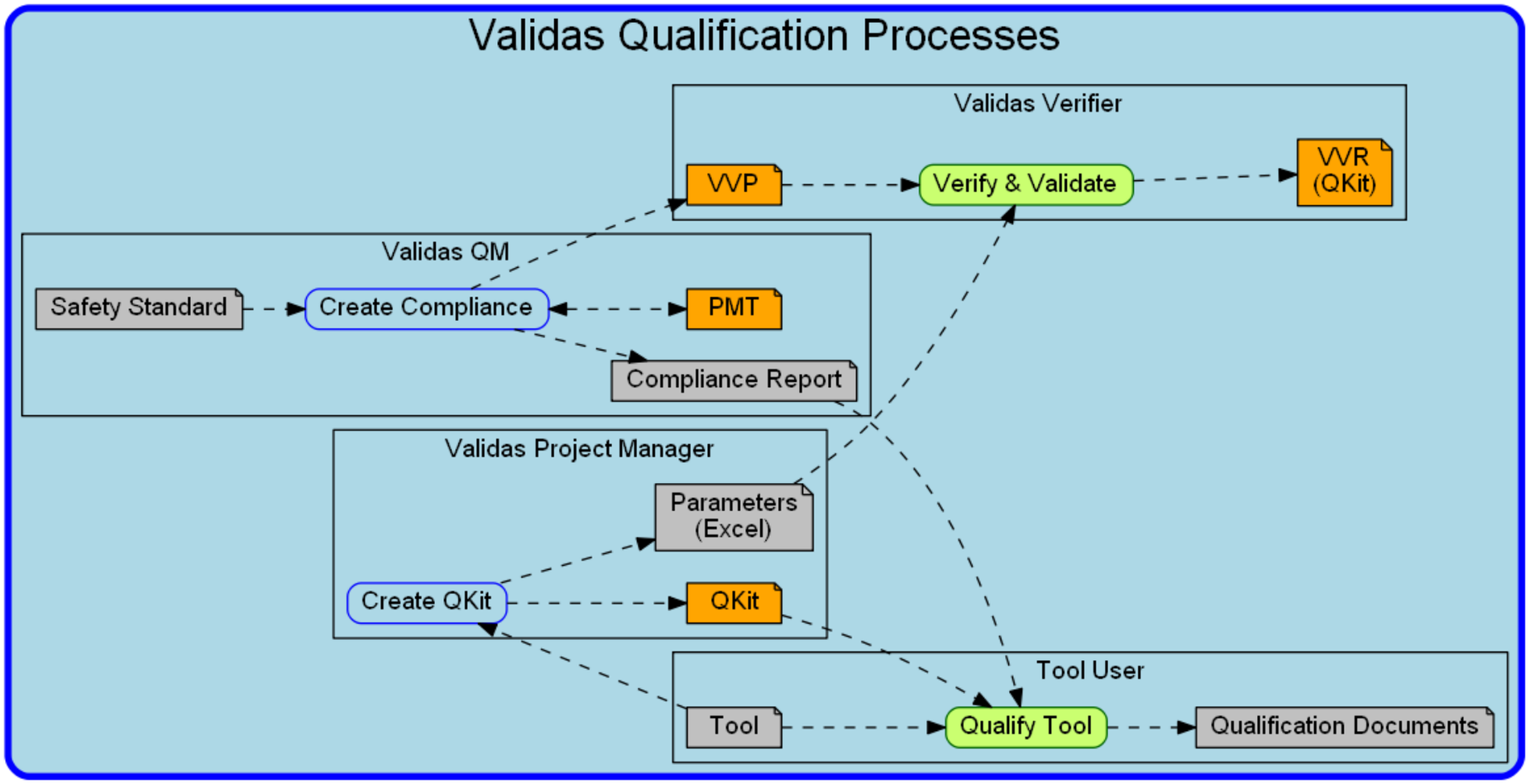


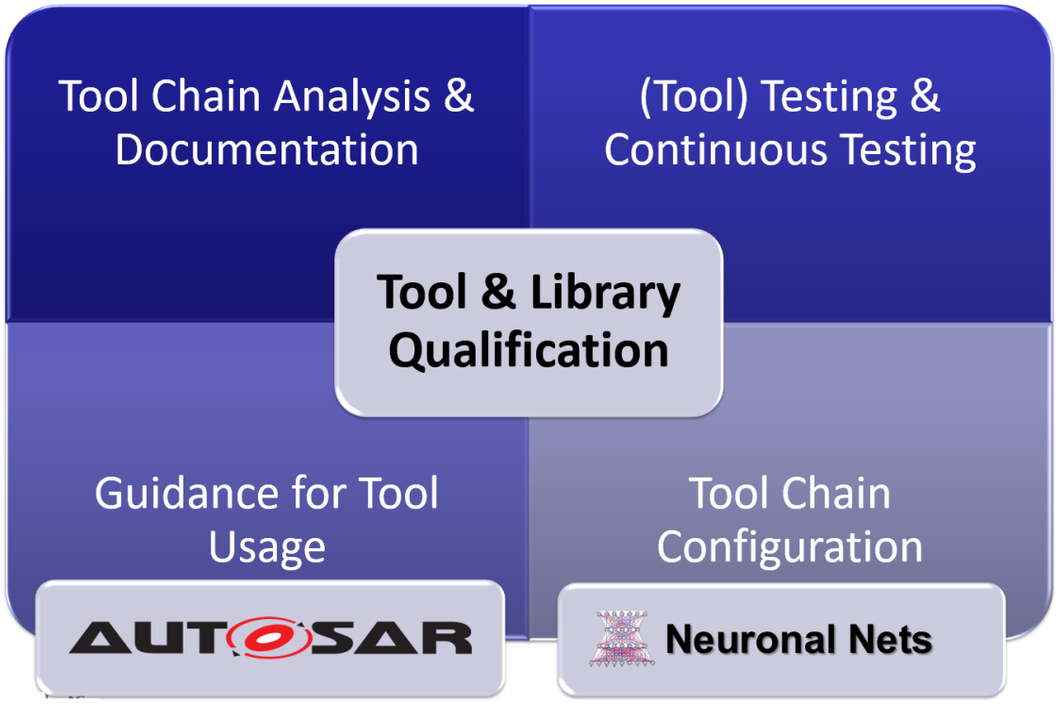
Oscar Slotosch, Validas AG

Reference and Qualification Processes

Validas AG About Us

- Our passion: guiding to build safe systems worldwide
- Our contribution: safe tools, safe methods and safe libraries.

- We are specialized on **tool and library qualification**



Contents

- **Reference Process**
  - Motivation
  - Solution
  - Process Modelling Tool (PMT)
- Tool Qualification Processes
- Process Compliance
- Summary

Motivation

- **Model & Modeling languages & tools are very powerful, e.g. UML, SYSML**
- **Modeling process has many phases**
  - Requirements Specification
  - Interface Specification
  - Design Specification
  - Implementation
- **Hard to describe processes precisely:**
  - Name: Architecture Specification
  - Input: UML-Model,
  - Output UML-Model,
  - Description: Model Architecture using Class Diagrams

- **Descriptions not verifiable:**
  - Is a modeled architecture OK?
  - Is modeling language used correctly?
- **Process descriptions sometimes not useful for practical applications**

Solution: Use Models

- **Use models for formalization of model-based processes**
- **Model captures**
  - Requirements, e.g. ISO 26262 (and compliances)
  - Processes
  - Models (using Meta Model)
  - Parameters
  - Tailoring
- **Provides all advantages of models for processes**
  - Precise definition
  - Static validation
  - Semantic Validation

