본 슬라이드는, 세미나 자료에서 일부 발췌한 자료입니다.

ISO26262의 소프트웨어 개발 프로세스

주식회사 Vitz
Embedded control 개발부 기능 안전 개발실
실장 모리카와 토시히사

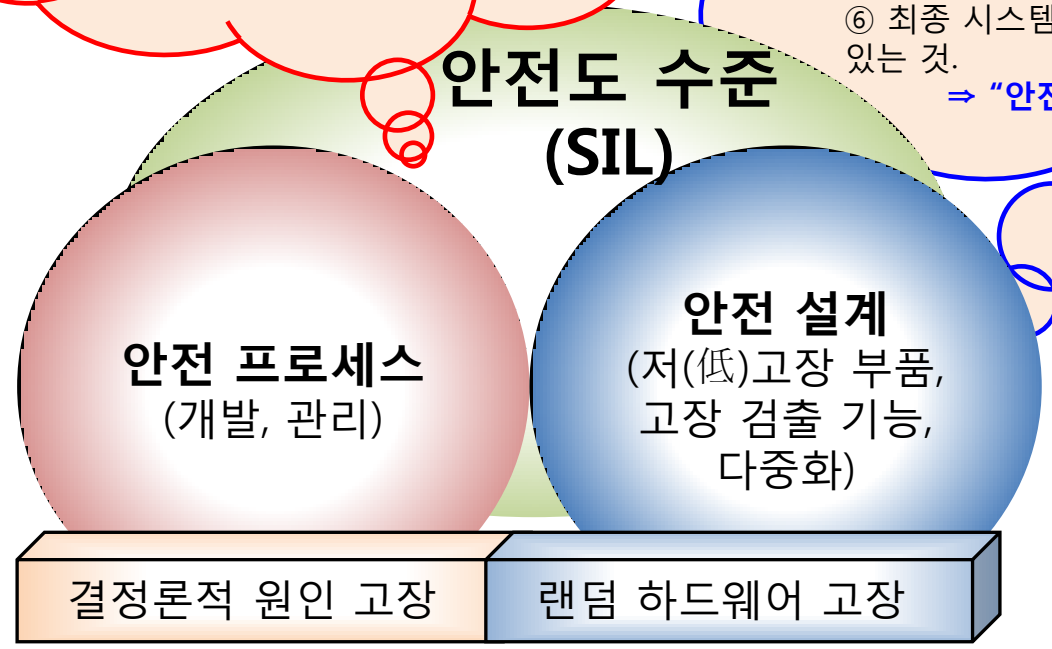
기능 안전의 달성에 필요한 것(안전 증명)

기능 안전 = 안전 증명

- 제 3자(인증 기관, 유저들)에 따라, **안전한 것인지 확인되어야 한다.**
- 크게는, 안전 프로세스·안전 설계의 두 가지 측면부터.

① "기능 안전 관리 규정"이 기능 안전 규격을 만족하고 있는 것.
② 실제 개발이, "기능 안전 관리 규정"에 정해진 대로 실시되고 있는 것.
⇒ **"기능 안전 관리 규정"이 핵심**

③ 시스템의 "안전 concept"이 기능 안전 레벨을 만족시키고 있는 것.
(안전 목표, 안전 분석, 안전 요구 사양, 안전 설계, 안전 매뉴얼 등)
④ 개발 도중의 성과물이 모두 문제가 없는 것.
(Traceability, 독립 검증)
⑤ 최종 성과물이 당초의 "안전 concept"을 만족하고 있는 것. (기능 안전, 환경 시험, 고장 삽입 시험 등)
⑥ 최종 시스템의 고장률이, SIL을 달성하고 있는 것.
⇒ **"안전 concept"이 핵심**



