Contract number: ITEA2 – 10039

Safe Automotive soFtware architEcture (SAFE)

ITEA Roadmap application domains:

Major: Services, Systems & Software Creation

Minor: Society

ITEA Roadmap technology categories:

Major: Systems Engineering & Software Engineering

Minor 1: Engineering Process Support

WP 3

Deliverable D3.2.4.b: Definition of COTS integration for SW and HW

Due date of deliverable: 28/08/13

Actual submission date: 31/01/14

Start date of the project: 01/07/2011 **Duration:** 42 months

Project coordinator name: Stefan Voget

Organization name of lead contractor for this deliverable: TÜV NORD Mobilität

Editor: Jens Christian Lisner

Contributors: Thomas Peikenkamp, Harald Günther, Markus Oertel

Reviewers: Thomas Wenzel, Karol Niewiadomski

Revision chart and history log

Version	**Date**	**Reason**
0.1	25.10.13	Initialization of document as update of deliverable D3.2.4.a
1.0	31.01.14	Final version ready for submission

1 Table of contents

2 List of figures

3 Executive Summary

Work task 3.2.4 targets the topic of re-use of previously developed hardware and software components, including COTS (Commercial Of The Shelf) products.

The document gives an overview of the requirements depicted in WP2 and allocated to WT3.2.4 for component qualification and the applicability of the proven in use argumentation. In addition related requirements derived from ISO 26262-8 are described and analyzed in view of re-use.

As a result of the analysis meta-model enhancements are proposed and potential guideline content is identified. The qualification guideline will be developed as part of WP6 including activities and integration measures for COTS qualification.

4 Introduction

This document provides information about the requirements and criteria for re-used components, including COTS products and components already in operation. In case of sufficient field data the proven in use argumentation can be considered.

The SAFE requirements are presented and analyzed. As a result initial proposals for meta-model enhancements are given to describe the required information related to re-use.

4.1 Scope of Work Task

Work task 3.2.4 focuses on the integration of COTS components and the reuse of hardware and software components. This includes the qualification of hardware and software components and the proven in use argumentation defined in ISO 26262-8, Clauses 12, 13, 14.

Qualification of HW/SW Components

Hardware and software components planned to be used in another environment have to be analyzed to determine the suitability for the intended application. The qualification process requires sufficient information on the component (e.g. safety requirements, interfaces, failure modes) and defines activities and measures in order to qualify the component for re-use. Previously developed components as well as COTS products can be subject to qualification. The re-use relevant information shall be identified and described to support the verification and validation processes according to ISO 26262.

Proven in Use Argumentation

Components already proved in operation without incidents can be re-used, if the candidate and the field data fulfill the required criteria. In this case a set of safety lifecycle subphases can be substituted by the proven in use credit to reduce development efforts. WT3.2.4 shall define criteria for the proven in use argumentation.

4.2 Dependencies to other Work Tasks

WT3.2.4 analyses the information, activities and measures required to re-use previously developed hardware and software components.

The meta-model enhancements to describe re-use relevant information of hardware and software components are based on the meta-model extensions of WT3.2.1 (System and Software) and WT3.2.2 (Hardware).

The contributions of WT3.2.4 to the meta-model are delivered to WT3.5 (Meta Model Definition) for integration and harmonization.

Qualification guideline content identified in WT3.2.4 serves as input to WP6 (Methodology).

5 Meta-Model Enhancements

In this chapter the requirements allocated to WT3.2.4 are presented and analyzed. Additional requirements supporting the description of re-use related properties are derived from ISO 26262-8, Clauses 12, 13 and 14.

The qualification of software and hardware components is analyzed separately, following the structure of the relevant parts of ISO 26262-8, due to deviating qualification criteria and goals.

For components where field data of a sufficient service period is available the application of the proven in use argumentation is described and the required criteria and measures identified. The proven in use argument can be applied to components previously developed, including COTS products or items not developed in compliance with ISO 26262 and allows the substitution of safety lifecycle subphases. The required activities and the subphases not covered by the proven in use argumentation are described.

As a result of the requirement analysis proposals for meta-model enhancements are given for component qualification and the proven in use argumentation. In a separate section common requirements regarding information of re-used components are presented.

For references to the ISO 26262 a short notation is used in order to improve readability. The notation x-y.z stands for ISO 26262-x, y.z. The requirement coverage tracing uses the short notation preceded by “ISO-” to distinguish ISO 26262 requirements and SAFE (work task) requirements.

5.1 Qualification of Software Components

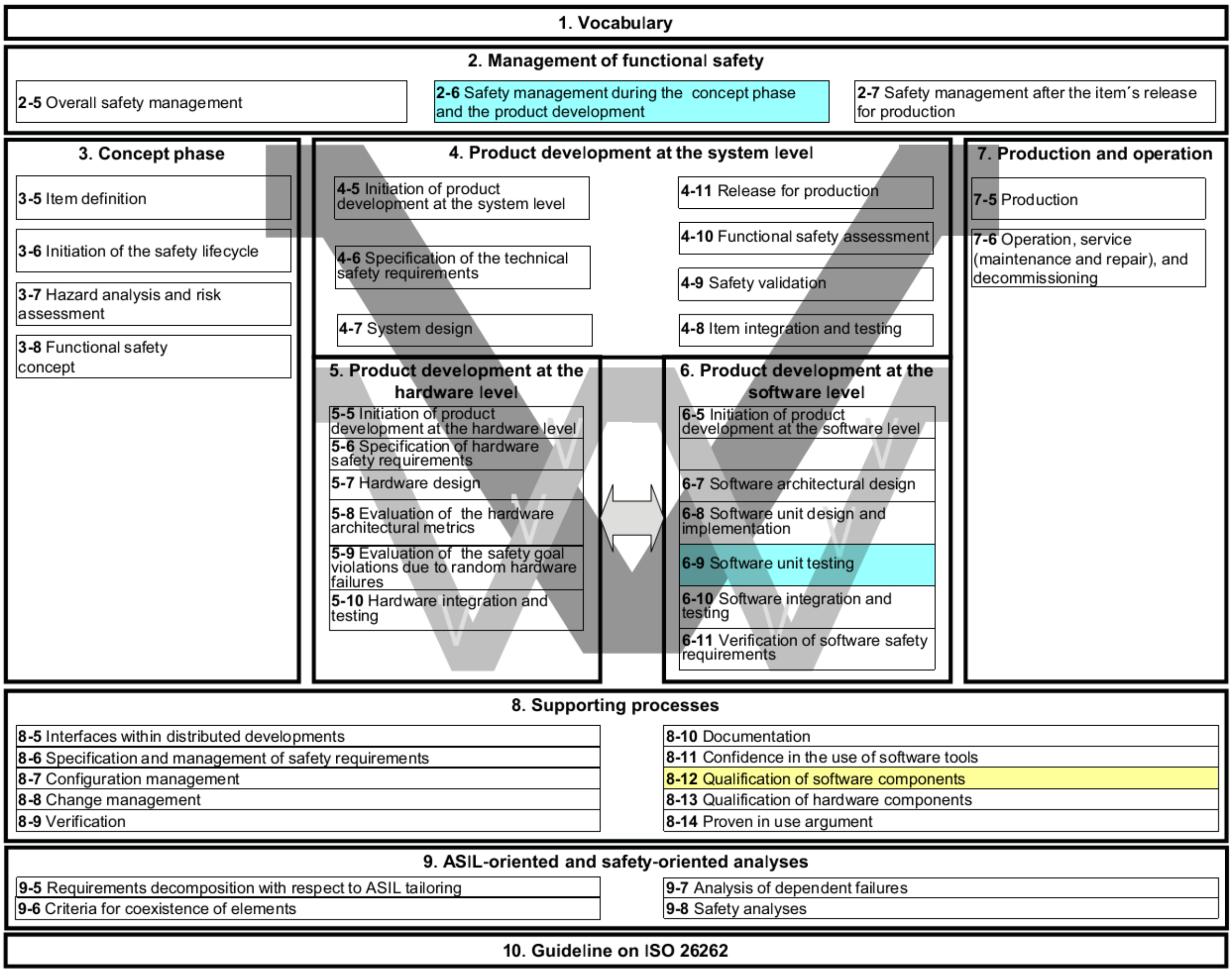
1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during the concept phase and the product development
2-7 Safety management after the item´s release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
4. Product development at the system level
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-11 Release for production
4-10 Functional safety assessment
4-9 Safety validation
4-8 Item integration and testing
7. Production and operation
7-5 Production
7-6 Operation, service (maintenance and repair), and decommissioning
5. Product development at the hardware level
5-5 Initiation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
5-9 Evaluation of the safety goal violations due to random hardware failures
5-10 Hardware integration and testing
6. Product development at the software level
6-5 Initiation of product development at the software level
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation
8-11 Confidence in the use of software tools
8-12 Qualification of software components
8-13 Qualification of hardware components
8-14 Proven in use argument
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
10. Guideline on ISO 26262

