SPI Japan 2012

차재용 기능 안전 규격 ISO 26262에 대응한 고신뢰 개발 프로세스와 활동

2012년 10월 11일

파나소닉㈜ 디바이스 사
개발 본부 기능 안전·DR추진 그룹
아베 슈지

기능 안전 규격 이란?

Panasonic
ideas for life

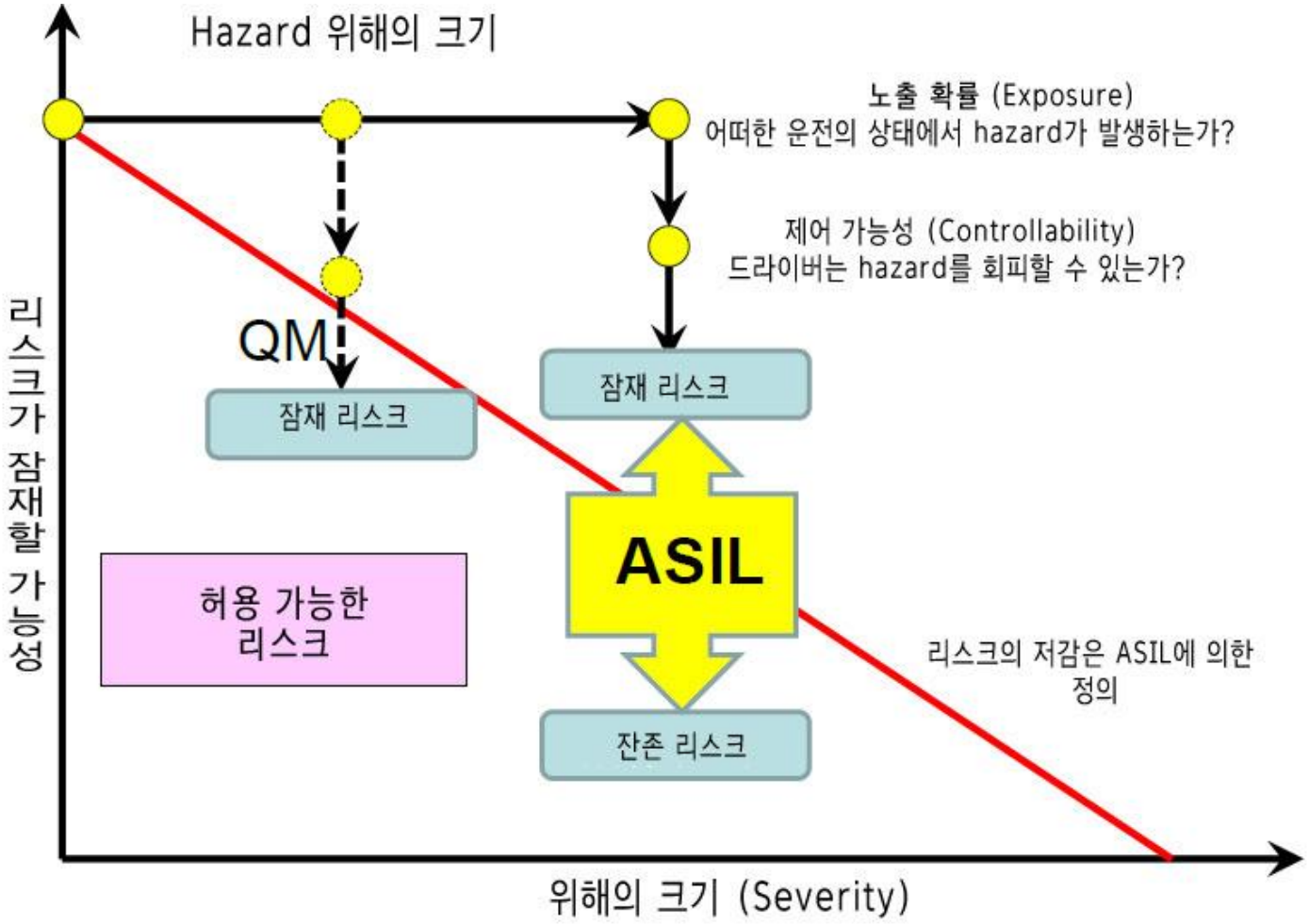
- 개발한 시스템이 안전하다는 것을 객관적으로 제 3자에게 설명할 수 있는 것
- 소송에 대비
- 차량 시스템이 갖는 불안전 리스크를 ASIL의 4단계로 표시. 불안전 리스크를 현재화(**顕在**化)시키지 않기 위한 요구를 정의

※ASIL: Automotive Safety Integrity Level

ASIL의 개념

Panasonic
ideas for life

Automotive Safety Integrity Level



기능 안전 규격이 요구하는 것

Panasonic
ideas for life

- 안전 라이프사이클
- 상세한 프로세스 정의
- Confirmation 방책
- 안전 Case
- 상세한 수법, 기법
- 하드웨어 부품 고장의 정량 평가
- 소프트웨어 툴의 적격성 확인
- Component의 적격성 확인

