International Journal of Reliability and Applications
Vol. 15, No. 2, pp. 151-161, 2014

ISO 26262 automotive functional safety: issues and challenges

Azianti Ismail

Faculty of Mechanical Engineering, Universiti Teknologi MARA, Malaysia

Liu Qiang*

Department of Industrial and Management Engineering, Daegu University, South Korea

Received 29 November 2014; revised 10 December 2014; accepted 12 December 2014

Abstract. Recently, the automotive industry has been introduced to ISO 26262 in November 2011 to address the necessity of safety risk from sensor to actuator by providing guidance in the form of requirements and processes. The malfunctioning behaviour of these systems could have significant impact on the safety of humans and/or the environment. 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. In this paper, the international trends on pre and post introduction of ISO 26262 through publications will be analyzed as well as to take a glimpse in the activities for implementing this standard by the automotive manufacturers. The issues and challenges which have been occurring from implementing this standard also will be highlighted.

Key Words: *Automotive, functional safety, ISO 26262, issues, publications*

1. 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 critical functions systems in road vehicle nowadays which consist of larger system architecture with complex interaction and interface. What about the general robustness of

*Corresponding Author.
E-mail address: *liuqiang@outlook.kr*

the system behaviour which is not a scenario-oriented as in software quality and controllability? 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. 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.

Table 1. Other established standards in the automotive industry

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

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 (Faller, 2004). 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 (Kafka, 2012).

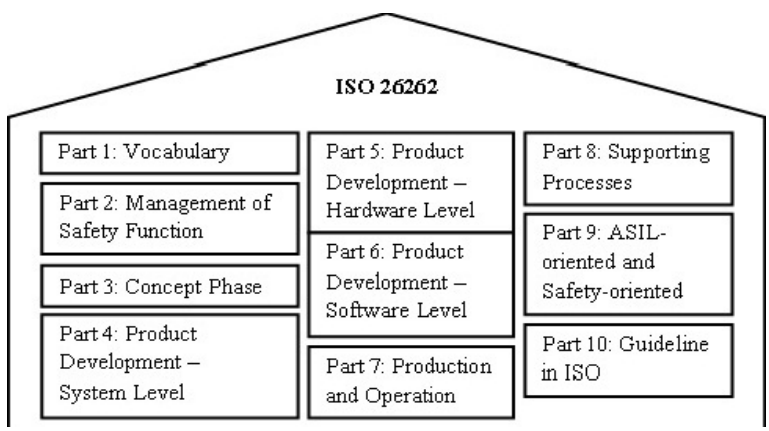

Figure 1. The parts involved in ISO 26262

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

2. IMPLEMENTATION OF ISO 26262

During the implementation of 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.

Therefore, functional safety requirements are derived and are allocated to elements based on preliminary architectural assumption of the items (Hillenbrand, Heinz, Adler, Matheis and Muller-Glaser, 2010). 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 to C is used. Table 2 shows some examples in classifying ASIL (Schwarz & Buechl, 2009).

