



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

공학박사 학위논문

자동차 안전무결성 수준(ASIL)에
기초한 FMEA 위험평가에
대한 연구



2016년 2월

부경대학교 대학원

기술경영협동과정

백 명 식

공학박사 학위논문

자동차 안전무결성 수준(ASIL)에
기초한 FMEA 위험평가에
대한 연구

지도교수 권 혁 무

이 논문을 박사학위 논문으로 제출함.

2016년 2월

부경대학교 대학원

기술경영협동과정

백 명 식

백명식의 공학박사 학위논문을 인준함.

2016년 2월 26일

위원장	공학박사	구 평 회	
위원	공학박사	옥 영 석	
위원	공학박사	양 성 민	
위원	공학박사	차 명 수	
위원	공학박사	권 혁 무	

목 차

I . 서 론	1
1.1 연구배경 및 목적	1
1.2 선행연구 분석	5
1.2.1 FMEA 선행연구	6
1.2.2 ISO 26262 선행연구	10
1.3 연구의 내용 및 구성	12
 II . ASIL과 FMEA의 위험평가	15
2.1 ASIL의 위험평가	15
2.1.1 ISO 26262 개요	15
2.1.2 위험원 분석 및 리스크평가(H&R)	21
2.1.2.1 상황분석과 위험원식별	21
2.1.2.2 위험사건의 분류	21
2.1.2.3 ASIL결정 및 수행	31
2.2 FMEA의 위험평가	33
2.2.1 FMEA 개요	33
2.2.2 위험평가	36
2.2.2.1 심각도(Severity)	37
2.2.2.2 발생도(Occurrence)	39
2.2.2.3 검출도(Detection)	41

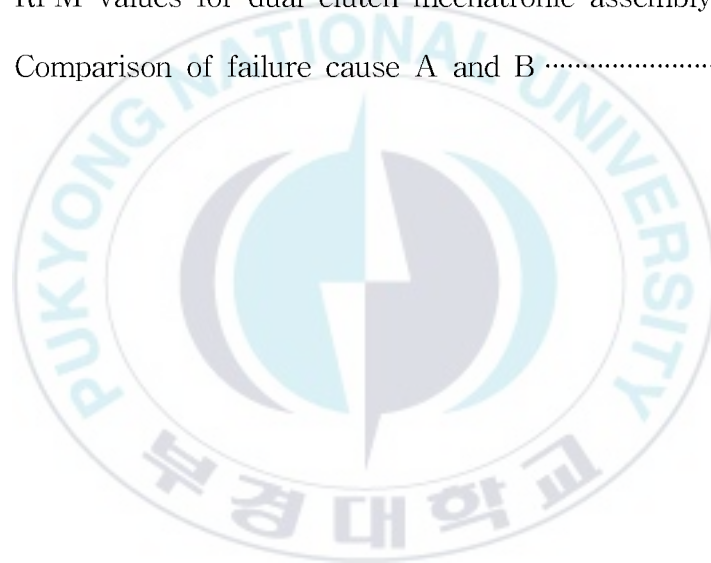
2.2.2.4 위험우선순위(RPN) 결정	43
III. ASIL 결정을 위한 기능안전 운전상황 분석	45
3.1 서론	45
3.2 표준에 의한 H&R 및 ASIL 결정의 한계	47
3.2.1 위험원과 위험사건	47
3.2.2 ASIL결정 절차의 한계	49
3.3 운전상황 분석 및 ASIL 결정단계	51
3.3.1 운전상황 분석	51
3.3.2 위험사건 식별 및 ASIL 결정단계	54
3.4 심각도와 노출확률 및 제어가능성 등급결정	55
3.4.1 심각도	55
3.4.2 노출확률	56
3.4.3 제어가능성	58
3.5 EPB 시스템 적용	60
IV. ASIL 기반 FMEA 위험평가 척도	64
4.1 서론	64
4.2 RPN과 ASIL의 비교	66
4.2.1 FMEA와 H&R	66
4.2.2 RPN과 ASIL의 결정절차	69
4.2.3 ASIL등급을 기반으로 한 RPN 개선	72
4.3 FMEA에 대한 수정된 위험척도	74

4.3.1 고장발생도 및 검출도에 대한 확률척도	74
4.3.2 수정된 심각도 점수와 RPM	75
4.4 사례 연구	77
4.4.1 Dual Clutch Transmission 사례	77
4.4.2 RPM 기반의 리스크평가	79
4.4.3 RPM의 민감도	83
4.4.4 실무적용을 위한 논의	89
4.4.4.1 RPN과 ASIL의 관계	89
4.4.4.2 RPN과 RPM의 의미	91
4.4.4.3 RPN과 RPM	93
4.4.4.4 RPM의 한계	94
V. 결론	97
5.1 연구 결과	97
5.2 향후 연구방향	99
참고 문헌	101
부 록	109

표 목 차

Table 1.1	Classification of shortcoming in FMEA	3
Table 1.2	Classification of literatures in FMEA and ISO 26262	5
Table 1.3	Modified FMEA sheet of Kim et al.(2010)	6
Table 1.4	Scope of studies	14
Table 2.1	Comparison of IEC 61508 and ISO 26262	16
Table 2.2	Classification example and classes of severity	23
Table 2.3	Classes of probability of exposure regarding duration in operational situations	25
Table 2.4	Classes of probability of exposure regarding frequency in operational situations	27
Table 2.5	Classification examples and classes of controllability	29
Table 2.6	ASIL Determination	31
Table 2.7	System design analysis	32
Table 2.8	Properties of modular system design	32
Table 2.9	Types of FMEA	34
Table 2.10	Evaluation criteria of severity in FMEA	38
Table 2.11	Evaluation criteria of occurrence in FMEA	40
Table 2.12	Evaluation criteria of detection in FMEA	41
Table 3.1	Factors of operational situation	53

Table 3.2	Factors of operational situation for EPB system	61
Table 3.3	ASIL Determination of EPB system	63
Table 4.1	An illustrative example of FMEA sheet for the dual clutch transmission	78
Table 4.2	Modified rank of occurrence and detection	81
Table 4.3	RPM for the illustrative example	82
Table 4.4	RPM values for dual clutch mechatronic assembly fault	83
Table 4.5	Comparison of failure cause A and B	93



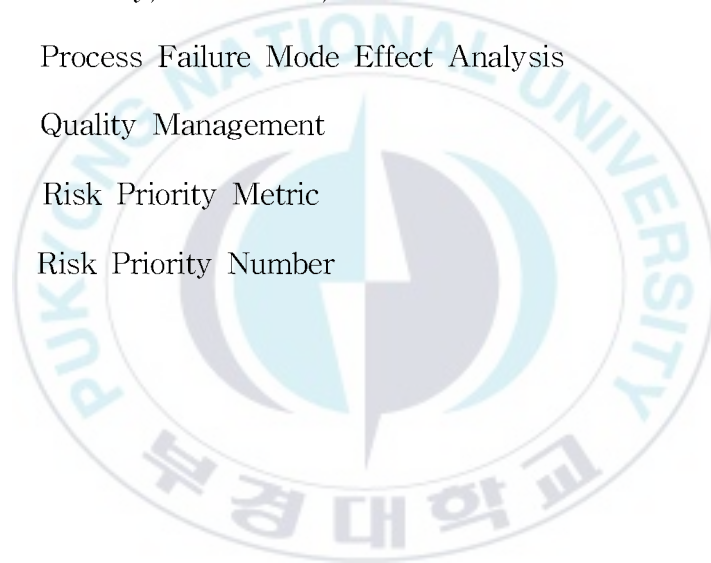
그 립 목 차

Figure 2.1	Overview of ISO 26262	20
Figure 2.2	Action process in FMEA	35
Figure 3.1	Fault leading to harm	48
Figure 3.2	Example of EPB system's hazardous event	49
Figure 3.3	Determination procedure of severity	56
Figure 3.4	The controllability for independent vs dependent cases	59
Figure 4.1	The input and output of H&R and FMEA from the ISO 26262 perspective	69
Figure 4.2	RPN and ASIL Determination	72
Figure 4.3	The determination of RPM	77
Figure 4.4	RPM vs Occurrence for dual clutch mechatronic assembly fault	84
Figure 4.5	RPM vs Occurrence for shift mechatronic assembly fault	85
Figure 4.6	RPM vs Occurrence for sensor fault	86
Figure 4.7	RPM vs Occurrence for ECU fault	87
Figure 4.8	RPM vs Occurrence for actuator fault	88
Figure 4.9	Comparison of RPN with ASIL on time horizon	90

Nomenclature

AAAM	Association for the Advancement of Automotive Medicine
AHP	Analytic Hierarchy Process
AIAG	Automotive Industry Action Group
AIS	Abbreviated Injury Scale
APQP	Advanced Product Quality Plan
ASIL	Automotive Safety Integrity Level
DEA	Data Envelopment Analysis
DEMATEL	Decision Making Trial and Evaluation Laboratory
DFMEA	Design Failure Mode Effect Analysis
DIA	Development Interface Agreement
ECU	Electronic Control Unit
E/E	Electrical and/or Electronic
EPB	Electrical Parking Brake
ER	Evidential Reasoning
ETA	Event Tree Analysis
FMFEA	Failure Mode Factors and Effects Analysis
FMEA	Failure Mode Effect Analysis
FMECA	Failure Modes Effects and Criticality Analysis
FMEDA	Failure Modes Effects and Diagnostic Analysis

FRPNs	Fuzzy Risk Priority Numbers
FTA	Fault Tree Analysis
GRP	Grey Relational Projection
H & R	Hazard Analysis and Risk Assessment
IEC	International Electrotechnical Committee
ISO	International Organization for Standardization
S, O, D	Severity, Occurrence, Detection
PFMEA	Process Failure Mode Effect Analysis
QM	Quality Management
RPM	Risk Priority Metric
RPN	Risk Priority Number



A Study on Risk Evaluation of FMEA Based on Automotive Safety Integrity Level

Myoung-Sig, Baek

Interdisciplinary Program of Management of Technology,
The Graduate School, Pukyong National University

Abstract

FMEA is a technique that identifies all possible failure modes and their potential causes of a design or a process and evaluates their effects. Although it is very widely adopted in the manufacturing as well as service industries, its risk evaluation metric RPN has room for further improvement. With all the previous studies on improvement of RPN, it still has some drawbacks such as (i) subjective and inconsistent evaluating process, (ii) uniform weight allocation to its three components, (iii) numerical figures without practical meaning except priority which also is doubtful, and (iv) dependence on intuitions and personal experiences of the FMEA members.

This thesis suggests a new risk evaluation metric RPM based on ASIL for application to the automotive industries. ASIL is determined through a systematic and logical risk evaluation process, i.e. H&R of ISO 26262. RPM provides more realistic information on the magnitude of risk for each failure mode and its corresponding causes,

compensating some drawbacks of the traditional FMEA. This thesis is structured as follows:

First, previous studies are reviewed on the traditional FMEA and the H&R process of ISO 26262 to develop a new risk evaluation metric and process. With FMEA, the works on the shortcomings of RPN and its improvement are reviewed. With ISO 26262, the works on H&R process and ASIL determination are mainly focused.

Next, a systematic model is proposed for classifying the three properties of the hazardous event and a refined procedure is suggested for ASIL determination. To determine a proper ASIL for each hazardous event with a proper safety goal, the right classes should first be determined for the three properties of the hazardous event: (i) severity of harm from the resultant accident, (ii) exposure to the relevant operational situation, and (iii) controllability to avoid the induced risks. ASIL can be clearly determined with right classes of these three properties. But no specific methodologies or processes for their classification can be found in ISO 26262, except only a rough guideline with a simplified set of illustrative tables. To perform a effective H&R in ISO 26262, an operational situation analysis model is suggested. The proposed model provides a specific method to get a more objective ASIL compared with that in the standard. Scrutinizing the current methodology, a refined method is developed. With an application example of “EPB system,” its effectiveness is validated for ASIL determination.

Finally, a modified systematic and logical approach for FMEA is suggested, which compensates some shortcomings of RPN with relevant strength of ASIL for Safety System. 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 RPM are devised. While the traditional FMEA provides only rough evaluation of relative risk for each failure, the proposed method provides a more logical and practical procedure of risk evaluation. The RPM provides not only a comparative priority rank but also the degree of physical seriousness. If the severity can be expressed as monetary amount of losses, RPM may have even more benefits for various applications.

I. 서론

1.1 연구배경 및 목적

산업 현대화를 주도해온 선진국에서는 미래를 위한 여러 가지 대안들을 준비하는 과정에서 그 기술적 우위를 지키는 핵심기술로 시스템분야를 꼽고 있다. 특히 시스템 기술은 개발, 생산, 품질에 있어서 불확실성과 위험을 체계적으로 관리하고 손실을 최소화하는 핵심기술로서 첨단산업의 선두를 유지하는 하나의 비결이 될 수 있다. 이러한 시스템 접근기술의 여러 방법들 중 하나가 FMEA(Failure Mode Effect Analysis)라고 할 수 있으며, 생산과 제품기술에서 FMEA는 단순히 고장과 결함을 체계적으로 파악하는 방법 이상의 의미를 가진다.

FMEA는 1950년대 초 프로펠라 추진항공기가 제트엔진 항공기로 전환되면서 유압장치가 전기장치로 구성되는 복잡한 조종시스템을 가진 제트기의 신뢰성 설계를 위해 처음 사용되었다. 이후 1960년대 NASA에서 우주선 개발 시 각 부품의 설계 결함으로 인한 위험을 평가하기 위해 사용되었고, 1980년대 포드(Ford) 엔지니어들에 의해 자동차산업에 도입되어 지금은 제조뿐만 아니라 서비스 산업에서도 매우 보편적으로 사용되는 품질개선 및 신뢰성 관리의 필수적 요건으로 간주되는 분석기법이다.

FMEA는 고장원인에 대한 시정 또는 예방활동의 우선순위를 결정하기 위해 RPN(Risk Priority Number: 위험우선 순위)을 사용하는데, RPN은

세 가지 위험요소인 심각도(Severity, 고장 영향의 심각성), 발생도(Occurrence, 원인에 의한 해당 고장을 생성할 가능성), 검출도(Detection, 제품이 고객에 도달하기 전에 원인 또는 고장 자체를 검출할 수 있는 능력)의 곱으로 구한다. 그러나 기존 FMEA의 RPN은 위험평가에 대하여 그다지 논리적 이고 체계적인 척도로 인정받지 못하고 있다. 많은 학자들은 RPN의 단점 때문에 위험평가에 대한 RPN 방법론을 비판하고 있다. 예를 들어, Wang et al.(2009)은 RPN의 세 가지 위험 요소가 실제 상황에서는 정확하게 평가되기 어렵다고 지적했다. Liu et al.(2011)과 Liu et al.(2012)은 RPN이 똑같은 값을 가지더라도 전혀 다른 위험의 의미를 가질 수 있다는 점, 위험의 세 가지 요소 즉 심각도, 발생도 및 검출도는 중요도가 같지 않다는 점, 순서적 의미 외에 별다른 의미가 없는 세 요소의 평가 값을 곱하여 수치로 나타냄으로써 그 값이 절대적인 의미를 갖는 것으로 오해를 불러일으킬 수 있다는 점, 등을 들고 있다. 또한 Liu et al.(2013)은 최근 논의된 FMEA에 대한 연구결과들을 대부분 검토하여 기존 FMEA의 단점을 Table 1.1과 같이 요약 정리하였다.

ASIL(Automotive Safety Integrity Level: 자동차 안전무결성 수준) 등급은 ISO 26262의 H&R(Hazard Analysis and Risk Assessment: 위험원 분석 및 리스크 평가)을 통해서 결정되고 있다. E/E(Electrical and/or Electronic: 전기/전자) 시스템의 개발 및 운영의 전 단계에 걸쳐 기능안전성 요건 설정의 토대가 되는 ASIL은 아이템이나 엘리먼트에 있어서는 안 될 잔존 리스크를 방지하기 위해 적용되는 안전무결성 등급 (ISO 26262-1, 2011)으로써 안전 목표와 함께 본격적인 아이템 개발 이전에 결정되어야 한다. 따라서 ASIL은 시스템 개발에서 가장 우선적으로 결정될 뿐만 아니라 제품의 안전요구사항 평가지표를 제공하기 때문에 시스템 개발의 핵심

요소라고 할 수 있다. FMEA는 잠재적 고장모드의 영향과 원인을 식별하는 예방에 초점을 맞춘 기술이지만, H&R은 기능안전에 대하여 특별한 관계가 있는 고장의 영향에 초점을 맞춘, 보다 체계적이고 논리적인 위험 평가 프로세스이다.

Table 1.1 Classification of shortcoming in FMEA

Component Issues	RPN Improvement
• The relative importance among O, S and D is not taken into consideration • Different combinations of O, S and D may produce exactly the same value of RPN, but their hidden risk implications may be totally different • The three risk factors are difficult to be precisely evaluated • The conversion of scores is different for the three risk factors	• The mathematical formula for calculating RPN is questionable and debatable • The RPN cannot be used to measure the effectiveness of corrective actions • RPNs are not continuous with many holes • Interdependencies among various failure modes and effects are not taken into account • The mathematical form adopted for calculating the RPN is strongly sensitive to variations in risk factor evaluations • The RPN considers only three risk factors mainly in terms of safety • The RPN elements have many duplicate numbers

본 연구에서는 안전 시스템을 위한 ASIL 결정에서 가장 중요한 단계인 위험사건분류와 관련된 절차를 체계화하여 제시하고, ISO 26262에서 체계적이고 논리적인 H&R의 핵심 결과물인 ASIL의 강점을 이용하여 FMEA의 위험평가 척도인 RPN의 단점을 보완하는 새로운 접근방식인 RPM (Risk Priority Metric)을 제시하고자 한다. 이를 통해 산업현장에서 자주 접할 수 있는 기존 FMEA의 문제점에 대한 현실적인 개선방안을 다음과 같이 제시한다.

첫째, ASIL 결정에서 가장 중요한 단계인 위험사건분류와 관련된 절차를 체계화하여 제시하고, ASIL 결정을 위해 수행되는 H&R 단계를 구체적으로 분석하여 산업현장에서 ISO 26262에 따라 제품을 개발할 초기의 ASIL을 결정할 단계에서, 보다 체계적인 접근이 가능하도록 해 준다.

둘째, ASIL에서 체계적이고 논리적으로 평가된 심각도를 반영함으로써, 구성요소에 대한 차별화된 중요도를 부여하고, 사람과 고장모드 및 운영 상황들 사이의 상호 작용을 고려한다.

셋째, 발생도 및 검출도는 확률에 의해 결정됨으로써 보다 객관적인 평가척도를 제공한다.

넷째, 검출되지 않은 예상 위험을 반영하여 현장 적용을 위한 현실적인 정보를 제공한다.

다섯째, RPM은 경계 값 내에서의 위험평가에 대한 정확한 정보를 제공한다.

1.2 선행연구 분석

본 연구와 관련된 선행연구들을 FMEA와 ISO 26262의 두 가지 범주로 구분하여 분석하면 Table 1.2와 같다. FMEA에는 본 연구와 연관된 위험평가 프로세스인 RPN과 FMEA에 대한 일반적인 연구인 기타로 분류한다. ISO 26262 역시 본 연구와 연관된 위험평가 프로세스인 H&R 및 ASIL과 ISO 26262의 일반적인 연구 및 ISO 26262와 다른 위험평가 기법과의 접목을 시도한 연구는 기타로 분류한다.

Table 1.2 Classification of literatures in FMEA and ISO 26262

Criteria		Literature
FMEA	RPN	Chang and Sun(2009), Chin et al.(2009), Kim et al.(2010), Liu et al.(2011), Liu et al.(2012), Liu et al.(2013), Liu et al.(2014), Sankar and Prabhu(2001), Wang et al.(2009), Xu et al.(2002),
	Other	Agung and Kwon (2012), Jang (2015), Linton (2003), Reiling et al.(2003), Sawhney et al.(2004), Shahin (2004), Teng et al. (2006),
ISO 26262	ASIL (H&R)	Cho et al.(2010), Ellims and Monk-house(2011), Ellims et al.(2012), Jesty et al.(2007), Kim and Jang(2011), Lee and Jeon (2013), Roh (2015), Schlummer et al.(2010),
	Other	Kim and Lee(2012), Lim(2013), Rivett (2009), Song (2013), Xie et al.(2011), Zhang et al.(2010), Zhao (2011)

1.2.1 FMEA 선행연구

먼저 FMEA에서 위험우선순위 결정을 위한 RPN과 관련한 선행연구내용을 검토한 결과는 다음과 같다. Chang and Sun(2009)은 보다 효과적인 심각도, 발생도, 검출도의 통찰력을 제공하기 위하여 DEA(Data Envelopment Analysis) 기법을 제안하였고, Chin et al.(2009)은 ER(Evidential Reasoning)을 기반으로 심각도, 발생도, 검출도 사이의 상대적 중요성을 고려하였다. Kim et al.(2007)은 RPN 평가시의 문제점을 “적용하고자 하는 제품에 적합하지 못한 평가기준의 적용”과 “평가자간 평가결과의 불일치를 가져오는 평가기준의 모호성”이라고 주장하고, 이러한 문제점을 개선하기 위해 심각도, 발생도, 검출도에 대한 평가기준을 재정립하였다. 또한 재정립된 평가기준이 용이하게 활용될 수 있도록 개선된 FMEA 양식을 Table 1.3과 같이 제시하였다.

Table 1.3 Modified FMEA sheet of Kim et al.(2010)

제품 / 기능	잠재적 고장 모드	고장의 잠재적 영향			심각도			분류	고장의 잠재원인 / 메카니즘	발생도		현 설계 관리		검출도		RPN	권고 조치 사항	책임 및 목표 완료 예정일	조치결과				
		공정	시스템	고객	공정	시스템	고객			공정	필드	예방관점	검출관점	공정	고객				조치내용	심각도	발생도	검출도	RPN

Liu et al.(2011), Liu et al. (2012)은 RPN이 동일한 값을 가지더라도 실제적으로 전혀 다른 위험의 의미를 가질 수 있다는 점과 심각도, 발생도, 검출도의 중요도가 같지 않다는 점, 산정된 RPN 값이 순서적 의미 외에 별

다른 의미가 없음에도 그 값이 절대적인 의미를 가지는 것으로 오해를 불러일으킬 수 있다는 점 등의 몇 가지 단점을 지적하였다. Liu et al.(2013)은 1992년부터 2012년까지 FMEA에 대한 연구결과들 대부분을 검토하여 기존 FMEA의 단점을 다음과 같이 요약 정리하였다.

첫째, 심각도, 발생도 및 검출도 사이의 상대적 중요성은 고려되지 않는다. 이들 세 요소는 RPN에 대한 기여도를 모두 똑같이 1~10 사이의 수치로 평가하도록 되어 있다. 그런데 동일한 점수부여 규칙을 설명하고 있는 FMEA 매뉴얼에서조차 이들의 상대적 중요도가 모두 같지 않다는 점을 인정하고 있다. 예를 들어 심각도 점수가 큰 경우에는 RPN값이 비록 작다고 하더라도 해당 고장모드에 대한 특정한 주의를 기울일 것을 권고하고 있다.

둘째, 동일한 RPN값을 생성하는 심각도, 발생도 및 검출도의 조합은 여러 가지가 있지만 그 숨겨진 위험에 미치는 영향은 완전히 다를 수 있다. 예를 들어 심각도 8, 검출도 5, 발생도 3인 유형의 고장과 심각도 3, 검출도 5, 발생도 8인 유형의 고장은 RPN 값이 똑같은 120이지만 전자가 훨씬 더 위험한 것으로 받아들여진다.

셋째, 심각도, 발생도 및 검출도의 세 위험 인자에 대하여 객관적으로 정확하게 평가하기 어렵다. FMEA는 구성팀원의 주관적인 직관과 경험에 의존한다. 정량적인 데이터가 없는 상황에서 경험과 직관만으로 점수를 부여할 때 1~10점을 명확하게 분리하여 수치로 부여하기 어렵다. 일반적으로 정성적인 판단을 토대로 점수를 부여할 때는 상, 중, 하의 3단계 혹은 심한 부정, 약간부정, 보통, 약간긍정, 심한긍정의 5단계 평가정도까지 비교적 객관성 있게 할 수 있는 것으로 인정된다.

넷째, RPN을 계산하는 공식은 의심과 논쟁의 여지가 있다. 세 가지 구

성요소는 잘 추정되었다 하더라도 종합적인 위험의 척도는 세 요소의 곱으로 평가하는 것이 합리적인지는 여전히 논의되어야 할 문제로 남는다.

다섯째, 점수의 변환은 세 가지 위험요소에 따라 다르다. 각 요소별 점수 부여 규칙이 정해져 있으나 이 규칙에 따르는 것이 각 요소에 대한 공정한 점수 배분방식인지는 보증하기 어렵다. 예를 들어 2,000개당 1개 정도의 고장원인이 발생할 때 발생도 5를 부여하는 것과 보조기능이 저하되어 편의 기능을 못할 때 심각도 5를 부여하는 것이 과연 합당하며, 대등하게 취급할 수 있는가는 논쟁의 여지가 있다.

여섯째, RPN은 수정 조치의 효과성을 측정하기 위해 사용될 수 없다. 일반적으로 수정조치 여부는 RPN 값 100을 기준으로 결정한다. 만약 RPN 값 200인 고장모드에 대한 수정 조치결과 RPN 값이 100으로 감소되었다면 위험도 절반으로 줄어들었다고 할 수 있는가에 대한 부분도 회의적이다.

일곱째, RPNs의 점수부여 기준이 정밀하지 못하다. 예를 들어 발생도의 경우 2,000개당 1개 고장이면 5점, 10,000개당 1개이면 4점을 부여하게 되어 있다. 만약 5,000개당 1개 고장일 경우 몇 점을 부여하여야 하는지에 대한 판단기준이 없다.

여덟째, 다양한 고장모드 및 영향 사이의 상호의존성은 고려되지 않는다. 현실상황에서 어떤 유형의 고장들은 서로 얽혀 있어서 한 유형의 고장이 다른 유형의 고장의 발생을 촉진시키기도 하고 지연시키기도 한다. 이러한 문제를 기존 FMEA에서는 고려하지 않고 있다.

아홉째, RPN을 계산하기 위한 식의 형태는 위험요소 평가의 변화에 민감하다. 일반적으로 RPN값이 100이상인 경우 조치를 취해야 할 상황으로 판단한다. 예로써 $S=6$, $O=10$, $D=1$ 이면 $RPN=60$ 이 되어 문제가 없는 것

으로 판단하게 된다. 그런데 $D=2$ 가 더 합당한 것으로 여겨진다면 $RPN=120$ 으로 조치대상이 된다. 이처럼 RPN을 세 요소의 곱으로 산정함으로써 같은 유형의 고장을 두고 조치여부에 대한 결론이 양 극단으로 오가게 된다.

열 번째, RPN은 안전 측면에서 단지 세 가지의 위험 요소만 고려한다. 고장에 따른 위험은 RPN의 세 요소인 심각도, 발생도, 검출도 뿐만 아니라 이러한 고장유형이 어느 정도 치명적인 상황에 노출될 수 있는지, 발견 시 얼마나 신속하게 조치가 가능한지 등에도 상당히 영향을 받는다고 할 수 있다.

또한 Liu, et al.(2014)은 GRP(Grey Relational Projection) 방법을 기반으로 위험우선순위 모델을 제안하였으며, Sankar and Prabhu(2001)는 전통적인 RPN 방법보다 더 확장된 새로운 위험우선순위(RPNs)를 소개하였다. Wang et al.(2009)은 RPN의 세 가지 위험인자가 실제 상황에서는 정확하게 평가되기 어려우며 고장모드의 우선순위를 결정하기 위한 FRPNs(Fuzzy Risk Priority Numbers)를 제안하였으며, Xu et al.(2002)는 불확실하고 부정확한 정보와 다양한 고장모드 사이의 상호의존성을 Fuzzy-logic을 기반으로 한 방법을 소개하였다.

기타 FMEA의 일반적인 연구로는 Agung and Kwon(2012)은 서비스 FMEA에서의 수정조치 전략을 제안하였다. 또한 Jang(2015)은 FMEA에서 고장원인의 계층적 구조에 대한 위험평가 방법을 확률이론에 기초하여 계층적 고장원인 구조 하에서 FMEA 실시방법, 공통고장원인 발생문제, 원인과 고장사이에서 시간적인 지연이 있을 경우에 대한 연구를 진행하였다. Linton(2003)은 FMEA가 제조 프로세스에서와 유사한 방식으로 서비스 프

로세스의 개발에 도움이 될 수 있다고 주장하였고, Reiling et al.(2003)은 의료서비스에 FMEA의 적용을 제안하였다. Sawhney et al.(2004)은 공급업체 개발을 위해 FMEA 적용방안을 제안하였으며, Shahin (2004)은 고객의 관점을 강조한 카노모델과 FMEA 통합모형을 제안하였다. 또한 Teng et al.(2006)은 공동 공급망 환경에 적용하기 위한 FMEA를 연구하여 프로세스 지침을 제공하기도 하였다.

1.2.2 ISO 26262 선행연구

ISO 26262(2011)는 자동차 기능안전성 국제표준으로써 전기, 전자, 소프트웨어 컴포넌트로 구성된 안전관련 시스템의 안전 수명주기 동안 수행되는 모든 활동에 적용된다. 또한 위험평가 프로세스인 H&R을 통하여 안전 목표 및 ASIL을 결정하게 된다. ASIL은 아이템 개발에 있어서 안전요구사항의 평가지표가 되며, 제품개발에 앞서 가장 우선적으로 결정될 뿐만 아니라 시스템, 하드웨어 및 소프트웨어의 개발절차 및 적용기법을 결정하는 시스템개발의 핵심요소라 할 수 있다. 하지만 표준에서는 ASIL 결정을 위한 전체적인 가이드라인만 제공되며, 운전상황 결정요인 등에 대한 구체적인 방법론이 제시되어 있지 않다. 따라서 산업현장에서 ISO 26262 표준 적용을 위하여 본 연구에서 다루는 ASIL 결정방법론에 대한 구체적인 제시가 필요하다. ISO 26262와 관련한 선행연구 내용들 중에서 본 연구에서 다루고자 하는 위험평가 프로세스인 H&R 및 ASIL 결정과 관련한 연구를 다음과 같이 분석하였다. Cho et al.(2010)은 ISO 26262요건을 충족하면서 개발체계 수립에 참조할 수 있는 기능안전성 중심의 자동차 개발방법론을

소개하였고, Ellims and Monk-house(2011)와 Ellims et al.(2012)은 개념 설계 단계의 실증적 분석을 위해 휠 내장 전기모터(In-wheel Electric Motor) 사례를 적용하여 ASIL 결정에 관한 연구를 수행하였으며, Jesty et al.(2007)은 원인결함연결고리 모형(Casual Chain Linking Faults Model)을 기반으로 한 위험원 분석과 관련된 연구를 하였다. Kim and Jang(2011)은 하드웨어 ASIL의 정량적 평가절차에 대하여 연구하였으며, Lee and Jeon (2013)은 ASIL 달성을 위한 하드웨어 통합단계에 관한 연구를 하였다. Roh (2015)는 자동차 위험원 분석 및 리스크 평가 활동을 수행하는데 있어서 오류를 줄이고 일관성을 높이면서 위험평가에 대한 지식 데이터베이스 구축을 할 수 있도록 온톨리지를 이용한 위험원 분석 및 리스크 평가를 제안하였다. Schlummer et al.(2010)은 ISO 26262에서 안전과 신뢰성의 정량적 방법에 자동차 기능안전 프로세스를 적용하여 위험원 분석 및 평가절차에 관련한 연구를 수행하였다.

