Automotive SPICE for Cybersecurity

ISO/SAE 21434 표준을 기반으로 하는 UNECE R155 자동차 사이버보안 법규에 따라 차량 제조사 및 각 부품사들은 차량 개발 라이프사이클 전반에 걸쳐 사이버보안 요건을 정의하고 이를 준수하여 사이버보안 엔지니어링 활동을 수행해야 합니다.

이에 따라 VDA QMC는 Automotive SPICE의 검증된 범위에 사이버 보안 관련 프로세스를 추가하여 사이버보안 엔지니어링을 위한 프로세스 참조 및 평가 모델 (Cybersecurity PAM)을 정의하고 기존 Automotive SPICE Guideline을 보완한 Automotive SPICE for Cybersecurity를 발행하였습니다.

ASPICE for Cybersecurity는 기존 ASPICE PAM 3.1 및 Guideline을 유지하면서 6개의 신규 프로세스를 추가하여 Cybersecurity engineering을 강화하였습니다.

Content of ASPICE for Cybersecurity

- **Part I: Process Reference and Assessment Model for Cybersecurity Engineering**

  → *사이버 보안 관련 개발 프로세스를 평가할 수 있도록 Automotive SPICE PAM 3.1을 보완함*

  → *이를 사용하여 평가를 수행하기 위한 전제조건으로 기존 VDA 범위에 대한 평가 결과가 존재하거나, 기존 ASPICE PAM과 Cybersecurity PAM을 둘 다 사용하여 VDA 범위에 대한 평가를 수행해야 함*

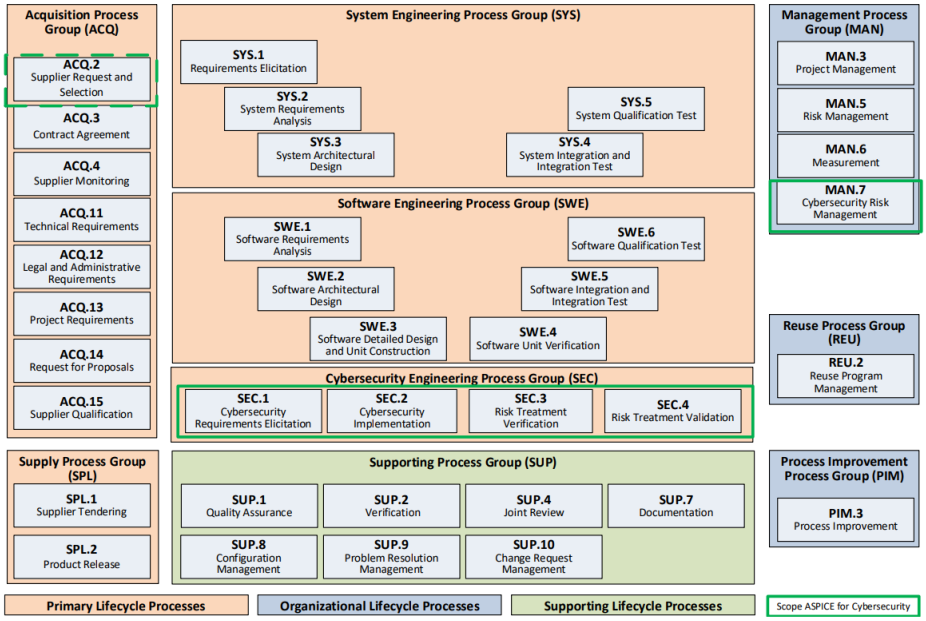
- **Part II: Rating Guidelines on Process Performance(Level1) for Cybersecurity Engineering**

  → *Part 1에 정의된 프로세스에 대한 해석 및 평가 지침이 포함하여 Automotive SPICE Guideline 1st ed.을 보완함*

  → *기존 ASPICE Guideline의 chapter.1 과 2*는 Part II에 그대로 적용됨*

** Chapter 1. Application of interpretation and rating guidelines, Chapter 2. Key concepts and overall guidelines*

ASPICE for Cybersecurity Process reference model – Overview



MAN.7
- CS 위험 관리(식별, 분석, 평가 및 처리) 활동을 다룸
- 위험 처리 옵션에 따른 모니터링 및 시정조치 정의
- ISO/SAE 21434 15장, 9.3장을 커버함

