application in electrical, electronics and programmable electronics, the need to carry out detailed safety analyses which focuses on the potential risk of malfunction is crucial for automotive systems. IEC 61508 has become a foundation for international standard safety-related system for airborne systems, railway, nuclear power plants, medical equipment, energy and process systems, machinery, furnaces and automobiles. The failure of such system could have significant impact on the safety of humans and/or the environment. Thus, ISO 26262 has been introduced in November, 2011 for automotive electrical/electronic (E/E) systems which address the complete safety installation from sensor to actuator with its technical as well as management issues. In this paper, the international trends on pre and post introduction of ISO 26262 will be analyzed in which to see the direction of potential research in this area.**

Keywords- ISO 26262; ASIL; style; automotive safety requirements; functional safety

I. INTRODUCTION

In the automotive industry advancements which resulted from pure mechanical to electronically controlled systems, new challenges have emerged in managing functional safety. Anti-lock Braking Systems (ABS), Electronic Stability Program (ESP), Adaptive Cruise Control (ACC), Emergency Brake Assistant (EBS), Brake-By-Wire (BBW), Steer-By-Wire (SBW), air bags, light control and tire pressure are some of the examples of the safety critical systems in automobile nowadays which consist of larger system architecture with complex interaction and interface.

Prior to ISO 26262, there are many standards that have been introduced which cover on quality management, testing of hardware and software as listed in table 1. Most of the testing is tailored for scenarios-oriented.

But what about the general robustness of the system behavior which is not scenario-oriented as in software quality and controllability?

TABLE I. OTHER ESTABLISHED STANDARDS IN THE AUTOMOTIVE INDUSTRY

Area Covered	Type of Standards
General Requirement	TS 16949 Applicable to E/E and mechanical
Testing – Assurance of hardware parts strength under certain scenarios	ISO 16750/11451/12405/ 21609
Assurance of robust protocol or interface	ISO 11898/14260/15118/ 17356

Concerns arise regarding this question has sparked the attention to develop functional safety standards for the automotive industry as guidelines to keep risk of the system at an acceptance level in any possible conditions. A new standard ISO 26262 on functional safety specifically for automotive electrical/electronic (E/E) systems has been introduced in November 2011 by the automotive industry.

This standard is evolved from IEC 61508 that fits for all industries which describes methods to classify risk and specifies requirements on how to avoid, detect and control systematic design faults, particularly in software development, random hardware faults and common cause failures, and to a lesser extend operating and maintenance errors which first published in 1998 [1].

This standard is introduced to overcome law-related issues such as liability for defects, product liability and public law. In the future, all automotive manufacturers must demonstrate all systems are aligned with ISO 26262 from the design to current development product process phases.

By having certification of ISO 26262, it will promote high confidence for customers to purchase automobiles in which prevention of accidents and the reduction of risks to be at an acceptable level. It helps to avoid errors in implementation, to prevent expensive recalls and to protect any damage on the established brand name [2].

In figure 1, there are ten parts covered by ISO 26262. It starts by describing the management of functional safety. Then, it covers from concept phase for example hazard analysis and risk assessment to the different level of product development which includes system, hardware and software.

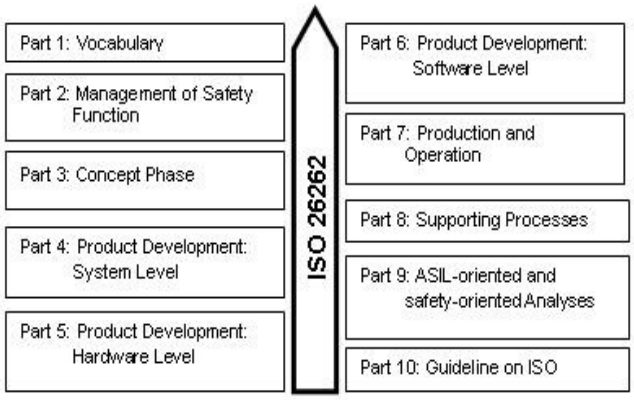

Figure 1. Parts involved in ISO 26262

Automotive Safety Integrity Level (ASIL) decomposition, analysis of dependent failures and safety analyses explain in part 9.

II. Implementation of ISO 26262

In implementing ISO 26262, all personnel and management who dealt with this system must be aware of the risks and action plans involving from systematic documentation, scheduled training and proper addressing all issues and problems to ensure everything is under control.

By implementing this standard effectively, it surely will gain an advantage for the automotive manufacturer as shown in figure 2. During the early phase, hazard analysis and risk assessment are performed based on the item defined in the system. Next, safety goals (SF) are determined and ASIL are assigned from all classified hazards.

In the development phase, technical safety requirements are established to more refine into software and hardware level. In practice, it is very challenging to change current running processes during a development.

