Lessons Learned: How to Write Good Safety Plans

Henrik Thane

Adj. Professor in Functional Safety, MDH

SAFETY INTEGRITY AB

2017-05-22

Recalls

- **February 21, 2016**, Volvo recalls 59,000 cars due to a *software* bug after some owners experienced their engines stopping and restarting while they were driving.

- **September 2016**, GM recalls 4.3 million vehicles globally for airbag software defect.
  The bug can prevent airbags from deploying in a crash. The defect, which affects all of GM's current full-size pickups and SUVs, is linked to one death and three injuries.

- April 2015, Nissan recalls ~23,000 Micra vehicles due to a software defect that caused the car to suddenly accelerate unintentionally.

- April 2004, Jaguar recalls 67,798 cars for transmission fix
  Software defect slams car into reverse gear if there is a major oil pressure drop.

There is something called Liability

(Product, Manufacturer and Criminal)

Liability

Manufacturer's Liability

- The manufacturer has to organize the company
  - Such that design, production and documentation faults are eliminated or detected.

Product Liability

- A product, that is put into service, must provide the level of safety (acceptable risk) which can be expected by the general public.

Reversal of Evidence

- The manufacturer has to show that it is not responsible for a fault.
- It is guilty until proven otherwise.

Prove Innocence

- Manufacturer's liability is excluded if
  - A failure can not be avoided/detected
  - Using current state-of-the-art technology when launching the product.

Criminal Liability

Which employees can be held liable?

– **Injury or death**, caused by an unsafe product will lead to criminal prosecution.

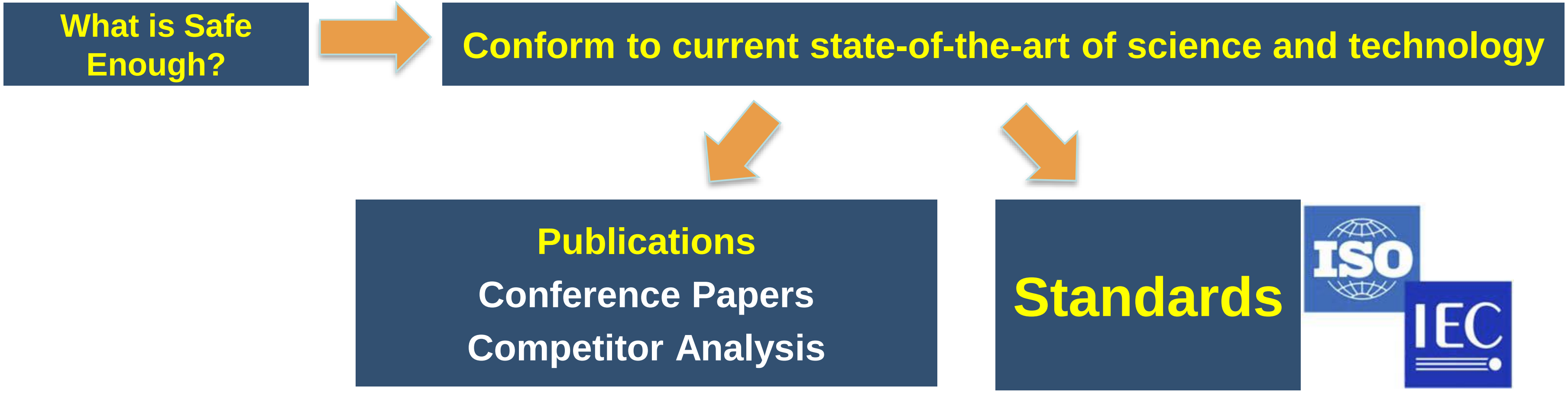
  - The judgment will always affect individual employees.

You need to Develop Safe Products

Why?

- A moral responsibility
- Reduce likelihood of systematic safety defects (*Recalls and Warranty)*
- Reduce responsibility for product liability (*Lawsuits)*
  - *Product, Manufacturer and Criminal Liability*

How?



What is Safe Enough?

Conform to current state-of-the-art of science and technology

Publications

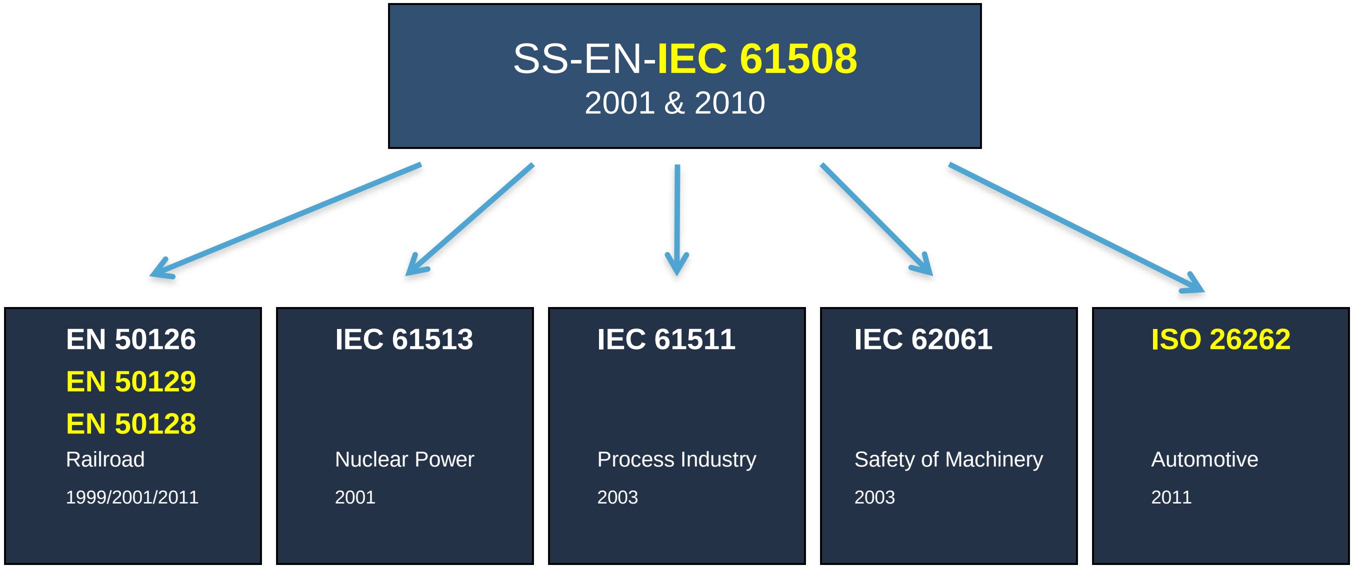
Conference Papers

Competitor Analysis

Standards

- The **key-date** is time of the delivery.
  - Even if start-of-production is earlier