기타 ISO 26262의 일반적인 연구와 FMEA 등 2가지 위험평가기법을 접목한 연구에 대하여 조사하였다. Kim and Lee(2012), Xie et al. (2011), Zhang et al.(2010)은 기능안전 영역에 FMEA를 적용하기 위한 연구를 수행하였으며, Lim(2013)은 자동차개발 프로세스 안에서 FMEA를 시스템적으로 수행할 수 있는 방법과 ISO 26262 요구사항인 FMEA 수행을 위한 시스템 FMEA의 ISO 26262 적용에 관한 연구를 통해 자동차개발 프로세스가 가진 상세설계 및 양산 공정검증에 집중된 전통적 문제점을 보완할 수 있는 방법론을 제시하였고, ISO 26262의 효과적 수행은 물론, 차량개발 후반에 발생할 수 있는 시스템적 문제점을 줄이기 위한 선행적 방법론을 제시하였다. Rivett(2009) ISO 26262의 기반이 되는 IEC 61508의 방법론을 적용한 연구를 수행하였으며, Song(2013)은 ISO 26262와 APQP(Advan-

ced Products Quality Planning)를 접목하여 두 가지 개발 프로세스를 동시에 구현할 수 있는 효과적인 제품개발 프로세스 방안을 제시하였다.

아직까지 새로운 국제표준인 ISO 26262에 대한 연구의 대부분은 표준의 이해수준에 그치는 상황이다. 따라서 ISO 26262의 체계적이고 논리적인 ASIL 결정방법을 이용하여 FMEA의 위험평가 척도인 RPN의 단점을 보완하는 연구는 자동차 산업현장에서 현실적인 정보를 이용한 의사결정기준을 제공하고 기존 FMEA의 유용성을 높이기 위해 필요하다.

1.3 연구의 내용 및 구성

FMEA는 위험평가를 위한 유용한 도구이면서 많은 단점을 가지고 있다. 이러한 단점을 보완하기 위해 많은 연구가 진행되었지만 아직 해결되지 않은 부분이 많이 남아 있다. 특히 체계적이지 못하고 비논리적인 RPN 산정에 대하여 많은 학자들이 지적하고 있다. 그러나 FMEA는 제조, 건설, 서비스분야 등 다양한 분야에서 리스크 사전예방 기법으로 활용되고 있으므로 핵심 출력물인 RPN 결정절차에 대한 단점을 보완할 필요가 있다. 본 논문에서는 안전시스템을 위한 ASIL 결정에서 가장 중요한 단계인 위험사건분류와 관련된 절차들을 체계화하여 제시하고, ASIL의 강점을 이용하여 RPN의 단점을 보완하는 새로운 위험평가 척도로서 RPM(Risk Priority Metric)을 제안한다. 본 논문은 ASIL 기반의 새로운 리스크 평가 척도를 제시하기 위해 전체 내용을 다섯 개의 장으로 나누어 서술한다.

제 1장은 연구의 배경 및 목적 그리고 연구 내용 및 구성을 기술한 서론 부분으로서, 본 연구를 수행하게 된 동기와 배경을 기술한다. 또한 FMEA와 ISO 26262에 대한 선행연구를 통하여 기존의 문헌과 선행연구를 활용하여 새로운 위험척도인 RPM을 제시하기 위한 근거를 마련한다.

제 2장은 ASIL과 FMEA에 대하여 ISO 26262(2011) 국제표준과 FMEA Reference Manual(Chrysler, Ford and General Motors, 2008)을 근거로 한 위험평가를 소개하여 ASIL과 FMEA의 이해를 돕고자 한다.

선행연구 내용 중 본 연구와 유사하게 ISO 26262와 다른 기법을 접목한 연구를 정리하면 Table 1.4와 같다. 먼저 Song(2012)은 ISO 26262와 APQP를 접목하여 두 가지 개발프로세스를 동시에 구현할 수 있는 효과적인 제품개발 프로세스 방안에 제시하였고, Lim(2013)은 시스템 FMEA의 ISO 26262 적용에 관한 연구를 통하여 시스템적 문제점을 줄이기 위한 선행적 방법론을 제시하고 ISO 26262의 효과적 수행방법을 연구하였다. Kim and Lee(2012)는 ISO 26262 적용을 위한 소프트웨어 FMEA를 연구하여 FMEA의 대상이 되는 컴포넌트를 정의하는 방안, 고장모드 및 잠재적 고장원인 식별방법, 소프트웨어 FMEA 결과를 통합한 효과적인 안전메커니즘 설계과정을 제시하였다.

본 연구는 이러한 선행연구를 토대로 하여 제 3장에서는 ASIL 결정을 위한 기능안전 운전상황을 구체적으로 분석한다. ISO 26262 표준에서는 ASIL 결정을 위해 위험사건의 심각도, 노출확률 및 제어가능성을 평가하는데 그 과정이 구체적으로 표준화 되어있지 않아서 수행자의 주관적 관점에 의해 결과가 달라질 소지가 있다. 따라서 국제표준인 ISO 26262의 현장적용을 위한 운전상황의 분석모형을 제시하여 ASIL 결정을 위한 체계적이고 쉬운 접근이 가능하도록 한다.

제 4장은 H&R과 FMEA를 비교하여 ASIL에서 심각도 정보를 추출하는 개선된 위험척도인 RPM을 제안한다. FMEA는 각 고장에 대한 상대적인 리스크의 개략적 평가를 제공하는데 비해, RPM은 ASIL의 강점과 함께 단점을 보완하여 리스크평가의 보다 논리적이고 실제적인 절차를 제공한다. 또한 사례를 통하여 이론의 타당성과 유효성을 확인한다.

Table 1.4 Scope of studies

Criteria	Literature
ISO 26262 + APQP	Song(2013)
ISO 26262 + FMEA	Lim(2013), Kim and Lee(2012) Ch. 3 : H&R Ch. 4 : ASIL + RPN

마지막으로 제 5장에서는 연구의 결론부분으로 연구의 결과를 종합하고 요약하여 결과가 주는 의미와 시사점을 살펴보고 연구의 한계와 향후의 연구방향을 제시한다.

II. ASIL과 FMEA의 위험평가

2.1 ASIL의 위험평가

2.1.1 ISO 26262 개요

최근 안전하면서도 편리한 자동차에 대한 요구가 늘어남에 따라 자동차에 사용되는 ECU(Electronic Control Unit: 전자제어장치)의 수가 급속히 증가하고 있다. 이에 따라 ECU의 오작동에 의한 위험을 감소시키고 기능 안전성을 확보하기 위해 자동차 내 E/E(Electrical and/or Electronic: 전기/전자)시스템에 특화된 ISO 26262가 2011년 11월 제정되었다. 이 표준은 전기, 전자 및 소프트웨어 등의 구성품으로 이루어지는 안전관련 시스템의 안전수명주기 전반의 모든 활동에 적용된다. 기술진보에 따른 시스템의 복잡성이 증대되고 소프트웨어 적용이 확대됨에 따라 시스템고장이나 우발적 하드웨어 고장 등으로 인한 리스크가 증대되고 있으며, ISO 26262는 이러한 리스크를 효과적으로 방지하기 위해 필요한 요구사항과 프로세스에 대한 지침을 제공하고 있다.

IEC 61508을 기반으로 한 이 표준은 자동차의 E/E시스템에 대하여 개발에서 운영, 유지보수 그리고 폐기에 이르기까지 방대하고 포괄적인 내용을 다루고 있다. IEC 61508 표준은 일반 E/E시스템의 안전에 관한 포괄적 규격이라는 한계가 있었다.

Table 2.1 Comparison of IEC 61508 and ISO 26262

Section	IEC 61508	ISO 26262
name	Functional safety of electrical/electronic programmable electronic safety-related systems	Road vehicles-Functional safety
Configura- tion	Part 1~7	Part 1~10
Level	SIL 1~4 (SIL 1 is the lowest)	ASIL A~D (ASIL A is the lowest)
industry characte- ristics	Project, Process industry mainly	Mass production, Moving vehicle
user	In general it's fixed and operated by trained personnel	Normal driving license holder
Operation condition	fixed	Driving road is uncertain
Environ- mental condition	Analysis of possible environmental conditions for your area	Environmental conditions depending on the area to be used are non-specific
Maintenan- ce	Preventive, predictive maintenance carried out	The users determine the maintenance and preservation.
Durability Life	fixed	Not defined

중전의 차량 안전은 전통적으로 차량 기능별로 관련 규정과 형식승인을 통해 차량 안전보장을 요구해왔다. 하지만 자동차가 최근 기계장치 중심에서 전기전자장치 중심으로 발전하고 차량기능 간 통합 및 교류가 증가하면

서 선진국을 중심으로 기존 기계장치 중심의 형식승인을 전자장치 중심으로 강화한 규정 및 지침의 필요성이 대두되었다. 따라서 글로벌 자동차 메이커들을 중심으로 기존의 자동차를 비롯한 항공, 원자력 발전시스템, 기차, 의료 등 안전관련 시스템의 전기전자장치기능안전의 가장 포괄적인 표준인 IEC 61508을 자동차 분야에 적용해본 결과 도출된 문제점을 해소하기 위해 자동차분야의 특성을 반영한 새로운 표준의 필요성을 인식하게 되어 ISO 26262를 개발하였다. Table 2.1은 IEC 61508과 ISO 26262의 차이점을 비교한 자료이다.

ISO 26262는 3,500Kg 이하의 차량에 하나 이상의 E/E 시스템을 포함하는 양산 승용차에 설치되는 안전관련 시스템에 적용하기 위한 표준으로 다음과 같은 목적을 가지고 있다. 첫째, ISO 26262는 기능안전성을 확보하기 위하여 각 단계별로 수행되는 제반 활동에 관한 요구사항을 명시하고 각 기업의 상황에 따라 맞춤화할 수 있도록 지원한다. 둘째, 자동차 분야의 특성을 반영한 안전무결성 수준인 ASIL 등급을 결정할 수 있도록 한다. 셋째, 제품의 잔류 리스크를 방지하기 위하여 ASIL 등급에 따라 적용할 수 있는 요구사항을 제시하고 있다. 넷째, 충분하고 만족스러운 안전수준이 달성되고 있음을 보장하기 위한 타당성확인(Validation) 및 입증(Confirmation)을 위한 수단(Measure)이 갖추어야 할 요구사항을 제시한다. 다섯째, 안전관련 전장품의 개발은 하드웨어 개발뿐만 아니라 소프트웨어 개발과 이들 간의 통합이 요구되므로 공급자와의 관계는 매우 중요하다. 따라서 제품개발 시 공급자와의 관계에 관한 요구사항을 제시하고 있다.

ISO 26262는 여러 단계의 제품개발을 위하여 Figure 2.1과 같은 V모형의 기준 프로세스 모델을 사용하고 있으며, 총 10개의 Part로 구성되어 있다.

Part 1 (Vocabulary: 용어)은 자동차 기능안전관련 용어를 정의한다.

Part 2 (Management of functional safety: 기능안전성 관리)는 기능안전성에 관련된 개발활동을 계획, 조정, 추적하는 요구사항을 정의하고 안전문화와 같이 조직차원에서 갖추어야 할 아이템(Item) 개발, 생산 이후에 걸친 전반적 안전경영 요구사항을 정의한다.

Part 3 (Concept phase: 개념단계)은 개발 아이টে에 대한 정의를 기반으로 위험원 분석 및 리스크 평가(H&R)을 통해 ASIL을 판정하는 방법과 안전 목표와 안전 메커니즘을 정의한다. Part 3는 제품개발 활동 초반에 수행해야 할 기본적인 단계로써 위험원 분석 및 리스크 평가를 통하여 안전 목표를 수립하고, 결정되는 ASIL 등급을 토대로 시스템, 하드웨어, 소프트웨어의 개발절차 및 적용기법을 결정하는 중요한 부분이다.

Part 4 (Product development at the system level: 시스템수준의 제품개발)는 전기전자시스템 이외 타 기술로 구현된 안전메커니즘의 타당성확인(Validation), 외부 수단으로 구현된 안전개념의 효과확인, 사람의 통제가능성 및 작동작업에 대한 전제 등의 검증(Verification) 활동 등으로 V모형에 따르는 시스템수준의 개발 및 기술적 요구사항을 정의한다.

Part 5 (Development at the hardware level: 하드웨어 수준의 제품개발)는 아이টে의 하드웨어 개발단계로 하드웨어 수준의 요구사항, 하드웨어 설계, 통합 및 검증활동에 대하여 정의한다.

Part 6 (Development at the Software level: 소프트웨어 수준의 제품개발)은 소프트웨어 수준의 요구사항 정의, 아키텍처 설계, 유닛(Unit) 설계 및 구현, 통합, 검증활동에 대하여 정의한다.

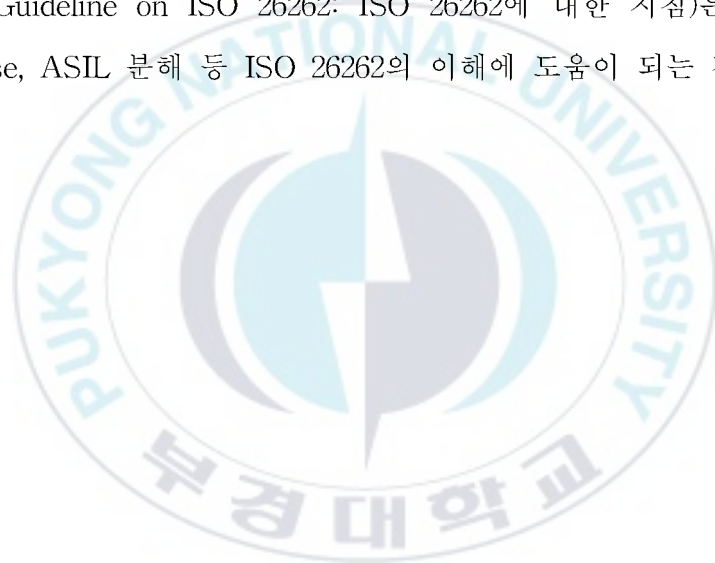
Part 7 (Production and operation: 생산 및 운용)은 엘리먼트나 아이টে의 생산을 위한 계획, 양산선행, 양산, 서비스, 폐기 등에 관한 요구사항을 정

의한다.

Part 8 (Supporting processes: 지원 프로세스)은 협력개발(DIA), 안전요구 사항의 명세 및 관리방법, 형상관리, 변경관리, 검증 등에 관한 요구사항을 정의한다.

Part 9 (ASIL-oriented and safety-oriented analysis: ASIL 및 안전기반 분석)는 자동차 안전무결성 수준(ASIL)의 결정을 위한 안전기반 분석방법론 등에 대하여 기술한다.

Part 10 (Guideline on ISO 26262: ISO 26262에 대한 지침)은 주요개념, Safety case, ASIL 분해 등 ISO 26262의 이해에 도움이 되는 정보를 기술한다.



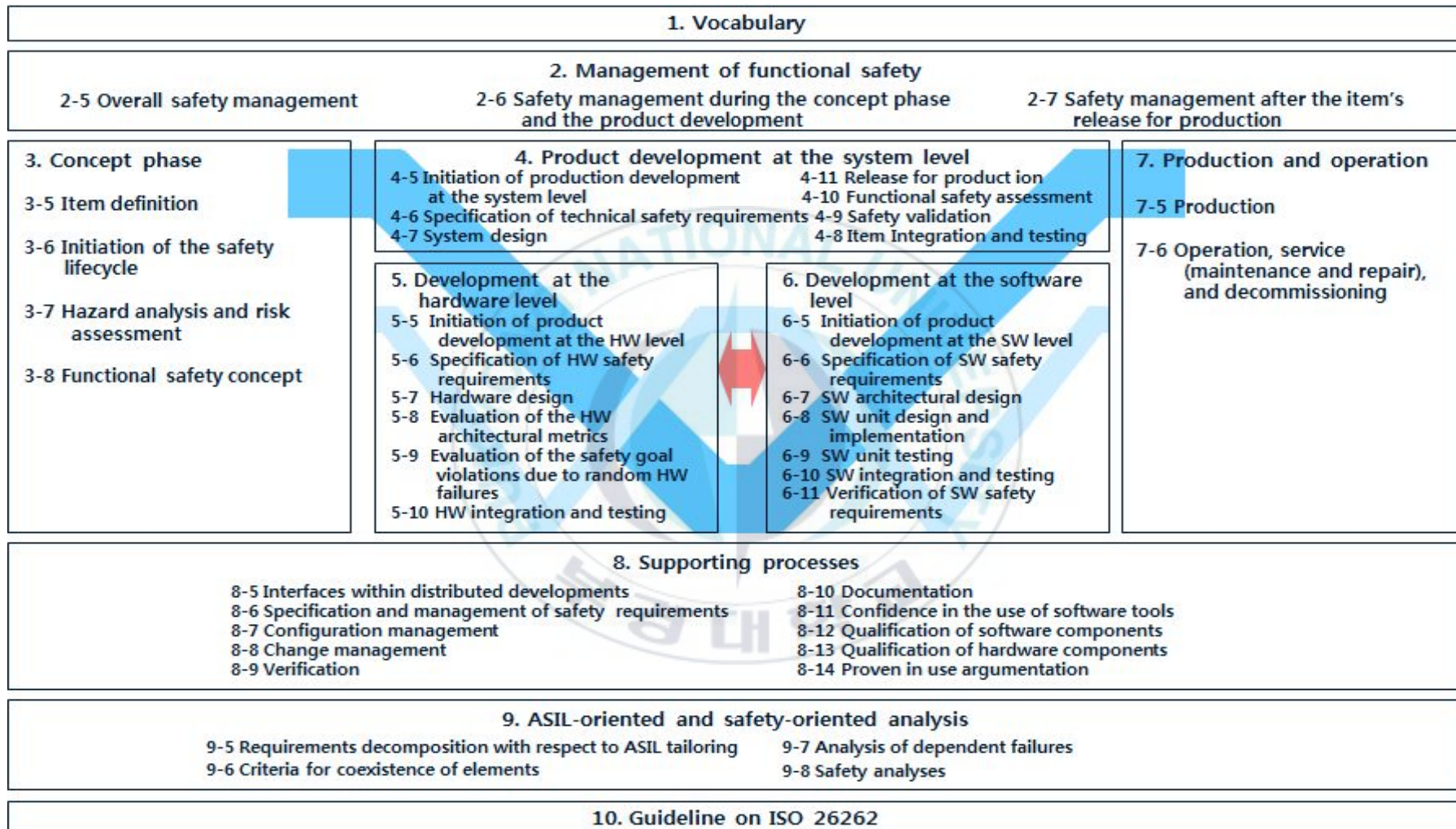


Figure 2.1 Overview of ISO 26262

2.1.2 위험원 분석 및 리스크 평가(H&R)

위험원 분석 및 리스크 평가(H&R)는 비합리적인 리스크를 방지하기 위해 아이템의 오동작이 유발시킬 수 있는 위험원(Hazard)을 식별하고 분류하여 위험사건의 예방 또는 완화와 관련된 안전 목표를 수립하는 것으로 Figure 2.1의 Part 3. 개념단계에서 실행된다.

아이템의 안전 목표는 비합리적 리스크 방지를 위해 H&R 및 ASIL 등급 결정을 토대로 수립되며, 안전 목표와 각 목표별 할당된 ASIL은 위험사건의 체계적인 평가를 통하여 심각도, 노출확률, 제어가능성 등 영향요소의 추정치를 고려하여 결정된다. ASIL은 H&R의 주요 출력물로서, 자동차 E/E 아이템의 기능 고장으로 인한 위험사건 발생의 리스크를 반영한다. H&R은 상황분석과 위험원 식별, 위험사건의 분류 및 ASIL 결정의 세 단계로 진행된다.

2.1.2.1 상황분석과 위험원 식별

상황분석과 위험원 식별은 위험사건을 야기할 수 있는 아이템의 잠재적이고 의도하지 않은 동작을 식별하는 것이다. 상황분석은 아이템의 오동작이 위험사건을 초래하는 운용상황과 운용모드를 기술하고, 위험원은 브레인스토밍(brainstorming), 체크리스트, 품질이력, FMEA, 현장조사 등 적합한 기법을 사용하여 체계적으로 결정된다.

2.1.2.2 위험사건의 분류

ISO 26262의 적용범위를 벗어난 것을 제외한 식별된 모든 위험사건은 분류되어야하며, 분류체계는 아이템의 위험사건과 관련된 심각도, 노출확

를, 제어가능성의 결정으로 구성된다.

1) 심각도(Severity)

심각도는 운전상황 및 시스템 고장을 고려하여 사람에게 끼칠 수 있는 잠재적인 위해(harm)의 정도를 추정한 것으로, 주어진 위험원에 대한 심각도를 결정하기 위해 운전자, 승객 및 차량 주변의 개인 등에 대하여 잠재적인 상해가 평가된다. 심각도는 S0, S1, S2, S3 네 개의 등급으로 분류되며, 각 위험사건에서 치명적인 부상에 대하여 S3, 부상이 없으면 S0이 부여된다. 심각도를 정하기 위해 약식상해등급(Abbreviated Injury Scale: AIS)를 참조할 수 있으며, AIS는 미국자동차의학진흥협회(Association for the Advancement of Automotive Medicine: AAAM)에 의해 개발된 것으로 부상 심각도를 정도에 따라 7등급으로 분류한다.

- AIS 0 : 부상 없음
- AIS 1 : 깊이 않은 상처, 근육 통증, 목뼈골절(whiplash) 등과 같은 경미한 부상
- AIS 2 : 깊은 상처, 15분 이내의 무의식 상태의 뇌진탕, 단순 장골 골절, 단순 늑골 골절 등과 같은 중간수준의 부상
- AIS 3 : 뇌 손상 없는 두개골 골절, 척추 손상 없는 4번 척추 아래 탈구, 역식 호흡 없는 하나 이상의 갈비뼈 골절 등과 같은 심각한 부상이지만 생명을 위협하지 않는 부상
- AIS 4 : 최대 12시간까지 무의식과 두개골 골절 또는 비 골절을 동반한 뇌진탕 및 역식호흡과 같은 심각한 부상(생명 위협, 생존 가능)

Table 2.2 Classification example and classes of severity

	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival)
Reference for single injuries (from AIS scale)	-AIS 0 and less than 10 % probability of AIS 1-6 -Damage that cannot be classified safety-related	More than 10 % probability of AIS 1-6 (and not S2 or S3)	More than 10 % probability of AIS 3-6 (and not S3)	More than 10 % probability of AIS 5-6
Examples	-Bumps with roadside infrastructure -Pushing over roadside post, fence, etc. -Light collision -Light grazing damage	-Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with very low speed -Side collision with a passenger car (e.g. intrudes upon passenger compartment) with very low speed	-Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with low speed -Side collision with a passenger car (e.g. intrudes upon passenger compartment) with low speed	-Side impact with a narrow stationary object, e.g. crashing into a tree (impact to passenger cell) with medium speed -Side collision with a passenger car (e.g. intrudes upon passenger compartment) with medium speed

Examples	-Damage entering/exiting parking space -Leaving the road without collision or rollover	-Rear/front collision with another passenger car with very low speed -Collision with minimal vehicle overlap (10% to 20%) -Front collision (e.g. rear-ending another vehicle, semi-truck, etc.) without passenger compartment deformation	-Rear/front collision with another passenger car with low speed -Pedestrian/bicycle accident while turning (city intersection and streets)	-Rear/front collision with another passenger car with medium speed -Pedestrian/bicycle accident (e.g. 2-lane road) -Front collision (e.g. rear-ending another vehicle, semi-truck, etc.) with passenger compartment deformation
----------	---	---	---	---

- AIS 5 : 척추에 손상을 동반한 4번 척추 아래 척추 골절, 장 파열, 심장파열, 뇌출혈을 포함한 12시간 이상 무의식과 같은 치명적인 부상(생명 위협, 생존 불확실)
- AIS 6 : 척추에 손상을 동반한 3번 척추 아래 척추 골절, 체강이 매우 심하게 개봉된 상처와 같은(흉곽과 복부에 구멍) 극도로 위험하거나 치명적인 부상

Table 2.2는 심각도 등급과 AIS에 따른 심각도 분류 예시를 나타낸 것이다.

2) 노출확률(Probability of exposure)

노출은 위험원이 될 수 있는 운용상황에 있는 상태를 말한다. 각 운영상황의 노출확률은 각 위험사건에 대한 이론적 해석을 기반으로 추정되며, 노출확률을 추정하려면 위험원 발생에 기여하는 관련 환경요소가 있는 시나리오를 평가해야 한다. 평가되는 시나리오는 운전이나 운용상황을 광범위하게 포함한다. 노출확률은 위험원 발생을 야기하는 관련된 환경 인자가 있는 운전상황의 지속시간이나 발생빈도로 평가한다. 노출확률의 등급 분류는 운용상황에 따라 적합한 기준을 사용하며, 최저 수준인 E0에서 최고 수준인 E4로 5가지로 구분된다. 지진, 허리케인, 산불 등 자연 재해와 아주 드물거나 불가능한 상황의 동시발생은 E0가 부여되며, E0 시나리오에만 관련된 위험원의 평가는 향후 분석에서 제외될 수 있다.

Table 2.3 Classes of probability of exposure regarding duration in operational situations

Description	E1		E2		E3		E4	
	Very low probability		Low probability		Medium probability		High probability	
Duration (% of average operating time)	Not specified		<1 % of average operating time		1 % to 10 % of average operating time		>10 % of average operating time	
Road layout	-		-Mountain pass with unsecured steep slope -Country road intersection -Highway entrance ramp -Highway exit ramp		-One-way street (city street)		-Highway -Secondary road -Country road	

E x a m p l e s	Road surface	-	-Snow and ice on road -Slippery leaves on road	-Wet road	-
	Nearby elements	-Lost cargo or obstacle in lane of travel (highway)	-In car wash Nearing end of congestion (highway)	-In tunnel -Traffic congestion	-
	Vehicle stationary state	-Vehicle during jump start -In repair garage(on roller rig)	-Trailer attached -Roof rack attached -Vehicle being refuelled -In repair garage (during diagnosis or repair) -On hoist	-Vehicle on a hill (hill hold)	-
	Manoeuvre	-Driving downhill with engine off (mountain pass)	-Driving in reverse (from parking spot) -Driving in reverse (city street) -Overtaking Parking (with sleeping person in vehicle) -Parking (with trailer attached)	-Heavy traffic (stop and go)	-Accelerating -Decelerating -Executing a turn (steering) -Parking (parking lot) -Lane change (city street) -Stopping at traffic light (city street) -Lane change (highway)
	Visibility	-	-	-Unlighted roads at night	-

**Table 2.4 Classes of probability of exposure regarding frequency
in operational situations**

Description		E1	E2	E3	E4
		Very low probability	Low probability	Medium probability	High probability
Frequency of situation		Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average
E x a m p l e s	Road layout	-	-Mountain pass with unsecured steep slope	-	-
	Road surface	-	-Snow and ice on road	-Wet road	-
	Nearby elements	-	-	-In tunnel -In car wash -Traffic congestion	-
	Vehicle stationary state	-Stopped, requiring engine restart (at railway crossing) -Vehicle being towed -Vehicle during jump start	-Trailer attached -Roof rack attached	-Vehicle being refuelled -Vehicle on a hill (hill hold)	-

	Manoeuv re	-	-Evasive manoeuvre, deviating from desired path	-Overtaking	-Starting from standstill -Shifting transmission gears -Accelerating -Braking -Executing a turn(steering) -Using indicators -Manoeuvring vehicle into parking position -Driving in reverse
--	---------------	---	--	-------------	--

Table 2.3은 운용상황의 시간과 관련된 노출확률 등급 및 예시를 나타내고 있으며, Table 2.4는 운용상황의 빈도와 관련된 노출확률 등급 및 예시를 나타낸다.

3) 제어가능성(Controllability)

제어가능성은 운전자나 잠재적 위험에 놓인 다른 사람이 위험사건을 충분히 제어할 수 있어 특정한 위해를 피할 수 있는 확률을 나타내며, 브레이크 고장, 고속 주행 시 에어백 해제 등의 운전 인자와 위험사건의 조합에 의한 운전시나리오로부터 추정한다. 제어가능성은 C0, C1, C2, C3 네 개의 등급으로 분류되며, 제어하기 어렵거나 제어 불가능한 것은 C3, 제어가능한 것은 C0로 분류된다. Table 2.5는 위험사건을 충분히 제어할 수 있어 위해를 피할 수 있는 제어가능성 등급 및 예시를 나타낸다.

Table 2.5 Classification examples and classes of controllability

Description		C0	C1	C2	C3
		Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
Driving factors and scenarios		Controllable in general	99 % or more of all drivers or other traffic participants are usually able to avoid harm	90 % or more of all drivers or other traffic participants are usually able to avoid harm	Less than 90 % of all drivers or other traffic participants are usually able, or barely able, to avoid harm
E x a m p l e s	Situations that are considered distracting	-Maintain intended driving path	-	-	-
	Unexpected radio volume increase	-Maintain intended driving path	-	-	-
	Warning message - gas low	-Maintain intended driving path	-	-	-
	Unavailability of a driver assisting system	-Maintain intended driving path	-	-	-
	Faulty adjustment of seat position while driving	-	-Brake to slow/stop vehicle	-	-
	Blocked steering column when starting the vehicle	-	-Brake to slow/stop vehicle	-	-

Failure of ABS during emergency braking	-	-	-Maintain intended driving path	-
Headlights fail while night driving at medium/high speed on unlighted road	-	-	-Steer to side of road or brake to stop	-
Motor failure at high lateral acceleration (motorway exit)	-	-	-Maintain intended driving path	-
Failure of ABS when braking on low friction road surface while executing a turn	-	-	-	-Maintain intended driving path, stay in lane
Failure of brakes	-	-	-	-Brake to slow/stop vehicle
Incorrect steering angle with high angular speed at medium or high vehicle speed (steering angle change not aligned to driver intent)	-	-	-	-Maintain intended driving path, stay in lane
Faulty driver airbag release when travelling at high speed	-	-	-	-Maintain intended driving path, stay in lane -Brake to slow/stop vehicle

2.1.2.3 ASIL 결정 및 수행

ASIL은 앞에서 설명한 심각도, 노출확률, 제어가능성 세 가지 요소의 추정 등급을 기반으로 Table 2.6과 같이 결정되며, 시스템 개발에서 가장 우선적으로 결정될 뿐만 아니라 제품의 안전요구사항 평가지표를 제공하기 때문에 시스템 개발의 핵심 요소라고 할 수 있다. 위험 사건을 위하여 결정된 ASIL은 안전 목표에 부합하게 지정되어야 하며, 부적절하게 낮은 ASIL 등급을 이끌지 않도록 하여야한다. ASIL은 A, B, C, D 등급으로 구분되며, ASIL A는 최저 안전무결성 수준, ASIL D는 최고 안전무결성 수준을 나타낸다. ASIL A~D 등급 외에 추가된 QM(품질경영) 등급은 품질경영시스템 외에 따로 ISO 26262를 준수하기 위한 요건이 필요하지 않음을 의미한다.

Table 2.6 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

ASIL 등급이 정해지면 등급에 따라 제시된 방법과 기법을 활용하여 수행하여야 하며, Table 2.7 및 Table 2.8은 시스템 설계 단계에서 ASIL 등급에 따른 수행 방법과 기법을 나타낸다.

Table 2.7 System design analysis

Methods		ASIL			
		A	B	C	D
1	Deductive analysis	o	+	++	++
2	Inductive analysis	++	++	++	++
- Deductive analysis methods include FTA, reliability block diagrams, Ishikawa diagram. - Inductive analysis methods include FMEA, ETA, Markov modelling.					

Table 2.8 Properties of modular system design

Methods		ASIL			
		A	B	C	D
1	Hierarchical design	+	+	++	++
2	Precisely defined interfaces	+	+	+	+
3	Avoidance of unnecessary complexity of hardware components and software components	+	+	+	+
4	Avoidance of unnecessary complexity of interfaces	+	+	+	+
5	Maintainability during service	+	+	+	+
6	Testability during development and operation	+	+	++	++

“++”로 구분된 ASIL은 방법이 매우 권장된다는 것을 나타낸다.

“+”로 구분된 ASIL은 방법이 권장된다는 것을 나타낸다.

“o”로 구분된 ASIL은 사용에 관한 권장사항이 없다는 것을 나타낸다.

