2018 에스피아이디 컨퍼런스

# Automotive 산업의 효율적인 ALM시스템 구축 방안

2018. 09. 13

spid

SIEMENS

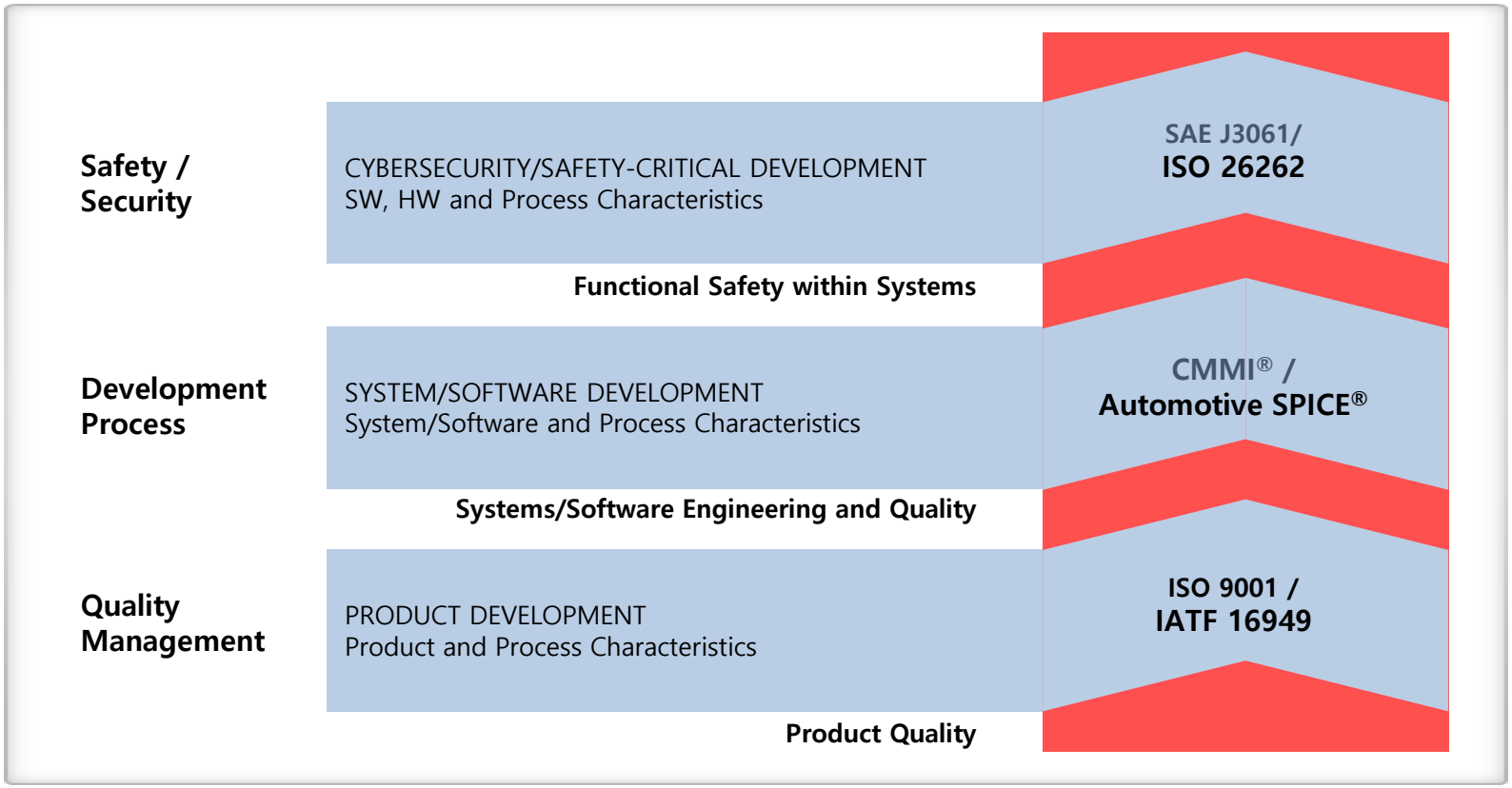
CMMI Institute Partner

# Contents

# Ⅰ. Global Automotive 품질 기준

# Global Automotive 표준 심화

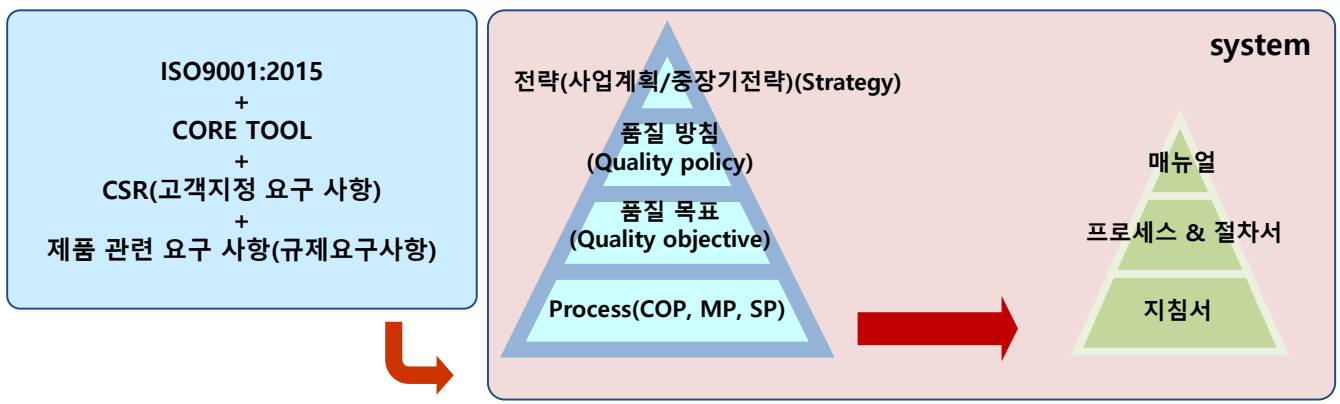
자동차 산업에서의 OEM이 요구하는 Supplier의 개발 품질 표준의 요구는
품질경영시스템 → 개발 프로세스 역량/성숙도 → 기능안전으로 심화 되고 있음.



