Automotive SPICE 기반의 기능안전성 통합 프로세스 구축

황선명, 정지훈
대전대학교
sunhwang@dju.kr

Automotive Fuctional Safety Integrated Process

Sun Myung Hwang, Ji Hoon Jeong
Daejeon University

요 약

본 논문은 자동차 분야의 품질 프로세스 모델인 Automotive SPICE와 기능안전성을 강조한 자동차 분야 ISO 26262 표준을 가지고 통합 프로세스심사 프레임워크를 구성하였다. 두 표준의 프로세스의 맵핑을 통해 심사에 활용할 수 있도록 구성해봄으로써 실제 심사 시 프로세스 능력 수준의 평가와 함께 소프트웨어의 기능안전성에 대한 수준도 판단해 볼 수 있도록 하였다.

1. 서론

CMMI(Capability Mutuality Model Integration)과 ISO/IEC 15504: Software Process Improvement and Capability dEtermination (SPICE)같은 프로세스 심사모델의 표준이 등장한 이후, 이들 표바탕으로 임베디드, 자동차, 항공 등 다양한 분야에 프로세스 심사모델을 접목시켜 사용하려는 시도가 이어져 왔다.

자동차 경우 세계적으로 가장 많이 사용되는 운송 수단 중에 하나로서 자동차에 대한 문제는 곧 생명과 직결될 수 있기에 안전에 대한 고려는 필수적이다. 자동차에 내장되는 소프트웨어는 점차 증가되고 있고 자동차의 개발 비용에서 차지하는 비율도 커지고 있다.

차량에 탑재될 소프트웨어의 품질을 높이기 위해서는 잘 갖추어진 프로세스뿐만 아니라 소프트웨어가 안전성도 갖추어야 한다. 두 가지 요소 모두 소프트웨어 품질에 관련된 것이므로 공통된 항목들을 갖추고 있을 것으로 가정하고 본 논문에서는 자동차 내장 소프트웨어의 프로세스 심사 프레임워크 표준인 Automotive SPICE와 자동차의 안전 관련 표준인 ISO 26262외의 비교 및 분석을 통해 통합된 심사 프레임워크 방안을 모색해 보고자 한다

2. Automotive SPICE

Automotive SPICE 는 ISO/IEC 15504 에 기반을 두어 만들어진 자동차용 소프트웨어의 프로세스 심사 모델이다. 유럽의 여러 자동차 회사가 주축이 된 Automotive Special Interest Group(AutoSIG)에서 2005년도에 Automotive SPICE를 발표했다. 현재 Automotive SPICE PRM 4.5, PAM은 2.5까지 발간되었다. Automotive SPICE의 프로세스는 <그림1>와 같이 3개의 생명주기, 7개의 그룹으로 구성되어 있다.

Automotive SPICE의 능력수준은 Incomplete 부터 Optimizing까지 6단계로 ISO/IEC 15504와 동일하게 구성되어 있으며, Process Attribute도 동일하게 구성되어 있다.

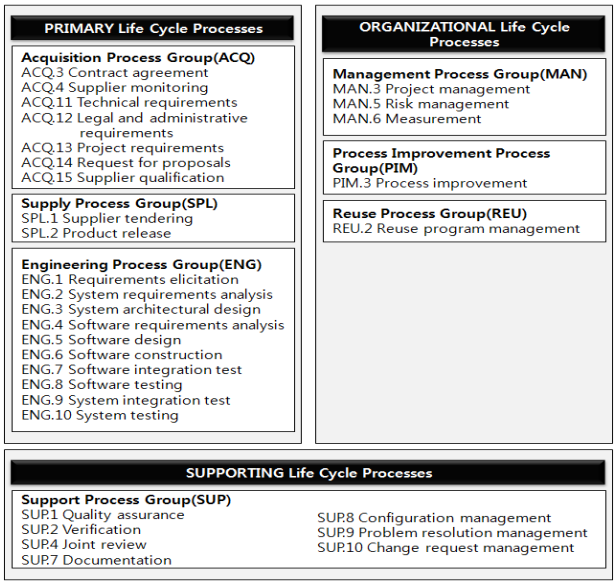

그림 1. Automotive SPICE 생명주기

3. ISO 26262

ISO 26262:Road vehicle - Functional safety는 IEC 61508을 지상 차량 내 전기/전자 시스템 응용 분야의 특정한 니즈에 적합하도록 변형시킨 표준이다. 이 표준은 제품 개발의 다양한 단계를 위해 프로세스 참조 모델로 V모델에 기반하고 있다.

ISO 26262는 총 9부로 구성되어 있으며 전체 구조는 <그림 2> 와 같다.