Goals of Process Modeling Tool

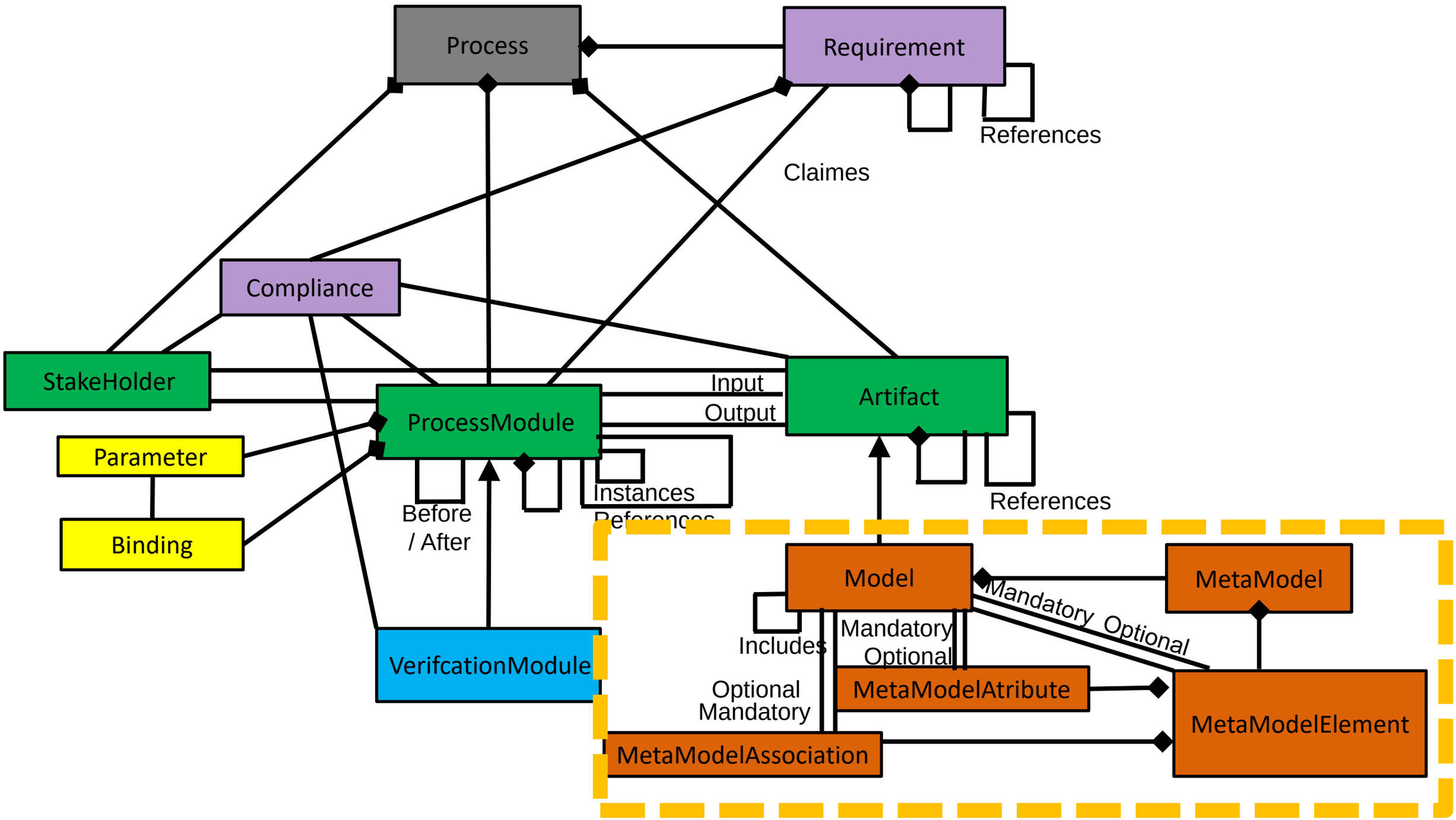
Goals: Making Safety Easier & Safer

- **Formalize & improve processes**
- **Show compliance with safety standards (Safety Plan)**
- **Support achieving compliance (Safety Case)**
- **Document processes**

Features:

- **Model processes (with BPMN like visualization)**
- **Validate processes (syntactically) for consistency and completeness**
- **Generate process & compliance reports**
- **Generate Verification & Validation Plans (for separate VVT)**
- **Can be used for modelling of model-based processes**
- **Has been used to certify Validas qualification processes**
- **Will be open source soon**

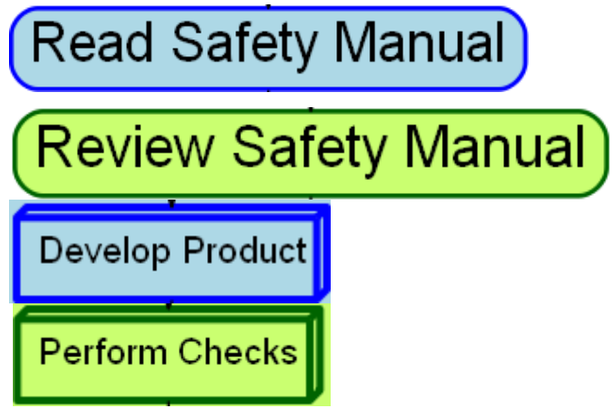
Model for Parameterized and Compliant Model-Based Processes

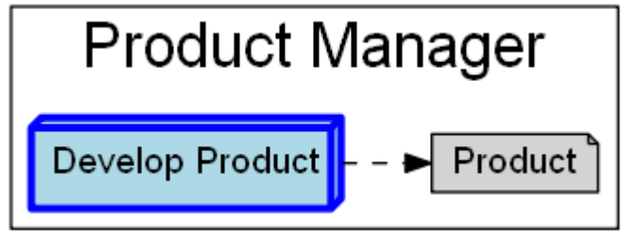


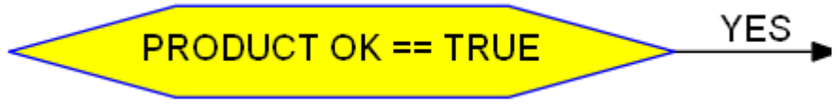
Graphical Notation

Elements

- Process Module: blue, rounded box:
- Verification Module: green, rounded box:
- Hierarchical Process Module: blue folders:
- Hierarchical Verification Module: green folders:
- Artifact: Grey box with note:
- Model: Orange box with note:
- StakeHolder: transparent box:
- Conditions: yellow routes:

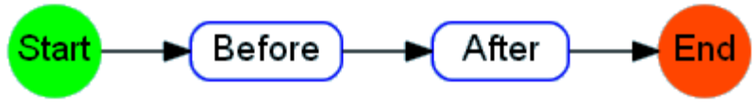






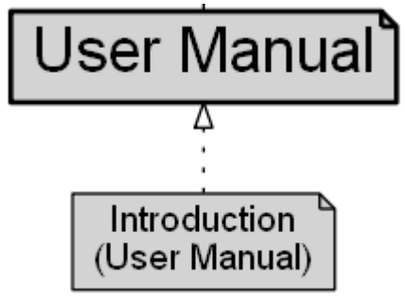
Relations

- Before After: solid arrow:
- Read/Write: dashed arrow:
- Artifact Containment: dotted arrow:

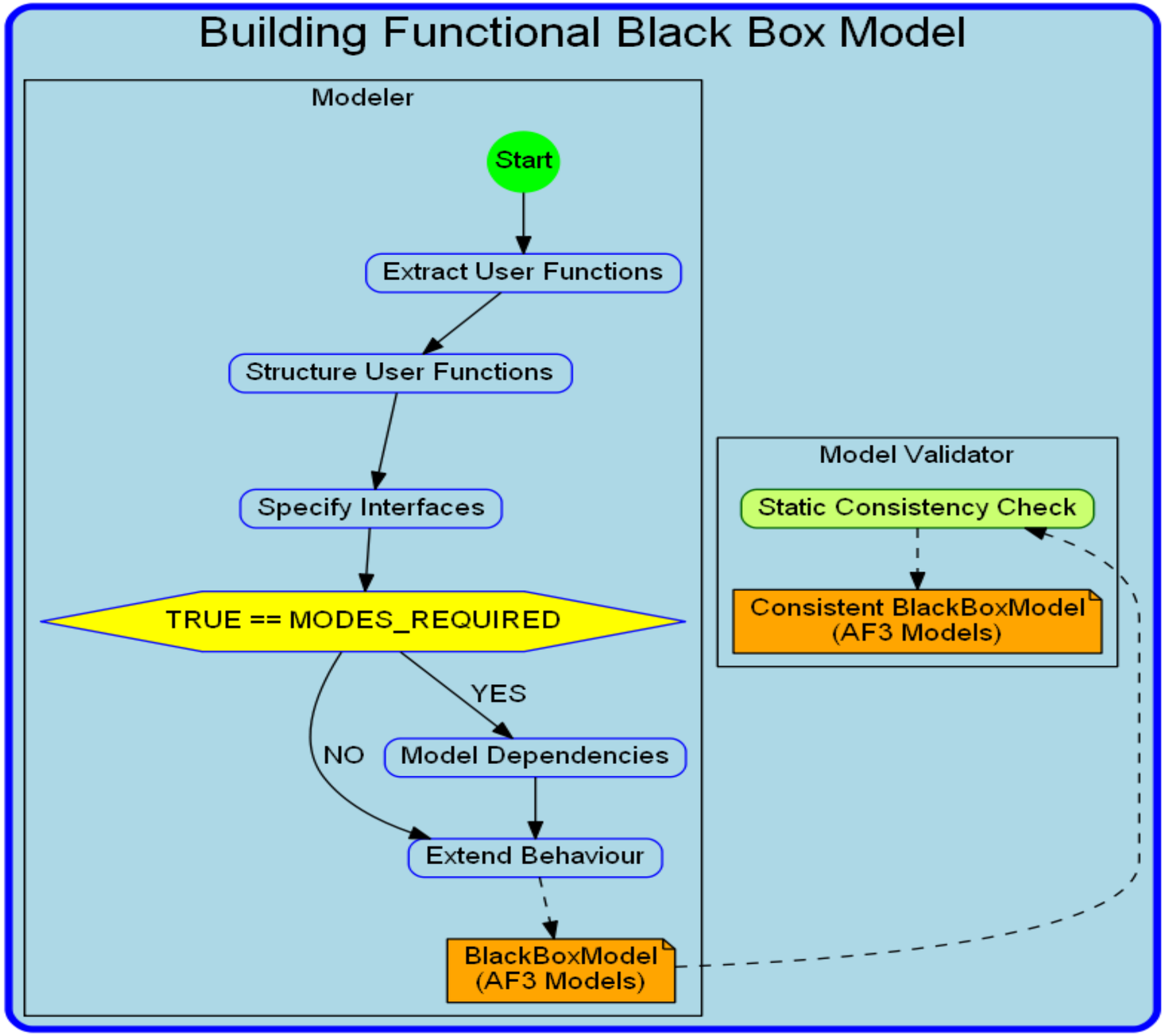


Default

- Start & End



Process Example (SPEDIT)