2.2 FMEA의 위험 평가

2.2.1 FMEA 개요

FMEA는 시스템, 제품 및 공정의 잠재적인 고장모드와 그 영향을 분석하여 잠재적 고장의 발생기회를 제거하거나 줄일 수 있는 조치를 취하고 이를 문서화하기 위한 체계적인 활동이다. 1950년대 초 프로펠라 추진항공기가 제트엔진 항공기로 전환되면서 유압장치가 전기장치로 구성되는 복잡한 조종시스템을 가진 제트기의 신뢰성 설계를 위해 사용된 것을 효시로 하여 1960년대에 NASA에서 우주선 개발 시 각 부품의 오기능을 브레인스토밍 방법으로 예측하려는 활동에 사용하였으며, 1980년대 포드 엔지니어들에 의해 자동차산업에 도입되어 지금은 제조뿐만 아니라 서비스 산업에서도 매우 보편적으로 사용되는 품질개선 및 신뢰성 관리의 필수적 요건으로 간주되고 있는 분석기법이다.

FMEA는 구성요소의 고장모드를 서브시스템에서 시스템으로 고장의 영향을 Bottom Up 방식으로 예측하는 기법으로, 정해진 구성요소가 발생할 수 있는 고장모드를 예측하고 기능 블록도에 따라 차례로 고장의 영향을 검토하여 문제점을 추출하는 것이다. FMEA는 용도에 따라 Table 2.9와 같이 구분되는데 시스템 기능상 고장과 영향을 최소화하기 위한 시스템 FMEA, 설계단계에서 전체 시스템에 미치는 고장을 최소화하기 위한 설계 FMEA, 공정상의 고장 발생을 최소화하기 위한 공정 FMEA, 설비의 고장과 고장영향을 최소화하기 위한 설비 FMEA, 서비스 관련 고장 및 결함이 발생하는 것을 최소화하기 위한 서비스 FMEA 등으로 구분한다.

Table 2.9 Types of FMEA

Section	Purpose	Effect
System FMEA	Minimize the effect of failure and fault occurring function in the system	Maximize of Quality, reliability, cost, maintainability
Design FMEA	Minimize the effect of faults for design on the entire system	Maximize of Quality, reliability, cost, maintainability
Process FMEA	Minimize that the failure occurs in the system or process	Maximize of system of quality, reliability, cost, maintainability, productivity
Machinery FMEA	Minimize the failure and the failure effect of equipment	Maximize of system of quality, reliability, cost, maintainability, productivity
Service FMEA	Minimize that service-related failure or defect is generated from the organization	Achieve customer satisfaction by maximizing quality reliability and service improvement

FMEA는 신제품, 신 공정개발 시 또는 제품 및 공정 변경 시 잠재적 고장모드를 구조적으로 분석하여 고장을 사전에 예방하고 체계적인 정보를 제공하여 제품 또는 공정의 중점관리대상을 선정하는 기준으로 활용되고 있다. FMEA의 전개는 제품 및 공정을 개발하거나 변경이 발생할 경우 관련 부서의 팀원을 주축으로 팀을 구성한 후 다음과 같은 주요 프로세스로 진행된다.

첫째 기능을 정의하여 대상물의 임무, 기능을 명확히 확인한다.

둘째 대상물을 기능별로 분해하고 어느 수준까지 분석할 것인지에 대한 분석 레벨을 결정한다.

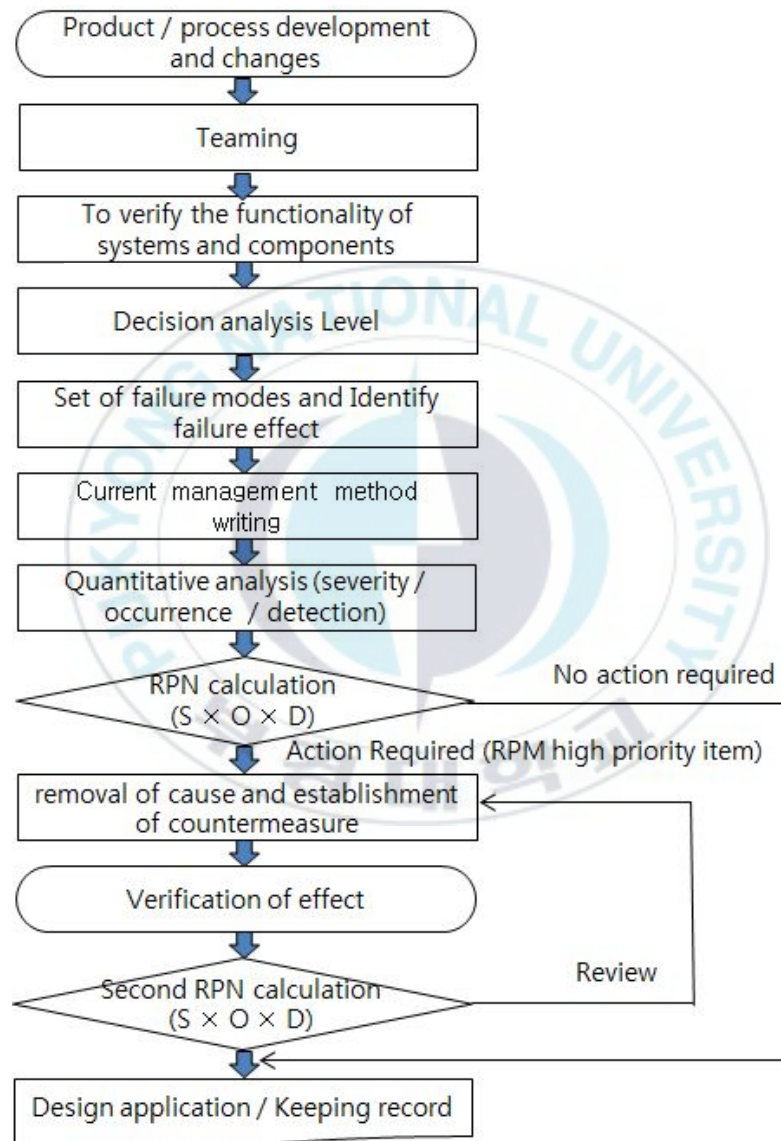


Figure 2.2 Action process in FMEA

셋째 과거의 고장 경험 또는 고장발생 등을 참고하여 예측되는 고장모드 (잠재적 고장모드 포함)를 열거한다.

넷째 고장모드가 발생하였을 경우 고장의 영향을 파악하고 원인을 추정한다.

다섯째 현재의 예방설계, 안전검증(주행시험, 설계검토, 불량방지 장치 등) 활동 등 현재 관리방법을 기술한다.

여섯째 평가기준에 따른 심각도, 발생도, 검출도의 등급을 산정하여 정량 분석을 실시한다.

일곱째 분석된 심각도, 발생도, 검출도를 곱하여 위험우선순위(RPN)를 산정하여 대책 및 조치가 불필요한 경우 설계에 반영하고 기록을 유지한다.

여덟째 재검토가 요구되는 항목은 고장원인을 제거하고, RPN이 높은 항목 별로 대책을 수립한다.

아홉째 수립된 대책에 따른 조치 결과에 대한 효과성을 검증한다.

열번째 수립된 대책과 조치 결과에 따른 심각도, 발생도, 검출도를 재평가 하여 RPN을 재 산정한 다음 별도의 대책과 조치가 불필요한 경우 설계에 반영한다.

2.2.2 위험평가

FMEA는 신제품의 설계 및 기존 제품의 설계 변경 시 적용하여 예상되는 불량문제, 고장문제, 안전문제 등을 검토하여 RPN이 낮을 경우에는 설계수정 없이 진행될 수 있지만, 고장 등급 또는 RPN이 정해진 기준 값 이

상이 될 경우에는 재검토하여 이에 대한 대책이 수립되어야 한다. RPN은 잠재적인 문제의 심각도, 발생도, 검출도를 곱한 값으로 각각의 값은 1에서 10의 값을 갖는다. 따라서 RPN 값은 1에서 1000까지의 값을 가질 수 있다. RPN의 값이 1이면 위험성이 거의 없는 것이지만 100이상이 넘어가면 위험성이 점차 커지는 것을 의미하며, 높은 RPN에 대하여 위험을 줄이기 위한 우선적인 노력이 필요하다. 하지만 일반적으로 RPN 값에 관계없이 심각도가 높은 고장모드에 대하여 특별한 주의를 기울여 대책을 수립하고 우선적으로 개선하는 것이 권장된다.

2.2.2.1 심각도(Severity)

심각도는 고장의 잠재적인 영향의 정도, 즉 잠재적 고장모드가 그 다음의 Component, Subsystem, System 또는 고객에게 미치는 영향의 정도를 말한다. 심각도는 RPN의 가장 중요한 구성요소로서 RPN의 점수에 상관없이 심각도가 높은 고장모드에 우선적으로 주의를 기울여야 한다. 고장 영향의 심각도(S)는 1~10사이의 숫자로 평가되며, 10이 가장 심각한 영향을 나타낸다. 심각도는 고장모드의 가장 높은 등급만 관리하며, Table 2.10은 심각도 등급을 평가하기 위한 기준을 나타낸다.

Table 2.10 Evaluation criteria of severity in FMEA

Effect	Severity of effect on product(Customer effect)	Rank	Effect	Severity of effect on process(Manufacturing/Assembly effect)
Failure to meet safety and/or regulatory requirement	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation without warning	10	Failure to meet safety and/or regulatory requirement	May endanger operator(machine or assembly) without warning
	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation with warning	9		May endanger operator(machine or assembly) with warning
Loss or degradation of primary function	Loss of primary function(vehicle inoperable, does not affect safe vehicle operation)	8	Major disruption	100% of product may have to be scrapped. Line shutdown or stop ship
	Degradation of primary function(vehicle operable, but at reduced level of performance)	7	Significant disruption	A portion of the production run may have to be scrapped. Deviation from primary process including decreased line speed or added manpower
Loss or degradation of secondary function	Loss of secondary function(vehicle operable, but comfort/convenience function inoperable)	6	Moderate disruption	100% of production run may have to be reworked off line and accepted
	Degradation of secondary function(vehicle operable, but comfort/convenience function at reduced level of performance)	5		A portion of the production run may have to be reworked off line and accepted

Annoyance	Appearance or audible noise, vehicle operable, item does not conform and noticed by most customers (>75%)	4	Moderate disruption	100% of production run may have to be reworked in station before it is processed
	Appearance or audible noise, vehicle operable, item does not conform and noticed by many customers (50%)	3		A portion of the production run may have to be reworked in station before it is processed
	Appearance or audible noise, vehicle operable, item does not conform and noticed by discriminating customers (<25%)	2	Minor disruption	Slight inconvenience to process, operation, or operator
No effect	No discernible effect	1	No effect	No discernible effect

2.2.2.2 발생도(Occurrence)

발생도는 잠재적인 고장원인 및 메카니즘이 발생할 가능성의 정도를 말한다. 발생도는 1~10의 숫자로 평가되며, 특정 원인의 발생가능성이 높은 것은 10, 거의 가능성이 없는 것은 1로 부여한다. 각 고장모드에는 여러 가지 원인이 있을 수 있으며, 발생도 등급은 주어진 고장모드의 각 원인마다 적절하게 부여된다. 등급부여는 유사부품의 서비스 이력, 필드 이력, 신품 또는 이관부품 여부, 적용변경 여부, 환경변화 등의 합리적 근거를 고려하여야 한다. Table 2.11은 FMEA에서 발생도 등급을 평가하기 위한 기준을 나타낸다.

Table 2.11 Evaluation criteria of occurrence in FMEA

Likelihood of failure	Occurrence of cause		Rank
	Design life/reliability of item/vehicle	Incidents per items/vehicle	
Very high	New technology/new design with no history	≥ 100 per thousand ≥ 1 in 10	10
High	Failure is inevitable with new design, new application, or change in duty cycle/operating conditions	50 per thousand 1 in 20	9
	Failure is likely with new design, new application, or change in duty cycle/operating conditions	20 per thousand 1 in 50	8
	Failure is uncertain with new design, new application, or change in duty cycle/operating conditions	10 per thousand 1 in 100	7
Moderate	Frequent failures associated with similar design or in design simulation and testing	2 per thousand 1 in 500	6
	Occasional failures associated with similar design or in design simulation and testing	0.5 per thousand 1 in 2,000	5
	Isolated failures associated with similar design or in design simulation and testing	0.1 per thousand 1 in 10,000	4
Low	Only isolated failures associated with almost identical design or in design simulation and testing	0.01 per thousand 1 in 100,000	3
	No observed failures associated with almost identical design or in design simulation and testing	≤ 0.001 per thousand 1 in 1,000,000	2
Very low	Failure is eliminated through preventive control		1

2.2.2.3 검출도(Detection)

검출도는 현재의 관리방법으로 고장원인을 검출하거나 고장모드를 검출할 수 있는 능력이다. 검출도 역시 1~10의 숫자로 평가되며, 검출 가능성이 거의 없을 경우 10, 검출 가능성이 거의 확실 할 때는 1이 부여된다. 검출도 등급이 감소되기 위해서는 계획된 설계관리(예방, 유효성확인, 검증활동)가 개선되어야 한다. Table 2.12는 FMEA에서 검출도 등급을 평가하기 위한 기준을 나타낸다.

Table 2.12 Evaluation criteria of detection in FMEA

Likelihood of detection by design control		Rank	Likelihood of detection	Likelihood of detection by process control	
No detection opportunity	No current design control; Cannot detect or is not analyzed	10	Almost impossible	No detection opportunity	No current process control; Cannot detect or is not analyzed
Not likely to detect at any stage	Design analysis/detection controls have a weak detection capability; Virtual analysis(e.g., CAE, FEA, etc) is not correlated to expected actual operating conditions	9	Very remote	Not likely to detect at any stage	Failure mode and/or error(cause) in not easily detected(e.g., random audits)
Post design freeze and prior to launch	Product verification/validation after design freeze and prior to launch with pass/fail testing(subsystem or system testing with acceptance criteria such as ride and handling, shipping evaluation, etc.)	8	Remote	Problem detection on post processing	Failure mode detection post-processing by operator through visual/tactile/audible means

	Product verification/ validation after design freeze and prior to launch with test to failure testing(subsystem or system testing until failure occurs, testing of system interactions, etc.)	7	Very low	Proble m detecti on at source	Failure mode detection in-station by operator through visual/tactile/ audible means or post-processing through use of attribute gauging (go/no-go, manual torque check/clicker wrench, etc.)
	Product verification/validation after design freeze and prior to launch with degradation testing(subsystems or system testing after durability test, e.g., function check)	6	Low	Proble m detecti on post process ing	Failure mode detection post-processing by operator through use of variable gauging or in-station by operator through use of attribute gauging(go/no-go, manual torque check/clicker wrench, etc.)
Prior to design freeze	Product validation (reliability testing, development or validation tests) prior to design freeze using pass/fail testing(e.g., acceptance criteria for performance, function checks, etc.)	5	Moderate	Proble m detecti on at source	Failure mode or error(cause) detection in-station by operator through use of variable gauging or by automated controls in-station that will detect discrepant part and notify operator(light, buzzer, etc.). gauging performed on setup and first-price check(for set-up cause only)
	Product validation (reliability testing, development or validation tests) prior to design freeze using test to failure(e.g., until leaks, yields, cracks, etc.)	4	Moderately high	Proble m detecti on post process ing	Failure mode detection post-processing by automated controls that will detect discrepant part and lock part to prevent further processing

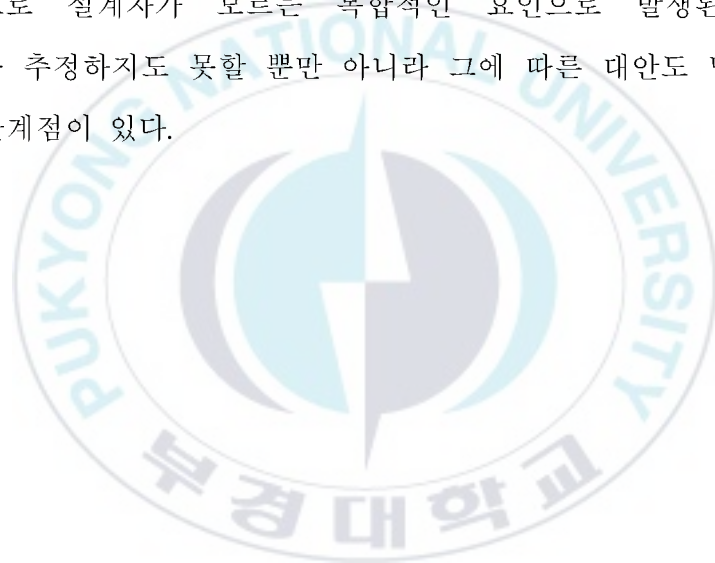
	Product validation (reliability testing, development or validation tests) prior to design freeze using degradation testing(e.g., data trends, before/after value, etc.)	3	High	Problem detection at source	Failure mode detection in-station by automated controls that will detect discrepant part and automatically lock part in station to prevent further processing
Virtual analysis-correlated	Design analysis/detection controls have a strong detection capability. Virtual analysis(e.g., CAE, FEA, etc) is highly correlated with actual or expected operating conditions prior to design freeze	2	Very high	Error detection and/or problem prevention	Error(cause) detection in-station by automated controls that will detect error and prevent discrepant part from being made
Detection not applicable; failure prevention	Failure cause or failure mode can not occur because it is fully prevented through design solutions(e.g., proven design standard, best practice or common material, etc.)	1	Almost certain	Detection not applicable; error prevention	Error(cause) prevent as a result of fixture design, machine design or part design. Discrepant part cannot be process/product design

2.2.2.4 위험우선순위(RPN) 결정

FMEA는 고장원인에 대한 시정 또는 예방활동의 우선순위를 결정하기 위해 RPN(Risk Priority Number: 위험우선순위)을 사용한다. RPN은 고장원인에 대한 심각도(S), 발생도(O), 및 검출도 (D)를 평가 한 후, 이들의 곱에 의해 정의된다. 즉

$$RPN = S \times O \times D$$

RPN 값은 1~1000 사이의 값으로 결정되며, 이때 높은 순위의 RPN값에 대해서 개선안 수립 및 실행을 통하여 위험을 줄이기 위한 노력을 해야 한다. 일반적으로 RPN 결과와 관계없이 심각도가 높을 때에는 별도의 개선 대책을 수립하여야 한다. FMEA를 원활하고 효과적으로 수행하기 위해서는 구성팀원의 역할이 매우 중요하다. 예를 들면, 심각도의 평가점수를 부여하는데 있어 서로 상반된 견해를 보이면 원활한 진행이 어렵기 때문이다. 또한 어떤 고장모드에 대해서 문제 원인을 찾을 때 지식부족으로 설계자가 모르는 복합적인 요인으로 발생된 경우라면 고장원인을 추정하지도 못할 뿐만 아니라 그에 따른 대안도 당연히 나올 수 없는 한계점이 있다.



Ⅲ. ASIL 결정을 위한 기능안전 운전상황 분석

3.1 서론

최근 안전하면서도 편리한 자동차에 대한 요구가 늘어남에 따라 자동차에 사용되는 ECU(Electronic Control Unit: 전자제어장치)의 수가 급속히 증가하고 있다. 이에 따라 ECU의 오작동에 의한 위험을 감소시키고 기능안전성을 확보하기 위해 자동차 내 E/E(Electrical and/or Electronic: 전기/전자)시스템에 특화된 ISO 26262가 제정되었다. IEC 61508을 기반으로 한 이 표준은 자동차의 E/E시스템에 대해 개발에서 운영, 유지보수 그리고 폐기에 이르기까지 방대하고 포괄적인 내용을 총 10개의 파트로 나누어 다루고 있다.

E/E 시스템의 개발 및 운영의 전 단계에 걸쳐 기능안전성 요건 설정의 토대가 되는 ASIL은 아이템이나 엘리먼트에 있어서는 안 될 잔존 리스크를 방지하기 위해 적용되는 안전무결성 등급(ISO 26262-1, 2011)이다. 따라서 ASIL은 안전 목표와 함께 본격적인 아이템 개발 이전에 결정되어야 한다. 이것은 위험원과 운전상황의 조합으로 도출되는 위험사건에 대해 세 가지 파라미터인 심각도, 노출확률 그리고 제어가능성을 토대로 결정되며 최저 수준인 ASIL A에서 최고 수준인 D까지 4수준이 있다. ASIL과 함께 제품의 안전 목표가 정해지는데 이를 통해 세부적인 안전요구사항을 도출

하고 기능안전개념(Functional Safety Concept)을 기술하게 된다. 기능안전 개념은 다시 시스템 수준의 제품 개발에서 기술적 안전 요구사항으로 구체화된다(Cho et al. 2010). 이와 같이 ASIL은 가장 우선적으로 결정될 뿐만 아니라 제품의 안전요구사항평가지표를 제공하기 때문에 시스템 개발의 핵심 요소라고 할 수 있다. 그러나 이러한 중요성에도 불구하고 ISO 26262에서는 ASIL 결정 절차와 관련하여 대략적인 가이드라인만 제공할 뿐 구체적인 수행절차나 방법론을 안내하고 있지 않다. 또한 표준 파트3의 부록 B에서 제공하고 있는 예시에서도 부분적인 내용만 다루고 있고 세부적인 지침이나 구체적인 설명이 없어서 표준을 이해하거나 현장에서 실행함에 있어 어려움이 많다. 이와 같은 실무 차원의 애로사항을 해결하는데 도움을 주기 위한 연구가 필요하지만 관련 국내외 연구들이 아직은 충분하지 않으며, ASIL결정 절차의 구체적 방안을 제시하는 연구는 찾아보기 어려운 실정이다.

본 장에서는 ASIL결정에서 가장 중요한 단계인 위험사건분류와 관련된 절차들을 체계화하여 제시하고자 한다. 제 3.2절에서는 ASIL결정을 위해 수행되는 H&R 단계를 구체적으로 분석한다. 제 3.3절에서는 위험사건분류에 필요한 운전상황의 범주를 표준을 토대로 정의하고 하위 범주를 상세화하였다. 제 3.4절에서는 위험사건 분류를 위한 체계적인 방법을 소개하고 제 3.5절에서는 EPB시스템 적용사례를 들어 설명한다.

3.2 표준에 의한 H&R 및 ASIL 결정의 한계

3.2.1 위험원(Hazard)과 위험사건(Hazardous Event)

ISO 26262에서 ASIL은 아이템 개발에 있어서 안전요구사항의 평가지표가 되므로 그 등급을 객관적으로 결정해야 한다. 이를 위해 개발 아이템의 정의를 토대로 H&R을 먼저 실시하여 위험원을 식별한다. 이어서 자동차의 운전상황과 위험사건을 도출하고 위험사건에 대한 심각도, 노출확률 그리고 제어가능성을 평가하여 ASIL과 안전 목표를 결정함으로써 H&R이 완료된다.

H&R에서 일단 위험사건에 대한 평가가 끝나고 나면 ASIL은 ISO 26262에서 제공한 기준에 따라 명확하게 결정할 수 있다. 그러나 그 이전의 절차에 대해서는 표준에 가이드라인 수준의 내용만 제공되고 있어 ASIL의 객관성 확보가 어려운 상황이다. 이것은 같은 위험사건이라 하더라도 다른 사람이 평가 할 경우 ASIL의 등급이 다르게 결정될 수 있음을 의미한다. 여기서 위험사건이라 함은 위험원과 운전상황이 결합되어 나타나는 것으로 자동차의 수명기간 동안 발생할 수 있는 무수히 많은 경우 수의 조합을 의미한다. 그리고 위험원은 아이템의 오동작으로 인해 야기되는 위해의 잠재적 근원으로 정의된다. 사전적 의미로 해석해 볼 때 잠재적 근원이라 함은 아이템 고장을 야기하는 부품의 결함이라고 볼 수 있다. Figure 3.1은 위험원 및 위험사건을 보다 명료하게 이해할 수 있도록 위해(harm)의 발생 과정을 시간 순으로 정리한 것이다.

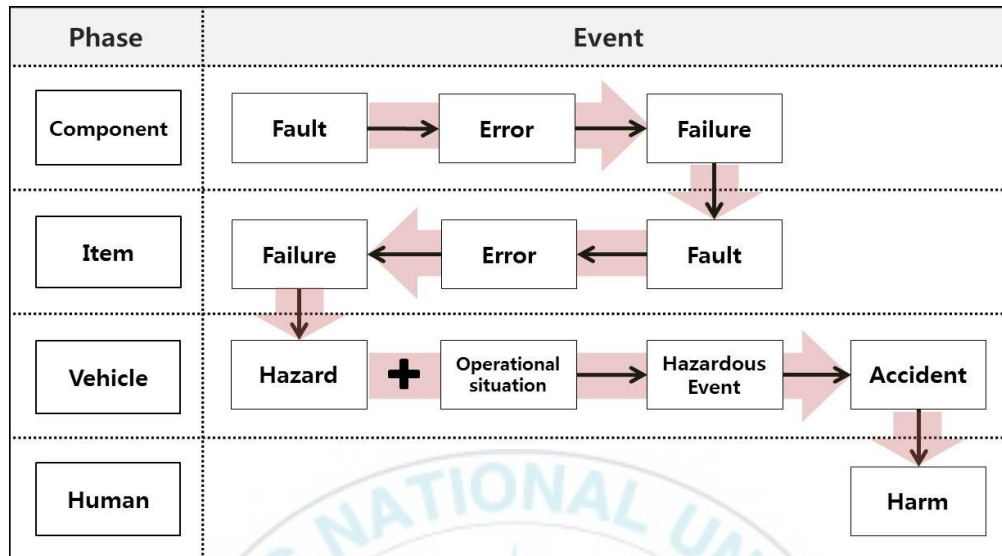


Figure 3.1 Fault leading to harm

Figure 3.1에 의하면 아이템 고장에 의해 유발된 오동작(위험원)은 운전 상황과 결합되어 위험사건이 된다. 위험사건의 결과로 사고가 발생하고 사고의 결과로 피해가 발생한다. 예를 들면 자동차의 EPB(Electrical Parking Brake)시스템의 고장은 엔진토크, 조향장치 및 전방조명장치의 오동작(위험원)을 유발하고 이것이 다시 특정 운전상황과 결합되어 사고로 이어 질 수 있다.

Figure 3.2는 ISO 26262 Part 10에서 제공하고 있는 위험사건의 예시를 재배열하여 나타낸 것으로 아이템 고장으로 인해 발생할 수 있는 위험사건과 가능한 위험사건의 결과를 보여주고 있다(ISO 26262-10, 2011).

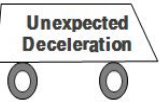
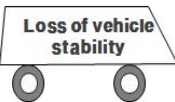
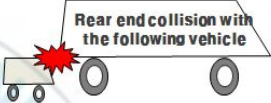
Item Failure	Hazard	Specific Situation	Hazardous Event	Possible Consequence
Unintended parking brake activation		High Speed	Unexpected deceleration at high speed	
		Taking a bend	Unexpected deceleration at taking a bend	
		Low friction surface	Unexpected deceleration at low friction surface	
		Medium-low speed and high friction surface	Unexpected deceleration at medium-low speed and high friction surface	

Figure 3.2 Example of EPB system's hazardous event

3.2.2 ASIL 결정절차의 한계

ISO 26262에서는 ASIL 등급결정을 위하여 위험사건의 심각도, 노출확률 그리고 제어가능성을 평가하는데 그 과정이 구체적으로 표준화되어 있지 않아서 수행자의 주관적 관점에 의해 결과가 달라질 소지가 있다. 또한 평가에 정성적인 요소도 있어서 IEC 61508에 비해 안전수준을 계량화하기 어려운 단점이 있다(Yun et al. 2009).

먼저 심각도는 위험사건의 원인이 되는 자동차의 운전자 및 동승자와 자전거 타는 사람, 보행자, 타 차량 탑승자와 같은 기타 인명을 포함하여 잠재적 리스크에 놓인 각 개인에 가해지는 위해의 심각한 정도를 말한다. 심각도 결정은 위험사건을 정성적으로 평가하여 약식상해등급(AIS)으로 분

류하는 것으로 최저 수준인 S0에서 최고 수준인 S3까지 4가지로 구분된다. 파트 3의 부속서 B에서는 심각도의 4가지 수준에 해당하는 위험사건의 예시를 제공하고 있는데 위험사건들이 평가되는 과정이나 근거가 명확히 설명되어 있지 않아 위험사건이 객관적으로 분류되었다고 보기 어렵다. 예를 들면, ‘도로변 구조물과의 충돌’을 서로 다른 사람이 평가할 경우 예시와 똑같이 심각도 S0으로 분류될 것이라는 보장이 없다.

두 번째로 노출확률은 위험원 발생을 야기하는 관련된 환경 인자가 있는 운전상황의 지속시간이나 발생 빈도로 평가한다. 노출확률의 분류는 최저 수준인 E0에서 최고 수준인 E4로 5가지로 구분된다. 파트 3의 부속서 B에서는 노출확률의 5가지 수준에 해당하는 환경인자 별로 운전상황을 예시하고 있는데 고려되어야 할 환경인자의 범위를 제시하고 있지 않아 시나리오 작성 시 혼란이 예상된다.

마지막으로, 제어가능성은 일반적인 운전자가 위험사건이 발생했을 때 계속해서 차량을 제어하거나 회복시킬 수 있는 확률에 대한 추정을 통해 평가되고 최저수준인 C0에서 최고 수준인 C3로 4가지 수준으로 분류된다. 파트 3의 부속서 B에서는 제어가능성의 4가지 수준에 해당하는 운전인자를 고려한 위험사건 예시를 제공하고 있는데 운전인자에 대한 명확한 정의나 범위가 제공되어 있지 않아 혼란이 예상된다. 예를 들면, ‘조명이 없는 도로에서 중/고속으로 야간 운전하는 동안 전방전조등 고장’이라는 위험사건과 ‘고속으로 주행 시 운전석 에어백의 잘못된 해제’라는 위험사건이 있을 때 전자의 경우는 환경인자라고 할 수 있는 조명이 없는 도로를 고려하였고 후자는 운전인자라 볼 수 있는 고속주행만 고려하였다.

이와 같이 ISO 26262에서는 ASIL결정을 위해 전체적인 가이드라인만 제공하고 있어 산업 현장에서 바로 사용하기에는 어려움이 많다고 판단된

다. 따라서 표준의 실용성을 높일 수 있도록 좀 더 체계적이고 구체화된 ASIL결정 방법론의 개발이 필요하다고 하겠다.

3.3. 운전상황 분석 및 ASIL 결정단계

3.3.1. 운전상황 분석

운전상황은 자동차가 운행되는 동안에 처할 수 있는 환경과 사용될 수 있는 상태들의 조합이다. 따라서 운전상황 분석을 위해서는 먼저 자동차가 처할 수 있는 환경과 사용범위를 정해야 한다. 그러나 ISO 26262에서도 이것과 관련된 명확한 내용을 구체적으로 기술하고 있지 않으므로 파트3의 부속서B에서 제공한 예시 및 한국도로교통공단의 통계(Road Traffic Safety Association, 2013)를 참고하여 운전상황 결정요인을 다음과 같이 운전자, 자동차, 도로 그리고 날씨를 포함한 환경으로 나누어 살펴보기로 한다. 4가지 운전상황 결정요인 중에서 자동차 운전에는 가장 큰 영향을 미치는 요인은 운전자이다. 왜냐하면 운전 중 운전자의 부적절한 행동은 어떤 다른 요인보다도 더 치명적인 사고를 유발할 수 있을 뿐만 아니라 운전자의 연령, 성별, 운전능력 등도 안전에 영향을 미치기 때문이다. 그러나 표준에서는 운전자는 운전하는데 적합한 상태에 있으며(예를 들면 운전자는 피곤하지 않다) 적합한 안전 교육을 받았고(운전자 면허가 있다) 기타 교통 참여자에게 리스크를 주지 않도록 주의 하는 것을 포함하는 모든 적용 가능한 법률적 규정을 준수한다고 가정하고 있으므로(ISO 26262-3,

2011) 여기서는 운전자를 고려대상에서 제외한다.