애매한 정의도 많다

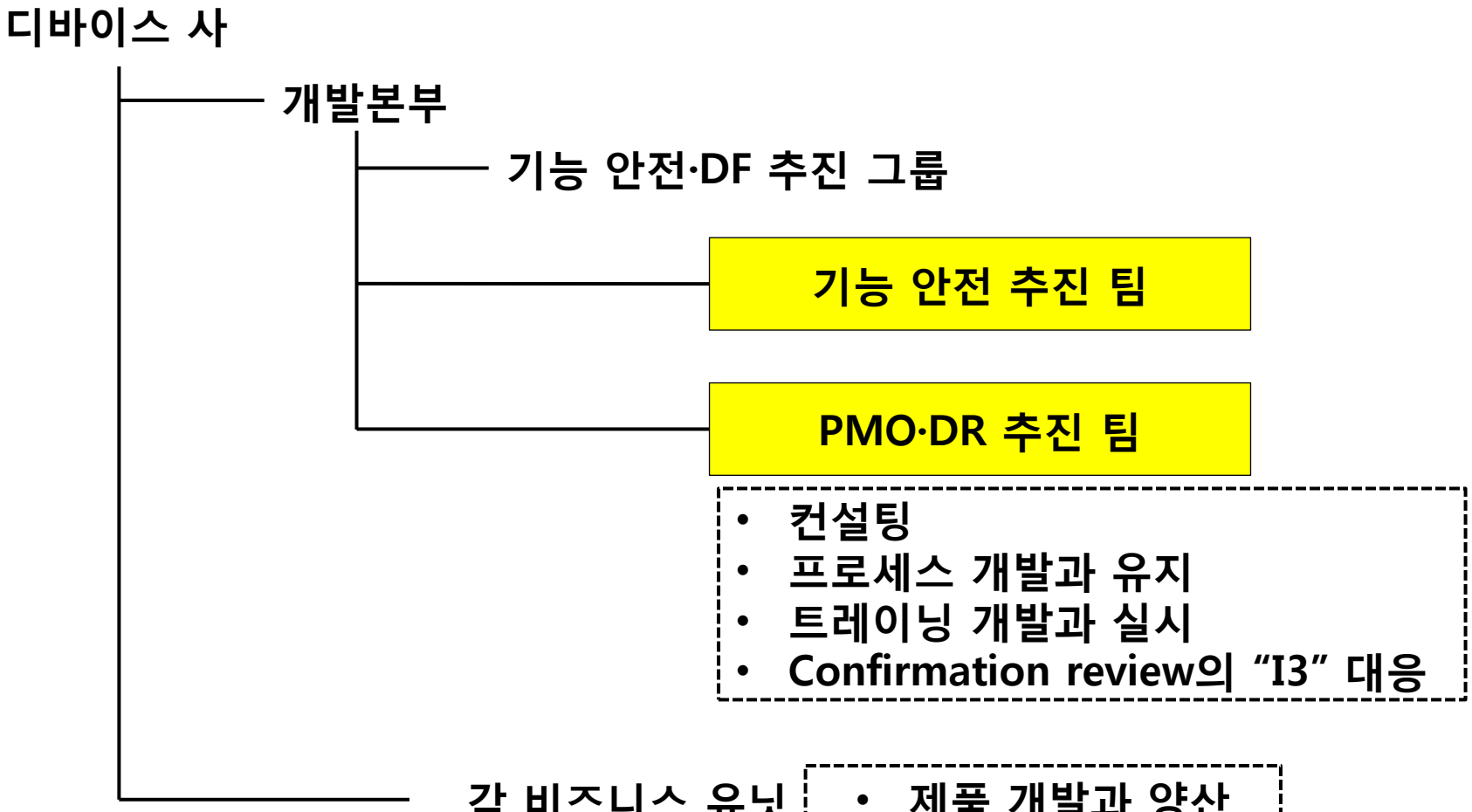
프로세스에 요구되는 것

Panasonic
ideas for life

- 규격이 갖는 추상성과 구체성, 애매성을 어떻게 취급하는가?
- 고객 요구 프로세스의 내장
  - Automotive SPICE와 CMMI
- 비차재, ASIL 비적용의 개발도 고려
- 기존 프로세스를 어떻게 살리는가?
- 종래의 제품 개발의 flow를 바꾸지 않는다
- 종래의 성과물 체계를 크게 바꾸지 않는다

디바이스 사에서의 기능 안전 추진 체제

Panasonic ideas for life



규격의 임팩트를 예감 → 전문 조직 구성

기능 안전 프로세스 개발

Panasonic
ideas for life

- 프로세스 인증 활동
  - Panasonic 전사적 수준의 기능 안전 프로세스 개발
  - 베이스 프로세스는 디바이스 사의 것을 제공 (시스템 제품 개발 관리 규정, 시스템/하드웨어/소프트웨어 개발 기준, 템플릿, 체크리스트)
  - 기능 안전 규격의 번역, 요구 사항의 분석
  - 기능 안전 가이드 라인에 흡수
- 활동 기간
  - 2011/4~2012/3
  - 2012/2/29 인증 취득

