

# 시스템 및 소프트웨어 보증 국제표준 (ISO/IEC/IEEE 15026) 동향

임태형 TTA 소프트웨어시험인증연구소 책임연구원

## 1. 머리말

지금은 너무나 익숙한 삶의 방식이지만, 불과 얼마 전까지만 해도 집에서 온라인으로 물건을 구매하고, 이동하면서 현금을 이체하는 것은 꿈같은 이야기였다. 빠르게 발전한 정보통신과 소프트웨어 기술은 이제 운전자의 개입 없이 스스로 도로를 달리는 자동차를 만들고, 의사와 판사를 대신하는 인공지능 시스템을 현실화하며, 드론으로 물건을 배송하는 시대를 열고자 한다. 인간의 삶의 영역 중 어느 한 곳도 소프트웨어를 비롯한 기술의 힘이 미치지 않는 곳이 없는 것처럼 느껴질 정도이다.

정보통신기술의 발달로 생활의 편리함은 커지고 있지만, 다른 한편으로 시스템의 오작동으로 인한 사람과 환경에 대한 안전사고, 개인의 프라이버시 침해나 보안 문제 등이 중요한 사회문제로 대두되고 있다. 특히 기존에는 제한된 영역에서 한정된 임무만 수행하던 정보통신 시스템이 이제는 인간의 생명과 직결된 자동차, 의료, 제조 분야 등에 빠르게 적용되면서 시스템 안전성, 신뢰성, 보안성 등을 확보하는

것이 시스템 및 소프트웨어 공학의 가장 중요한 과제 중 하나가 되었다.

엔지니어를 비롯한 연구자들은 시스템 및 소프트웨어의 결함을 최소화하고 품질을 확보하기 위해 지금까지 많은 노력을 해 왔다. 그 결과 다양한 시스템 및 소프트웨어 개발방법론, 시험방법론 등이 등장했고, 관련 국제표준이 제정되었다. 그러나 기존의 공학 기법들은 시스템과 소프트웨어가 충분히 믿을 수 있고, 안전하다는 것을 직접적으로 보증하지는 않는다. 기존 공학 기법들 대부분이 시스템의 품질에 대해 ‘최선’을 추구하는 방식이지 ‘보증’을 추구하는 방식이 아니기 때문이다. 즉, 기존의 시스템 및 소프트웨어를 개발하고 시험하는 방법론은 기본적으로 ‘시간 대비 효과’의 측면에서 가용한 시간과 투입 자원에 따라 최선을 다해 결함을 제거하려고 노력은 하지만, 그 결과에 대해서는 어떠한 보증도 하지 않는다. 운전면허증에 비유하자면, 운전면허증이 제공하는 정보는 면허소지자가 ‘운전을 할 수 있다’는 사실을 나타낼 뿐이지, 운전자가 ‘어떤 상황에서도 사고를 일으키지 않는다’는 것을 포함하

지 않는다는 것과 비슷하다.

이는 무한대의 비용과 시간을 투자한다고 해도 대규모 시스템이나 소프트웨어의 결함을 완벽히 제거할 수는 없다는 근본적이고 현실적인 어려움에 바탕을 두고 있다. 이러한 사정을 감안한다고 해도 자율자동차, 무인 의료 시스템, 드론 배송이 현실이 되는 시대에 여전히 제한적인 몇 가지 시험을 통과했다는 사실만으로 시스템을 운용하는 것은 매우 위험하다. 사소한 시스템의 오작동이 치명적인 사고로 이어질 수 있는 가능성이 낮다고 해도 '0'은 아니기 때문이다. 시스템을 구성하는 부품의 수, 소스코드는 계속해서 증가할 것이고, 인공지능 등 알고리즘 자체의 복잡도가 높고 검증이 어려운 신기술이 계속 도입될 것이다. 뿐만 아니라 운용환경은 때때로 예측하지 못한 불확실한 상황으로 급변할 수 있다. 이러한 어려운 조건에서도 시스템이 안전하고, 신뢰할 수 있으며, 보안 문제가 발생하지 않는다는 믿음을 사용자에게 줄 수 있어야 한다. 따라서 시스

템 및 소프트웨어 보증에 대해 다루고 있는 유일한 표준인 ISO/IEC/IEEE 15026<sup>1)</sup>은 큰 의미를 지닌다. 본고에서는 2019년 개정된 파트 1을 비롯하여 15026의 파트별 내용을 간략히 소개한다.

