Proceedings of the Asia Pacific Industrial Engineering & Management Systems Conference 2012
V. Kachitvichyanukul, H.T. Luong, and R. Pitakaso Eds.

Incorporating ISO 26262 Development Process in DFSS

Min Koo Lee
Department of Information and Statistics,
Chungnam National University, Daejeon 305-764, Korea
Tel: +82 42 821 5409, Email: sixsigma@cnu.ac.kr

Sung-Hoon Hong
Department of Industrial & Information Systems Engineering,
Chonbuk National University, Chonju, Chonbuk 561-756, Korea
Tel: +82 63 270 2331, Email: shhong@chonbuk.ac.kr

Dong-Chun Kim
Dept. of Industrial & Information Systems Engineering,
Chonbuk National University, Korea
dongckim@jbnu.ac.kr

Hyuck Moo Kwon†
Department of Systems Management and Engineering,
Pukyong National University, Busan 608-737, Korea
Tel: +82 51 629 6480, Email: iehmkwon@pknu.ac.kr

Abstract. The automotive ECU market is rapidly growing due to the increasing demand for convenience and safety in driving environment. In a typical high-end car, the number of ECUs is increasing up to 70 and now the automobile is more an electronic product than a mechanical one. ISO 26262 provides a V model for ECU development process to secure safety against vehicle. In this article, we introduce the outline of ISO 26262 development/design process and compare it with DFSS process. And we suggest a way to incorporate the ISO 26262 in DFSS. We also provide some discussions on the suggested model.

Keywords: ECU, ISO 26262, DFSS

1. INTRODUCTION

The increasing requirements of safety and convenience in driving environment accelerates the demand for automotive ECUs(Electronic Control Units) in the semiconductor market. By 2014, the automotive ECU market is expected to grow up to $4.8 billion. (Bellotti and Mariani, 2010). Now a typical high-end car includes almost 70 ECUs with increasing trend. The increasing number of ECUs makes a vehicle a more complicated system, which carries safety issues together. Thus, safety related ECUs need to be developed and manufactured so that it can guarantee its functional safety when incorporated into a vehicle.

ISO 26262 is aiming to guarantee the functional safety by introducing safety notions at every level of automotive ECU development. It provides a V model for development process which is characterized by two main straps – develop/design and verification/validation. The development/design strap is requirement flow down, i.e. top down process and the verification/validation strap is integrating up and test, i.e. bottom up process. The core part of the product development process consists of three levels; system level, hardware level, and software level. The system level clearly specifies and allocates the requirements to the hardware and the software system, making proper adjustment between the two if necessary. The hardware and software developments are performed in parallel, keeping their interfaces in mind.

The ISO 26262 well describes the requirements, necessary works and their resulting products for each development phase. But it lacks explanation on the working steps to follow and the methodologies and tools to be used in each step. There are several suggestions which may help implement ISO 26262 requirements. Jost et al.(2010) proposed a methodology to plan and monitor the safety development process. Krammer et al.(2101) used requirements engineering for development of safety relevant

† : Corresponding Author

automotive embedded systems in the context of ISO 26262. Jost et al.(2011) and Krammer and Bourrouilh(2011) may also be referred to. The six sigma DFSS process may provide another good complement for ISO 26262 product development process. In this article, we are going to suggest an improved model of product development by incorporating ISO26262 V model and DFSS process.

2. THE ISO 26262 AND DFSS PROCESS

2.1 The ISO 26262 Product Development Process

Basically, the ISO 26262 process is composed of three phases; concept, product development, and production and operation. Figure 1 depicts the ISO 26262 process in the perspective of safety lifecycle. The usual product development and design process includes the concept and the product development phase of Figure 1. Only the first two phases are considered here as the core parts of product development process.

The final output of the concept phase is the functional safety requirements (FSRs) for an item. They are derived from the right safety goals (SGs) and the automotive safety integrity levels (ASILs), which should be supported by a sound analysis of hazard and risk assessment. The item may be either a totally new development or a modification of an existing item. In the latter situation, an impact analysis should be carefully performed and its results should be reflected in the succeeding activities.

