PSM 기반의 ISO 26262 기능안전 측정지표 수립

도성룡*, 강현구*
*현대오트론(현대자동차 그룹) 품질팀
e-mail : SungRyong.Do@hyundai-autron.com / imdsr@smu.ac.kr

Establishing of ISO 26262 Functional Safety Measures based on PSM

SungRyong Do*, HyunKoo Kang*
*Quality Engineering Team, Hyundai Autron(Hyundai Motor Group)

요 약

차량 내 전기전자제어시스템의 안전성 확보를 위해 2011 년 ISO 26262 기능안전 표준이 제정되었다. 조직 내에서는 이 표준을 적용하여 프로세스 구축 및 평가체계를 수립하고 있다. 하지만 ISO 26262 분야에서는 측정지표 기반의 정량적 평가체계 수립 연구 및 사례가 부족하다. 본 연구에서는 PSM 기반의 ISO 26262 기능안전 측정지표 수립방안과 컨셉-시스템-소프트웨어 개발 단계에 적용한 사례를 제시한다. 본 연구를 적용하는 조직에서는 기능안전 활동에 대한 객관적인 평가기준 수립 가이드를 제공받을 수 있을 것으로 기대한다.

1. 서론

차량 내 전기전자제어시스템이 급격히 증가하면서 이로 인한 안전 사고가 이슈로 부각되고 있다. 이에 차량의 안전성 확보를 위한 ISO 26262 기능안전 표준이 2011 년 11 월 제정[1]되었고, 현재 완성차 및 부품 제조사들은 이를 적용하고 있다.

ISO 26262 는 차량의 안전성 확보를 위해 컨셉부터 운용/폐기 단계별 수행해야 하는 활동과 적용기법을 명시하고 있다.

일반적으로 프로세스 활동에 대한 평가를 위해 체크리스트 기반의 정성적 방식과 측정지표(Measures) 기반의 정량적 방식을 활용한다. 하지만 ISO 26262 기능안전 분야에서는 측정지표 기반의 정량적 평가에 대한 연구 및 적용사례가 부족한 상황이다.

본 연구에서는 타 분야에서 이미 검증된 PSM(Practical Software and System Measurement)을 기반으로 ISO 26262 기능안전 측정지표 수립방안과 컨셉-시스템-소프트웨어 개발 단계에 적용한 사례를 제시한다.

본 연구를 적용하는 조직에서는 안전관련 활동에 대한 객관적인 평가기준 수립 가이드를 제공받을 수 있다. 또한 조직 내 안전관리자, 안전분석자 등 역할별 담당자에게 적절한 지표를 제공함으로써 의사결정에 도움을 줄 것으로 기대한다.

2. 관련연구

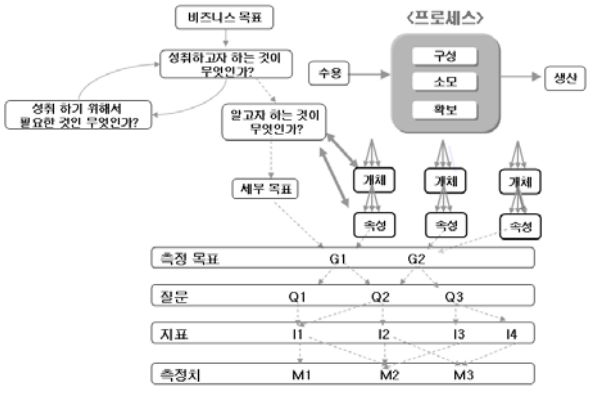
2.1. ISO 26262

ISO 26262 는 3.5t 이하 승용차의 에어백, 엔진, 브레이크 등의 제어시스템에 적용되며, 컨셉, 시스템, 소프트웨어, 하드웨어 개발 단계별 절차 및 설계, 테스팅, 안전분석 등의 기법을 명시하고 있다. 이는 총 10 개 파트, 43 개 요구사항 및 권고사항으로 구성되어 있다. 특히, Part 3 - Part 7 까지의 ISO 26262 개발 생명주기는 (그림 1)과 같이 컨셉 개발, 제품(시스템, 하드웨어, 소프트웨어) 개발 그리고 생산/운용 단계로 구성되어 있다.