Functional Safety Standards



SS-EN-**IEC 61508**

2001 & 2010

EN 50126

EN 50129

EN 50128

Railroad

1999/2001/2011

IEC 61513

Nuclear Power

2001

IEC 61511

Process Industry

2003

IEC 62061

Safety of Machinery

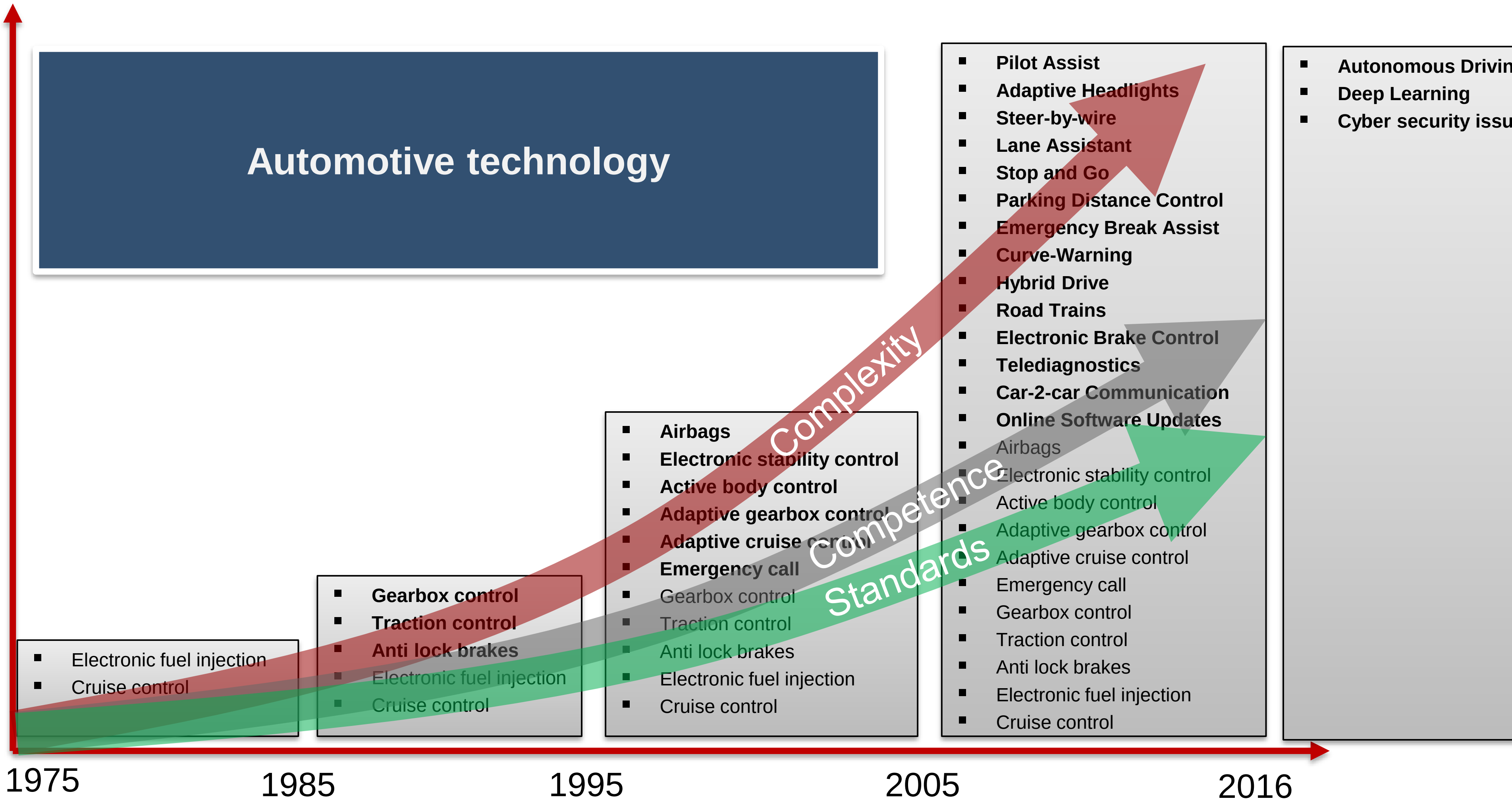
2003

ISO 26262

Automotive

2011

State-of-the-Art vs Standards



- Electronic fuel injection
- Cruise control

- **Gearbox control**
- **Traction control**
- **Anti lock brakes**
- Electronic fuel injection
- Cruise control

- **Airbags**
- **Electronic stability control**
- **Active body control**
- **Adaptive gearbox control**
- **Adaptive cruise control**
- **Emergency call**
- Gearbox control
- Traction control
- Anti lock brakes
- Electronic fuel injection
- Cruise control

- **Pilot Assist**
- **Adaptive Headlights**
- **Steer-by-wire**
- **Lane Assistant**
- **Stop and Go**
- **Parking Distance Control**
- **Emergency Break Assist**
- **Curve-Warning**
- **Hybrid Drive**
- **Road Trains**
- **Electronic Brake Control**
- **Telediagnostics**
- **Car-2-car Communication**
- **Online Software Updates**
- Airbags
- Electronic stability control
- Active body control
- Adaptive gearbox control
- Adaptive cruise control
- Emergency call
- Gearbox control
- Traction control
- Anti lock brakes
- Electronic fuel injection
- Cruise control

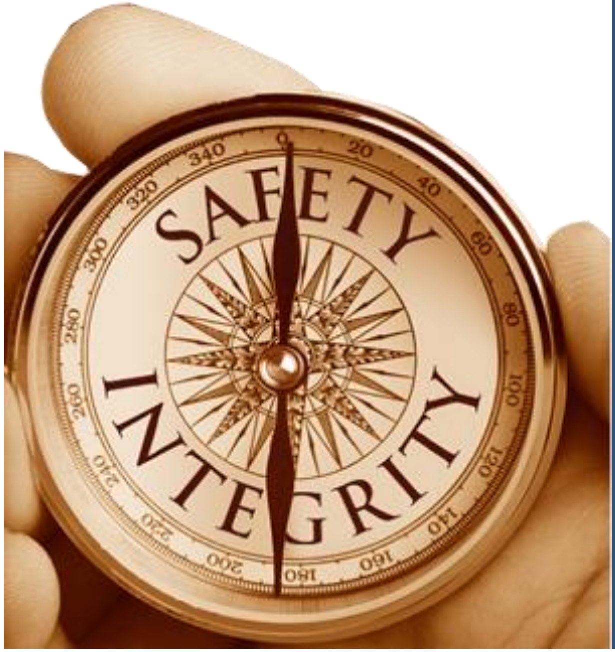
- **Autonomous Drivin**
- **Deep Learning**
- **Cyber security issu**

Typically 7-10 years between releases of standards

If you like BBQ

A classic offset smoker. Yeah!!!

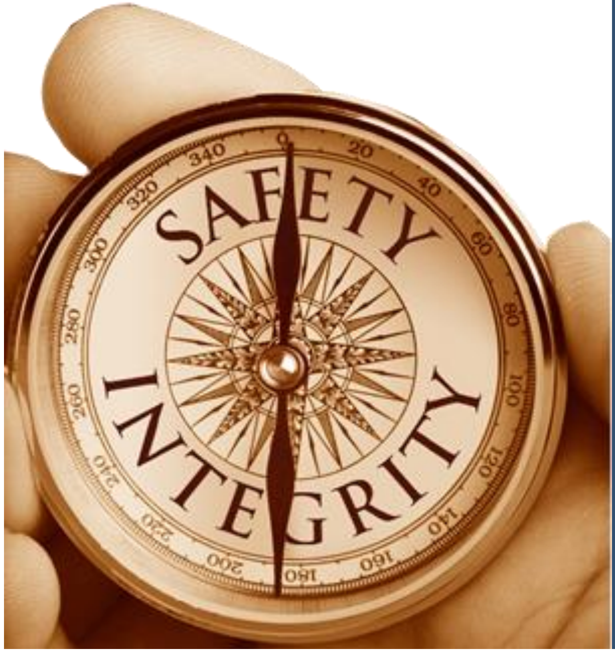
Why a Safety Plan?



