ISSN 1229-1889(Print)
ISSN 2287-9005(Online)
J Korean Soc Qual Manag Vol. 42, No.4: 543-562, December 2014
http://dx.doi.org/10.7469/JKSQM.2014.42.4.543

ASIL에 기초하여 수정된 안전시스템 FMEA 위험평가척도

백명식 * · 장현애 ** · 권혁무 **†

* 한국품질재단 부산경남지역본부
** 부경대학교 시스템경영공학부

A Modified Metric of FMEA for Risk Evaluation Based on ASIL of Safety System

Baek, Myoung-Sig * · Jang, Hyeon Ae ** · Kwon, Hyuck Moo **†

* Busan & Gyeongnam Regional Division, Korean Foundation for Quality
** Department of Systems Management and Engineering, Pukyong National University

ABSTRACT

Purpose: The purpose of this study is to suggest a modified approach that compensates some shortcomings of RPN with relevant strength of ASIL for Safety System and suggests systematic and logical approach for FMEA.

Methods: By comparing the objectives, determination procedures, and key conceptual differences of RPN and ASIL, a refined method of risk evaluation and a new risk metric are devised.

Results: While the traditional FMEA provides only rough evaluation of relative risk for each failure, the proposed method compensates its shortcomings with relevant strength of ASIL and provides a more logical and practical procedure of risk evaluation.

Conclusion: The new metric RPM provides not only a comparative priority rank but also the degree of physical seriousness. Besides, it may have even more benefits for various applications if the severity can be expressed as monetary amount of losses.

Key Words: FMEA, RPN, RPM, H&R, ASIL, Safety System

● Received 12 July 2014, 1st revised 25 Setember 2014, 2nd revised 19 November, accepted 28 November 2014
† Corresponding Author(iehmkwon@pknu.ac.kr)

1. Introduction

FMEA (failure mode effect analysis) is widely adopted technique for evaluation of risk due to defects on the initial system design. Since FMEA was first developed in the 1960s by the aerospace industry, it is now a very popular tool not only in the manufacturing but also in service industries (Chen 2007). For example, Onodera (1997) investigated about 100 FMEA applications and found that it is used virtually at every stage of the modern industrial process. Linton (2003) argued that FMEA can assist the development of service process in a manner similar to manufacturing process, Reiling et al. (2003) recognized applicability of FMEA to healthcare service. Sawhney et al. (2004) suggested FMEA application for supplier development. Emphasizing the view of customers, Shahin (2004) suggested to integrate FMEA with the Kano model. Zhao(2011) presented a process oriented quality control approach based on FMEA. Agung and Kwon(2012) proposed a corrective action strategy in service FMEA. There are numerous more works unlisted here.

FMEA uses RPN (risk priority number) for determining the priority of corrective or preventive actions against failure causes. The RPN is a mathematical product of the three risk factors, i.e., severity (the seriousness of failure effect), occurrence (the likelihood that a cause will create the corresponding failure), and detection (the ability to detect the cause or the failure itself before it reaches the customer). However, the RPN of the traditional FMEA does not seem to be accepted as a fine and logical metric for risk evaluation. Many authors criticize the RPN methodology because of its shortcomings. For example, Wang et al.(2009) pointed out that the three risk factors of RPN are difficult to be precisely evaluated in the real situation. Liu et al.(2011) and Liu et al.(2012) explained several shortcomings such as possible same RPN values for different risk implications, ignored difference of relative importance among the three risk factors, possible misleading due to mathematical product of meaningless ordinal numbers, and etc. Similar drawbacks are pointed out by many authors like Chin et al.(2009a, 2009b), Chang and Sun(2009), Abdelgawad and Fayek(2010), Chang et al.(2010), Tay and Lim(2010), Chang and Cheng(2010, 2011), Zhang and Chu(2011), Gargama and Chaturvedi(2011), Zammori and Gabbrielli(2011), Yang et al.(2011), Kutlu and Ekmekcioglu(2012), Xiao et al.(2011) and so on. The frequently mentioned limitations may be summarized as (i) unrealistic assumption of equally weighted RPN elements, (ii) same RPN values possible even with totally different risk context, (iii) possible inconsistent rating among FMEA team members, and (iv) lack of scientific basis for RPN calculation. Liu et al.(2013) summarized the shortcomings of the traditional FMEA in a table reviewing most of recent discussions.

While FMEA is a prevention-oriented technique focused on identifying potential failure modes, their effects and causes, H&R (hazard analysis and risk assessment) is a more systematic and logical risk evaluation process which is focused on the effect of a failure with special concern about functional safety. ASIL is a key output of H&R and reflects the risk of a hazardous event caused by functional failure of an automotive E/E(electrical and/or electronic) item. Thus, each ASIL includes more dependable information on severity of failure effects for each safety requirement or goal. When we perform FMEA after H&R for an automotive E/E item or a safety system, it may be better to use severity information already included in ASIL than to brainstorm on severity again. As we see in the works of Zhang et al.(2010), Kim and

Lee(2012), and Xie et al.(2011), there are increasing efforts to apply FMEA to the area of functional safety. Examining a common denominator of FMEA and H&R carefully, it may be possible to fined an improved method of risk evaluation that can mitigate some limitations of RPN.

In this paper, we are going to compare FMEA with H&R and devise a method of extracting severity information from ASIL to suggest an improved risk metric. This paper is organized as follows: Section 2 compares RPN with ASIL, Section 3 suggests a modified metric RPM, Section 4 provides some insights for practitioners with an illustrative example, and conclusion is followed in Section 5.

2. Comparison of RPN and ASIL

2.1 FMEA and H&R

FMEA is a technique to analyze the potential failure modes of a system and their effects. In order to perform FMEA, we should first define the target system and all its functions to be implemented. Each function may have several failure modes in the perspective of customer or user requirements. Failure is termination of the ability to perform a required function (ISO 26262-1, 2011).

