철도소프트웨어에 대한 프로세스 성숙도 적용 연구
A Study on Process Maturity Approach for Railway Software

정의진* 신경호** 이강미*** 조현정***
Eui-jin Joung Kyung-ho Shin Kang-mi Lee Hyun-jeong Cho

ABSTRACT

The softwares in a railway system are being used in the area of railway control system, directly associated to safety, as well as in the field of data collection or database, which is not related to safety. Also the software takes the form of □□Embedded□□ that let it behave at the level of system, instead of independent operation. Consequently, it can be considered that the safety of software is combined with that of hardware, and also directly connected to system safety. 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 former one is to check the states of the finally launched products, rather than to examine the manufacturing processes and work forces, the latter approach assumes that the process maturity should be based to make good quality and sound software. The product approach is to check the safety of products by performing proper tests (White Box or Black Box test) to developed products depending on each Lifecycle, and 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 dEtermination : ISO/IEC15504). The two points of approach are all necessary in the railway system. 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.

---

1. 서론

철도제어시스템, 인공위성제어시스템, 원자력발전소제어시스템 등은 고장이 발생할 경우 사회·경제적인 큰 문제를 야기할 수 있는 안전성이 매우 중요한 시스템(Safety-Critical System)이다. 이러한 시스템들의 사소한 고장은 수천억 원의 경제적 손실을 야기할 수 있으며, 뿐만 아니라 인명 피해와도 직접적인 연관을 지닌다. 따라서 대부분의 선진국에서는 이러한 시스템의 안전성을 확보하기 위해서 개발 기법, 기준 및 체계를 구축하고, 인허가 기관을 설치하여, 기준 및 체계에 적합하게 개발된 시스템만을 인증함으로써 안전성을 확보하고 있다.

특히, 1980년대 이후, 컴퓨터 기술의 향상으로 인해서 기존의 기계적으로 제어되던 아날로그 시스템들이 컴퓨터를 기반으로 하는 디지털 시스템으로 대체됨에 따라 이들 시스템의 안전성이 더욱 중요시되고 있다. 디지털 제어 시스템은 소프트웨어에 의해서 프로그래밍 되며, 이 소프트웨어는 용도에 적합하게 설계된 컴퓨터에 설치되어 제어 기능을 수행하게 된다. 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.

---

* 한국철도기술연구원 선임연구원, 정회원
** 한국철도기술연구원 주임연구원, 정회원
*** 한국철도기술연구원 연구원, 정회원

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.

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.

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 프로세스가 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 CMMI와 ISO/IEC 15504 (SPICE)를 들 수 있다.

1장에서는 철도시스템의 안전성과 관련하여 철도소프트웨어의 현황에 대하여 다루었고, 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.

2. 철도안전 법체계 및 표준과의 관계

건교부 사업인 철도종합안전기술개발사업 중 한국철도기술연구원 주관으로 2005년부터 2008년까지 수행하는 “철도소프트웨어 안전기준 체계구축” 과제의 목적은 철도에 사용되는 컴퓨터 기반 제어기의 소프트웨어 안전성 확보를 위한 안전규제 체계의 개발이다. 즉, 아래 그림에서와 같이 현재 철도안전법, 시행령, 시행규칙의 하위 법령으로 철도소프트웨어에 대한 안전기준을 마련하고, 이에 대한 해석을 뒷받침할 수 있는 지침을 개발하는 것이다. 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.