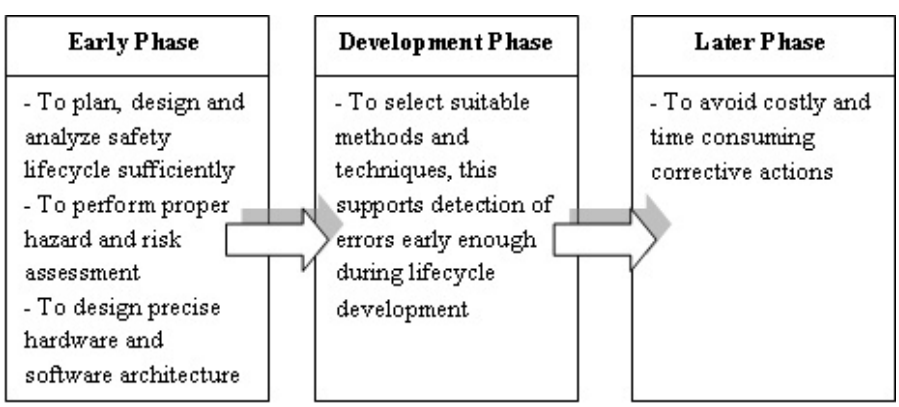

Figure 2. ISO 26262 Implementation in phases

Table 2. Examples of ASIL Classification

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

3. PUBLICATION RELATED TO ISO 26262

Currently, this study has reviewed the total of 25 papers published in academic journals, conference proceedings and magazine which are related to ISO 26262. All the publications are categorized based on parts mentioned in the standard which ranging from part 3 to part 9. Some of the publications just mentioned generally regarding ISO 26262 introduction or implementation. Specified automotive systems category represents the case study that involved in the implementation of ISO 26262. From Figure 3, part 6 represents software level development in the standard has the highest number of publications. This is due the fact that software is the most critical part in functional safety. Researchers from Institute for Information Processing Technology (KIT) in Germany have published four papers on software architecture modeling related to part 6 (Hillenbrand et al., 2010; Hillenbrand, Heinz and Muller-Glaser, 2010; Hillenbrand, Heinz, Adler and Muller-Glaser, 2012; Hillenbrand, Heinz, Adler, Matheis, 2012). From University Erlangen-Nuremberg, the researchers have developed Timed Usage Models to enhance the development methods in the development and integration phase at a German OEM (Siegl, Hielscher and German, 2010; Siegl, Hielscher, German and Berger, 2011).

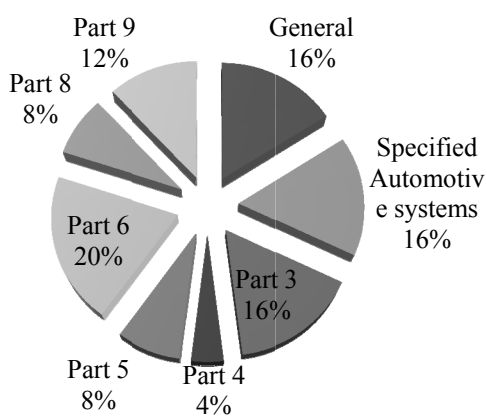

Figure 3. Percentage of publications in ISO 26262

Specified automotive systems such as lane assistance (Dittel and Aryus, 2010), air suspension (Habli, Ibarra, Rivet and Kelly, 2010), dual clutch transmission (Zhang, Li and Qin, 2010), fuel level estimation (Dardar, Gallina, Johnsen, Lundqvist and Nyberg, 2012), electric vehicle braking (Sinha, 2011), active brake assist (Ridderhof, Gross and Doerr, 2007) and electric vehicle Li-Ion battery pack (Taylor, Krithivasan and Nelson, 2012) have been published based on sharing experiences of implementation and highlighting the challenges they have encountered. European countries that are involved in Work Groups for drafting ISO 26262 such as Germany, France, Austria, Italy, and Sweden have contributed in the publications more compare to other countries. Framework proposal on implementation, application as in case study and suggestion on tools or techniques are some of the preferred topics in the publications. The draft of the ISO 26262 started in 2009, since then the number of publications has increased especially in the year of 2011 in which the introduction of the full standard. The automotive industry was aware of the emerging of the standard earlier before its introduction in November, 2011. Some of the publications prior to 2011 are based on the draft in which has been released to the automotive industry. Some of the publications have voiced out their concerns on the issues regarding the implementation of this standard such as ambiguity in the ASIL classification (Coyle, Hinchey, Nuseibeh and Fiadeiro, 2010; Ridderhof et al., 2007; Ward and Crozier, 2012), compatibility with current systems (Hamann, Sauler, Kriso, Grote and Mossinger, 2009; Ridderhor et al., 2007), telematics (Hoppe, Kiltz, Lang and Dittmann, 2007; Trapp, Schneider and Liggesmeyer, 2013), electromagnetic disturbance (Alexandersson, 2009) and electrical safety in low carbon vehicles (Ward, 2011).

4. RESEARCH TRENDS

In table 3, 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 and Safe IT package.

5. DISCUSSIONS

Some of the issues and challenges such as ASIL classification, integration with current systems, telematics, electromagnetic disturbance and electrical safety in low carbon vehicles have been highlighted in the publications that are important which may lead to finding more gaps in the standard.

5.1. ASIL classification

The standard does not prescribe any specific tools and techniques to fulfill the stated requirements (Jeon, Cho, Jung, Park and Han, 2011). Palin et al. (2011) have agreed that it

is more toward guidelines and every researcher has his own way of interpreting or understanding the standard. Thus, different analysis tools or techniques may lead to different ASIL even when using the same set of data. Ridderhof et al.(2007) have discussed that ambiguity in calculation may exist. Therefore, more research can be applied in suggesting suitable tools and techniques through case studies in performing ASIL classification. Improvement of the current tools and techniques to be more flexible and compatible with current practices also is needed.

5.2. Integration with current existing systems

Assimilation of current practices with the new standard is a challenge for the automotive industry in reducing redundancy, time and resources. Born et al. have recommended a transition from a document-centric approach to safety analysis and associated documentation to a model-based approach after gaining experience with the application of ISO 26262 in a pilot project at a German car manufacturer (Born, Favaro and Kath, 2010). Hamann et al. (2009) have shared experiences of implementation of ISO 26262 at Robert Bosch GmbH in which some of the requirements are overlapping with ISO/TS 16949, Automotive SPICE and CMM1. As suggested by Schwarz and Buechl (2009), ISO 26262 implementation should start with pilot projects and right attitudes.