Table 3.1은 운전상황을 결정하는 요인 중 운전자를 제외하고 자동차, 도로, 환경의 세 요인을 기준으로 세부요인들을 분류하여 정리한 것이다. 첫 번째 요인인 자동차는 그 기능 및 유지보수 상태 등이 안전에 영향을 미칠 수 있으나 불필요한 복잡성을 줄이기 위해 자동차는 기능적으로 문제 없이 설계 및 제작되었고 유지·보수 상태도 양호하다고 전제하고 오직 기능안전과 관련된 요소만 고려한다. 자동차에서 기능안전과 관련된 요소로는 운전속도, 외부부착물, 운전모드 그리고 작동이 있다. 각 요소들은 다시 세분화되어 하위요소를 가진다. 운전속도의 하위요소는 매우느림, 느림, 보통, 빠름, 매우빠름이 있고 외부부착물의 하위요소는 부착물이 있는 경우와 없는 경우가 있는데 전자에는 트레일러나 루프 랙 등이 부착된 경우가 포함된다. 운전모드의 하위요소는 주행, 주차, 주유 그리고 수리 상태이다. 마지막으로 작동은 엔진, 속력, 방향 그리고 운행이다.

도로는 교통안전에 영향을 줄 수 있는 곡률, 경사, 배치, 외장 그리고 주변여건의 5가지 요소로 분류하였다. 각 요소들은 다시 하위요소들로 분류되는 경우도 있는데, 예를 들어 주변여건의 경우 장애물의 여부, 교통량의 정도, 보행자의 교통 정도로 구분하여 고려한다. 곡률은 도로의 직선도를 반영하여 직선과 곡선으로 구분한다. 경사는 평탄한 도로와 경사진 도로로 구분하고 배치는 터널, 다리, 교차로, 횡단보도, 고속도로 등 많은 경우가 있지만 상황을 단순화 하고자 도로 배치로 인한 시계상태의 좋고 나쁨으로 구분했다. 도로의 외장은 포장, 비포장, 험로로 구분하였다. 환경은 주로 날씨와 관련된 요소인 노면상태, 시계, 온도 그리고 바람으로 분류하였다. 노면상태는 건조, 습함, 결빙이 있다.

Table 3.1 Factors of operational situation

Factor	Sub-factor	Element	State
Vehicle	Driving Speed		Very low, low, Normal, High ,Very high
	External Attachment		Without, With
	Operational Mode		Driving, Parking, Fuelling, Repairing
	Maneuver	Engine	Off, On
		Velocity	Accelerating, Constant, Decelerating
		Direction	Lane Keeping, Lane Changing, Turning
		Movement	Stop, Forward, Backward
Road	Linearity		Straight, Curved
	Slope		Plain, Sloped
	Layout		blocked(invisible), Unblocked(visible)
	Coarseness		Paved, Unpaved, Troublesome
	Nearby Elements	Obstacle	Clean, Obstacle (e.g. lost cargo dropped in lane of travel)
		Traffic	Light, Heavy
		Pedestrians	None, Some, Many
Environ ment	Surface		Dry, Wet(by rain etc), Icy
	Visibility		Dark, Clean, Blurry
	Temperature		Low, Medium, High
	Momentum		Windy, Calm

시계는 어두움, 밝음, 흐림이 있고 온도는 저온, 중온, 고온이 있다. 바람은 센바람과 잔잔한 바람으로 구분하였다.

3.3.2 위험사건 식별 및 ASIL 결정 단계

Table 3.1을 토대로 운전상황을 재 정의하면 운전상황 결정요인의 각 하위요인들의 조합이라 할 수 있다. 예를 들면, ‘자동차는 보통속도를 유지하며 외부 부착물 없이 직진 운행 중이며 도로는 직선이며 교통정체는 없고, 온도는 중온이고 맑은 날씨로 시계는 밝다.’ 라고 표현된다. 그러나 이와 같은 표현방법은 하나의 운전상황이 지나치게 길고 세분화되어 위험사건을 매우 조밀하게 분류되도록 한다. 이는 제어가능성과 심각도 등급을 매기기 쉽게 하지만, 수많은 서로 다른 운전상황은 결과적으로 노출 관련 등급을 낮게 만들어 해당 안전 목표의 ASIL을 부적절하게 낮추도록 유도할 수 있으므로 기능안전 관점에서 불필요하다고 판단되는 요소는 제거하거나 축약된 표현방법을 찾아 좀 더 간단한 운전상황을 만들 필요가 있다. 여기서 운전상황이라 함은 운전상황 결정요인 중에서도 위험원과 관련이 있는 요소의 상태별 조합을 의미한다. 따라서 의미 있는 운전상황을 도출하려면 위험원에 대해 기능안전과 관련이 있는 운전상황 결정요인들을 선별하는 작업이 선행되어야 할 것이다. 이후 운전상황과 위험원의 결합을 통해 위험사건을 식별하고 ASIL을 평가한다면 불필요한 과정을 줄일 수 있을 것이다. 본 항에서는 ASIL 평가까지의 단계를 좀 더 구체화하여 다음과 같이 제안한다.

단계 1. 아이템 정의를 기반으로 모든 고장모드 식별

단계 2. 고장모드로부터 위험원 도출

단계 3. 위험원과 Table 3.1을 비교 검토하여 위험사건을 유발할 수
있는 운전상황 결정요인 식별

단계 4. 각 해당 요소별 상태 조합에 의한 운전상황 도출

단계 5. 위험원과 운전상황의 결합을 통한 위험사건 식별

단계 6. 위험사건별 심각도, 노출확률, 제어가능성 평가

단계 7. 위험사건별 ASIL 결정

3.4 심각도와 노출확률 및 제어가능성 등급 결정

3.4.1 심각도

주어진 위험사건의 심각도를 결정하기 위해서는 운전자, 차량 주위의 승객과 사람들 또는 차량 주변에 있는 개인에 대해 잠재적인 부상, 즉 위해 정도를 평가해야 한다. 여기서 부상이란 함은 사고로 인해 인체에 미치는 물리적인 해나 손상의 결과를 의미하고 부상의 심각도는 위험원이 어떤 운전상황과 처해 있느냐에 따라 달라진다. 그러므로 심각도는 위험원과 운전상황의 결합인 위험사건이 사고로 연결되었을 경우를 추정하여 얻어진 결과를 평가하여 결정한다. 일단 위해 정도에 대한 추정치가 얻어지면 ISO 26262 파트3 Table을 참고하여 심각도 등급을 정해줄 수 있다. Figure 3.3은 심각도 결정과정을 도시한 것이다.

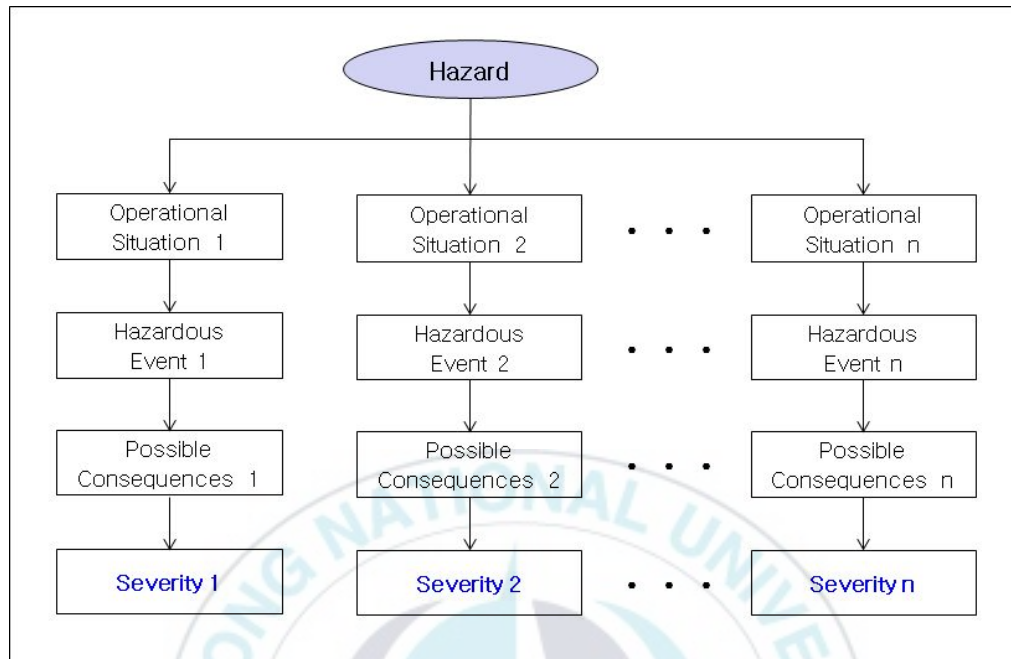


Figure 3.3 Determination procedure of severity

3.4.2 노출 확률

노출확률을 추정하려면 위험사건의 발생을 야기하는 운전상황 결정요인들의 조합으로 나타나는 시나리오를 평가해야 한다. 노출확률은 운전상황 결정요인 및 하위요인들의 상태에 대하여 지속기간이나 발생빈도를 추정하여 얻을 수 있다. 추정을 위한 통계자료는 관련기관들을 통해 확보하거나 새로운 데이터를 수집할 수 있다.

노출확률 결정의 첫 번째 단계에서는 운전상황 결정요인의 상태별 확률을 계산하고, 두 번째 단계에서는 운전상황 결정요인의 상태들이 서로 독

립적으로 일어난다고 가정하고 운전상황별 확률을 계산한다. 세 번째 단계에서 상태들 간의 의존성을 고려하여 앞서 도출된 확률을 조정한다. 마지막으로, 하나의 위험사건에 대한 노출확률을 추정한다. 이해를 돕기 위해 예를 들어 보자. 운전상황 결정요인 중 ‘자동차_운전속도’와 ‘도로_배치’를 각각 SF1, SF2라 하자. SF1의 경우 매우느림, 느림, 보통, 빠름 그리고 매우빠름으로 5개 상태가 있는데 각각을 X1, X2, X3, X4 그리고 X5라고 하고 그것의 노출확률을 1/15, 3/15, 5/15, 4/15 그리고 2/15이라고 하자. 한편, SF2는 시계불량과 시계양호인 2개의 상태가 있는데 각각을 Y1, Y2라고 하고 그것의 노출확률을 1/12, 11/12이라고 하자. 만약 특정 위험사건이 운전상황 (X4, Y1)일 때 일어난다고 하고 각 상태들이 독립적으로 일어난다고 가정한다면 위험사건이 일어날 노출확률은

$$\Pr(\text{SF1}=\text{X4}, \text{SF2}=\text{Y1}) = \Pr(\text{SF1}=\text{X4})\Pr(\text{SF2}=\text{Y1}) = (4/15)(1/12) = 1/45$$

이다. 이것은 ISO 26262 파트3에서 제공하는 기준에 의해 노출확률 E3(평균운용 시간의 1%~10%)에 해당한다. 그러나 운전상황 결정요인의 상태들 사이에 의존성이 존재한다면 위험사건의 노출확률은 달라질 것이다. 가령 시계가 불량한데 속도가 빠름이 될 확률은

$$\Pr(\text{SF1}=\text{X4}|\text{SF2}=\text{Y1}) = 1/50$$

이라고 하자. 이 경우 위험사건이 일어날 확률은

$$\begin{aligned}\Pr(\text{SF1}=\text{X4}, \text{SF2}=\text{Y1}) &= \Pr(\text{SF2}=\text{Y1})\Pr(\text{SF1}=\text{X4}|\text{SF2}=\text{Y1}) = (1/12)(1/50) \\ &= 1/600\end{aligned}$$

이다. 이것은 E2(평균운용 시간의 <1%)에 해당하여 앞서 의존성을 고려하지 않은 등급보다 낮게 된다.

3.4.3 제어가능성

제어가능성에 대한 확률 추정치는 일반적인 운전자가 위험원이 발생했을 때 계속해서 차량을 제어 또는 회복시킬 수 있거나 또는 근처에 있는 사람이나 해당 위험원에 처한 사람이 스스로 위험원 회피에 기여할 수 있다는 점을 감안해서 평가해야 한다. 이와 같은 추정은 운전인자가 포함된 운전 상황 결정요인과 위험원이 결합된 위험사건을 평가함으로써 가능하며 노출 확률과 같은 방식으로 진행한다. 예를 들어 운전상황 결정요인 중 ‘자동차_운전속도’와 ‘자동차_외부부착물’을 각각 SF1, SF2라 하자. 어떤 특정 위험 사건은 SF1의 경우 ‘빠름’인 상태와 SF2의 경우는 ‘부착물 있음’ 상태일 때 발생한다고 하자. 각각의 상태를 X4, Y2라고 하고 제어확률을

$$\Pr(\text{SF1}=\text{X4}) = 0.99$$

$$\Pr(\text{SF2}=\text{Y2}) = 0.95$$

이라 하자. 만약, 각 상태가 독립적으로 발생한다면 위험사건 (X4, Y2)의 제어확률은

$$\begin{aligned}\Pr(\text{SF1}=\text{X4}, \text{SF2}=\text{Y2}) &= \Pr(\text{SF1}=\text{X4})\Pr(\text{SF2}=\text{Y2}) \\ &= (0.99)(0.95)=0.9405\end{aligned}$$

가 될 것이다. 이것은 ISO 26262 파트3에 의해 제어가능성 C2(모든 운전자나 기타 교통 참여자의 90%이상은 일반적으로 위험을 피할 수 있다)에 해당한다. 그러나 상태들 사이에 의존성이 존재한다면 위험사건 (X4, Y2)의 제어확률은 달라질 것이다. 일반적으로 빠른 속도에서 부착물이 있을 경우는 없을 경우보다 제어확률이 낮아질 것이므로 여기서는

$$\Pr(\text{SF1}=\text{X4}|\text{SF2}=\text{Y2}) = 0.80$$

라고 하자. 그러면 위험사건 (X4,Y2)이 제어될 확률은

$$\begin{aligned}\Pr(\text{SF1}=\text{X4}, \text{SF2}=\text{Y2}) &= \Pr(\text{SF2}=\text{Y2})\Pr(\text{SF1}=\text{X4}|\text{SF2}=\text{Y2}) \\ &= (0.95)(0.8) = 0.76\end{aligned}$$

이 될 것이다. 이것은 C3(모든 운전자나 기타 교통 참여자의 90%미만은 일반적으로 위해를 피할 수 있다)에 해당하므로 앞서 상태들 간의 의존성을 고려하지 않은 등급보다 높은 수준이다. 전술한 예에서는 운전상황 결정요인의 각 상태들이 위험사건 제어확률을 감소시키는 방향으로 의존적일 경우만을 서술하였으나 증가시키는 방향으로 의존적일 경우도 있을 수 있다.

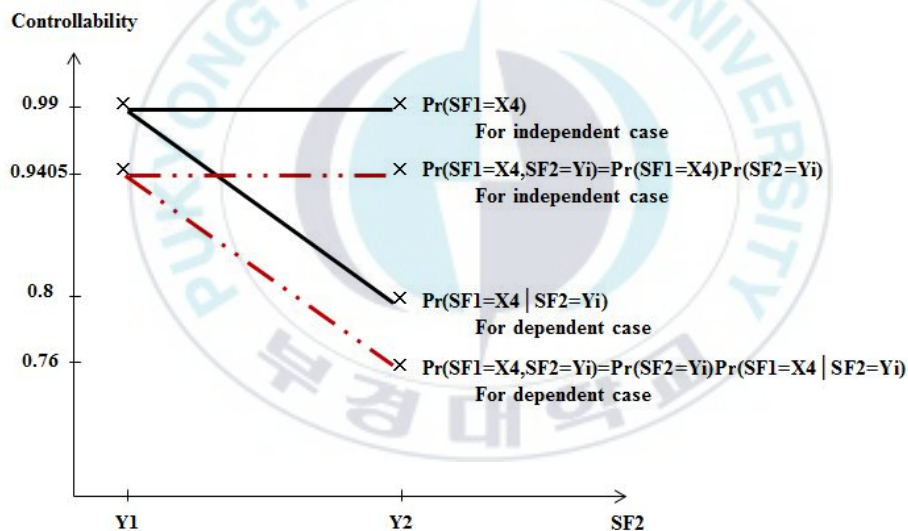


Figure 3.4 The controllability for independent vs dependent cases

Figure 3.4는 이해를 돕기 위해 운전상황의 두 결정요인이 독립적일 경우와 의존적일 경우를 전술한 예를 토대로 비교 도시한 것이다. 만약 운전상황 결정요인의 각 상태들이 위험사건 제어확률을 증가시키는

방향으로 의존적이라면 그림의 형태 역시 증가하는 방향으로 바뀌게 될 것이다.

3.5 EPB시스템 적용

지금까지 운전상황 결정요인들을 토대로 운전상황을 정의한 후 위험사건을 도출하고 그 심각도, 노출확률, 제어가능성을 평가하여 ASIL을 결정하는 과정에 대하여 논의하였다. 이 절에서는 Figure 3.2에서 인용된 EPB시스템에 3.3.2항에서 제안한 과정을 적용해보기로 한다. 먼저 1단계로 아이템은 EPB시스템으로 정의하였고 2단계의 가능한 위험원은 모두 도출되었다고 가정하자. 여기서 설명을 위하여 위험원들 중 예시된 ‘Unexpected Deceleration’만을 고려하기로 한다. 단계 3에서는 먼저 주어진 위험원 ‘Unexpected Deceleration’과 결합되었을 때 위험을 일으킬 가능성이 큰 운전상황 결정요소들을 선택하고 이들의 상태와 위험원이 결합될 수 있는 경우들을 Table 3.2와 같이 나타내었다. 여기서 운전상황 결정요인으로서 운전속도, 외부부착물, 속력, 방향, 곡률, 경사, 배치, 노면, 시계가 선택되었다. 또한, 선택된 요인별로 위험원과 결합되어 가장 심각한 위험을 초래하게 될 상태는 짙은 배경색으로 구분하여 나타내었다. 단계 4는 단계 3에서 선택된 요소들을 토대로 심각도, 노출확률, 제어가능성에 비추어 높은 ASIL이 부여될 가능성이 큰 운전상황(요인별 상태들의 조합)만 고려한다. 이것은 한 아이템이 위험사건과 관련하여 여러 개의 ASIL을 가질 경우 가장 높은 ASIL을 부여하도록 권장하고 있기 때문이다. 실제로는 훨씬 더

많은 운전상황이 있겠으나 여기서는 다음 세 가지만 고려한다.

- 운전상황1 : 부착물이 있는 자동차가 매우 빠른 속도로 차선 변경
- 운전상황2 : 시계가 불량한 경사가 있는 곡선도로
- 운전상황3 : 어둡고 결빙인 도로

Table 3.2 Factors of operational situation for EPB system

Factor	Sub-factor	Element	state				
Vehicle	Driving speed		Very low	Low	Normal	High	Very high
	External attachment		Without			With	
	Maneuver	Velocity	Accelerating		Constant	Decelerating	
		Direction	Lane Keeping		Lane Changing	Turning	
Road	Linearity		Straight			Curved	
	Slope		Plain			Sloped	
	Layout		Blocked			Unblock	
Environment	Surface		Dry		Wet	Icy	
	Visibility		Dark		Clean	Blurry	

단계 5에서는 단계 4의 운전상황과 위험원을 결합하여 위험사건을 정의한다. 도출된 운전상황과 위험원을 결합하면 다음과 같은 위험사건이 정의된다.

- 위험사건 1 : 부착물이 있는 자동차가 매우 빠른 속도로 차선 변경

도중 예기치 않은 감속

- 위험사건 2 : 시계가 불량한 경사가 있는 곡선도로에서 예기치 않은 감속
- 위험사건 3 : 어두운 결빙 도로에서 예기치 않은 감속

단계 6에서는 각 위험사건별로 심각도, 노출확률 및 제어가능성 등급을 결정해야 하는데 모두 비슷한 방법을 따르게 되므로 여기서는 위험사건 1에 대해서만 살펴본다. 먼저 심각도를 결정하기 위해서는 위험사건으로 발생할 수 있는 사고를 유추하고 그 결과 입게 될 위해의 정도를 정해야 한다. 위험사건 1의 경우 바로 옆 차선에서 뒤따라오는 차량이 추돌하는 사고로 이어질 수 있으며 부착물까지 있으므로 매우 빠른 속도를 감안할 때 치명적인 부상을 입을 수 있는 것으로 판단된다. 따라서 ISO 26262의 심각도 등급 기준을 참조하여 S3를 부여한다. 다음으로 승용차가 부착물을 장착하고 다니는 비율은 5%, 차선을 변경하는 비율은 40%, 부착물을 장착한 차량이 매우 빠른 속도로 주행할 가능성은 10%라고 한다면 노출확률이 $(0.05)(0.4)(0.1) = 0.002$ 이 되어 등급 E2를 부여한다.

마지막으로 부착물까지 장착된 자동차를 매우 빠른 속도로 운전하면서 차선을 변경하다가 예기치 않은 감속으로 뒤따르던 차량과 충돌하였을 때 운전자가 차량을 제어할 수 있는 가능성은 희박하다고 판단되므로 등급 C3를 부여한다.

단계 7에서는 결정된 심각도, 노출확률 및 제어가능성 등급을 토대로 ASIL을 정해주는데, S3, E2, C3의 경우 ASIL 등급은 B이다. Table 3.3은 비슷한 방법으로 위험사건 2와 3에 대해서도 ASIL을 결정하여 정리한 것이다.

Table 3.3 ASIL Determination of EPB system

Hazard	Sub-factor	State	Operational situation	E	Hazardous event	Possible Consequence	S	C	ASIL
Unexpected deceleration	Speed	Very high	Changing lane with an attachment high speed	E2	Unexpected deceleration in changing lane with an attachment at high speed	Rear end collision with the following vehicle	S3	C3	B
	External attachment	With							
	Velocity	Accelerating							
	Direction	Lane changing							
	Linearity	Curved	Curved road with blocked steep slope	E2	Unexpected deceleration at curved road with blocked steep slope	Rear end collision with the following vehicle	S1	C2	QM
	Slope	Sloped							
	Layout	Blocked							
	Surface	Icy	Dark icy surface	E2	Unexpected deceleration at dark icy surface	Loss of vehicle stability	S0	C1	-
	Visibility	Dark							

IV. ASIL기반 FMEA 위험평가 척도

4.1 서론

FMEA(Failure Mode Effect Analysis)는 초기 시스템 설계결함으로 인한 위험을 평가하기 위해 널리 사용되고 있는 기법이다. 1950년대 초 제트기의 신뢰성 설계를 위해 사용된 것을 효시로 하여 1960년대에 항공우주산업 분야에 활용되면서, 지금은 제조뿐만 아니라 서비스산업에서도 매우 보편적으로 사용되는 도구이다. Onodera(1997)는 약 100개의 FMEA 적용 사례를 조사하여 FMEA가 실제 현대 산업 프로세스의 모든 단계에서 사용된다는 것을 확인하였다.

FMEA는 고장원인에 대한 시정 또는 예방활동의 우선순위를 결정하기 위해 RPN(Risk Priority Number)을 사용한다. RPN은 세 가지 위험 인자인 심각도(Severity, 고장 영향의 심각성), 발생도(Occurrence, 원인에 의한 해당 고장을 생성 할 가능성), 및 검출도(Detection, 제품이 고객에 도달하기 전에 원인 또는 고장 자체를 검출할 수 있는 능력)의 곱으로 구한다. 그러나, 기존 FMEA의 RPN은 위험평가에 대하여 논리적이고 좋은 척도로 인정받지 않는다. 많은 학자들은 RPN의 단점 때문에 위험평가에 대한 RPN 방법론을 비판한다. 예를 들어, Wang et al.(2009)은 RPN의 세 가지 위험 인자가 실제 상황에서는 정확하게 평가되기 어렵다고 지적했다. Liu et al.(2011)과 Liu et al.(2012)은 똑같은 RPN

값을 가지더라도 전혀 다른 위험의 의미를 가질 수 있다는 점, 위험의 세 가지 요소 즉 심각도, 검출도 및 발생도는 중요도가 같지 않다는 점, 순서적 의미 외에 별다른 의미가 없는 세 요소의 평가 값을 곱해서 RPN을 계산함으로써 그 값이 절대적인 의미를 갖는 것으로 오해를 불러 일으킬 수 있다는 점 등 몇 가지 단점을 설명했다. 비슷한 단점이 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) 등 많은 학자들에 의해 지적 되었다. 자주 언급되는 내용은 다음과 같다

- i) RPN의 세 가지 구성요소간의 상대적 중요도를 고려하지 않는다
- ii) 동일한 RPN 값을 가짐에도 위험 측면에서 완전히 다른 의미를 가질 수 있다
- iii) RPN은 평가자의 경험과 직관에 의존하므로 평가에 일관성이 없을 수 있다
- iv) RPN 계산방식에 과학적 근거가 부족하다.

FMEA는 잠재적 고장모드의 영향과 원인을 식별하는 예방에 초점을 맞춘 기법이지만, H&R은 기능안전에 대하여 특별한 관계가 있는 고장의 영향에 초점을 맞춘, 보다 체계적이고 논리적인 위험평가 프로세스이다. ASIL은 H&R의 주요 출력물이며 자동차 E/E 아이템의 기능고장으로 인한 위험사건 발생의 리스크를 반영한다. 따라서 각각의 ASIL에는 각각의 안전요구사항이나 목표에 대한 고장 영향의 심각도에 대한 신뢰할 수 있는 정보가 포함되어 있다.

자동차의 E/E 아이템 또는 안전시스템에 대하여 H&R을 실시한 후 FMEA를 수행 할 때, 또 다시 심각도에 대하여 브레인스토밍 하는 것 보다 이미 ASIL에 포함된 심각도 정보를 사용하는 것이 효율적이다. FMEA와 H&R의 공통점을 주의 깊게 살펴보면, RPN의 몇 가지 한계를 경감 시킬 수 있는 개선된 위험평가 방법을 발견할 수 있다.

이번 장에서는 H&R과 FMEA를 비교하여 ASIL에서 심각도 정보를 추출하는 개선된 위험척도 방법을 제안 할 것이다. 본 장의 구성은 제 4.2절에서는 ASIL와 RPN을 비교하고, 제 4.3절에서는 수정된 위험평가 척도인 RPM을 제안하며, 제 4.4절에서는 사례를 통하여 실무자들을 위한 몇 가지 통찰을 제시한다.

4.2 RPN과 ASIL의 비교

4.2.1 FMEA와 H&R

FMEA는 시스템의 잠재적 고장모드와 그 영향을 분석하는 기법이다. FMEA를 수행하기 위해서 먼저 목표시스템과 그에 구현될 모든 기능이 정의되어야 한다. 각 기능은 고객 또는 사용자의 요구사항에 비추어 여러 가지 고장모드를 가질 수 있다. 고장은 필요한 기능을 수행할 수 있는 능력이 종료됨을 의미한다(ISO 26262-1, 2011). FMEA는 시스템의 모든 가능한 잠재적 고장모드를 식별하는 것으로 시작하여 고장으로 인한 영향을 파악하고, 그 심각도를 평가한다. 기존 FMEA에서 고장 영향의 심각도(S)

는 10이 가장 심각한 영향으로 1~10사이의 숫자로 평가된다. 고장모드의 심각도는 보통 최악의 영향을 기준으로 점수를 부여한다. 또 다른 한편으로는 고장 메커니즘 또는 원인이 결정되고, 그 발생 가능성(O)이 추정된다. 각 원인의 발생을 검출(D) 할 가능성은 현재의 제어 방법을 고려하여 평가된다. 고장원인의 발생도 및 검출도 역시 1~10사이의 숫자로 평가된다. 발생도는 고장원인이 매우 자주 발생할 때 10이 부여되므로 주의를 요하지만, 검출도 10은 고장원인이 거의 검출 불가능할 때 부여된다. RPN은 각 고장원인의 위험을 평가하는 심각도, 발생도 및 검출도를 나타내는 세 개의 숫자의 곱으로 얻어진다. 기본적으로, FMEA는 네 가지의 주요 활동으로 구성된다.

- i) 잠재적 고장모드의 확인
- ii) 고장 영향을 확인하고 그 심각도 평가
- iii) 고장 메커니즘 또는 고장원인 추론 및 그 발생도와 검출도 추정
- iv) 각 고장모드와 원인에 대한 RPN 기반의 위험 평가 및 개선조치

H&R은 ISO 26262의 위험 평가 과정으로서 위험원의 존재 하에서 시작된다. ISO 26262-1(2011)에 따르면, 위험원은 아이템의 오작동으로 인하여 야기되는 위해(개인의 건강에 미치는 물리적인 해나 손상)에 대한 잠재근원이다. 오작동은 시스템이 설계 의도대로 작동하지 않는 고장이나 의도되지 않은 작동이다. 따라서 위험원은 인체에 물리적인 해나 손상을 초래할 수 있는 시스템 고장으로 이해될 수 있다. H&R은 FMEA보다 고장의 심각성 및 각 고장의 심각한 영향에 더 초점을 맞춘 것이다. 게다가, H&R은 시스템 고장이 위험사건을 초래하게 될 운용상황과 운용형태를 고려하고 있다. 또한 운전자들에 기초하여 각 위험사건의

제어가능성과 각 운용상황에 노출될 확률을 추정한다. 따라서 H&R의 핵심 결과물은 ASIL등급과 함께 위험사건 및 안전 목표의 목록이다.

FMEA와 H&R 모두 위험평가와 관련되어 있고 위험을 회피하는 것이 목적이지만 위험의 내용은 서로 다르다. 전자의 목적은 위험의 일반적인 유형을 줄일 수 있는 개선된 설계를 달성하는 것이고, 후자의 목적은 인체에 국한된, 보다 구체적인 유형의 위험을 방지하는 것이다. 두 기법은 동일한 핵심 입력물 즉, 목표시스템의 기능목록을 필요로 한다.

그러나 핵심출력은 다소 다른데 전자는 고장모드와 원인에 대응하는 RPNs이고, 후자는 위험사건에 대응하는 안전 목표와 ASILs이다. FMEA는 고장원인에 초점이 맞추어져 있고 H&R은 고장영향에 초점이 맞추어져 있으므로 RPN은 고장의 원인과 연관되어 있고 ASIL은 위험사건 즉, 고장 영향과 연관되어 있다.

H&R은 개념 단계에서 실행(ISO 26262-3, 2011) 되는 반면, FMEA는 개념단계의 아이템수준에서 위험원 추출(ISO 26262-3, 2011) 또는 제품 개발 단계에서 안전 밸리데이션(ISO 26262-4, 2011), 또는 안전 분석(ISO 26262-5, 2011)에 사용될 수 있다. 따라서 FMEA는 사전실행 된 H&R을 이용하여 고장모드 분석을 수행할 수 있다. Figure 4.1은 ISO 26262의 관점에서 H&R과 FMEA의 입력과 출력을 비교한 것이다. 안전시스템을 위한 다양한 개발활동에 FMEA를 적용하는 경우, 대부분의 고장영향은 안전과 밀접하게 관련된다. FMEA에서 고장영향의 심각도는 안전시스템의 해당고장에 의한 위험사건의 원인과 자연스럽게 연결된다. ISO 26262의 H&R은 FMEA보다 더 체계적이고 과학적인 위험평가과정이므로, 결국 ASIL은 FMEA 팀원의 주관적 직관에 대부분 의존하는 RPN보다 고장의 심각도에 대하여 더 객관적이고 신뢰할 수 있는 정보를 제공한다. 따라서

본 장에서는 ISO 26262에 의거한 안전시스템을 개발할 때 결정된 ASIL의 정보를 이용하여 RPN의 일부 단점을 보완할 것이다.

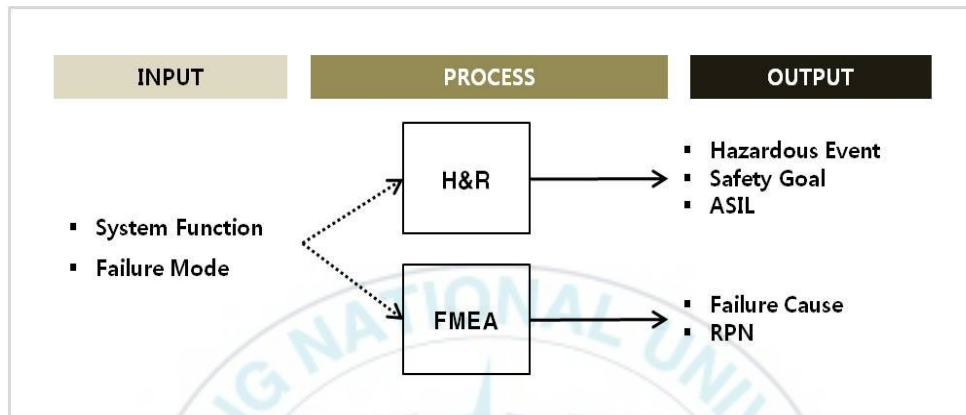


Figure 4.1 The input and output of H&R and FMEA from the ISO 26262 perspective

4.2.2 RPN과 ASIL의 결정 절차

RPN과 ASIL은 리스크 평가를 위해 FMEA와 H&R의 주요 결과물을 이용한다. 본 항에서는 RPN과 ASIL의 논리적인 차이를 찾기 위해 이들의 결정절차를 비교 할 것이다.

