

철도분야 소프트웨어로의 SPICE 적용 연구

정의진\* 신경호  
한국철도기술연구원

A Study on the Adoption of SPICE in the Railway Software

Joung, Eui-jin\* Shin, Kyung-ho  
KRII (Korea Railroad Research Institute)

**Abstract** - It can be considered that the safety of software is combined with that of hardware, and also directly connected to system safety. Because the software in the railway system takes the form of Embedded that let it behave at the system level, instead of independent operation, the safety of the railway S/W is also important. The approach, for ensuring the quality and safety of those software, can be considered with two points of view. Those are views seeing from products, and from processes. The two points of approach are all necessary in the railway system. For the first of all, the process approach is to validate maturity of the organizations in accordance to the judging processes of organizations, which are specified by CMMI(Capability Maturity Model Integration) or SPICE(Software Process Improvement and Capability dTermination : ISO/IEC15504). In this paper, as the first step of them, we are trying to find approaches to estimate the maturity of manufacturer and assessment organization in the railway system.

세스가 해당 목표를 달성하고 있는지 평가하는 것을 말한다. 프로세스 심사를 통하여 얻을 수 있는 것은 해당 조직의 개발 능력(Capability) 결정뿐만 아니라 자체 프로세스 개선(Improvement)에도 중요한 지표를 제공받을 수 있다. 이와 같은 프로세스 심사 방법으로 가장 대표적인 것으로 SEI의 CMMI(Capability Maturity Model Integration)와 ISO/IEC 15504 (SPICE : Software Process Improvement and Capability dTermination)를 들 수 있다.

다음의 2장에서는 철도안전법과 안전기준, 표준과의 관계를 제시하였으며, 3장에서는 프로세스 성숙도 심사 모델인 CMMI와 SPICE에 대하여 분석하였으며, 4장에서는 SPICE를 기준으로 프로세스 성숙도 모델에 대하여 세부 사항을 기술하였다. 5장에서는 결론으로 향후 과제 진행 방향에 대하여 언급하였다.

1. 서 론

컴퓨터 기술의 향상으로 인해서 기존의 기계적으로 제어되던 아날로그 시스템들이 컴퓨터를 기반으로 하는 디지털 시스템으로 대체됨에 따라 이들 시스템의 안전성이 더욱 중요시되고 있다. 디지털 제어시스템은 기존의 아날로그 시스템에 비해 훨씬 복잡한 제어 기능을 효과적으로 수행할 수 있고, 소프트웨어 프로그래밍이 기존의 RLL(Relay Ladder Logic)과 같은 하드웨어 프로그램 작업에 비해 효율적이라는 장점을 지닌다. 하지만, 이러한 소프트웨어는 그 복잡성으로 인해서 점점 그 정확성을 확보하기가 어려워지고 있으며, 1990년대 이후부터는 소프트웨어 오류로 인해서 발생한 사고들이 다수 보고되고 있다. 따라서, 이들 시스템들의 소프트웨어 안전성을 확보하기 위해서, 다수의 국가와 기관들에서 소프트웨어의 안전성 및 신뢰성을 보장할 수 있는 방안들을 제안하고 있다.

2. 철도안전 법체계 및 표준과의 관계

철도분야의 안전을 확보하기 위한 법체계로는 아래 그림에서와 같이 철도안전법, 철도안전법시행령, 철도안전법시행규칙 및 하위 고시로 건설교통부 고시가 있다. 건설교통부 고시로는 현재 철도차량, 철도시설분야의 안전기준이 고시되어 있으며, 이에 대한 해석을 뒷받침할 수 있는 지침이 개발 중에 있다. 철도 소프트웨어 분야에서도 마찬가지로 안전기준 마련을 위한 연구가 진행 중에 있으며, 건설교통부 고시로 제정될 안전기준은 기존의 국제규격(IEC, ISO 등), 국내규격(KS 등), 산업체 표준(IEEE 표준 등)과 동떨어져 제시되어서는 않되며, 이를 아우르면서 제시되어야 한다.

소프트웨어 개발과 관련된 일정 지연, 비용 초과, 고객의 불만족 등을 해소하기 위한 방안으로 제품자체의 품질을 향상시키는 방법과 제품을 개발하는 프로세스 관리를 통한 문제해결 방안을 생각할 수 있다. 최근에 시도되고 있는 여러 가지 방법 가운데, 본 논문에서는 프로세스 관리를 통한 문제 해결 방안에 대하여 고려하여 보았다.