## ISO와 IATF가 작성한 기술 규격으로 자동차 관련 품질 시스템 요구사항 규정한 것

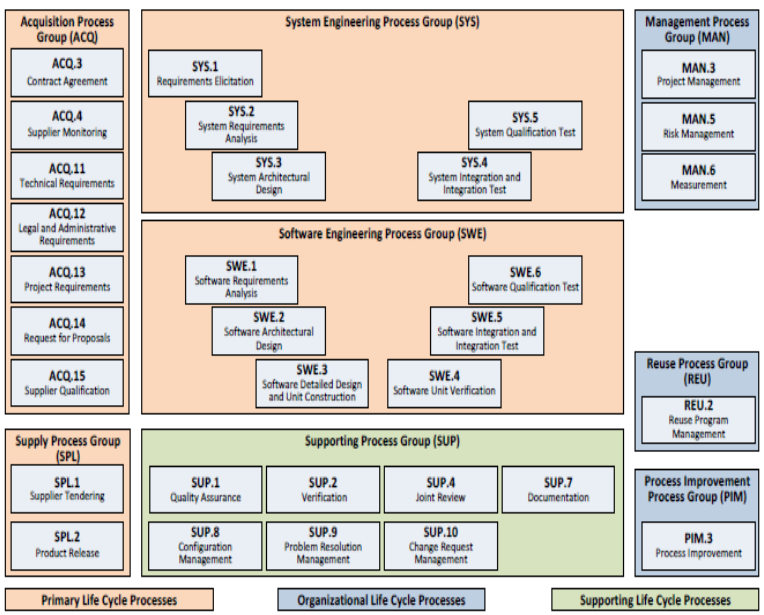
- **Automotive 9 OEM 주도로 품질 경영 시스템**
  - 미국 Big 3 OEM(다임러 크라이슬러, GM, 포드)
  - 유럽 자동차 OEM(BMW, 푸조-시애트론, 피아트, 폭스바겐, 르노) 등
- **기존의 VDA6.1, AVSQ 와 같은 인증을 통합 가능**
- **범위 : 자동차 생산과 조립, 설치, 서비스 및 소프트웨어 내장 제품에 대해 적용**
  **(production, assembly, installation, services, product with embedded SW)**

« 품질경영시스템 전반에 대한 요구사항이다 보니, 개발 프로세스에 대한 요구사항이 포괄적/추상적 »



# 유럽을 중심으로 한 OEM들이 공급업체의 System/Software 개발 역량을 평가하기 위해 만듦

## A-SPICE 프로세스 참조 모델 VDA QMC




출처 : Automotive SPICE® Process Assessment Model Version 3.0 : 2015)

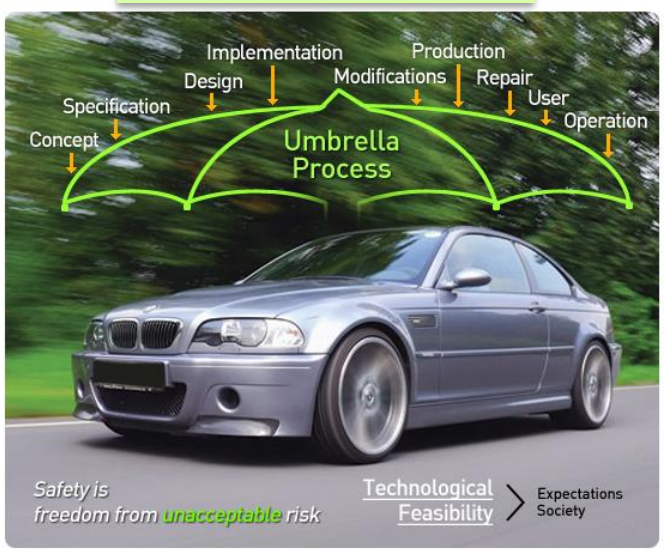
- **Automotive Domain에 특화된** 프로세스 (HIS에서 출발→現 VDA 이관)
- **A-SPICE의 목적은**
  - OEM이 공급자를 선정하기 위한 평가, 기준
  - System, SW 프로세스에 대한 개선 및 능력에 대한 결정
- **수행 작업과 작업 결과물이 구체적으로 정의**
- **프로세스 성숙도는 평가 모델을 통해 Certificate**

- HIS : Hersteller Initiative Software ( 2017년 VDA로 흡수 )
- VDA : 독일 자동차 공업 연합회

기능 안전성 관리, 구상 단계(개념설계), 제품 개발(System 레벨, Hardware 레벨, Software 레벨), 생산 및 운영, 지원 프로세스 등 총 10개 파트로 구성, 총 43개의 요구사항 및 권고사항 가이드.

