Journal of the Korean Society of Safety, Vol. 29, No. 4, pp. 160-167, August 2014

http://dx.doi.org/10.14346/JKOSOS.2014.29.4.160

ASIL 결정을 위한 기능안전 운전상황 분석 모형

백명식 · 장현애* · 권혁무†*

한국품질재단 부산경남지역본부 · *부경대학교 시스템경영공학부

(2014. 2. 13. 접수 / 2014. 7. 15. 채택)

A Model of Operational Situation Analysis with Functional Safety for ASIL Determination

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

Busan & Gyeongnam Regional Division, Korean Founation for Quality

*Department of Systems Management and Engineering, Pukyong National University

(Received February 13, 2014 / Accepted July 15, 2014)

Abstract : 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. In this paper, we try to present a systematic model for classifying the three properties of the hazardous event and suggest a refined procedure of ASIL determination. The proposed model provides a specific method to get a more objective ASIL compared with that in the standard. Scrutinizing the current methodology, we develop a refined method and also provide an illustrative example.

Key Words : ISO26262, H&R (Hazard Analysis and Risk Assessment), ASIL (Automotive Safety Integrity Level).

1. 서 론

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 ASIL(Automotive Safety Integrity Level: 자동차 안전무결성 수준)은 아이템이나 엘리먼트에 있어서는 안 될 잔존 리스크를 방지하기 위해 적용되는 안전무결성 등급[1]이다. 따라서 ASIL은 안전목표와 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 안전목표가 정해지는데 이를 통해 세부적인 안전요구사항을 도출하고 기능안전개념(Functional Safety Concept)을 기술하게 된다. 기능안전개념은 다시 시스템 수준의 제품 개발에서 기술적 안전 요구사항으로 구체화된다.[2]

이와 같이 ASIL은 가장 우선적으로 결정될 뿐만 아니라 제품의 안전요구사항평가지표를 제공하기 때문에 시스템 개발의 핵심 요소라고 할 수 있겠다. 그러나 이러한 중요성에도 불구하고 ISO 26262에서는 ASIL 결정 절차와 관련하여 대략적인 가이드라인만 제공할 뿐 구체적인 수행절차나 방법론을 안내하고 있지 않다.[3] 또한 표준 파트3의 부록 B에서 제공하고 있는 예

† Corresponding Author : Hyuck Moo Kwon, Tel : +82-51-629-6480, E-mail : iehmkwon@pknu.ac.kr
Department of Systems Management and Engineering, Pukyong National University, 45 Yonso-ro, Nam-gu, Busan 608-737, Korea

시에서도 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 않다. 먼저 국내 연구로는 ISO 26262 요건을 충족하면서 개발체계 수립에 참조할 수 있는 기능안전성 중심의 자동차 개발 방법론을 소개하는 연구[4]와 ASIL 성취를 위한 하드웨어 통합단계에 관한 연구가 있다.[5] 해외 연구로는 위험원 분석과 관련된 연구가 있는데 원인결함연결고리모형(Causal Chain Linking Faults Model)을 기반으로 한 연구[6]와 IEC 61508의 방법론을 적용한 연구[7] 그리고 ISO 26262에서 위험원 분석 및 평가 절차에 관련된 연구가 있다.[8] 그리고 ASIL 결정에 관한 연구로는 개념설계 단계의 실증적 분석을 위해 휠 내장 전기모터(In-wheel Electric Motor)에 적용한 사례 연구가 있다.[3),9)] 그러나 ASIL결정 절차의 구체적 방안을 제시하는 연구는 찾아보기 어려운 실정이다.

본 논문에서는 ASIL결정에서 가장 중요한 단계인 위험사건분류와 관련된 절차들을 체계화하여 제시하고자 한다. 2장에서는 ASIL결정을 위해 수행되는 H&R(Hazard Analysis and Risk Assessment: 위험원 분석 및 리스크 평가) 단계를 구체적으로 분석한다. 3장에서는 위험사건분류에 필요한 운전상황의 범주를 표준을 토대로 정의하고 하위 범주를 상세화하였다. 4장에서는 위험사건 분류를 위한 체계적인 방법을 소개하고 5장에서는 적용사례를 들어 설명한다. 끝으로 6장에서는 논문의 주제를 요약하고 향후 연구 방향에 대해 기술한다.