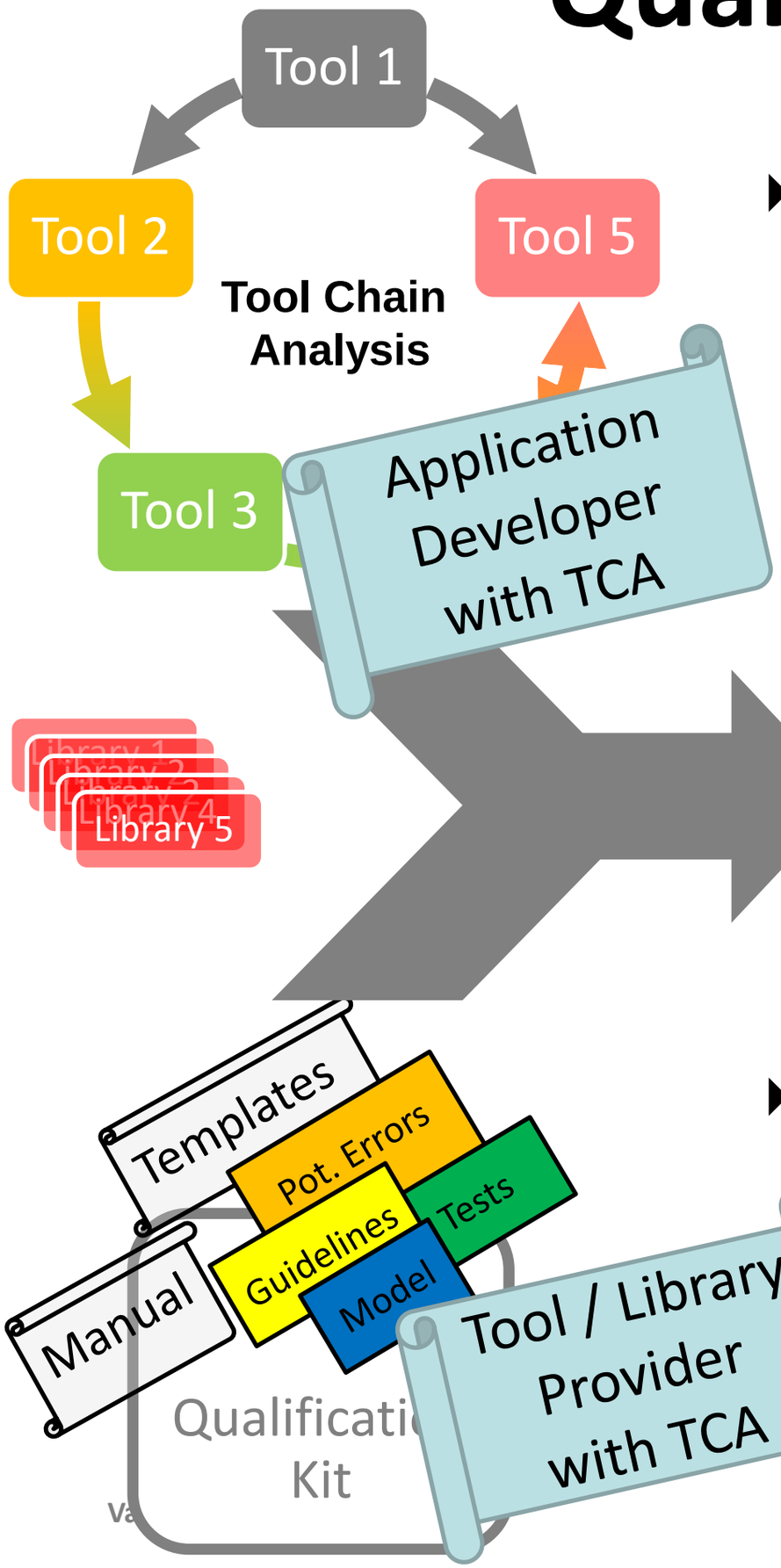
Advantages

- **Technically:**
  - Precise Definition
  - Syntactic Validation (Automatically)
  - Semantic Validation: Check Lists
- **Methodically:**
  - Clarification of process & models using meta-model:
    - What is allowed?
    - What is optionally?
    - What is forbidden?
  - Precise documentation of process
  - Basis for tools support: Is this a valid architecture?
  - Formalization / Modelling triggers valuable discussions
- **Argue & document compliance with requirements, e.g. ISO 26262**