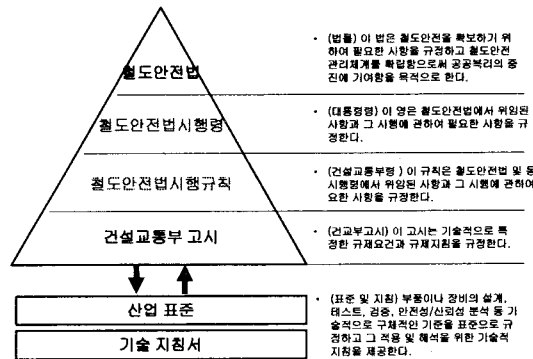


그림 1. 철도안전법과 표준과의 관계

소프트웨어 개발에 있어서 프로세스란, 소프트웨어개발 조직의 목표달성을 위해 조직 내에서 사용하는 자원(사람, 장비, 기술, 방법론)과 활동, 방법, 실무지침을 말하며, 프로세스 심사란, 개발 조직이 사용하고 있는 프로

그림 2는 철도소프트웨어 안전기준을 작성하는데 있어서 생명주기 공경, 계획, 요구명세, 설계, 시험, 설치 등으로 구분하여 참조하여야 하는 규격 및 표준과의 관계

를 도식화하여 나타낸 것이다.

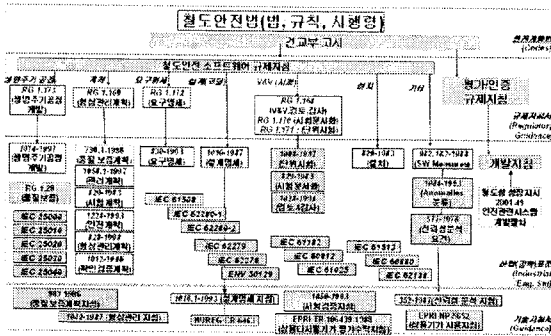


그림 2. 철도S/W안전기준과 표준과의 관계

철도S/W의 신뢰성 및 안전성을 향상시키기 위해서는 제품관점에서 좋은 제품을 만들고, 정확한 시험으로 개발된 제품의 품질이 원하는 수준에 도달했는지를 판단하는 경우가 있으며, 이와는 다른 관점에서 좋은 제품은 좋은 조직 체계에서 만들어진다. 프로세스적인 관점이 있다. 원자력분야와 같이 안전성이 중요한 철도시스템에서 소프트웨어의 안전성을 확보하기 위해서는 Product 관점 및 Process 관점 모두 검토할 필요가 있다고 사료된다. (1)~(2)

### 3. 프로세스 성숙도 모델

#### 3.1 CMMI

CMMI(Capability Maturity Model Integration) 프로젝트는 미국 국방성(Department of Defense)의 지원 하에 NDIA(National Defense Industrial Association)의 시스템공학위원회에서 산학협력 프로젝트로 시작되었다. 본 프로젝트는 조직의 사업 전반에 걸쳐서 개발 프로세스를 개선하고자 하는 조직에 초점을 맞추어, 소프트웨어공학과 시스템공학으로 양분된 프로세스 모델을 하나로 통합하여 개발하고자 하는 것이었다. 여러 CMM 모델을 통합하여 CMMI 모델을 사용함으로써 상황에 맞추어 여러 모델을 사용하여야 했던 조직의 비용 중복을 막고, 사업 전반에 걸친 프로세스 개선 및 평가에 효과를 얻고자 하는 것이었다. 그동안 여러 분야에 독자적인 CMM이 존재하였으며, 그 영역은 다음과 같다.

- SW-CMM (Capability Maturity Model for Software Engineering) : SEI에서 개발된 S/W 공학 분야의 CMM
  - SE-CMM (Capability Maturity Model for Systems Engineering) : EIA/IS 731 (Electronic Industries Alliance Systems Engineering Capability Model, Interim Standard) 표준과 EPIC(Enterprise Process Improvement Collaboration)에 의해 만들어진 Systems Engineering 분야 CMM과 INCOSE에 의해 만들어진 SECAM(Systems Engineering Capability Assessment Model)을 통합한 모델
  - IPPD-CMM (Capability Maturity Model for IPPD) : 미국 국방성(DoD)과 산업계에 의해 IPPD (Integrated Product and Process Development) 환경에 초점이 맞추어진 프로세스 성숙도 모델 (EPIC에 의해 draft 형태로 공표됨.)
  - SS-CMMI : 공급업체 소싱 분야의 CMM
- 위 4가지 CMM분야를 통합하여 정리한 것이 다음의 CMMI이다.