*자동차 전체 시스템이 적용대상이며 개발 초기부터 생산, 폐기까지 전체 생명주기에서 안전 관련 요구사항 포함*

**ISO26262 10 Part Process**




- ISO 26262의 차량 안전성 보전 등급인 ASIL은 자동차 제품 특성 반영 한것. / 위험도에 따라 A~D단계분류.

**재난 요인별 심각도 분석**

TABLE 1. 잠재적 재난이나 위험에 대한 심각도 등급

| 등급 (Class) | S0 | S1 | S2 | S3 |
|---|---|---|---|---|
| 설명 | No injuries | Light and moderate injuries | Severe and life-threatening injuries (survival probable) | Life-threatening injuries (survival uncertain), fatal injuries |

**재난 요인별 노출 가능성 분석**

위험 및 재난의 노출 가능성 등급

| 등급 (Class) | E0 | E1 | E2 | E3 | E4 |
|---|---|---|---|---|---|
| 설명 | Incredible | Very low probability | Low probability | Medium probability | High probability |

**재난 요인별 통제 가능성 분석**

재난 통제 가능성 등급

| 등급 (Class) | C0 | C1 | C2 | C3 |
|---|---|---|---|---|
| 설명 | Controllable in general | Simply controllable | Normally controllable | Difficult to control to uncontrollable |

**ASIL 정의**

| ASIL Definition | C1 | C2 | C3 |
|---|---|---|---|
| S1 | E1 | QM | QM | QM |
| | E2 | QM | QM | QM |
| | E3 | QM | QM | A |
| | E4 | QM | A | B |
| S2 | E1 | QM | QM | QM |
| | E2 | QM | QM | A |
| | E3 | QM | A | B |
| | E4 | A | B | C |
| S3 | E1 | QM | QM | A |
| | E2 | QM | A | B |
| | E3 | A | B | C |
| | E4 | B | C | D |

QM(Quality Management) : 기능안전과 무관

High

ASIL A: 기능안전등급 A
ASIL B: 기능안전등급 B
ASIL C: 기능안전등급 C
ASIL D: 기능안전등급 D

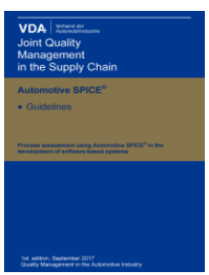
*기능안전은 반드시 A-SPICE 의활동을 모두 요구하고 그 위에서 기능안전 활동을 추가적으로 요구 함.*

# Ⅱ. Automotive SPICE 주요 요건

## Automotive SPICE Guidelines_1st Edition 2017 발표

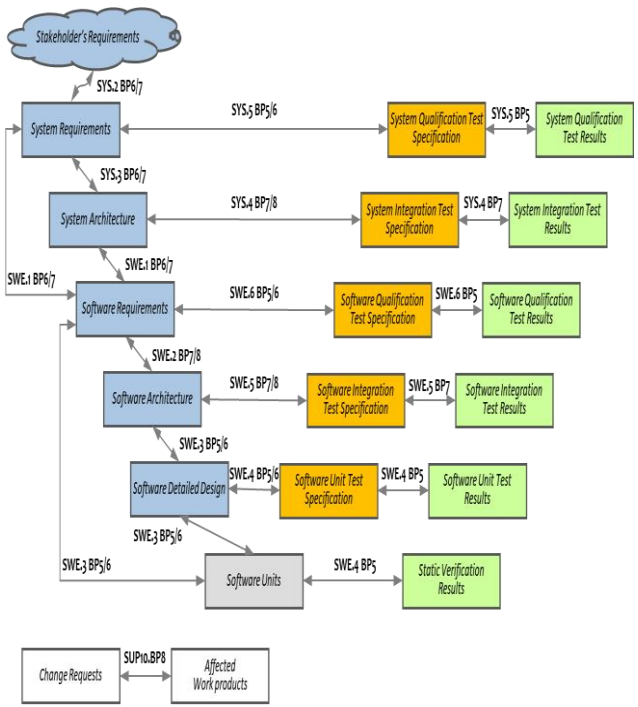
*목적: 자동차 산업 모델의 해석과 적용을 지원하고 평가 결과의 비교 하는 Rule, 지침서, 권장 사항 제공*

- **VDA (Verband der Automobilindustrie) :**
  - German Association of the Automotive Industry
  - 1901년 1월 독일에서 창립
- **Join Quality Management in the Supply Chain**
- **Quality Management in the Automotive Industry**




- 왜? 가이드 라인이 필요한가?
  - **To reduce the diverging assessment results**
- Rules and Recommendations
  - **287 Rules and 197 Recommendations**
  - **333 Contents related rules and recommendation and 151 Dependencies**

## Traceability and Consistency in Automotive SPICE




- 고객의 요구사항부터 개발 요구사항, 개발 설계, 테스트 케이스, 테스트 결과까지 양방향 의존성이 분석되고 추적되어야 함

  (20개 산출물의 상호 추적성을 요구 )

- 양방향 추적은 "완전성"을 확보해야 함.
  ( 누락없이 상위 요소와 하위 요소는 Mapping 되어야 함 )
- 추적되는 컴포넌트는 'Single' 단위로 추적되어야 한다.
  (Single test case는 Single SW 요구사항과 대응되어 추적되어야 함)
- 추적되는 모든 산출물들의 내용은 서로 모순되지 않고 서로 일치해야 한다.