ACQ.2
- ASPICE ACQ.3, 14, 15에서 CS 관련 측면을 모아 ACQ.2로 정의
- CS 측면에서 공급자 평가, 선택 및 계약, 합의에 중점
- 기본 산출물 Request for proposal을 Request for quotation으로 변경
- ISO/SAE 21434 7.4.1과 7.4.2장을 커버함

SOLUTIONLINK

Automotive SPICE for Cybersecurity

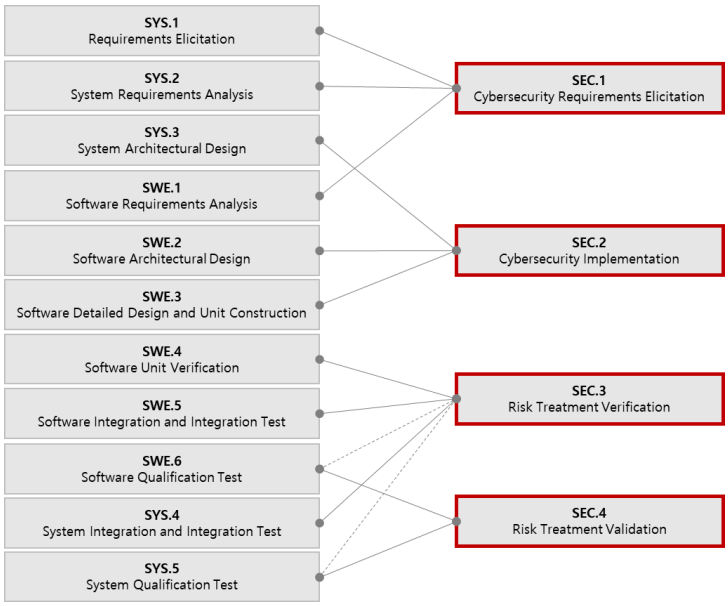
SEC.1 Cybersecurity Requirements Elicitation
- CS 목표와 CS 요구사항 도출에 대해 다룸
- CS 요구사항은 시스템 또는 소프트웨어 요구사항 명세에 수집됨
- ISO/SAE 21434 9.4 와 9.5장을 커버함

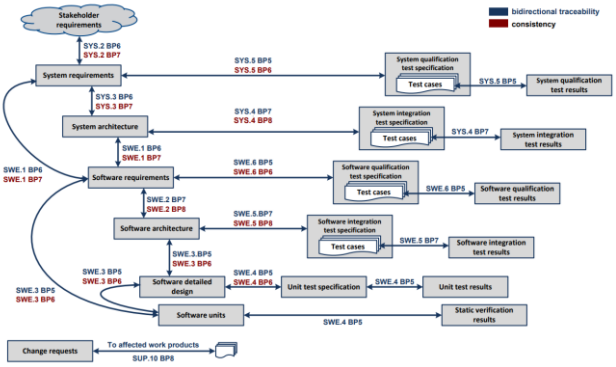
SEC.2 Cybersecurity Implementation
- CS claims를 제외한 위험 완화가 필요한 위험 처리에 대해 다름
- 시스템과 소프트웨어의 구분 없이 아키텍처 설계, 상세 설계 및 구현을 다룸
- 취약점(vulnerabilities)의 식별 및 커뮤니케이션에 대해 다름
- ISO/SAE 21434 10.4.1장을 커버함

SEC.3 Risk treatment verification
- 위험 처리 수단 및 CS 요구사항 및 아키텍처 설계에 대한 구현 준수 여부를 다룸
- ISO/SAE 21434 10.4.2장을 커버함