## 2. 시스템 및 소프트웨어 보증의 개념

ISO/IEC/IEEE 15026의 내용을 소개하기 전에 '보증(Assurance)'의 개념에 대해 먼저 알아보자. 시스템 및 소프트웨어 공학에서 보증은 품질과 관련된 용어이다. ISO/IEC 25010[1]에는 기능적 합성, 수행효율성, 호환성, 유용성, 신뢰성, 보안, 유지관리성, 이동성 등 총 8가지 품질 특성을 정의하고 있으며, 이러한 품질 특성은 시스템의 요구사항에 반영되거나 시험의 기준으로 활용되었다. 이 때에도 품질 보증(Quality Assurance)이라는 용어가 일반적으로 통용되었으나, 여기서 말하는 보증의 개념은 다소 제한적이고 모호한 의미를 갖



[그림 1] 시스템 및 소프트웨어 보증의 개념도

1) 파트 1을 제외한 나머지 3개 파트는 모두 ISO/IEC 표준이지만, 본고에서는 전체 시리즈를 언급할 때 2019년 개정된 파트 1을 기준으로 ISO/IEC/IEEE로 표기한다.

는다. 기존 시스템 및 소프트웨어 공학이 추구하는 보증의 개념은 시스템이 예측된 환경에서 정해진 절차에 따라 동작시켰을 때 기대한 바와 같이 문제없이 동작함을 의미한다. 이러한 수준의 보증 개념에서는 극단적인 상황이나 예외적인 상황, 돌발적 상황, 비정상적이거나 악의적인 시스템 조작 등은 중요한 고려사항이 아니었다.

그러나 보안이나 안전과 관련된 시스템과 소프트웨어는 비정상적, 예외적인 상황에 대해 반드시 고려되어야 한다. 대부분의 문제가 기존 품질 보증의 영역 밖에 속하는 비정상적이고, 예외적 상황에서 발생하기 때문이다. 예컨대 시스템에 악의적으로 접근하려는 공격자는 설계자의 의도에 따라 정해진 규칙을 준수하면서 행동하지 않으며, 자율주행자동차의 운행환경인 도로의 상태, 날씨, 주변 차량의 움직임 등은 모두 통제 밖의 대상이며 불확실성의 세상이다. 이러한 도전적인 상황에서도 시스템의 안전과 보안에 대한 믿음이 요구되기 때문에 보증의 개념에 대해 새롭게 접근할 필요가 있다.

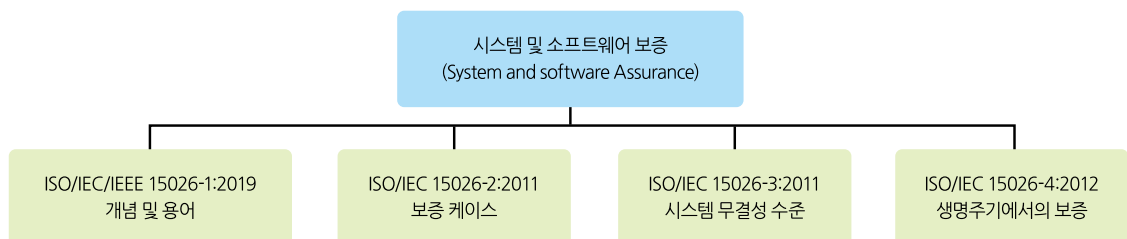
기존의 시스템 및 소프트웨어 공학의 한계를 벗어나기 위해 보안 공학 및 안전 공학이 제시한 접근 방법은 위험 분석이다. 위험 분석은 시스템이 정상적으로 동작하는 시나리오 외에도 발생가능한 모든 잠재적인 사고의 시나리오를 가정하는 것부터 시작한다. 단지 정해진 요구사항을 착실하게 단계

별로 준수하여 개발하는 기존 생명주기를 따르는 것에 그치는 것이 아니라, 개발 초기부터 적극적으로 예외적이고 비정상적인 상황을 가정하여 분석하고 대비책을 마련하는 데 초점을 둔다. 이러한 관점에서의 보증은 보안이나 안전사고가 발생하지 않는다는 시스템에 대한 신뢰를 객관적 근거로 주장하는 것이다. 15026은 이러한 발전된 보증의 개념을 ISO/IEC/IEEE 15288[2], ISO/IEC/IEEE 12207[3]과 같은 기존 생명주기 프로세스와도 상호보완적으로 활용하는 것을 목표로 한다.