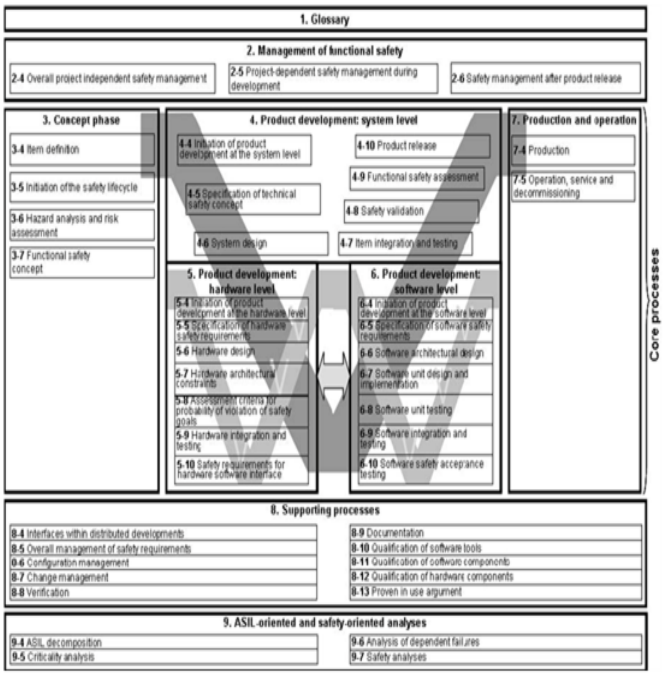

그림 2. ISO 26262 전체 생명주기

4. Automotive SPICE와 ISO 26262의 통합

4.1 통합 프로세스 구축 전략

통합 프로세스 구축 전략의 수립은 다음과 같이 계획하였다. 먼저, Automotive SPICE의 능력 수준과 ISO 26262의 ASIL수준이 함께 심사될 수 있도록 하기 위하여 다음과 같은 전략을 수립한다.

● Automotive SPICE의 Base Practice를 확장한다.
● 안전에 대한 Base Practice를 추가한다.
● 각 프로세스에 작업산출물을 추가한다.
● Automotive SPICE의 능력수준 2단계에 해당하는 General Practice를 확장한다.
● Automotive SPICE의 능력수준 3단계에 해당하는 General Practice를 확장한다.
● ASIL을 반영하기 위해 ISO 26262의 각 프로세스에 있는 방법 및 수단 표를 사용한다

심사의 결과는 Automotive SPICE와 ISO26262 각각을 다음과 같이 분리 또는 합쳐서 보여줄 수 있도록 구성한다.

● Automotive SPICE 만의 심사 결과
● 기능안전성과 관련된 practice와 방법에 대한 심사결과
● 두 가지가 통합된 심사 결과
● 통합된 심사의 rating이 Automotive SPICE와 ISO 26262에 대한 각각의 심사 결과로 분리 가능하도록 한다.
● Automotive SPICE 심사의 문서 finding과 이에 대한 rating과 근거 데이터가 분리되어 기록될 수 있도록 한다.
● ISO 26262 심사의 문서 finding과 이에 대한 rating과 근거 데이터가 분리되어 기록될 수 있도록 한다.
● 두 가지의 데이터를 팀에 제시하고, 프로필을 비교해서 제시한다.

통합된 심사를 통해 Automotive SPICE의 능력 수준에 따라 안전 관련 practice와 방법이 대략적으로 적용되었는지 파악할 수 있도록 구성한다. 통합된 심사는 ISO/IEC 16504의 심사와 마찬가지로 제품의 품질이 아닌 프로세스와 방법의 사용에 대해 초점을 둔다.

4.2 비즈니스 프로세스 모델표기법(BPMN)을 이용한 통합 심사 프로세스

비즈니스 프로세스 모델링 표기법(Business Process Modeling and Notation, BPMN)은 사업 프로세스를 플로우 차트 형식으로 정의하는 표준화된 방법이다. 2004년도에 BPMI Notation Working Group에 의해 최초로 발표되었고 OMG 표준으로 제정되어 있다. BPMN의 목적은 프로세스의 초안을 만드는 비즈니스 분석자, 프로세스에 따라 기술을 구현할 책임이 있는 개발자, 프로세스를 관리 감독하는 사업 책임자 모두에게 쉽게 이해할 수 있는 표기법을 제공하는 것이다. 또한, 비즈니스 프로세스의 구현을 설계한 XML언어를 비즈니스 중심의 표기법으로 가시화 시키는 것이다.

통합된 심사 프로세스를 시각적으로 표현하기 위해 OMG 표준인 BPMN 1.2를 사용하여 도식화 하였다. 도식화한 ENG.4 소프트웨어 요구사항 명세 프로세스는 <그림3>와 같이 나타내었다.