RPN을 얻기 위해서는 각 고장모드의 심각도, 발생도 및 검출도가 추정되어야 한다. 심각도는 각 고장의 영향과 관련되며, 하나의 고장모드에 대하여 여러 가지의 영향이 나타나고 이에 따른 심각도 숫자가 여러 개 있을 수 있다. 심각도는 1~10으로 구분되며 절대적으로 심각한 영향은 10, 무시할 수 있는 영향은 1로 부여한다. 하나의 고장모드에 대하여 여러

가지 영향에 따른 여러 개의 심각도가 있는 경우, 해당 고장모드에 관련된 영향들의 심각도 중 가장 높은 심각도만으로 평가한다. 발생도 또한 1~10으로 구분되며, 특정 원인의 발생가능성이 높은 것은 10, 거의 가능성이 없는 것은 1로 부여한다. 각 고장모드에는 여러 가지 원인이 있을 수 있으며, 발생도 등급은 주어진 고장모드의 각 원인에 적절하게 부여된다. 검출도는 현재의 관리방법으로 고장원인을 검출하거나 고장모드를 검출할 수 있는 능력이다. 검출도 역시 1~10등급으로 구분되며, 검출 가능성이 거의 없을 경우 10, 검출 가능성이 거의 확실 할 때는 1이 부여된다. 따라서 고장원인에 대한 심각도(S), 발생도(O), 및 검출도 (D)를 평가 한 후, 이들의 곱에 의해 RPN은 정의된다. 즉

$$RPN = S \times O \times D \quad (4.1)$$

ASIL은 불합리한 잔여위험을 피할 목적으로 적용되는 안전척도와 시스템의 필요한 요구사항들을 지정하기 위한 것으로 최소 엄격수준인 A부터 가장 엄격한 수준인 D까지 4등급 중 하나로 정해진다(ISO 26262-3, 2011). ASIL은 위험사건과 관련된 심각도(Severity), 노출확률(Probability of Exposure) 및 제어가능성(Controllability) 세 가지 요소에 의해 결정된다. 심각도는 운전상황 및 시스템고장을 고려하여 사람에게 끼칠 수 있는 잠재적인 위해의 정도를 추정한 것이다. 심각도는 S0, S1, S2, S3 네 개의 등급으로 분류되며, 각 위험사건에서 치명적인 부상에 대하여 S3, 부상이 없으면 S0이 부여된다. 노출은 위험원이 될 수 있는 운용상황에 있는 상태를 말하며, 각 운용상황의 노출확률은 각 위험사건에 대한 이론적 해석을 기반으로 추정한다. 노출확률은 E0, E1, E2, E3, E4 다섯 등급으로 분류되며 최고 노출가능성 수준은 E4, 최저 노출가능성 수준은 E0로 분류된다. 제어

가능성은 운전자나 잠재적 위험에 놓인 다른 사람이 위험사건을 충분히 제어할 수 있어 특정한 위해를 피할 수 있는 확률을 나타내며, 브레이크 고장, 고속주행 시 에어백해제 등의 운전인자와 위험사건의 조합에 의한 운전시나리오로부터 추정한다.

제어가능성은 C0, C1, C2, C3 네 개의 등급으로 분류되며, 제어하기 어렵거나 제어 불가능한 것은 C3, 제어가능 한 것은 C0로 분류된다. ASIL은 이러한 세 가지 요소의 추정등급을 기반으로 ISO 26262-3(2011)에 의해 제공되는 Table 2.5를 사용하여 결정된다. ASIL A~D 등급 외에 추가된 QM(품질경영) 등급은 품질경영시스템 외에 따로 ISO 26262를 준수하기 위한 요건이 필요하지 않음을 의미한다.

Figure 4.2는 RPN과 ASIL의 결정절차를 비교 설명하고 있다. RPN과 ASIL 모두 시스템고장과 관련 있지만, RPN은 고장원인 같은 사전 고장 요소에 더 의존하고 ASIL은 고장영향(위험원)과 운용상황 같은 사후 고장 요소에 더 의존한다. ASIL의 세 가지 요소는 안전 또는 위험과 연결되어 고장영향의 중대성을 평가하기 위한 수단으로서 사용된다. RPN이 FMEA 팀원의 주관적인 직관과 경험에 의존하는 반면, ASIL은 상당히 체계적이고 객관적 절차를 거쳐 결정됨에 주목해야 한다. 그러므로 ASIL은 고장영향의 리스크 또는 심각도가 RPN 경우보다 더 객관적인 지표로 생각할 수 있다.

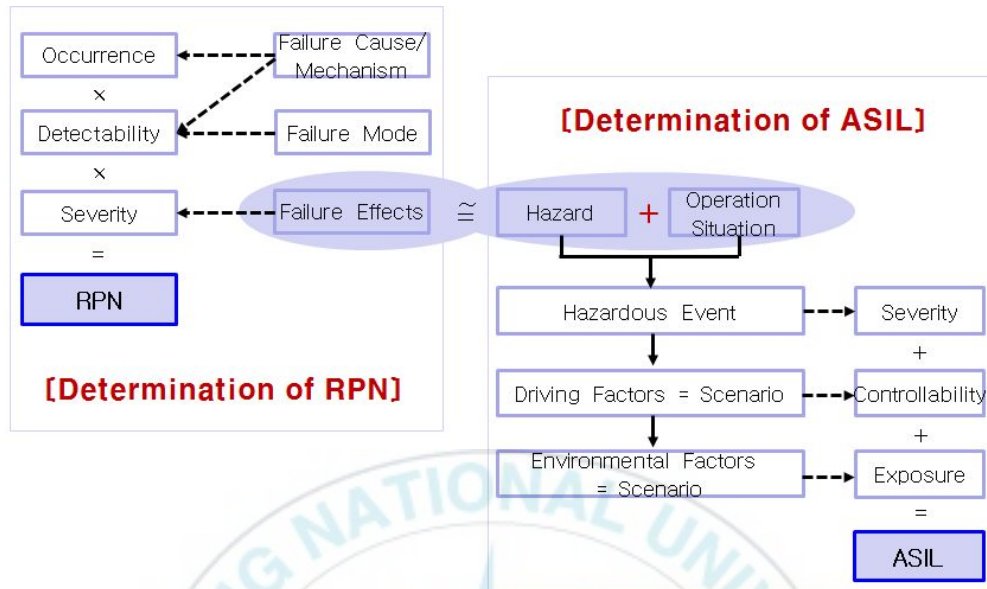


Figure 4.2 RPN and ASIL Determination

4.2.3 ASIL 등급을 기반으로 한 RPN 개선

FMEA는 리스크평가 및 설계개선을 위해 널리 사용되는 기법이지만, 결과물인 RPN은 일관성 없는 순위결과로 인하여 객관성이 다소 부족하다. Sankar과 Prabhu (2001)는 개별 순위척도의 비선형적 특성에 의해 결과가 왜곡되고 있다고 지적했다. 또한, RPN 점수시스템은 다른 기업 간의 객관적인 비교가 어려울 수 있다. Ireson et al.(1996)은 기존 FMEA는 RPN 값에 관계없이 심각도가 높은 고장모드에 집중해야 한다고 하였다. 이것은 기존 FMEA의 RPN을 적용하는데 몇 가지 한계가 있음을 의미한다. Eubanks et al.(1997), Bertolini et al.(2006), Jeegadeshnan et al.(2007), Oolkalkar et al.(2009), Agung and Kwon(2010), 그리고 Kwon et al.(2011)

등의 많은 학자들은 기존 FMEA를 보완하기 위한 개선된 방법을 찾기 위하여 많은 노력을 하였다. 숫자를 사용하여 위험을 평가하는 RPN은 여러 가지 편리한 점이 있고, 기업 간의 위험 수준을 비교하는 객관적 통계로도 사용하지만 많은 문제가 발생할 수 있다. 이것은 ISO 26262와 같은 국제 표준에서 RPN에 근거하여 일부 요구사항들을 강요하는 경우 흔히 발생할 수 있다.

본 항에서는 ASIL 순위 결정 방법에 기초한 RPN 점수계산절차의 개선에 초점을 맞출 것이며, 소개되는 새로운 개념의 ASIL은 위험평가를 위하여 보다 체계적인 순위결정 절차를 제공하고 있으나, 보다 정교하게 개선할 여지가 남아 있다. 기본적으로 ASIL은 심각도, 노출확률 및 제어가능성 세 가지 요소에 의존하며, 이들 요소를 결정하기 위한 특정 프로세스 또는 방법은 표준에서는 제공되지 않는다. 이와 관련한 자세한 논의는 Ellims and Monkhouse(2012)를 참조하면 될 것이다.

RPN과 ASIL의 결정절차를 비교해 보면 몇 가지 개선할 방법을 찾을 수 있다. 첫째, 발생도 및 검출도를 1~10 등급 이상의 확률로 표시한다. 기존 FMEA에 의해 제공된 평가기준은 실제로 확률과 밀접한 관련이 있다. 발생도와 검출도의 확률을 대략적인 추정치에 사용할 수 있다면, 기존 1~10 등급 체계보다 사용하기에 더 효과적일 것이다. 다음으로 심각도는 RPN과 ASIL에서 동일한 용어를 사용하지만, 그 결정절차와 의미는 매우 다르다. RPN의 심각도는 우수한 등급척도이지만 그 결정과정은 ASIL과 비교했을 때 그다지 논리적이지 않다. ASIL의 심각도 등급결정은 운용상황, 환경, 운전자인자를 모두 고려하고 있다. 사실 RPN의 심각도 개념은 고장의 결과 위험사건의 심각도, 노출확률 및 제어가능성의 조합된 영향에서 기인하는 전체적인 심각성에 가깝다. RPN의 심각도 요소에 이러한 개념을

적용한다면 그 결과는 매우 의미가 있을 것이다. 즉, ASIL의 세 가지 요소에 대한 적합한 등급을 선정하고, 이들을 RPN의 심각도에 적절히 적용할 수 있다는 것이다.

4.3 FMEA에 대한 수정된 위험 척도

4.3.1 고장 발생도 및 검출도에 대한 확률 척도

FMEA 매뉴얼(Chrysler etc., 2008)과 핸드북(Ford design Institute, 2004)에 따르면, 발생도는 특정원인/메커니즘이 발생할 가능성의 정도를 말한다. 그 평가기준은 표로 제시하였고, 발생 가능한 고장률을 고려하여 1~10의 등급으로 나타낸다. 발생도 등급은 각 고장원인 또는 메커니즘에 대하여 부여되고, 고장률은 고장모드와 직접적으로 연관되어 있다. 시간 순서를 고려하면, 원인은 해당고장에 선행되어서 나타난다. 그러므로 고장률에 의한 원인의 발생도를 결정하는 것은 그다지 논리적이지 않다. 상기 매뉴얼에서 고장원인 발생률은 원인이 발생하는 순간에 고장이 발생하는 것으로 간주하여 해당 고장률과 동일하다고 가정한 것으로 보인다. 또한, 이미 고장률을 알고 있다면 발생확률을 정확하게 구할 수 있는데, 굳이 정밀하지 못한 1에서 10까지의 등급을 부여하는 것은 이해하기 어렵다. 따라서 기존 FMEA의 발생도 순위에 대한 논리적 결함을 해결하기 위하여 각 고장원인의 발생률을 사용하기로 한다. 여기에서 하나의 고장모드에 대하여 여러 가지 원인이 있을 수 있음을 참고하고,

발생률 $\lambda_{i1}, \lambda_{i2}, \dots, \lambda_{in_i}$ 을 가진 고장모드 FM_i 에 대한 n_i 개의 발생원인이 있다고 가정하자. 고장률이 일정하다고 할 때, 고장모드 FM_i 의 j 번째 고장원인은 식(4.2)를 이용하여 발생하는 확률을 얻는다.

$$O_{ij} = 1 - e^{-\lambda_{ij}}, \quad i = 1, 2, \dots, m \text{ and } j = 1, 2, \dots, n_i \quad (4.2)$$

또한, RPN에 고장모드 또는 원인에서 기인된 위험을 반영하기 위하여 고장모드 FM_i 의 검출되지 않은 원인들의 추정 비율 $D_{i1}, D_{i2}, \dots, D_{in_i}$ 을 검출 척도로 사용할 것이다.

4.3.2 수정된 심각도 점수와 RPM

FMEA에서 심각도는 발생도, 검출도와는 전혀 다른 의미를 갖는다. 발생도 및 검출도에 대한 등급은 확률과 밀접하게 관련되는 반면, 심각도 등급은 확률의 개념과는 거리가 멀다. 심각도는 특히 안전과 관련된 위험을 고려 할 때, 해당 고장으로 인해 인체의 상해 또는 물리적 손상의 심각성을 반영한다. 여기서는 자동차 기능안전 관련 전기/전자 부품산업에 적용하기 위한 FMEA 심각도의 수정된 척도를 얻기 위하여 ISO 26262-3 (2011)의 방법을 사용할 것이다. 고장으로 인한 위해의 심각도는 운용상황, 환경 및 운전자 상태에 의해 악화될 수 있으므로, 이러한 요소는 심각도에 대한 수정된 척도에서 합리적으로 반영 될 것이다. 이를 위한 간단한 방법 중 하나는 ASIL의 구성요소인 심각도, 노출확률 및 제어가능성 등급의

숫자를 차용하는 것이다. 우선, 다음과 같이 각 ASIL 구성 요소의 등급에 숫자를 부여한다.

- Severity class number: S0→1, S1→2, S2→3, S3→4
- Exposure class number: E0→1, E1→2, E2→3, E3→4, E4→5
- Controllability class number: C0→1, C1→2, C2→3, C3→4 (4.3)

다음으로, 세 가지 등급의 곱에 의한 심각도 점수를 얻으면

$$Si = \text{Severity Class(SC)} \times \text{Exposure Class(EC)} \times \text{Controllability Class(CC)} \quad (4.4)$$

S는 1~80 의 넓은 값의 범위를 가질 수 있다. 만약 관련된 충분한 정보가 있다면, 심각도 점수를 위험사건에 의한 손실금액으로 변환할 수도 있다. 따라서 각 고장원인에 대한 수정된 RPN은 기존 FMEA의 발생도(O), 검출도(D) 그리고 심각도(S)에 기초하여 얻어진다. 발생도와 검출도는 확률이므로, 수정된 RPN은 심각도 점수의 기대 값을 나타낸다. 고장 발생 확률은 일반적으로 매우작고, $O \times D \times S$ 결과는 소수점 미만의 값을 가질 수 있으므로 용이하지 않다. 따라서 기존의 RPN에서 RPM(Risk Priority Metric)을 정의하면 다음과 같다.

$$\text{RPM} = O \times D \times S \times 1,000,000 \quad (4.5)$$

Figure 4.3은 기존의 RPN에서 수정 된 RPM의 결정 절차를 나타낸다.

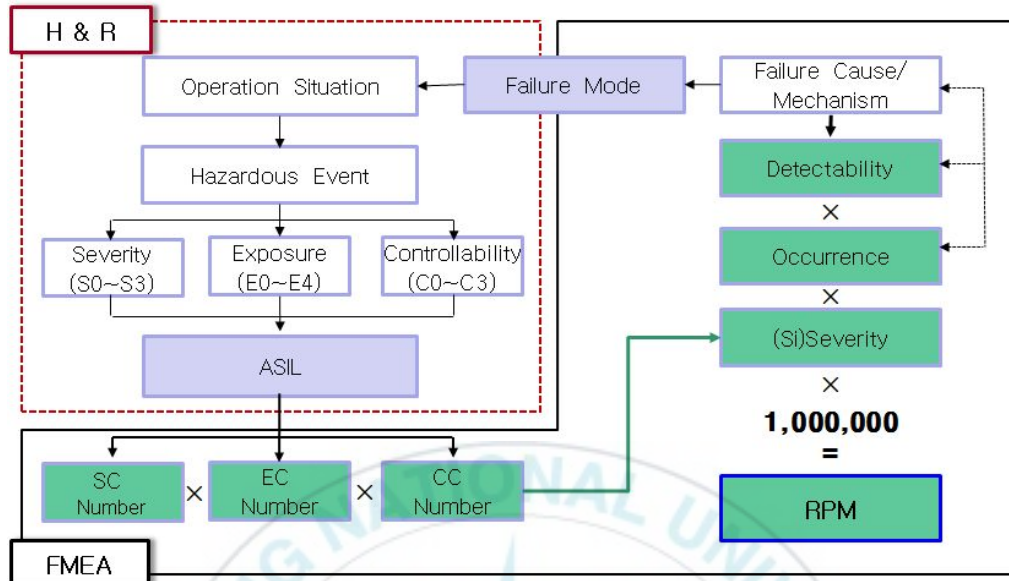


Figure 4.3 The determination of RPM

4.4 사례 연구

4.4.1 Dual Clutch Transmission 사례

Table 4.1은 “Dual Clutch Transmission”의 ASIL 결정을 위하여 2가지 고장모드에 대한 FMEA 및 기능안전성 분석을 적용한 사례를 Zhang et al.(2010)에서 일부분 발췌하였다. 비교목적을 위해 일부수치는 합리성을 벗어나지 않는 한도에서 모델에 맞게 변경되거나 추가되었다.

Table 4.1 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	7	dual clutch mechatronic assembly fault	4	dual clutch mechatronic assembly inspection	3	84	5
	loss of acceleration		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

Table 4.1에서 “loss of acceleration”은 차량의 기능저하 단계에서 동작할 수 있음을 의미한다. 따라서 기존 FMEA 기준에 의해 고장모드 “clutch disengaging”에 부여되는 심각도는 7이다. 그리고 “possible collision”은 자동차 안전운행에 영향을 미치는 것을 의미하며, 해당하는 고장모드 “incorrect gear position”는 운전 중 일부증상을 가질 것이므로 그 심각도는 9로 선정되었다.

4.4.2 RPM 기반의 리스크 평가

이번 항에서는 앞의 사례를 토대로 RPM의 계산을 보여줄 것이다. 첫째, 각 고장원인의 발생도를 고려한다. 첫 번째 원인 "dual clutch mechatronic assembly fault"은 Table 4.1에서 발생도 4이다. 기존 FMEA에 따르면, 발생도 4는 1/10,000에 상당한다. 이것을 식(4.2)를 사용하여 확률로 변환할 수 있다. 따라서 수정된 발생도 척도에 의해 아래의 확률로 얻어진다.

$$O_{11} = 1 - e^{-0.0001} = 9.99 \times 10^{-5} \quad (4.6)$$

두 번째 원인 "shift mechatronic assembly fault"에 대한 발생도 역시 4이며, 기존 FMEA에 따른 고장발생률은 1/10,000에 상당한다. 이것을 식(4.2)를 사용하여 확률로 변환하면 아래의 확률로 얻어진다.

$$O_{12} = 1 - e^{-0.0001} = 9.99 \times 10^{-5} \quad (4.7)$$

세 번째 원인 "sensor fault"에 대한 발생도는 3이고, 기존 FMEA에 따른 고장발생률은 1/100,000에 상당한다. 이것을 식(4.2)를 사용하여 확률로 변환하면 아래의 확률로 얻어진다.

$$O_{21} = 1 - e^{-0.00001} = 9.99 \times 10^{-6} \quad (4.8)$$

네 번째 원인 "ECU fault"에 대한 발생도는 2이고, 기존 FMEA에 따른 고장발생률은 1/1,000,000에 상당한다. 이것을 식(4.2)를 사용하여 확률로 변환하면 아래의 확률로 얻어진다.

$$O_{22} = 1 - e^{-0.000001} = 9.99 \times 10^{-7} \quad (4.9)$$

마지막으로 다섯 번째 원인 "actuator fault"에 대한 발생도는 4이고, 기존 FMEA에 따른 고장발생률은 1/10,000에 상당한다. 이것을 식(4.2)를 사용하여 확률로 변환하면 아래의 확률로 얻어진다.

$$O_{23} = 1 - e^{-0.0001} = 9.99 \times 10^{-5} \quad (4.10)$$

각 고장원인에 대한 발생도의 확률 값을 구하였다. 다음으로, Table 4.1의 검출도를 확률로 수정한다. 검출도의 등급기준은 기존 FMEA에서는 간단한 가이드라인이 제시되어 있다. 검출도 확률에 대한 상세한 정보는 이 간단한 가이드라인으로부터 사용할 수 없기 때문에, 여기서는 단순히 설명을 위한 목적으로 원래 검출도 등급의 역수를 검출도 확률로 사용한다. 물론, 관련 데이터를 사용할 수 있다면 실제 데이터를 이용한 확률 값을 사용하는 것이 더 효과적이다. 예를 들어, Table 4.1의 첫 번째 고장 원인 "dual clutch mechatronic assembly fault"의 검출도 등급 3은 검출 확률 1/3로 변환한다. 실제 적용에서는 이 확률이 실제데이터 또는 엔지니어링 기술을 토대로 추정되어야 할 것이다. 수정된 검출도는 고장 원인을 발견하지 못할 확률을 나타낸 것이다. 따라서 상기 첫 번째 고장 원인에 대한 검출도는 다음과 같다.

$$D_{11} = 1 - 1/3 = 2/3 \quad (4.11)$$

순서에 따라 동일한 방법으로 다른 원인에 의한 검출도 적용결과는 다음과 같다.

$$D_{12} = 1 - 1/5 = 4/5 \quad (4.12)$$

$$D_{21} = 1 - 1/5 = 4/5 \quad (4.13)$$

$$D_{22} = 1 - 1/5 = 4/5 \quad (4.14)$$

$$D_{23} = 1 - 1/3 = 2/3 \quad (4.15)$$

Table 4.2는 각 원인에 의한 발생도 및 검출도 적용결과를 나타낸다.

마지막으로, 심각도 평가는 좀 더 복잡하다. 앞의 분석에 의해 해당 ASIL을 이용할 수 있는 경우, 심각도는 식(4.3)과 (4.4)를 사용하여 쉽게 평가될 수 있다. 예를 들어, Zhang et al.(2010)은 고장 "clutch disengaging"로 인한 잠재적 위험원 "upshift failure"에 대하여 심각도, 노출확률 및 제어가능성의 해당 등급은 S1, E3, 및 C3이므로 ASIL A를 부여한다. 따라서 SC = 2, EC = 4, CC = 4 가 된다.

Table 4.2 Modified rank of occurrence and detection

Failure Mode	Failure Cause	O	D
clutch disengaging	dual clutch mechatronic assembly fault	9.99×10^{-5}	2/3
	shift mechatronic assembly fault	9.99×10^{-5}	4/5
incorrect gear position	sensor fault	9.99×10^{-6}	4/5
	ECU fault	9.99×10^{-7}	4/5
	actuator fault	9.99×10^{-5}	2/3

여기서 FMEA의 고장 "clutch disengaging"의 심각도를 구하면 다음과 같다.

$$S_1 = 2 \times 4 \times 4 = 32 \quad (4.16)$$

Zhang et al.(2010)의 연구에는 잠재적 위험원 "collision due to incorrect gear position"에 대한 ASIL과 심각도, 노출확률 및 제어가능성의 등급은 나와 있지 않다. 그러므로 여기서는 사례를 위해 심각도 S2, 노출확률 E3와 제어가능성 C3를 부여하여 ASIL B로 가정한다. ISO 26262-3 부속서 B(2011)를 참조하면, 차량의 충돌이 자주 심각한 부상을 초래할 수 있기 때문에 심각도 등급 S2는 정당한 것이다. 따라서 FMEA의 고장 "incorrect gear position"에 대한 심각도 순위를 다음과 같이 얻을 수 있다.

$$S_2 = 3 \times 4 \times 4 = 48 \quad (4.17)$$

Table 4.3은 심각도(S), 발생도(O) 및 검출도(D)를 위의 값을 기초하여 산정하고, RPM은 식(4.5)를 이용하여 계산한 것을 요약한 것이다.

Table 4.3 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^{-5}	2/3	2,131	3
		shift mechatronic assembly fault	9.99×10^{-5}	4/5	2,557	2
incorrect gear position	48	sensor fault	9.99×10^{-6}	4/5	384	4
		ECU fault	9.99×10^{-7}	4/5	38	5
		actuator fault	9.99×10^{-5}	2/3	3,197	1

4.4.3 RPM의 민감도

FMEA handbook(Ford Design Institute, 2004)은 발생도 및 검출도에 대한 기준을 표로 제공한다. 그러나 고장률의 경계 값에서는 발생도에 대한 명확한 기준이 없다. 또한, 검출도에 대해서도 막연한 지침만 제공된다. 기존 FMEA에서 발생도 및 검출도에 동일 값이 있듯이 고장률과 검출 확률에서도 동일 값이 있을 수 있다. 따라서 경계 값 내 고장률과 검출 확률 변화에 대한 측면에서 RPM 값의 변화 시험은 의미가 있을 것이다.

Table 4.4 RPM values for dual clutch mechatronic assembly fault

Failure Cause	S	발생도 4에 따른 고장률 및 경계값	검출도 3에 따른 검출확률 및 경계값	RPM (×1,000,000)
dual clutch mechatronic assembly fault	32	0.000055	1/2	880
		0.0001		1,600
		0.0003		4,800
		0.000055	2/3	1,173
		0.0001		2,133
		0.0003		6,400
		0.000055	3/4	1,320
		0.0001		2,400
		0.0003		7,200

Table 4.1에서 첫 번째 고장원인 "dual clutch mechatronic assembly fault"의 발생도 및 검출도는 각각 4와 3이다. 여기서는 발생도 4는 고장률

0.0001, 발생도 3은 고장률 0.00001, 발생도 5는 고장률 0.0005에 해당한다. 따라서 발생도 4에 대한 고장률의 경계 값으로서 0.000055와 0.0003를 고려한다. 설계관리가 잠재적인 고장원인과 이어지고 고장모드를 탐지할 가능성이 높은 경우에는 검출도 3을 부여하는 것으로 기술되어 있다. 하지만 이것은 검출확률의 경계 값을 결정하기에 매우 모호한 표현이다. 검출도 3에 대해서 확률 값 2/3를 이미 할당하였으므로 경계 값 확률로 1/2과 3/4을 고려한다. Table 4.4는 고장원인에 대한 발생도의 고장률과 경계 값 및 검출도의 검출확률 및 경계 값에 의한 RPM 결과를 나타내며, Figure 4.4는 주어진 검출도에 대하여 그 경계범위 내에서 발생확률에 따른 RPM 값의 변화를 보여준다.

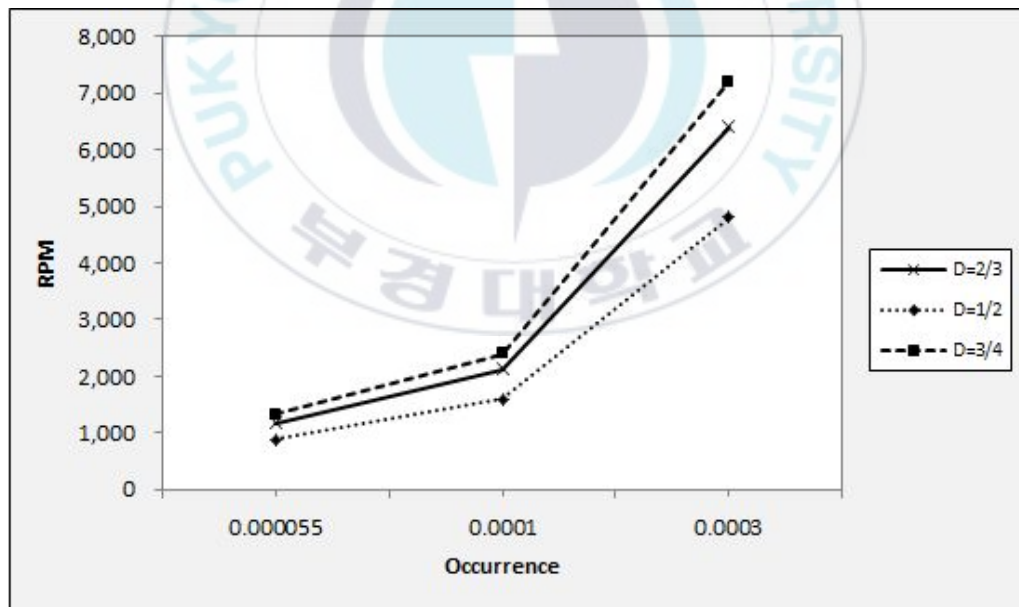


Figure 4.4 RPM vs Occurrence for dual clutch mechatronic assembly fault

두 번째 고장원인 "shift mechatronic assembly fault"에 대해서도 살펴 보면 발생도 및 검출도는 각각 4와 5이다. 여기서도 발생도 4는 고장률 0.0001, 발생도 3은 고장률 0.00001, 발생도 5는 고장률 0.0005에 해당한다. 따라서 발생도 4에 대한 고장률의 경계 값으로서 0.000055와 0.0003을 고려한다. 검출도 5에 대해서 확률 값 4/5를 이미 할당 하였으므로 경계 값 확률로 3/4과 5/6을 고려한다. 두 번째 고장원인 "shift mechatronic assembly fault"에 대한 RPM은 첫 번째 고장원인과 동일한 방법으로 산정된다. Figure 4.5는 주어진 검출도에 대하여 경계범위 내에서 발생확률에 따른 RPM 값의 변화를 보여준다.

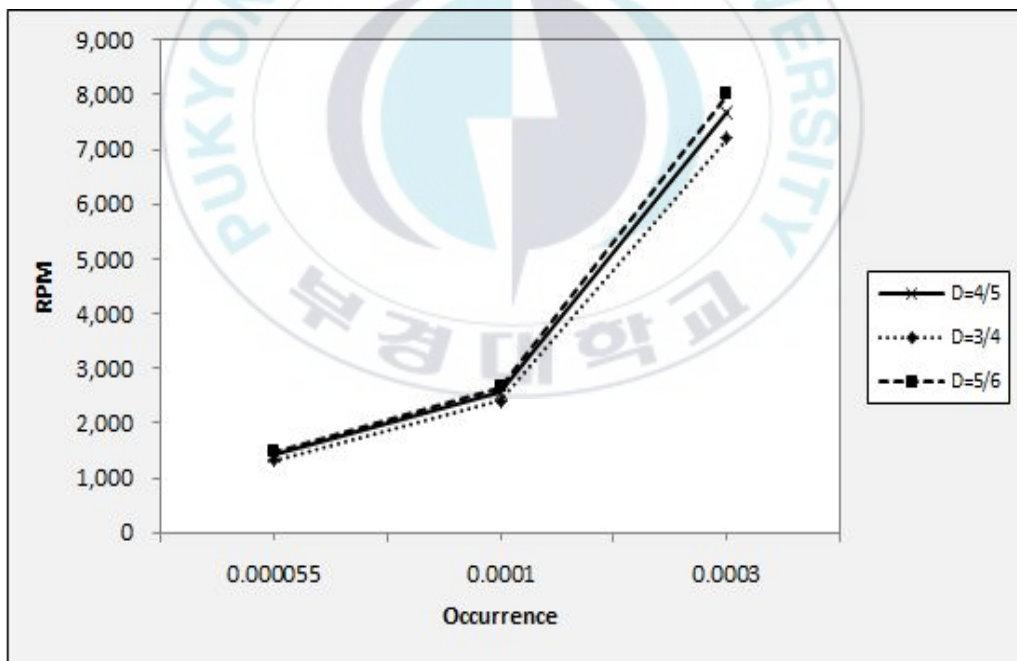


Figure 4.5 RPM vs Occurrence for shift mechatronic assembly fault

세 번째 고장원인 "sensor fault"는 발생도 및 검출도는 각각 3과 5이다. 여기서는 발생도 3은 고장률 0.00001, 발생도 2는 고장률 0.000001, 발생도 4는 고장률 0.0001에 해당한다. 따라서 발생도 3에 대한 고장률의 경계 값으로서 0.0000055와 0.000055를 고려한다. 검출도 5에 대해서 확률 값 4/5를 이미 할당하였으므로 경계 값 확률로 3/4과 5/6을 고려한다. 세 번째 고장원인 "sensor fault"에 대한 RPM은 첫 번째 고장원인과 동일한 방법으로 산정된다. Figure 4.6은 주어진 검출도에 대하여 그 경계범위 내에서 발생확률에 따른 RPM 값의 변화를 보여준다.