2. 표준에 의한 H&R 및 ASIL 결정의 한계

2.1. 위험원과 위험사건

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 안전목표를 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

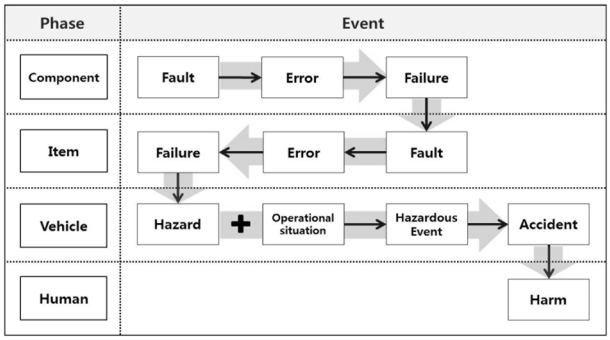

Fig. 1. Fault leading to harm.

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. Fig. 1은 위험원 및 위험사건을 보다 명료하게 이해할 수 있도록 위해의 발생과정을 시간 순으로 정리한 것이다.

Fig. 1에 의하면 아이템 고장에 의해 유발된 오동작(위험원)은 운전상황과 결합되어 위험사건이 된다. 위험사건의 결과로 사고가 발생하고 사고의 결과로 위해가 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.

Fig. 2는 ISO 26262 파트10에서 제공하고 있는 위험사건의 예시를 재배열하여 나타낸 것으로 아이템 고장으로 인해 발생할 수 있는 위험사건과 가능한 위험사건의 결과를 보여주고 있다.[10]

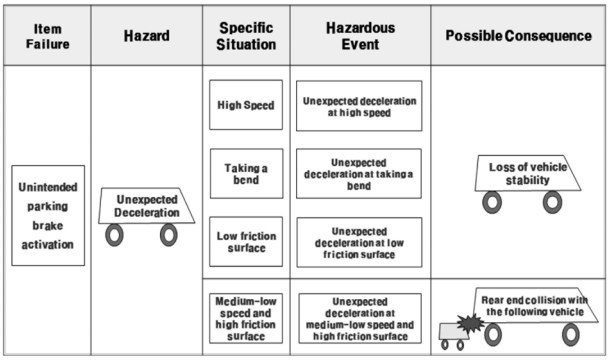

Fig. 2. Example of EPB system's hazardous event.

2.2. ASIL 결정절차의 한계

ISO 26262에서는 ASIL 등급결정을 위해 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.[11)]

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.[12)] 심각도 결정은 위험사건을 정성적으로 평가하여 약식상해등급(AIS)으로 분류하는 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 발생빈도로 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 최저 수준인 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 판단된다. 따라서 표준의 실용성을 높일 수 있도록 좀 더 체계적이고 구체화된 ASIL결정 방법론의 개발이 필요하다고 하겠다.

3. 운전상황 분석 및 ASIL 결정단계

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 사용 범위를 정해야 한다. 그러나 ISO 26262에서도 이것과 관련된 명확한 내용을 구체적으로 기술하고 있지 않으므로 파트3의 부속서B에서 제공한 예시 및 한국도로교통공단의 통계를[13)] 참고하여 운전상황 결정요인을 다음과 같이 운전자, 자동차, 도로 그리고 날씨를 포함한 환경으로 나누어 살펴보기로 한다.

4가지 운전상황 결정요인 중에서 자동차 운전에 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[12)] 여기서는 운전자를 고려대상에서 제외한다.