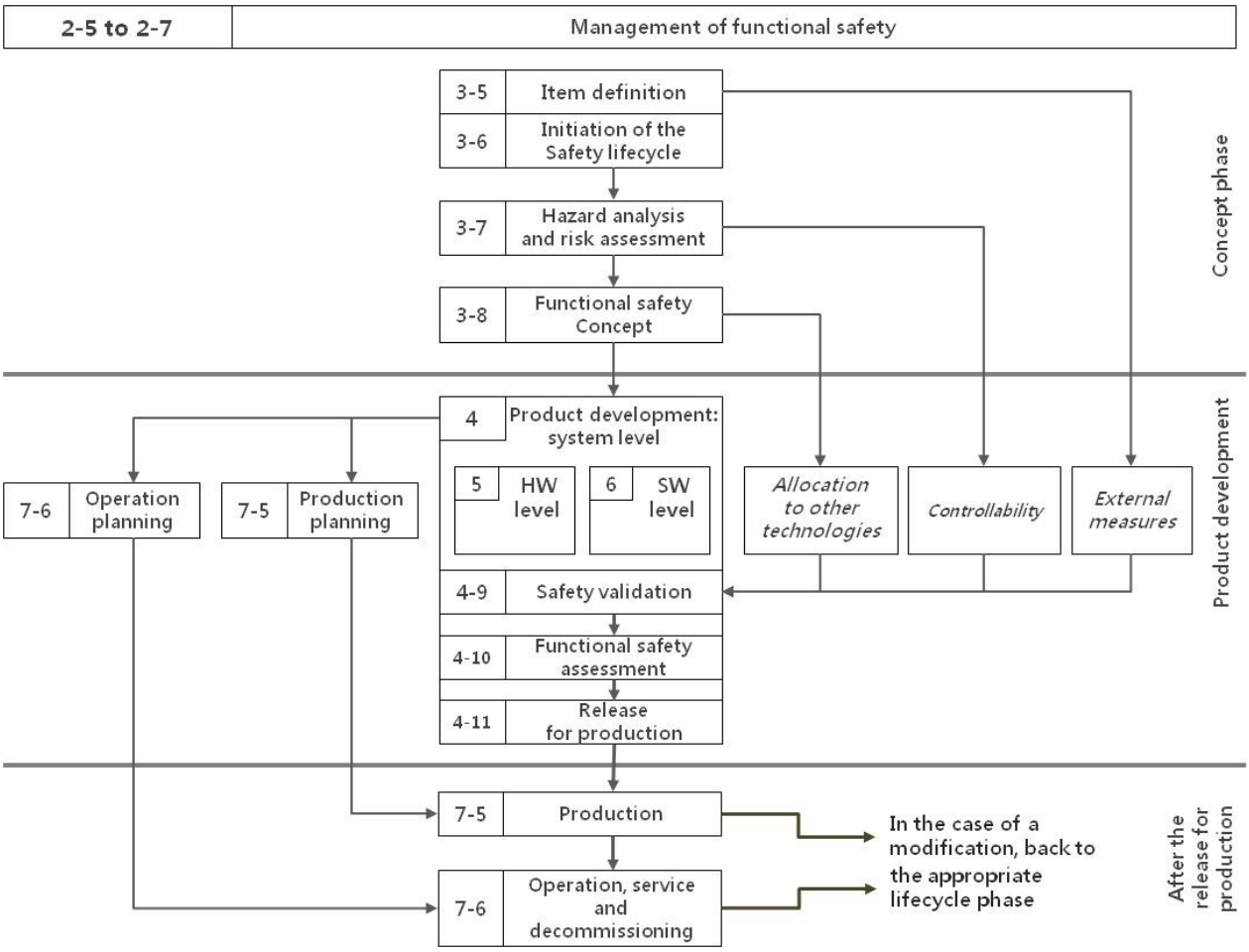

Figure 1. Safety Lifecycle of ISO 26262

During the product development at the system level, the technical safety requirements (TSRs) are defined on the basis of the FSRs. And the system architecture is established to meet the requirements. TSRs may be refined during the

establishment of system architecture and should be properly allocated to the HW and SW elements of the system. The requirements for HW-SW interface (HSI) should also be defined at the system level. During the specification of TSRs, ASIL decomposition may be applied for economic or technical purpose. After finishing the development activities at the HW and SW level, the both elements are integrated into an item to form a complete system, ensuring compliance with each safety requirement. The item again is integrated with other systems or the vehicle and tested for safety.