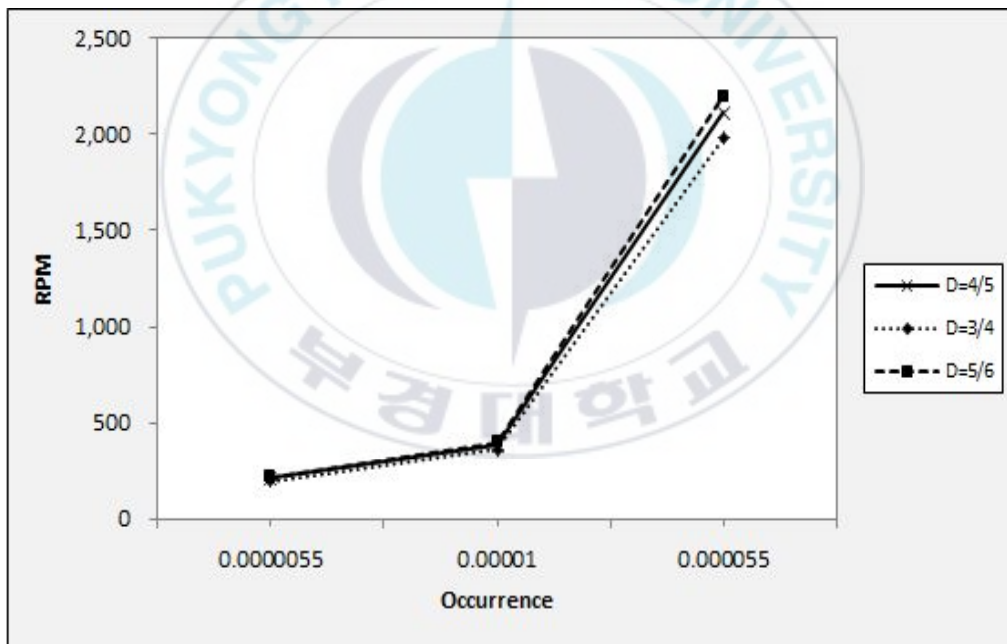


Figure 4.6 RPM vs Occurrence for sensor fault

네 번째 고장원인 "ECU fault"는 발생도 및 검출도는 각각 2와 5이다. 여기서의 발생도 2는 고장률 0.000001, 발생도 1은 고장률 0, 발생도 3은 고장률 0.000001에 해당한다. 따라서 발생도 2에 대한 고장률의 경계 값으로서 0.0000005와 0.0000055를 고려한다. 검출도 5에 대해서 확률 값 4/5를 이미 할당하였으므로 경계 값 확률로 3/4과 5/6을 고려한다. 네 번째 고장원인 "ECU fault"에 대한 RPM은 첫 번째 고장원인과 동일한 방법으로 산정되며, Figure 4.7은 주어진 검출도에 대하여 그 경계범위 내에서 발생확률에 따른 RPM 값의 변화를 보여준다.

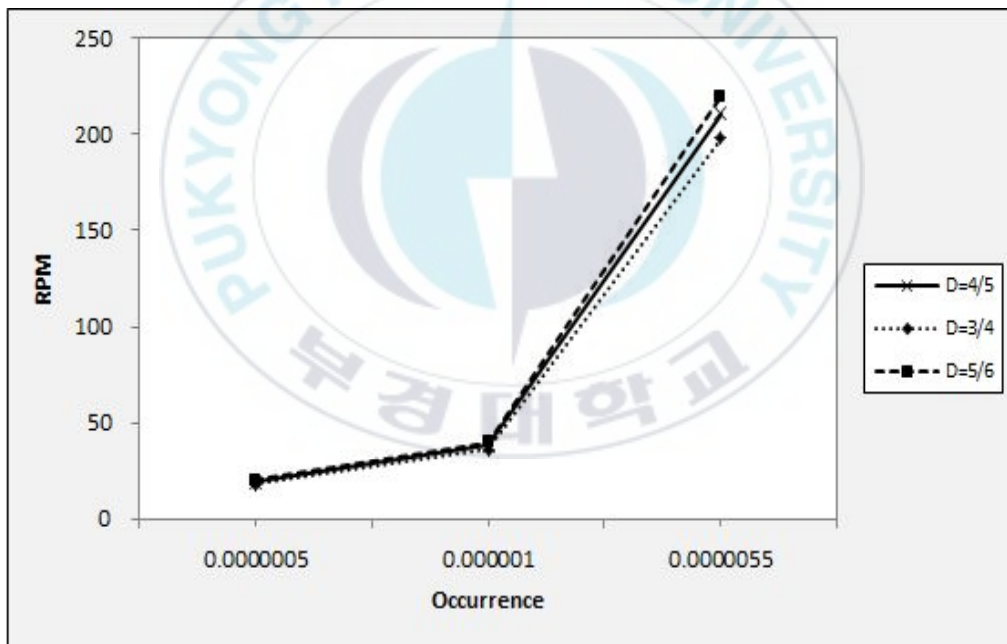


Figure 4.7 RPM vs Occurrence for ECU fault

다섯 번째 고장원인 "actuator fault"의 발생도 및 검출도는 각각 4와 3이다. 여기서는 발생도 4는 고장률 0.0001, 발생도 3은 고장률 0.00001, 발생도 5는 고장률 0.0005에 해당한다. 따라서 발생도 4에 대한 고장률의 경계 값으로서 0.000055와 0.0003을 고려한다.

검출도 3에 대해서 확률 값 2/3를 이미 할당하였으므로 경계 값 확률로 1/2과 3/4을 고려한다. 다섯 번째 고장원인 "actuator fault"에 대한 RPM 역시 첫 번째 고장원인과 동일한 방법으로 산정된다. Figure 4.8은 주어진 검출도에 대하여 그 경계범위 내에서 발생확률에 따른 RPM 값의 변화를 보여준다.

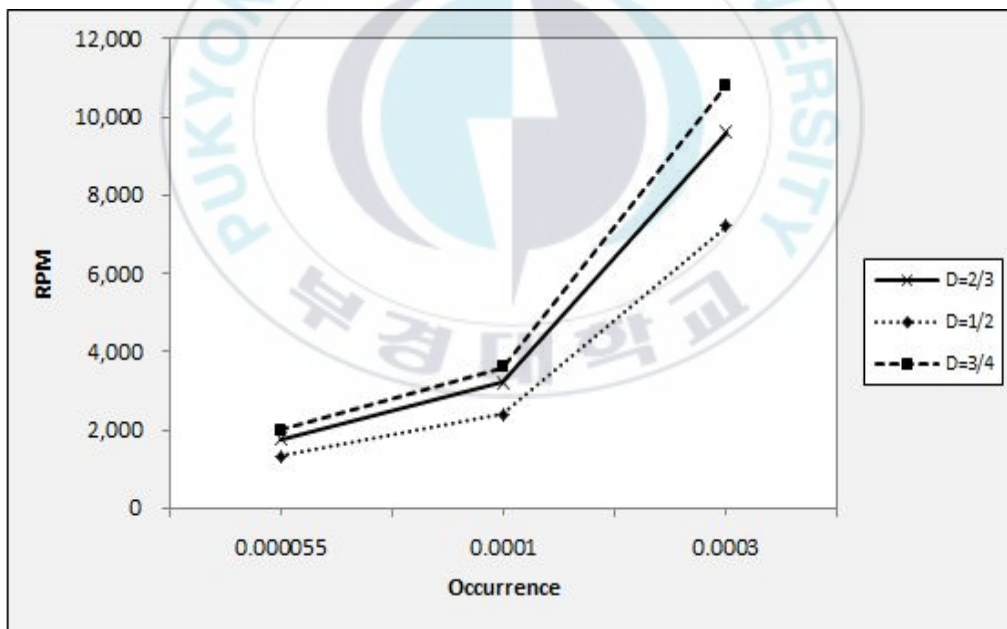


Figure 4.8 RPM vs Occurrence for actuator fault

민감도 분석 결과 RPM이 기존 RPN보다 경계범위 내에서 발생도 및 검출도의 확률변화에 대하여 더 민감함을 보여주고 있다. 여기서 RPN은 기존 FMEA에서 변경되지 않는다는 것에 주목해야 한다. 그러나 RPM은 순위가 변경되기 위해서는 RPM의 값이 크게 변화될 수 있다.

첫 번째 고장원인 "dual clutch mechatronic assembly fault"에 대한 검출확률 값 2/3이 정확하고 고정된 값이라고 하고 고장원인에 대한 발생도는 0.0003이라면 RPM은 고장원인 "shift mechatronic assembly fault" 과 "actuator fault"보다 더 큰 6,400이 된다. Table 4.3에서 알 수 있듯이 이 둘 위험의 우선순위를 각각 2번과 1번 이었다. 따라서 RPM의 위험우선순위는 기존 FMEA의 RPN이 변하지 않는 경우에도 완전히 바뀔 수 있다. 기존 FMEA에서는 RPN 값이 동일하여 위험순위가 같아도 RPM은 값이 다를 수 있으며, 위험순위도 다를 수 있다. 이는 경계범위 내에서 발생도 및 검출도의 확률변화가 RPM이 RPN보다 더 민감하다는 것을 의미한다. 따라서 RPM은 검출되지 않은 위험의 예상 심각도를 반영하고 실제적인 적용을 위한 의미 있는 척도이다. 사례는 기존의 위험평가 척도인 RPN이 고장원인의 위험우선순위에 대해 혼동을 주거나 왜곡된 정보를 제공할 수 있음을 보여준다.

4.4.4 실무적용을 위한 논의

4.4.4.1 RPN과 ASIL의 관계

RPN과 ASIL은 모두 세 가지 요소의 평가를 요구한다. ASIL은 "심각도", "노출확률" 및 "제어가능성"에 근거하여 결정되는 반면, RPN은

“심각도”, “발생도” 및 “검출도”에 근거하여 결정된다. 새로운 모형을 논의하기 전에, 이러한 전문용어는 의미가 정확히 이해되고 전달되도록 아래에 상세히 설명하였다. 각 단계별 시간 축을 함께 본 다면 각 용어의 개념을 보다 명확하게 이해할 수 있다. Figure 4.9는 ASIL 및 RPN 결정 요소에 해당하는 고장원인, 고장, 위험원, 위험사건 그리고 사고를 보여준다.

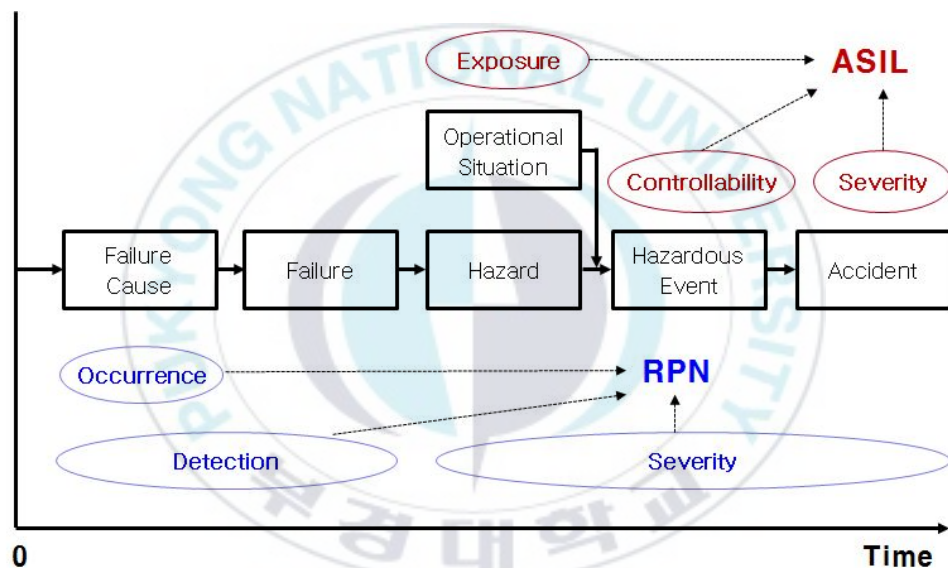


Figure 4.9 Comparison of RPN with ASIL on time horizon

“심각도”는 비록 ASIL과 FMEA에서 같은 용어로 사용되지만, 그 의미는 매우 다르다. ASIL의 심각도는 노출확률 및 제어가능성과는 별도로 이미 발생한 위험사건의 심각성이다. FMEA의 심각도는 자체의 노출확률 및 제어가능성 개념을 포함한 고장영향의 전반적인 심각성에 더 가깝다. 따라서 위기상황에 노출되어 있지 않거나 쉽게 제어 가능한 경우

FMEA에서의 고장모드는 그다지 심각하지 않을 수 있다. 한편, 고장으로 인한 위험사건이 위험한 운용상황에 거의 노출되지 않을 경우에도 높은 심각도 등급을 가질 수 있다. ASIL에서의 노출확률은 위험의 존재에 관계없이 차량이 특정 운용상황에 직면할 가능성을 반영한다. 제어가능성은 위험원 및 특정 운용상황의 조합인 위험사건에 의해 평가된다. 따라서 자동차 안전시스템에 관한 한 RPN에서의 고장영향의 심각도는 그 하나의 요소 즉, 심각도, 노출확률 또는 제어가능성의 개별적인 요소보다는 전반적으로 위험사건의 ASIL 등급에 반영될 것이다. 기존 FMEA에 따르면 발생도 및 검출도는 각 고장원인에 의하여 결정되므로 RPN의 심각도를 제외한 두 가지 요소가 고장원인과 밀접하게 연관되어 있는 반면에 ASIL의 세 가지 요소는 고장결과와 연관되어 있다. 예를 들어, FMEA handbook(Ford Design Institute, 2004)에서는 FMEA Sheet를 샘플로 제공한다. 따라서 ASIL 등급이 부여된 안전시스템에 대해서 FMEA를 실시할 때 ASIL로 부터 발생도나 검출도에 대한 의미 있는 정보를 유추할 수는 없을 것이다. 하지만, 심각도에 대한 가치 있는 정보는 ASIL로 부터 얻을 수 있다. ASIL A에 해당하는 고장은 그다지 심각하지 않을 것이고, ASIL D에 해당하는 고장은 대단히 심각할 것이라고 추정할 수 있다.

4.4.4.2 RPN과 RPM의 의미

기존 FMEA는 RPN을 계산하기 위하여 심각도, 발생도 및 검출도에 각각 1~10의 동일한 숫자범위를 부여한다. 이것은 중요도가 서로 다르더라도 세 구성요소에 동일한 가중치를 적용한다는 것을 의미한다. 기존 FMEA에 대하여 많은 자료에서 “심각도는 RPN의 가장 중요한

구성요소이다”라고 언급한다. 기존 FMEA의 권고에 따르면, 심각도가 높은 고장모드는 해당 RPN이 작은 경우에도 특별한 주의를 기울여야 한다. 이것은 기존 RPN이 단지 비교목적을 위한 참조 값이며, 시정 또는 개선 조치에 대한 중요한 의사결정의 기준은 아닐 것이라는 증거를 제공한다. 4.2.1 절에서 언급된 RPN의 중요한 문제점을 고려하면 새로운 척도인 RPM은 안전시스템에 대한 RPN의 개선된 위험평가 척도를 제시한 것이다.

FMEA는 개념단계의 H&R 후 ISO 26262를 수행할 때 ASIL 정보를 이용할 수 있으며, 또한 ASIL 정보를 FMEA의 심각도 점수에 반영할 수 있다. ASIL에서 노출확률, 제어가능성은 확률개념을 포함하고 있으므로 심각도, 노출확률 그리고 제어가능성의 등급을 나타내는 숫자는 심각도의 기대치를 반영한 것이다. 따라서 고장모드의 심각도 점수를 얻기 위해 식(4.4)를 사용하는 것은 합리적이다. 대략적인 확률정보는 FMEA의 RPN 발생도에 등급을 부여하는데 사용할 수 있어야 한다. 비록 그것이 대략적인 추정이더라도 발생도를 평가하기 위해 추정된 확률 값을 사용하는 것은 효과적일 수 있다. 검출도에서도 비슷한 논리의 적용이 가능하다. 이러한 논의에 기초하여 RPM은 식(4.5)와 같이 FMEA에서 안전시스템에 대한 위험평가의 새로운 척도로 구성되었다.

RPM은 실제로 각 고장모드 또는 원인에 대한 예상된 심각도로 이해될 수 있다. 따라서 RPM을 무시한다면, 기존 FMEA처럼 심각도의 중복을 고려하지 않고 해당 고장모드 또는 원인을 무시할지도 모른다. 또한, RPM은 보다 체계적이고 논리적으로 평가된 심각도에 기초하여 결정될 것이다.

4.4.4.3 RPN과 RPM

4.2.1 절에서 논의된 바와 같이 기존 FMEA의 RPN은 몇 가지 중요한 문제점을 가지고 있다. Chrysler, Ford and General Motors(2008)에 의한 FMEA reference manual에서 발췌한 Table 4.5의 예를 보자. 매뉴얼에서는 고장원인 B의 RPN이 고장원인 A의 RPN보다 더 크지만 고장원인 A를 먼저 조치하도록 권고한다. 그 이유는 고장원인 A의 심각도가 B의 심각도보다 더 크기 때문이다.

Table 4.5 Comparison of failure cause A and B

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

이 예에서 위험척도로서의 RPN의 한계를 말하고 있으며, 비록 모든 세 가지 요소에 동일한 비중이 부여되더라도 심각도는 다른 두 가지보다 더 중요하다는 것을 말한다.

FMEA 매뉴얼은 수정조치에 대한 RPN의 의사결정 기준 값을 설정하지 않도록 권장하고 있지만 새로운 척도의 RPM은 실제로 심각도의 기대 값을 나타내므로, 의사결정 기준 값으로 사용해도 될 것이다. ASIL 판정 절차에 따라 심각도 요소는 보다 체계적이고 논리적인 접근을 통해 평가된다. 비록 ASIL 자체는 차이가 없다 하더라도, 그 판정절차는 단지 고장뿐만 아니라 환경과 운전요인 및 운용상황을 고려한 꽤 논리적인 프로세스다. ASIL에 대한 체계적인 위험평가 과정에서는 RPM의 심각도에 대하여 RPN보다 더 많은 가중치를 부여하는 것이 타당하다. 그리고

발생도 및 검출도는 원래의 개념을 반영하여 자연스럽게 확률척도로 변경되었다. 이러한 데이터를 이용 가능한 경우 통계적인 추정도 가능하다. 통계적 접근은 발생도 및 검출도에 대한 보다 객관적인 추정을 보장한다. 비록 통계적 추정치를 이용할 수 없는 경우라도, 적어도 기존 FMEA의 값에 기초하여 4.4.2절의 방법을 적용할 수 있다. 이 단순한 수정은 RPN의 문제점을 상당부분 보완할 수 있다.

Table 4.1의 사례를 보면 고장모드 "clutch disengaging" 와 "incorrect gear position"의 심각도 점수는 각각 7 및 9이다. 각 고장원인에 대한 발생도 및 검출도를 평가한 후, 고장 "clutch disengaging"의 원인 "shift mechatronic assembly fault"는 최대 RPN 값 140을 갖는다. 그러나 기존 FMEA에 따르면 RPN 값에 관계없이 고장 "incorrect gear position"의 원인 "sensor fault"에 먼저 주의를 기울여야한다. RPN은 'Risk Priority Number'의 약자로 '위험우선순위'를 나타내지만 그것은 무의미할 수 있다. 여기서 RPN 대신 RPM을 사용한다면, Table 4.3은 고장 "incorrect gear position"의 원인 "actuator fault"에 먼저 조치를 취할 것을 권하는 보다 합리적인 결과를 보여준다. 실제로, RPM은 고장원인의 예상되는 심각도를 나타내기 때문에 작업의 우선순위를 결정하는데 일반적으로 사용할 수 있다.

4.4.4.4 RPM의 한계

FMEA reference manual의 권고에 따르면 고장모드 "incorrect gear position"의 모든 원인은 고장모드 "clutch disengaging" 이전에 고려되어야 한다. 그러나 Table 4.3의 RPM 값은 그 권고에 부합되지 않는다. 이는 두 가지로 이해될 수 있다.

- i) 비록 심각도의 가중치는 식(4.4)에 의해 조정되었으나 그것은 충분하지 않을 수 있다.
- ii) 그 조정된 가중치가 적절하지만 매뉴얼에서 심각도에 너무 많은 가중치를 부여하였기 때문일 수 있다.

ii)의 경우 RPM에 의해 결정된 위험우선순위 또한 잘못된 결정으로 오해될 수도 있다. 고장으로 인한 예상손실의 총액을 알 수 있을 경우, 그것은 예상 총 손실과 식(4.4)의 심각도 점수를 대체함으로써 쉽게 수정될 수 있다. 그러나 그것 또한 해당 고장으로 인한 손실의 모든 정보를 얻기는 어려울 수 있다. Table 4.1과 Table 4.3을 비교해 보면 동일한 고장 "incorrect gear position"에 대한 원인 "sensor fault" 와 "actuator fault"의 우선순위가 변한다. 이 상황에서 우선순위는 발생도 및 검출도가 정확하게 추정되는 상태에서 효과적이다. RPM에서 발생도 및 검출도는 자연스럽게 원래의 개념을 반영한 확률에 의해 평가된다. 이러한 접근은 발생도 및 검출도에 대한 보다 객관적인 척도를 보장할 수 있다. 그러나 동시에 이용할 수 있는 충분한 데이터를 요구하므로 일반적인 상황에서는 가능하지 않을 수도 있다.

기존 FMEA의 RPN은 일반적으로 과거의 경험과 실무자 또는 엔지니어의 직관에 따라 결정되는 3가지 구성요소의 비율에 의존하므로 불가피하게 주관적인 경향이 있다. 또한 RPN 평가기법은 인간, 고장형태 및 운영 상황들 사이의 상호 작용을 고려하지 않는다. 그리고 동일하게 가중된 구성요소는 인정할 수 없는 우선순위 결과를 만든다. 기존 FMEA에서 주관성이 더하여 얻어진 RPN은 시정 또는 개선조치를 결정하는 절대적인 기준이 되지 않는다. 따라서 RPN은 각 고장원인에 대한 상대적 중요성의 대

략적인 평가결과만을 결국 제공한다. 그러나 RPM은 ASIL을 사용하여 보다 체계적이고 논리적으로 접근한다. 비록 ASIL 그 자체는 잘 구별되지 않는다 하더라도, 그 판정 절차는 고장뿐만 아니라 환경과 운전요인 및 운전상황을 고려한 상당히 논리적인 프로세스이다.



V. 결 론

5.1 연구결과

FMEA(Failure Mode Effect Analysis)는 설계 및 공정에서 발생할 수 있는 잠재적 고장유형을 식별하고 그 원인을 분석하여 위험을 평가하는 기법이다. 시스템이나 공정에 발생 가능한 문제점과 원인을 사전에 식별하여 예방이 가능하도록 할 뿐만 아니라 적용하기 쉽고 간단하여 1950년대 제조 산업에서 시작하여 지금은 서비스 산업에서도 매우 보편적으로 사용되고 있다. 그러나 FMEA의 위험평가 척도인 RPN은 구성요소에 대한 주관적인 점수 부여, 구성요소별로 동일한 중요도 적용, 평가결과 수치의 실질적 의미 결여 등을 포함한 여러 가지 단점으로 인하여 논리적이고 체계적인 척도로 인정받지 못하고 있다. 본 연구에서는 ISO 26262의 체계적이고 논리적인 위험평가프로세스인 H&R의 주요 출력물인 ASIL을 기반으로 FMEA의 RPN을 보완할 수 있는 새로운 위험평가척도 RPM을 제안하였다. RPM은 기존 FMEA의 문제점 중 많은 부분을 보완하며 각 고장모드 및 원인에 대한 위험의 중요성에 더 현실적인 정보를 제공할 수 있는 척도이다.

기존 FMEA의 단점을 보완하고 새로운 위험평가척도인 RPM을 제시하기 위하여 먼저 ISO 26262의 H&R 단계를 구체적으로 분석하였다. H&R의 단계별 검토과정에서 노출확률, 제어가능성에 대한 확률추정은 운전상황의 결정요인이 독립적일 경우와 상호 의존적인 경우 다르게 나타날 수

있으며, 그 결과 ASIL 등급에도 영향을 미친다는 것을 확인하였다. ISO 26262에서 H&R의 효과적인 수행을 위하여 운전상황 분석모형을 제안하였다. 모형을 예시로 제공된 “EPB 시스템”에 적용해봄으로써 산업현장에서 ISO 26262의 ASIL 결정을 위해 효과적으로 사용될 수 있음을 확인하였다.

다음으로 기존 RPN의 세 가지 구성요소 중 발생도 및 검출도를 확률치도로 변환하여 확률기반의 위험우선순위 척도인 RPM을 제안하였다. 확률을 이용한 추정수치는 기존 1~10등급 체계보다 효과적이고 합리적인 결과를 도출할 수 있도록 해준다. 따라서 RPM은 발생도 및 검출도에 대한 보다 객관적인 추정을 보장해준다. 또한, 시정 또는 개선조치를 위해 합리적인 우선순위를 제공할 뿐만 아니라 개선효과를 보다 객관적이고 의미 있는 수치로 평가할 수 있도록 해준다. RPM에 반영된 기존 FMEA의 세 가지 위험구성요소 중 심각도는 ASIL의 결정절차에 기초하여 결정될 수 있도록 하였다. 고장으로 인한 위험의 심각도는 운용상황, 환경, 운전자 상태에 영향을 받게 되므로 ASIL의 심각도 결정과정에서는 이들 요소 및 요소 간 상호작용을 고려하도록 하고 있다. 또한 ASIL 등급 결정을 위해 심각도 뿐만 아니라 위험사건에 노출될 확률과 위험상황을 제어할 수 있는 능력까지 고려하고 있으므로 ASIL 등급에는 고장에 기인된 위험요소들이 종합적으로 반영되어 있다고 할 수 있다. 본 논문에서 제안된 RPM은 이와 같이 체계적으로 결정된 ASIL 등급에 포함된 정보를 모두 반영하여 위험을 평가할 수 있도록 고안된 척도이다.

기존 FMEA와 비교하기 위하여 발생도 및 검출도의 경계 값에서의 확률변화에 대한 민감도분석을 검토하였다. 기존 FMEA에서는 위험의 내용이나 정도가 완전히 다른 경우에도 동일한 RPN 값을 가질 수 있다는 문제점이 있다. 이와 같은 상황에서 RPM은 어떤 결과를 보여주는지 검토하

기 위해 실시된 민감도분석 결과 RPM이 위험에 대한 변별력이 기존의 척도인 RPN보다 뛰어남을 보여주었다. 즉, RPN은 고장원인의 위험우선순위에 대해 혼동을 주거나 왜곡된 정보를 제공할 수 있는 반면, RPM은 검출되지 않은 위험의 예상 심각도를 반영하여 실제로 의미 있는 정보를 제공할 수 있었다.

마지막으로 사례 연구를 통하여 제안된 RPM의 타당성과 유효성을 검토하였다. 사례에서 RPM과 기존 RPN이 고장원인에 대한 우선순위가 상이하게 나타났다. 이것은 RPN이 구성요소에 대하여 동일한 가중치부여, 위험평가의 주관적 판단 및 고장모드와 영향사이의 상호의존성 무시 등으로 인해 왜곡된 정보를 제공할 수 있음을 나타낸다. 기존의 FMEA 매뉴얼에도 명시되어 있는 바와 같이 RPN의 결과는 시정 또는 개선조치를 결정하는 절대적인 기준이 되지는 못한다. 반면, RPM은 각 고장모드 및 그 원인에 대한 위험의 중요성에 현실적인 정보를 제공한다. 즉 RPM은 체계적이고 합리적인 과정을 통해 결정된 ASIL 등급에 기초한 심각도의 기대 값을 나타내기 때문에 상대적인 비교를 위한 위험우선순위뿐만 아니라 위험이 어느 정도인가를 나타내는 절대적인 값으로서도 실질적인 의미를 가지는 척도이다.

5.2 향후 연구방향

ISO 26262 표준에서는 ASIL 결정을 위한 운전상황 결정요인 중 인적요인을 배제하고 있음에 따라, 본 연구에서도 ASIL 결정을 위한 모형에서

인적요인이 배제되었다. 하지만 운전 중 운전자의 부적절한 행동은 다른 어떤 요인보다도 더 치명적인 사고를 유발할 수 있을 뿐만 아니라 운전자의 연령, 성별, 운전능력 등도 안전에 영향을 미친다. 또한, 고장원인의 발생확률 및 검출확률의 결정방법에 대한 구체적인 방법이 제시되어 있지 않다. 이러한 본 연구의 한계를 극복하기 위해서는 인적요인 반영 및 산업현장의 실제 데이터를 이용한 확률 값 측정 등에 관련된 추가 연구가 필요할 것으로 사료된다.

또한, 고장원인들이 상호 의존적으로 발생할 경우와 고장원인들이 계층적으로 얹혀 있는 경우는 산업현장에서도 자주 접할 수 있는 상황이므로 고장의 기능적 정보를 제공하는 동시에 정량적 리스크 평가를 위해 이에 대한 확장된 연구도 필요하다. 그리고 고장원인에 대한 관리방법의 변경에 따른 검출도의 변화를 고려하여 최적의 관리방법을 선택하는 의사결정문제로 확장하는 것도 가치 있는 연구가 될 것이다. 아울러 심각도 점수를 위험사건의 손실금액으로 산정하여 재무성과와 연계하는 것도 의미 있는 연구가 될 것이다.

Reference

- [1] 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.
- [2] Agung, S. and Kwon, H. (2010) "An Expected Loss model for Risk Prioritization in Service FMEA." *California Journal of Operations Management*, 8, 27-38.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] 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.
- [7] 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.

- [8] 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.
- [9] Chen, J. K. (2007) "Utility Priority Number Evaluation for FMEA," *Journal of Failure Analysis and Prevention*, 5, 321-328.
- [10] Chin, K. S., Wang, Y. M., Poon, G. K. K. and Yang, J. B. (2009a) "Failure mode and effects analysis by data envelopment analysis," *Decision Support Systems*, 48, 246-256.
- [11] Chin, K. S., Wang, Y. M., Poon, G. K. K. and Yang, J. B. (2009b) "Failure mode and effects analysis using a group-based evidential reasoning approach," *Computers and Operations Research*, 36, 1768-1779.
- [12] Cho, J. H., Jung, Y. J., Jeon, S. H., Han, T. M. and Kim, H. S. (2010) "An Implementation of automotive development methodology Based on ISO 26262", *The Korean Society of Automotive Engineers 2010 Annual Conference and Exhibition*, pp.2052-2059.
- [13] Chrysler LLC, Ford Motor Company and General Motors Corporation, (2008) *FMEA Reference Manual*, 4thed.
- [14] Ellims, M., Monkhouse, H. E. and Lyon, A. (2011) "ISO 26262: Experience Applying Part 3 To An In-Wheel Electric Motor", *IET International Conference on System Safety*, pp.1-8.
- [15] Ellims, M. and Monkhouse, H. E. (2012) "AGONISING OVER ASILS: Controllability and the In-Wheel Motor," *System Safety, Proceedings of Incorporation the cyber security conference*, pp.1-8.