Table 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 문제없이 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 세분화 되어 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,

Table 1. Factors of operational situation

Factor	Subfactor	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
Environment	Surface		Dry, Wet(by rain etc), Icy
	Visibility		Dark, Clean, Blurry
	Temperature		Low, Medium, High
	Momentum		Windy, Calm

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

3.2. 위험사건 식별 및 ASIL 결정 단계

Table 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[12] 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 연구에서는 ASIL 평가까지의 단계를 좀 더 구체화하여 다음과 같이 제안한다.

단계 1. 아이템 정의를 기반으로 모든 고장 모드 식별
단계 2. 고장모드로부터 위험원 도출
단계 3. 위험원과 Table 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

4. 심각도와 노출확률 및 제어가능성 등급 결정

4.1. 심각도

주어진 위험사건의 심각도를 결정하기 위해서는 운전자, 차량 주위의 승객과 사람들 또는 차량 주변에 있는 개인에 대해 잠재적인 부상, 즉 위해정도를 평가해야 한다.[12] 여기서 부상이라 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 Table B.1을 참고하여 심각도 등급을 정해줄 수 있다. Fig. 3은 심각도 결정과정을 도시한 것이다.

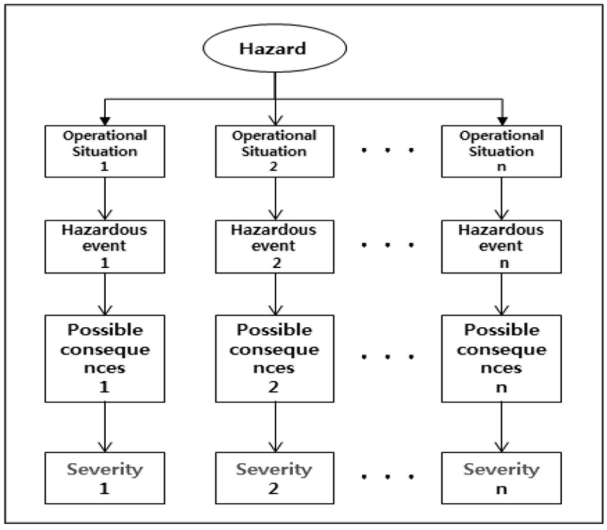

Fig. 3. Determination procedure of severity.

4.2. 노출확률

노출확률을 추정하려면 위험사건의 발생을 야기하는 운전상황 결정요인들의 조합으로 나타나는 시나리오를 평가해야 한다.[12] 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 독립적으로 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

$$\begin{aligned}\Pr(SF1=X4,SF2=Y1) &= \Pr(SF1=X4)\Pr(SF2=Y1)\\ &= (4/15)(1/12)=1/45\end{aligned}$$

이다. 이것은 ISO26262 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

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

이라고 하자. 이 경우 위험사건이 일어날 확률은

$$\begin{aligned}\Pr(SF1=X4,SF2=Y1) &= \Pr(SF2=Y1)\Pr(SF1=X4|SF2=Y2)\\ &= (1/12)(1/50)=1/600\end{aligned}$$

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

4.3. 제어가능성

제어가능성에 대한 확률 추정은 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 운전상황 결정요인과 위험원이 결합된 위험사건을 평가함으로써 가능하며 노출확률과 같은 방식으로 진행한다.

예를 들어 운전상황 결정요인 중 '자동차_운전속도'와 '자동차_외부부착물'을 각각 SF1, SF2라 하자. 어떤 특정 위험사건은 SF1의 경우 '빠름' 인 상태와 SF2의 경우는 '부착물 있음' 상태일 때 발생한다고 하자. 각각의 상태를 X4, Y2라고 하고 제어확률을

$$\Pr(SF1=X4) = 0.99,$$
$$\Pr(SF2=Y2) = 0.95$$

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

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

가 될 것이다. 이것은 ISO26262 파트3에 의해 제어가능성 C2(모든 운전자나 기타 교통 참여자의 90%이상은 일반적으로 위해를 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

$$P(SF1=X4|SF2=Y2) = 0.80$$

라고 하자. 그러면 위험사건 (X4,Y2)이 제어될 확률은

$$P(SF1=X4,SF2=Y2) = P(SF2=Y2)P(SF1=X4|SF2=Y2)$$
$$= (0.95)(0.8) = 0.76$$

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. Fig. 4는 이해를 돕기 위해 운전상황의 두 결정요인이 독립적일 경우와 의존적일 경우를 전술한 예를 토대로 비교 도시한 것이다. 만약 운전상황 결정요인의 각 상태들이 위험사건 발생확률을 증가시키는 방향으로 의존적이라면 그림의 형태 역시 증가하는 방향으로 바뀌게 될 것이다.