After TSRs are specified at the system level, the product development activities at the HW and SW levels are performed at the same time. The product development at the HW level includes the HW implementation of TSRs, the analysis of potential HW faults and their effects, and the coordination of SW development. The HW safety requirements (HSRs) are derived from the FSRs and TSRs without losing consistency. And the HSI specification specifies the HW and SW interaction, including its HW devices controlled by SW and the HW resources supporting the execution of SW. The HW architecture of the item is established and the safety mechanism is implemented so that the random HW failures are coped with effectively. The HW architectural metrics such as the single-point fault and latent fault metrics are evaluated to verify the effectiveness of the HW architecture. And then HW integration and testing is followed.

At the SW level, the SW safety requirements (SSRs) are specified on the basis of the TSRs. The SSRs considers the constraints of the HW and the impact of these constraints on the SW. The SW architectural design is developed and verified. The SW units are specified on the basis of the SW architectural design and implemented with static verification. Then SW unit testing and SW integration and testing are executed. The embedded SW is demonstrated fulfilling the SSRs.

2.2 The Six Sigma DFSS Product Development Process

DFSS(Design For Six Sigma) may be defined as a systematic methodology using tools, training, and measurements to enable the design of products, services, and processes that meet customer expectations at six sigma quality levels. DFSS optimizes the design process to achieve six sigma performance and integrates characteristics of Six Sigma at the outset of new product development with a disciplined set of tools. (Brue and Launsby, 2003)

For the step by step approach to completion of a project, there are several models available, i.e., PIDOV(Plan – Identify – Design – Optimize - Validate), DMADV(Define – Measure – Analyze – Design – Verify), IDOV(Identify – Design – Optimize - Validate), DMADOV, CDOV(Concept – Design - Optimization – Verification) and so on. (Creveling et al., 2003 and Yang, 2003) It depends on the companies and consultants which model to take. Here we describe the DMADV model briefly to compare with the ISO 26262 product development process.

In Define phase, among many potential projects, one is selected and defined in detail. The project goals and the requirements of customers are specified. The scope is clearly determined and a team is set up so that the project scope can be completely covered. The execution schedule is also planned.

In Measure phase, the customer needs and specifications are assessed. CTQs(Critical To Quality) are extracted from the customer needs. Measurement system and allowable tolerances are determined on CTQs. The baseline capabilities are evaluated and goals are established. The risks related with CTQs are also assessed. It should be noted that, in Six Sigma, the measurable CTQ is usually denoted by Y and the key information is basically provided by numerical figures.

Analyze phase includes two steps; concept design and design elements specification. For determining the design concept, many ideas are developed to achieve the performance goals imposed on the CTQs. The various preliminary concepts from the ideas are evaluated by appropriate criteria. The evaluation criteria should be agreed among the project team members in advance. After the best design concept is selected, design elements are specified to realize it. In Six Sigma, the elements or parameters that affect Ys are usually denoted by Xs.

In Design phase, the detailed design is developed. For the system representative of the selected design concept, the design elements are analyzed and flow down to the detailed design factors. This is a CTQ flow down process, where the system is diagrammed to identify the transfer functions (dependencies) between Ys and Xs at various levels of the system, such that the Xs at one level are the Ys at a lower level and the Ys at one level are the Xs at a higher level. The requirements on each X are specified so that the capability goals on the CTQ Ys can be achieved through the capability flow up process. The capability flow up is a process of determining upwardly the capabilities of Xs or Ys at one level by aggregating the capabilities of Xs at lower levels. Based on the requirements specifications on the bottom line Xs, the detailed designs are developed, evaluated, selected, and optimized.

The Verify phase is to ensure that the design meets the customer requirements using simulation, pilot test, mockup test, and trial product production. The performance goals on the CTQs are checked to be achieved. If necessary, further improvement of the design should be performed. The strategy and control plan for the manufacturing process should also be established. Documentation of the whole process is required for the future reference.

3. THE DFSS PROCESS FOR ISO 26262

3.1 The Framework of the Combined Process

Basically, the two processes are concerned with product development. ISO 26262 is more focused on What's while DFSS is more on How's. The phases of the two can be properly matched each other. The detailed requirements of ISO 26262 can be allocated to each phase of the DFSS process. The methodologies and tools of DFSS may be used in each step of the development process.