FMEA begins with identifying all possible potential failure modes of a system. On the one side, the effects are derived and their severities are evaluated for each failure mode. In traditional FMEA, the severity (S) of a failure effect is assessed by a number between 1 and 10 with 10 the most severe effect. The severity of a failure mode usually represents its worst effect. On the other side, failure mechanism or causes are determined and possibilities of their occurrences (O) are estimated. The chance of detecting occurrence of each cause (D) is assessed considering the current control method. The occurrence and detection of a failure cause are also assessed by numbers between 1 and 10. A failure cause with occurrence number 10 will occur very frequently, while a failure cause with detection number 10 can hardly be detected. RPN is obtained by a mathematical product of the three numbers representing severity, occurrence and detection for evaluating the risk of each failure cause. Basically, FMEA consists of four key activities; i) identification of potential failure modes, ii) derivation of failure effects and evaluation of their severities, iii) inference of failure mechanisms or failure causes and estimation of their occurrences and detections, and iv) overall risk evaluation based on RPN for each failure mode and cause and taking improvement actions.

H&R is the risk assessment process of ISO 26262. H&R begins under presence of hazard. According to ISO26262-1(2011), hazard is potential source of harm (physical injury or damage to the health of persons) caused by malfunctioning behavior of the item. Malfunctioning behavior is failure or unintended behavior of a system with respect to its design intent. Thus hazard may be understood as failure of a system which possibly results in physical injury or damage to the human body. Therefore, H&R is concerned with a more severe set of failures than FMEA and more focused on the serious effect of each failure. Besides, H&R considers operational situations and operating modes in which the system failure will result in a hazardous event. H&R also estimates the controllability of each hazardous event based on the driving factors and the

probability of exposure of each operational situation. The key outputs of H&R are, thus, a list of hazardous events and safety goals with ASIL.

Both of FMEA and H&R are concerned with risk assessment, of which the objective is avoiding different contexts of risks. The one aims to achieve an improved design which can reduce a general type of risks, the other aims to avoid a more specific type of risks which are confined to human body. Both techniques require the same key input, i.e., a list of functions of the target system. But the key outputs are somewhat different; failure modes and causes with corresponding RPNs for the one and hazardous events with corresponding safety goals and ASILs for the other. FMEA is more focused on the failure cause while H&R is more focused on the failure effect. Thus, RPN is related with a failure cause and ASIL is linked with a hazardous event, i.e., a failure effect. While H&R is executed in concept phase (ISO 26262-3, 2011), FMEA can be used for the extraction of hazards at the item level in concept phase (ISO 26262-3, 2011) or for safety validation (ISO 26262-4, 2011) or safety analyses (ISO 26262-5, 2011) in product development phase. Thus, when FMEA is performed on the basis of pre-executed H&R, failure modes may be inputs to the analyses. Figure 1 compares the input and output of H&R and FMEA from the ISO 26262 perspective.

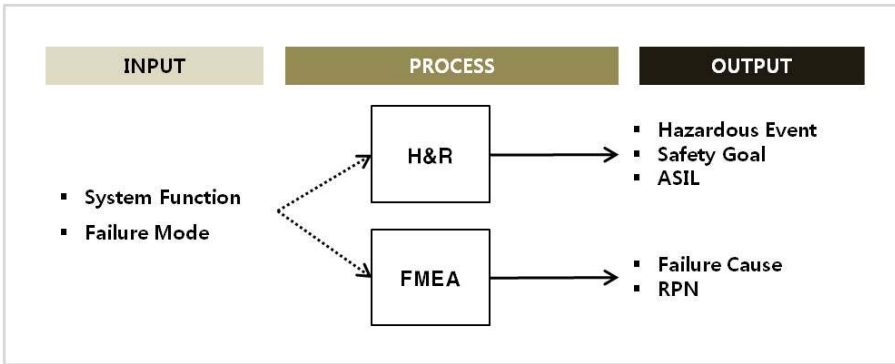

Figure 1. The Input and Output of H&R and FMEA from the ISO 26262 Perspective

When FMEA is applied to various developing activities for a safety system, most failure effects are closely related with safety. The severity of a failure effect in FMEA is naturally linked with the hazardous event caused by the corresponding failure of the safety system. Since H&R of ISO 26262 is a more systematic and scientific risk evaluation process than FMEA, its outcome ASIL provides more objective and dependable information on the severity of failure than RPN that mostly depends on the subjective intuitions of FMEA team members. When we develop a safety system as to ISO 26262, we may expect to complement some drawbacks of RPN by using ASIL information appropriately.

2.2 Determination Procedures of RPN and ASIL

RPN and ASIL are the key outputs of FMEA and H&R for risk assessment purpose. Aiming to catch out their logical difference, we are going to compare their determination procedure. To obtain RPN, the se-

verity, occurrence, and detection of each failure mode should be estimated. The severity is related with the effects of each failure. There may be more than one effect on the customers and thus two or more severity numbers for each failure mode. Severity number takes 10 for an absolutely serious effect and 1 for a negligible effect. When there are several severity numbers due to several effects for one failure mode, the largest number is allocated to the severity of the corresponding failure mode. Occurrence reflects the likelihood that a specific cause will occur, with 10 for very highly probable and with 1 for hardly probable. Again, there may be many causes for each failure mode. Occurrence number is duly allocated to each cause of a given failure mode. Detection is the ability of the proposed current design control to detect the potential failure cause or failure mode. 10 is allocated when it is absolutely uncertain to detect and 1 when almost certain. After evaluating the severity(S), occurrence (O), and detection (D) for a failure cause, RPN is defined by their mathematical product, i.e.

$$RPN = S \times O \times D. \tag{1}$$

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 (ISO 26262-3, 2011). It is also determined by three factors; severity, exposure, and controllability. The severity applies to the harm to each person potentially at risk, considering the relevant operational situation and system failure. One of the four classes S0, S1, S2, and S3 is assigned to each hazardous event with S0 for no injuries and S3 for fatal injuries. Exposure is a state of being in an operational situation that can be hazardous if coincident with the failure mode under analysis. The probability of exposure of each operational situation is estimated based on a defined rationale for each hazardous event. One of the five classes E0, E1, E2, E3, and E4 is assigned to each hazardous event, E0 for incredible and E4 for high probability. Based on the estimated classes of these three factors, ASIL is determined using Table 1 which is provided by ISO 26262-3(2011).The controllability reflects the probability that the driver or other persons potentially at risk is able to gain sufficient control of the hazardous event such that they are able to avoid the specified harm. It is estimated from driving scenario derived by combination of hazardous events and driving factors such as failure of brake, faulty airbag release when travelling at high speed and so on. One of the four classes C0, C1, C2, and C3 is assigned to each hazardous event with C0 for controllable in general and C3 for difficult to control or uncontrollable.