Figure 1: Overview of SW Qualification related subphases

The diagram gives an overview of the subphases (cyan) containing measures or activities explicitly required or adapted by the qualification of software components (yellow).

In order to re-use a software component that is not newly developed (e.g. COTS or previously developed components) qualification measures have to be performed to ensure a development in compliance with ISO 26262.

The qualification can help to avoid re-development of software components with similar or identical functionality resulting in reduced development costs.

The objective of the qualification is to provide evidence for the suitability of the software components to be re-used in items newly developed in compliance with ISO 26262.

5.1.1 Prerequisites and Supporting Information

As a prerequisite to the qualification for re-use the requirements of the software component have to be available.

Related work product:

- Software Safety Requirements Specification (6-6.5.1)

Covers: ISO-8-12.3.1

The design specification and the results of previous verification measures can be considered for supporting information.

Related work products:

- Software Architectural Design Specification (6-7.5.1)
- Software Unit Design Specification (6-8.5.1)
- Software Verification Report (6-11.5.3)

Covers: ISO-8-12.3.2

5.1.2 Planning of Qualification

The Safety Plan shall be refined during qualification planning to include the following information:

- Unique identification of the software component
- Maximum target ASIL of any safety requirement related to the software component
- Qualification activities to be carried out

Related work product:

- Safety Plan (8-12.5.3)

Covers: ISO-8-12.4.2.1

5.1.3 Documentation of Component

The specification of the software component shall include the following information:

- Requirements of software component
- Description of configuration
- Description of interfaces
- Application manual (if applicable)
- Description of integration
- Definition of reactions under anomalous operating conditions
- Dependencies with other software components
- Description of known anomalies and work-around measures

Related work product:

- Software Component Documentation (8-12.5.1)

Interfaces and dependencies are described during the concept phase on system and software development level. The descriptions are covered by the Item Definition (see D3.2.1.a, 5.2.2), the Hardware Software Interface Specification (see D3.2.1.a, 5.3.8.1) and the Software Architectural Design Specification (6-7.5.1).

The description of integration measures are covered by the Software Component Model (see D3.2.1.a, 4.1).

Proposal: The known anomalies can be described by an error model. The description of the work-around measures could be modeled as an additional attribute for the EAST-ADL Anomaly class.

Covers: ISO-8-12.4.3.1

Covers: WT324_REQ_4, 08_034

Covers: WT324_REQ_5, 08_035

Covers: WT324_REQ_6, 08_036

5.1.4 Activities of Qualification

The verification of the software component shall show requirement coverage (in accordance with ISO 26262-6, Clause 9) and must not result in known errors that lead to violations of safety requirements. Both normal operating conditions and the behavior in case of failure shall be covered.

The methods for structural coverage metrics at software unit level are provided in ISO 26262-6, Table 12.

The different types of behavior can be modeled in EAST-ADL using Behavior and ErrorBehavior classes.

Covers: ISO-8-12.4.3.2

The verification is only valid for an unchanged implementation of the software component.

Proposal: In the SAFE model the verification result should be linked to the unique identification of the software component to ensure the validity of the results. If the implementation is modified the requirement coverage has to be verified anew.

Covers: ISO-8-12.4.3.4

In case of target ASIL D the completeness of the test cases for the structural coverage shall be verified. If the verification result shows insufficient coverage, additional test cases shall be specified or a rationale has to be provided.

Covers: ISO-8-12.4.3.3

Proposal: The qualification activities and measures should be part of the qualification guideline.

Covers: WT324_REQ_4, 08_034

5.1.5 Documentation of Qualification

The documentation of the qualification of the software component shall include:

- Unique identification
- Unique configuration
- Person or organization responsible for the qualification
- Description of environment
- Results of verification measures

- Maximum target ASIL

The information on unique identification and maximum target ASIL are included in the refined Safety Plan.

Related work product:

- Software Component Qualification Report (8-12.5.2)

Proposal: The documentation of the qualification should be based on the standard documentation of verification results and extend its structure by qualification specific attributes.

Covers: ISO-8-12.4.3.5

Covers: WT324_REQ_4, 08_034

5.1.6 Verification of Qualification

The qualification results and the validity of these results regarding the intended use of the software component shall be verified and if necessary additional measures shall be applied.

The compliance of the specification with the requirements of the intended use of the software component shall be verified.

Proposal: The verification activities should be described in the qualification guideline.

Covers: ISO-8-12.4.4

5.1.7 Qualification Criteria

The software component can be considered as qualified if the following criteria are fulfilled:

- Specification of the software component is available
- Software component complies with its requirements (evidence available)
- Suitability of software component for intended use (evidence available)
- Software development process is based on appropriate national or international standard (evidence available)

Proposal: The criteria required to qualify a software component should be described in the guideline. Depending on the availability and validity of the evidence a property shall be assigned to the modeled software component indicating the qualification status.