Why do we need a safety plan?

- Manage the development of a safe product
  - Required by many standards
- Plan how to provide sufficient evidence and arguments that he product is safe
  - Plan how to argue that the system is safe (the Safety Case)
- Prove your innocence for liability purposes
  - Show systematic approach compliant with state-of-the-art
  - Due to scope of product, a safety plan may have to cover several different standards but also “state-of-the-art methods” for new technology (e.g., deep learning vision systems, AI, cyber security, etc.)

What should a safety plan cover?



What should a safety plan capture?

- A lifecycle/development process
- Your company's development process
  - In all likelihood you will have to modify your existing process.
- Harmonize it with target standard's requirements
  - Or other state-of-the-art covering publications when necessary.

All have V-model process models (…so far)

- You are allowed to use other models as long as the evidence in the end looks like you followed a V-model
  - E.g., for Agile development

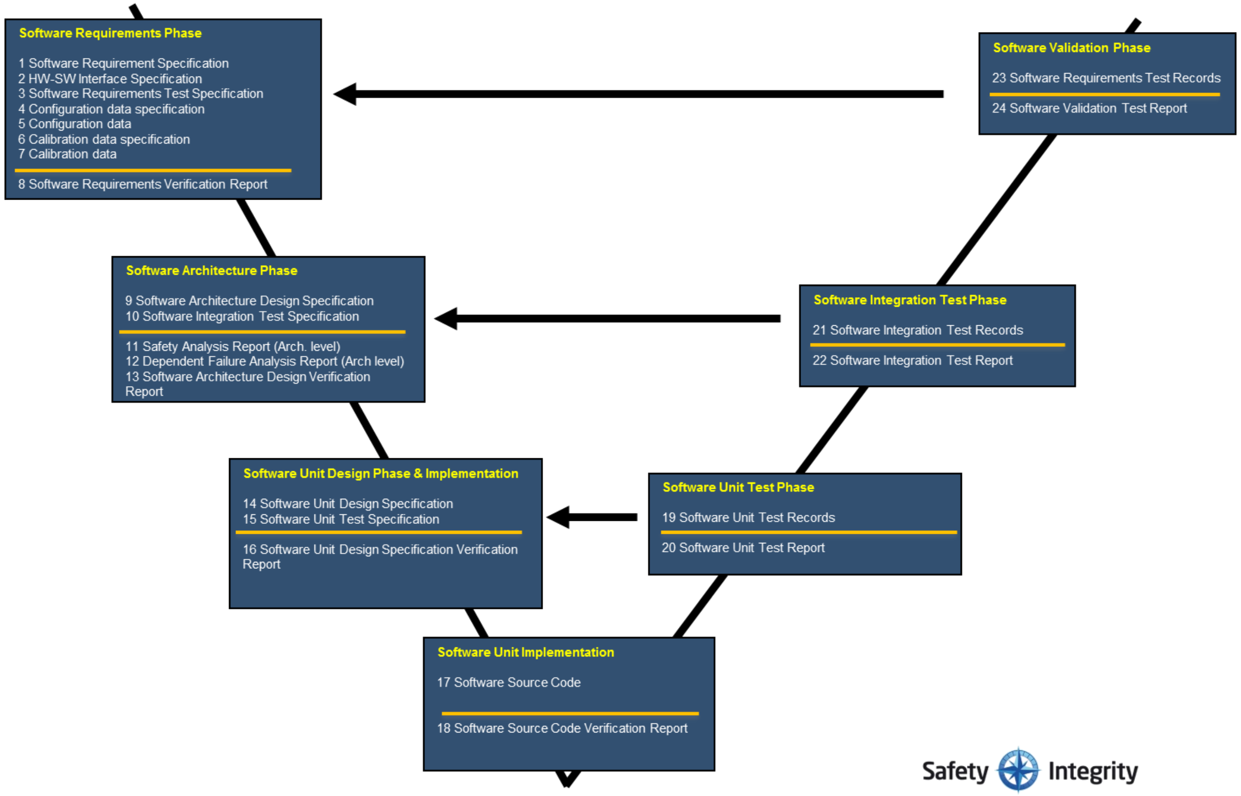
Standards typically have many process requirements

- >500 ISO26262 (~92% process related)
- >350 EN50128 (~95% process related)

The safety plan should cover

Work products/artifacts

- Result from a process step e.g.:
  - Hazard analysis, Identifying Safety Functions, Writing Safety Requirements,
  - Architecture design, Diagnostic design, Test records,
  - Review protocols, Change requests, etc.



Software Requirements Phase

1 Software Requirement Specification
2 HW-SW Interface Specification
3 Software Requirements Test Specification
4 Configuration data specification
5 Configuration data
6 Calibration data specification
7 Calibration data

8 Software Requirements Verification Report

Software Architecture Phase

9 Software Architecture Design Specification
10 Software Integration Test Specification

11 Safety Analysis Report (Arch. level)
12 Dependent Failure Analysis Report (Arch level)
13 Software Architecture Design Verification Report

Software Unit Design Phase & Implementation

14 Software Unit Design Specification
15 Software Unit Test Specification

16 Software Unit Design Specification Verification Report

Software Unit Implementation

17 Software Source Code

18 Software Source Code Verification Report

Software Unit Test Phase

19 Software Unit Test Records

20 Software Unit Test Report

Software Integration Test Phase

21 Software Integration Test Records

22 Software Integration Test Report

Software Validation Phase

23 Software Requirements Test Records

24 Software Validation Test Report

Extracting Work Products

How to extract the work products' process requirements?

- Easy in some standards like EN50128:2011
  - Explicit work product requirements listed
  - Sorted in order of work products
- More difficult in others (e.g., ISO13849:2013)
  - No explicit work products defined - mostly implicit in text.
- Tedious work for ISO26262

  Work products are spread out all over the standard´s parts and not sorted/assembled

