# A Study on Situation Analysis for ASIL Determination

Hyeon Ae Jang and Hyuck Moo Kwon
Department of Systems Management and Engineering, Pukyong National University, Busan, Korea
Email: {ie-jha, iehmkwon}@pknu.ac.kr

Sung-Hoon Hong
Department of Industrial & Information Systems Engineering, Chonbuk National University, Jeonju, Korea
Email: shhong@chonbuk.ac.kr

Min Koo Lee
Department of Information and Statistics, Chungnam National University, Deajeon, Korea
Email: sixsigma@cnu.ac.kr

***Abstract*—For developing a safety-related E/E system in compliance with ISO 26262, it is very important to determine a right ASIL for each hazardous event with a proper safety goal. ASIL depends on the three properties of the hazardous event, i.e. severity of harm from the resultant accident, exposure to the relevant operational situation, and controllability to avoid the relevant risks. Once the right classes are given for these three properties, ASIL can be clearly determined without any inconsistency among all the people concerned. But ISO 26262 does not provide specific methodologies or processes for clear classification of the three properties. Instead, it only provides a rough guideline with a simplified set of example tables. This study tries to present a refined procedure of ASIL determination. The modified approach provides a more systematic and specific method to get a more objective result. We scrutinize the current methodology first and develop a refined modification. We also provide an applicative illustration based on the example given in the standard.**

***Index Terms*—ISO26262, automotive safety integrity level (ASIL), hazard analysis and risk assessment (H&R), operational situation**

## I. Introduction

In the automotive industries there is an increasing trend of adopting ECUs (Electronic Control Units) into the vehicles for satisfying safety and convenience requirements of the market. Since the increasing the number of ECUs makes a vehicle more complicated system, the safety related ECUs need to guarantee its functional safety to avoid unreasonable risk due to their malfunctioning behavior.

ISO 26262 is the most recently published international standard for functional safety of E/E (Electrical and/or Electronic) systems. Although it is more refined than previous functional safety related standards like IEC 61508, it still containing vague and unclear contents here and there. As Ellims and Monkhouse [1] pointed out, for example, instead of providing a process or methodology for determining ASIL (Automotive Safety Integrity Level), it presents only a simplified set of example tables.

Since ASIL determination is the very first part of system development, it affects following safety activities greatly and is a very important part of the safety life cycle. Basically ASIL is determined as a result of H&R (Hazard Analysis and Risk Assessment) together with safety goal. Considering the importance of ASIL determination, there are too few studies on this subject. Ellims and Monkhouse [1] examined some issues they encountered during the development of an in-wheel electronic motor and argued that perceived emphasis on ASIL ratings is misplaced and potentially counterproductive. Jesty *et al*. [2] presented a generic approach to hazard analysis which is similar to ISO 26262. But there are no works which direct a clear and specific guidance to ASIL determination. This is may be partly because there can be so many possible combinations of environmental and driving elements including the road and weather conditions, yielding a huge number of potential situations.

In this study, we try to go a step further by scrutinizing the possible driving situation and classifying it into a set of categories based on some reasonable criteria. In Section 2, we review the process how the accident occurs and the current approach to ASIL determination with its limitations. In Section 3, we present a more specific way of situation analysis and ASIL determination. Section 4 provides an illustrative example and some discussions. And section 5 gives the conclusion.

## II. Review on ASIL Determination

### A. Understanding Hazard and Hazardous Event

ASIL determination is a very important step for developing a safety related E/E systems in the standard ISO 26262. ASIL is determined as a result of H&R based on the item definition. H&R is performed in the order of

Manuscript received January 28, 2014; revised July 9, 2014.

situation analysis, hazard identification, classification of hazardous events, and determination of ASIL and safety goals. Given the hazardous events are properly and correctly classified, ASIL can be easily determined by the table provided in the standard without leaving any ambiguities. But the standard does not provide any specific methodology or process for classifying the hazardous events. It only provides a simplified set of example tables. Thus, there still remain many confusing and vague factors for right classification of the hazardous events including the terminology. For example, in ISO 26262-1 [3], hazard is defined as potential source of harm caused by malfunctioning behavior of the item. Considering the linguistic meaning of 'source,' hazard may be naturally understood as the component fault. But Section 4.3 of ISO 26262-10[4] states "A subset of failures at the item level will be hazards if additional environmental factors permit the failure to contribute to an accident scenario." And hazardous event is defined as combination of a hazard and an operational situation by the standard. But the requirement 7.4.2.1.1 of ISO 26262-3[5] states "The operational situations and operating modes in which an item's malfunctioning behavior will result in a hazardous event shall be described, both for cases when the vehicle is correctly used and when it is incorrectly used in a foreseeable way." This implies that a hazardous event is not simply a combination of a hazard and an operational situation. It is the outcome of the combination of the two.