Considering the similarities and differences as well as the strengths and weaknesses, we combine the two processes into one development process as to the following rules:

i) The production and operation phase of ISO 26262 is not included in the proposed development process.
ii) The main flow of the development follows the DFSS DMADV process.
iii) Each sub phase or clause of ISO 26262 are allocated to an appropriate phase of DMADV considering the activities suitable for each phase.
iv) All the requirements of ISO 26262 should be satisfied after the proposed development process is finished.
v) Appropriate DFSS tools and methodologies may be better to be recommended for each development phase to efficiently implement ISO 26262 requirements. But detailed description is omitted to avoid too much complexities.
vi) To focus on the functional safety issue, all the activities of each phase are described in the context of ISO 26262. Even though the activities irrelevant to safety are not explained separately, they can be treated similarly.

Figure 2 shows the framework of the combined development process of DFSS and ISO 26262. There may be some activities added for executing the development as a DFSS project.

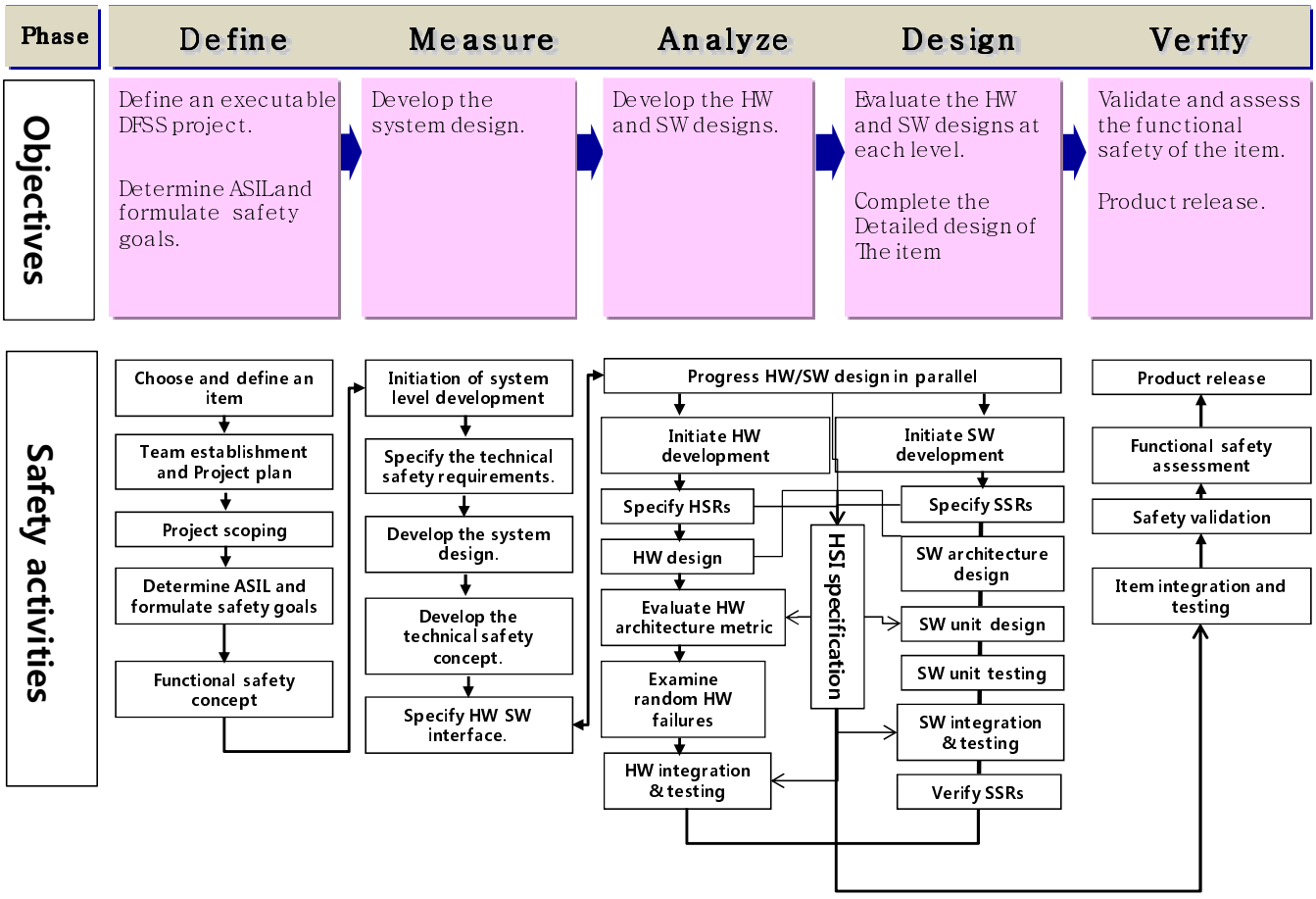

Figure 2. The Framework of DFSS Process for ISO 26262

3.2 Activities and Outputs for Each Phase

Define Phase

The basic objective of Define phase is to define an executable DFSS project in the perspective of ISO 26262. The main activities correspond to those of the concept phase of ISO 26262-3. A decision is made on which item shall be developed considering the business strategy and environment. At first, many items may be considered as promising. But, since the resources are limited, only one or a few of them can be selected for development. To make a decision, various Six Sigma tools can be used such as Pareto analysis, selection matrix, portfolio analysis, and so on. For each item selected, a description of the item should be developed with regard to its functionality, interfaces, environmental conditions, legal requirements, known hazards, and so on. The boundary of the item and its interfaces as well as assumptions concerning other items, elements, systems and components are determined. The result of these activities will provide item definition and its preliminary architecture.

Then a DFSS project is launched with appointment of the project manager, who may be the safety manager himself or may appoint another qualified person or assign the role of the safety manager among two or more persons. The project team is established with a group of competent members so that every aspect of the development activities can be covered. The team prepares the project plan and safety plan, where the latter may be included in the former as its part. On the details to be included in the safety plan, Clause 6.4.3.5 of ISO 26262-2 can be referred.