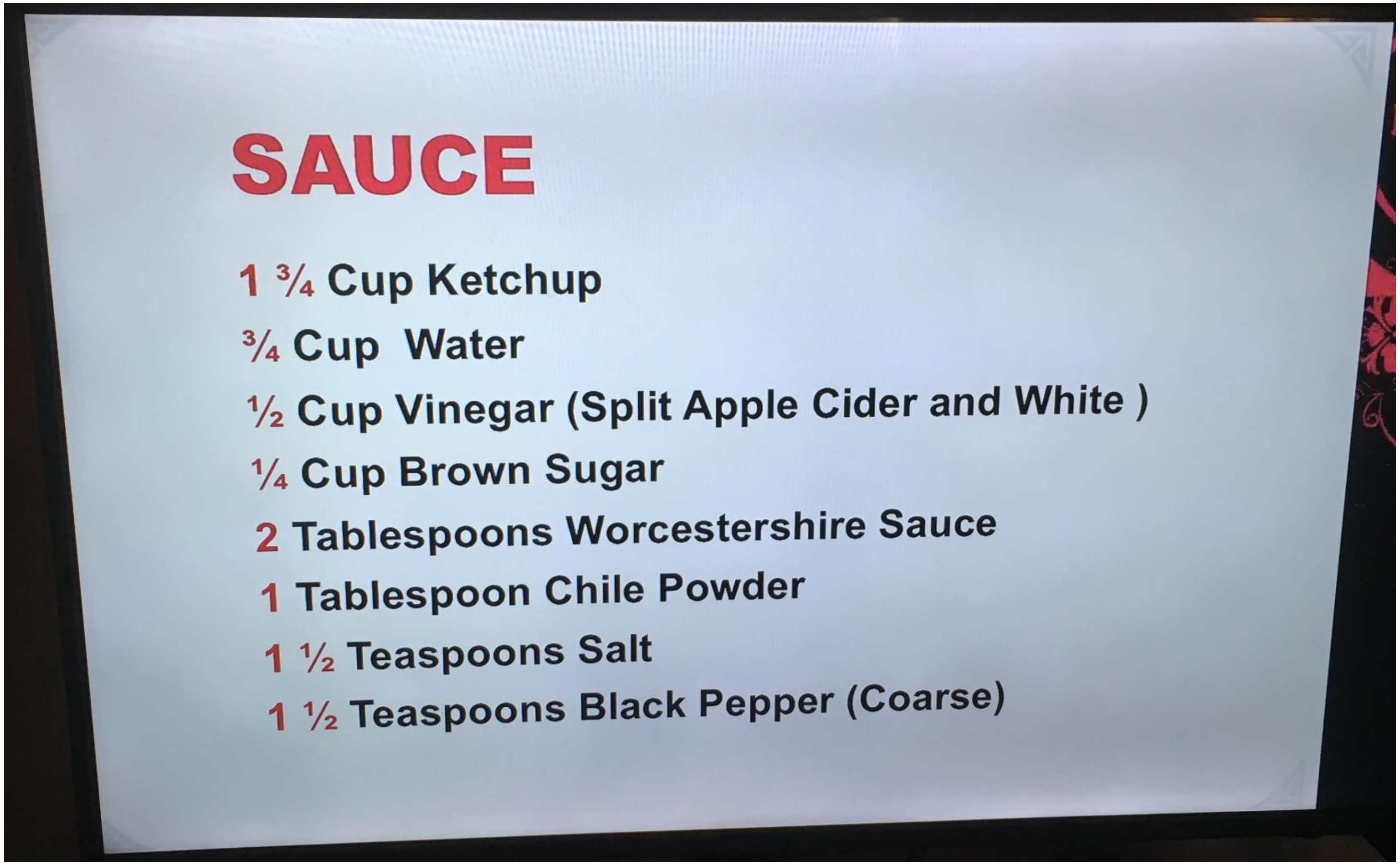
  E.g., Safety Plan:

  - 26262-2
    - 6.5.1 (6.4.3-6.4.5), 7
  - 26262-3
    - 6.5.1. 6.5.2
  - 26262-4
    - 5.5.2 (5.4.1-5.4.4)
  - 26262-5
    - 5.5.1 (5.4.1-5.4.4)
  - 26262-6
    - 5.5.1 (5.4.1-5.4.7), 7.5.2 (7.4.7), C.5.3 (C.4.1, C.4.4, C.4.5, C.4.9 and C.4.10)
  - 26262-8

Strategy for extracting work products

- How to extract work product requirements?
  - Hard work for ISO26262
    - Sort and assemble all requirements for each work product.
    - You have to do this for over a hundred work products
  - For standards like ISO13849 and IEC62061
    - Take inspiration from other standards (like EN50128 and A Spice)
    - Remember that all safety standards so far have a V-model
      - Use it as a harness
      - Take generic work product “titles” from other standards
        - » map all target standards requirements to work products
- Organization next →

Excellent sauce from Franklin's BBQ



SAUCE

1 ¾ Cup Ketchup

¾ Cup Water

½ Cup Vinegar (Split Apple Cider and White)

¼ Cup Brown Sugar

2 Tablespoons Worcestershire Sauce

1 Tablespoon Chile Powder

1 ½ Teaspoons Salt

1 ½ Teaspoons Black Pepper (Coarse)

Organization

- Organization
  - Roles
    - If not explicit in standard
      - Take inspiration from other standards
        - » Like EN50128

Requirements Manager

Designer

Implementer

Tester

Verifier

Integrator

Validator

Assessor

Project Manager

: Configuration Manager

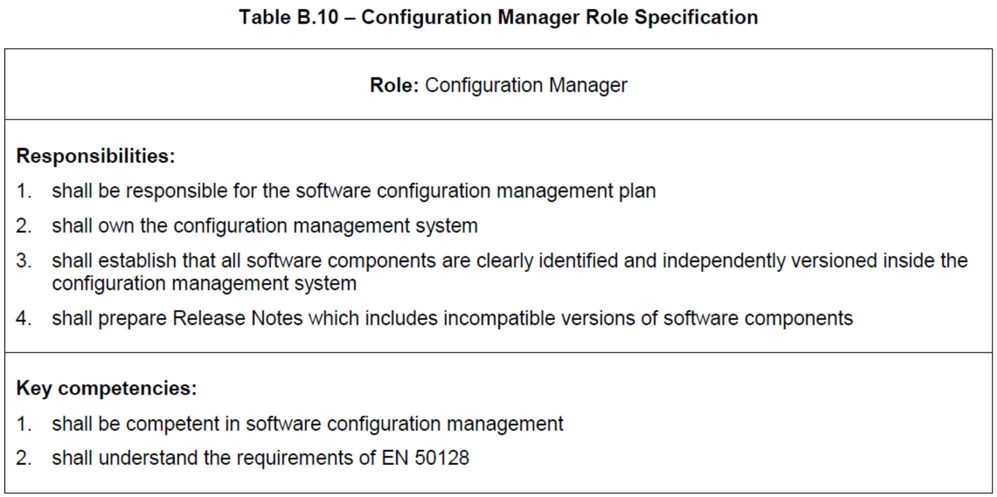


Table B.10 – Configuration Manager Role Specification

Role: Configuration Manager
Responsibilities: 1. shall be responsible for the software configuration management plan 2. shall own the configuration management system 3. shall establish that all software components are clearly identified and independently versioned inside the configuration management system 4. shall prepare Release Notes which includes incompatible versions of software components
Key competencies: 1. shall be competent in software configuration management 2. shall understand the requirements of EN 50128

  - Use RACI charts
    - Allocate Role to work products
    - Allocate 1st level reviewers, 2nd level reviewers, and Authorization for each work product

Roles & RACI charts

LEGEND		PROCESS STEP TO EXECUTE		OUTPUT / WORK PRODUCT	
ORANGE		Write/Specify/Design/Implement		Primary work product	
BLUE	BLUE	1st Review	2nd Review	Review record	Review record
YELLOW		Test and Validation		Test record	
GREEN		Summarizing Verification and Validation		Report	
BROWN		Approval		Released work product	