- [16] Eubanks, C. F., Kmenta, S. and Ishii, K. (1997) "Advanced FMEA Using behavior Modeling." Proceedings of ASME Design Engineering Technical Conference, Sacramento, California, pp.1-10.
- [17] Ford Design Institute, (2004) FMEA handbook, Version 4.1.
- [18] 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, pp.102-110.
- [19] Ireson, W. G., Coombs, Jr. C. F. and Moss, R. Y. (1996) "Hand-book of reliability engineering and management Second Edition." McGraw-Hill.
- [20] ISO 26262-1 (2011) Road vehicles - Functional safety-part 1: Vocabulary.
- [21] ISO 26262-3 (2011) Road vehicles - Functional safety-part 3: Concept phase.
- [22] ISO 26262-4 (2011) Road vehicles - Functional safety-part 4: Product development at the system level.
- [23] ISO 26262-5 (2011) Road vehicles - Functional safety-part 5: Product development at the hardware level.
- [24] ISO 26262-10 (2011) Road vehicles - Functional safety-part 10: Guideline on ISO 26262.
- [25] Jang, H. A. (2015) "Risk Evaluation of Hierarchical Failure Causes in FMEA" Doctoral Thesis, Pukyong National University, Korea.
- [26] Jeegadeshnan, 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.
- [27] Jesty, P. H., Ward, D. D. and Rivett, R. S. (2007) “Hazard analysis for programmable automotive systems”, Technology International Conference on System Safety, pp.106-111.
- [28] Kim, B. C., Kim, S. S. and CHO, J. H. (2012) “ISO 26262 Fundamental technical guide”, Korean Foundation for Quality.
- [29] Kim, H. H., and Lee, N. H. (2012) “The Case Study on Software FMEA for the Efficient Improvement of Functional Safety,” KSAE 2012 Conference, 1303-1308.
- [30] Kim, S. Y., Yun, W. Y., Kim, H. G. (2007) “Reestablishment of RPN Evaluation Method in FMEA Procedure for Motors in Household Appliances”, Journal of Korean society for quality management, 35, pp.1-9
- [31] 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, pp.61-67.
- [32] 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.
- [33] Lee, D. K. and Jeon, J. H. (2013) “Method of hardware integration tests for ASIL achievement”, The Korean Society of Automotive Engineers 2013 Annual Conference and Exhibition, pp.2450-2456.

- [34] 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.
- [35] 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.
- [36] 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.
- [37] 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.
- [38] Liu, H. C., You, C., J. X., Fan, X. J. and Lin, Q. L. (2014) Failure mode and effects analysis using D numbers and grey relational projection method, Expert Systems with Applications, Vol. 41, pp. 4670-4679.
- [39] Roh, K. H. (2015) "Hazard Analysis and Risk Assessment for Determination of Automotive Safety Integrity Level Based on Ontology" Doctoral Thesis, Dongguk University, Korea.
- [40] Onodera, K. (1997) "Effective techniques of FMEA at each life-cycle stage" Proceeding of Annual Reliability and Maintainability Symposium, pp.50-56.

- [41] 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.
- [42] Reiling, J. G., Knutzen, B. L. and Stoecklein, M. (2003) "FMEA-the cure for medical errors." Qual. Progr., 8:67-71.
- [43] Rivett, R. S.(2009) "Hazard identification and classification: ISO 26262-the application of IEC 61505 to the automotive sector" SIL Determination, 2009 5th IET Seminar, pp.1-24.
- [44] Road Traffic Safety Association. (2013) "Analysis of Traffic Accident", No. 2013-0257-114, pp.43-54.
- [45] 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 Quality & Reliability Management, 3: 324-335.
- [46] Sawhney, R., Padiyar, A. and Li, Y. (2004). "FMEA based approach for supplier development," Proceedings of IIE Annual Conference and Exhibition, pp.7-16
- [47] Schlummer, M., Althaus, D., Braasch A. and Meyna, A. (2010) "ISO 26262 - The relevance and importance of qualitative and quantitative methods for safety and reliability issues regarding the automotive industry", Journal of KONBiN, pp.165-176.
- [48] Shahin, A. (2004) "Integration of FMEA and the Kano model: An exploratory examination." Int. J. Qual. Reliab. Manage., 21: 731-746.

- [49] Song, J. Y. (2013) "Proposal of Product Development Process considering ISO 26262, APQP" Master's Thesis, Chungnam National University, Korea.
- [50] 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.
- [51] Teng, S. G., Ho, S. M., Shumar, D. and Liu, P.C. (2006) "Implementing FMEA in a collaborative supply chain environment" *International Journal of Quality & Reliability Management*, Vol. 23, No.2, pp.179-196.
- [52] 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.
- [53] 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.
- [54] Xie, Y., Li, J. and Zhang, A. (2011) "Extended FMEA Method Applied in the Field of Functional Safety," *9th International Conference on Reliability, Maintainability and Safety(ICRMS)*, 615 -618.
- [55] Xu, K., Tang, L.C., Xie, M., Ho, S.L. and Zhu, M.L.(2002) Fuzzy assessment of FMEA for engine systems, *Reliability Engineering and System Safety*, Vol. 75, No.1, pp.17-29.

- [56] 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.
- [57] Yun, S. H., Kim, Y. J., Choi, Y.J., Kim, J.S. and Ahn, S.H. (2009) "A study on international standards and safety requirements for the development of automotive safety-related software", *The Korean Society of Automotive Engineers 2009 Annual Conference and Exhibition*, pp.1884-1890.
- [58] 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.
- [59] 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*, August 13-15, 2010, Dalian, China.
- [60] 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.
- [61] 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.

부록

국내·외 자동차 교통사고 통계분석

본 부록은 ISO 26262 파트3의 ASIL 결정을 위해 선행되어지는 자동차 운전상황 분석에 필요한 국내·외 교통사고와 관련된 통계자료를 필요에 따라 요약 정리한 것이다. 교통사고 통계자료는 일반적으로 다양한 내용을 다루고 있으나 여기서는 자동차 운전상황 분석 시 주로 고려될 수 있는 교통사고 발생요인을 중심으로 요약 정리하였다. 특히, 발생요인 중에서도 인적요인, 차량요인, 도로환경 및 기상상태요인을 중심으로 정리하였다.

1. 교통사고 용어정리¹⁾

1) 교통사고

- 차의 교통으로 인하여 사람을 사상하거나 물건을 손괴한 것을 말함
- 이 책자에서 교통사고는 경찰이 처리한 사람이 다치거나 사망한 사고의 자료를 근거로 함

2) 교통사고 인적피해 구분

- 사망 : 교통사고 발생 시로부터 30일 이내에 사망한 경우
(1999년까지는 72시간 내 사망)
- 중상 : 교통사고로 인하여 3주 이상의 치료를 요하는 부상을 입은 경우
- 경상 : 교통사고로 인하여 5일 이상 3주 미만의 치료를 요하는 부상

1) 본 용어정리는 2013년도 국가승인(협의)통계 제132020호 16~19페이지 인용함.

을 입은 경우

- 부상신고 : 교통사고로 인하여 5일 미만의 치료를 요하는 부상을 입은 경우

3) 인명피해에 따른 교통사고의 구분

- 대형사고 : 사망자가 3명 이상이거나 부상자(사망자 포함)가 20명 이상인 사고
- 사망사고 : 사망자가 1명 이상인 사고
- 중상사고 : 사망자 없이 중상자가 1명 이상인 사고
- 경상사고 : 사망자, 중상자 없이 경상자가 1명 이상인 사고
- 부상신고 사고 : 사망자, 중상자, 경상자 없이 부상신고자가 1명 이상인 사고

4) 사고 당사자 구분

- 제1당사자는 당해 교통사고에 관계한 사람 가운데 과실이 중한 사람을 의미함
- 사고 관련자 중 1당사자 이후의 당사자 순위는 당해 사고와의 관련성 정도를 기준으로 함

5) 차종의 구분

- 차 : 도로교통법 제2조의 규정에 의해 자동차, 건설기계, 원동기장치자전거, 자전거, 사람 또는 가축의 힘이나 그 밖의 동력에 의하여 도로에서 운전되는 것을 말함
- 자동차 : 자동차관리법 제2조의 규정에 의한 승용, 승합, 화물, 특수, 이륜차를 말함
- 건설기계 : 건설기계관리법 시행령 제2조 별표 1호 규정에 의한 19종 건설기계(덤프트럭, 아스팔트살포기, 노상안정기, 콘크리트 믹서기, 콘

크리트 펌프, 천공기 등)를 말함

- 경운기 : 농업기계화촉진법에 의한 농기계중 동력경운기 및 농업용 트랙터를 말함
- 원동기장치자전거 : 자동차관리법 제3조의 규정에 의한 이륜자동차 가운데 배기량 125cc이하의 이륜자동차 또는 배기량 50cc미만(전기를 동력으로 하는 경우에는 전격출력 0.59KW미만)의 원동기를 단 차를 말함

6) 교통사고의 유형

- 교통사고의 유형은 충돌유형과 대상에 따라 차 대 사람, 차 대 차, 차량단독, 차 대 열차로 구분함
- 차 대 차 사고 : 차와 다른 차가 충돌·추돌 또는 접촉한 사고
- 차 대 사람 사고 : 차가 보행자를 충격한 사고
- 차량단독 사고 : 운전자, 차, 도로상에 설치된 각종 시설물 또는 자연물이 원인이 되어 차가 스스로 전도·전복·추락·충격한 사고(차량단독 사고 후 그 충격 등으로 다른 차 또는 보행자를 충격한 경우 차량단독 사고로 처리)

7) 도로의 종류

- 도로의 구분은 도로법 제8조(도로의 종류와 등급)에 의한 분류에 따르며 도로의 종류는 고속국도, 일반국도, 특별시도·광역시도, 지방도, 시도, 군도, 구도 등으로 구분됨

8) 도로 형태

- 단일로 횡단보도상이란 해당 도로구간에서 차량의 교차가 발생하지 않은 경우로서, 횡단보도(안전표지 등으로서 보행자의 횡단용으로 사용할 수 있도록 표시되고 있는 부분) 위에서 발생한 사고를 말함

- 단일로 횡단보도부근이란 횡단보도가 설치되어 있는 경우에 그 측단에서 30m 이내의 도로부분에서 발생한 사고를 말함
- 단일로 터널 안이란 터널 내를 말하며, 입구의 도로부분은 포함하지 않음
- 단일로 교량위란 교량과 고가차도(철도 또는 도로와 교차하는 지점의 교통을 원활히 하기 위해 설치한 입체시설물) 위에서 발생한 사고를 말함
- 교차로 내란 교차로 내에서 발생한 사고를 말함
- 교차로부근이란 교차로 측단에서 30m 이내의 도로부분에서 발생한 사고를 말함
- 건널목이란 도로와 철도가 교차하는 구간으로 자동차단기, 간수, 경보기 등이 설치되어 있는 곳에서 발생한 사고를 말함
- 기타/불명이란 도로 등에 부속 설치된 서비스구역(휴게소, 주유소 등) 주차구역 등과 같이 상기 도로형태 어느 것에도 해당하지 않는 것을 말함

9) 주, 야의 구별

- 주간이란 일출부터 일몰까지, 야간은 일몰에서 일출까지 시간을 말함

10) 기상조건에 따른 구분

- 맑음이란 구름이 대략 80% 미만인 경우를 말함
- 흐림이란 구름이 대략 80% 이상인 경우를 말함
- 비란 비가 오고 있는 상태를 말함
- 안개란 물방울, 연기 등으로 인해 시야가 200m 이내인 경우를 말함
- 눈이란 눈, 진눈깨비, 우박이 오고 있는 상태를 말함

11) 치사율

- $[사망자/발생건수] \times 100$ (사고 100건당 사망자수를 의미함)

12) 사망률

- $[사망자/(사망자+부상자)] \times 100$ (사상자중에서 사망자가 차지하는 비율)

13) 사망사고율

- $[사망사고/인피사고] \times 100$ (전체사고 중 사망사고가 차지하는 비율)
- 상대사망사고율: 각 항목의 사망사고율을 평균 사망사고율로 나눈 값

14) 단위의 끝자리

- 반올림된 경우가 있으므로 합계와 불일치 할 수 있음

2. 국내 교통사고 분석 (발생요인 중심으로)²⁾

1) 인적요인별 특성

가. 운전면허취득 경과 년 수 별 교통사고

1당사자의 운전면허취득 경과 년 수별 발생건수는 면허취득 경과 년 수가 15년 이상 운전자의 사망사고가 45.1%인 2,331건으로 가장 많았으며, 다음으로는 5년 미만이 16.6%인 856건, 10년 이상 15년 미만이 14.9%인 772건, 5년 이상 10년 미만이 14.5% 749건 등의 순으로 나타났다. [Table A-1 / Figure A-1 참고]

2) 본 내용은 도로교통공단에서 발간한 「2013년판 교통사고 요인분석」 30~61페이지에서 인용하였음.

Table A-1 운전면허취득 경과 년 수별 교통사고

면허경과년수	구분		발생건수		사망자수		부상자수	
	건	구성비	명	구성비	명	구성비	명	구성비
계	5,165	100	5,392	100	3,273	100		
소계	856	16.6	905	16.8	696	21.3		
1년 미만	223	4.3	237	4.4	195	6.0		
1-2년 미만	173	3.3	181	3.4	171	5.2		
2-3년 미만	170	3.3	175	3.2	110	3.4		
3-4년 미만	132	2.6	149	2.8	55	1.7		
4-5년 미만	158	3.1	163	3.0	165	5.0		
5년 이상-10년 미만	749	14.5	777	14.4	591	18.1		
10년 이상-15년 미만	772	14.9	799	14.8	480	14.7		
15년 이상	2,331	45.1	2,442	45.3	1,322	40.4		
기타/불명	457	8.8	469	8.7	184	5.6		

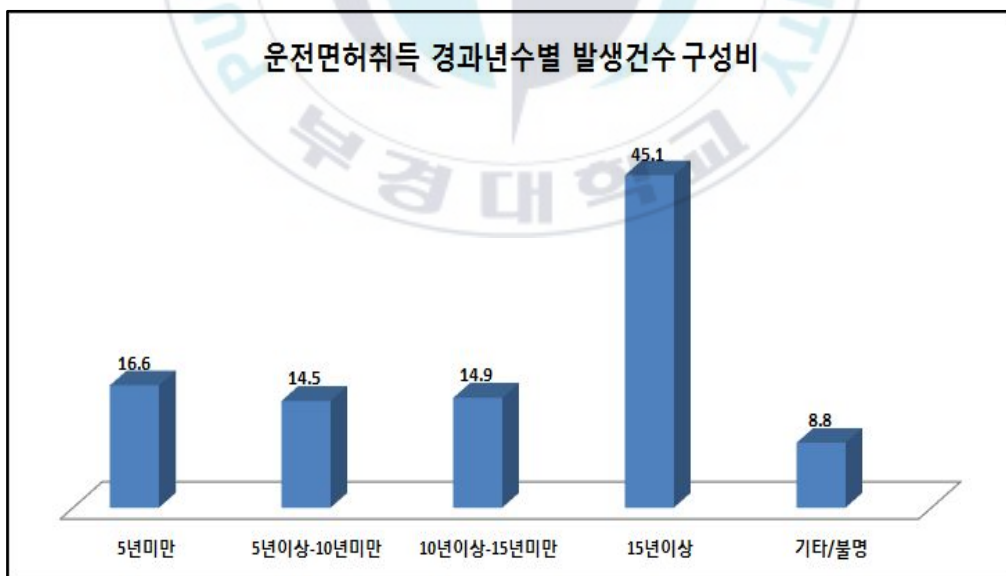


Figure A-1 운전면허취득 경과 년 수별 발생건수 구성비

나. 행동유형별 교통사고

사망사고의 1당사자 행동유형별 교통사고 발생건수는 직진중이 전체의 79.3%인 4,098건으로 가장 많았으며, 좌우 회전중이 11.1%인 572건, 진로 변경중이 2.7%인 141건, 후진중이 1.8%인 94건 등의 순으로 나타났다. 사망자수와 부상자수의 구성비 비교에서는 직진중과 앞지르기 중에 발생한 사망사고가 부상사고에 비해 상대적으로 많은 것으로 나타났으며, 그 외의 행동유형에서는 부상사고가 많이 발생한 것으로 분석되었다. [Table A-2 / Figure A-2 참고]

Table A-2 행동유형별 교통사고

구분 행동유형	발생건수		사망자수		부상자수	
	건	구성비	명	구성비	명	구성비
계	5,165	100	5,392	100	3,273	100.0
직진 중	4,098	79.3	4,288	79.5	2,626	80.2
좌우회전 중	572	11.1	592	11.0	326	10.0
U턴 중	54	1.0	54	1.0	62	1.9
출발 중	24	0.5	24	0.4	0	0.0
후진 중	94	1.8	95	1.8	5	0.2
앞지르기 중	42	0.8	47	0.9	30	0.9
진로변경 중	141	2.7	150	2.8	151	4.6
주·정차 중	20	0.4	20	0.4	19	0.6
기타/불명	120	2.3	122	2.3	54	1.6

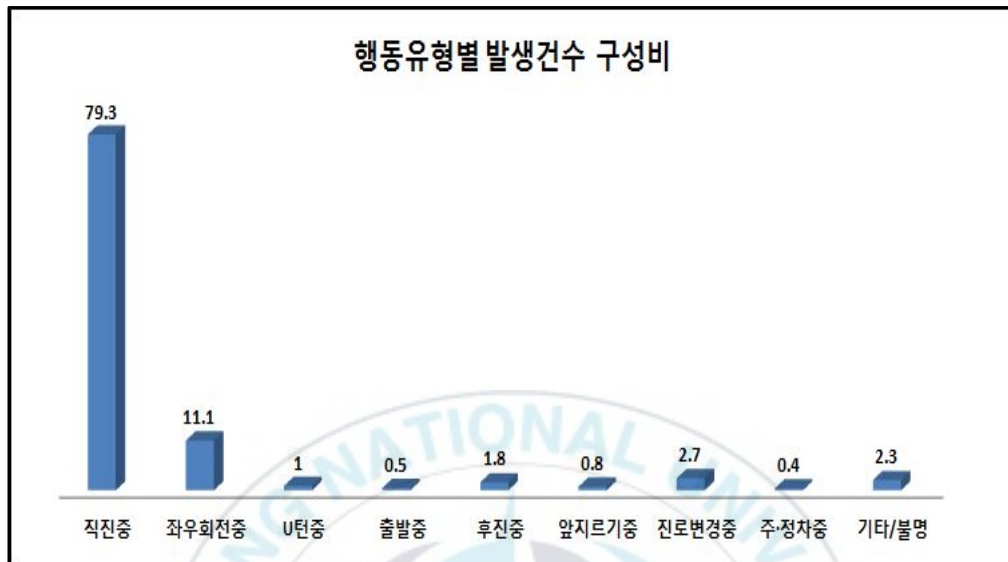


Figure A-2 행동유형별 발생건수 구성비

다. 인적유발요인별 교통사고³⁾

인적유발요인 1당사자 교통사고 발생건수를 보면 인적요인이 있는 경우는 전방주시태만으로 인한 교통사고가 2005년과 2006년 모두 약 55% 이상을 차지하여 가장 높았고 다음으로는 심심건강상태로 인한 사고가 2005년과 2006년 모두 높게 나타났다. 전체사고 중 인적요인이 없는 사고의 경우는 2005년과 2006년 모두 약 20%미만으로 나타났다. [Table A-3 / Figure A-3 참고]

3) 본 내용은 도로교통공단에서 발간한 「교통사고분석 자료집」 2007-3(통권3호) 70페이지에서 인용하였음.

Table A-3 인적 유발요인1당 교통사고

인적요인	구분	2005			2006		
		발생건수	사망자수	부상자수	발생건수	사망자수	부상자수
계		214,171	6,376	342,233	213,745	6,327	340,229
전방주시태만		125,482	3,717	200,493	128,935	3,799	204,262
환경요인에 의한 발견지연		2,614	118	4,486	1,559	98	2,414
심리적 요인에 의한 판단잘못		8,884	202	14,978	9,389	211	15,409
고의적 운전행태		1,672	20	2,898	1,670	36	2,831
차량조작 잘못		3,607	186	6,413	3,476	168	6,155
심신건강상태 불량		17,837	500	32,723	19,820	520	36,188
기타 인적요인 있음		5,057	178	7,570	3,189	121	4,878
인적요인 없음		40,645	829	61,908	39,364	886	60,100
기타/불명		8,373	626	10,764	6,343	488	7,992

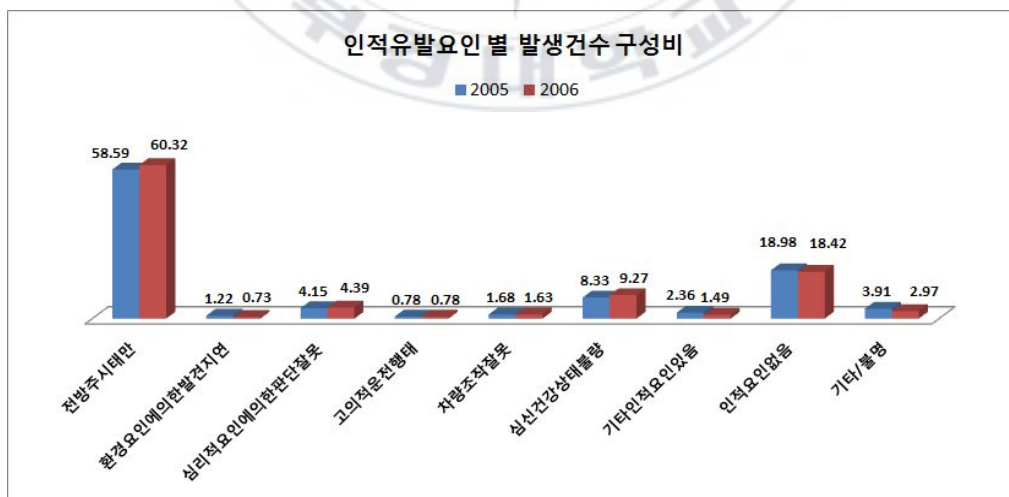


Figure A-3 인적유발요인별 발생건수 구성비

2) 차량적 유발요인별 특성4)

차량적 유발요인 1당사자 교통사고 발생건수를 보면 차량적 요인이 있는 경우는 제동장치 불량 2005년 612건인 0.29%로 2006년 530건 0.25%로 가장 많았으며 다음으로는 적재물 안전조치 불량이 차지하였다. 그리고 전체 교통사고 건수 중에서 차량적 요인이 없는 경우가 2005년 2006년 모두 발생건수의 90% 이상을 차지하여 가장 많았다. [Table A-4 / Figure A-4 참고]

Table A-4 차량적 유발요인 1당

구분 차량요인	2005			2006		
	발생 건수	사망 자수	부상 자수	발생 건수	사망 자수	부상 자수
계	214,171	6,376	342,233	213,746	6,327	340,229
제동장치 불량	612	11	1,234	530	24	1,132
조향장치 불량	187	4	329	154	8	265
엔진장치 불량	14	3	28	22	0	46
타이어 불량	192	24	416	198	43	445
등화장치 불량	19	3	24	9	1	11
불법개조	5	1	6	4	1	8
과도한 선풍	10	0	11	9	0	12
적재물 안전조치 불량	270	10	444	193	6	294
기타(차량적 요인 있음)	7,472	227	11,797	3,284	91	5,194
차량적요인 없음	197,731	5,622	38,052	204,018	5,829	326,277
기타/불명	7,659	471	9,892	5,324	324	6,545

4) 본 내용은 도로교통공단에서 발간한 「교통사고분석 자료집」 2007-3(통권3호) 70페이지에서 인용하였음.

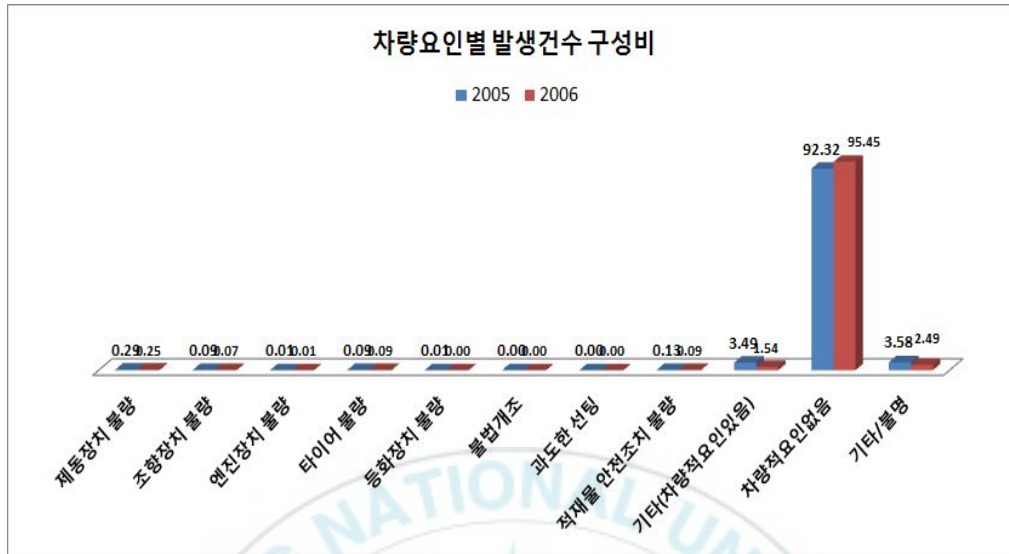


Figure A-4 차량요인별 발생건수 구성비

3) 도로환경요인별 특성

가. 도로종류별 교통사고

사망사고의 도로종류별 발생현황은 특별·광역시도에서 25.2%인 1,300건이 발생하여 가장 많았으며, 다음으로는 시도 23.2%인 1,196건, 일반국도가 20.1%인 1,040건, 지방도가 15.5%인 800건 등의 순으로 나타났다. 사망사고와 부상사고의 구성비 비교에서는 일반국도와 지방도, 군도, 고속국도에서는 사망사고의 구성비가 부상사고에 비해 상대적으로 높은 반면, 특별·광역시도와 시도에서는 사망사고의 구성비가 상대적으로 낮은 것으로 나타났다. [Table A-5 / Figure A-5 참고]

Table A-5 도로종류별 교통사고

도로종류 \ 구분	발생건수		사망자수		부상자수	
	건	구성비	명	구성비	명	구성비
계	5,165	100	5,392	100	3,273	100
일반국도	1,040	20.1	1,101	20.4	756	23.1
지방도	800	15.5	830	15.4	585	17.9
특별광역시도	1,300	25.2	1,333	24.7	597	18.2
시도	1,196	23.2	1,236	22.9	589	18.0
군도	305	5.9	319	5.9	119	3.6
고속국도	325	6.3	371	6.9	604	18.5
기타	199	3.9	202	3.7	23	0.7

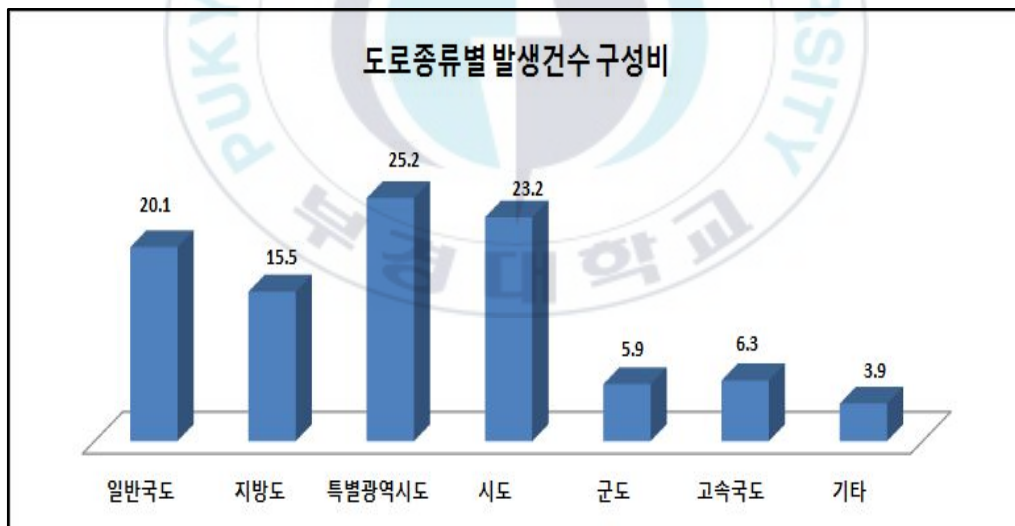


Figure A-5 도로종류별 발생건수 구성비

나. 도로형태별 교통사고

사망사고의 도로형태별 발생현황은 단일 로에서 발생한 사고가 3,585건으로 전체 사망사고의 69.4%, 교차로에서 발생한 사고는 1,428건으로 전체의 27.6%로 나타나 단일로가 교차로에 비해 사망사고가 2.5배가 많은 것으로 나타났다. 사망사고와 부상사고의 구성비를 비교해 보면 단일 로에서는 사망사고 발생률이 부상사고에 비해 상대적으로 높은 반면, 교차로에서는 부상사고가 발생률이 사망사고 발생률에 비해 높은 것으로 나타났다. [Table A-6 / Figure A-6 참고]

Table A-6 도로형태별 교통사고

도로형태		구분		발생건수		사망자수		부상자수	
		구분		건	구성비	명	구성비	명	구성비
계				5,165	100	5,392	100	3,273	100
소계				3,583	69.4	3,755	69.6	2,297	70.2
단 일 로	횡단보도 상			235	4.5	239	4.4	41	1.3
	횡단보도 부근			95	1.8	100	1.9	19	0.6
	터널 안			40	0.8	44	0.8	47	1.4
	교량 위			80	1.5	87	1.6	60	1.8
	기타단일로			3,133	60.7	3,285	60.9	2,130	65.1
소계				1,428	27.6	1,475	27.4	908	27.7
교 차 로	교차로 내			892	17.3	922	17.1	647	19.8
	교차로부근			536	10.4	553	10.3	261	8.0
건널목				2	0.0	3	0.1	1	0.0
고가도로 위				26	0.5	28	0.5	27	0.8
지하도로 내				8	0.2	9	0.2	4	0.1
기타/불명				118	2.3	122	2.3	36	1.1

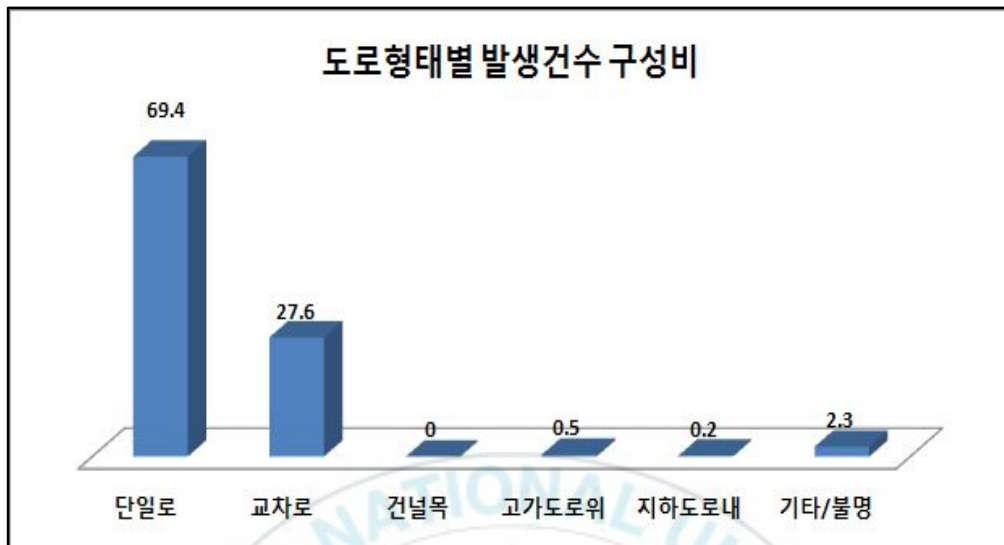


Figure A-6 도로형태별 발생건수 구성비

다. 도로선형별 교통사고

사망사고의 도로선형별 발생현황은 직선로에서 전체의 80.3%인 4,148건이 발생하여 대부분을 차지하였으며, 커브·곡각도로에서는 19.1%인 987건이 발생한 것으로 나타났다. 세부 도로선형별 사망사고 발생건수 구성비를 부상사고와 비교해보면 사망사고는 부상사고에 비해 커브곡각도로에서의 사고가 상대적으로 많이 발생한 반면, 직선도로에서는 부상사고 발생률이 사망사고에 비해 상대적으로 높은 것으로 나타났다. [Table A-7 / Figure A-7 참고]