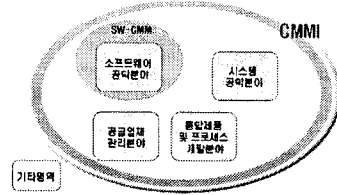


그림 3. CMMI로의 통합

### 3.2 ISO/IEC1504 (3)

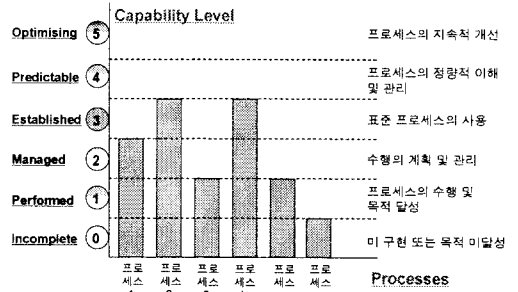


그림 4. SPICE의 Dimension

ISO/IEC15504(SPICE: Software Process Improvement Capability determination)는 CMMI와 마찬가지로 조직의 프로세스를 개선하고 평가하기 위한 활동을 지원하기 위하여 현재의 프로세스 상태를 파악하여 그 성숙도를 측정한다. SPICE는 크게 두 영역으로 나누어진다. 심사 대상 프로세스에 대하여 다른 Reference model 영역과 Reference model의 심사를 통해 Process의 Capability Level을 정하는 Assessment model 영역이 있다. 그림에서 가로축이 Reference model 영역에 해당하고, 세로축이 Assessment model 영역에 해당한다. 심사대상 프로세스를 정한 Reference model은 S/W 뿐만 아니라 System 분야 등 모든 분야에 대하여 다를 수 있는데 이는 SPICE가 S/W 영역을 넘어서 모든 Process에 대한 심사가 가능하도록 구성 되었다는 것을 의미한다.

### 4. 프로세스 성숙도 모델의 영역

CMMI와 SPICE의 프로세스 성숙도 모델은 주관기관 다를 뿐, 다루는 영역이나 심사 프로세스가 동일하다고 볼 수 있다. 여기에서는 SPICE의 두개의 영역을 중점을 두어 다루었다.

#### 4.1 Reference model 영역

SPICE에서 Reference model이란 심사 대상 프로세스로 ISO/IEC15504에서 제시하는 Reference model의 조건을 만족하면 심사대상 프로세스가 될 수 있다. 조건은 다음과 같다.

- Model의 목적 : 프로세스 능력의 심사 목적에 적합하여야 한다.
- Model의 범위 : 프로세스 및 능력차원에 대하여 범위를 언급하여야 한다.
- Model의 구성요소 및 지표 : 프로세스 수행지표 및 능력지표를 제시하여야 한다.
- 대응 (Mapping) : 프로세스 수행지표, 프로세스 능력지표를 Reference 모델과 대응하여야 한다.
- 해석 : 검증 가능한 공식적 매커니즘에 대한 설명이 있어야 한다.

현재 SPICE에서는 S/W 영역과 SE영역에 대하여 다른 국제 기준과 연계하고 있다. S/W 영역에서 쓰이는 프로세스는 ISO/IEC 12207(Software Life Cycle Processes)과 연동되도록 하고 있으며, 시스템 엔지니어링과 관련된 프로세스는 ISO/IEC 15288 (Systems Engineering System Life Cycle Processes)을 따르도록 하고 있다. ISO/IEC 12207의 프로세스는 다음 표와 같이 3개의 프로세스는 Primary, Organization, Support의 3개 Life Cycle영역으로 구분하고 있으며, Primary에 조달, 공급, 공학, 운영의 4개 그룹, Organization에 관리, 프로세스 개선, 자원 및 인프라, 재사용의 4개 그룹, Support에 구성관리, 품질보증의 2개 그룹으로 세분하여 나누고 있으며, 총 48개의 프로세스가 정의되어 있다.

