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)
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.
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
Automotive technology

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

1975
1985
1995
2005
2016

State-of-the-Art vs Standards

- 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
- Telediagnoses
- 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

Complexity

Typically 7-10 years between releases of standards

Autonomous Driving
- Deep Learning
- Cyber security issues
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 the 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?

- 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)
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.

The safety plan should cover
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 (6.4.1-5.4.4)
  • 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 ➔
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
  – 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

<table>
<thead>
<tr>
<th>Role: Configuration Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsibilities:</td>
</tr>
<tr>
<td>1. shall be responsible for the software configuration management plan</td>
</tr>
<tr>
<td>2. shall own the configuration management system</td>
</tr>
<tr>
<td>3. shall establish that all software components are clearly identified and independently versioned inside the configuration management system</td>
</tr>
<tr>
<td>4. shall prepare Release Notes which includes incompatible versions of software components</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key competencies:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. shall be competent in software configuration management</td>
</tr>
<tr>
<td>2. shall understand the requirements of EN 50128</td>
</tr>
</tbody>
</table>

– Use RACI charts
  • Allocate Role to work products
  • Allocate 1st level reviewers, 2nd level reviewers, and Authorization for each 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)**
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…

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

<table>
<thead>
<tr>
<th>ISO26262 Work product</th>
<th>Existing Process Document</th>
<th>Compliance?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project management plan</td>
<td>Missing</td>
<td></td>
</tr>
<tr>
<td>Safety Plan</td>
<td>[30][36]</td>
<td>P</td>
</tr>
<tr>
<td>Confirmation review of the safety plan</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>Item integration and testing plan</td>
<td>[33]</td>
<td>P</td>
</tr>
<tr>
<td>Confirmation review of the item integration and testing plan</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>Validation plan</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>Confirmation review of the validation plan</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>Verification plan</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>Software verification plan</td>
<td>[33]</td>
<td>P</td>
</tr>
<tr>
<td>Configuration management plan</td>
<td>[27]</td>
<td>P</td>
</tr>
<tr>
<td>Change management plan</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>Documentation management plan</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>Production plan</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>Production control plan</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>Maintenance plan</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>Documentation guideline</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>Software design and coding guidelines</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>Tool Qualification Plan</td>
<td>[34][32]</td>
<td>N</td>
</tr>
<tr>
<td>Tool application guidelines</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>Functional safety assessment plan</td>
<td>Missing</td>
<td>N</td>
</tr>
<tr>
<td>All plans verification report</td>
<td>Missing</td>
<td>N</td>
</tr>
</tbody>
</table>
• 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.
• 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
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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
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 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

- 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