  ( 검토 활동을 통한 일관성 확인 증거 요구 )
- 추적성은 자동화를 통해 이루어지는 것이 가장 바람직하다.

  만약, 수동(엑셀 등)방식으로 추적하는 경우 복잡한 추적 관계를 완전하게 커버 했다는 것을 증명할 수 있어야 한다.

## Ensure Change Management

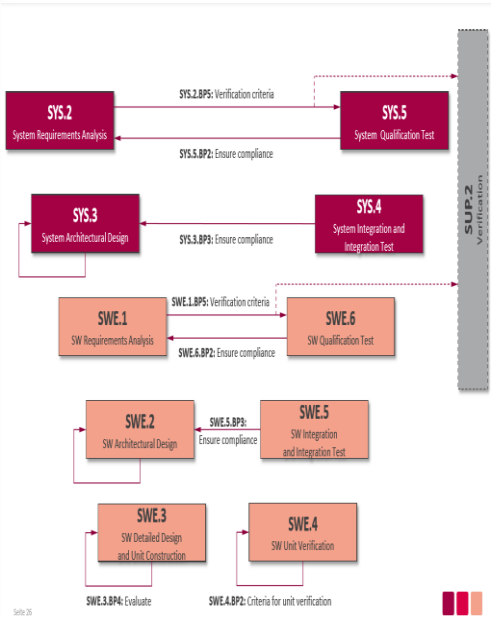
- 모든 변경 사항이 추적되어야 한다. 즉, 변경 요청부터 변경 완료까지 변경 상태가 단계별로 추적되어야 한다.
- 변경으로 인해 영향 받는 범위, 심각도 등을 CCB를 통해 변경 의사 결정이 수행되어야 한다.
- 모든 변경은 이해 관계자의 기술적 측면, 부작용 가능성의 의견이 의사소통 되어야 한다.
- 변경에 대한 타당성, 위험성, 복잡성 및 영향 등으로 체계적으로 평가되고 문서화 되어야 한다.
- 변경 결과는 모든 관련 산출물이 확인 되어야 한다. ( 퇴행 테스트 결과, 변경된 부분에 대한 테스트 결과, 수정된 작업 산출물의 검토 결과 등)
- 변경 관리는 자동화를 통해 이루어지는 것이 가장 바람직하다. 만약, 수동 방식으로 수행하는 경우 모든 변경 상태 별로 관련된 산출물들이 추적된다는 것을 증명할 수 있어야 한다.

## Plausibility checks of work product

- 모든 개발 산출물들의 최종 변경 일자의 적시성과 변경 이력의 적합성을 점검 (20개 산출물의 상호 추적성을 요구 )
- 점검 직전에 산출물이 생성된 경우 늦게 문서화 된 타당한 이유가 없는 한 점검 대상에서 제외시킨다.
  ( 즉, 산출물이 적시에 기록되고 변경되지 않았다면, 산출물을 인정하지 않는다는 것 )
- 산출물들은 최종본만 존재하면 안되고, 최초 생성부터 진화해 나가는 중간 과정의 검토 본, 승인본을 거쳐 최종 본까지 모두 존재 해야 인정된다.

# Automotive SPICE 주요 요건 > SW 검증

## SW Verification 활동에 대한 요건 강화 (개발 문서 Review, 정적 분석, 동적 검증, 코드 리뷰 등)




- 최소 요구사항 명세, 아키텍처 설계, 상세 설계에 대해서 관련 이해관계자의 "동의"를 요구 (System, HW, SW)
  → 작업 산출물이 "Review" 되어야 함.
- Written feedback from customer (고객의 서면 피드백 )
- 관련 이해관계자들이 동의하는 평가를 했다는 독립적인 진술 (회의록, 검토 체크리스트, 검토 결과서 등)이 존재
- 소프트웨어 단위 검증은 "정적 검증", "동적 검증", "코드 리뷰" 3가지를 요구
- 소스 코드에 대한 "정적 검증 " 수행 로그가 없는 경우 Software unit verification을 완전하게 수행했다고 인정하지 않음
- 소스 코드에 대한 개발자(선임개발자들에 의한)의 "코드 리뷰 " 수행을 요구 ( 정적 검증으로 발견할 수 없는 비즈니스 로직 에러)
- "동적 검증"에서는 "VDA Code Metrics"에서 정의된 커버리지 요구
- 테스트 자동화(CI체계 및 정적검증 툴)를 통해 수행하는 것을 권장 함.
- 모든 테스트 단계에서 "퇴행 테스트(Regression test)"에 대한 전략을 요구
  → "퇴행 테스트"가 수행되지 않은 경우 테스트에서 식별된 결함들의 시정조치 확인을 보장할 수 없다고 판단

## Ensure Quality Analysis

- 품질 보증 활동이 해당 프로젝트 이해관계와 상충되는 경우 ( 비용적, 인사권 등)는 독립성을 보장한다고 볼 수 없다.
- 품질 보증 활동 인원이 해당 프로젝트의 품질을 보증 할 수 있는 역량, 가용 Effort 가 부족하다면 품질 보증 활동이 제대로 이루어졌다고 볼 수 없다.
- 해당 프로젝트에 납품하는 협력업체에 대한 품질 보증 활동이 반드시 수행되어야 한다.
- 단순히 작업 산출물의 존재 여부만 확인하는 품질 보증 활동은 인정하지 않는다.
- 프로젝트의 품질 목표를 달성할 수 있는 상세한 체크리스트를 활용하여 프로세스와 작업 산출물을 감사(Audit)해야 한다.