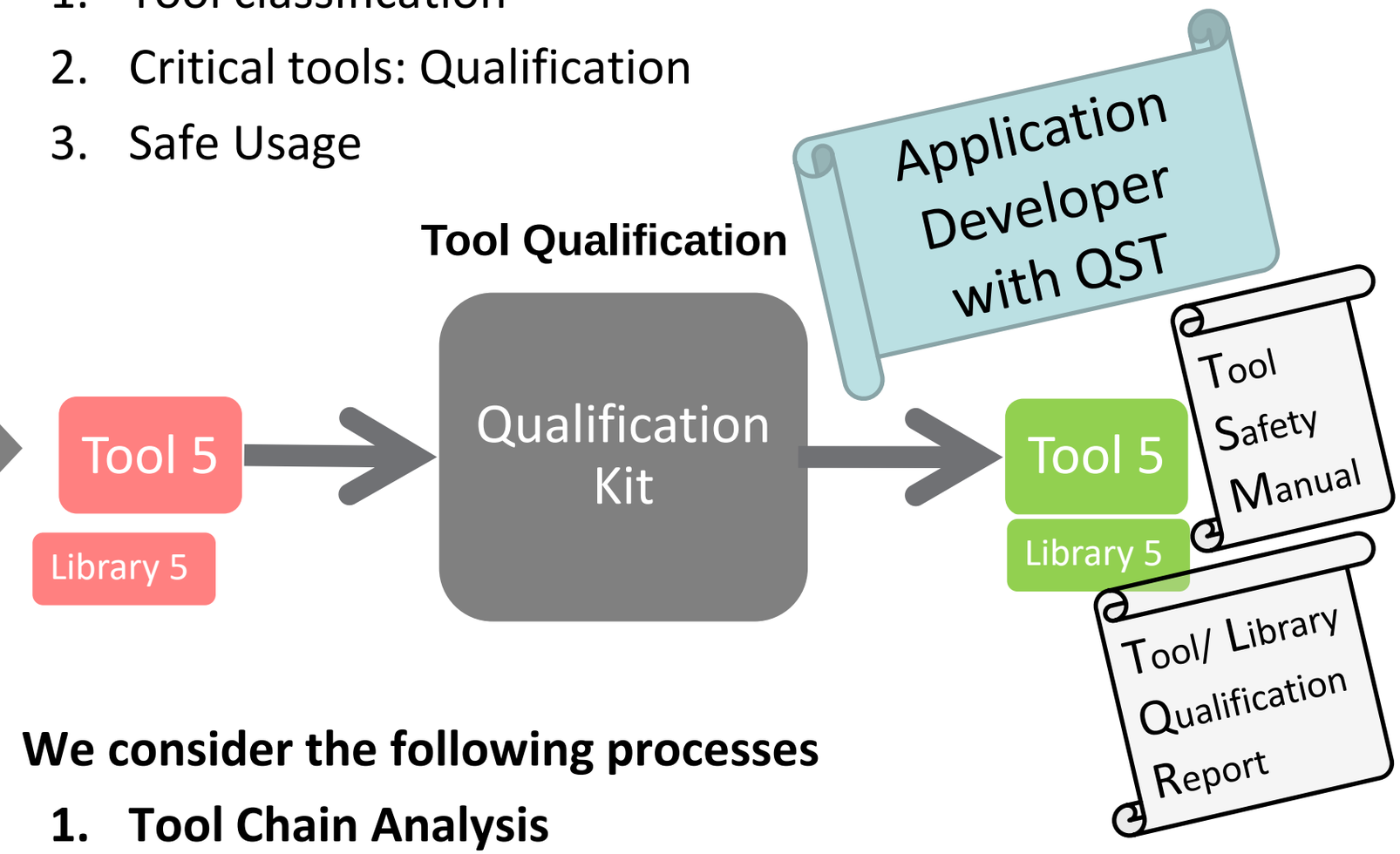
Contents

- Reference Process
  - Motivation
  - Solution
  - Process Modelling Tool (PMT)
- **Tool Qualification Processes**
- Process Compliance
- Summary