For correct and proper classification of each hazardous event, we must first understand hazard and hazardous event clearly. Fig. 1 depicts the process of occurrence of an accident and it facilitates our clear understanding of hazard and hazardous event. After scrutinizing the relevant descriptions in the standard carefully, hazard and hazardous event are marked into the Fig. Note that, an item failure may induce several malfunctioning behaviors.

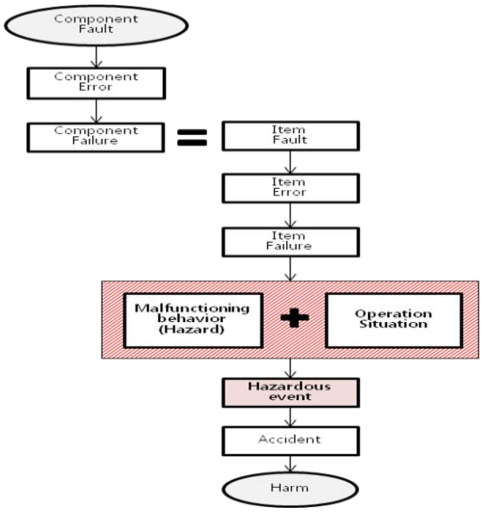


Figure 1. Hazard and hazardous event in the path of accident occurrence

For example, failure of the electrical power supply system can cause malfunctioning behaviors relevant to such functions as engine torque, power assisted steering, and forward illumination. Also, for each malfunctioning behavior, there may be several operational situations that could result in accidents causing damages to the human body. As an illustration of identifying hazards and hazardous events, an example of EPB (Electrical Parking Brake) system is excerpted from ISO 26262-10 [4] and reproduced as Fig. 2.

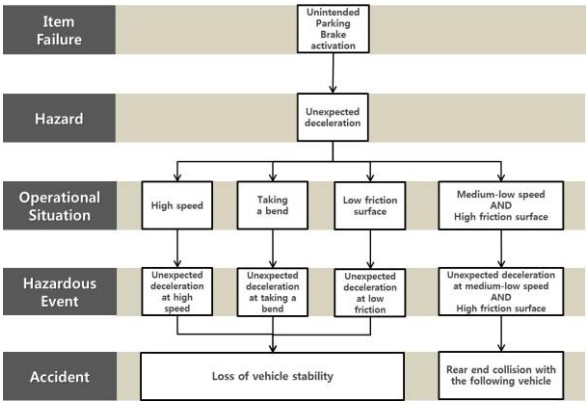


Figure 2. Example of hazards and hazardous events for EPB system

### B. Limitations of ISO 26262 ASIL determination

An initial estimate of the SIL for the vehicle was performed using both the method proposed by MISRA [6] and that specified in ISO 26262 Part3. ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of E/E systems within road vehicles. The concept of SIL(safety integrity level) was introduced during the development of IEC 61508 as a measure of the quality or dependability of a system which has a safety function – a measure of the confidence with which the system can be expected to perform that function ([7]). SIL applies solely to the E/E/PE safety-related systems and other risk reduction measures and is a measure of the likelihood of those systems/facilities satisfactorily achieving the necessary risk reduction in respect of the specified safety functions. Once the tolerable risk has been set, and the necessary risk reduction estimated, the SIL for the safety-related systems can be allocated. In IEC 61508 [8], four SIL are specified, 4 being the highest level and 1 being the lowest. ISO 26262 defines ASIL as the "necessary requirements of ISO 26262 and safety measures to apply for avoiding an unreasonable residual risk." ASIL is one of the four levels A,B,C, and D to specify the system's necessary requirements and safety measures to apply for avoiding an unreasonable residual risk, with D representing the most stringent and A the least stringent level ([3]). It is also determined by three properties of the hazardous event; severity, exposure, and controllability where