Table A-7 도로선형별 교통사고

도로선형 구분		발생건수		사망자수		부상자수	
		건	구성비	명	구성비	명	구성비
계		5,165	100	5,392	100	3,273	100
소계		491	9.5	525	9.7	471	14.4
좌 커 브	오르막	56	1.1	66	1.2	58	1.8
	내리막	158	3.1	174	3.2	221	6.8
	평지	277	5.4	285	5.3	192	5.9
소계		496	9.6	529	9.8	429	13.1
우 커 브	오르막	76	1.5	78	1.4	66	2.0
	내리막	132	2.6	142	2.6	103	3.1
	평지	288	5.6	309	5.7	260	7.9
소계		4,148	80.3	4,308	79.9	2,359	72.1
직 선	오르막	265	5.1	278	5.2	159	4.9
	내리막	364	7.0	384	7.1	217	6.6
	평지	3,519	68.1	3,646	67.6	1,983	60.6
기 타		30	0.6	30	0.6	14	0.4

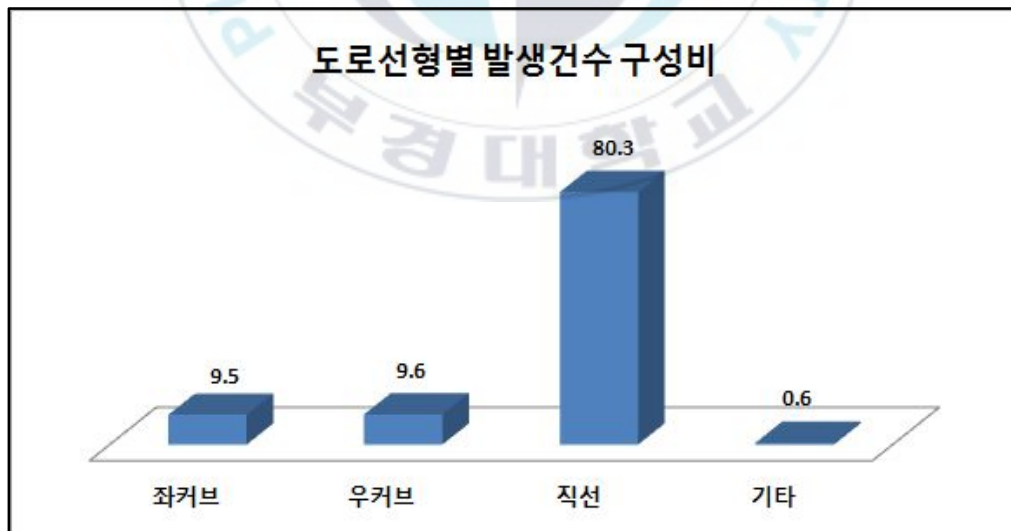


Figure A-7 도로선형별 발생건수 구성비

라. 기상상태별 교통사고

사망사고의 기상상태별 발생현황은 맑은 날에 사망사고가 78.7%인 4,067건이 발생하여 대부분을 차지하였으며, 다음으로는 비 오는 날이 11.4%, 흐린 날이 7.6%, 눈 오는 날이 1.2%, 안개 낀 날이 0.6% 등의 순으로 나타났다. 사망사고와 부상사고의 구성비를 비교해 보면 사망사고는 부상사고에 비해 맑은 날에는 상대적으로 적게 발생한 반면, 흐린 날과 비 오는 날, 안개 낀 날에는 부상사고에 비해 상대적으로 많이 발생한 것으로 나타났다. [Table A-8 / Figure A-8 참고]

Table A-8 기상상태별 교통사고

도로선형 \ 구분	발생건수		사망자수		부상자수	
	건	구성비	명	구성비	명	구성비
계	5,165	100	5,392	100	3,273	100
맑음	4,067	78.7	4,233	78.5	2,545	77.8
흐림	392	7.6	407	7.5	253	7.7
비	587	11.4	625	11.6	420	12.8
안개	31	0.6	35	0.6	19	0.6
눈	61	1.2	63	1.2	33	1.0
기타/불명	27	0.5	29	0.5	3	0.1

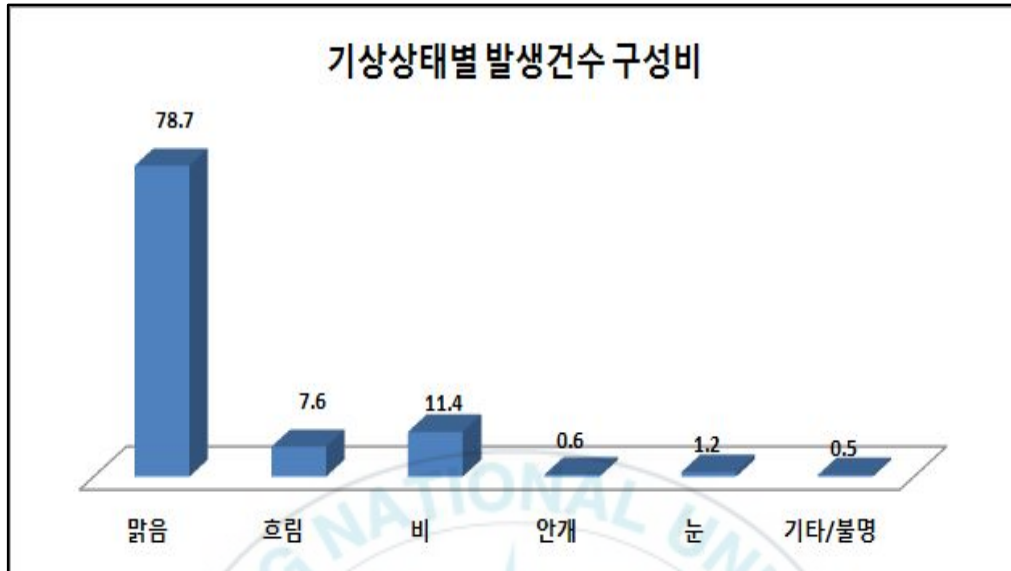
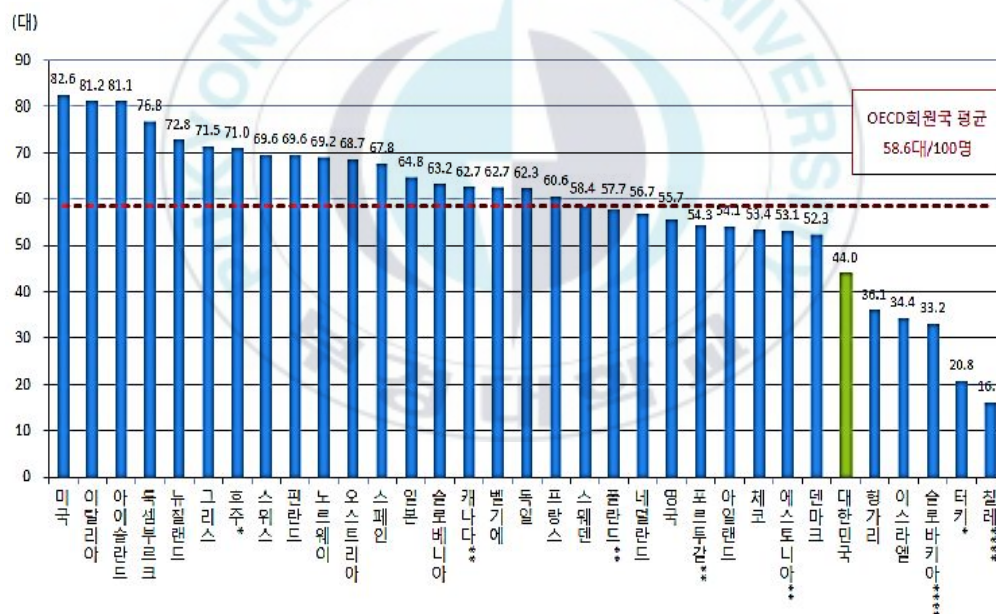


Figure A-8 기상상태별 발생건수 구성비

3. OECD 회원국 교통사고 비교⁵⁾

1) 교통여건

2011년 기준 OECD 주요국의 인구, 자동차 보유대수, 국토면적 1인당 GDP와 도로연장 등 교통여건을 비교한 결과를 그림으로 설명한다. Figure A-9는 인구 100명당 자동차 보유대수를 보여주고 있다. 미국이 82.6대로 가장 많고, 다음으로 이탈리아 81.2대, 아이슬란드 81.1대 등의 순이었다. 우리나라는 OECD 평균인 58.6대의 약 75.1% 수준인 44.0대의 자동차를 보유하고 있는 것으로 나타났으며 이는 33개국 중 28번째로 많은 수치이다.



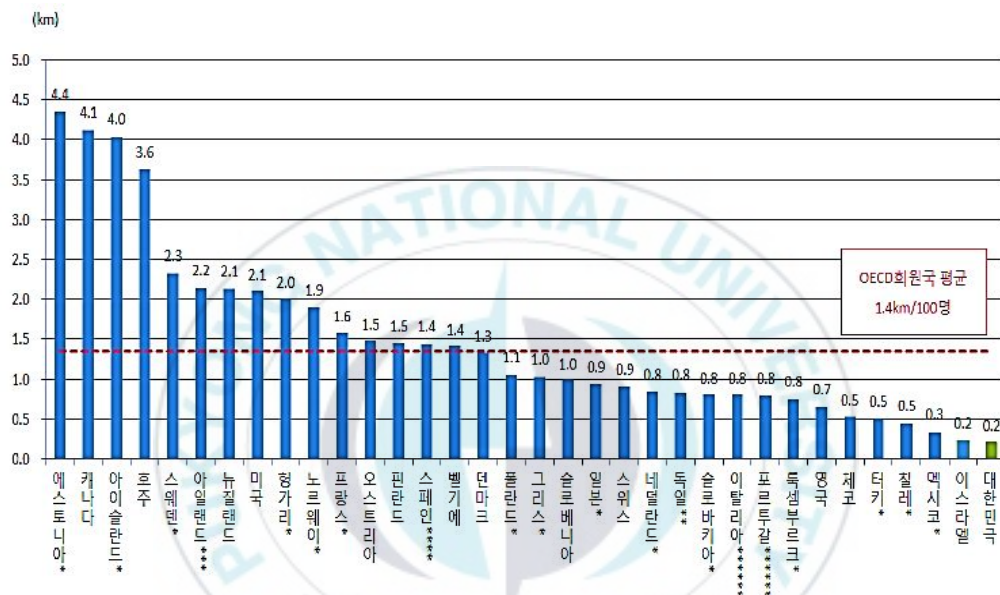
주) 인구1명당 자동차보유대수 = (자동차보유대수/인구)×100

*-2010년, **-2009년, ***-2008년, ****-2007년

Figure A-9 인구 100명당 자동차 보유대수(2011년)

5) 본 내용은 도로교통공단에서 발간한 「OECD회원국 교통사고 비교」 2013년판 1~42페이지에서 인용하였음.

Figure A-10과 같이 인구 100명당 도로연장은 에스토니아가 4.4Km로 가장 길었고, 다음으로 캐나다 4.1Km, 아이슬란드가 4.0Km, 호주가 3.6Km 등의 순이었다. 우리나라는 OECD 회원국 중 가장 짧은 0.2Km로 OECD 회원국 평균인 1.4Km의 약 14% 수준이었다.



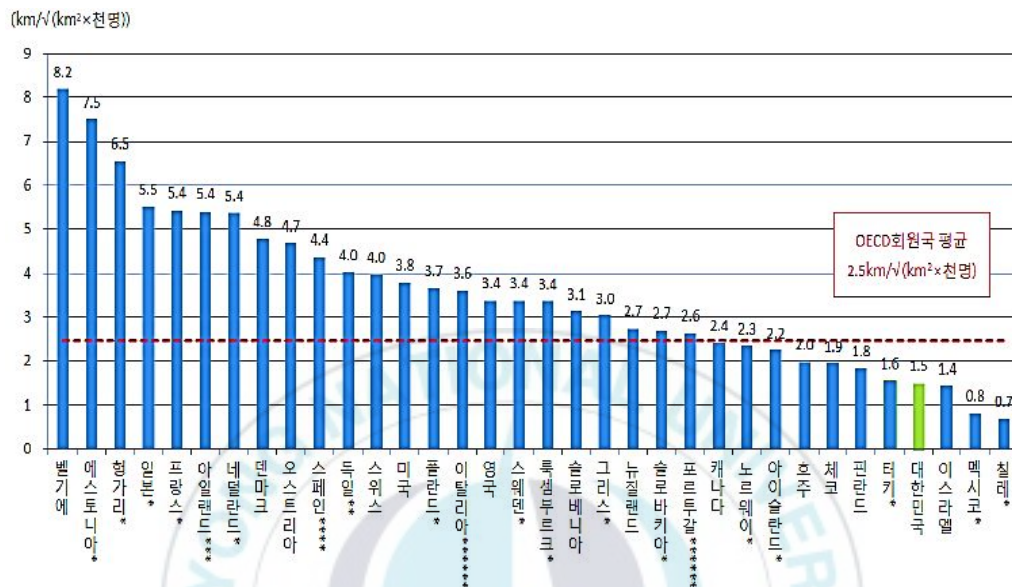
주) 인구1명당 도로연장 = (도로연장/인구)×100

*-2010년, **-2009년, ***-2008년, ****-2007년, *****-2006년, *****-2005년

Figure A-10 인구 100명당 도로연장(2011년)

Figure A-11은 인구, 국토면적과 도로연장 사이의 관계를 나타낸 국토계수당 도로밀도를 비교한 것이다. 국토계수당 도로밀도는 벨기에가 8.2로 가장 높았고 다음으로 에스토니아 7.5, 헝가리 6.5, 일본 5.5, 프랑스, 아일랜드, 네덜란드가 각각 5.4등의 순이었다. 우리나라는 1.5로 전체 OECD 국가 중 31번째로 높게 나타났으며 OECD 회원국 평균인 2.5의 약 60% 수준

이었다. 우리나라보다 국토계수당 도로밀도가 낮은 나라로는 이스라엘, 멕시코, 칠레가 있었다.

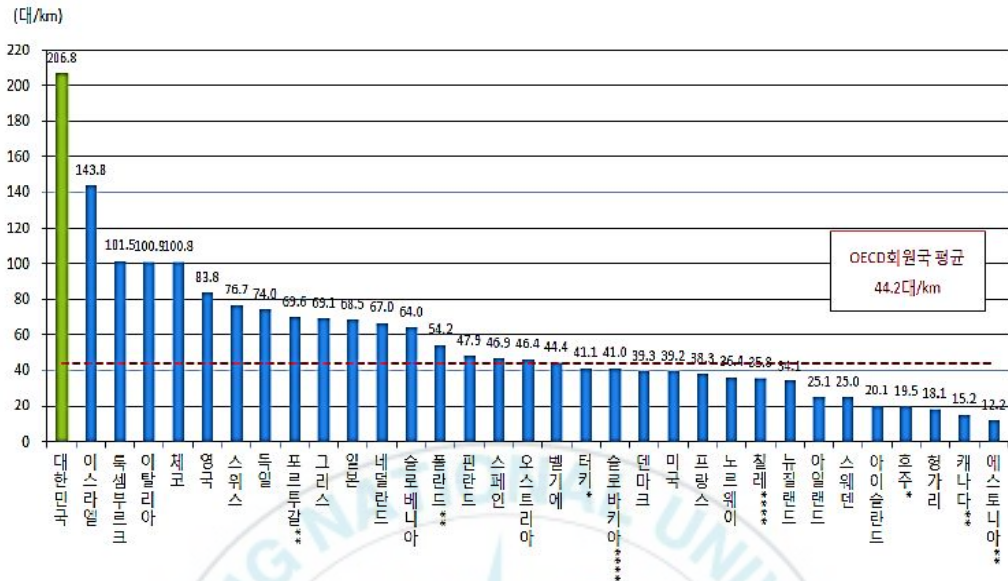


주) 국토계수당 도로밀도 = 도로연장/(국토면적×인구)^{1/2}

*-2010년, **-2009년, ***-2008년, ****-2007년, *****-2006년, *****-2005년

Figure A-11 국토계수당 도로밀도(2011년)

Figure A-12와 같이 도로연장 1Km당 자동차 보유대수는 우리나라가 206.8대로 가장 많았다. 멕시코와 칠레를 제외한 OECD 32개국의 평균은 44.2대로 우리나라는 이에 비해 4.7배 이상 많았다.



주) 도로연장 1Km당 자동차 보유대수 = (자동차 보유대수/도로연장)

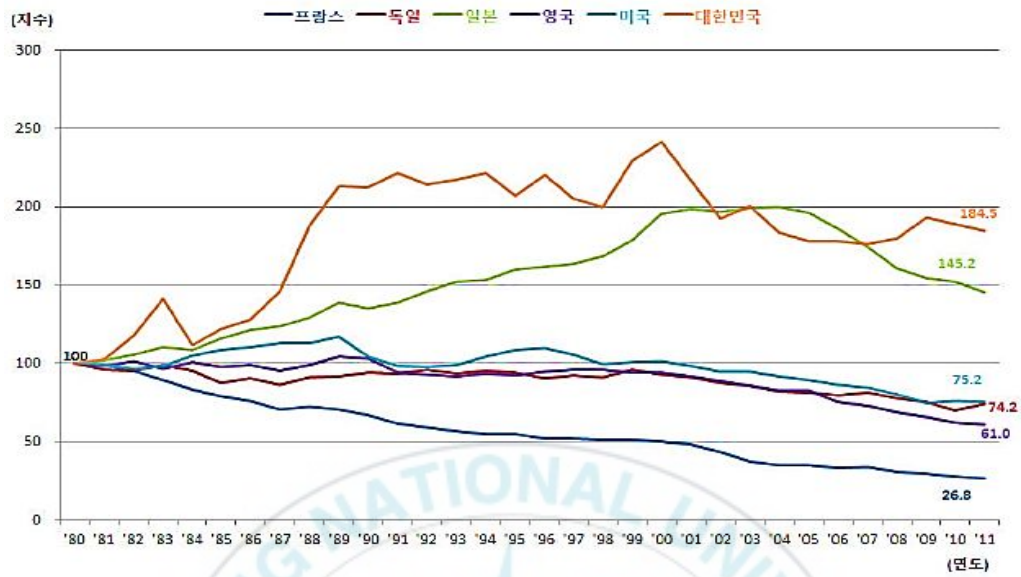
*-2010년, **-2009년, ***-2008년, ****-2007년

Figure A-12 도로연장 1Km당 자동차 보유대수(2011년)

2) 교통사고 발생건수 추세

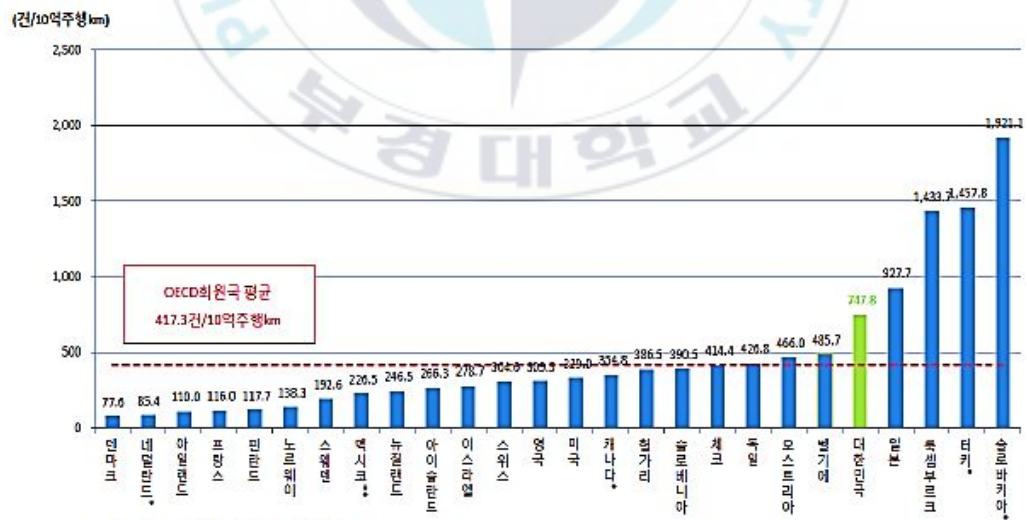
Figure A-13은 1980년을 기준으로 한 주요국의 교통사고 발생지수를 나타낸 것이다. 프랑스, 독일, 영국과 미국은 1980년에 비해 교통사고가 감소하였다. 특히 프랑스는 1980년에 비해 2011년의 교통사고 30%이하 수준으로 감소한 것으로 나타났다. 반면 우리나라와 일본은 1980년에 비해 2011년의 교통사고가 각각 1.8배, 1.5배 증가한 것으로 분석되었다.

Figure A-14는 OECD 국가별 10억 주행 Km당 교통사고 발생건수는 덴마크가 77.6건으로 가장 적었으며, 우리나라는 747.8건으로 파악된 27개국 중 22위를 차지하였다. OECD 회원국의 평균 10억 주행 Km당 교통사고 발생건수는 417.3건으로 우리나라는 평균대비 약 1.8배 많은 것으로 나타났다.



주 : 1) 교통사고 발생지수 = (해당 연도 발생건수/1980년 발생건수) × 100
 자료 : <http://internationaltransportforum.org/IRTADUsers>, 13.7

Figure A-13 주요국의 교통사고 발생지수

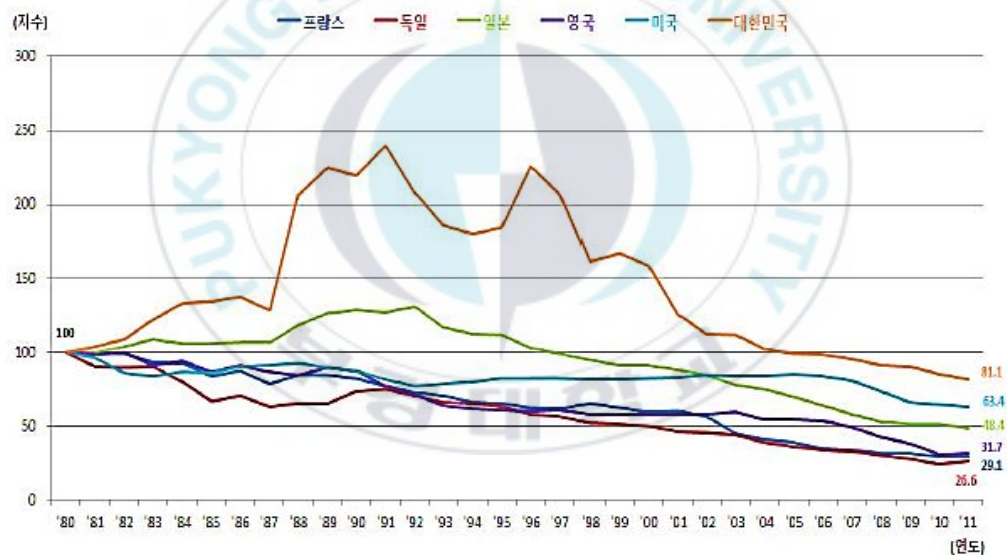


주 : 1) * - 2010년, ** - 2009년
 자료 : <http://internationaltransportforum.org/IRTADUsers>, 13.7

Figure A-14 10억 주행 Km당 교통사고 발생건수(2011년)

3) 교통사고 사망자수 추세

Figure A-15는 1980년을 기준으로 한 주요국의 교통사고 사망지수를 나타낸 것이다. 1980년을 지수 100으로 하였을 때, 2011년 우리나라는 81.1, 프랑스 29.1, 독일 26.6, 영국 31.7 등으로 우리나라를 비롯한 주요국가 모두에서 1980년에 비해 사망자수가 감소한 것으로 나타났다. 특히 프랑스, 독일과 영국의 경우 2011년 사망자수가 1980년에 비해 절반 이하로 감소했으며, 일본 역시 절반 가까이 감소한 반면 우리나라는 약 19% 감소하는데 그친 것으로 나타났다.



주 : 1) 교통사고 사망지수 = (해당 연도 사망자수/1980년 사망자수) × 100

자료 : <http://internationaltransportforum.org/IRTADUsers>, '13.7

Figure A-15 주요국의 교통사고 사망지수

4) 교통사고 발생현황

Figure A-16과 같이 전년대비 교통사고 발생건수 증감률은 네덜란드가 -44.4%로 감소 폭이 가장 컸고, 터키가 27.3%로 증가폭이 가장 컸다. 32개국 중 23개국에서도 전년도에 비해 교통사고 발생건수가 감소했고, 9개국은 증가하였다.

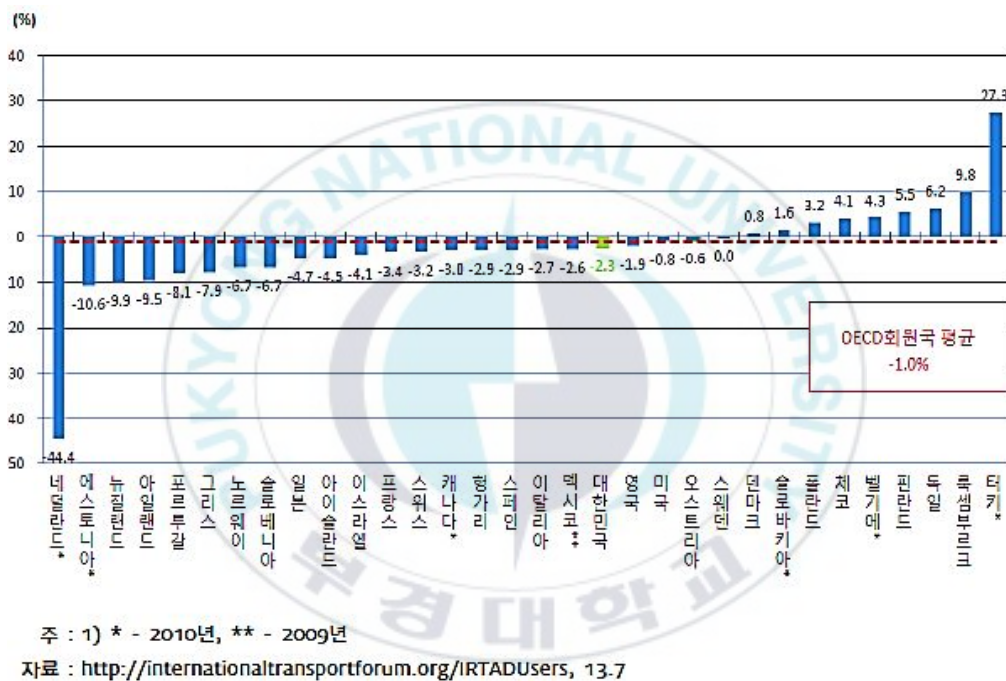
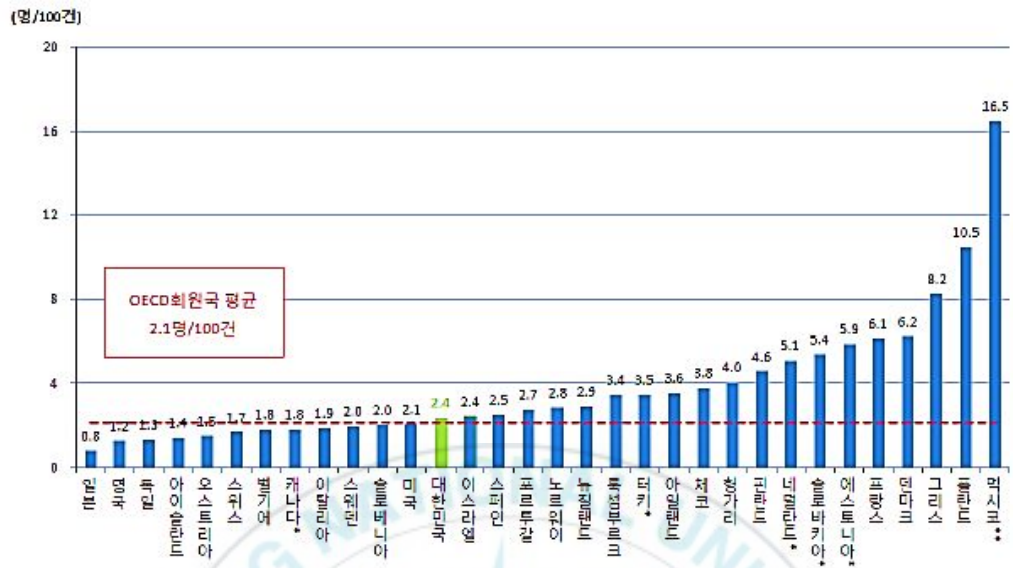


Figure A-16 전년대비 교통사고 발생건수 증감률

Figure A-17과 같이 교통사고 100건당 사망자수인 치사율은 일본이 0.8로 가장 낮았고, 다음으로 영국 1.2, 독일 1.3, 아이슬란드 1.4 등의 순으로 낮았다. 반면 멕시코가 16.5로 가장 높았고, 다음으로 폴란드 10.5, 그리스 8.2 등의 순으로 높았다. OECD 회원국의 평균 치사율은 2.1이었는데, 우리나라는 평균보다 약간 높은 2.4로 32개국 중 13위를 차지하였다.



주 : 1) 치사율 = (사망자수/발생건수) × 100
 2) * - 2010년, ** - 2009년
 자료 : <http://internationaltransportforum.org/IRTADUsers>, 13.7

Figure A-17 교통사고 치사율

감사의 글

설레임과 두려움으로 시작했던 기술경영(MOT) 박사과정을 마치는 문턱에서 지난 시간을 되돌아봅니다. 늦게나마 배움이 좋아서 나름 열정적이고 부지런히 생활하였고, 기쁨과 깨달음이 많은 시간이었습니다. 이렇게 작은 열매 하나를 맺으면서 도와주신 많은 분들께 감사의 마음을 전합니다.

뒤늦은 배움을 끝까지 마칠 수 있을지 자신할 수 없었던 지난 시간동안 끊임없는 지도와 관심으로 이끌어 주신 권혁무 지도교수님 진심으로 감사드립니다. 논문심사를 해주시면서 세심한 검토와 조언을 주신 구평희 교수님, 옥영석 교수님, 양성민 교수님 그리고 차명수 교수님 감사합니다. 학위과정동안 음으로 양으로 따뜻한 관심과 후의를 베풀어주신 김병남 교수님, 이운식 교수님, 오수철 교수님, 고시근 교수님, 김영진 교수님, 김민수 교수님, 박병무 교수님, 서원철 교수님, 신승준 교수님 등 학부 교수님들과 과정동안 많은 지식을 주셨던 홍재범 교수님, 김정배 교수님, 최승욱 박사님께도 감사의 말씀 드립니다. 그리고 든든한 학과사무실 지킴이 정현진 선생님을 비롯하여 행정 일로 불편함이 없도록 지원해 준 이은주 선생님, 김나경 선생님, 정유경 선생님께 감사합니다.

자기계발의 중요성을 강조하시면서 지속적으로 지원을 해주시는 한국품질재단 유병택 이사장님, 남대현 대표님, 윤석운 원장님, 양기성 본부장님, 염순홍 원장님, 송지영 원장님과 모든 임직원 감사합니다. 특히 부산,경남 지역본부에서 바쁜 업무에도 최선을 다하는 안경준 과장과 김혜환 매니저

에게도 고마움을 전합니다.

힘들고 어려울 때 항상 많은 조언과 도움을 주신 이명주 교수님, 이병룡 박사님, 이희식 박사님, 유진희 박사님, 최후림 박사님, 장현애 박사님 감사합니다. 그리고 배움을 같이하며 열심히 최선을 다한 MOT 선배님들 감사합니다.

마지막으로 농사지으시며 7남매 훌륭하게 키워주신 부모님 정말 감사합니다. 항상 인생의 참된 의미를 되새겨 주시는 장인, 장모님 감사합니다. 집안의 든든한 기둥인 큰 누님, 매형 감사합니다. 무엇보다 제일 기뻐하고 축하해 주었을 동생 영애 너무 보고 싶습니다. 그리고 옆에서 항상 힘과 용기가 되어준 아내 박선민과 아들 종훈 사랑합니다.