Table 1. ASIL determination

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Figure2 illustrates and compares the determination procedures of RPN and ASIL. While they both are related with failures of a system, RPN is more dependent on pre-failure elements like failure cause and ASIL is more dependent on post-failure elements like failure effect (hazard) and operational situation. The three factors of ASIL are all linked with safety, or risk in another word, and used as means for evaluating seriousness of failure effect.

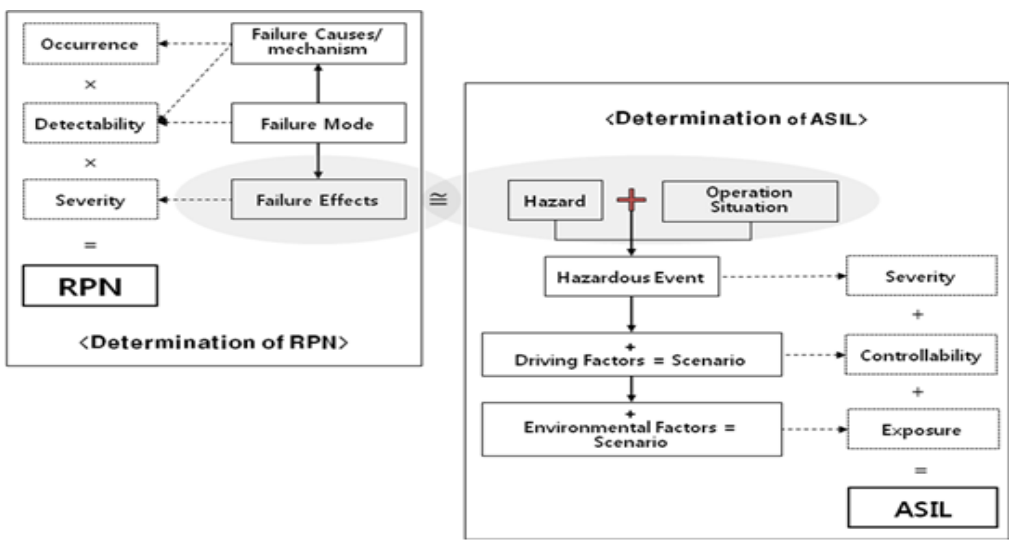

Figure 2. RPN and ASIL Determination

It should be noted here that, wile RPN is likely to depend on the subjective intuition and experience of the FMEA team members, ASIL is determined through quite a systematic and objective procedure. Thus, ASIL can be considered as a much more objective indicator of risk or severity of the failure effect than RPN.

2.3 Improvement opportunities for RPN based on ASIL Scoring

Although FMEA is a widely used technique for risk evaluation and design improvement, RPN is somewhat lack of objectivity, which may result in inconsistent ranking. Sanker and Prabhu (2001) noted that the distortion is compounded by the nonlinear nature of the individual ranking scales. Moreover, RPN scoring system may be different among companies and difficult to be compared objectively. In the traditional FMEA, they recommended that special attention should always be focused on high-severity failure mode regardless of the RPN value (Ireson et al. 1996). This implies the RPN of the traditional FMEA has some limits for its application. Up to now, many authors such as Eubanks et al.(1997), Bertolini et al.(2006), Jeegadeshan et al.(2007), Oolkalkar et al.(2009), Agung and Kwon(2010), and Kwon et al.(2011) tried to find out improved methods for complementing the traditional FMEA. We may have, of course, much benefit from using a single number like RPN to evaluate risk. Using RPN as an objective metric to compare risk levels among different companies, however, may cause various problems. This may happen when an international standard like ISO 26262 imposes some requirements on the industries based on RPN. A newly introduced concept ASIL is quite good for risk evaluation and provides a more systematic ranking procedure. But there still remains room for further sophistication. Basically, ASIL depends on the three factors; severity, exposure, and controllability. A specified process or methodology for determining these factors, however, is not provided in the standard. See Ellims and Monkhouse (2012) for further discussion in this regard.

If we scrutinize the determination procedure of RPN and ASIL, we might extract some improvement ideas for one from the other. In this article, we will focus on improving the RPN scoring procedure based on the idea of ASIL ranking. First, occurrence and detection are better represented by probabilities than 1~10 scales. Their evaluation criteria provided by the traditional FMEA actually is closely related with probability. Even when only rough estimates are available for the probabilities of occurrence and detection, they are better to be used than 1~10 scales. Next, for severity, we use the same terminology in RPN and ASIL but its determination procedure is quite different and its meaning may also be different. In RPN, severity rating has quite a fine scale but its determination is not so logical when compared with that of ASIL. For determining severity class of ASIL, the operational situation, environmental and driving factor are also considered. Moreover, the severity concept of RPN in FMEA is closer to the overall seriousness attributable to the combined effect of severity, exposure and controllability of a hazardous event resulted from a failure. If we introduce these concepts into the severity factor of RPN, the result will be more meaningful. That is, once the three factors of ASIL are appropriately ranked, there may be a proper way to incorporate them into the severity factor of RPN.

3. A Modified Risk Metric for FMEA

3.1 Probability Metric for Failure Occurrence and Detection

According to the FMEA reference manual (Chrysler etc., 2008) and handbook (Ford design Institute, 2004), occurrence is the likelihood that a specific cause/mechanism will occur. And it is ranked on a scale of 1 to 10 considering the possible failure rates, where its evaluation criterion is suggested in a tabular form. Note that the number of occurrence ranking is assigned to each failure cause or mechanism and failure rate is directly linked to failure mode itself. If we consider the time order, a cause must precede the corresponding failure. It does not seem to be logical to determine the occurrence of cause by the failure rate. This manual seems to assume that the occurrence rate of a failure cause is the same as its corresponding failure rate, which implies a failure occurs at the moment its cause occurs. Besides, it can be hardly understood why the number 1 to 10 should be assigned after we already know the failure rates. To correct these logical defects of occurrence ranking in the traditional FMEA, we suggest to using the occurrence rate of each failure cause.