Covers: ISO-8-12.4.1

5.2 Qualification of Hardware Components

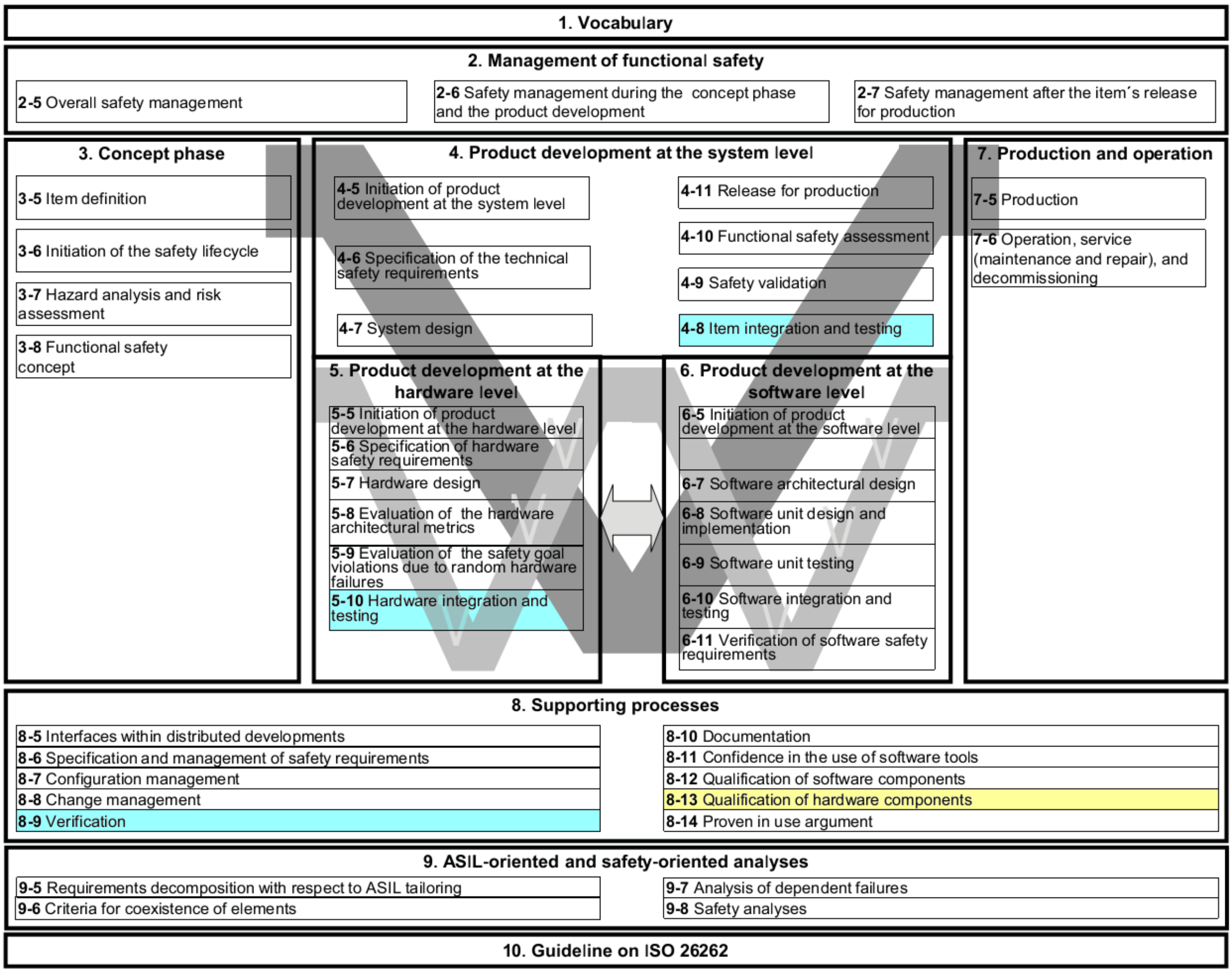
1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during the concept phase and the product development
2-7 Safety management after the item´s release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
4. Product development at the system level
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-11 Release for production
4-10 Functional safety assessment
4-9 Safety validation
4-8 Item integration and testing
7. Production and operation
7-5 Production
7-6 Operation, service (maintenance and repair), and decommissioning
5. Product development at the hardware level
5-5 Initiation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
5-9 Evaluation of the safety goal violations due to random hardware failures
5-10 Hardware integration and testing
6. Product development at the software level
6-5 Initiation of product development at the software level
6-6 Specification of software safety requirements
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation
8-11 Confidence in the use of software tools
8-12 Qualification of software components
8-13 Qualification of hardware components
8-14 Proven in use argument
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
10. Guideline on ISO 26262

Figure 2: Overview of HW Qualification related subphases

The diagram gives an overview of the subphases (cyan) containing measures or activities explicitly required or adapted by the qualification of hardware components (yellow).

Hardware components previously developed in another context have to be qualified, if they are intended to be reused.

The objective of the qualification is to verify the suitability of reuse of the hardware component as part of another item or element developed in compliance with ISO 26262.

Although every safety-related hardware component or part developed or used in compliance with ISO 26262 is subject to standard qualification measures, more complex hardware components require a qualification in accordance with ISO 26262-8, Clause 13. The applicability of the described measures is limited to intermediate hardware components or parts.

Besides the evidence for the suitability of reuse another objective of the qualification is to provide relevant information regarding failure modes, their distribution and the diagnostic capabilities of the hardware item.

The following goals shall be achieved by the qualification of an intermediate hardware component or part:

- Functional performance complies with safety concept
- Identification of failure modes and models

- Sufficient robustness
- Identification of limits of use

Although the qualification reduces the necessary safety measures in the lifecycle of the hardware component or part regarding its development the component has to be integrated and tested in accordance with ISO 26262-4 or ISO 26262-5 or both, depending on its level.

The qualification can be performed theoretically by analysis or practically by testing or by combining both methods.

5.2.1 Prerequisites and Supporting Information

The qualification of hardware components or parts requires the following information to be available:

- Related safety requirements
- Qualification criteria (analysis or tests)
- Hardware component or part specification

Related work product:

- Hardware Safety Requirements Specification (5-6.5.1)

The Hardware Safety Requirements Specification includes the test and qualification criteria.

The hardware component or part specification from the manufacturer is not developed as part of the safety lifecycle. If unavailable the requirement of the specification can be substituted with assumptions on the hardware component or part specification.

Proposal: The meta-model should provide an attribute for hardware component properties to indicate if the property is based on an assumption.

The test criteria defined in the Hardware Safety Requirements Specification can be considered as supporting information.

Covers: ISO-8-13.3

5.2.2 Qualification Criteria

The qualification in accordance with ISO 26262-8, Clause 13 shall only be applied to hardware components or parts of intermediate complexity.

Proposal: The meta-model should support an attribute for hardware components specifying their level of complexity based on the following enumeration:

- Basic part
- Intermediate part
- Intermediate component
- Complex component

As another criterion the relevant failure modes shall be verifiable by testing, analysis or both.

Proposal: The criteria required for carrying out the activities for the qualification of hardware components or parts should be part of the guideline.

Covers: ISO-8-13.4.1.1

Covers: WT324_REQ_7, 08_037

5.2.3 Planning of Qualification

The qualification of hardware components or parts shall be planned, describing the following information:

- Identification and version of hardware component or part
- Specification of environment (intended use)
- Qualification strategy and rationale
- Necessary tools required by strategy
- Responsible person or party to carry out qualification strategy
- Assessment criteria for qualification

Related work product:

- Qualification Plan (8-13.5.1)

Proposal: The input required and the necessary information provided by the qualification plan including the assessment criteria should be part of the guideline.