5. EPB시스템 적용

지금까지 운전상황 결정요인들을 토대로 운전상황을 정의한 후 위험사건을 도출하고 그 심각도, 노출확률, 제어가능성을 평가하여 ASIL을 결정하는 과정에 대해 논의하였다. 이 장에서는 Fig. 2에서 인용된 EPB 시스템에 3.2절에서 제안한 과정을 적용해보기로 한다. 먼저 1단계로 아이템은 EPB시스템으로 정의하였고 2단계의 가능한 위험원은 모두 도출되었다고 가정하자. 여기서는 설명을 위해 위험원들 중 예시된 '예기치 않은 감속'만을 고려하기로 한다.

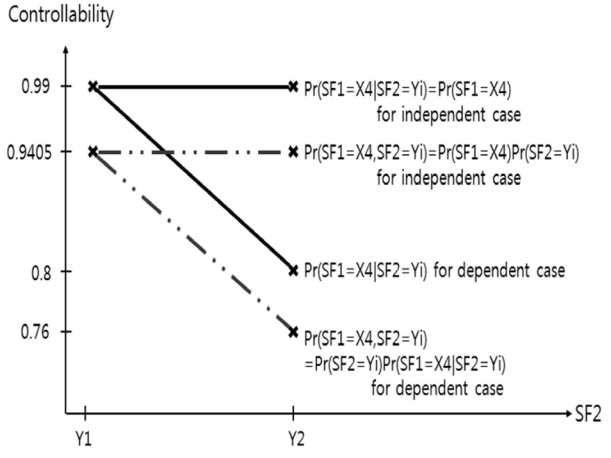

Fig. 4. The controllability for independent vs dependent cases.

단계 3에서는 먼저 주어진 위험원 '예기치 않은 감속'과 결합되었을 때 위해를 일으킬 가능성이 큰 운전상황 결정요소들을 선택하고 이들의 상태와 위험원이 결합될 수 있는 경우들을 Table 2와 같이 나타내었다. 여기서는 운전상황 결정요인으로서 운전속도, 외부부착물, 속력, 방향, 곡률, 경사, 배치, 노면, 시계가 선택되었다. 또한, 선택된 요인별로 위험원과 결합되어 가장 심각한 위험을 초래하게 될 상태를 짙은 배경색으로 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

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

- 위험사건1 : 부착물이 있는 자동차가 매우 빠른 속도로 차선 변경 도중 예기치 않은 감속
- 위험사건2 : 시계가 불량한 경사가 있는 곡선도로에서 예기치 않은 감속
- 위험사건3 : 어두운 결빙 도로에서 예기치 않은 감속

Table 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

Table 3. ASIL Determination of EPB System

Hazard	Subfactor	State	Operational situation	E	Hazardous event	Possible Consequence	S	C	ASIL
Unexpected deceleration	Speed	Very high	Changing lane with an attachment at high speed	E4	Unexpected deceleration in Changing lane with an attachment at high speed	Rear end collision with the following vehicle	S2	C2	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 light 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							

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) = 0.002이 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 3은 비슷한 방법으로 위험사건 2와 3에 대해서도 ASIL을 결정하여 정리한 것이다.

6. 결 론

ISO 26262에서는 ASIL 결정을 위해 관련 운전상황을 식별하여 위험사건을 도출하고 각 사건별 심각도, 노출확률 및 제어가능성을 평가하는 과정이 구체적으로 기술되어 있지 않다. 따라서 표준이 제시한 전체적인 가이드라인과 간단한 예시만으로 실제 현장에서 적용할 경우 어려움이 있는 실정이다.