5.3. Introduction of telematics, electromagnetic disturbance and low Carbon vehicle

Telematics or accessibility in which involve with vehicle to vehicle and vehicle to infrastructure communication such as car 2 car communication, plug and play, may induce security vulnerabilities and endangering the automotive critical functions systems. Hoppe et al. (2007) have described how Trojan horses virus attack via the internet can reduce the functionality of electronic throttle control systems. Thus, higher and tighter security is definitely required to enhance the security against intended attacks. 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. Trapp, Schneider and Liggesmeyer (2013) have suggested that together with ISO 15408, the designed-in security and safety countermeasures should b established such as quantification schemes and methods to recognize the weaknesses regarding security risks and hazards in the electronic systems. ISO 15408 is a standard for the assessment and evaluation of security objectives of software availability.

Electromagnetic disturbance imposed surroundings such as in radar system or high power transmission is not considered in the standard (Alexandersson, 2009). Since most automobiles have been transformed into embedded computing systems with about hundred electronic control units (ECUs) and several networks running complex distributed applications, robust design is required to ensure the functionality of the systems.

For low carbon emission vehicle such as electric and hybrid, electrical safety is very crucial whether there is a leakage of hazardous voltage onto the vehicle chassis and shuts down the high voltage system. Correct functionality of an electronic system is compulsory to achieve the required level of electrical safety in which is not addressed in the standard (Ward, 2011). Separate automotive functional safety is required for low carbon emission vehicle.

Table 3. Early researches related to introduction of ISO 26262

Area	Title	Description
Concept phase Case Study	ISO 26262: Experience applying Part 3 to an in wheel electric motor (Elliams et al., 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., 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., 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., 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 (Sinha, 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., 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., 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., 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., 2011)	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.
ASIL-oriented and safety-oriented analyses	The use and abuse of ASIL Decomposition in ISO 26262 (Ward and Crozier, 2012)	Correct application of ASIL decomposition is shown especially in the complex architecture.

6. CONCLUSIONS

In the long term, the positive result of this implementation would achieve many benefits to the automotive industry. Even though, it will take some time for this standard to be fully integrated for existing safety-related E/E systems, the benefits from this implementation will raise the competitiveness in the global automotive market. 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 automotive safety assessment. 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. By knowing that the standard is on its way to being adopted by the automotive industry, there are many challenges and opportunities for research supporting the processes and methods. 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. It is said that this standard is expected to become the industry standard in 2018 for the European automotive electronic systems.

REFERENCES

Alexandersson, S. (2009). Functional Safety and EMC for the Automotive Industry, *IEEE 2008 International Symposium on Electromegnetic Compatibility*, 1–6.

Braun, J., Miedl, C., Geyer, D., Mottok, J. and Minas, M. CCapability of Single Hardware Channel for Automotive Safety Applications according to ISO 26262, *In Proceedings of Applied Electronics (AE), International Conference*, 41-46.

Born, M., Favaro, J., and Kath, O. (2010). Application of ISO DIS 26262 in practice, *In Proceedings of the 1st Workshop on Critical Automotive applications Robustness & Safety*, 3-6.

Coyle, L., Hinchey, M., Nuseibeh, B., and Fiadeiro, J. L. (2010). Guest Editors' Introduction: Evolving Critical Systems, *Computer*, **43**, 28–33.

Dardar, R., Gallina, B., Johnsen, A., Lundqvist, K., and Nyberg, M. (2012). Industrial Experiences of Building a Safety Case in Compliance with ISO 26262, *In 2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops*, 349–354.

Dittel, T., and Aryus, H.J. (2010). *How to "Survive" a Safety Case according to ISO 26262*, In E. Schoitsch (Ed.), Computer Safety, Reliability, and Security, Heidelberg: Springer Berlin Heidelberg, 6351, 97–111.

Ellims, M., Monkhouse, H. and Lyon, A. (2011) ISO 26262: Experience Applying Part 3 to an in-wheel Electric Motor, *In Proceedings of System Safety 6th IET International Conference*, 1-8.

Faller, R. (2004). Project experience with IEC 61508 and its consequences, *Safety Science*, **42**, 405–422.

Habli, I., Ibarra, I., Rivett, R. S., and Kelly, T. (2010). Model-Based Assurance for Justifying Automotive Functional Safety, *In SAE 2010 World Congress & Exhibition*, 2010–01–0209.

Hamann, R., Sauler, J., Kriso, S., Grote, W., and Mössinger, J. (2009). Application of ISO 26262 in Distributed Development ISO 26262 in Reality, *In SAE World Congress & Exhibition*, 2009–01–0758.