# Ⅲ. Automotive 요구하는 주요요건 대응방안

# 도구를 활용하여 Human Error 최소화

## Automotive 인증의 특징 때문

- 모든 개발 산출물은 요구사항, 설계, 코드, 테스트 설계, 테스트 수행, 테스트 결과가 빠짐없이 추적되어야 함
- 모든 형상관리는 적시에 변경되고 변경 내역이 모두 추적되어야 함
- 모든 문제(결함, 이슈, 부적합사항)들은 모든 변경요청과 형상 변경과 일관성을 유지해야 하며, 문제는 등록부터 해결될 때까지 그 상태가 추적되어야 함
- 이러한 모든 추적,일관성이 확보되지 않고, 누락되면 달성이 불가능

**신규 제품 개발**

- 새로운 요구사항
- 유사한 제품 요구사항

개발 중에 변경되는 요구사항 많아짐

**영향도 분석 (영향받는 문서,형상 파악 )**

ISO26262 , A-SPICE에서 요구하는 Single 단위로 영향 받는 것을 파악해서 반영하는 것은 사람에 의해서는 **Human Error를 방지할 수 없다.**

**파생 제품 개발**

- 기존 요구사항
- 추가 기능 요구사항
- 변경 기능 요구사항

영향도 분석 (영향 받는 문서,형상 파악 )

- 기존 설계서, 테스트 케이스
- 추가된 설계, 테스트 케이스
- 변경된 설계, 테스트 케이스

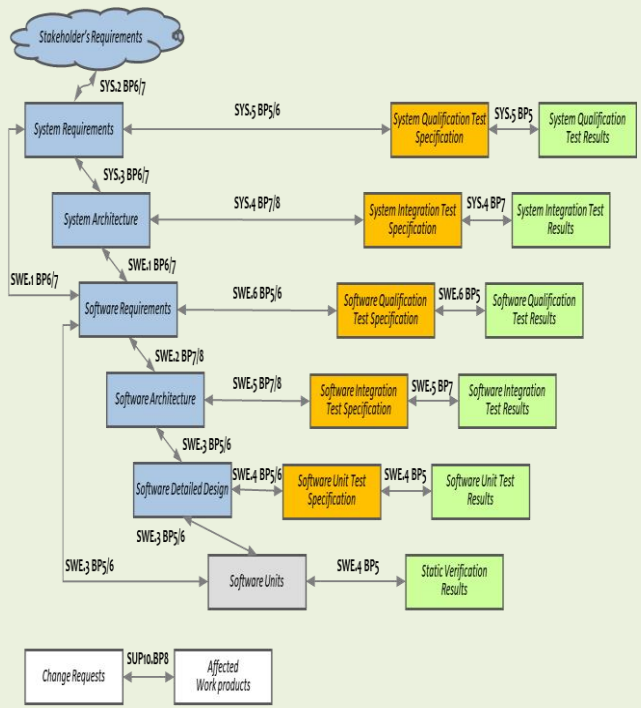
# Application LifeCycle Management

ALM 도구의 요구사항, 형상관리, 테스트관리, 자원관리, 추적성 등의 기능을 활용하여 Automotive 요구하는 요건에 적합하게 사용 및 구축 운영 가능.

# Automotive 요건 > Traceability and Consistency

고객의 요구사항부터 개발 요구사항, 개발 설계, 테스트 케이스, 테스트 결과까지 양방향 의존성이 분석되고 추적되어야 한다.

## Traceability and Consistency 요건




## ALM 도구 활용


1. 요구사항 관리 요구사항관리.avi
2. 개발설계 관리 개발설계.avi
3. 테스트케이스 관리Test관리.avi
4. 양방향 추적가능(Mapping)
5. 추적되는 모든 산출물 확인 가능
6. 자동 추적 메트릭스 Report
   추적_메트릭스.avi

# Automotive 요건 > Change Management

모든 변경 사항이 추적되어야 한다.

## Change Management 요건

1.변경 요청부터 변경 완료까지
변경 상태가 단계별로 추적되어야 함.
2.변경으로 인해 영향 받는 범위, 심각도 등
분석, 확인 되어야함.
3. 모든 관련 산출물이 확인 되어야 함.
4. 변경관리 자동화 되어야 함.

## ALM 도구 활용


1. 형상 관리 – SVN
2. 변경 관리- WorkFlow 정의
3. 변경 상태별 분석 Report
4. 변경에 따른 영향도 분석

변경관리_영향도분석.avi

# Automotive 요건 > Plausibility Checks

모든 작업 산출물의 타당성 검사가 되어야 한다.

## 타당성 검사 요건

1. 개발 산출물들의 최종변경일자의 적시성/ 변경 이력의 적합성 점검.
2. 20개의 산출물의 상호 추적성.
3. 산출물들은 버전, 이력관리 되어야함.

## ALM 도구 활용


1. 산출물 형상관리
2. 산출물이력관리
3. 산출물 간의 추적 메트릭스

[산출물이력_추적메트릭스.avi]

# Automotive 요건 > Software 검증

SW Verification 활동에 대한 요구 강화 (개발 문서 Review, 정적 분석, 동적 검증, 코드 리뷰 등)

## SW 검증 요건

1. 작업 산출물 Review 되어야 함.
2. 회의록, 검토 결과서 등 존재
3. 소프트웨어 단위 검증 3가지 요구

   "정적 검증", "동적 검증", "코드 리뷰"
4. 소스 코드에 대한 개발자의 "코드 리뷰 " 수행 요구

.