Example ROLES

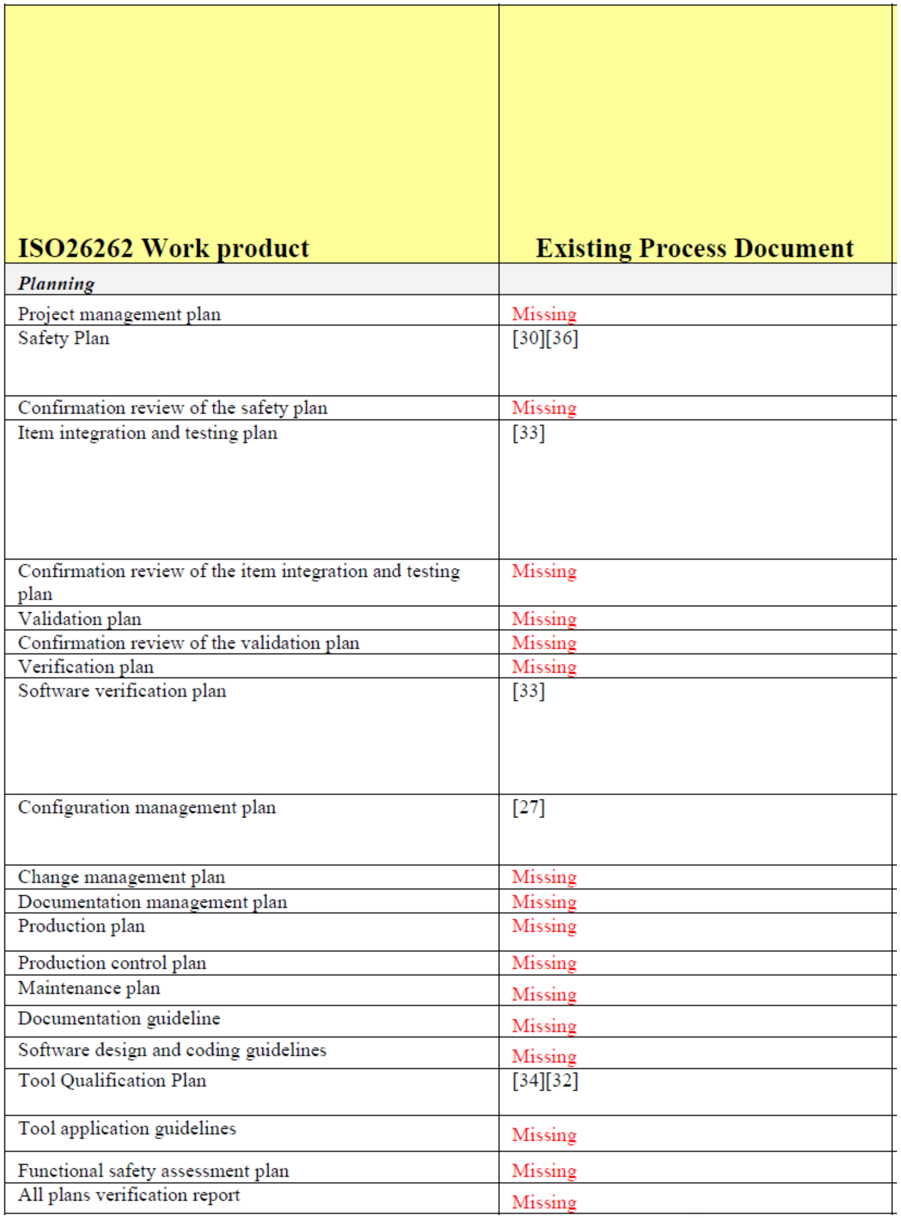
- Project Manager (PM)
- Safety Manager/Quality Assurance Manager (QM)
- Verification Team (VT)
- Verification Lead (VL)
- Test Team (TT)
- Requirements Team (RT)
- Architect (A)
  - May be split into System/HW/SW
- Developer (D)
  - May be split into HW and SW
- Maintenance Team/ Change Control (MT)
- Maintenance and configuration Lead (ML)
- Documentation Team (DT)

Work product #	Org. Units / Roles Work Products / Activities	PREPARE	1ST REVIEW	2ND REVIEW	APPROVE
	Planning phase				
1)	Project plan	PM	VT/VL	QM	PM
2)	Development plan	QM	VT	VL	PM
3)	Verification & Validation plan	VL	VT	QM	PM
4)	Maintenance & Configuration plan	QM	VT	VL	PM
5)	Documentation plan	DT	VT/VL	QM	PM
6)	Tools and COTS qualification plan	A	VT/VL	QM	PM
7)	Quality assurance plan	QM	VT	VL	PM
8)	All plans verification report	VL	VT	QM	PM
	Concept phase				
9)	Capture stakeholder requirements	RT	VT/VL	QM	PM
10)	System definition	RT	VT/VL	QM	PM
11)	Tailor Lifecycle	QM	VT	VL	PM
12)	System requirements specification	RT	VT/VL	QM	PM
13)	Configuration specification	RT	VT/VL	QM	PM
14)	System validation test specification	TT/TL	VT/VL	QM	PM
15)	Concept verification report	VL	VT	QM	PM
	Development phase				
	System Level SW/HW				
16)	System Architectural Design	A	VT/VL	QM	PM
17)	Allocate system requirements	A	VT/VL	QM	PM
18)	HW/SW interface specification	A	VT/VL	QM	PM
19)	Refine configuration specification	A	VT/VL	QM	PM
20)	Failure modes analysis (system focus)	A	VT/VL	QM	
21)	Diagnostics Design	A	VT/VL	QM	
22)	System Integration Test Specification	TT/TL	VT	QM	PM
23)	Tools and COTS qualification Report	A	VT/VL	QM	PM
24)	System Level Verification report	VL	VT	QM	PM

Existing company process?

How to harmonize with the standard?

- List all required work products
- Match and cross-reference existing examples of:
  - Plans
  - Reports
  - Templates
  - Specifications
  - Test protocols
  - Review checklists
  - etc…

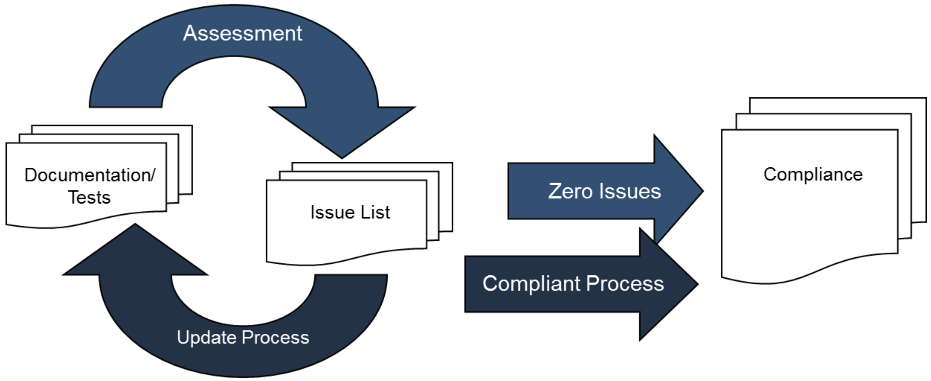


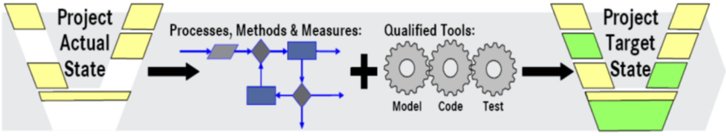
ISO26262 Work product	Existing Process Document
Planning	
Project management plan	Missing
Safety Plan	[30][36]
Confirmation review of the safety plan	Missing
Item integration and testing plan	[33]
Confirmation review of the item integration and testing plan	Missing
Validation plan	Missing
Confirmation review of the validation plan	Missing
Verification plan	Missing
Software verification plan	[33]
Configuration management plan	[27]
Change management plan	Missing
Documentation management plan	Missing
Production plan	Missing
Production control plan	Missing
Maintenance plan	Missing
Documentation guideline	Missing
Software design and coding guidelines	Missing
Tool Qualification Plan	[34][32]
Tool application guidelines	Missing
Functional safety assessment plan	Missing
All plans verification report	Missing