### 3. ISO/IEC/IEEE 15026 구성 및 개요

ISO/IEC/IEEE 15026은 국제표준 단체인 ISO와 IEC의 통합기술위원회 JTC1 산하의 분과 위원회 SC7에서 담당하고 있다. SC7은 생명주기 프로세스, 소프트웨어 테스트, 요구공학, 품질 모델 및 평가 등 시스템 및 소프트웨어 공학 분야 전반을 담당하고 있다. ISO/IEC/IEEE 15026은 크게 4개의 파트로 구성되어 있다.

- ISO/IEC/IEEE 15026-1:2019 파트 1: 개념 및 용어[4]
- ISO/IEC 15026-2:2011 파트 2: 보증 케이스(Assurance Case)[5]
- ISO/IEC 15026-3:2015 파트 3: 시스템 무결성 수준(System integrity levels)[6]
- ISO/IEC 15026-4:2012 파트 4: 생명주기에서의 보증[7]



[그림 2] ISO/IEC/IEEE 15026의 구성

〈표 1〉 ISO/IEC/IEEE 15026-1의 개정 사항

| 구분                 | 개정 사항                                            |                                                                                                                                                                                                                       |
|--------------------|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | 용어 정의 변경                                         | 신규 정의 추가                                                                                                                                                                                                              |
| 3.1 보증과 특성 관련 용어   | 1개(Dependability)                                | 2개(Attribute, Condition)                                                                                                                                                                                              |
| 3.2 제품과 프로세스 관련 용어 | 없음                                               | 없음                                                                                                                                                                                                                    |
| 3.3 무결성 수준 관련 용어   | 2개(Integrity Level, Integrity Level Requirement) | 13개(Initial Risk, Integrity Level Claim, Level of Risk, Likelihood, Residual Risk, Risk Criteria, Risk Reduction Measure, Risk Source, Risk Treatment, System-of-Interest, Target Risk, Threat Agent, Tolerable Risk) |
| 3.4 조건과 결과 관련 용어   | 2개(Risk, Error)                                  | 2개(Dangerous Condition, Property-of-Interest)                                                                                                                                                                         |
| 3.5 조직 관련 용어       | 없음                                               | 없음                                                                                                                                                                                                                    |

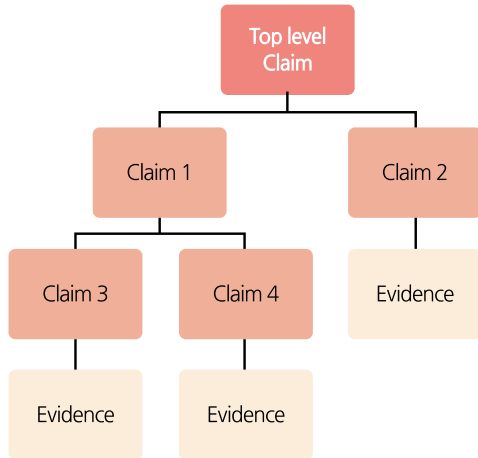
파트 1은 시스템 및 소프트웨어의 보증 개념 및 관련 용어 정의를 다루고 있다. 파트 1의 목적은 좁게 보면 15026의 나머지 파트들과의 공통 이해의 기반을 마련하기 위한 것이고, 넓게 보면 ISO/IEC/IEEE 15288, 12207 등 생명주기 표준과 협업하는 데 필요한 용어 정의이다. 파트 1은 2013년에 표준으로 제정된 후 2019년 3월에 개정되었다. 개정의 가장 큰 이유는 2015년에 시스템 무결성 수준이 파트 3으로 제정되면서 관련 용어가 새롭게 추가되었기 때문이다.