Note that there may be several causes for one failure mode, say FM_i. Suppose that there are n_i causes for FM_i with occurrence rates $\lambda_{i1}, \lambda_{i2}, \dots, \lambda_{in_i}$. Assuming constant rates for failure occurrence, we obtain the probability that the $(i,j)^{th}$ failure cause occurs as

$$O_{ij} = 1 - e^{-\lambda_{ij}}, \quad i = 1, 2, \dots, m \text{ and } j = 1, 2, \dots, n_i \tag{2}$$

To make RPN reflect the risk due to failure modes or causes, the estimated proportions $D_{i1}, D_{i2}, \dots, D_{in_i}$ of undetected causes of FM_i will be used for detection metric.

3.2 Modified Severity Score and RPM

In FMEA, severity has quite different meaning from those of the other two factors. While the numbers for ranking occurrence and detection are closely related with probability, the number for ranking severity is far from probability concept. It reflects the seriousness of physical injury or damage to the human body due to the corresponding failure especially when safety-related risk is under consideration. To obtain a modified metric of severity in FMEA for application to automotive functional safety related E/E component industries, we are going to use the idea in ISO26262-3(2011).

Since the severity of harm due to a failure can be aggravated by the operational situation, environmental and operator conditions, these factors will reasonably be reflected in the modified metric for severity. One simple approach for this purpose may be to multiply the numbers of ASIL component classes; severity, exposure, and controllability. We first assign numbers to the classes of each ASIL component as follows:

- Severity class number: S0→1, S1→2, S2→3, S3→4 ;
- Exposure class number: E0→1, E1→2, E2→3, E3→4, E4→5 ; (3)
- Controllability class number: C0→1, C1→2, C2→3, C3→4 ;

Next, we obtain the severity score as the mathematical product of three class numbers as

$$S = \text{Severity Class (SC)} \times \text{Exposure Class (EC)} \times \text{Controllability Class (CC)} \quad (4)$$

Note that S can have its value from 1 to 80, wider range of value. If we have sufficient information, the severity score may be transformed into a monetary amount of losses due to the hazardous event. Now, the modified RPN for each failure cause is also obtained on the basis of occurrence (O), detection (D) and severity (S) as in the traditional FMEA. Since O and D are probabilities, the modified RPN is the expected value of severity score. Note that the probability of failure occurrence is usually very small and the product $O \times D \times S$ may take its value smaller than zero, which is not convenient to handle. So we define RPM(Risk Priority Metric) in place of conventional RPN as

$$RPM = O \times D \times S \times 1000000. \quad (5)$$

Figure 3 depicts the determination procedure of modified RPM.

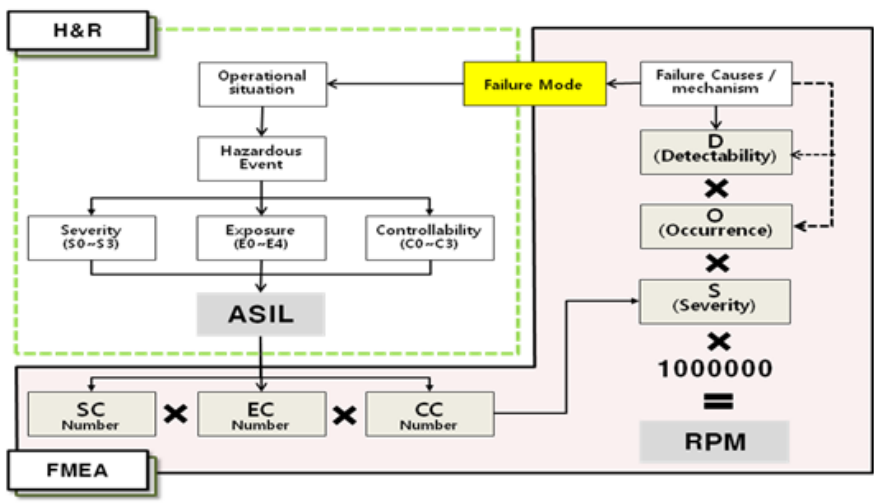

Figure 3. The Determination of RPM

4. Discussions for Practitioners Based on an Example

4.1 An Illustrative Example

Table 2 shows an example of which some part is excerpted from Zhang et al.(2010) which provides an application example of both FMEA and functional safety analysis for ASIL determination with a dual clutch transmission. Some numerical figures are added or slightly changed as necessary to fit our model for illustration purpose without violating rationality. For example, in Table 2, loss of acceleration implies that the vehicle is operable at a reduced level of performance. Thus, according to the traditional FMEA rule, se-

verity ranking 7 is assigned to the failure mode "clutch disengaging". And possible collision implies that it affects safe vehicle operation. But the corresponding failure "incorrect gear position" will have some symptom during operation and its severity is ranked as 9.

Table 2. An Illustrative Example of FMEA Sheet for the Dual Clutch Transmission

Failure Mode	Potential Effects	S	Failure Causes	O	Current Design Controls	D	RPN	Rank
clutch disengaging	shifting failure loss of acceleration	7	dual clutch mechatronic assembly fault	4	dual clutch mechatronic assembly inspection	3	84	5
			shift mechatronic assembly fault	4	shift mechatronic assembly inspection	5	140	1
incorrect gear position	damage of gearbox possible collision	9	sensor fault	3	sensor fault diagnosis	5	135	2
			ECU fault	2	ECU fault diagnosis	5	90	4
			actuator fault	4	actuator fault diagnosis	3	108	3

4.2 Risk Evaluation based on RPM

Now, we are going to demonstrate calculation of RPM based on the previous example. First, consider the occurrence of each failure cause. The first cause “dual clutch mechatronic assembly fault” has 4 for occurrence ranking in Table 2. According to the traditional FMEA, the number 4 corresponds to 1 per thousand items. This can be converted into a probability using formula (2). Thus, our modified occurrence metric is obtained by

$$O = 1 - e^{-0.001} = 9.99 \times 10^{-4} \tag{6}$$

as a probability. The new occurrence metric for the remaining causes can be obtained similarly.

Next, detection in Table 2 should be modified into probability. The ranking criteria for detection are suggested only as a rough guideline by the traditional FMEA. Since detail information on the probability of occurrence is not available from this rough guideline, we simply use the reciprocal of the original detection rank as the probability of detection for only illustrative purpose. It will be better, of course, to use estimated probability values if relevant data are available. For example, the detection rank 3 of the first failure cause in Table 2 will be transformed into the probability of detection as $1/3$. In the real application, of course, this probability should be estimated by real data or on the basis of engineering knowledge.