사내 멤버를 끌어들여 공통 이해

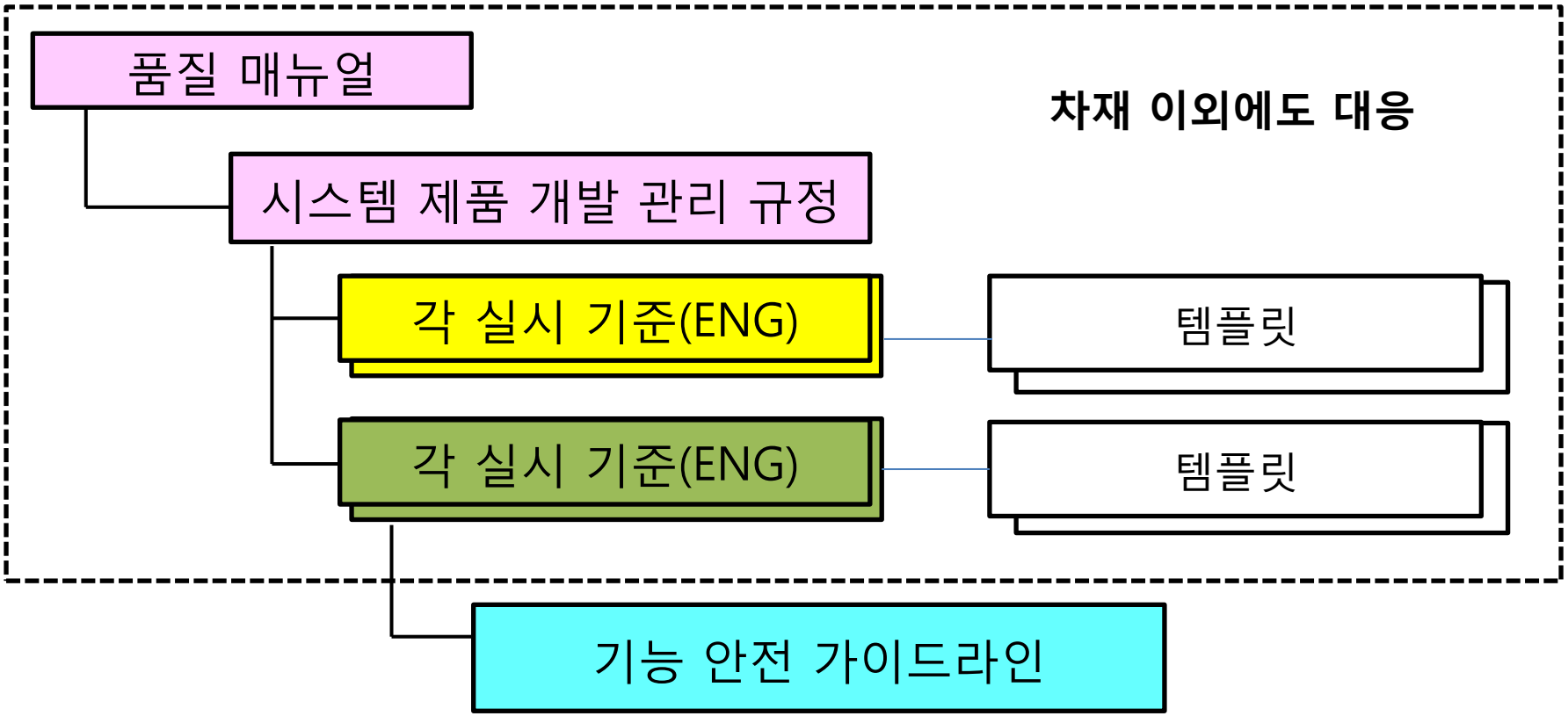
유의해야 할 점

Panasonic
ideas for life

- 안전 라이프사이클
  - 과거부터 구축해 온 Automotive SPICE/CMMI 대응의 소프트웨어 프로세스를 베이스로 확장
  - ASIL 차재, ASIL 비 적용 차재, 비차재에 대응
  - 기능 안전 규격 전용의 구조를 만들지 않는다
  - 하드웨어 개발을 어떻게 끌어들이는가
- 안전을 확인하는 confirmation 방책의 도입
  - 새롭게 도입하지 않고, 지금까지 실시하고 있는 조직 활동에 할당한다.
    → confirmation 리뷰, 기능 안전 감사, 기능 안전 어세스먼트
  - ISO 26262 특유의 내용은 보충한다 (독립성, 리뷰 기법 등)
- 수법의 도입
  - SW는 지금까지의 활동에 비교하여 추가 항목은 적다
- 안전 concept 형성과 이를 위한 분석이 가장 중요
- 하드웨어의 평가 지표
  - 고장률 등은 확인하고 있지만, 정량적인 평가 지표는 새로운 활동이 필요

개발 리소스는 한정되어 있다. 새로운 구조로는 하지 않는다.