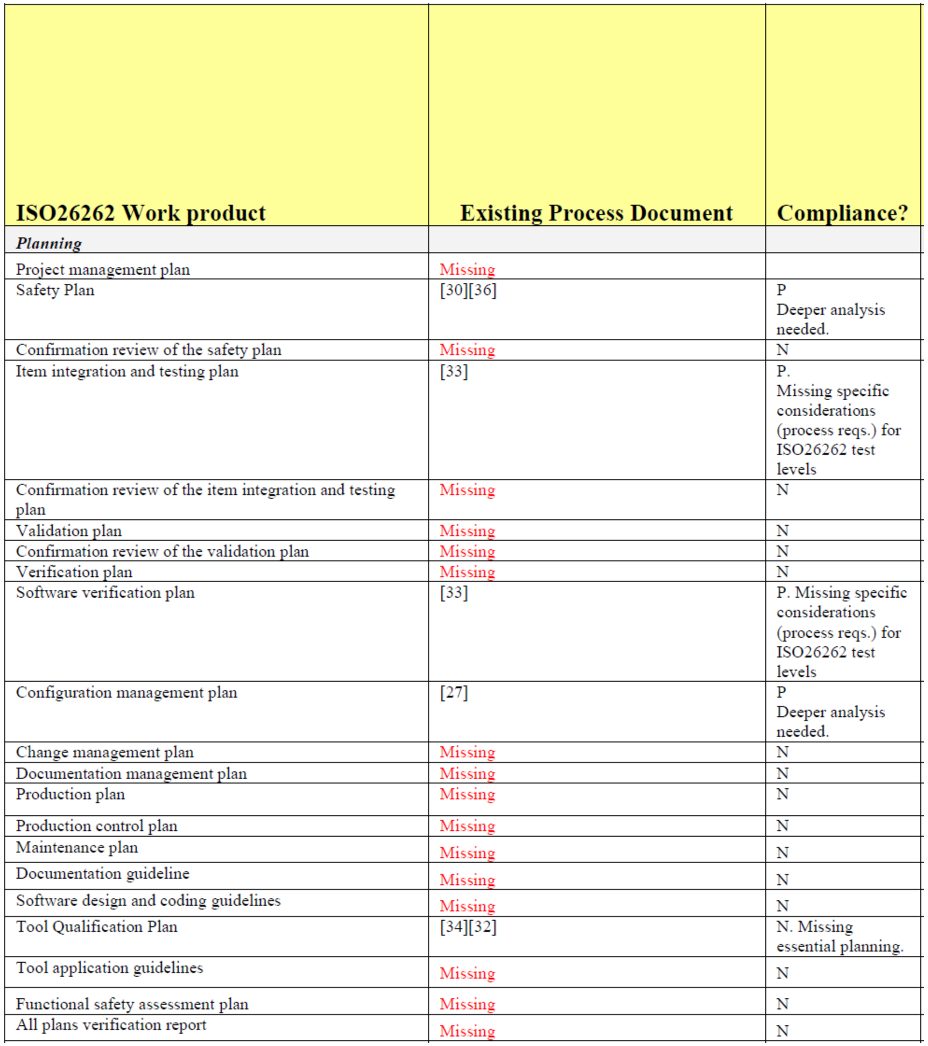
Existing company process?

Perform GAP analysis

- Identify issues
  - Update each work product process step for standard compliance
  - Update templates and company documentation
  - Review and repeat GAP until no issues

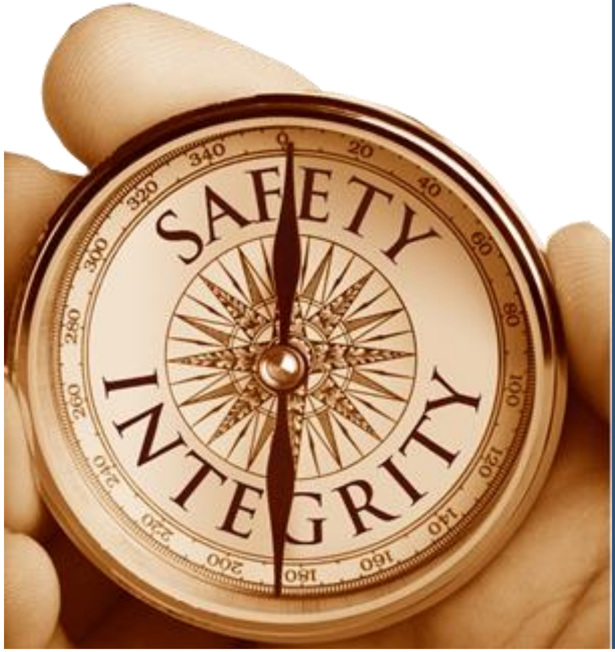






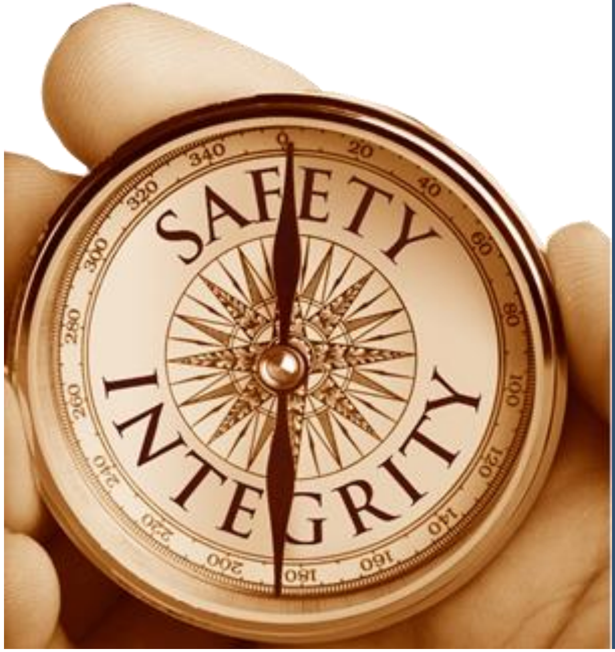
ISO26262 Work product	Existing Process Document	Compliance?
Planning		
Project management plan	Missing	
Safety Plan	[30][36]	P Deeper analysis needed.
Confirmation review of the safety plan	Missing	N
Item integration and testing plan	[33]	P. Missing specific considerations (process reqs.) for ISO26262 test levels
Confirmation review of the item integration and testing plan	Missing	N
Validation plan	Missing	N
Confirmation review of the validation plan	Missing	N
Verification plan	Missing	N
Software verification plan	[33]	P. Missing specific considerations (process reqs.) for ISO26262 test levels
Configuration management plan	[27]	P Deeper analysis needed.
Change management plan	Missing	N
Documentation management plan	Missing	N
Production plan	Missing	N
Production control plan	Missing	N
Maintenance plan	Missing	N
Documentation guideline	Missing	N
Software design and coding guidelines	Missing	N
Tool Qualification Plan	[34][32]	N. Missing essential planning.
Tool application guidelines	Missing	N
Functional safety assessment plan	Missing	N
All plans verification report	Missing	N