Next, the team must determine whether the item under development is a new one or just a modification of an existing item. In the latter case, impact of the modification should be analyzed and the safety life cycle is tailored accordingly. See Clause 6.4.2 of ISO 26262-3. After tailoring, i.e. omitting or performing in a different manner, the safety related activities, the set of all the necessary activities with regard to the item development (the project scope) can be determined.

Next, H&R(Hazard analysis and risk assessment) is performed to identify and categorize the hazards and to formulate the SGs. The hazards can be identified using such techniques as brainstorming, checklist, quality history, FMEA, and field studies. For classifying the hazardous events, see Clause 7.4.3 of ISO 26262-3. SGs and their assigned ASIL(Automotive Safety Integrity Level) are determined by a systematic evaluation of hazardous events, considering their severity, probability of exposure, and controllability.

As the final step of Define phase, the functional safety concept is specified. That is, the FSRs are derived from the SGs and allocated to the preliminary architectural elements of the item or to external measures. The output of Define phase should includes:

- Organization-specific rules and processes for functional safety
- Evidence of competence
- Evidence of quality management
- Item definition
- Preliminary architecture of the item
- Impact analysis
- Project plan
- Safety plan
- Safety case
- Functional safety assessment plan
- Confirmation measure reports
- H&R
- SGs
- Verification review report of H&R and SGs
- Functional safety concept
- Verification report of the functional safety concept

Measure Phase

In Measure phase, all the activities of the product development phase at the system level of ISO 26262-4 are performed. The objective is to develop the system design for the item. It begins with determining and planning the activities during the individual sub-phases, including functional safety activities and necessary supporting processes.

Considering the functional safety concept and the preliminary architectural assumptions, the TSRs are specified. The TSRs are technical requirements to implement the functional safety concept. They are specified by detailing the item level FSRs into the system level technical requirements, keeping in mind the system properties; the external interfaces, the environmental conditions or functional constraints, and the system configuration requirements. The TSRs should specify how the system shall respond to stimuli that affect the achievement of the SGs. ASIL decomposition may be applied during the specification of TSRs.