(그림 1) ISO 26262 개발 생명주기

2.2. PSM(Practical Software and System Measurement)

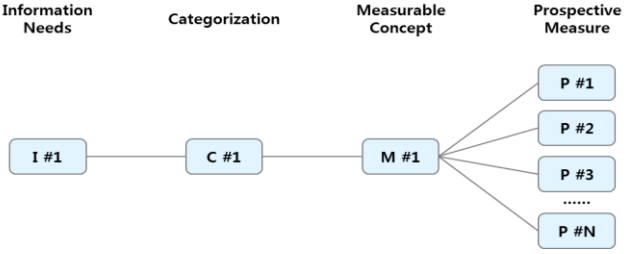
PSM 은 ISO/IEC 15939[2] 측정 프로세스의 표준 방법론으로 GQM(Goal-Question-Metric) 접근법에 기반한다[3].



(그림 2) GQM 접근법

GQM 은 비즈니스 목표를 식별하고, 목표를 정량화한 측정지표 수립 및 데이터 수집을 체계적으로 지원하는 방법이다[3]. GQM 접근법을 도식화하면 (그림 2)와 같다.

PSM 은 (그림 3)과 같이 Top-Down 방식이며, 4 단계로 구성되어 있으며, 최종 결과물은 ICM(Information Category-Measurable Concept-Prospective Measure) 표 형태로 도출된다[4].



(그림 3) PSM 의 측정 체계

[PSM 의 4 단계]
- 1 단계. 측정 요구사항(Information Needs) 식별
- 2 단계. 측정 요구사항 분류(Categorization)
- 3 단계. 측정컨셉(Measurable Concept) 정의
- 4 단계. 측정지표(Prospective Measure) 수립

본 연구에서는 PSM 체계를 ISO 26262 기능안전 측정지표 수립에 적용한다. ISO 26262 기능안전 표준 제정 전후로 안전(Safety) 분야에 PSM 적용 연구가 수행되어 왔다. J. Murdoch, G. Clark, A. Powell, and P. Caseley 은 2003 년 미 국방성(Department of Defense)의 안전관련 도메인에 PSM 적용 방안에 대한 연구를 진행하였다[5]. S. Drabble 은 2009 년 연구에서 안전 시스템 개발에 투입되는 공수 예측 및 투입 공수에 대한 ROI(Return On Investment) 회수 방안을 제안하였다[6]. Y. Luo, J. Stelma, and M. van den Brand 은 2015 년 연구에서 ISO 26262 기능안전 부문에 PSM 적용 연구를 처음으로 수행하였다[7].

ISO 26262 기능안전 개발 프로세스에 PSM 을 적용 연구는 시작 단계이다. 특히, 기존 연구[7]도 컨셉 개발 단계에만 적용하였다. 또한 측정 지표들 간의 연계성(Relation)을 파악하지 못한 한계가 있다.

이에 본 연구에서는 J. Murdoch 의 연구[5]를 기반으로 기존 연구들의 한계점을 보완하여, ISO 26262 기능안전 개발 프로세스의 PSM 적용 방안을 제시한다. 또한 적용 방안의 검증을 위해 컨셉-시스템-소프트웨어 개발 프로세스에 적용한 사례를 소개하고, 개발 단계 별 지표 연계모델을 제시한다.

3. 연구제안 및 사례

본 연구에서 제안하는 PSM 기반의 ISO 26262 기능안전 측정지표 수립단계 및 적용사례는 다음과 같다.