- E (exposure): state of being in an operational situation that can be hazardous if coincident with thefailure mode under analysis
- C (controllability): ability to avoid a specified harm or damage through timely reactions of the persons involved, possibly with support from external measures
- S (severity): estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation

Once the classes of these three properties are given, ASIL can be easily determined by the ASIL determination table provided in ISO 26262-3 ([5]). But the more difficult task is to determine the right classes of severity, exposure, and controllability for each hazardous event. This is because ISO 26262 does not provide any clear and specified methodology of classification for each property. It only provides a simplified set of example tables of classification for the three properties.

To begin with severity classification, one of S0, S1, S2, and S3 are allocated to a specific hazardous event with S3 the severest. The standard provides only a rough guideline for classification. For example, both S2 and S3 are concerned with life-threatening injuries, where the one is for 'survival probable' and the other is for 'survival uncertain.' This is a very ambiguous expression and we can hardly classify a specific hazardous event into 'survival probable' or 'survival uncertain' with a unanimous vote. Even when AIS (Abbreviated Injury Scale) is used, S2 (more than 10% probability of AIS 3-6) and S3 (more than 10% probability of AIS 5-6) cannot be clearly classified. In fact, S0, S1, S2, and S3 do not seem to be mutually exclusive and exhaustive events. For probability of exposure, a set of clear cut threshold values can be defined between the neighbor classes. The standard presents two criteria for classification of probability of exposure, i.e. duration and frequency. But it does not provide clear cut classification criteria. Even with a set of perfect threshold values, there still remains the problem concerning how the probability should be estimated. Finally, the controllability is also related with probability and requires an estimation of the probability that the driver will be able to retain or regain control of a vehicle if a given hazard were to occur. Since there can be a huge number of possible operational situations, correct estimation of the three elements is not an easy task to do.

As a whole, ISO 26262 ASIL determination procedure or methodology needs to be further refined. We need a more systematic and specified approach to ASIL determination.

## III. Operational Situation Analysis

### A. Operational Situation

ASIL is determined through H&R beginning with analyzing the operational situation. The operational situation is composed of four key factors that determine the traffic safety, i.e. the driver, the vehicle, the road, and the environment including weather. The driver may be the most important factor affecting safety. Any interrupting behavior of the driver like phone call, eating, nuisances from children or other passengers may cause a critical accident. The age, driving habit and competence of the driver may also affect safe driving. But when we analyze the operational situation for ASIL determination, the driver factor can be excluded from consideration because ISO 26262 addresses possible hazards caused by malfunctioning behavior of E/E safety-related systems including interaction of these systems. The essential objective of ISO 26262 is to avoid unreasonable risks and is not to avoid all kinds of risks, including those due to inappropriate driving activities. We assume that only a qualified driver will operate the vehicle.

With the vehicle factor, its designed function, maintenance state, and other characteristics may affect driving safety. But we assume it will be properly designed, manufactured, and maintained. We only analyze it from the aspect of functional safety, i.e. driving speed, external attachment, operational mode, and maneuvering state. The driving speed may be low, medium, or high. The vehicle may be sole or attached with external stuffs such as trailer or roof rack. The operational mode may be driving, parking, fuelling, and repairing. The maneuvering state may have four sub-elements; engine on/off, accelerating/decelerating, turn/lane change/lane keep, and stop/driving forward/driving backward.

As the road factor, we define six elements affecting the traffic safety; linearity, slope, layout, surface, and nearby elements. The linearity is concerning whether the road is straight or curved. The slope is concerning whether the road is plain or sloped. The road layout has many possible spots like tunnel, bridge, crosswalk, intersection, highway entrance/exit ramp and so on. The road surface may be as paved/unpaved and dry/wet/snow/ice. The nearby elements may include lost cargo, obstacle in lane of travel, traffic congestion, and etc.

The environment factor is mainly concerned with weather conditions, time of the day, season of the year, and some other external conditions.

### B. Categorizing Operational Situations

As briefly mentioned in the previous section, there can be infinitely many different operational situations. Thus, to analyze the situations effectively, we need an appropriate and systematic criterion. Since there are so many elements that determine a specific situation, they will be classified into hierarchically structured categories, considering their impacts on functional safety.