During the system design, the system architecture is established. The system design should be based on the functional concept, the preliminary architectural assumptions, and the TSRs. The technical safety concept is developed by allocating TSRs to HW and SW. The requirements arising from the system architecture are added, including the HSI. The HSI should specify the HW and SW interactions and be consistent with the technical safety concept. The output of Measure phase should includes:

- Refined project plan
- Refined safety plan
- Item integration and testing plan
- Validation plan
- Refined functional safety assessment plan
- TSRs specifications
- System verification report

- Refined validation plan
- Technical safety concept
- System design specification
- HIS specification
- Specification of requirements for production, operation, service and decommissioning
- Refined system verification report
- Safety analysis reports

Analyze Phase

In Analyze phase, the HW and SW developments are performed in parallel. It begins with determine and plan the activities during the individual sub-phases of HW and SW developments.

Next, the HW and SW safety requirements are derived from the technical safety concept and system design specification. Then HW design and SW architectural design are developed. HW design includes HW architectural design and HW detailed design. The former represents all HW components and their interaction with one another, while the latter represents the interconnections between HW parts at the level of electrical schematics. The SW architectural design represents all SW components and their interactions in a hierarchical structure, including descriptions of both static and dynamic aspects. The SW unit design may be implemented as a model or directly as a source code in accordance with the modeling or coding guidelines respectively.

ISO 26262 does not separate the unit testing activities from the HW and SW development processes. The development itself is a repeating process of refining and testing or evaluating the developed design. We classify the developing and refining activities into Analyze phase, with the evaluating or testing activities classified into Design phase. The output of Analyze phase includes:

- Refined safety plan
- SW verification plan
- SW Design and coding guidelines
- SW tool application and guidelines
- HSR and SSR specification
- HSI specification
- HSRs verification report
- SW verification report
- HW design specification
- SW architectural design specification
- HW and SW safety analysis report
- HW design verification report
- SW safety analysis report
- SW dependent failures analysis report
- SW unit design specification
- SW unit implementation
- Specification of requirements for production, operation, service and decommissioning

Design Phase

In this phase, the outputs of Analyze phase are evaluated or tested and refined. Thus, the activities of Analyze and Design phase are recursively executed until the optimal and satisfiable design is attained.

For HW design, the HW architecture metric is evaluated and random HW failures are examined. Then HW integration and testing is followed. For SW design, each SW unit is tested and integrated into a larger module which again is to be tested. After integration and testing activities are finished at the SW level, it should be demonstrated the embedded SW fulfils all the SSRs. The output of Design phase include:

- Analysis of the effectiveness of the architecture of the item
- Review report of evaluation of the effectiveness of the architecture of the item
- Analysis of SG violations due to random HW failures
- Specification of dedicated measures for HW
- Review report of evaluation of SG violations due to random HW failures
- HW integration and testing report
- Refined SW verification plan
- Refined SW verification specification
- Refined SW verification report
- SW Configuration data specification
- SW Calibration data specification
- SW Configuration data
- SW Calibration data
- SW Verification specification
- SW Verification report

Verify Phase

In Verify phase, four activities are performed; item integration and testing, safety validation, functional safety assessment, and product release.

The item integration and testing is executed by three steps; i) the HW and SW of each element are integrated and tested, ii) the elements are integrated into a complete system to make the item and tested, and iii) the item is integrated with other systems within a vehicle and with the vehicle itself and tested. This process is to test compliance with each safety requirement and to verify that the design covering the safety requirements are correctly implemented by the entire item.

Safety validation provides evidence of compliance with the SGs and appropriateness of the functional safety concepts for the functional safety of the item. It also provides evidence that the SGs are correct, complete and fully achieved at the vehicle level.

The functional safety achieved by the item is assessed and the resulting report is provided. The assessment is based on the safety case, safety plan, confirmation review reports, audit report if available, and functional safety assessment plan.

At the completion of the item development, the release for production criteria is specified. The release for production confirms that the item complies with the FSRs at the vehicle level.

The output of Verify phase include

- Item integration and testing plan
- Integration testing specification
- Integration testing report
- Validation plan
- Validation report
- Functional safety assessment report
- Release for production report

4. DISCUSSIONS

We suggested a model of product development process integrating the ISO 26262 safety life cycle into the six sigma DFSS process. The prime objective is to meet all the requirements of ISO 26262 through a more systematic and comprehensive process of DFSS. There can be many other requirements for an item to be developed, which are directly connected to its intended functions but not related to its functional safety. Though the requirements are focused on functional safety, the non safety related requirements may be treated similarly during the development process.