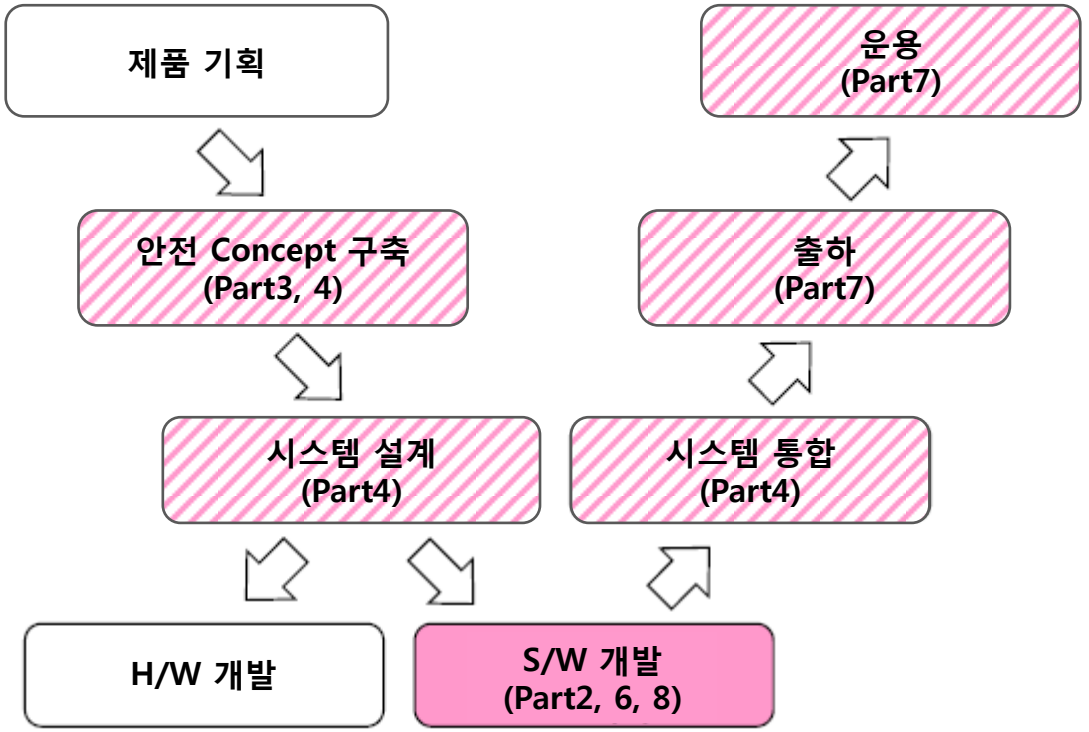
Concept phase
①③

실현 Phase
V
⑤⑥
②④

소프트웨어 개발에 관한 요구 범위

ISO 26262	요구사항
Part2	기능 안전 개발 프로세스 (개발, 관리)
Part6	
Part8	
Part3	소프트웨어에서 안전책
Part4	소프트웨어에서 안전책 시스템 개발과의 통합방법
Part7	유저의 요구사항

기능 안전 개발의 전체 흐름



< Part2 >
5 전체적으로 안전한 관리
6 concept phase와 제품 개발 간의 프로젝트 관리
7 제품 release 후의 안전 관리

< Part6 >
5 소프트웨어 레벨에서 제품 개발의 개시
6 소프트웨어 안전 요구의 상세 사양
7 소프트웨어 아키텍처 설계
8 소프트웨어 단위의 설계 및 구축
9 소프트웨어 단위 테스트
10 소프트웨어 통합 및 테스트
11 소프트웨어 안전 요구 타당성 검증
Annex C 소프트웨어 configuration

< Part8 >
5 분담 개발 내의 인터페이스
6 안전 요구의 사양과 관리
7 configuration 관리
8 변경 관리
9 verification
10 문서화
11 소프트웨어 툴의 검정
12 소프트웨어 컴포넌트의 검정
13 하드웨어 컴포넌트의 검정
14 사용 과정 증명

이들을 FSMP (Functional Safety Management Plan: 기능 안전 관리 계획) 규정 문서로 정리한다.

기본적으로 FSMP는 개발 제품마다 준비한다.

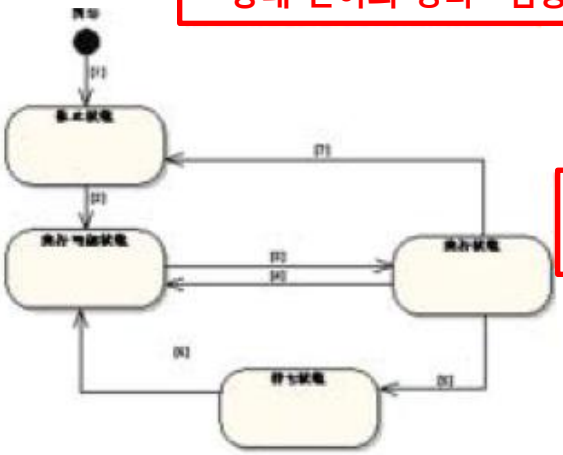
ISO 9000의 QM (Quality Management)이나 Automotive-SPICE의 관리 규정과 큰 차이는 없다.