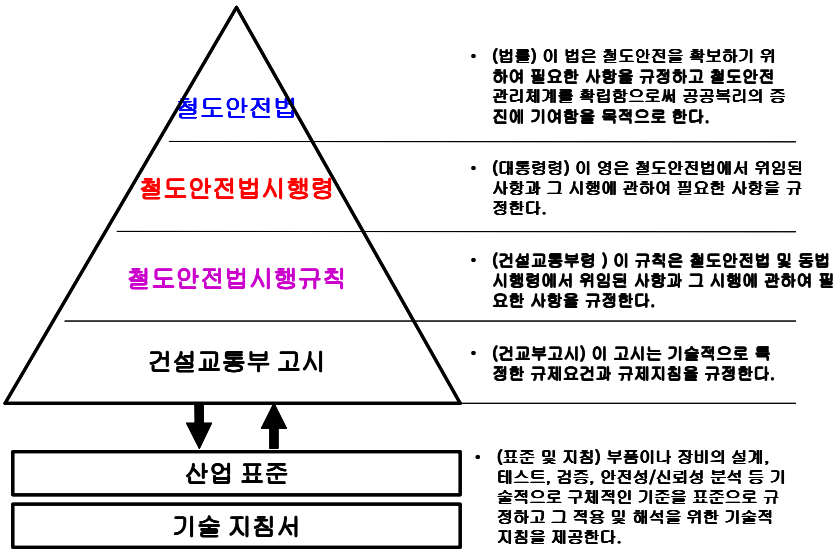

그림 1. 철도안전법과 표준과의 관계

아래 그림은 철도소프트웨어 안전기준을 작성하는데 있어서 생명주기 공정, 계획, 요구명세, 설계, 시험, 설치 등으로 구분하여 참조하여야 하는 규격 및 기준과의 관계를 도식화하여 나타낸 것이다.

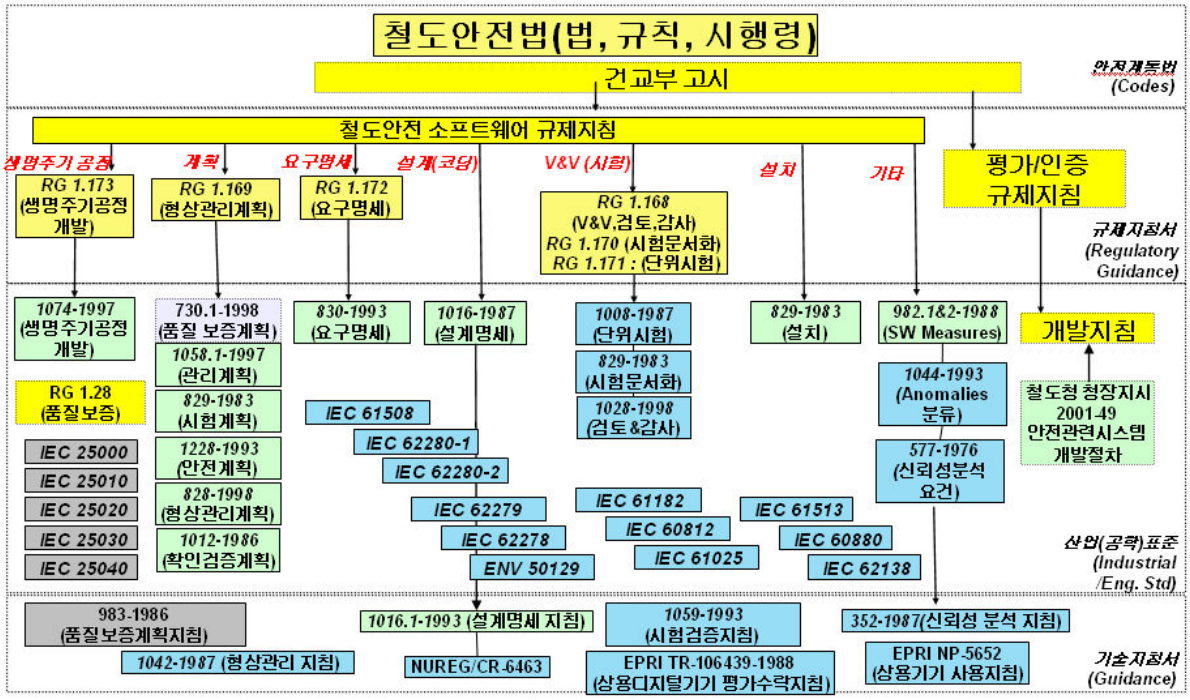

그림 2. 철도S/W안전기준과 표준과의 관계

또한 S/W 안전과 관련된 이해관계자는 S/W 개발자, S/W 구매자, S/W 심사 및 평가자 등으로 나누어 질 수 있으며, 각 이해관계자가 제시된 철도 S/W 안전기준에 맞추어 제품을 개발, 선정, 심사하기 위해서 하여야 할 일에 대하여도 제시할 예정이다.