Qualification Processes

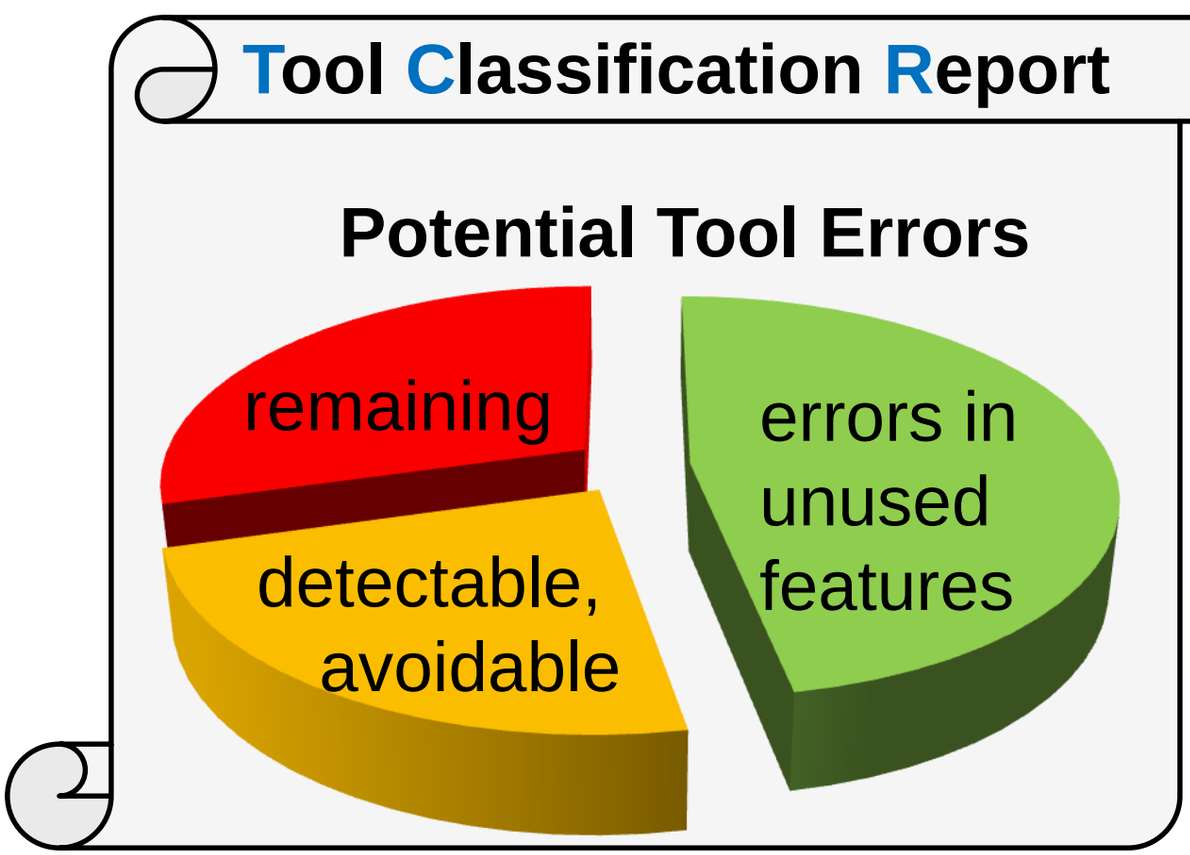


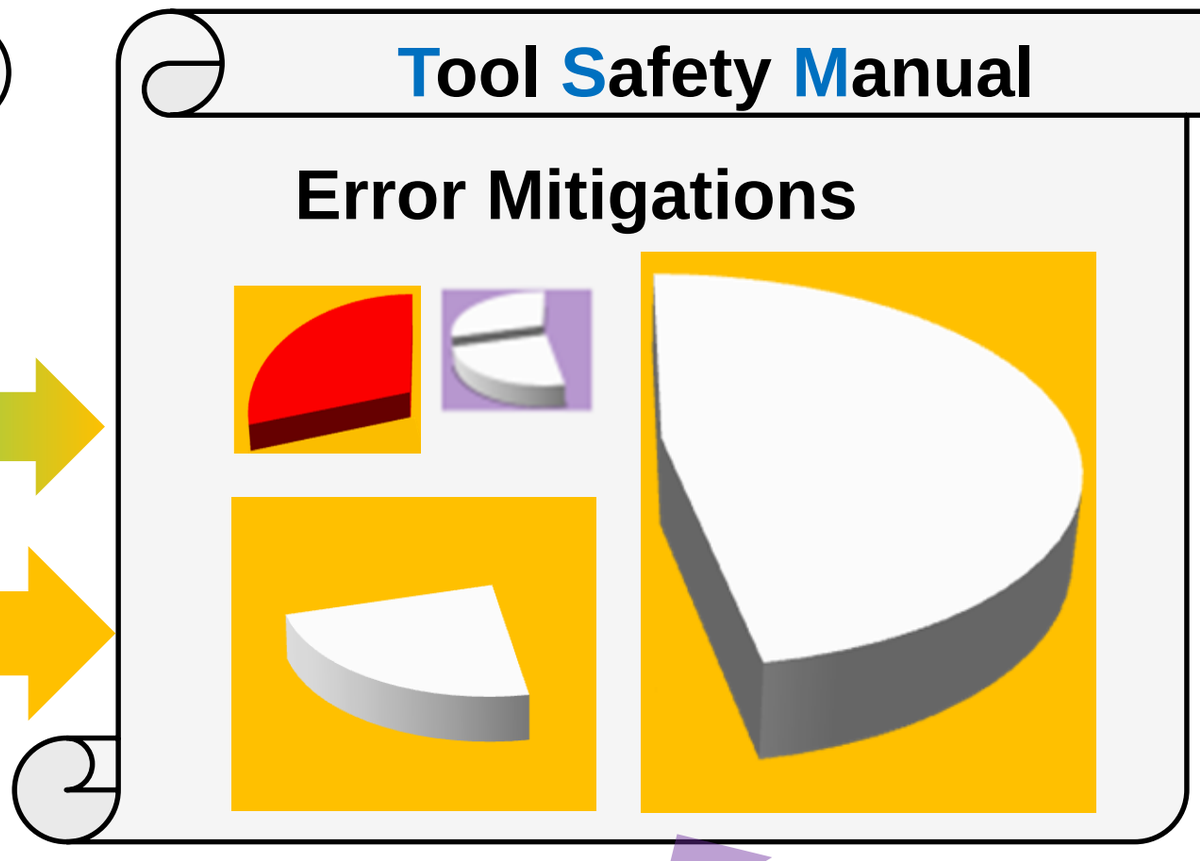
- **Standards (ISO 26262, IEC 61508, DO 178, EN 50128) require a safe usage of all SW development tools & libraries**
  1. Tool classification