For the top level categories, we consider three factors; vehicle, road, and environment. We define four vehicle sub-factors as driving speed, external attachment, operational mode, and maneuvering state; five road sub-factors as linearity, slope, layout, coarseness, nearby elements; four environment sub-factors as surface, visibility, temperature, and momentum. The maneuvering state has again four elements; engine, velocity, direction, and movement. The nearby elements also contain three elements; obstacle, traffic, and pedestrians. Note that this classification does not adhere strictly to linguistic definition of each word. We use these terms for classifying those elements that impact driving safety from the driver's viewpoint. Thus, some words may have different meaning from the original. Each sub-factor or element has two or more states. For example, driving speed may have one of the five states; very slow, slow, normal, fast, and very fast. The possible states for each sub-factor and element are described in Table I.

A combination of the states of factors constitutes an operational situation. For example, there can be a situation where a vehicle is driving forward at the normal constant speed without any external attachment along to the straight plain paved road. The traffic flow is smooth and the road surface is clear and brightly visible since the weather is clean and not windy with temperature 15 ˚C. But such a description of a specific operational situation is too lengthy and should be reduced into a compact sentence, eliminating unnecessary sentences from the viewpoint of functional safety.

TABLE I. CATEGORY OF OPERATIONAL SITUATION

| Factor | Sub- factor | Element | State |
|---|---|---|---|
| Vehicle | Driving Speed | | Very Slow, Slow, Normal, Fast, and Very Fast |
| | External Attachment | | No external attachment, External attachment |
| | Operational Mode | | Driving, Parking, Fuelling, Repairing |
| | Maneuver | Engine | On, Off |
| | | Velocity | Accelerating, Constant, Decelerating |
| | | Direction | Lane Keeping, Lane Changing, Turning |
| | | Movement | Stop, Forward, Backward |
| Road | Linearity | | Straight, Curved |
| | Slope | | Plain, Sloped |
| | Layout | | Invisible (blocked) , Visible (unblocked) |
| | Coarseness | | Paved, Unpaved, Troublesome |
| | Nearby Elements | Obstacle | Clean, Obstacle (e.g. lost cargo dropped in lane of travel) |
| | | Traffic | Smooth flow, Congestion |
| | | Pedestrians | No, A Few, Many |
| Environment | Surface | | Clear, Water ( by rain etc), Snow/Ice |
| | Visibility | | Dark, Bright, Foggy |
| | Temperature | | Low, Medium, High |
| | Momentum | | Windy, Calm |

### C. Identifying Hazardous Events

As mentioned in the previous section, it is very tedious to define a specific operational situation considering all the elements of driving factors. For effective analysis, unnecessary elements should be excluded before specifying the situation. To obtain a properly defined set of hazardous events, the following procedure is suggested:

- Step1: Identify all the failure modes based on the item definition.
- Step2: Infer malfunctioning behaviors from each failure mode and identify hazards.
- Step3: For each hazard, select key situation sub-factors and elements that could be hazardous if they are in specific states in combination with the hazard.
- Step4: Define and list up the hazardous events.

Note that an operational situation is a combination of the states of the key situation sub-factors or elements, and one hazardous event corresponds to one operational situation. All possible combinations of the states of the key situation sub-factors and elements should first be listed up to identify all hazardous events relevant to a specific hazard.

## IV. ASIL DETERMINATION

### A. Severity Class Determination

According to ISO 26262-3[5], the potential injuries as a result of a hazard are evaluated for the driver, passengers and people around the vehicle, or to individuals in surrounding vehicles to determine the severity class for a given hazard. But the potential injuries depend on the hazard type as well as the specific situation faced by the vehicle. The potential injuries can be estimated by surmising each operational situation paired with the given hazard. And then, the severity class may be determined according to ISO 26262-3[5]. Fig. 3 illustrates this procedure.