3.1. 측정 요구사항(Information Needs) 식별

ISO 26262 개발 프로세스에 포함되는 역할별 측정 요구사항을 식별한다. 일반적으로 ISO 26262 개발을 위해서는 안전관리자, 안전분석자, 안전 시스템/하드웨어/소프트웨어 개발자 역할이 필요하다. 본 연구에서는 "안전분석자" 측면에서 측정 요구사항을 식별한다. 안전분석자의 개발 단계 별 주요 측정 요구사항은 (그림 4)의 3-1 과 같다.

- 컨셉 개발(Concept Development)
  - Hazard 가 모두 식별되었는가?
  - Safety Goal 은 모든 Hazard 를 포함하는가?
  - 모든 기능안전 요구사항이 Safety Goal 로부터 도출되었는가?

- 시스템 개발(System Development)
  - 모든 시스템 안전요구사항이 컨셉 단계의 기능안전 요구사항으로부터 도출되었는가?

- 소프트웨어 개발(Software Development)
  - 모든 소프트웨어 안전요구사항이 시스템 단계의 시스템 안전요구사항으로부터 도출되었는가?

3.2. 측정 요구사항 분류(Categorization)

역할 별 도출한 측정 요구사항을 기존의 ICM 표[4]에 매핑하거나 매핑이 안 되는 경우는 새로운 카테고리를 도출한다. 기존 측정 요구사항은 일정(Schedule), 규모(Size), 자원(Resource), 제품 품질(Product Quality), 프로세스 성과(Process Performance), 기술 효율성(Technology Effectiveness), 고객 만족도(Customer Satisfaction)로 분류된다.

본 연구에서 안전분석자의 측정 요구사항은 요구사항 개발 프로세스 이행을 통해 모든 요구사항이 식별되었는지에 대한 사항이므로 프로세스 성과로 분류하였으며, 결과는 (그림 4)의 3-2 와 같다.

3.3. 측정컨셉(Measurable Concept) 정의

측정 요구사항을 만족하는 구현 컨셉이며, 측정 요구사항 분류의 세부 항목이기도 한다. 정의한 측정컨셉을 ICM 표[4]에 매핑하거나 매핑이 안 되는 경우는 새로운 측정컨셉을 도출한다.

본 연구에서 안전분석자의 측정 요구사항은 이전 단계의 출력물이 다음 단계로 입력되어 충분히 반영되었는지를 확인하는 것이므로, 프로세스 완전성(Process Completeness)으로 정의하였다. 예를 들어, 시스템 개발 단계의 안전요구사항이 소프트웨어 개발 단계의 안전요구사항으로 완전히 반영되었는지를 확인하는 컨셉의 측정이다. 프로세스 완전성은 기존 ICM 표[4]에 정의된 사항이 아니므로, 신규로 정의하였다. 결과는 (그림 4)의 3-3 과 같다.

3.4. 측정지표(Prospective Measure) 수립

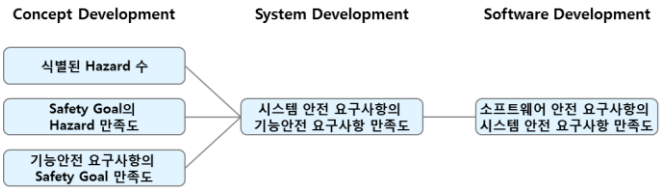
측정컨셉에 따라 측정 요구사항을 만족하는 실제 지표를 수립한다. 이는 데이터를 수집하는 최소 단위이거나 최소 단위의 계산식 결과일 수도 있다.

본 연구의 컨셉 개발 단계에서는 식별된 Hazard 수, Safety Goal 의 Hazard 만족도, 기능안전 요구사항의

No.	Phase (3-1)	Information Needs (3-2)	Information Category (3-3)	Measurable Concept (3-4)	Prospective Measure
1	Concept	Hazard가 모두 식별되었는가?	Process Performance	Process Completeness	식별된 Hazard 수
2	Concept	Safety Goal은 모든 Hazard를 포함하는가?	Process Performance	Process Completeness	Safety Goal의 Hazard 만족도
3	Concept	모든 기능안전 요구사항이 Safety Goal로부터 도출되었는가?	Process Performance	Process Completeness	기능안전 요구사항의 Safety Goal 만족도
4	System	모든 시스템 안전요구사항이 컨셉 단계의 기능안전 요구사항으로부터 도출되었는가?	Process Performance	Process Completeness	시스템 안전요구사항의 기능안전 요구사항 만족도
5	Software	모든 소프트웨어 안전요구사항이 시스템 단계의 시스템 안전 요구사항으로부터 도출되었는가?	Process Performance	Process Completeness	소프트웨어 안전요구사항의 시스템 안전요구사항 만족도