Safety Plan Use-Cases 1



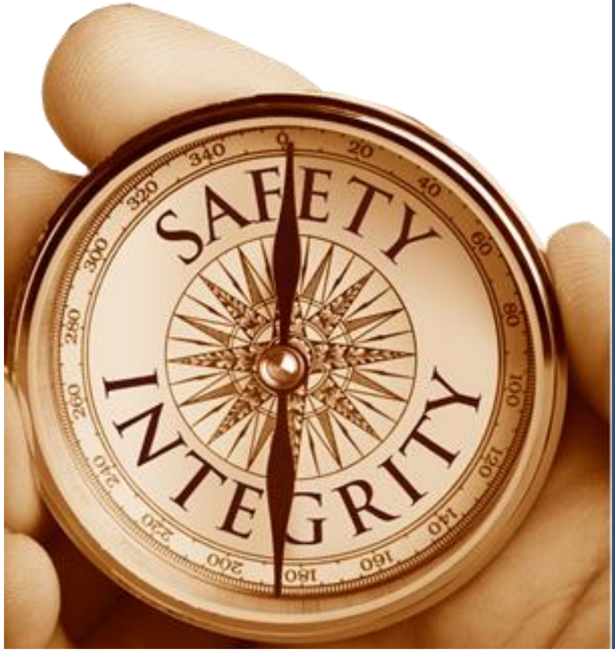
- Full scope
  - For example, Auto Brake system in car:
    - Cover everything from Hazard analysis to validation in a car.
    - Including
      - Concept phase with hazard and risk analysis
      - System development
      - HW development
      - SW development, and
      - Series production.

Safety Plan Use-Cases 2



- Limited scope
  - Reusable platform
    - E.g., Execution, communication, diagnostics, and configuration framework
    - May only capture process from architecture level and below
    - No hazards or safety functions on system/vehicle level to relate to
      - Validation not possible (that safety functions work)
      - Only SIL, PL or ASIL requirements on process/product for all functional requirements.

Safety Plan Use-Cases 3



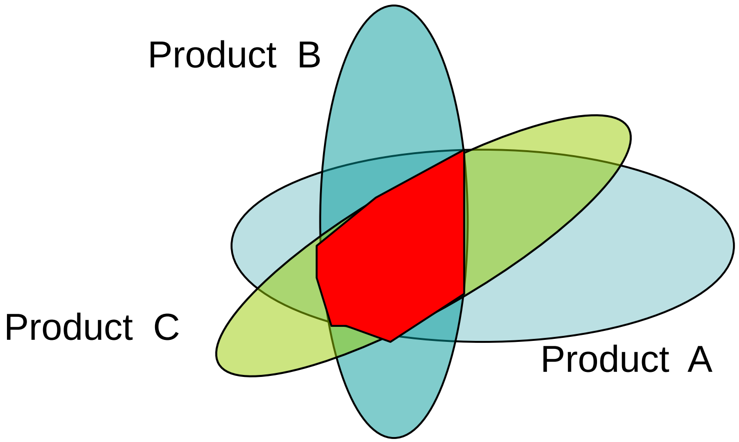
- Generic Product
  - That is only parametrized
  - No product/SW/HW development only configuration
  - Only development process for Application Configuration

- Different target standards
  - E.g., Functional Safety + Cyber Security

Product Line Safety Plans

How to identify commonalities between safety management use-cases

- Find common denominator
  - Work product scoping
- Use this as basis for common safety plan and process certification



	Work Product 1	Work Product 2	Work Product 3	Work Product 4	Work Product 5	Work Product 6	Work Product 7
Product A	Yes	No	No	Yes	Yes	Yes	No
Product B	Yes	No	Yes	No	Yes	Yes	No
Product C	Yes	Yes	Yes	No	Yes	Yes	Yes

Lessons learned: Writing Safety Plans

Product Liability

- You are assumed guilty of any safety related failures and accidents until you have proven otherwise.
- You prove your innocence by developing and maintaining your product according to the state-of-the-art
  - Defined by current functional safety standards (when in scope of standard)
  - For new technology
    (e.g., fully autonomous driving) – defined by state-of-the-art in published research.

Lessons learned: Writing Safety Plans

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 50128

June 2011

ICS 35.240.60; 45.020; 93.100

Supersedes EN 50128:2001

English version

**Railway applications -
Communication, signalling and processing systems -
Software for railway control and protection systems**

Applications ferroviaires -
Systèmes de signalisation, de
télécommunication et de traitement -
Logiciels pour systèmes de commande et
de protection ferroviaire

Bahnanwendungen -
Telekommunikationstechnik,
Signaltechnik und
Datenverarbeitungssysteme -
Software für Eisenbahnsteuerungs- und
Überwachungssysteme

This European Standard was approved by CENELEC on 2011-04-25. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

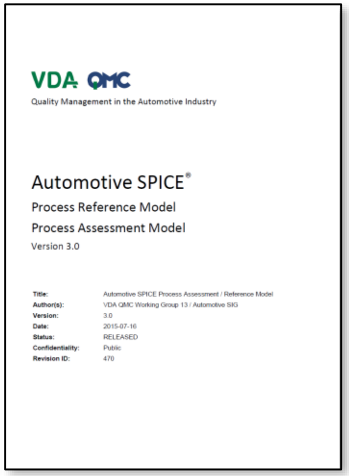
CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

© 2011 CENELEC - All rights of exploitation in any form and by any means reserved worldwide for CENELEC members.

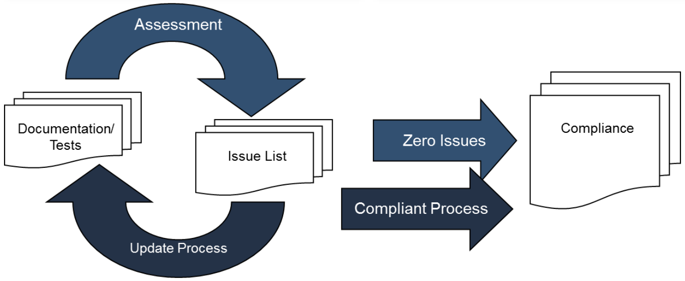
Ref. No. EN 50128:2011 E

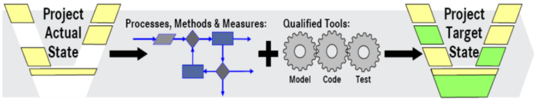


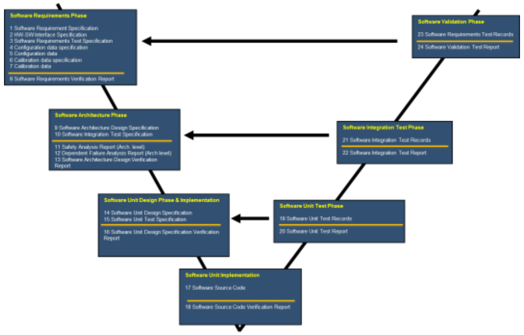
VDA QMC
Quality Management in the Automotive Industry