The modified detection should represent the probability of fail to detect the failure cause. Thus, the detection for the first failure cause will be

$$D = 1 - 1/3 = 2/3 \tag{7}$$

Similar methods are applied to the other causes and summarized in Table 3.

Table 3. Modified Rank of Occurrence and Detection

Failure Mode	Failure Cause	O	D
clutch disengaging	dual clutch mechatronic assembly fault	9.99×10^{-4}	$2/3$
	shift mechatronic assembly fault	9.99×10^{-4}	$4/5$
incorrect gear position	sensor fault	4.99×10^{-4}	$4/5$
	ECU fault	1.00×10^{-4}	$4/5$
	actuator fault	9.99×10^{-4}	$2/3$

Finally, evaluation of severity will be more complicated. If the corresponding SIL is available by previous analysis, however, the severity can easily be evaluated using (3) and (4). For example, Zhang et al.(2010) gives ASIL A to the potential hazard "upshift failure" due to the failure "clutch disengaging". The corresponding classes of severity, exposure, and controllability are S1, E3, and C3. Thus, SC = 2, EC = 4, and CC = 4. And we obtain the severity rank of the failure "clutch disengaging" for FMEA as

$$S_1 = 2 \times 4 \times 4 = 32 \tag{8}$$

Since Zhang et al.(2010) does not provide the ASIL and classes of severity, exposure, and controllability for the potential hazard "collision due to incorrect gear position", we assigned ASIL B with the same classes of exposure and controllability E3 and C3 except that of severity S2. Referring to ISO 26262-3 Annex B (2011), the severity class S2 is justifiable because a vehicle collision may frequently result in severe injuries. Thus, we get the severity rank of the failure "incorrect gear position" for FMEA as

$$S_2 = 3 \times 4 \times 4 = 48 \tag{9}$$

Based on the values of O, D and S, the RPM is calculated using Formula (5) and summarized in Table 4.

Table 4. RPM for the illustrative example

Failure Mode	S	Failure Cause	O	D	RPM	Rank
clutch disengaging	32	dual clutch mechatronic assembly fault	9.99×10^{-4}	$2/3$	21,312	3
		shift mechatronic assembly fault	9.99×10^{-4}	$4/5$	25,574	2
incorrect gear position	48	sensor fault	4.99×10^{-4}	$4/5$	19,161	4
		ECU fault	1.00×10^{-4}	$4/5$	3,840	5
		actuator fault	9.99×10^{-4}	$2/3$	31,968	1

4.3 Sensitivity of RPM

The FMEA handbook(Ford Design Institute, 2004) provides the occurrence and detection rating tables. For occurrence number, however, no clearcut criterion is available with a boundary value of failure rate. Moreover, for detection number, only a vague guideline is provided. With the same numbers of occurrence and detection in the traditional FMEA, there may be many possible values of failure rate and detection probability. So it will be meaningful to examine the change of RPM value with respect to change of the failure rate and detection probability within the boundary limits.

For illustration, only the failure cause "dual clutch mechatronic assembly fault" is considered. The occurrence and detection numbers for this cause are 4 and 3, respectively. According to the occurrence rating table, the occurrence number 4 corresponds to the failure rate 0.001, 5 to 0.002, and 3 to 0.0005. Thus, we consider the boundary failure rates as 0.00075 and 0.0015 for the occurrence number 4. The detection rating table states "high chance the design control will detect a potential cause/mechanism and subsequent failure mode" for detection number 3. But this is a very ambiguous expression to determine the boundary values of detection probability. Since we have already assigned the probability 2/3 for detection number 3, we take 1/2 and 3/4 as the boundary probabilities.

For given detection numbers, Figure 4 shows change in RPM values when the occurrence probability changes within its boundary limits. Note that the RPN will remain unchanged under traditional FMEA. But the value of RPM can be significantly changed so that the rank of RPM may also be changed. Suppose that the detection number 2/3 is correct and unchanged but the occurrence is actually 0.0015 for this failure cause. Then its RPM will be 31976 that is greater than those of the failure causes "shift mechatronic assembly fault" and "actuator fault." As seen in Table 4, these two were ranked number 2 and 1, respectively, in risk priority. Thus, the rank of risk priority may be changed totally even when the RPN of the traditional FMEA remains unchanged. In other words, several different RPM values with different ranks of risk may correspond to the same RPN value of the traditional FMEA. This implies that RPM is more sensitive than RPN with respect to change in probability of occurrence and detection within their boundary limits.

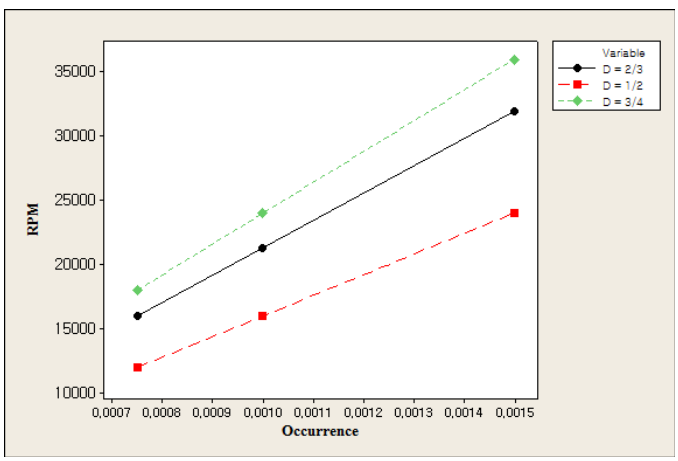

Figure 4. RPM vs occurrence for "dual clutch mechatronic assembly fault"

RPM reflects the non-detected expected severity in its definition and is a meaningful metric for practical applications. Therefore, the illustrative example shows that RPN may provide misleading or distorted information about the risk priority of the failure causes.

4.4 Discussions for Practitioners

- The relationship of RPN and ASIL

Both RPN and ASIL require evaluation of three factors. RPN is determined on the basis of severity, occurrence and detection, while ASIL is determined on the basis of severity, exposure and controllability. Before discussing our model, these terminologies are carefully examined to avoid misunderstanding their exact meaning. The concept of each terminology may be more clearly understood if its corresponding time horizon is considered together. Figure 5 shows sequential occurrences of failure cause, failure, hazard (item's malfunction due to the failure), hazardous event and accident with corresponding ASIL and RPN determination factors.