표 1. ISO/IEC 15504의 프로세스

PRIMARY Life Cycle Processes
<b>1. Acquisition Process Group (ACQ)</b> ACQ.1 Acquisition preparation ACQ.2 Supplier selection ACQ.3 Contract agreement ACQ.4 Supplier monitoring ACQ.5 Customer acceptance
<b>2. Supply Process Group (SPL)</b> SPL.1 Supplier tendering SPL.2 Software release SPL.3 Software acceptance support
<b>3. Engineering Process Group (ENG)</b> ENG.1 Requirement elicitation ENG.2 System requirement analysis ENG.3 System architectural design ENG.4 Software requirement analysis ENG.5 Software design ENG.6 Software construction ENG.7 Software integration ENG.8 Software testing ENG.9 System integration ENG.10 System testing ENG.11 Software installation ENG.12 Software & system maintenance
<b>4. Operation Process Group (OPE)</b> OPE.1 Operational use OPE.2 Customer support
ORGANIZATIONAL Life Cycle Processes
<b>1. Management Process Group (MAN)</b> MAN.1 Organizational alignment MAN.2 Organization management MAN.3 Project management MAN.4 Quality Management MAN.5 Risk Management MAN.6 Measurement
<b>2. Process Improvement Process Group (PIM)</b> PIM.1 Process establishment PIM.2 Process assessment PIM.3 Process improvement
<b>3. Resource &amp; Infrastructure Process Group (RIN)</b> RIN.1 Human resource management RIN.2 Training RIN.3 Knowledge management RIN.4 Infrastructure
<b>4. Reuse Process Group (REU)</b> REU.1 Asset management REU.2 Reuse program management REU.3 Domain engineering
SUPPORTING Life Cycle Processes
<b>Support Process Group (SUP)</b> SUP.1 Quality assurance SUP.2 Verification SUP.3 Validation SUP.4 Joint review SUP.5 Audit SUP.6 Product evaluation SUP.7 Documentation SUP.8 Configuration management SUP.9 Problem resolution management SUP.10 Change request management

## 4.2 Assessment model 영역

프로세스, 즉 Reference 모델을 평가하기 위한 Assessment model 영역에서는 Process Attribute(PA)를 기반으로 프로세스의 평가를 수행한다. PA는 주어진 능력에 도달했는지 여부를 결정하는 데 사용되며, 프로세스 능력의 특정 측면을 측정한다. Level 1 PA의 평가지표는 각각의 프로세스에 대한 Base Practice(BP)와 Work Product(WP)의 여부로 판단하며, Level 2-5의 PA는 각각 PA에 대한 Generic Practice(GP)와 Generic Resource(GR), Generic Work Product(GWP)로 판단한다. 각각의 PA는 Percentage scale로 rating하여 N(Not achieved), P(Partially achieved), L(Largely achieved), F(Fully achieved)로 계산된다. 또한 프로세스 능력은 6단계(0-5단계) level로 되어 있다. 표2와 3은 각각의 PA에 대한 설명 및 Assessment model의 rating을 나타낸 것이다. 각각의 PA에 대하여 rating 함으로써 각 PA에 대한 N, P, L, F를 도출할 수 있으며, Level은 이전단계의 PA rating이 모두 F이고, 최종단계 Level의 PA가 L이거나 F이면 해당 Level을 달성하였다고 본다.

표 2. Process Attribute (PA)

Level 0 : Incomplete process
Level 1 : Performed process
PA 1.1 Process performance attribute
Level 2 : Managed process
PA 2.1 Performance management attribute
PA 2.2 Work product management attribute
Level 3 : Established process
PA 3.1 Process definition attribute
PA 3.2 Process resource attribute
Level 4 : Predictable process
PA 4.1 Process measurement attribute
PA 4.2 Process control attribute
Level 5 : Optimizing process
PA 5.1 Process change attribute
PA 5.2 Continuous improvement attribute

표 3. Process Attribute Rating

Rating	달성도
N(Not achieved)	0% ~ 15%
P(Partially achieved)	16% ~ 50%
L(Largely achieved)	51% ~ 85%
F(Fully achieved)	86% ~ 100%

## 5. 향후 진행 방향

철도 S/W의 품질 및 안전성을 향상시키기 위해서는 Product 관점에서 또한 Process 관점에서 접근하여야 한다. Product 관점은 제품자체에 대한 것이고, Process 관점은 제품을 만드는 조직의 성숙도에 대한 것이다. 본 논문에서는 S/W Process 관점에서 프로세스의 성숙도를 평가하기 위한 모델로 CMMI와 SPICE에 대하여 알아보았으며, 특히 SPICE 관점에서의 심사 대상 프로세스, 즉 Reference model과 심사 모델인 Assessment model에 대하여 살펴보았다. 향후 철도분야에 적합한 개발 및 검증 프로세스를 구축하기 위해서 여러 심사 모형의 적용에 대한 연구를 진행할 필요가 있을 것으로 사료된다.

### [참고 문헌]

- [1] ISO/IEC 9126 "Information Technology-Software Quality Characteristics and Metrics-Part 1,2,3"
- [2] ISO/IEC 14598 "Information Technology-Software Product Evaluation-Part 1-6"
- [3] ISO/IEC 15504 "Information Technology-Process Assessment-Part 1-5"