This is only a trial model for integration of ISO 26262 and DFSS, needing further refinements. Or a wholly different approach may be suggested in the future. One key objective of this paper is to provide a more systematic, comprehensive and easy-to-use model for product development in compliance with the ISO 26262 requirements. Since ISO 26262 demands a very tough and complicated structure of requirements, its implementation in the industrial practices is quite difficult. We hope our model can help mitigate such difficulties or barriers. For a better integrated model of product development, a lot of efforts for further refinements are needed to complement its shortages.

Besides, there are many tools and methodologies to be provided or developed for performing many activities required by ISO 26262. How to perform impact analysis and tailoring in case of modification? How to perform ASIL decomposition? How to prepare the safety case systematically? These How's are some examples waiting for answers. The framework of the development process with only What's may not provide much help to those attempting to implement ISO 26262 requirements. Further studies are needed to develop a whole and structured set of methodologies and tools that ensures complete satisfaction of ISO 26262 requirements.

ACKNOWLEDGMENT

This work was supported by the Quality Innovation and Infrastructure Development program through the Korea Institute for Advancement of Technology funded by the Ministry of Knowledge Economy, Republic of Korea

REFERENCES

Bellotti, M. and Mariani, R., "How future automotive functional safety requirements will impact microprocessors design," *Microelectronics Reliability*, 50, 1320 – 1326, 2010.

Brue, G. and Launsby, R. G., *Design for Six Sigma*, McGraw-Hill, 2003.

Creveling, C. M., Slutsky, J. L., and Antis, Jr., D., *Design for Six Sigma in technology and product development,* Pearson Education, Ltd., 2003.

ISO 26262 Road vehicles – Functional Safety, 1st ed, 2011-11-15.

Jost, H., Hahn, A., Hausler, S., Köhler, S., Gačnik, J., Köster, F., and Lemmer, K., "Supporting Qualification: Safety Standard Compliant Process Planning and Monitoring," IEEE Symposium on Product Compliance Engineering (ISPCE), 1-6, 2010.

Jost, H., Kohler, S., and Koster, F., "Towards a Safer Development of Driver Assistance Systems by Applying Requirements-Based Methods," 14th International IEEE Conference on Intelligent Transportation Systems (ITSC), 1144-1149, 2011

Krammer, M., Armengaud, E., and Bourrouilh, Q., "Method Library Framework for Safety Standard Compliant Process Tailoring," 37th EUROMICRO Conference on Software Engineering and Advanced Applications (SEAA), 302-305, 2011.

Krammer, M., Marko, N., Armengaud, E., Geyer, D. and Griessnig, G., "Improving Methods and Processes for the Development of Safety-Critical Automotive Embedded Systems," IEEE Conference on Emerging Technologies and Factory Automation(ETFA), 1-4, 2010.

Yang, K., *Design for Six Sigma: a roadmap for product development,* Mc Graw Hill, 2003.

AUTHOR BIOGRAPHIES

Min Koo Lee is a professor in Department of Information and Statistics, Faculty of Chungnam National University, Korea. He received a Doctoral Degree from the Department of Industrial Engineering at KAIST, Korea in 1993. His teaching and research interests include six sigma business strategy and statistical quality control. His email address is sixsigma@cnu.ac.kr

Sung Hoon Hong is a professor in Department of Industrial and Information Systems Engineering, Faculty at Chonbuk National University, Korea. He received a Doctoral Degree from the Department of Industrial Engineering at KAIST, Korea in 1991. His teaching and research interests include six sigma business strategy and statistical quality control. His email address is shhong@chonbuk.ac.kr

Dong Chun Kim is an adjunct professor of Department of Industrial and Information Systems Engineering at Chonbuk National University, Korea. He received a Doctoral Degree from the school of engineering and applied science (SEAS) at George Washington University, U.S.A in 1996. His research interests include six sigma business strategy and green design methodology. His email address is dongckim@chonbuk.ac.kr

Hyuck Moo Kwon is a Professor of Department of Systems Management and Engineering at Pukyong National University. He received his M. S. and Ph.D. degrees in Industrial Engineering from KAIST. His research interests include quality engineering, six sigma business strategy and statistical quality control. His email address is iehmkwon@pknu.ac.kr