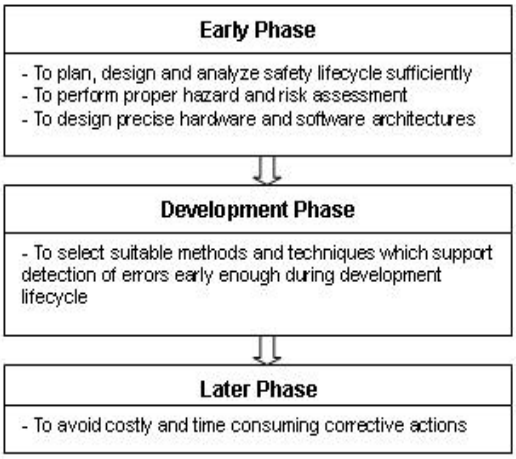

Figure 2. ISO 26262 Implementation in phases

Therefore, functional safety requirements are derived and are allocated to elements based on preliminary architectural assumption of the items [3].

Thus, pilot projects are selected for the implementation of the ISO 26262 as starting point. For new model development, the potential malfunctions of the future systems should be analyzed and be addressed right at the beginning.

All the corresponding safety requirements are prepared and completed during the development and subsequent phases.

Based on severity, probability of exposure and controllability, ASIL is classified into four different levels where level D constitutes the highest level of safety integrity and level A the lowest. Usually ASIL A-C are used. Table 2 shows some examples in classifying ASIL [4].

III. Research Trends

In table III, some of research works have been published prior to the launched of ISO 26262 based on the area within the standard which from concept phase to ASIL-oriented and safety-oriented analyses. For existing safety-related E/E systems, it will take some time for this standard to be fully integrated. The positive outcome of this implementation would gain lots of benefits to the industry in the long term.

Currently, there are software packages available in the market to assist and to support the implementation and certification of ISO 26262, such as AUTOSAR [5] and Safe IT package [6].

In the future, the introduction of telematics or accessibility to outside networks will expose the systems to various issues related to safety and security within the automobiles.

Table II. Examples of ASIL Classification

ASIL Level Random Hardware Failure Targets Value	**Systems**	**Hazard**	**Safety Goal**
A $< 10^{-6}\ h^{-1}$	Window lifter	Pinching limit	Avoid unintended closing
B $< 10^{-7}\ h^{-1}$	Low beam	Low beam failure during low light driving	Provide low beam
C $< 10^{-7}\ h^{-1}$	Electronic Stability Program (ESP)	Activation of faulty break	Avoid unintended braking
D $< 10^{-8}\ h^{-1}$	Electronic Steering Column Lock	Activation of faulty locks while driving	Avoid unintended locking

TABLE III. RESEARCH RELATED TO INTRODUCTION OF ISO 26262

Area	Title	Author & Year	Description
Concept phase Case Study	ISO 26262: Experience applying Part 3 to an in wheel electric motor	Elliams et al. Protean Electric Ltd., UK [7] Sept 2011	Discussion on the limits and strengths in implementing activities which are item definitions, process initiation, hazard and risk assessment and functional safety concept suggested in ISO 26262: Part 3
	System safety and ISO 26262 compliance for Automotive Lithium-Ion Batteries	Taylor et al. kVA, USA [8] Nov 2012	Applied hazard analysis and risk assessment on control systems of charging and discharging of Li-ion battery pack from safety goals down to the technical safety requirements.
Concept Phase FMEA	FMEA based on electric and electronic architectures of vehicles to support the safety lifecycle ISO/DIS 26262	Hillenbrand et al. Institute Information Processing Technology, FZI Informatik, Aquintos GmbH, Germany [3] 2010	Electric and electronic architecture (EEA) model and FMEA are linked together for faster and more consistent data input for safety analyses.
Concept Phase FTA	Failure calculation with priority FTA method for Functional safety of complex automotive subsystems	Takeichi et al. Tokyo University of Marine Science and Technology, Japan and TUV SUD Japan Ltd. [9] July 2011	Operation-time, proof test-timing and diagnosis-related parameters should be taken into account for reasonable estimation of hazard/failure rates of overall systems.
Concept Phase Fault Tolerance	Architectural design and reliability analysis of a fail-operational brake-by-wire system from ISO 26262 perspectives	Purnendu Sinha General Motors R&D, India [10] March 2011	A system-level-architecture for a fail-operational brake-by-wire system with fault-tolerance requirements.
Software	Formal specification and systematic Model-Driven Testing of embedded automotive systems	Sieg et al. University Erlangen-Nuremberg and Automotive Safety Technologies GmbH, Germany [11] Nov 2011	Verification and validation during development phase based on advanced software testing methods using Timed usage model based on Markov-Chain usage models.
Hardware	Capability of single hardware channel for automotive safety application according to ISO 26262	Braun et al. University of applied Sciences Regensburg, AVL Software & Functions GmbH, Germany [12] Sep 2012	Series production redundant hardware concepts like dual core microcontrollers running in lock-step-mode is used to reach ASIL D requirements.
	Automotive Hardware Development according to ISO 26262	Jeon et al. Electronic Telecommunication Research Institute, South Korea [13] Feb 2011	Calculation steps of controlling random hardware failure which includes single point metric and latent point metric are shown.
Supporting Process	Towards A safer development of Driver Assistance Systems by Applying requirements-Based Methods	Jost et al. University of Oldenburg Institute of	Application of ontology as tool chain to address the new demand in the requirements management in ISO 26262 for a safer development of driver assistance systems.