4단계의 프로세스 구조

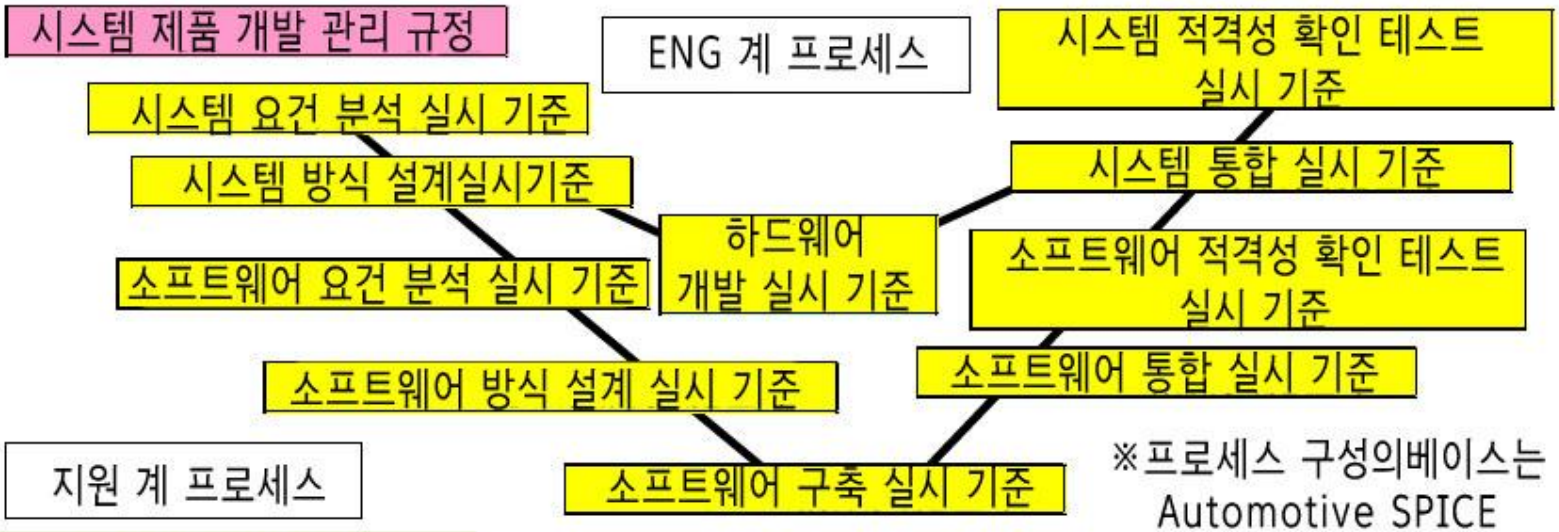


※ 조직 관련의 프로세스(개선, 측정 등)는 각 조직에서 준비

개발은 기능 안전/차재 만으로는 안 된다.

프로세스 구성

Panasonic
ideas for life



※프로세스 구성의베이스는 Automotive SPICE CMMI의 요소도 포함한다

지원 계 프로세스

- 프로젝트 계획 수립 기준
- 프로젝트 관리 기준
- 요구사항 관리 기준
- 구성(형상)관리 기준
- 문제 해결 실시 기준
- 시스템 제품 변경 관리 기준
- 외주 관리 기준
- 시스템 제품 DR 실시 기준
- 시스템제품 품질 감사 실시 기준
- 시스템 제품 AQ 체크 및 제품 심사 실시 기준

기능 안전가이드라인

- 안전 요구사항 정의 가이드라인
- 시스템 설계 가이드라인
- 시스템 테스트 가이드라인
- 소프트웨어 설계 가이드라인
- 소프트웨어 코딩 가이드라인
- 소프트웨어 코드 분석 가이드라인
- 소프트웨어 테스트 가이드라인

- MBD 개발 가이드라인
- 안전분석 가이드라인
- 기능 안전 계획 수립 가이드라인
- 스킬(인원의 적격성 및 자격)인정 가이드라인
- 소프트웨어 툴 인정 가이드라인
- 소프트웨어 컴포넌트 인정 가이드라인
- 하드웨어 설계 가이드라인