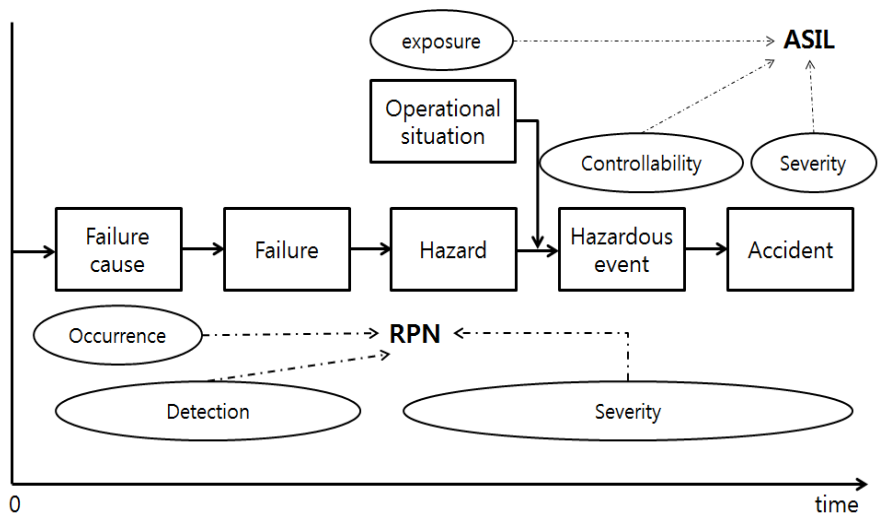

Figure 5. Comparison of RPN with ASIL on time horizon

Note that, even though the same terminology 'severity' is used in ASIL and FMEA, the meaning of each is quite different. Severity in ASIL is seriousness of a hazardous event when it already happened, with exposure and controllability considered separately. Severity in FMEA is closer to overall seriousness of a failure effect, containing exposure and controllability concept in itself. Thus, in FMEA, a failure mode may not be so much severe if it is scarcely exposed to a critical situation or it is easily controllable. On the other hand, a hazardous event resulting from a failure may have a high severity class since even if it can be hardly exposed to a critical operational situation. Exposure in ASIL reflects the possibility that a vehicle confronts a specific operational situation regardless of existence of a hazard. Controllability is evaluated on a hazardous event that is a combination of a hazard and a specific operational situation. Thus, as long as

an automotive safety system is concerned, the severity of a failure effect in RPN is expected to be reflected in the ASIL of the corresponding hazardous event rather than in its single factor, that is, severity, exposure or controllability.

All the three factors of ASIL are linked with the result of a failure, while the factors of RPN are closely linked with the cause of a failure except severity. According to the traditional FMEA, occurrence and detection are determined for each failure cause. See, for example, the sample FMEA sheet provided in the FMEA handbook (Ford Design Institute, 2004). Thus, when FMEA is performed on a safety system with ASIL, we may not induce meaningful information of occurrence or detection from ASIL. But, for severity, a valuable information can be obtained from ASIL. We may presume that, with ASIL D, the corresponding failure will be very much severe, while it will be not so much severe with ASIL A.

- The Meaning of RPN and RPM

The traditional FMEA assigns numbers in the same range of 1 ~ 10 to severity, occurrence, and detection for calculating RPN. This implies that it applies the same weight to the three components even though the importance is different each other. As implicitly stated in various sources of the traditional FMEA, severity is the most important component of RPN. According to the recommendation of the traditional FMEA, a failure mode with high severity score should always be taken special attention even if its corresponding RPN is small. This provides an evidence that the conventional RPN is only a reference value for comparative purpose and may not be a critical decision criterion for a corrective or improvement action.

Considering the critical weaknesses of RPN stated in Section 2.1, a new metric RPM is suggested to improve RPN as risk evaluation metric for a safety system. When FMEA is performed as to ISO 26262 after H&R of the concept phase, ASIL information is already available and it can be reflected into severity score of FMEA. Since exposure and controllability classes in ASIL contain probability concept, the product of the numbers representing the classes of severity, exposure and controllability will reflect the expected degree of severity. Therefore, it will be reasonable to use Formula (4) to obtain the severity score of a failure mode. Concerning occurrence in RPN of FMEA, a rough probabilistic information should already be available to assign numbers. It may be better to use the estimated probability value for evaluating occurrence even if it is a rough estimation. Similar reasoning is possible for detection. Based on these arguments, RPM is constructed as a new metric of risk evaluation for a safety system in FMEA as Formula (5).

RPM may actually be understood as the expected severity of each failure mode or cause. So, if the RPM is negligible, we may neglect the corresponding failure mode or cause without redundant consideration of severity again as in the traditional FMEA. Moreover, RPM is determined on the basis of more systematically and logically evaluated severity.

- RPM as an improved metric for RPN

As argued in Section 2.1, RPN of the traditional FMEA has some significant weaknesses. Let's take an example of Table 5 excerpted from the FMEA reference manual by Chrysler, Ford and General Motors(2008). The manual recommends to take actions on A prior to B even though the latter has a greater

RPN value than the former. The manual states for the reason that the severity of A is greater than that of B. This example speaks loudly the limitations of RPN as a risk metric and the severity is more important than the other two even if the same weight is assigned to all the three factors.

Table 5. Comparison of failure cause A and B

Failure Cause	S	O	D	RPN
A	9	2	5	90
B	7	4	4	112

While the FMEA reference manual recommended not to use a threshold value of RPN for corrective actions, a threshold value of the new metric RPM may be used since RPM actually represents the expected severity. Under the ASIL determination procedure, the severity factor is evaluated through a more systematic and logical approach. Although, ASIL itself does not have a fine discrimination, its determination procedure is quite a logical process that considers not only failure but also operational situations with environmental and driving factors. In the course of systematic risk evaluation process for ASIL, the severity is duly granted more weight in RPM than in RPN. And occurrence and detection are changed into probability metrics, reflecting their original concepts more naturally. They can be estimated statistically if data is available. The statistical approach guarantees us to get more objective estimates for occurrence and detection. Even if their statistical estimates are not available, we may at least apply the method in Section 4.2 based on their values of the traditional FMEA. This simple modification may compensate a considerable proportion of weaknesses of RPN.