## ALM 도구 활용


1. Review 관리
2. 결과물 산출물 생성

   Review관리.avi
3. 테스트도구 와 연동하여

   테스트결과 및 상태 확인

   Test관리.avi

Ensure Independence and objectivity QA

## Quality Analysis 요건

1. 프로젝트 이해 당사자 독립성 보장
2. 프로젝트별 인력 R&R 관리
3. 프로젝트별 작업(일정) 관리
4. 프로젝트별 진척율 관리

## ALM 도구 활용


1. 프로젝트별 인력 관리
2. 프로젝트별 권한관리
3. 프로젝트 진척율관리
4. 개인별 리소스 관리

프로젝트관리.avi

# Summary

- ISO26262 & ASPICE는 기본적인 품질 프로세스로 QM을 요구
  - ✓ TS 16949, ISO 9001, ISO 12207, CMMI L3, A-SPICE Lv1 등 적용
  - ✓ 이를 위해 기본적인 요구사항/형상/변경/이슈/품질 관리가 요구

- ISO26262 & ASPICE의 성공을 위해 ALM 시스템 구축 필요
  - ✓ 통합된 하나의 환경으로 ALM 프로세스 구축
  - ✓ ISO 26262의 8-11에 명시된 신뢰성이 확보된 ALM 솔루션의 도입 필요
  - ✓ 향 후 확장을 위해서 PLM 도구들과의 연동을 고려한 ALM 솔루션 검토

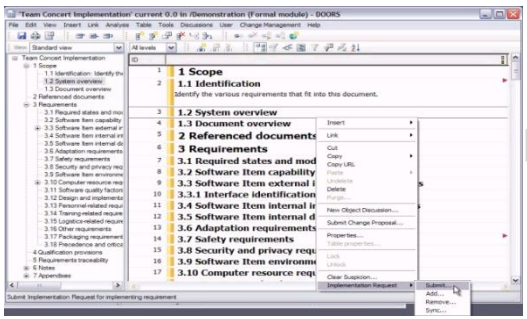
# Siemens Polarion ALM

## 애플리케이션 라이프사이클 관리 기능을 통합하여 협업, 투명성, 추적 기능 향상

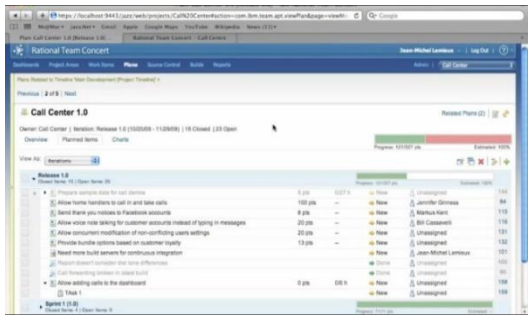
# IBM Collaborative Lifecycle Management(CLM)

Collaborative Lifecycle Management위한 IBM Rational 솔루션은 Application Lifecycle Tool을 결합하여 소프트웨어 제공

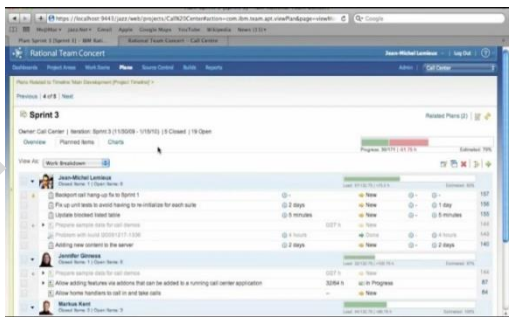
# Planning, Execution & Dashboard



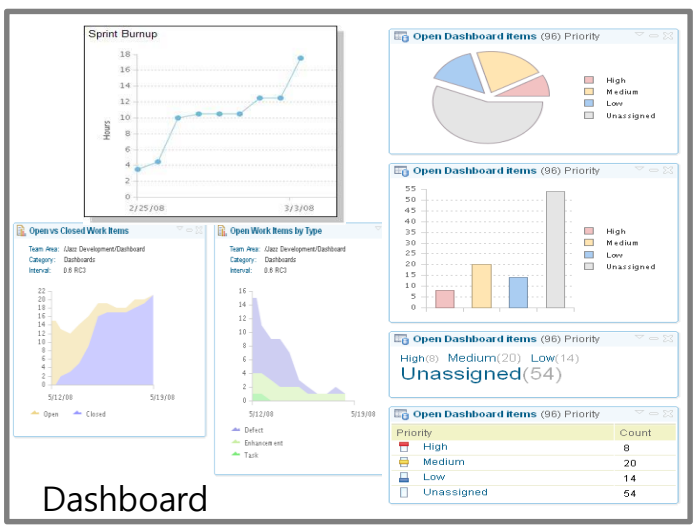
요구사항 등록 (Task)