파트 2는 15062가 추구하는 보증 개념의 핵심이라고 할 수 있는 보증 케이스를 다루고 있다. 보증 케이스는 시스템의 개발·운영에서 예상되는 어려움이나 장애요소로 식별된 리스크에도 불구하고 시스템이 성공적으로 동작하리라는 증거에 기초해서 주장하는 것이다. 이를 위해 보증 케이스는 주장과 이를 뒷받침하는 증거, 그리고 이들 사이의 논증으로 구성된 트리 구조를 갖는다. 결국 15026에서 추구하는 보증의 개념은 보증의 대상과 목표를 정의하고, 이를 뒷받침하는 증거들을 수집하여, 이들 사이의 객관적이고 논리적인 논증의 구조를 완성하는 것이며, 보증 활동의 최종 산출물은 보증 케이스의 형태로 구체화된다.

파트 3은 시스템 및 소프트웨어 보증을 위한 무결성 수준에 대해 다룬다. 무결성 수준은 보증 케

이스와 마찬가지로 시스템의 보증에서 매우 중요한 개념이다. 무결성 수준은 위험 분석의 결과로 결정된다. 위험 분석은 시스템에 대해 우리가 알지 못하는 것과 알아야 하는 것 사이의 균형을 맞추는 작업이라고 할 수 있다. 즉, 시스템의 다양한 불확실성에 대응하는 현실적인 방법은 모든 불확실성을 동일한 기준에서 처리하지 않고, 예상되는 사고의 파급력이나 발생 가능성을 고려해 차등적으로 처리하는 것이다. IEC 61508[8]에서는 같은 맥락에서 SIL(Safety Integrity Level)을 정의하여 사용하고 있다. 다만 IEC 61508의 SIL은 하드웨어의 특성을 반영하여 고장률이나 수리 기간 등을 정량화하기에 용이하지만 소프트웨어는 고장 특성과 수리 방법도 다르기 때문에 정량화하기 어려운 부분이 많다. 이러한 이유로 15026에서는 시스템과 관련한 위험이 명확히 정의되지 않거나 시스템의 구성요소 간 의존 구조가 불확실한 경우에 무결성 수준을 활용하기보다는 보증 케이스를 사용하는 편이 더 좋다고 설명하고 있다. 즉, 무결성 수준과 비교해서 보증 케이스는 보다 일반적으로 적용할 수 있는 보증의 근거가 될 수 있다.

파트 4는 생명주기의 프로세스 관점에서 보증을 다룬다. 생명주기의 각 단계에서 보증 케이스를 만들 때 필요한 작업들을 설명하고, 기존 생명주기 프로세스와 연계하는 방안을 다룬다. 시스템과 소프



[그림 3] 보증 케이스의 구조 예시

〈표 2〉 무결성 수준 및 기준의 예시

| 무결성 수준                | 무결성 수준의 기준(주장) |                                      |
|-----------------------|----------------|--------------------------------------|
| 가용성<br>(Availability) | a              | 요구되는 MTTR <sup>2)</sup> 이 1일 이하인 경우  |
|                       | b              | 요구되는 MTTR이 1시간 이하인 경우                |
|                       | c              | 요구되는 MTTR이 10분 이하인 경우                |
| 신뢰성<br>(Reliability)  | A              | 요구되는 MTBF <sup>3)</sup> 가 1개월 이상인 경우 |
|                       | B              | 요구되는 MTBF가 6개월 이상인 경우                |
|                       | C              | 요구되는 MTBF가 1년 이상인 경우                 |
| 보안성<br>(Security)     | I              | 요구되는 EAL <sup>4)</sup> 이 1 이상인 경우    |
|                       | II             | 요구되는 EAL이 4 이상인 경우                   |
|                       | III            | 요구되는 EAL이 7 이상인 경우                   |

트웨어의 생명주기 동안 많은 이해관계자가 존재하며, 보증을 위해 다양한 이해관계자를 반드시 고려해야 한다. 보증의 전제조건이 되는 다양한 시스템 제약 사항이 결국 서로 다른 이해관계자의 관점에 의해 결정되기 때문이다. 시스템 소유자, 사용자, 개발자, 운영자 등 서로 다른 관점에서 시스템에 요구하는 보증 대상을 명확히 정의하고 이에 관련된 불확실성을 최대한 줄이고, 타당한 신뢰의 근거들을 마련하는 것이 생명주기 활동에서 보증의 역할이다.

