ISO 26262 - Safety Mechanism

" 기능 안전 (Functional Safety)을 성공적으로 제공하는 전장 제품을 개발하기 위해서는 설정된 안전 목표 (Safety Goal)에서 식별된 안전 상태(Safe State)를 유지하기 위한 효과적인 안전 메커니즘 (Safety Mechanism)의 설계가 요구됩니다. "

ISO 26262에서는 안전 메커니즘을 다음과 같이 정의하고 있습니다 : "안전 상태 **(safe state)**로 도달하거나 유지하기 위해 결함 **(faults)** 검출 또는 고장 **(failure)** 제어를 수행하는 전기/전자장치의 기능이나 엘리먼트 **(elements)** 또는 기타 기술로 구현된 기술적 해결책 **(technical solution)**", **Technical solution** implemented by E/E functions or **elements**, or by **other technologies**, to detect **faults** or control **failures** in order to achieve or maintain a **safe state**"
(출처 : ISO 26262, Road vehicles - Functional safety, 2011-11-15)

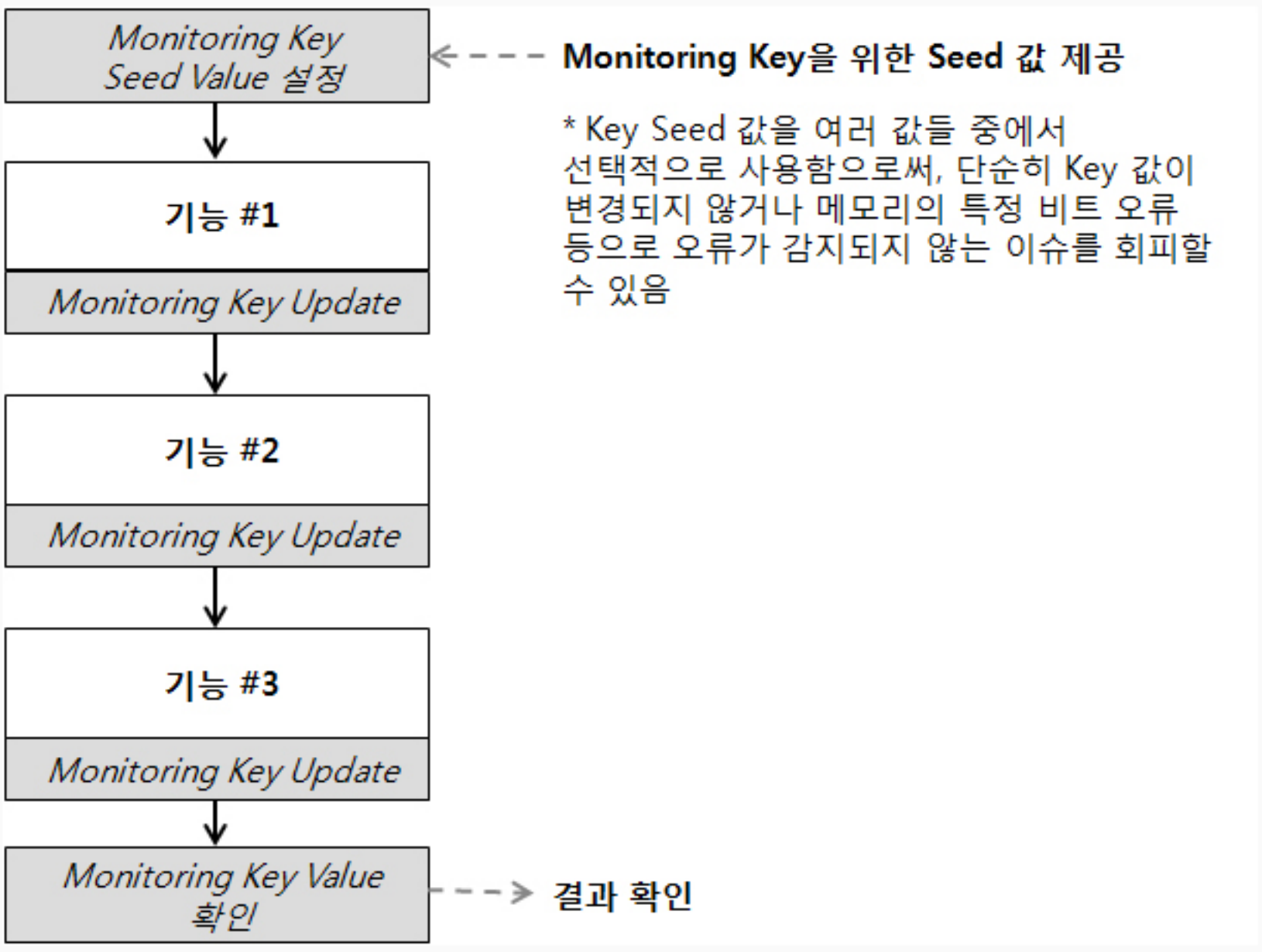
또한, ISO 26262에서는 ASIL 등급에 따라서 전장용 소프트웨어에 적용되어야 하는 대표적인 안전 메커니즘 목록을 다음과 같이 가이드 하고 있습니다.

분류	안전 메커니즘
오류감지 (Error Detection)	Control flow monitoring
	Detection of data errors
	Diverse software design
	External monitoring facility
	Plausibility check
오류처리 (Error Handling)	Correcting codes for data
	Graceful degradation
	Independent parallel redundancy
	Static recovery mechanism

이 중 오류 감지(Error Detection)에 해당하는 안전 메커니즘들에 대한 설명은 다음과 같습니다.

Control flow monitoring

제어 흐름 오류 (Control flow error)는 전압 이상, 버퍼 오버플로우 등으로 프로그램의 제어 흐름이 부적절한 곳으로 이동 하면서 발생하는 오류입니다. 이러한 제어 흐름 오류의 발생을 감지하기 위해서 제안된 기법이 제어 흐름 모니터링(Control flow monitoring) 입니다. 예를 들어 3개의 기능이 순서대로 진행되어야 하는 경우 다음과 같이 제어 흐름 모니터링을 수행 할 수 있습니다.



Detection of data errors

제어 흐름 오류와 마찬가지로 메모리 및 데이터 버스 상의 장애로 데이터에 대한 오류가 발생할 수 있습니다. 이러한 데이터 오류들은 오류 감지 코드 (error detecting code)와 데이터 중복 저장 (multiple data storage) 기법으로 발생을 감지할 수 있습니다.

Diverse software design

특정 방식의 설계에서 발생할 수 있는 결함을 감지하기 위해서 소프트웨어 설계의 다양성 (diversity)을 활용할 수 있습니다.

External monitoring facility

외부에 모니터링 기능을 추가함으로써 오류를 안정적으로 감지할 수 있습니다. 즉, 별도의 Watchdog 기능을 추가함으로써 오류를 감지하는 기법입니다.

Plausibility check

신뢰성 검사 (Plausibility check – Plausibility "그럴듯 함")는 Assert 검사와 같이 일반적으로 확인하기 쉬운 조건들을 검사 함으로써 비교적 적은 노력으로 오류를 확인하는 기법입니다.