종래의 프로세스를 살리다

Panasonic ideas for life

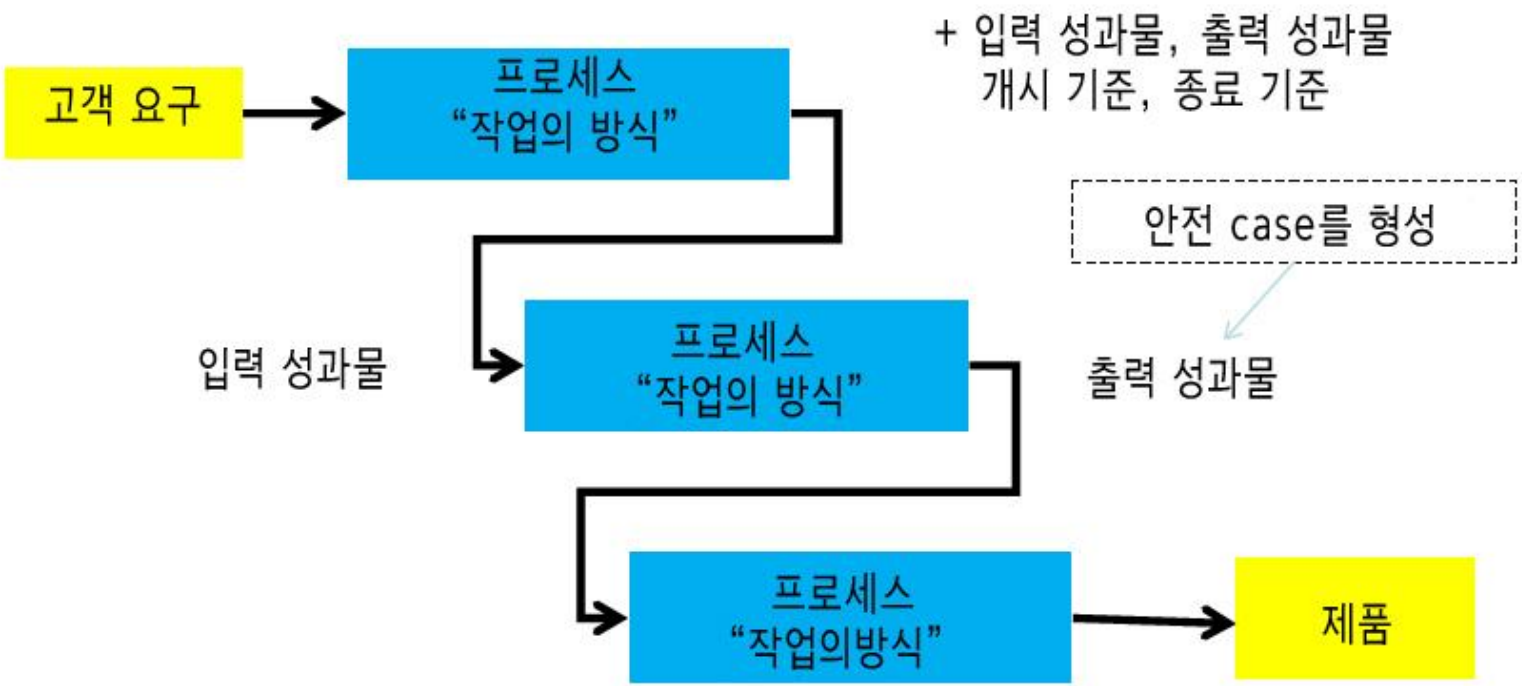
프로세스의 특징

Panasonic
ideas for life

- 종래의 소프트웨어 개발 프로세스에 하드웨어 부분을 강화
  - CMMI와 Automotive SPICE의 내장
- 개발 프로세스와 기능 안전 요구를 분리
  - "개발 프로세스"와 기능 안전 활동을 기재한 "기능 안전 가이드라인"으로 분리
- 제도적 수준의 안전 문화를 형성
  - 품질/안전 경영과 프로젝트 관리, confirmation measure에 의한 확실한 프로세스 준수

ASIL 적용/비적용, 차재·비차재에 대응

프로세스 어프로치



- 프로젝트는, 프로세스를 이용하여 각 프로세스의 출력을 이어서, 입력 성과물(고객 요구)로부터 출력 성과물(제품)을 산출한다.
- 실제 프로세스의 연계는, 프로젝트 계획(반복 계획)에서 상세화.

Traceability의 확립

안전 case

Panasonic
ideas for life

안전 목표
기능 요구

기능안전
concept

사양화

늘었다

기술 안전
concept

시스템
요건 사양서

시스템
아키텍쳐
설계서

소프트웨어
요건 사양서

하드웨어
요건 사양서

소프트웨어
아키텍쳐
설계서

하드웨어 설계서

하드웨어 metric

소프트웨어
상세 설계서

회로도

P판 패턴

소스 코드

부품 명세

각 프로세스의 출력 성과물에서 구성

+ 리뷰 기록
+ Confirmation measure 결과

각 테스트 계획과 결과

- 시스템 적격성 확인 테스트
- 시스템 통합 테스트
- 소프트웨어 적격성 확인 테스트
- 소프트웨어 통합 테스트
- 하드웨어 통합 테스트
- 유닛 테스트
- 하드웨어 기능 block 테스트

프로세스 출력 성과물에서 구성

Confirmation 방책의 활동

Panasonic
ideas for life

Confirmation 리뷰

ISO 267262의 요구가
올바르게 구축되어 있는가?