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 만들어진다는 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 (CMMI, SPICE)

3.1 CMMI (Capability Maturity Model Integration)

CMMI 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.

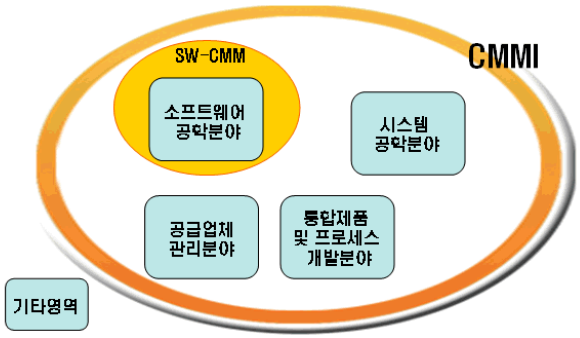

그림 3. CMMI로의 통합

3.2 ISO/IEC1504 (SPICE : Software Process Improvement Capability dEtermination) [3]

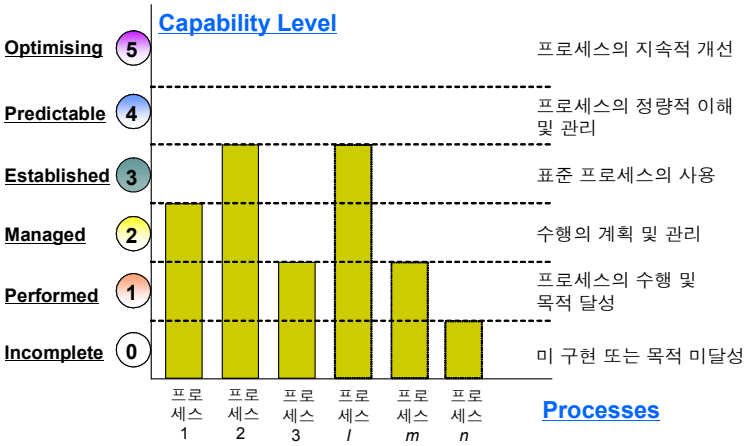

그림 4. SPICE의 Dimension

ISO/IEC 15504(SPICE)는 CMMI와 마찬가지로 조직의 프로세스를 개선하고 평가하기 위한 활동을 지원하기 위하여 현재의 프로세스 상태를 파악하여 그 성숙도를 측정한다. SPICE는 크게 두 영역으로 나누어진다. 심사대상 프로세스에 대하여 다룬 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 뿐만이 아니라 System 분야 등 모든 분야에 대하여 다룰 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 주관기관만 다를 뿐, 다루는 영역이나 심사 프로세스가 동일하다고 볼 수 있다. 여기에서는 SPICE의 두개의 영역을 중점을 두어 다루었다.

4.1 Reference model 영역

SPICE에서 Reference model 이란 심사 대상 프로세스를 말하는 것으로 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 능력 지표를 Reference 모델과 대응하여야 한다.
- 해석 : 검증 가능한 공식적 메커니즘에 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, 전체적으로 총 48개의 프로세스가 정의되어 있다.