(그림4) PSM 기반의 ISO 26262 기능안전 측정지표 적용사례

Safety Goal 만족도 지표를 수립하였다. 시스템 개발 단계에서는 시스템 안전요구사항의 기능안전 요구사항 만족도, 소프트웨어 개발 단계에서는 소프트웨어 안전요구사항의 시스템 안전요구사항 만족도 지표를 수립하였다. 결과는 (그림 4)의 3-4 와 같다. 수립한 측정지표를 토대로 개발 단계 별 지표 간 연계모델을 정의한 예시는 (그림 5)와 같다.



(그림 5) 개발 단계 별 지표 간 연계모델

4. 결론 및 향후 계획

최근 차량의 안전과 관련된 ISO 26262 기능안전 표준이 제정되면서, 이 표준을 조직 내부 프로세스에 적용하고 있다. 이렇게 적용된 프로세스는 측정지표를 기반으로 객관적이며 정량적인 평가가 수행되어야 한다.

본 연구에서는 PSM 기반의 ISO 26262 기능안전 측정지표 수립방안과 컨셉-시스템-소프트웨어 개발에 적용한 사례를 제시하였다.

본 연구를 적용하는 조직에서는 ISO 26262 기능안전 개발 프로세스에 대한 객관적인 평가를 위한 가이드를 제공받을 수 있다. 또한 조직 내 프로세스의 역할별 담당자에게 적절한 지표와 분석 결과를 제공함으로써 의사결정에 도움을 줄 것으로 기대한다.

추가적으로 다음의 연구를 진행할 예정이다. 첫째, 측정지표 간 연계 모델을 구체화하고, 상관성을 파악한다. 둘째, 에어백, 엔진, 변속기 등 특정 시스템에 본 연구의 제안 방안을 적용하여, 실질적인 검증을 수행할 계획이다. 끝으로, ISO/IEC 25010 품질특성과 본 연구를 통해 도출한 지표의 비교 매핑을 통한 검증을 수행할 예정이다.

참고문헌

[1] “ISO 26262 : Road Vehicles – Functional Safety,” 2011.
[2] ISO/IEC, “Systems and Software Engineering -Measurement Process. ISO/IEC 15939,” 2007.
[3] V. Basili, J. Heidrich, M. Lindvall, J. Munch, M. Regardie, D. Rombach, C. Seaman, and A. Trendowicz, “GQM + Strategies: A Comprehensive Methodology for Aligning Business Strategies with Software Measurement,” arXiv Preprint arXiv:1402.0292, 2014.
[4] “Information Category-Measurable Concept-Prospective Measures (ICM) Table v7.0a final,” 2012.
[5] J. Murdoch, G. Clark, A. Powell, and P. Caseley, “Measuring Safety: Applying PSM to the System Safety Domain,” In Proceedings of the 8th Australian Workshop on Safety Critical Systems and Software - Volume 33, SCS '03, pages 47-55, 2003.
[6] S. Drabble, “Safety Process Measurement - Are We There Yet?,” In Chris Dale and Tom Anderson, editors, Safety-Critical Systems: Problems, Process and Practice, pages 195-207, Springer London, 2009.
[7] Y. Luo, J. Stelma, and M. van den Brand, "Functional Safety Measurement in the Automotive Domain: Adaptation of PSM," Proceedings of the 1st International Workshop on Automotive Software Architecture. ACM, 2015.