Covers: ISO-8-13.4.4.1

Covers: WT324_REQ_7, 08_037

5.2.4 Qualification Argument

The qualification shall show compliance of the performance of the hardware component or part with its specification. The comprehensive argument shall include information on the behavior in normal environmental conditions and in combination with assumed failure initiating events.

The argument shall be based on a combination of the following types of information, whereas a rationale has to be given for each assumption or extrapolation:

- Results of analytical methods and assumptions
- Data from operational experience
- Results of previous tests

Proposal: The SAFE model should support a description of rationales to be given for assumptions or elements based on assumptions.

Covers: ISO-8-13.4.5

5.2.5 Qualification by Analysis

A qualification through analysis relies on a rationale for the analytical methods and assumptions used. The analysis can be used for the extrapolation of testing data and to determine the effects of smaller changes in the already tested hardware component.

The following aspects shall be considered by the analysis:

- All environmental conditions the component is exposed to
- Limits of the environmental conditions
- Additional operational strains

The analysis shall be expressed in a comprehensible form by using extrapolations, mathematical models, damage analysis or similar analytical methods.

Related work product:

- Qualification Report (8-13.5.3)

Covers: ISO-8-13.4.6

Covers: WT324_REQ_7, 08_037

5.2.6 Qualification by Testing

A qualification through testing assesses the compliance of the hardware component or part with its functional requirements under the intended environmental and operational conditions.

The qualification has to consider the limits of the accuracy of the test results caused by deviations of environmental conditions or extrapolation errors.

The test plan shall contain the following information:

- Description of functions
- Number and sequence of planned tests
- Requirements for assembly and connections
- Procedure for accelerated ageing
- Simulated operating and environmental conditions
- Pass/fail criteria
- Measured environmental parameters
- Requirements for testing equipment
- Maintenance and replacement processes during testing

The results of the test shall be included in the Qualification Report.

Related work products:

- Hardware Component Test Plan (8-13.5.2)
- Qualification Report (8-13.5.3)

Covers: ISO-8-13.4.7.1

Covers: ISO-8-13.4.7.3

A standardized test specification shall be used, which can be based on the ISO 16750 series or equivalent company standards.

Proposal: The SAFE model should support references to external test specifications that can be linked to a test plan.

Covers: ISO-8-13.4.7.2

Based on the test results and the results of the analysis it shall be documented in the Qualification Report whether the hardware component or part has passed or failed the qualification.

The Qualification Report shall then be verified in accordance with ISO 26262-8, Clause 9.

Proposal: The required validation and verification measures should be described in the guideline. Depending on the results of testing and analysis a property shall be assigned to the modeled hardware component indicating the qualification status.

Covers: ISO-8-13.4.8

5.3 Proven In Use Argument

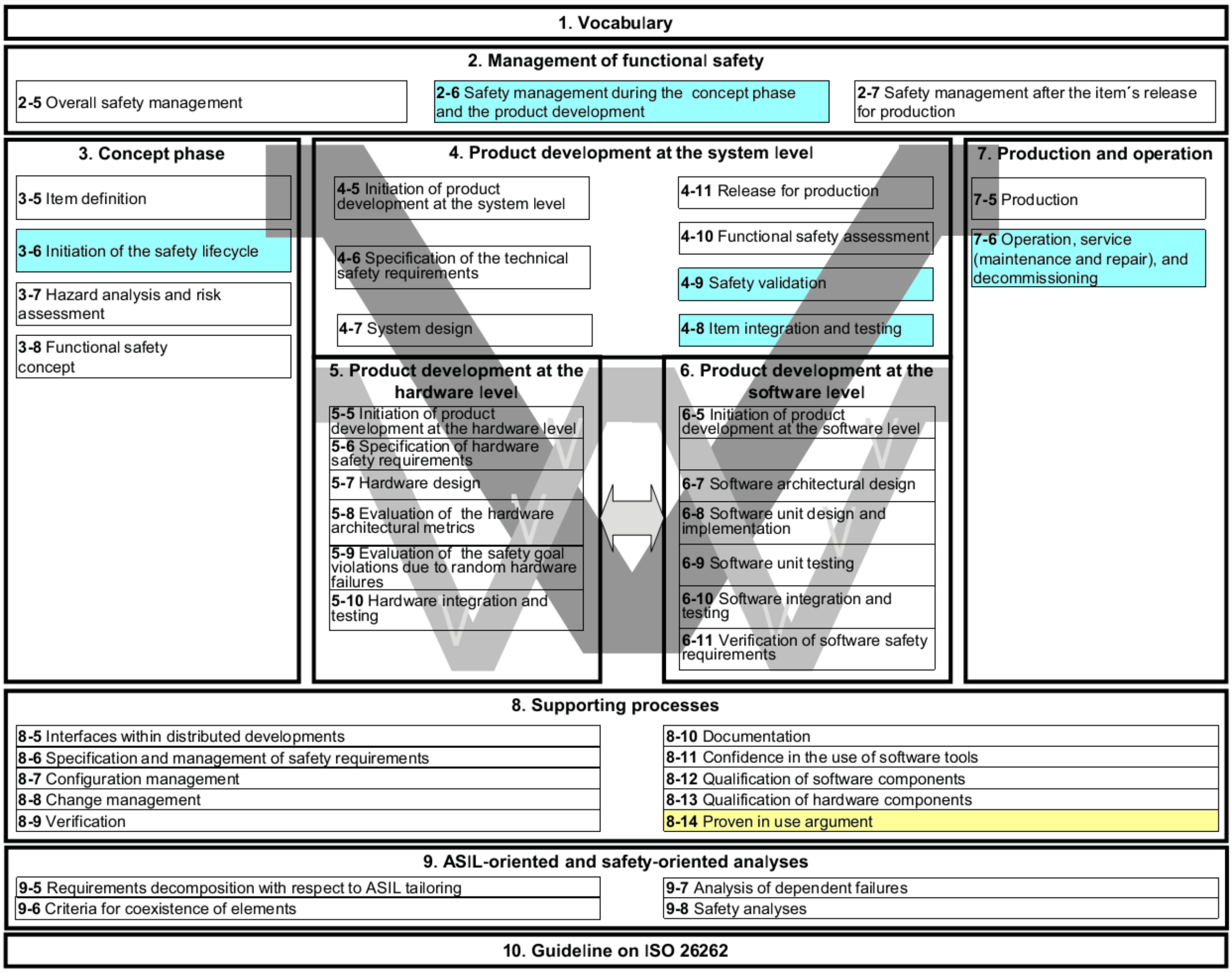
1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during the concept phase and the product development
2-7 Safety management after the item´s release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
4. Product development at the system level
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-11 Release for production
4-10 Functional safety assessment
4-9 Safety validation
4-8 Item integration and testing
7. Production and operation
7-5 Production
7-6 Operation, service (maintenance and repair), and decommissioning
5. Product development at the hardware level
5-5 Initiation of product development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
5-9 Evaluation of the safety goal violations due to random hardware failures
5-10 Hardware integration and testing
6. Product development at the software level
6-5 Initiation of product development at the software level
6-6 Specification of software safety requirements
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation
8-11 Confidence in the use of software tools
8-12 Qualification of software components
8-13 Qualification of hardware components
8-14 Proven in use argument
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analyses
10. Guideline on ISO 26262

Figure 3: Overview of subphases related to Proven in Use Argument

The diagram gives an overview of the subphases (cyan) containing measures or activities explicitly required or adapted by the proven in use argumentation (yellow).