For illustration, let's return to the example of Table 2. The severity scores of the failure modes "clutch disengaging" and "incorrect gear position" are 7 and 9 respectively. After evaluating occurrence and detection for each failure cause, however, the cause "shift mechatronic assembly fault" of the failure "clutch disengaging" has the biggest RPN value 140. According to the traditional FMEA, however, we must take care first of the cause "sensor fault" of the failure "incorrect gear position" regardless of RPN value. It may be a nonsense that RPN stands for 'Risk Priority Number'. If we use RPM instead of RPN, Table 4 recommends to take actions first on the cause "actuator fault" of the failure "incorrect gear position", showing a more reasonable result for this example. Actually, RPM may usually be used to decide priority of taking actions, since it reflects an expected severity of a failure cause.

- Limitations of RPM

If we follow the recommendation of the FMEA reference manual, all the causes of the failure mode "incorrect gear position" should be considered prior to those of the failure mode "clutch disengaging". But the RPM values of Table 4 do not agree with that recommendation. This may be understood in two ways; i) even though the weight of severity is adjusted by (4), it may not be sufficient, or ii) the adjusted weight is appropriate but the manual puts too much weight on severity. In case ii), the risk priority determined by

RPM will also mislead to a wrong decision. If the expected total amount of loss due to the failure is available, it may be easily modified by replacing the severity score of (4) with the expected total loss. But it may also be difficult to get all the necessary information of losses due to the corresponding failure.

Comparing Table 4 with Table 2, the priorities of the causes "sensor fault" and "actuator" fault for the same failure "incorrect gear position" are also changed. In this situation, the priority is effective on the condition that occurrence and detection are correctly estimated, which may not be so easy. In RPM, occurrence and detection are evaluated by probabilities, reflecting their original concepts more naturally. This approach may guarantee more objective metrics for occurrence and detection. But it, at the same time, requires sufficient data available which may not be possible in a common situation.

RPN of the traditional FMEA depends on the rating of three components that is usually determined on the basis of the past experiences and intuition of the practitioners or engineers. RPN gives us rough evaluation of relative importance for each failure cause, which unavoidably tends to be subjective after all. RPM is based on a more systematic and logical approach using ASIL. Although, ASIL itself does not have a fine discrimination, its determination procedure is quite a logical process that considers not only failure but also operational situations with environmental and driving factors. The new metric RPM is sure to have more logical and practical meaning. However, it goes only a step further than RPN and also has several limitations to overcome in the future study.

5. Conclusion

Based on the careful comparison of RPN and ASIL determination procedures, we suggested a modified approach to FMEA. Of the three components of FMEA, occurrence and detection are converted into probability metrics. And severity is determined through a more logical and sophisticated process based on the ASIL determination procedure. A numerical example shows that the RPM and the conventional RPN may be different in both the priority orders of failure causes and in the practical meaning.

In the traditional FMEA, the technique to evaluate the RPN does not consider interactions among human, failure mode and operational situations. And equally weighted components may result in an unacceptable priority order of RPN. In addition to subjectivity of the traditional FMEA, its resulting RPN does not provide an absolute criterion to decide corrective or improvement action. As the traditional FMEA manual pointed out, a failure cause may need correction even with small RPN if its corresponding severity score is large. The modified FMEA compensates most of these weaknesses of the traditional FMEA. Compared with the traditional FMEA, the proposed method can provide more realistic information on the magnitude of risk for each failure mode and its corresponding cause. That is, the RPM provides a risk metric with real meaning, which not only provides a comparative priority rank but also the degree of physical seriousness as an absolute quantity since it actually is representing an expected severity. If the severity can be expressed as monetary amount of losses, the RPM may have even more benefits for various applications.

This study suggests a refined conceptual method for risk evaluation system, however, it is only at its ini-

tial stage and has several shortcomings. Neither the possible scenarios of hazardous events are considered completely nor a systematic method is provided to find them. And some assumptions such as constant failure occurrence may be unrealistic. These shortcomings may be overcome by introducing some core concepts of FMECA, FMEDA and other relevant methodologies. The unexplored problems are widely open to further studies.

Acknowledgement

This research was supported by the MOT (Management Of Technology) Professional Manpower Training Business through the Ministry of Trade, Industry and Energy (1415134318)

REFERENCES

Abdelgawad, M., and Fayek, A. R. 2010. "Risk management in the construction industry using combined fuzzy FMEA and fuzzy AHP." Journal of Construction Engineering and Management 136:1028-1036.

Agung, S., and Kwon, H. 2010. “An Expected Loss model for Risk Prioritization in Service FMEA.” California Journal of Operations Management 8:27-38.

Agung, S., and Kwon, H. 2012. "Corrective Action Strategy based on SWOT Analysis in Service FMEA." Journal of the Korean Society for Quality Management 40:25-38.

Bertolini, M., Braglia, M., and Carmignani, G. 2006. “An FMECA-based Approach to Process Analysis.” International Journal of Process Management and Benchmarking 20:127-145.

Chang, D. S., and Sun, K. L. P. 2009. "Applying DEA to enhance assessment capability of FMEA." International Journal of Quality and Reliability Management 26:629-643.

Chang, K. H., and Cheng, C. H. 2010. "A risk assessment methodology using intuitionistic fuzzy set in FMEA." International Journal of Systems Science 41:1457-1471.

Chang, K. H., and Cheng, C. H. 2011. "Evaluating the risk of failure using the fuzzy OWA and DEMATEL method." journal of Intelligent Manufacturing 22:113-129.

Chang, K. H., Cheng, C. H., and Chang Y. C. 2010. "Reprioritization of failures in a silane supply system using an intuitionistic fuzzy set ranking technique." Soft Computing 14:285-298.

Chen, J. K. 2007. “Utility Priority Number Evaluation for FMEA.” Journal of Failure Analysis and Prevention 5:321-328.

Chin, K. S., Wang, Y. M., Poon, G. K. K., and Yang, J. B. 2009. "Failure mode and effects analysis by data envelopment analysis." Decision Support Systems 48:246-256.