준 형식 수법의 실시 예

※ 당사 RTOS 개발 문서에서 발췌

상태 전이도

상태 전이의 정리 · 검증



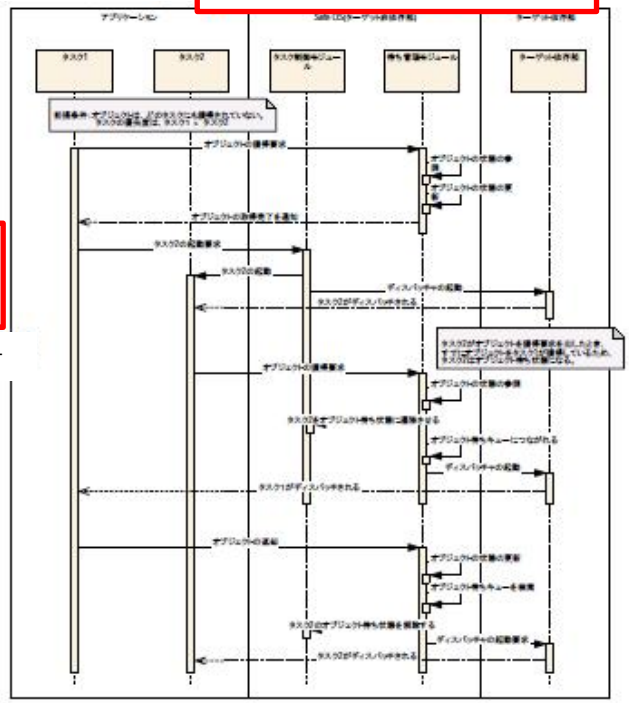
+

상태 · 시간의 복합 검증

= 타임패트리네트 해당

Sequence도

Sequence의 정리 · 검증



소프트웨어 구성도

모듈 간의 관련 · I/F 정의

결정표

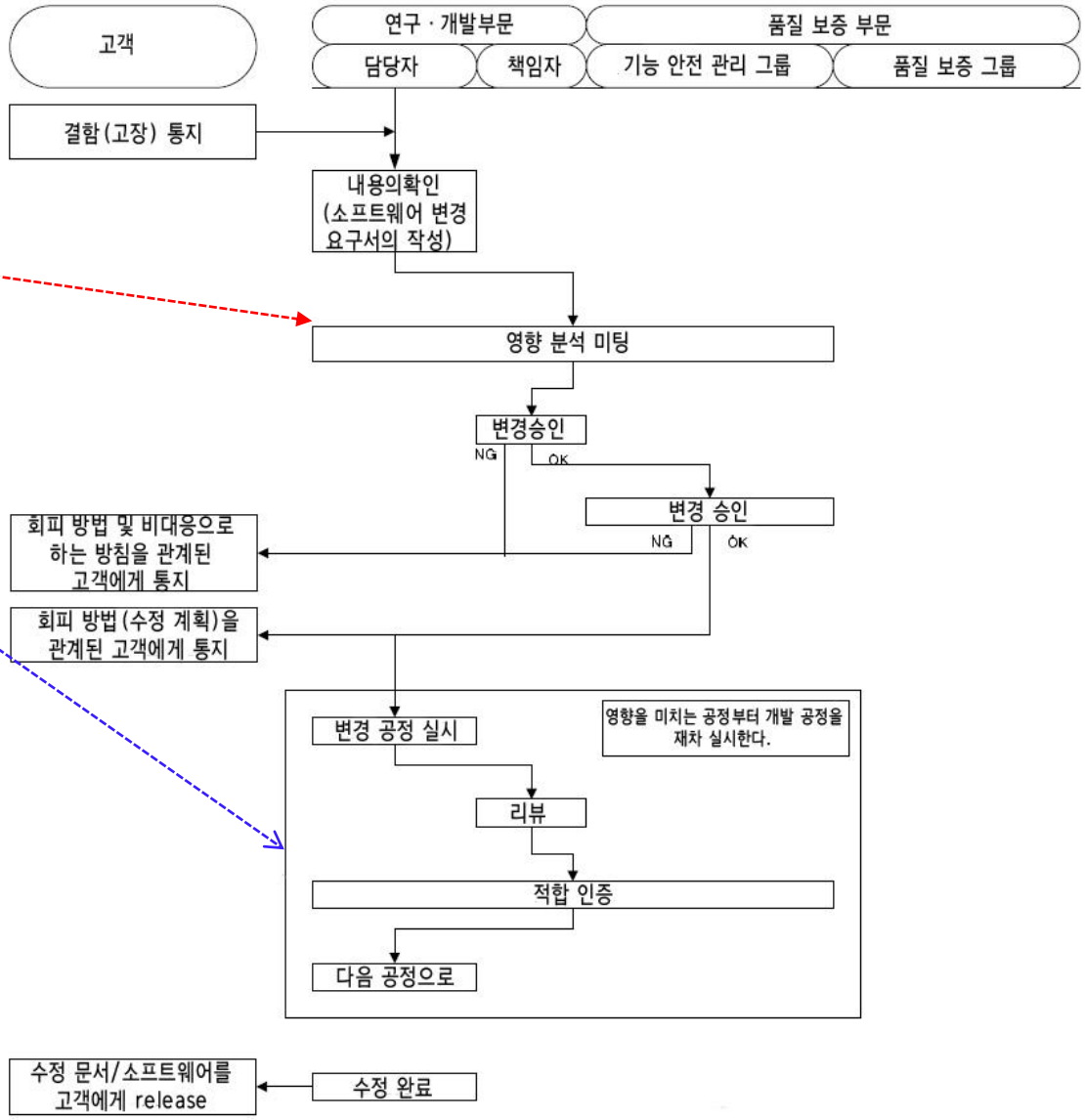
복잡한 조건 실행의 정리 · 검증

カーネルへの処理要求	割込みハンドラ	Y	N	N	N
	タスクで発生したCPU例外ハンドラ	-	Y	N	N
	タスク処理要求　優先度 現在のタスクより高い	-	-	Y	N
	タスク処理要求　優先度 現在のタスク以下	-	-	-	Y
ディスパッチャ	ディスパッチ処理が実行される	-	-	X	-
実行される処理単位	割込みハンドラ	X	-	-	-
	CPU例外ハンドラ	-	X	-	-
	タスク処理　優先度 現在のタスクより高い	-	-	X	-
	タスク処理　優先度 現在のタスク以下	-	-	-	X

소프트웨어 변경 프로세스

- 완성된 소프트웨어를 변경하는 경우는, 신중하게 대응할 필요가 있다.