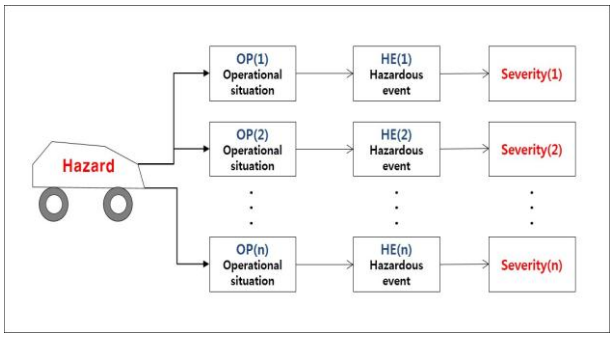


Figure 3. Determination of severity class

### B. Exposure Class Determination

To determine the exposure class for a hazardous event, we should estimate the probability that each key sub-factor or element is in a specific state. Necessary information may be obtained from relevant service agencies. We first estimate the probability for each sub-factor or element individually. Next, calculate the probabilities of specific operational situations, assuming independency among sub-factors and elements. And then, considering the correlations among sub-factors and elements, the probabilities of specific operational

situations are adjusted. Finally, the exposure class of a specific hazardous event is determined.

For illustration, suppose there are two sub-factors SF1 and SF2 that constitutes an operational situation. SF1 has two possible states 1 and 2 with probabilities 1/12 and 11/12, respectively. SF2 has three possible states 1, 2, and 3 with probabilities 6/15, 5/15, and 4/15, respectively. Assume that a hazardous event occurs if SF1 is in state 1 and SF2 is in state 3 under existence of a specific hazard. If SF1 and SF2 are mutually independent, then the occurrence probability of this hazardous event will be obtained as (1/12)(4/15) = 1/45. This will result in E3 class of exposure for this hazardous event. But if there is a strong correlation between SF1 and SF2 and the conditional probability that SF2 is in state 3 given SF1 is in state 1 is only 1/50, then the occurrence probability of this hazardous event will be obtained as (1/12)(1/50) = 1/600, which will result in E2 class of exposure.

### C. Controllability Class Determination

To determine the controllability class, we should estimate the probability that a qualified normal driver can control the vehicle's malfunctioning behavior due to the relevant failure mode. This probability will depend on the state in which each sub-factor or element is. First, estimate the probability of control when each sub-factor or element is in specific states individually. Next, calculate the probability of control for each operational situation, assuming independency among sub-factors and elements in view of controllability. And then, considering the correlations among sub-factors and elements in view of controllability, the probability of control is adjusted. Finally, the controllability class of a specific hazardous event is determined.

For illustration, suppose there are two sub-factors SF1 and SF2 that constitute an operational situation. SF1 has two possible states 1 and 2. SF2 has three possible states 1, 2, and 3. Assume that a hazardous event occurs if SF1 is in state 1 and SF2 is in state 3 under existence of a specific hazard. Assume that the driver can control the relevant malfunctioning behavior 99% of the time when SF1 is in state 1 and 95% of the time when SF2 is in state 3. When SF1 and SF2 are mutually independent in view of controllability, then the probability of control will be obtained as (0.99)(0.95) = 0.9405. This will result in C2 class of controllability for this hazardous event. But if there is a strong correlation between SF1 and SF2 in view of controllability, this result should be modified appropriately. Suppose that the driver can control the relevant malfunctioning behavior of the vehicle by 80% of the time when SF1 is in state 1 with SF2 in state 3. Then the controllability class will be C3.

## V. Conclusion

A more refined approach to ASIL determination is proposed for implementing functional safety based on ISO 26262. ASIL depends on the three properties of the hazardous event, i.e. severity of harm from the resultant accident, exposure to the relevant operational situation, and controllability to avoid the relevant risks. Once the right classes are given for these three properties, ASIL can be clearly determined without difficulty. But ISO 26262 does not provide specific methodologies or processes for clear classification of the three properties. The refined procedure provides a more objective method to determine ASIL.

Especially, a detailed method of operational situation analysis is provided. Hazardous events can be systematically identified based on the operational situation analysis relevant to a specific hazard. For each hazardous event, methodologies are presented to determine classes of the three ASIL properties of severity, exposure, and controllability. This approach is expected to be easier to use in practical applications.

However, there remains much work to be done, including detail information for classifying the three properties of ASIL objectively. Besides, more studies on the analysis of operational situation are required. These remaining works are expected to be done in future researches.

## Acknowledgment

This work is partly supported by the Quality Innovation and Infrastructure Development program through the MOTIE (Ministry of Trade, Industry & Energy), Republic of Korea.