Automotive SPICE®
Process Reference Model
Process Assessment Model
Version 3.0

Title:	Automotive SPICE Process Assessment / Reference Model
Author(s):	VDA QMC Working Group 13 / Automotive SIG
Version:	3.0
Date:	2015-07-16
Status:	RELEASED
Confidentiality:	Public
Revision ID:	470







Software Requirements Phase
1 Software Requirement Specification
2 HW-SW Interface Specification
3 Software Requirements Test Specification
4 Configuration data specification
5 Configuration data
6 Calibration data specification
7 Calibration data
8 Software Requirements Verification Report

Software Architecture Phase
9 Software Architecture Design Specification
10 Software Integration Test Specification
11 Safety Analysis Report (Arch. level)
12 Dependent Failure Analysis Report (Arch level)
13 Software Architecture Design Verification Report

Software Unit Design Phase & Implementation
14 Software Unit Design Specification
15 Software Unit Test Specification
16 Software Unit Design Specification Verification Report

Software Unit Implementation
17 Software Source Code
18 Software Source Code Verification Report

Software Unit Test Phase
19 Software Unit Test Records
20 Software Unit Test Report

Software Integration Test Phase
21 Software Integration Test Records
22 Software Integration Test Report

Software Validation Phase
23 Software Requirements Test Records
24 Software Validation Test Report

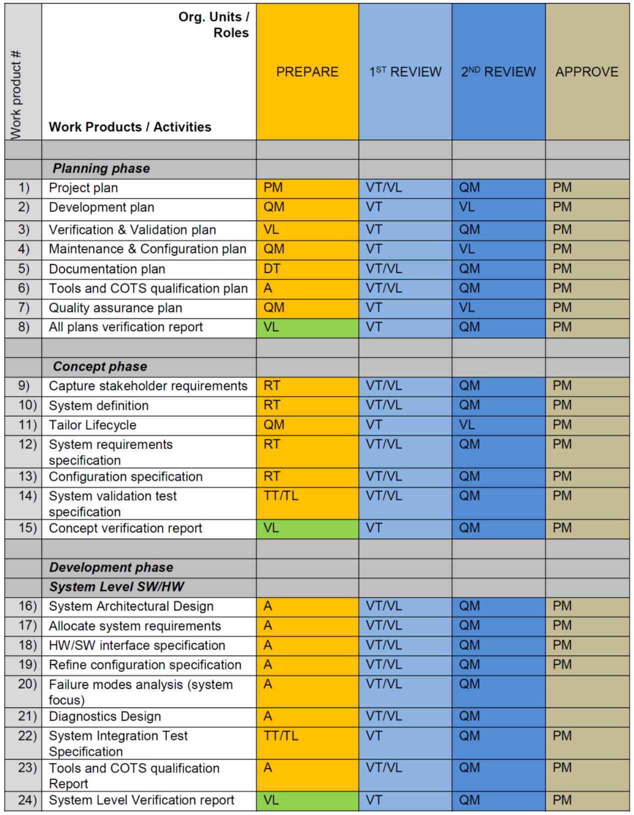
Lessons learned regarding writing safety plans

- Take inspiration from other standards
  - Good ones are EN50128 and Automotive Spice
- Be aware when writing safety plan that using a single standard may not cover the state-of-the-art as required by Liability Law.
- Capture all essential work products in target standard
  - If in doubt use V-model as harness
    - Take essential work products from other standards and map target standards requirements to those work products
  - Harmonize with existing company process
  - Cross-reference existing documentation
  - Perform GAP analysis → update safety plan/process until harmonized
- The regular process and the safety process must be harmonized otherwise people will no do the work.

Lessons learned: Writing Safety Plans

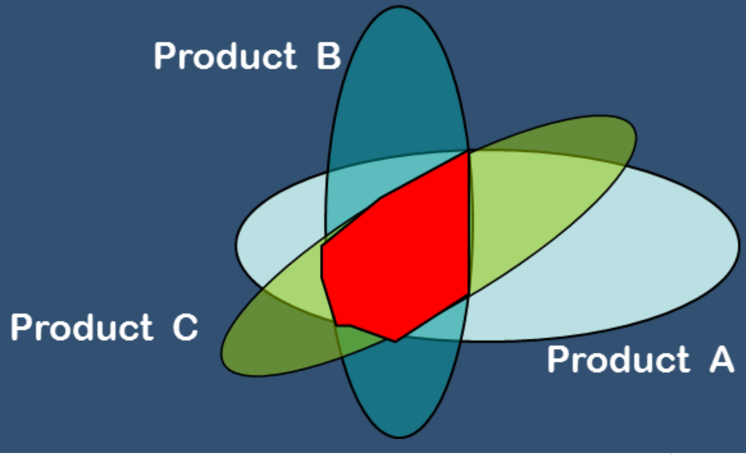
Example ROLES

- Project Manager (PM)
- Safety Manager/Quality Assurance Manager (QM)
- Verification Team (VT)
- Verification Lead (VL)
- Test Team (TT)
- Requirements Team (RT)
- Architect (A)
  - May be split into System/HW/SW
- Developer (D)
  - May be split into HW and SW
- Maintenance Team/ Change Control (MT)
- Maintenance and configuration Lead (ML)
- Documentation Team (DT)



Work product #	Org. Units / Roles Work Products / Activities	PREPARE	1ST REVIEW	2ND REVIEW	APPROVE
	Planning phase				
1)	Project plan	PM	VT/VL	QM	PM
2)	Development plan	QM	VT	VL	PM
3)	Verification & Validation plan	VL	VT	QM	PM
4)	Maintenance & Configuration plan	QM	VT	VL	PM
5)	Documentation plan	DT	VT/VL	QM	PM
6)	Tools and COTS qualification plan	A	VT/VL	QM	PM
7)	Quality assurance plan	QM	VT	VL	PM
8)	All plans verification report	VL	VT	QM	PM
	Concept phase				
9)	Capture stakeholder requirements	RT	VT/VL	QM	PM
10)	System definition	RT	VT/VL	QM	PM
11)	Tailor Lifecycle	QM	VT	VL	PM
12)	System requirements specification	RT	VT/VL	QM	PM
13)	Configuration specification	RT	VT/VL	QM	PM
14)	System validation test specification	TT/TL	VT/VL	QM	PM
15)	Concept verification report	VL	VT	QM	PM
	Development phase				
	System Level SW/HW				
16)	System Architectural Design	A	VT/VL	QM	PM
17)	Allocate system requirements	A	VT/VL	QM	PM
18)	HW/SW interface specification	A	VT/VL	QM	PM
19)	Refine configuration specification	A	VT/VL	QM	PM
20)	Failure modes analysis (system focus)	A	VT/VL	QM	
21)	Diagnostics Design	A	VT/VL	QM	
22)	System Integration Test Specification	TT/TL	VT	QM	PM
23)	Tools and COTS qualification Report	A	VT/VL	QM	PM
24)	System Level Verification report	VL	VT	QM	PM

- Lessons learned regarding writing safety plans
  - Define Roles
    - These are usually implicit in most standards
  - Allocate work products to roles in RACI charts
    - Define Verifiers and Approvers
  - For companies with many different safety related products of different types (E2E, platforms, GP + config.)
    - Find common denominator in process and set a template process.



THANK YOU!

“Laws are like Sausages, its better to not see them made”

-Otto Von Bismarck

henrik.thane@safetyintegrity.se

Safety Integrity