- 영향 분석
  +
  재 검증(Verification) 필수.

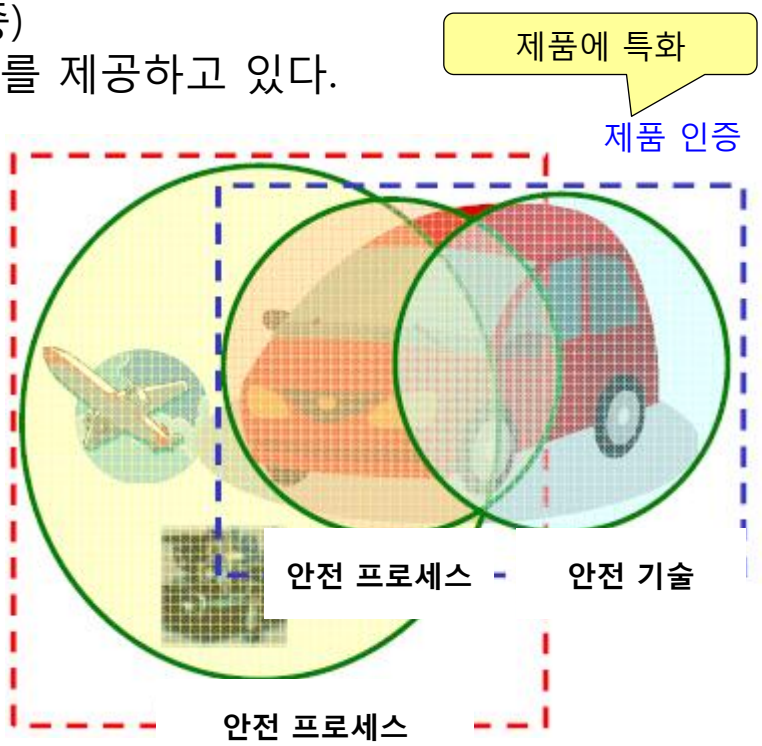
- 변경 관리, 구성 관리, 조직 간의 제휴도 깊게 관련한다.



TUV의 기능 안전 인증의 종류

기능 안전에서는, 제품 마다 인증을 실시한다. (제품 인증)
한편, 인증 기관(TUV)은, 아래의 2가지 종류의 인증 형태를 제공하고 있다.

	프로세스 인증	제품 인증
개념	"규정(안전 프로세스)"에 대한 인증	"결과(안전 프로세스+안전 설계)"에 대한 인증
적용 범위	다양한 제품에 적용 가능	제품 마다 인증이 필요
유효 기한	3년간	제품이 파기될 때까지
개발 프로세스	범용적인 개발 프로세스	제품에 특화(特化)한 개발 프로세스
대상 하드웨어	한정할 수 없음	고정



<주의사항>
- **인증 취득 유무에 관계 없이, 개발 시에 실시하는 내용은 같다.**
  (누군가가 실시하는가의 차이. 인증 기관 비용의 차이 정도)
- **소프트웨어 프로세스는, 어느 기능 안전 규격에서도 거의 동등.**

프로세스 인증

복수의 제품은 물론, 광범위한 산업에 공통으로 적용 가능