## References

[1] M. Ellims and H. E. Monkhouse, "Agonising over ASILs: Controllability and the in-wheel motor," presented at the Incorporation the cyber security conference, Oct. 1-8, 2012.
[2] P. H. Jesty, D. D. Ward, and R. S. Rivett, "Hazard analysis for programmable automotive systems," presented at the Technology International Conference on System Safety, October, 2007.
[3] ISO 26262-1, Road vehicles –Functional safety-part 1: Vocabulary, 2011.
[4] ISO 26262-10, Road vehicles –Functional safety-part 10: Guideline on ISO 26262, 2012.
[5] ISO 26262-3, Road vehicles –Functional safety-part 3: Concept phase, 2011.
[6] MISRA, "The use of controllability for the classification of automotive vehicle hazards," *MISRA Technical Report*, Version 1, Jan. 2007.
[7] W. G. Gulland, *Methods of Determining Safety Integrity Level (SIL) Requirements- Pros and Cons*, London: Springer, 2004, pp. 105-122.
[8] IEC 61508-5, Functional Safety of Electrical/Electronic /Programmable Safety-Related Systems-Part5: Examples of Methods for the Determination of Safety Integrity Levels, 2010.

**Hyeon Ae Jang** was born in Busan, Korea. She received the M.S. degree in industrial engineering from Pukyong National University in 2010. Since then, she has been studying quality management engineering for PhD degree at the same University.
She has participated in Quality Innovation Infrastructure Project organized by MOTIE as a researcher since 2010.
Her main areas of research interest are quality management and engineering, reliability engineering.

**Hyuck Moo Kwon** was born in Daegu, Korea. He received the B.B.S. degree in business administration from Seoul National University, Korea, in 1979, the M.S. degree in industrial engineering from KAIST(Korea Advanced Institute of Science and Technology) in 1981, and the Ph.D. degree in engineering from KAIST in 1994.

He has industrial experiences in two Korean companies for around 5 years. He is currently a professor at the department of Systems Management and Engineering in Pukyong National University, Korea. His research interests cover quality management and engineering, reliability engineering, and design of experiments, with consulting experience on six sigma business strategy over 15 years. He has published over 50 technical papers in journals including the Journal of KIIE, IIE Transactions, European Journal of Operational Research, Naval Research Logistics, Metrika, International Journal of Production Research, International Journal of Production Economics, and etc.

**Sung-Hoon Hong** was born in Seoul, Korea. He received the B.S. degree in industrial engineering from Korea University, Korea, in 1984, the M.S. degree in industrial engineering from KAIST(Korea Advanced Institute of Science and Technology) in 1986, and the Ph.D. degree in engineering from KAIST in 1991.

He is currently a professor at the department of Industrial &Information Systems Engineering in Chonbuk National University, Korea. His research interests cover quality management and engineering, reliability engineering, and design of experiments, with consulting experience on six sigma business strategy over 15 years. He has published over 80 technical papers in journals including Journal of Quality Technology, IIE Transactions, International Journal of Production Research, Naval Research Logistics, International Journal of Production Economics, European Journal of Operational Research, Computers and Industrial Engineering, Engineering Optimization and etc.

**Min Koo Lee** was born in Seoul, Korea, in 1963. He received the B.E. degree in industrial engineering from the AJOU University, Korea, in 1987, and the M.S. and Ph.D. degrees in industrial engineering from the Korea Advanced Institute of Science and Technology (KAIST), Korea, in 1989 and 1993, respectively.

In 1993, he joined the Management Science Research Center, KAIST, as a Researcher. Since September 2005, he has been with the Department of Information and Statistics, Chungnam National University, Daejeon, where he was an Associate Professor, became a Professor in 2010. He is currently Chair of Department of Information and Statistics. His current research interests include statistical process control, six sigma business strategy, and process optimization. Dr. Lee is a Director of the Korean Society for Quality Management; the Korean Institute of Plant Engineering; the Korean Institute of Decision Science. He is a Life Member of the Korean Society for Quality Management, the Korean Institute of Plant Engineering, the Korean Institute of Industrial Engineering, and the Korean Institute of Reliability Engineering.

He published many papers in the European Journal of Operation Research, Computer & I.E., International Journal of Production Research, Economics, Industrial Engineering, and Journal of Quality Technology etc.