The proven in use argument can be considered for items or elements intended to be re-used, which are already in operation and providing sufficient field data is available. It can be applied to identical or similar items or to related work products.

The proven in use argument serves as an alternate means of compliance with ISO 26262 and can reduce development effort by substitution of safety lifecycle subphases with the proven in use credit.

Safety management activities that are related to integration measures or the results of the proven in use argument are not covered by the proven in use credit.

The motivations for the proven in use argument include:

- Automotive application carried over to another target
- Additional function implemented in ECU
- Candidate developed prior to release of ISO 26262
- Candidate used in another safety-related industry
- Widely used COTS product

The proven in use argument addresses two main criteria:

- Relevance and sufficiency of field data
- Safety-related impact of changes to the candidate since the service period

Covers: WT324_REQ_2, 04_065

5.3.1 Prerequisites and Supporting Information

The preparation of the proven in use argument requires information on the candidate. From the previous service period of the candidate field data shall be available. Regarding the intended use of the candidate the following information is required:

- Specification of candidate
- Safety goals or safety requirements with ASIL
- Intended operating modes and interfaces
- Foreseeable operational situation

If the safety case of the previous use of the candidate was developed in accordance with ISO 26262-2, 6.5.3 it can be considered as supporting information.

Since the proven in use argument can be applied to a candidate that may not have been developed in accordance with ISO 26262, some work products of the safety case might not be available. In this case missing work products regarding the safety case can be substituted by equivalent data from the development of the candidate.

Proposal: In case the proven in use candidate was not developed according to SAFE methodology all relevant characteristics of the candidate should be modeled based on the external input (candidate specification, safety requirements, interface description).

The SAFE model should support the substitution of work products normally required by the safety lifecycle in order to cover candidates not developed in accordance with ISO 26262. An attribute could be assigned to a work product describing if it was substituted by (referenced) external data.

Covers: ISO-8-14.3

5.3.2 Proven In Use Credit

The proven in use argument allows subphases of the development of the proven in use candidate to be omitted. If the field data and changes to the candidate comply with the requirements of the proven in use argument the activities and work products of the subphases can be substituted by the proven in use credit.

The planning of the proven in use credit shall be part of the Safety Plan in accordance with ISO 26262-2, 6.4.3.5.

Related work product:

- Safety Plan (8-14.5.1)

Covers: ISO-8-14.4.2.2

The proven in use credit shall be limited to the safety lifecycle subphases and activities covered by the proven in use argument of the candidate. It can be applied to subphases and activities of the development of the proven in use candidate but does not cover the integration of the candidate in new items or elements. Therefore the following measures have to be performed in order to maintain the proven in use credit:

- Integration and testing measures in accordance with ISO 26262-4, Clause 8
- Safety validation of the item embedding the proven in use candidate in accordance with ISO 26262-4, Clause 9
- Confirmation measures of the item embedding the proven in use candidate in accordance with ISO 26262-2, 6.4.7

Proposal: The description of the limitations of the proven in use credit should be part of the guideline for the proven in use argument.

Covers: ISO-8-14.4.2.3 - ISO-8-14.4.2.6

5.3.3 Information on Candidate

A description of the candidate and its previous use shall be available.

The information shall at least include:

- Identification and traceability with description of internal elements
- Fit, form and function requirements describing candidate characteristics
- Safety requirements and corresponding ASILs of previous use

Related work product:

- Description of candidate for proven in use argument (8-14.5.2)

Covers: ISO-8-14.4.3.1

5.3.4 Analysis of Changes

Changes to the proven in use candidate affect the applicability of the proven in use credit. All changes have to be analyzed in order to be able to decide whether the proven in use credit covers these changes or not.

The following types of changes shall be considered for the identification of changes to the candidate and its environment:

- Changes to the candidate's design
- Changes to the candidate's implementation
- Changes to the configuration or calibration data
- Changes to the environment

Different measures have to be applied depending on the architectural level of the proven in use candidate.

Changes to an item or its environment introduced for the purpose of future application require an impact analysis to be performed. If necessary the safety lifecycle has to be tailored in accordance with ISO 26262-3, 6.4.2.

Changes to an element or its environment intended to be used in a different item shall be subject to change management in accordance with ISO 26262-8, Clause 8.

All changes to a candidate that are independent of future applications and introduced after the candidate's service period shall provide evidence that the proven in use status remains valid.

The results of the analysis of all changes to the candidate and its environment shall be documented.

Related work product:

- Proven in use analysis reports (8-14.5.3)

Proposal: The activities and measures required by the analysis depending on the type and architectural level of the changes to the candidate or its environment should be described in the guideline.

Covers: ISO-8-14.4.4

5.3.5 Analysis of Field Data

The field data of the service period of the proven in use candidate shall be analyzed in view of failures caused by the candidate with the potential to cause a violation of a safety goal.

Evidence shall be provided that the candidate has been kept under configuration management and change management during and after its service period.

Covers: ISO-8-14.4.5.1

The service period of the candidate shall be calculated as the sum of the observation periods of all specimens with a sufficient duration of their observation period. Only specimens with an observation period exceeding the average yearly vehicle operation time shall be considered for the calculation of the service period.

Covers: ISO-8-14.4.5.2.2, ISO-8-14.4.5.2.3

A rationale for the calculation of the service period shall be available.

Covers: ISO-8-14.4.5.2.1

Depending on the ASIL assigned to the candidate a limit is defined for the incident rate. If no ASIL is assigned to the candidate the limits for ASIL D shall be applied.

ASIL	Observable incident rate
D	$< 10^{-9}$/h
C	$< 10^{-8}$/h
B	$< 10^{-8}$/h
A	$< 10^{-7}$/h

The service period shall comply with each safety goal related to the candidate based on the limit of the incident rate with a single-sided lower confidence level of 70% (chi-square distribution).

The minimum service period required has to be calculated based on the number of safety-related incidents.

ASIL	Minimum service period without observable incident
D	$1.2 * 10^{9}$ h
C	$1.2 * 10^{8}$ h
B	$1.2 * 10^{8}$ h
A	$1.2 * 10^{7}$ h

Covers: ISO-8-14.4.5.2.4

If the field data available does not cover the minimum service period required to obtain the proven in use status the proven in use credit may be anticipated provisionally.

In this case the field data of the service period is checked against an increased limit for the incident rate, which allows an incident rate three times higher than the limit for the proven in use status, resulting in a decreased minimum service period required for the interim period.