기능 안전 어세스먼트

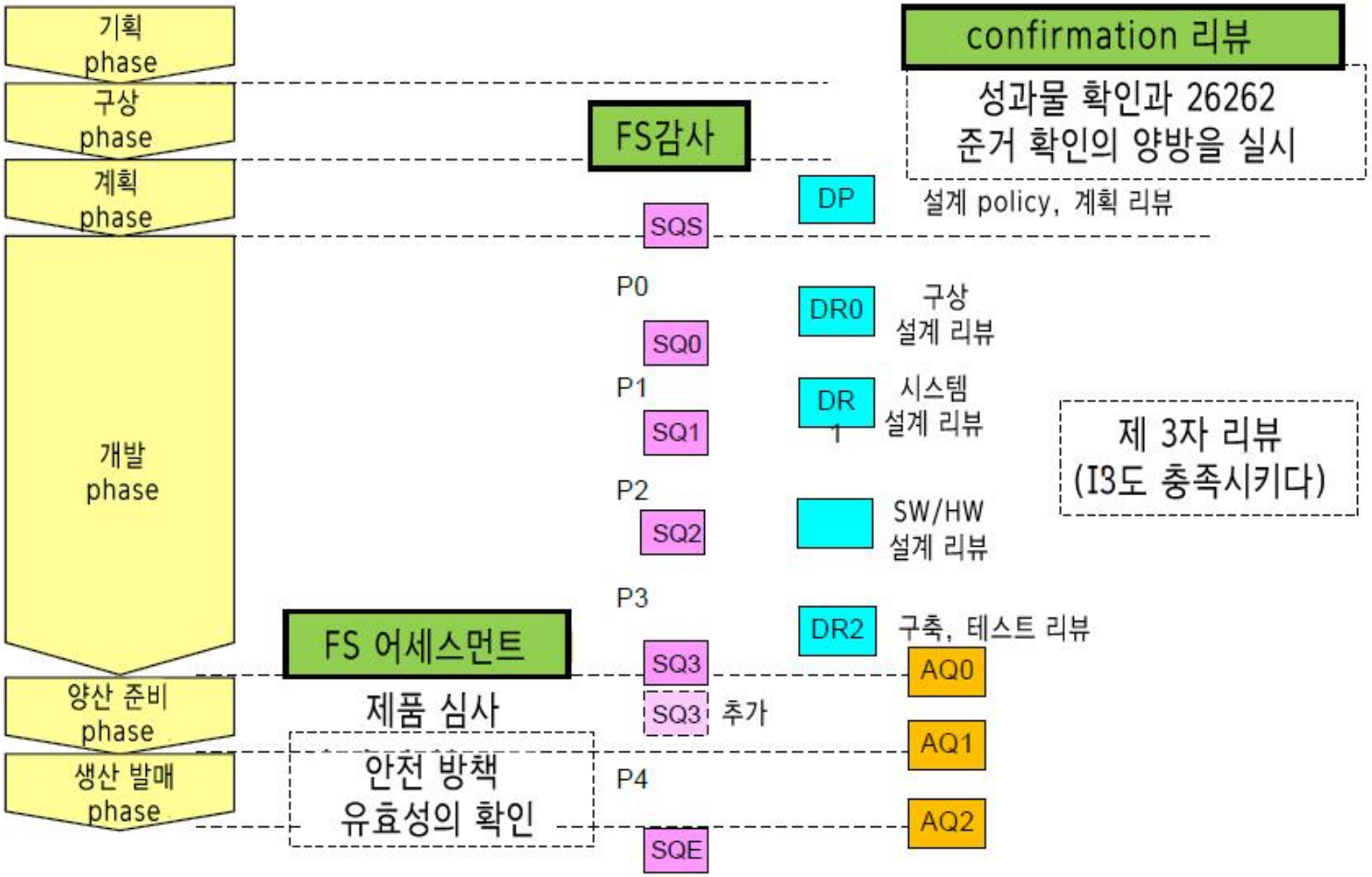
제품은 안전한가?