  2. Critical tools: Qualification
  3. Safe Usage

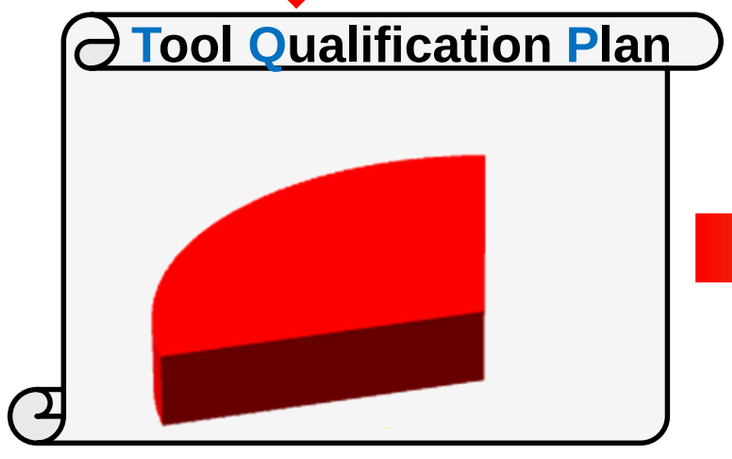


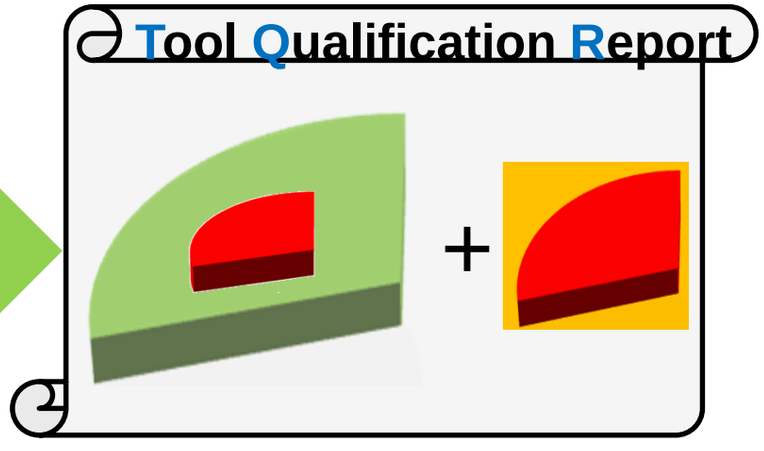
- **We consider the following processes**
  1. **Tool Chain Analysis**
  2. **Qualification Kit Creation**
  3. **Tool Qualification**