Covers: ISO-8-14.4.5.2.5

If an incident is observed during the interim period one of the following two measures has to be taken:

- The limit for the observable incident rate used for the interim period shall be replaced by the more strict value according to ISO 26262-8, 14.4.5.2.4
- Evidence that the cause of the observed incident is fully identified and eliminated in accordance with ISO 26262 shall be provided and recorded in the safety case

Covers: ISO-8-14.4.5.2.6

In case the failure rate of the candidate shows a non-constant distribution, additional measures such as dedicated endurance tests or a longer observation period shall be applied to compensate the higher variance of the failure rate.

Covers: ISO-8-14.4.5.2.7

Any incident caused by the candidate and observed during the period of operation shall be recorded if the incident has the potential to lead to a violation of a safety goal.

If it is intended to apply the proven in use argument in future development processes the field monitoring process for functional safety incidents related to the item shall ensure the validity of the field data in accordance with ISO 26262-7, 6.4.2.1.

Covers: ISO-8-14.4.5.3

The analysis of the field data and its results shall be documented.

Related work product:

- Proven in use analysis reports (8-14.5.3)

Covers: ISO-8-14.4.5

Proposal: The activities and measures required by the analysis of field data of the proven in use candidate should be part of the guideline. The description should include the calculation of the minimum service period and the criteria for a provisionally proven in use credit.

Proposal: The SAFE model should support information on incidents within the field data. The technical characteristics of the incident could be provided using an error model extended by hazard related information.

5.4 Well-trusted Design Principles

For technical solutions introduced to reduce systematic failures, the Safe product shall allow to specify the compliance of the solution to well-trusted automotive systems design principles.

For requirements assigned with ASIL D, a justification must be provided in case the technical solution is not implementing a well-trusted design principle.

Proposal: An attribute should be assigned to system design elements to indicate if a well-trusted design principle is used for the development of the element. The status (well-trusted) shall be assigned depending on the result of the impact analysis. Additionally the SAFE model should provide means to apply a rationale to system designs used for justification.

Covers: WT324_REQ_1, 04_064

Covers: ISO-4-7.4.3.4, ISO-4-7.4.3.6

An impact analysis shall verify the suitability of the well-trusted design principle applied to the technical solution. The impact analysis has to consider the underlying assumptions and shall include:

- Capability and feasibility of determined diagnostics
- Environmental constraints
- Timing constraints
- Compatibility of determined resources
- Robustness of system design

Covers: ISO-4-7.4.3.5

5.5 Meta Model Requirements and Proposed Extensions

This chapter contains proposals for meta-model enhancements not specifically related to one of the preceding chapters, but more general requirements the qualification of a component or the proven in use argument have in common.

5.5.1 Re-use and Qualification

The SAFE model should provide an attribute to identify reused or qualified components. The DevelopmentCategory enumeration could therefore be extended:

- new
- modified
- reused with modifications
- reused without modifications

An attribute QualificationStatus should be assignable to Safe items and related work products using the following enumeration values:

- unqualified
- qualified
- proven in use (provisionally)
- proven in use
- well-trusted

- **Covers**: WT324_REQ_3, 05_003

5.5.2 External Data

The meta-model should support specifications or data from external sources.

This is required by:

- Qualification of software components:
  - Requirement specification of re-used software component (8-12.3.1)
  - Design specification of re-used software component (8-12.3.2)
  - Results of previous verification measures (8-12.3.2)
  - Application Manual of re-used software component (8-12.4.3.1)
- Qualification of hardware components:
  - Hardware component or part specification (8-13.3.1)
- Proven in use argument:
  - Field data from previous service period (8-14.3.1)

6 Proposed Meta-Model Extension

In this chapter a proposal for the meta-model extension towards COTS is presented.

6.1 General extension of existing Elements

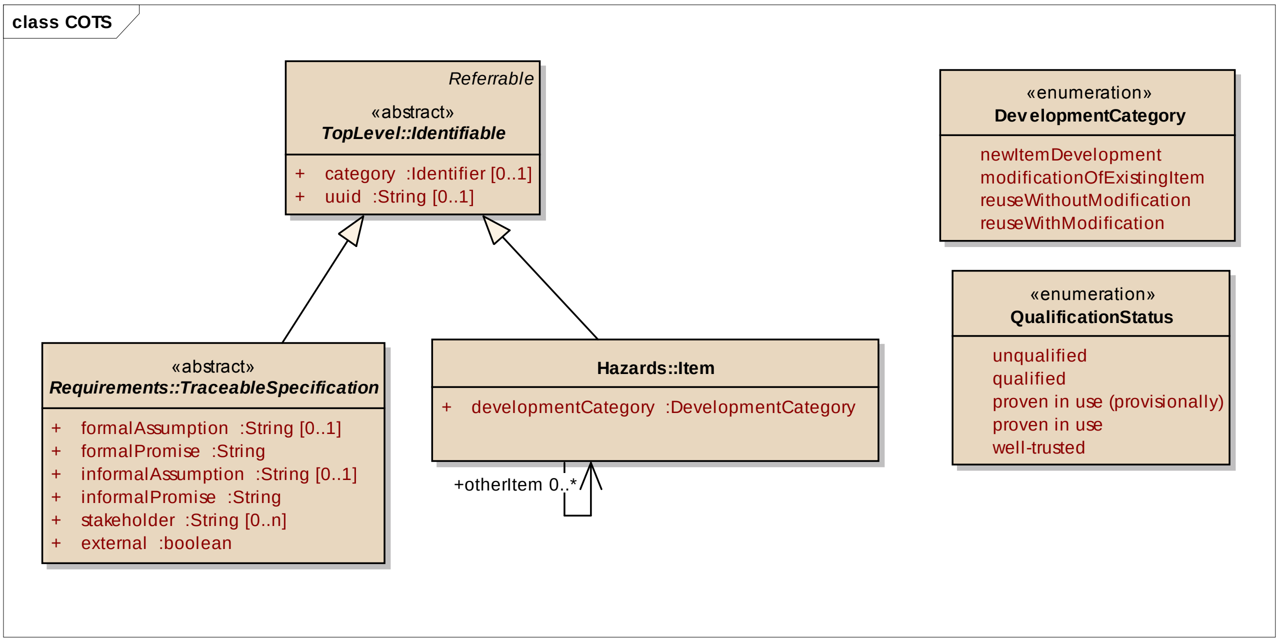

Figure 4 General meta-model extension for COTS qualification

To support re-useable components in the SAFE meta-model a few modifications on existing elements are necessary. Each item is extended with a development category to indicate if the item is a new development or has been already in use. Furthermore the traceable specification is extended with a separation of the formal and informal specification into assumptions and promises. This distinction enables to state the assumption, which must be valid, for each requirement in order to guarantee the promise. Therefore a matching can be performed from the assumed required properties of the component that needs to be integrated, to the assumptions made in the item development process.