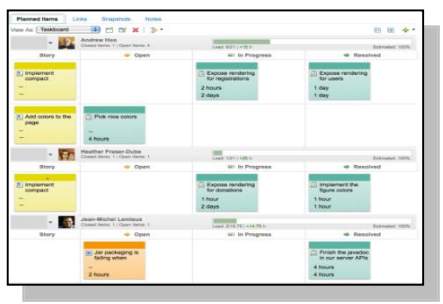
작업항목 릴리즈계획



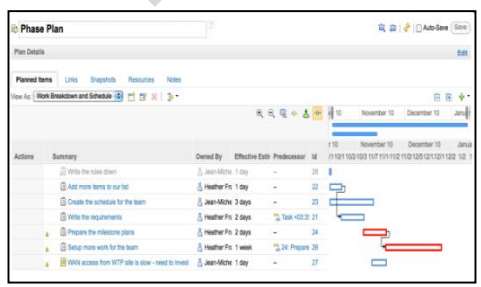
작업항목 반복 계획 실행




Dashboard



Taskboards




Gantt charts

Planning & Execution

# Ⅳ. ISO 26262기반 차량 기능 안전

## ALM 시스템구축 사례

# Case . A사 ISO 26262기반 차량 기능 안전 컨설팅

- **Business Challenges :**
  1. 기능안전 프로세스 개선 및 엔지니어링 컨설팅
  2. Application LifeCycle Management 시스템 구축
- **목적 :**
  1. 기능안전 기반 관리체계 구축 및 엔지니어링 수행 역량 확보
  2. ALM 시스템 구축 및 내재화
- **수행 목표 및 범위 :**

| | | | |
|---|---|---|---|
| 추진 목표 | 기능안전 체계 구축 | | • 기능안전 대응 개발 프로세스 구축, 조직체계 구축, 개발환경 구축<br>• ALM 시스템 구축 및 내제화 |
| | 기능안전 HW 개발 역량 확보 | | • 프로젝트 수행을 통한 기능안전 Part5 개발 활동 역량 확보 |
| 대상 제품 (아이템) | | | • xxxxxxxxxxxxxxxxx |
| 기능안전 표준<br>적용 범위 및 등급 | 적용 표준 | | • 차량 기능안전 표준 (ISO 26262 Road Vehicle - Functional Safety) |
| | 적용 등급 | | • ASIL B |
| | 적용 범위 | 안전 관리 / 분석 | • Part 2. Management of functional safety |
| | | 제품 개발 | • Part 5. Product development at the hardware level (Full set) |
| | | 지원/관리 | • Part 8. Supporting processes (이해 수준) |