#### 4. 맺음말

인공지능 기술의 발전으로 우리는 기계가 인간을 대체할지도 모르는 급격한 변화의 시기를 눈앞에 두고 있다. 정보통신 시스템은 단순한 기능을 넘어, 복잡한 상황을 인지하고 환경에 적응하여 의사결정까지 스스로 내리도록 점점 진화하고 있다. 복잡한 시스템에서는 시스템의 오작동이 단지 어느 한 부품의 오작동에서 비롯된다고만 한정 지을 수 없다. 정

적으로 동작하는 시스템 구성요소들 사이에서도 의도하지 않거나 예측할 수 없는 상호작용에 의해 시스템이 오작동할 수 있고, 그 결과 사람이나 환경에 치명적 해를 끼칠 가능성이 존재한다. 시스템이 인간의 삶 속에 더 깊이 침투할수록 우리는 시스템에 대한 신뢰를 확신할 수 있어야 한다. 불확실한 상황에서도 시스템이 안전하고, 신뢰할 수 있으며, 보안 문제가 발생하지 않는다는 믿음을 사용자에게 줄 수 있어야 한다.

이러한 흐름 속에서 시스템 및 소프트웨어 보증을 다루는 유일한 표준인 ISO/IEC/IEEE 15026의 중요성은 점점 더 커질 수밖에 없다. 다만 2019년 개정된 파트 1을 제외하고 나머지 파트는 개정이 시급하며, 특히 15026의 핵심인 보증 케이스를 다룬 파트 2는 2011년 개정 후 많은 시간이 지났다. 이는 표준기관에서도 보증에 대한 확실한 해답을 고민하고 있다는 의미로 해석할 수 있으며, 한편으로 국내의 시스템 및 소프트웨어 공학의 연구자에게는 좋은 기회가 될 수도 있다. 15026에 지속적

2) Mean Time Recovery: 고장 후 수리 시간

3) Mean Time Between Failure: 고장 후 다음 고장이 발생할 때까지의 시간

4) Evaluation Assurance Level: ISO/IEC 15408에서 정의한 보안 관련 평가보증 수준

으로 관심을 갖고 시스템의 신뢰성을 높일 수 있는  
발판을 마련해야 한다. 

#### 주요 용어 풀이

- 평가 보증 등급(EAL, Evaluation Assurance Level): 정보 보호 시스템 공통 평가 기준(CC, Common Criteria)의 보증 요구 사항으로 이루어진 패키지. 정보 기술(IT) 제품 또는 시스템의 평가 결과 보안 기능을 만족한다는 신뢰도 수준을 정의한 것이다. 평가 보증 등급(EAL)은 IT 제품 또는 시스템의 형상 관리, 배포 및 운영, 개발, 설명서, 생명주기 지원, 시험, 취약성 평가 등을 포함하고, CC는 평가 보증 등급(EAL)을 7개의 등급(EAL1 ~ EAL7)으로 구분한다. 일반적으로 EAL 등급이 높아질수록 대상 제품 및 시스템에 대한 제출물 양이 많아지고 평가자가 더 많은 부분을 엄밀하고 상세하게 검토 및 시험을 한다.

#### 참고문헌

- [1] ISO/IEC 25010, Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models
- [2] ISO/IEC/IEEE 15288:2015, Systems and software engineering - System life cycle processes
- [3] ISO/IEC/IEEE 12207:2017, Systems and software engineering - Software life cycle processes
- [4] ISO/IEC/IEEE 15026-1:2019, Systems and software engineering - Systems and software assurance - Part 1: Concepts and vocabulary
- [5] ISO/IEC 15026-2:2011, Systems and software engineering - Systems and software assurance - Part 2: Assurance case
- [6] ISO/IEC 15026-3:2015, Systems and software engineering - Systems and software assurance - Part 3: System integrity levels
- [7] ISO/IEC 15026-4:2012, Systems and software engineering - Systems and software assurance - Part 4: Assurance in the life cycle
- [8] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety related systems