6.2 Extension for HW Qualification

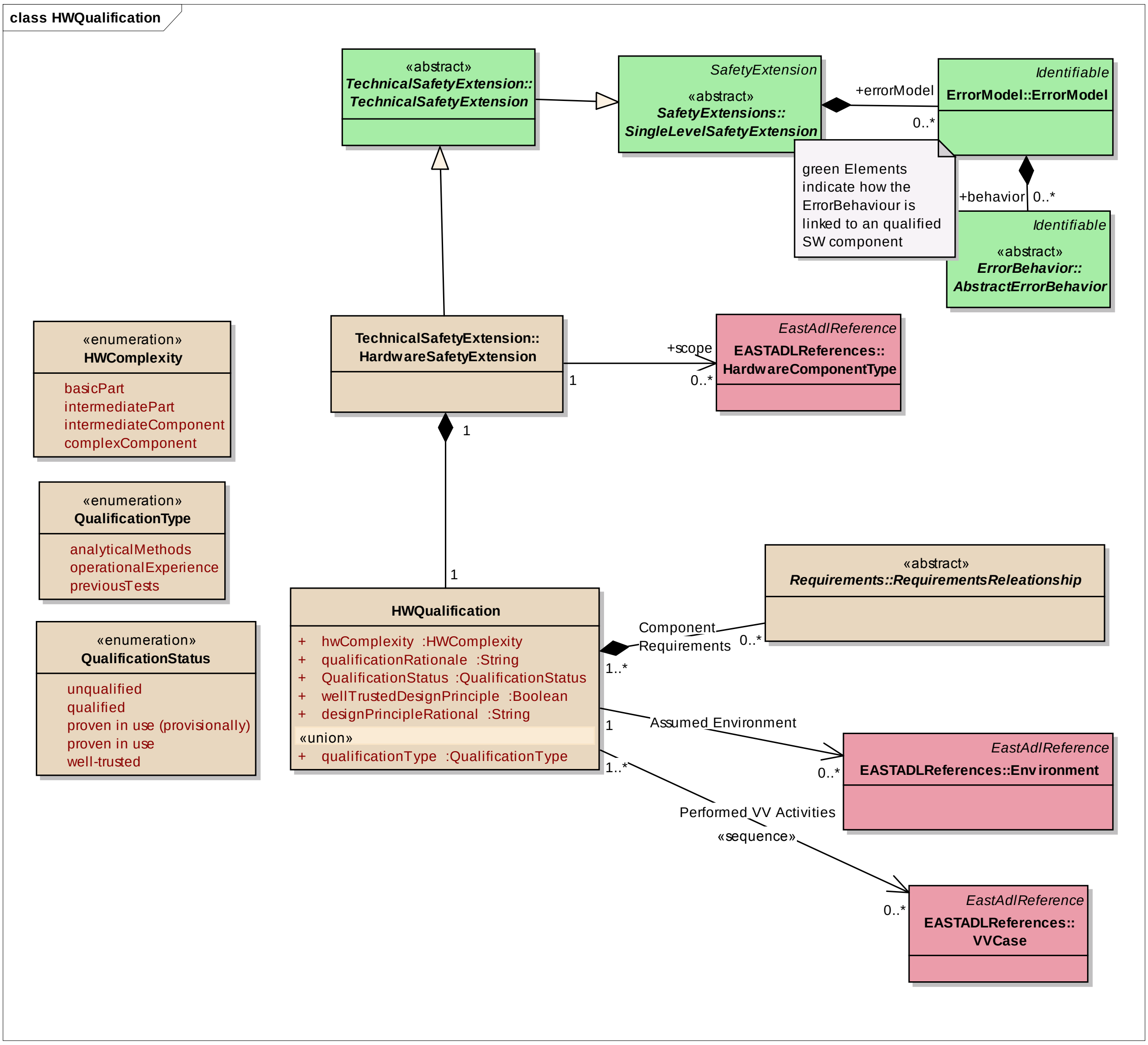

Figure 5 Meta-model extension for HW COTS qualification

The hardware safety extension of the SAFE meta-model is extended with a new class called HWQualification. This class includes all relevant qualification information. In particular, it aggregates a set of requirement links to point to the requirements that are specific to the integrated component, but are not necessarily relevant for the item. To separate between these two types an additional set of links is necessary.

For each HWQualification the complexity of the hardware which needs to be qualified is defined in a configured enumeration. Also the type of the qualification is stored; multiple elements from the enum shall be selectable.

Also, it can be specified if well-trusted design principles have been used. In addition to the Boolean flag which can be used for filtering purpose, also a rational can be stored, giving a first overview of which design principles had been applied.

To identify the assumed environment of the component an EAST-ADL model, including an environmental specification, can be referenced. Also all the already performed VVCases can be linked.