본 연구에서는 표준의 현장 적용을 돕기 위하여 운전상황의 분석 모형을 제안하였다. 또한 ISO 26262 파트10에서 H&R의 예시로서 제공하고 있는 EPB시스템에 제안된 모형을 적용하는 과정을 보여 줌으로써 이해를 쉽게 하도록 하였다. 제안된 모형은 현장에서 ISO 26262에 따라 제품을 개발하고자 초기에 ASIL을 결정할 때, 보다 체계적이고 쉬운 접근이 가능하도록 해 줄 수 있다.

실제 현장에서 발생하는 운전상황은 가능한 경우가 무수히 많고 복잡하다. 이것을 소수의 의미 있는 범주로 빠짐없이 분류할 수 있도록 기준과 방법을 제시하는 것은 쉬운 작업이 아니다. 본 연구는 그러한 작업에 대한 초기 시도로 볼 수 있으나 인적요인에 의한 영향을 배제함으로 인해 모형의 직접적인 현장 적용에 한계가 있다. 향후 산업현장에 유용하게 적용되기 위해서는 많은 비판적 및 보완적 연구들을 통해 엄밀하게 검토되고 정밀하게 다듬어져야 될 것이다. ISO 26262는 우리나라 경제에 큰 비중을 차지하고 있는 자동차 산업에 직접적으로 연관된 표준인 만큼 앞으로도 관련된 후속연구가 많이 수행되기를 기대한다.

감사의 글: 이 논문은 부경대학교 자율창의학술연구비(2014년)에 의하여 연구되었음

References

1) ISO 26262-1, “Road Vehicles -Functional Safety-Part 1: Vocabulary”, 2011.
2) J. H. Cho, Y. J. Jung, S. H. Jeon, T. M. Han and H. S. Kim, “An Implementation of Automotive Development Methodology Based on ISO 26262”, The Korean Society of Automotive Engineers 2010 Annual Conference and Exhibition, pp. 2052~2059, 2010.

3) M. Ellims and H. E. Monkhouse, “Agonising Over ASILs: Controllability and the In-Wheel Motor”, System Safety, Incorporation the Cyber Security Conference, pp. 1~8, 2012.
4) J. H. Cho, Y. J. Jung, S. H. Jeon, T. M. Han and H. S. Kim, “An Implementation of Automotive Development Methodology Based on ISO 26262”, The Korean Society of Automotive Engineers 2010 Annual Conference and Exhibition, pp. 2052~2059, 2010.
5) D. K. Lee and J. H. Jeon, “Method of Hardware Integration Tests for ASIL Achievement”, The Korean Society of Automotive Engineers 2013 Annual Conference and Exhibition, pp. 2450~2456, 2010.
6) P. H. Jesty, D. D. Ward and R. S. Rivett, “Hazard Analysis for Programmable Automotive Systems”, Technology International Conference on System Safety, pp. 106~111, 2007.
7) R. S. Rivett, “Hazard Identification and Classification: ISO 26262 - The Application of IEC 61505 to the Automotive Sector”, SIL Determination, 2009 5th IET Seminar, pp.1~24, 2009.
8) M. Schlummer, D. Althaus, A. Braasch and A. Meyna, “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, 2010.
9) M. Ellims, H. Monkhouse and A. Lyon, “ISO 26262: Experience Applying Part 3 To An In-Wheel Electric Motor”, IET International Conference on System Safety, pp.1~8, 2011.
10) ISO 26262-10, “Road Vehicles -Functional Safety-Part 10: Guideline on ISO 26262”, 2011.
11) S. H. Yun, Y. J. Kim, Y. J. Choi, J. S. Kim and S. H. Ahn, “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, 2009.
12) ISO 26262-3, “Road Vehicles -Functional Safety-Part 3: Concept Phase”, 2011.
13) Road Traffic Safety Association, “Analysis of Traffic Accident”, No. 2013-0257-114, pp. 43~54, 2013.