표 1. ISO/IEC 15504의 프로세스

PRIMARY Life Cycle Processes	ORGANIZATIONAL Life Cycle Processes
1. Acquisition Process Group (ACQ)	**1. Management Process Group (MAN)**
ACQ. 1 Acquisition preparation	MAN.1 Organizational alignment
ACQ. 2 Supplier selection	MAN.2 Organization management
ACQ. 3 Contract agreement	MAN.3 Project management
ACQ. 4 Supplier monitoring	MAN.4 Quality Management
ACQ. 5 Customer acceptance	MAN.5 Risk Management
2. Supply Process Group (SPL)	MAN.6 Measurement
SPL.1 Supplier tendering	
SPL.2 Software release	**2. Process Improvement Process Group (PIM)**
SPL.3 Software acceptance support	PIM.1 Process establishment
3. Engineering Process Group (ENG)	PIM.2 Process assessment
ENG.1 Requirement elicitation	PIM.3 Process improvement
ENG.2 System requirement analysis	**3. Resource & Infrastructure Process Group (RIN)**
ENG.3 System architectural design	RIN.1 Human resource management
ENG.4 Software requirement analysis	RIN.2 Training
ENG.5 Software design	RIN.3 Knowledge management
ENG.6 Software construction	RIN.4 Infrastructure
ENG.7 Software integration	**4. Reuse Process Group (REU)**
ENG.8 Software testing	REU.1. Asset management
ENG.9 System integration	REU.2 Reuse program management
ENG.10 System testing	REU.3 Domain engineering
ENG.11 Software installation	
ENG.12 Software & system maintenance	

4. Operation Process Group (OPE) OPE.1 Operational use OPE.2 Customer support	
SUPPORTING Life Cycle Processes	
Support Process Group (SUP)	
SUP.1 Quality assurance	SUP.6 Product evaluation
SUP.2 Verification	SUP.7 Documentation
SUP.3 Validation	SUP.8 Configuration management
SUP.4 Joint review	SUP.9 Problem resolution management
SUP.5 Audit	SUP.10 Change request management

4.2 Assessment model 영역

Reference 모델, 즉 프로세스에 대한 평가를 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 평가 지표는 각각의 프로세스에 대한 Base Practice(BP)와 Work Product(WP)의 여부로 판단하며, Level 2~5의 PA는 각각이 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. 다음 표는 각각의 PA에 대한 설명 및 Assessment model의 rating과 level을 나타낸 것이다. 각각의 PA에 대하여 rating 함으로써 각 PA에 대한 N, P, L, F를 도출할 수 있으며, 이는 다음 표의 규칙에 따라 Level을 정하게 된다. 즉, 이전단계의 PA rating이 모두 F이고, 최종단계 Level의 PA가 L이거나 F이면 해당 Level을 달성하였다고 본다.

표 2. Process Attribute

Process Attribute ID	Capability Levels and Process Attribute Names
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	내 용
N Not achieved	0%~15%: There is little or no evidence of achievement of the defined attribute in the assessed process.
P Partially achieved	16%~50%: There is evidence of a sound systematic approach to and achievement of the defined attribute in the assessed process. Some aspects of achievement may be unpredictable.
L Largely achieved	51%~85%: There is evidence of a sound systematic approach to and significant achievement of the defined attribute in the assessed process. Performance of the process may vary in some areas or work units.

F Fully achieved	86%~100%: There is evidence of a complete and systematic approach to and full achievement of the defined attribute in the assessed process. No significant weaknesses exist across the defined organizational unit.

표 4. Process Attribute Level

Level	Process Attributes	Rating
Level 1: Performed.	Process performance	Largely or fully
Level 2: Managed.	Process Performance	Fully
	Performance Management	Largely or fully
	Work Product Management	Largely or fully
Level 3: Established.	Process Performance	Fully
	Performance Management	Fully
	Work Product Management	Fully
	Process Definition and Tailoring	Largely or fully
	Process Resource	Largely or fully
Level 4: Predictable.	Process Performance	Fully
	Performance Management	Fully
	Work Product Management	Fully
	Process Definition and Tailoring	Fully
	Process Resource	Fully
	Process Measurement	Largely or fully
	Process Control	Largely or fully
Level 5: Optimizing	Process Performance	Fully
	Performance Management	Fully
	Work Product Management	Fully
	Process Definition and Tailoring	Fully
	Process Resource	Fully
	Process Measurement	Fully
	Process Control	Fully
	Process Change	Largely or fully
	Continuous Improvement	Largely or fully

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 일반 S/W의 프로세스 심사에 사용되는 SPICE를 철도분야에 맞도록 적용하는 작업을 진행하고자 한다.

[참고문헌]

[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"