		Transportation Systems, German Aerospace Center, Germany [14] Oct 2011	
ASIL-oriented and safety-oriented analyses	The use and abuse of ASIL Decomposition in ISO 26262	D.D Ward and S.E. Crozier, MIRA Limited, UK [15] Oct 2012	Correct application of ASIL decomposition is shown especially in the complex architecture.

IV. Conclusions

Since ISO 26262 does not describe in details which methods and techniques to be applied in fulfilling the stated requirements, many studies and research can be further explored in this area.

Application of various methods and techniques ranging from hazard and risk assessment to development of system, software and hardware could significantly contribute to assist the automotive industry for implementing this new standard.

ISO 26262 provides guidance to the automotive industry to maintain a safety level that has been achieved to a higher level and also for new generation safety systems.

System faults and random hardware faults are some of the challenges in the increasing complexity and interaction of the E/E systems of rapid growing automobile's features in safety-critical markets.

References

[1] F. Rainer, “Project experience with IEC 61508 and its consequences”, Safety Science, vol. 42, no. 5, pp. 405-422, 2004.

[2] P. Kafka, “The automotive standard ISO 26262, the innovative driver for enhanced safety assessment”, Technology for Motor Cars, Procedia Engineering, vol. 45, pp. 2-10, 2012.

[3] M. Hillenbrand, M. Heinz, N. Adler, J. Matheis, and K.D. Muller-Glaser, "Failure mode and effect analysis based on electric and electronic architectures of vehicles to support the safety lifecycle ISO/DIS 26262”, In Proceedings of Rapid System Prototyping (RSP), 2010 21st IEEE International Symposium , pp.1-7, 2010.

[4] J. Schwarz, “Functional safety and automotive software – introduction ISO 26262 Daimler, In Proceedings of 10th Workshop of Critical Software System, pp. 27-28, 2012.

[5] AUTOSAR, available at: http://www.eetimes.com/design/automotive-design/4213069/AUTOSAR-architecture-expands-safety-and-security-applications/

[6] SAFE IT, available at: http://www.ti.com/ww/en/functional_safety/safeti/SafeTI-61508.html?DCMP=safeti&HQS=hercules-safeti-pr-lp1

[7] M. Ellims, H. Monkhouse and A. Lyon, "ISO 26262: Experience applying part 3 to an in-wheel electric motor," In Proceedings of System Safety 6th IET International Conference, pp. 1-8, 20-22, 2011.

[8] W. Taylor, G. Krithivasan and J.J. Nelson, "System safety and ISO 26262 compliance for automotive lithium-ion batteries," In Proceedings of Product Compliance Engineering (ISPCE) IEEE pp.1,6, 2012.

[9] M. Takeichi, Y. Sato, K. Suyama and T. Kawahara, “Failure rate calculation with priority FTA method for functional safety of complex automotive subsystems”, In Proceedings of Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), pp. 55-58, 2011.

[10] P. Sinha, “Architectural design and reliability analysis of a fail-operational brake-by-wire system from ISO 26262 perspectives”, Reliability Engineering & System Safety, vol. 96, no. 10, pp. 1349-1359, 2011.

[11] S. Siegl, K.S. Hielscher, R. German, and C. Berger, “Formal specification and systematic model-driven testing of embedded automotive systems”, In Proceedings of Design, Automation & Test in Europe Conference & Exhibition (DATE), pp. 1-6, 2011.

[12] J. Braun, C. Miedl, D. Geyer, J. Mottok and M. Minas, "Capability of single hardware channel for automotive safety applications according to ISO 26262," In Proceedings of Applied Electronics (AE), International Conference, pp. 41, 46, 5-7 Sept. 2012.

[13] S.H. Jeon, J.H. Cho, Y. Jung, S. Park and T.M. Han, "Automotive hardware development according to ISO 26262", In Proceedings of Advanced Communication Technology (ICACT), 13th International Conference, pp. 588-592, 2011.

[14] H. Jost, S. Kohler and F. Koster, "Towards a safer development of driver assistance systems by applying requirements-based methods," In Proceedings of Intelligent Transportation Systems (ITSC), 14th International IEEE Conference, pp. 1144, 1149, 2011.

[15] D.D. Ward and S.E. Crozier, "The uses and abuses of ASIL decomposition in ISO 26262," In Proceedings System Safety, incorporating the Cyber Security Conference, 7th IET International Conference, pp. 1,6, 15-18 Oct. 2012.