기능 안전감사

rule은 올바르게 사용되고, 준수되고 있는가?
대상은 소프트, 하드 양쪽모두

기존의 개발 라이프사이클의 이벤트에 할당

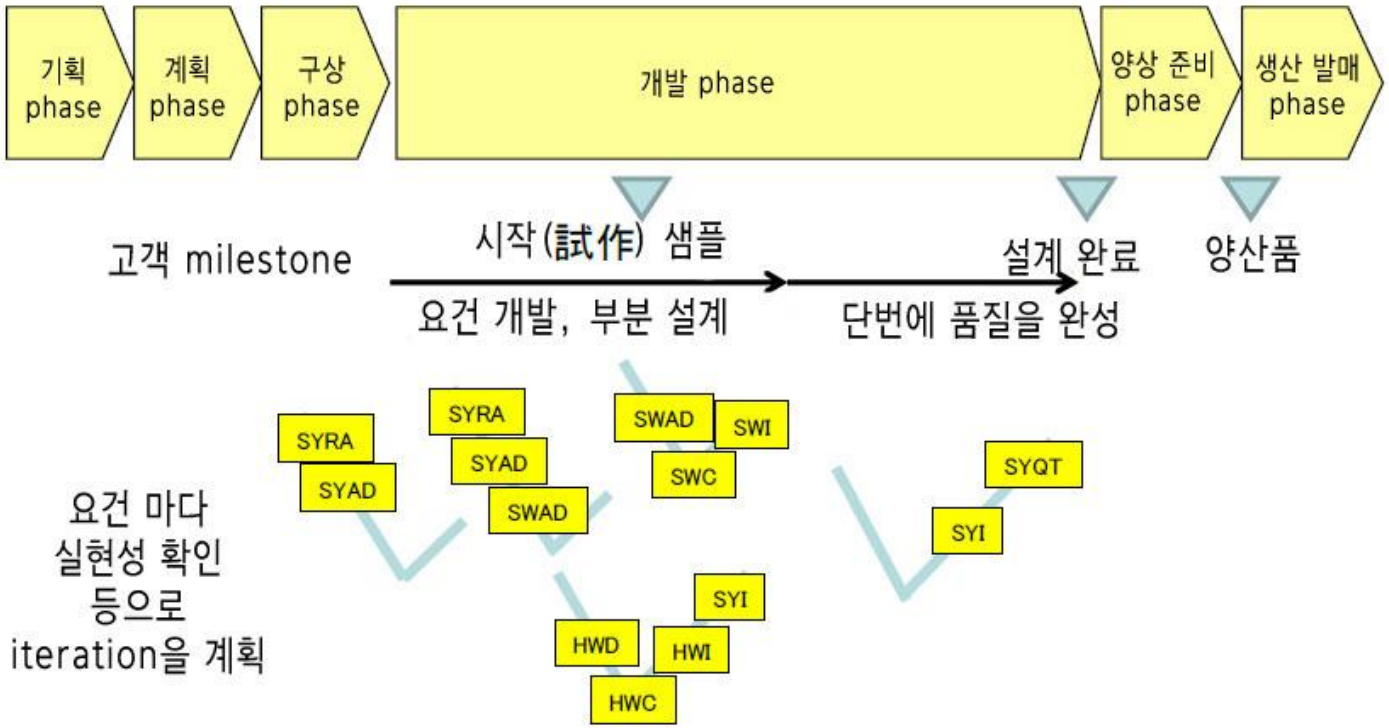
기존의 개발 이벤트에 할당



종래의 이행 승인 gate에 할당한다

반복 계획

Panasonic
ideas for life



"고객 샘플 납품이나 내부 이벤트에 맞춰 실시하는 프로세스" 와
"액티비티를 선택하여 작은 v를 몇번이고 돌리는 프로세스" 어프로치는
현실적인 개발을 실현

종래의 사고방식에 적용

소프트웨어 툴의 적격성 확인

Panasonic
ideas for life

- 조직 레벨에서 사용하는 툴을 통일
  - Use case를 명시하고, 툴의 적격성을 평가
- 적격성 확인 결과는 프로젝트에서 공유

과거에서부터 사용하던 툴로 사내에서 통일

전문 팀에 의한 서포트

Panasonic ideas for life

- 기능 안전 규격을 아는 기술자 육성
  - 기능 안전 규격과 기능 안전 프로세스를 아는 기술자의 육성~ 출장 연수에 의한 전원 교육
- 기능 안전 규격을 사용할 수 있는 전문가 육성
  - 먼저 3명의 전문 팀 멤버가 전문가가 된다.
    · SW, HW의 제품 개발을 경험
  - Panasonic 전사에 기능 안전 WG를 설립.
    · 중심 멤버와의 discussion에 의한 절차탁마!
  - Pilot의 실제 프로젝트에서 먼저, 기능 안전 활동의 형식을 만든다.
  - OJT를 통해 전문가를 만들어 간다.
  - ASIL 적용 프로젝트가 늘기 전에 빠르게 대응한다.

노하우를 회사 전체에 전파하는 것이 중요

기능 안전 스킬 향상

Panasonic ideas for life

- 기능 안전 트레이닝
  - 적격성 인정 가이드라인에 필요 스킬을 명시
  - 차재용 기능 안전 제품 개발 코스 (1일)
    · 규격의 교육과 연습 (안전 concept와 하드웨어의 매트릭스 산출)
  - 시스템 제품 개발 프로세스 코스 (0.5일)
    · 기능 안전 대응 프로세스 교육
  - 전(全) 차재 개발 담당자의 교육을 목표로 한다 (2012/4 개강)
- 기능 안전 엔지니어링 스킬 정의
  - 기능 안전 concept 정의를 위한 컨설팅