6.3 Extension for SW Qualification

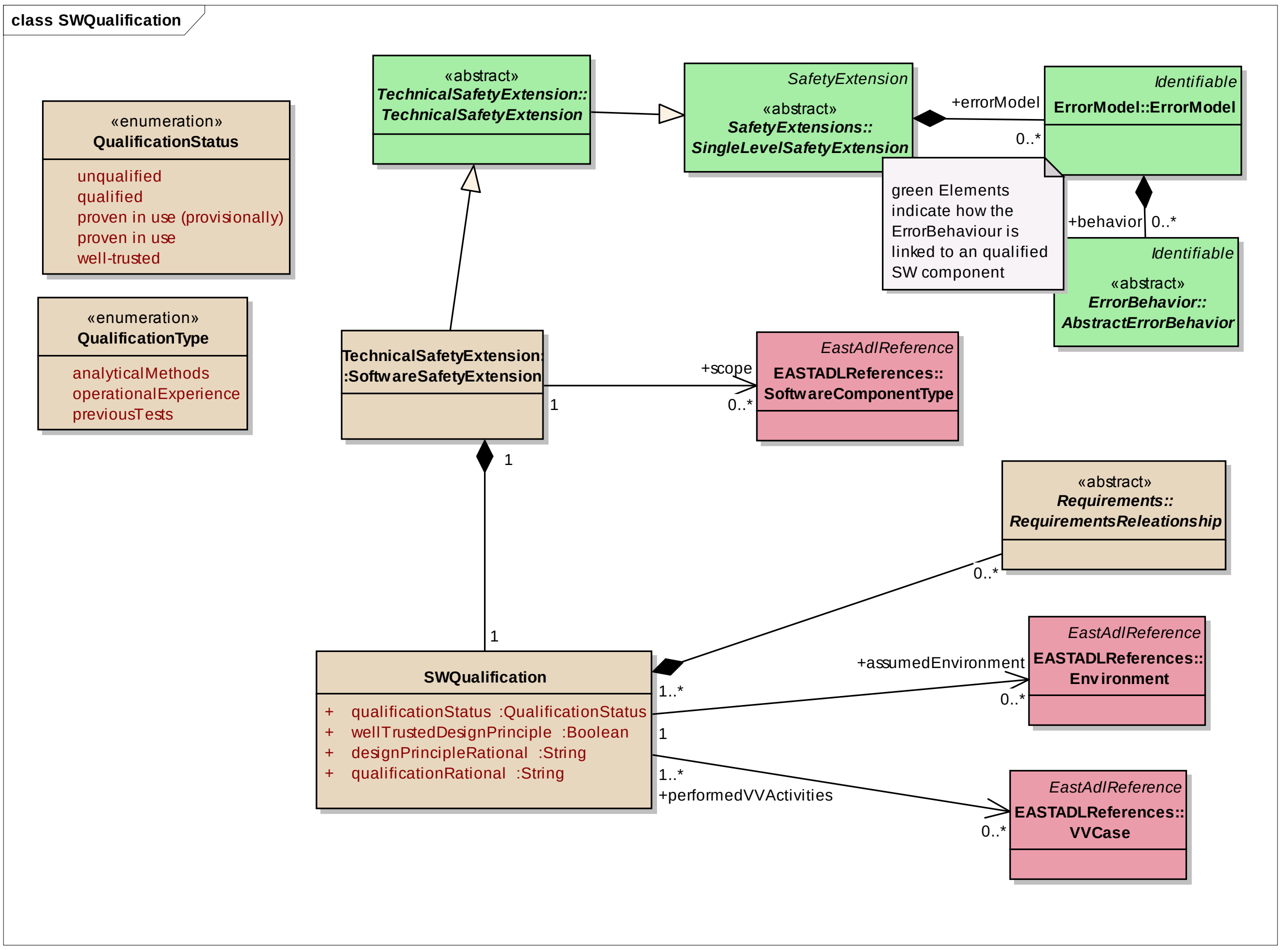

Figure 6 Extension for SW COTS qualification

The software qualification component is designed identically to the HWQualification class.

Exceptions are the missing HWComplexity attribute which does not apply for software. Also the qualification type has been removed since this distinction is not explicitly stated for SW Components in the ISO 26262.

6.4 Extension for Proven in Use

Since a proven in use argumentation can be performed at many phases of the safety lifecycle, the abstract SingleLevelSafetyExtension is extended with a proven in use argument. This argument does not aggregate the collected FieldData itself, but links to them. Furthermore, it is able to identify the elements that have been changed in comparison to the element being in long term use. Also changes to the environmental assumptions can be captured.

There are two references to verification and validation activities from the EAST-ADL verification package. One reference identifies the verification case representing the impact analysis of the changes the other reference identifies all the integration verification activities.

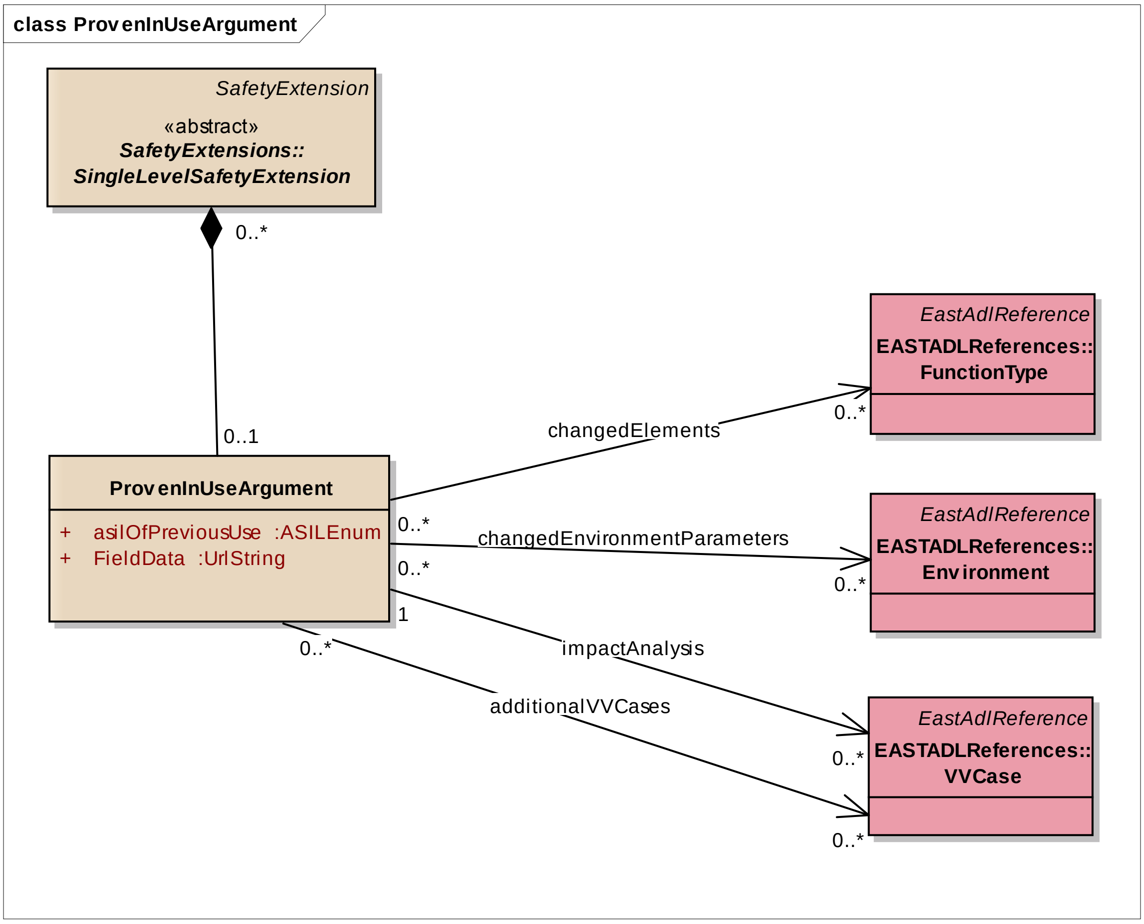

Figure 7 Extension of the meta-model regarding the proven in use argumentation

7 Conclusions and Discussion

This document shall provide an overview about the criteria for the integration of COTS products and the information required on re-use components as well as proposals for meta-model enhancements, including new and extended meta-model elements or data types (e.g. enumerations) to provide means necessary for re-use related component description.

The deliverable D3.2.4.b also defines content not represented in the SAFE model, that shall be part of a guideline providing criteria definitions and supporting information on activities and measures for the qualification of components and the application of the proven in use argument.

The proposed meta-model enhancements for hardware and software elements have to be synchronized with the meta-model extensions of WT3.2.1 and WT3.2.2 in order to harmonize the model properties required for the description of re-use related information.

8 References

[1] International Organization for Standardization: ISO 26262 Road vehicles - Functional safety. (2011)

[2] ATESST2: EAST-ADL Domain Model Specification (v2.1, 2010)

[3] D3.2.1.a: Proposal for extension of meta model for software and system modeling

[4] D3.2.4.a: Definition of COTS integration guideline and description for SW and HW

9 Acknowledgments

This document is based on the SAFE and SAFE-E projects. SAFE is in the framework of the ITEA2, EUREKA cluster program Σ! 3674. The work has been funded by the German Ministry for Education and Research (BMBF) under the funding ID 01IS11019, and by the French Ministry of the Economy and Finance (DGCIS). SAFE-E is part of the Eurostars program, which is powered by EUREKA and the European Community. The work has been funded by the German Ministry of Education and Research (BMBF) and the Austrian research association (FFG) under the funding ID E!6095. The responsibility for the content rests with the authors.