Chin, K. S., Wang, Y. M., Poon, G. K. K., and Yang, J. B. 2009. "Failure mode and effects analysis using a group-based evidential reasoning approach." Computers and Operations Research 36:1768-1779.

Chrysler LLC, Ford Motor Company, and General Motors Corporation. 2008. FMEA Reference Manual, 4th ed.

Ellims, M., and Monkhouse, H. E. 2012. “AGONISING OVER ASILS: Controllability and the In-Wheel Motor.” System Safety, Proceedings at The Incorporation the cyber security conference, 1-8.

Eubanks, C. F., Kmenta, S., and Ishii, K. 1997. “Advanced FMEA Using behavior Modeling.” Proceedings of ASME Design Engineering Technical Conference, California: Sacramento, 1-10.

Ford Design Institute. 2004. FMEA handbook, Version 4.1.

Gargama, H., and Chaturvedi, S. K. 2011. "Criticality assessment models for failure mode effects and criticality analysis using fuzzy logic." IEEE transactions on Reliability 60:102-110.

Ireson, W. G., Coombs, Jr. C. F., and Moss, R. Y. 1996. "Handbook of reliability engineering and management Second Edition." McGraw-Hill.

ISO 26262-1. 2011. Road vehicles -Functional safety-part 1: Vocabulary.

ISO 26262-3. 2011. Road vehicles -Functional safety-part 3: Concept phase.

ISO 26262-4. 2011. Road vehicles -Functional safety-part 4: Product development at the system level.

ISO 26262-5. 2011. Road vehicles -Functional safety-part 5: Product development at the hardware level.

Jeegadeshan, C., Arunachalam, V. P., Devadasan, S. R., and Srinivasan, P. S. S. 2007. "Design and Development of Modified Service FMEA Model." International Journal of Service and Operations Management 1:111-126.

Kim, H., and Lee, N. 2012. "The Case Study on Software FMEA for the Efficient Improvement of Functional Safety." KSAE 2012 Conference, 1303-1308.

Kutulu, A. C., and Ekmekcioglu, M. 2012. "Fuzzy failure modes and effects analysis by using fuzzy TOPSIS-based fuzzy AHP." Expert Systems with Applications 39:61-67.

Kwon, H. M., Hong, S. H., Lee, M. K., and Agung, S. 2011. "Risk Evaluation Based on the Time Dependent Expected Loss Model In FMEA." Journal of the Korea Society of Safety 6:104-110.

Linton, J. D. 2003. "Facing the challenges of service automation: An enabler for e-commerce and productivity gain in traditional service." IEEE Trans, Eng., Manage 4:478-487.

Liu, H. C., Liu, L., Bian, Q. H., Lin, Q. L., Dong, N., and Xu, P. C. 2011. "Failure mode and effects analysis using fuzzy evidential reasoning approach and grey theory." Expert Systems with Applications 38:4403- 4415.

Liu, H. C., Liu, L., and Liu, N. 2013. "Risk Evaluation Approaches in Failure Mode and Effects Analysis: A Literature Review." Expert Systems with Applications 40:828-838.

Liu, H. C., Liu, L., Liu, N., and Mao, L. X. 2012. "Risk Evaluation in Failure Mode and Effects Analysis with extended VIKOR method under fuzzy environment." Expert Systems with Applications 39:12926- 12934.

Onodera, K. 1997. "Effective techniques of FMEA at each life-cycle stage." Proceeding of Annual Reliability and Maintainability Symposium, 50-56.

Oolkalkar, A. D., Joshi, A. G., and Oolkalkar, D. S. 2009. "Quality Improvement in Haemodialysis Process Using FMEA." International Journal of Quality and Reliability Management 8:817-830.

Reiling, J. G., Knutzen, B. L., and Stoechlein, M. 2003. "FMEA-the cure for medical errors." Qual. Progr. 8:67-71.

Sankar, N. R., and Prabhu, B. S. 2001. "Modified approach for prioritization of failures in a system failure mode and effects analysis." International journal of Qaulity & Reliability Management 3:324-335.

Sawhney, R., Padiyar, A., and Li, Y. 2004. "FMEA based approach for supplier development." Proceedings of IIE Annual Conference and Exhibition 7-16.

Shahin, A. 2004. "Integration of FMEA and the Kano model: An exploratory examination." Int. J. Qual. Reliab. Manage 21:731-746.

Tay, K. M., and Lim, C. P. 2010. "Enhancing the failure mode and effect analysis methodology with fuzzy inference techniques." Journal of Intelligent and Fuzzy Systems 21:135-146.

Wang, Y. M., Chin, K. S., Poon, G. K. K., and Yang, J. B. 2009. "Risk Evaluation in failure mode and effects analysis using fuzzy weighted geometric mean." Expert Systems with Applications 36:1195-1207.

Xiao, N. C., Huang, H. Z., Li, Y. F., He, L. P., and Jin, T. D. 2011. "Multiple failure modes analysis and weighted risk priority number evaluation in FMEA." Engineering Failure Analysis 18:1162-1170.

Xie, Y., Li, J., and Zhang, A. 2011. "Extended FMEA Method Applied in the Field of Functional Safety." Maintainability and Safety(ICRMS), 9th International Conference on Reliability, 615-618.

Yang, J., Huang, H. Z., He, L. P., Zhu, S. P., and Wen, D. 2011. "Risk evaluation in failure mode and effects analysis of aircraft turbine rotor blades using Dempster-Shafer evidence theory under uncertainty." Engineering Failure Analysis 18:2084-2092.

Zammori, F., and Gabbrielli, R. 2011. "ANP/RPN: A multi criteria evaluation of the risk priority number." Quality and Reliability Engineering International 28:85-104.

Zhang, H., Li, W., and Quin, J. 2010. "Model-based Functional Safety Analysis Method for Automotive Embedded

System Application." International Conference on Intelligent Control and Information Processing, China: Dalian. August 13-15.

Zhang, Z. F., and Chu, X. N. 2011. "Risk prioritization in failure mode and effects analysis under uncertainty." Expert Systems with applications 38:206-214.

Zhao, X. 2011. “A Process Oriented Quality Control Approach Based on Dynamic SPC and FMEA.” Int. J. of Industrial Engineering: Theory, Applications and Practice 18:444-451.