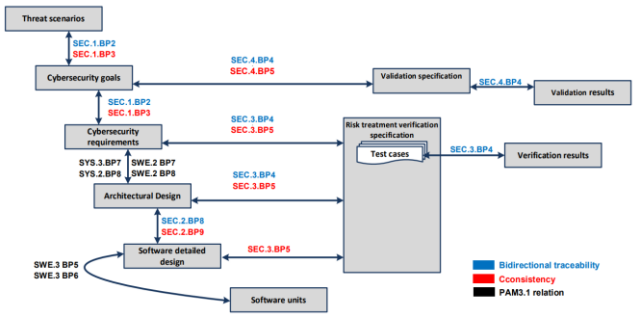
SEC.4 Risk treatment validation
- CS 목표의 구현 준수 여부를 다룸
- ISO/SAE 21434 11장을 커버함

ASPICE for Cybersecurity PAM은 ASPICE PAM 3.1의 V&V (Plan, specify, perform, traceability & consistency, communicate) 구조를 그대로 따르고 있습니다.





ASPICE - Traceability and Consistency



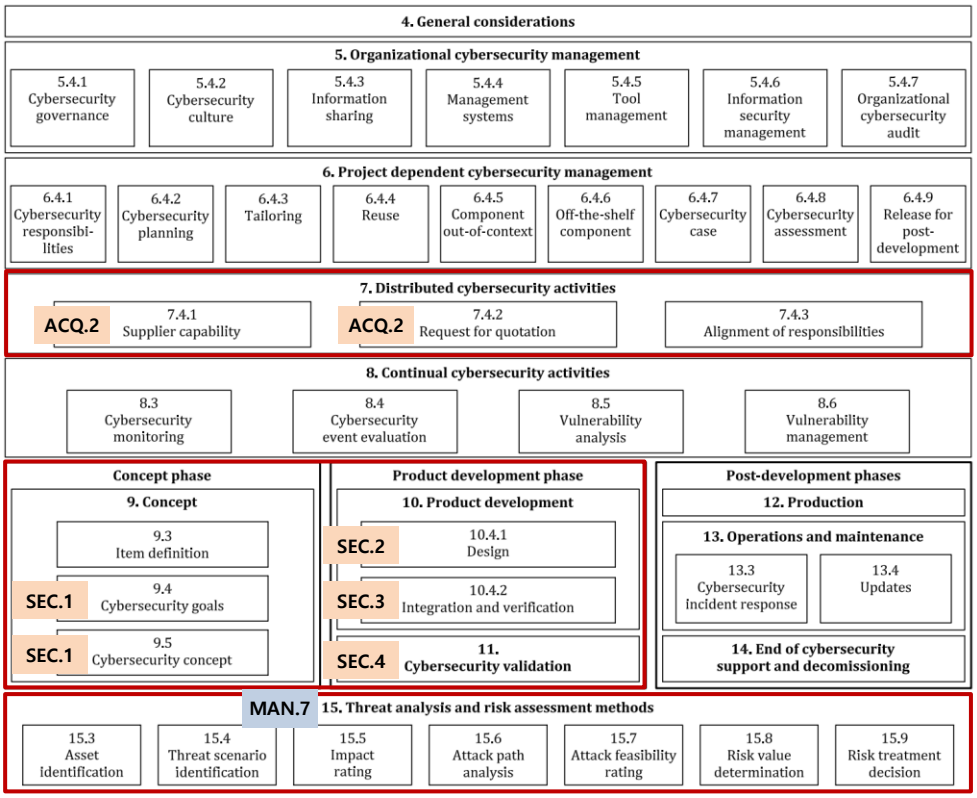
ASPICE for Cybersecurity - Traceability and Consistency

SOLUTIONLINK

Coverage of ISO/SAE 21434

ASPICE는 일반적으로 개발 프로젝트에서 제품 개발에 중점을 둡니다. 조직 수준에서 수행되는 사이버 보안 활동과 개발 이후 활동에 대한 다음의 ISO/SAE 21434 영역은 ASPICE for Cybersecurity에서 다루지 않습니다.

- 조직 사이버 보안 프로세스(ISO/SAE 21434의 5장)
- 지속적인 사이버 보안 활동(ISO/SAE 21434의 8장)
- 생산(ISO/SAE 21434의 12장)
- 운영(ISO/SAE 21434의 13장)
- 지원 종료 및 폐기(ISO/SAE 21434의 14장)



Mapping between ISO/SAE 21434 & ASPICE for Cybersecurity

출처: intacs information letter(2022.10)