# Case . A사 ISO 26262기반 차량 기능 안전 컨설팅

## 기능안전 관리 (ISO 26262 Part 2)

### 기능안전 조직 표준 프로세스 수립

■ 표준 프로세스 구축 내용

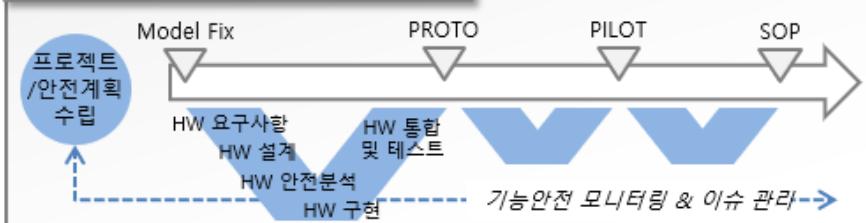
관리 ⇔ HW 개발 프로세스 ⇔ 지원 활동

- 기능안전 계획수립
- 기능안전 모니터링/ 이슈관리

HW 개발 프로세스:
- HW 요구사항 개발
- HW 안전분석
- HW 설계
- HW 아키텍처 평가
- HW 통합 및 테스트

지원 활동:
- 요구사항 추적관리
- 문서/형상 관리
- 변경관리
- SW도구 평가/인정

### 기능안전 프로젝트 관리



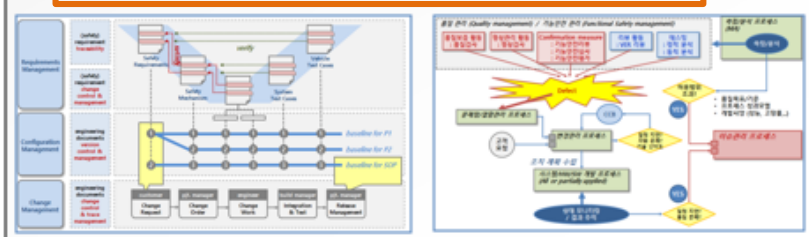

## 기능안전 지원 (ISO 26262 Part 8)

### 기능안전 조직 표준 프로세스 수립

Polarion ALM 적용 범위

■ 프로젝트/기능안전 지원 활동

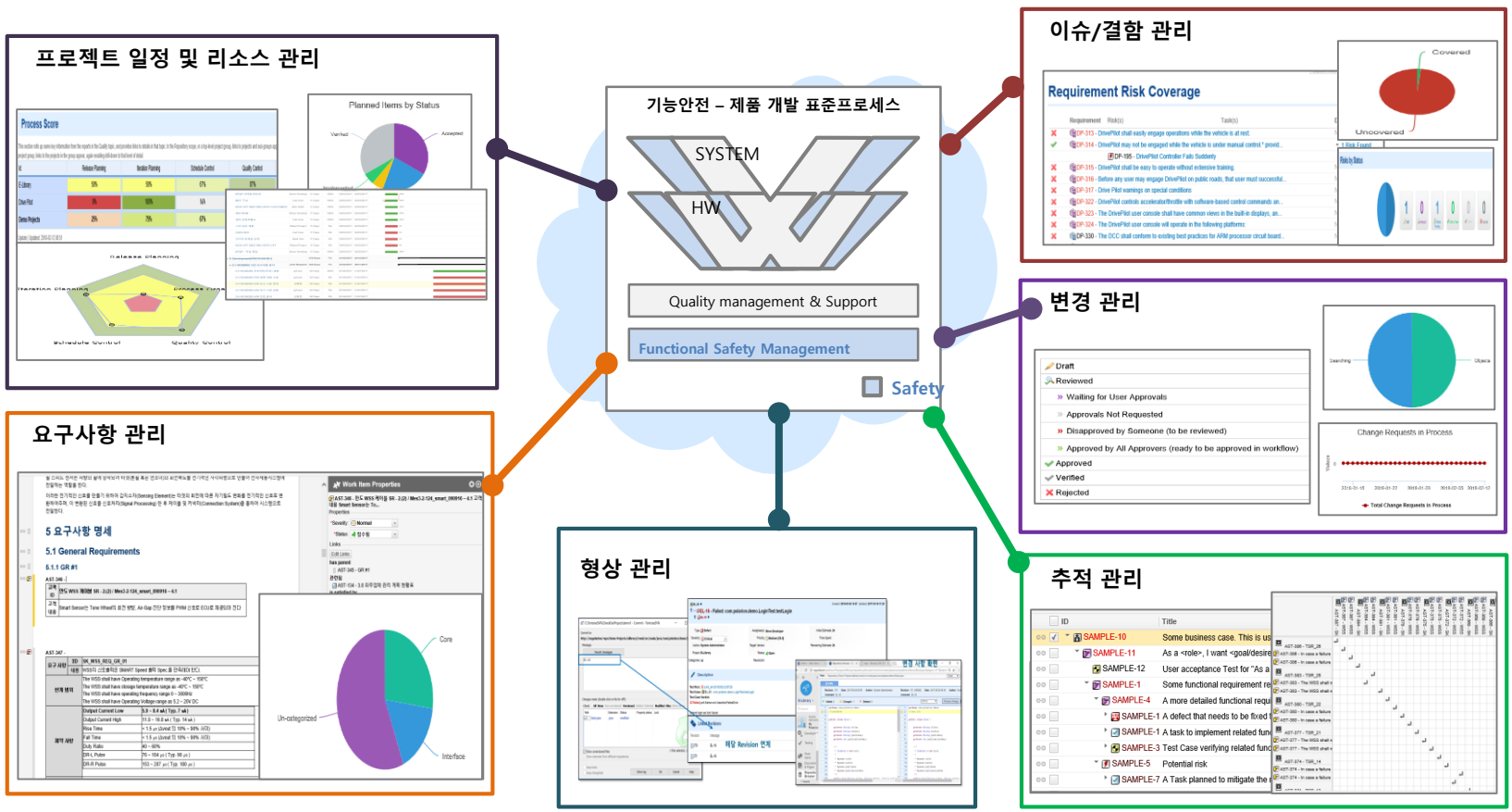
- 요구사항 추적관리
- 문서/형상 관리 및 변경 요청 추적 관리
- 문제점/결함 추적 관리
- 고객 기능안전 리뷰 관리
- SW도구평가 및 인정



Polarion ALM: 프로젝트 산출물 관리

# Case . A사 ISO 26262기반 차량 기능 안전 컨설팅

기능안전 프로세스 기준으로 프로젝트 일정관리 / 요구사항 관리/ 이슈관리/ 형상 변경관리 등
Polarion ALM에 적용하여 ALM 시스템 구축 완료



# Case . A사 ISO 26262기반 차량 기능 안전 컨설팅

## ▪ 솔루션 Result

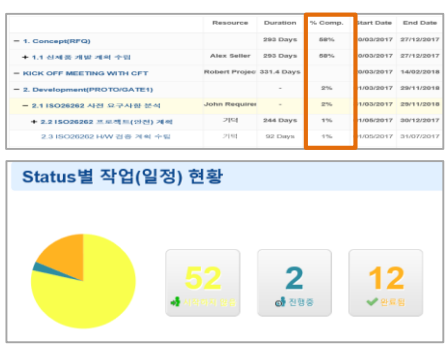
✓ 전문 도구인 Polarion ALM을 활용한 양산 실무 적용을 위한 제품 개발프로세스 체계 확립

✓ 요구사항 부터 테스트까지 추적성 확보 및 Coverage 관리

✓ Customer 심사대응 산출물 확보

### 체계적인 프로세스 관리

1. 제품개발 프로세스 적용한 체계적인 운영관리
2. 시스템을 통한 진행 상태 모니터링

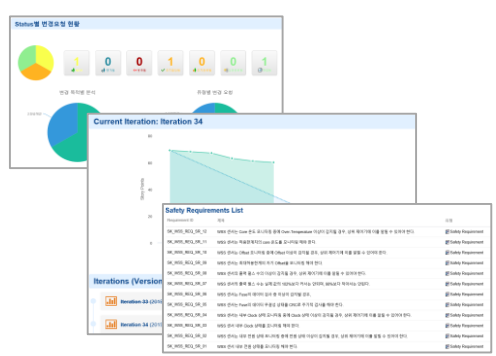



### 추적 관리

1. 다양한 Link정의 및 추적성 확보
2. Work 연관된 Task 분석
3. Open 이슈/결함 연관된 Task관리
4. Task별 추적 데쉬보드 활용
5. 이슈/결함 Coverage 관리
6. 이슈/결함 종료까지 추적관리


### 다양한 분석

1. Status별 분석 현황
2. 작업항목별 List 조회
3. 다양한 분석 지표 / PDF Export




# 질문과 답변

## We have Answers

# 감사합니다.

Thanks for your attention

저희 ㈜에스피아이디는 고객사의 만족을 위해 최선을 다합니다.