기능 안전 국제표준들의 구조적 커버리지 요건

<표 1>은 도메인별 기능 안전 표준의 기준이 되는 IEC 61508에서 요구하는 테스트 방법입니다. 여기서 R (Recommended)과 HR (Highly Recommended)은 필수적으로 수행해야 하는 요건을 의미합니다. 이때, HR은 R에 우선하며, HR을 고려하지 않을 경우에는 그에 대한 사유가 계획단계에서 부터 명시되고, 인증 평가자의 동의를 받아야 합니다.

IEC 61508에서는 테스트 결과가 만족해야 할 문장 (Statement) 커버리지가나 결정 (Decision) 커버리지와 같은 구체적인 구조적 커버리지 기준을 정하지는 않고 있습니다. 즉, IEC 61508은 특정 IT융합 제품 영역을 대상으로 하지 않고 있기 때문에, 각 테스트 단계에 대한 수행 결과의 Pass/Fail 기준을 테스트 계획 수립 시 적절하게 설정하고 수행할 것을 요구하는 등 기법적인 준수 보다는 절차적인 준수 위주로 제시하고 있습니다.

■ <표1> IEC 61508: Dynamic Analysis and Testing 요건

Table B-2		Safety Integrity Level			
		SIL1	SIL2	SIL3	SIL4
1	Boundary value analysis	R	HR	HR	HR
2	Error guessing	R	R	R	R
3	Error seeding	—	R	R	R
4	Performance modeling	R	R	R	HR
5	Equivalence classes and input partition testing	R	R	R	HR
6	Structure-based testing	R	R	HR	HR

항공 분야의 기능 안전 표준인 DO-178B의 안전 무결성 등급은 A~D로 나누어지며 A가 제일 높은 등급입니다. <표 2>는 DO-178B에서 요구하는 코드 커버리지 요건으로, ○와 ●는 모두 커버리지가 달성되어야 함을 의미합니다. 단, ●는 테스트 자체가 독립적으로 수행되어야 합니다. DO-178B에서는 IEC 61508과는 달리 안전 무결성 등급에 따라 달성되어야 하는 구조적 커버리지 기준을 제시하고 있기는 하지만, 해당 커버리지가 어떤 특정 테스트 단계 (단위/통합/시스템)의 수행 결과로 만족해야 함을 요구하지는 않고 있습니다. 즉, 최고 안전 무결성 등급의 제품 개발 시 단위 테스트 단계에 MC/DC 커버리지를 만족하지 않아도 된다는 것을 의미합니다.

■ <표2> DO-178B: Verification of Verification Process Results 요건

Table A-7		Applicability by SW Level			
		A	B	C	D
1	MC/DC Coverage	●			
2	Decision Coverage	●	●		
3	Statement Coverage	●	●	○	
4	Data Coupling and Control Coupling Coverage	●	●	○	

<표 3>은 자동차 분야의 기능 안전 표준인 ISO 26262의 소프트웨어 단위 테스트에 대한 결과 검증을 위해 사용되는 코드 커버리지 기준에 대한 요건입니다. +와 ++는 각각 IEC 61508의 R과 HR에 해당합니다. ISO 26262는 DO-178B보다 더 엄격해서 특정 테스트 단계에서 달성해야 할 구조적 커버리지 요건을 제시하고 있습니다. 즉, 코드 기반의 단위 테스트는 물론, 모델 기반의 개발일 경우에도 모델에 유사한 구조적 커버리지 기준을 적용해야 하며, 통합 테스트 단계에서도 함수 (Function) 커버리지가 같은 구조적 커버리지를 적용한 결과를 요구하고 있습니다.

■ <표3> ISO26262: Structural coverage metrics at the software unit level 요건

Table 12		ASIL			
		A	B	C	D
1a	Statement Coverage	++	++	+	+
1b	Branch Coverage	+	++	++	++
1c	MC/DC (Modified Condition/ Decision) Coverage	+	+	+	++

소프트웨어 안전성 테스트 방법

짧은 개발주기를 맞추기 위해 개발이 거의 완료되는 시점에 집중적으로 테스트를 수행해 온 국내 IT융합 제품의 개발현실에서는 기능 안전 국제표준에서 요구하는 테스트 요건을 맞추기 매우 어렵습니다. 이는 기존 프로젝트 수행 방식 대비 최고 안전 무결성 등급의 경우 약 40~100% 이상의 노력을 추가로 요구하기 때문 입니다.

국제표준을 만족하면서도 효과적으로 테스트를 수행하기 위해서는

- 1) 제품 계획 초기 단계부터 더욱 더 철저한 **테스트 전략 및 계획을 수립**하고
- 2) 가능한 빨리 테스트 케이스를 쓰기 시작하는 **테스트 주도로 개발**하고
- 3) 좋은 테스트 요구사항을 가지기 위해 **추적성을 지속적으로 확보**하고
- 4) **모델 기반으로 테스트**할 수 있는 환경을 구성하고
- 5) 마지막으로, 각 단계별로 목적에 맞는 **신뢰성이 입증된 자동화 도구를 사용**하는 노력이 필요합니다.