Hillenbrand, M., Heinz, M., Adler, N., Matheis, J., and Muller-Glaser, K. D. (2010). Failure Mode and Effect Analysis based on Electric and Electronic Architectures of Vehicles to Support the Safety Lifecycle ISO/DIS 26262, *In IEEE International Symposium on Rapid System Prototyping (RSP)*, 1–7.

Hillenbrand, M., Heinz, M., Adler, N., Müller-Glaser, K., Matheis, J., and Reichmann, C. (2010). ISO/DIS 26262 in the Context of Electric and Electronic Architecture Modeling, In H. Giese (Ed.), Architecting Critical Systems, Springer Berlin Heidelberg, 6150, 179–192.

Hillenbrand, M., Heinz, M., Matheis, J.,and Müller-Glaser, K. D. (2012). Development of Electric/Electronic Architectures for Safety-related Vehicle Functions, *Software: Practice and Experience*, **42**, 817–851.

Hillenbrand, M., Heinz, M., Muller-Glaser, K. D., Adler, N., Matheis, J., and Reichmann, C. (2010). An Approach for Rapidly Adapting the Demands of ISO/DIS 26262 to Electric/electronic Architecture modeling*, IEEE International Symposium on Rapid System Protyping*, 1–7.

Hoppe, T., Kiltz, S., Lang, A., and Dittmann, J. (2007). Exemplary Automotive Attack Scenarios: Trojan horses for Electronic Throttle Control System (ETC) and replay attacks on the power window system*, VDI BERICHTE*, 165.

Jeon, SH., Cho, J.-H., Jung, Y., Park, S., & Han, T.M. (2011). Automotive Hardware Development according to ISO 26262, *In 13th International Conference on Advanced Communication Technology*, 588–592.

Jost, H., Kohler, S. and Koster, F. Towards a Safer Development of Driver Assistance Systems by Applying Requirements-based methods, *In Proceedings of Intelligent Transportation Systems (ITSC)*, 1144-1149.

Kafka, P. (2012). The Automotive Standard ISO 26262, the Innovative Driver for Enhanced Safety Assessment & Technology for Motor Cars, *Procedia Engineering*, **45**, 2–10.

Palin, R., Ward, D., Habli, I., and Rivett, R. (2011). ISO 26262 Safety Cases: Compliance and Assurance, *In 6th IET International Conference on System Safety*, 12-15.

Ridderhof, W., Gross, H. G., and Doerr, H. (2007). Establishing Evidence for Safety Cases in Automotive Systems–A case study, In F. Saglietti & N. Oster (Eds.), Computer Safety, Reliability, and Security, Springer Berlin Heidelberg, 4680, 1–13.

Schwarz, J., and Buechl, J. (2009). Preparing the Future for Functional Safety of Automotive E/E-Systems, *In 21st (ESV) International Technical Conference on the Enhanced Safety of Vehicles*, 1–3.

Siegl, S., Hielscher, K., and German, R. (2010). Model Based Requirements Analysis and Testing of Automotive Systems with Timed Usage Models, *In IEEE International Requirements Engineering Conference*, 345–350.

Siegl, S., Hielscher, K., German, R., and Berger, C. (2011). Formal Specification and Systematic Model-Driven Testing of Embedded Automotive Systems, *Test*, 1–6.

Sinha, P. (2011). Architectural Design and Reliability Analysis of a Fail-operational Brake-by-wire System from ISO 26262 Perspectives, *Reliability Engineering & System Safety*, **96**, 1349–1359.

Takeichi, M., Sato, Y., Suyama, K., and Kawahara, T. (2011) 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)*, 55-58.

Taylor, W., Krithivasan, G., and Nelson, J. J. (2012). System Safety and ISO 26262 Compliance for Automotive Lithium-Ion Batteries, *IEEE Symposium on Product Compliance Engineering (ISPCE)*, 1–6.

Trapp, M., Schneider, D., and Liggesmeyer, P. (2013). A Safety Roadmap to Cyber-physical Systems*, In Perspectives on the Future of Software Engineering*, 81-94.

Ward, D. (2011). System Safety in Hybrid and Electric vehicles, *In Proceedings of the Australian System Safety Conference*, 79–84.

Ward, D., and Crozier, S. (2012). The Uses and Abuses of ASIL Decomposition in ISO 26262, *In System Safety, incorporating the Cyber Security Conference*, 1–6.

Zhang, H., Li, W., and Qin, J. (2010). Model-based Functional Safety Analysis Method for Automotive Embedded System Application, *International Conference on Intelligent Control and Information Processing (ICICIP)*, 761–765.