안전문화형성

※ 디바이스 사의 기술 강좌

전문 팀 (기능 안전 추진 팀)에 의한 대응

사내 연수를 통해 全 개발자 교육 / 컨설팅으로 개별 육성

컨설팅에 의해 가능한 것

Panasonic ideas for life

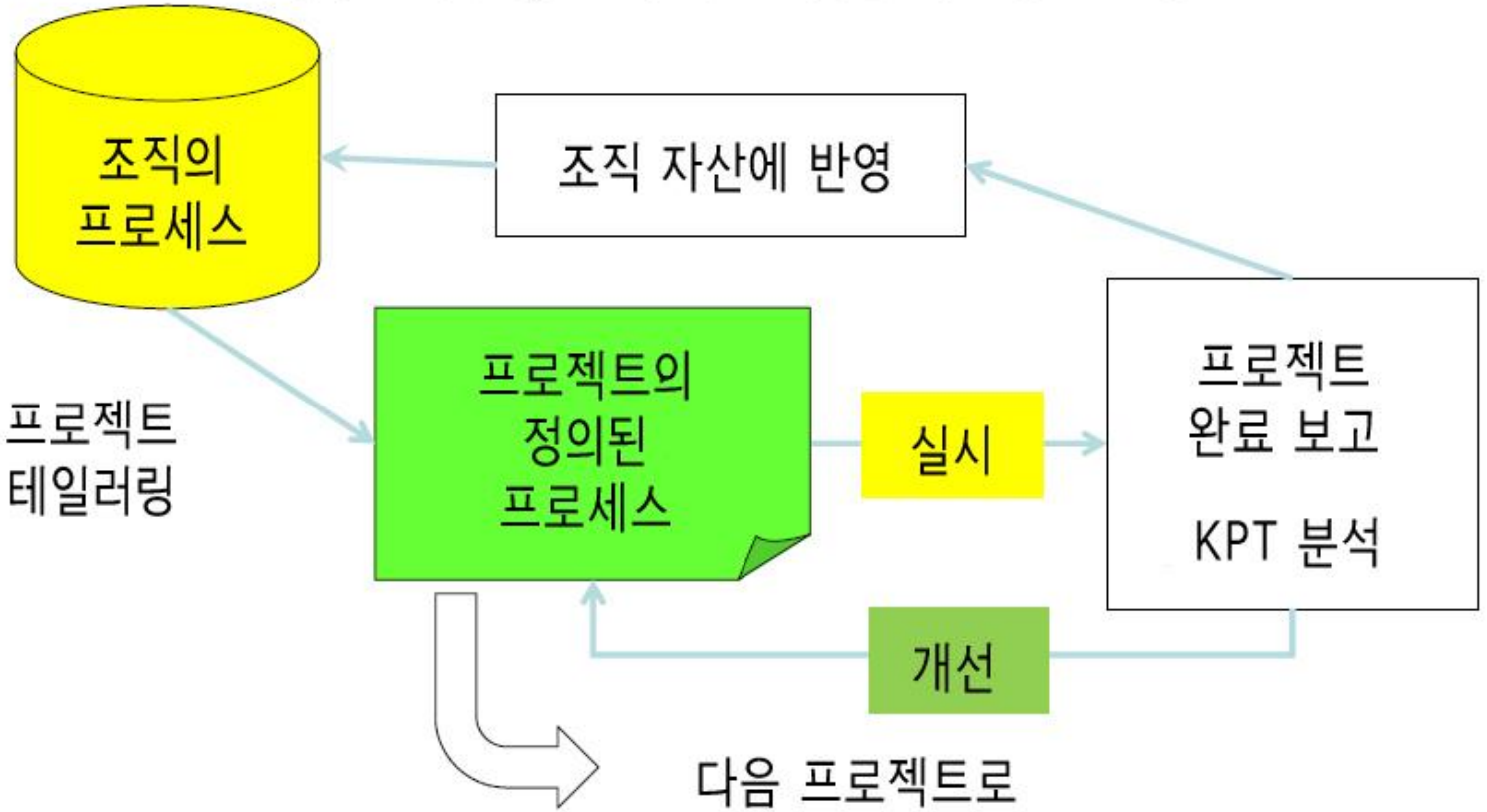
- 기능 안전 활동의 형태
  - 안전 분석과 기술 안전 concept 형성
  - 고장률 계산
  - 안전 프로세스의 실시
  - Confirmation measure의 실시
  - 소프트웨어 툴의 적격성 확인
- 고생하고 있는 점
  - 하드웨어 기술자의 내재화가 어려움(특히 Part4, Part5)
    . 안전 방책은 종래의 fail-safe인 정도 만족
    . 그것을, 제 3자에게 아는 형태로 쓰게 하는 것에 난항
  - 안전 관련, 비안전 관련 요소의 명확한 분리
  - 인터뷰에 의한, 주기능과 안전 메커니즘의 분리
  - 안전 분석 결과를 연관 지은 기술 안전 concept 형성
    . IEC 62380 바탕의 고장률 설계와 DC의 argument
  - 소프트웨어 기술자의 내재화는 smooth
    . Part6, Part8 (일부를 제외한)은 Automotive SPICE의 요구에 가깝다.

- **전문 팀 멤버도 현장과 함께 배우고, 기능 안전 활동의 형태를 확립하고, 회사 전체에 전파**
- **Panasonic 사내의 다른 사례를 담당하고 있는 멤버와 정보 교환과 공통 해석**

개선 활동에 의한 효율화를 목표로 한다

Panasonic ideas for life

자율 개선, 계속 개선의 중요성



목표로 하는 형태는 이 것. 스스로 생각하는, 효율화

본 내용은 일본 [SPI Japan 2012]에서 발표된 공개 자료를 ㈜카이젠컨설팅이
번역한 내용으로, 내용의 개편 및 수정이 불가합니다.