프로세스의 시작과 끝을 Start Event와 End event를 사용하여 나타내었고, 각 IBP를 Activity를 사용하여 나타내었다. 그리고 이들간의 관계를 Sequence Flow로 연결하여 절차를 나타내었다. 각 BP마다 나오는 산출물들은 Data Object와 Associate Flow 를 이용해 나타내었고 추적성의 연결은 Message Flow를 활용하여 기술하였다.

최종적으로 ENG.4 프로세스 전체를 Lane 으로 묶어 각 Activity가 ENG.4 에 해당한다는것을나타내었다.

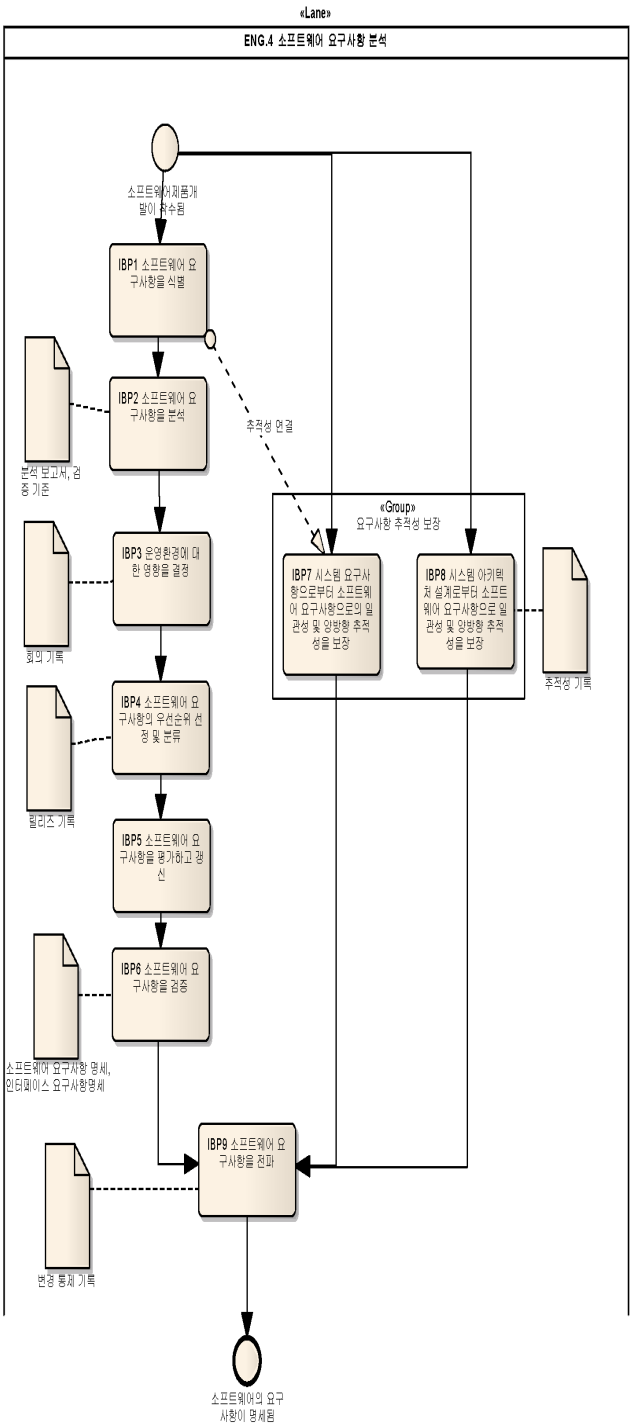

그림 3. 통합된 프로세스의 Diagram(ENG.4, BPMN)

5. 결론

ISO/IEC 15504 표준을 자동차 분야에 맞게 변형한 Automotive SPICE와 기능안전성에대한 기본 표준인 IEC 61508을 자동차 분야에 맞게 변형한 ISO 26262 표준을 가지고 통합 심사 프레임워크를 구성하였다. 두 표준의 프로세스의 맵핑을 통해 심사에 활용할 수 있도록 구성해봄으로써 실제 심사 시 프로세스 능력 수준의 평가와 함께 소프트웨어의 기능안전성에 대한 수준도 판단해 볼 수 있도록 하였다.

참고문헌

[1] J.Pernstal (2010), An Industrial Case Study investigating the Integration of Product Development and Manufacturing in Development of Automotive Software Intensive Systems, Software Quality Journal,

[2] Richard Messnarz (2009), "Integrated Automotive SPICE and Safety Assessments", pp. 279~288

[3] Paolo Panaroni (2008), "Safety in Automotive Software: an Overview of Current Practices"

[4] ISO/IEC 15504:2004, "Information technology – Process assessment

[5] ISO/IEC WD 15004:2010, "Information technology – Process assessment "

[6] www.automotivespice.com, "Automotive SPICE"

[7] Klaus Hoermann (2008), "Automotive SPICE in Practice", pp. 1~10