Tool Qualification Kit Documents









Known Errors

QKit User Guide

QKit Developer Guide

QKit Verification and Validation Plan

QKit Verification and Validation Report

SPEDIT-Qualification Kits (“Growing”)

- **Growing QKit: partial, can be extended**
- **Compliant with ISO 26262, IEC 61508, DO-178, EN 50128,…**
- **Build according to Validas TÜV-certified compliance process**
- **AutoFocus-QKit**
  - Qualifies Schedule generation feature of AutoFOCUS
  - First QKit for a formal methods tool
  - Based on interface & redundancy
  - Demonstration -> Exhibition (Validas)
- **PTC-Modeller-QKit**
  - Qualifies Basic DataBase Functionality (“No Side-Effects”!!)
  - “Mitigates” other features
  - Demonstration -> Validas

Contents

- Reference Process
  - Motivation
  - Solution
  - Process Modelling Tool (PMT)
- Tool Qualification Processes
- **Process Compliance**
- Summary

Motivation: (QKit-)Compliances

Product - ASIL	ASIL D
Item	
SEooC	
Unchanged SWC („Library“)	
Tool	

SWC Qualification Kit:
(6-SEOOC Compliant)

- Function-Specifications
- Potential Errors
- Known Bugs
- Code-Coverage (**ALL ASIL**)
- **Architecture**
- **Programming Guidelines**
- **Tool Qualification Reports**
- **Many** Tests / TAU
- …

SWC Qualification Kit:
(8-12 Compliant)

- Function-Specifications
- Potential Errors
- Known Bugs
- **Code-Coverage (ASIL D)**
- **negative** Tests / TAU
- …

Tool Qualification Kit:
(8-11 Compliant)

- Feature-Specifications
- Potential Errors
- Known Bugs
- **Mitigations**
- Requirements Tests / TAU
- …

similar structures:
development processes

Process Modeling Tool PMT

Model-Based Process

Formalize

Link Requirements to Processes and Verification Actions

Tailor Parameters

ISO 26262,
IEC 61508, ..

Formalize

PMT

VALIDAS
1.11.2
Toolchain Analyzer

QKit

Parameter Values

Generate

Generate

Generate

VVT

Process Description

Compliance Report

Verification Validation Plan

Project: V&V

Verification Validation Report


ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

CERTIFICATE
No. Q4B 18 01 03748 001

Holder of Certificate: Validas AG
Arnulfstr. 27
80335 Munich
GERMANY

Factory(ies): Validas AG
Arnulfstr. 27, 80335 Munich, GERMANY

Certification Mark:

Scope of Certificate: QKit development process for software support tools

Applied Standard(s): IEC 61508-1:2010
IEC 61508-3:2010
IEC 61508-4:2010
ISO 26262-1:2011
ISO 26262-2:2011
ISO 26262-8:2011

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No.: VM92017C

Valid until: 2021-01-30

Date, 2018-01-31
Page 1 of 1

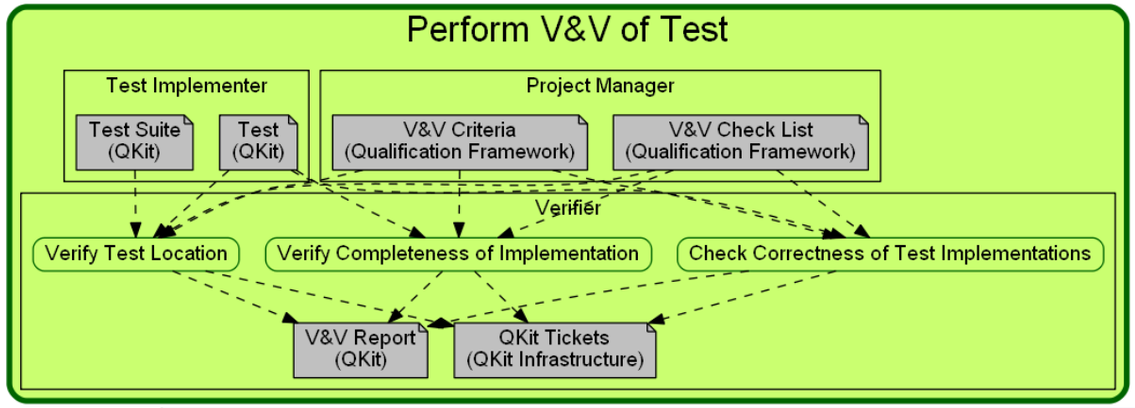
TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

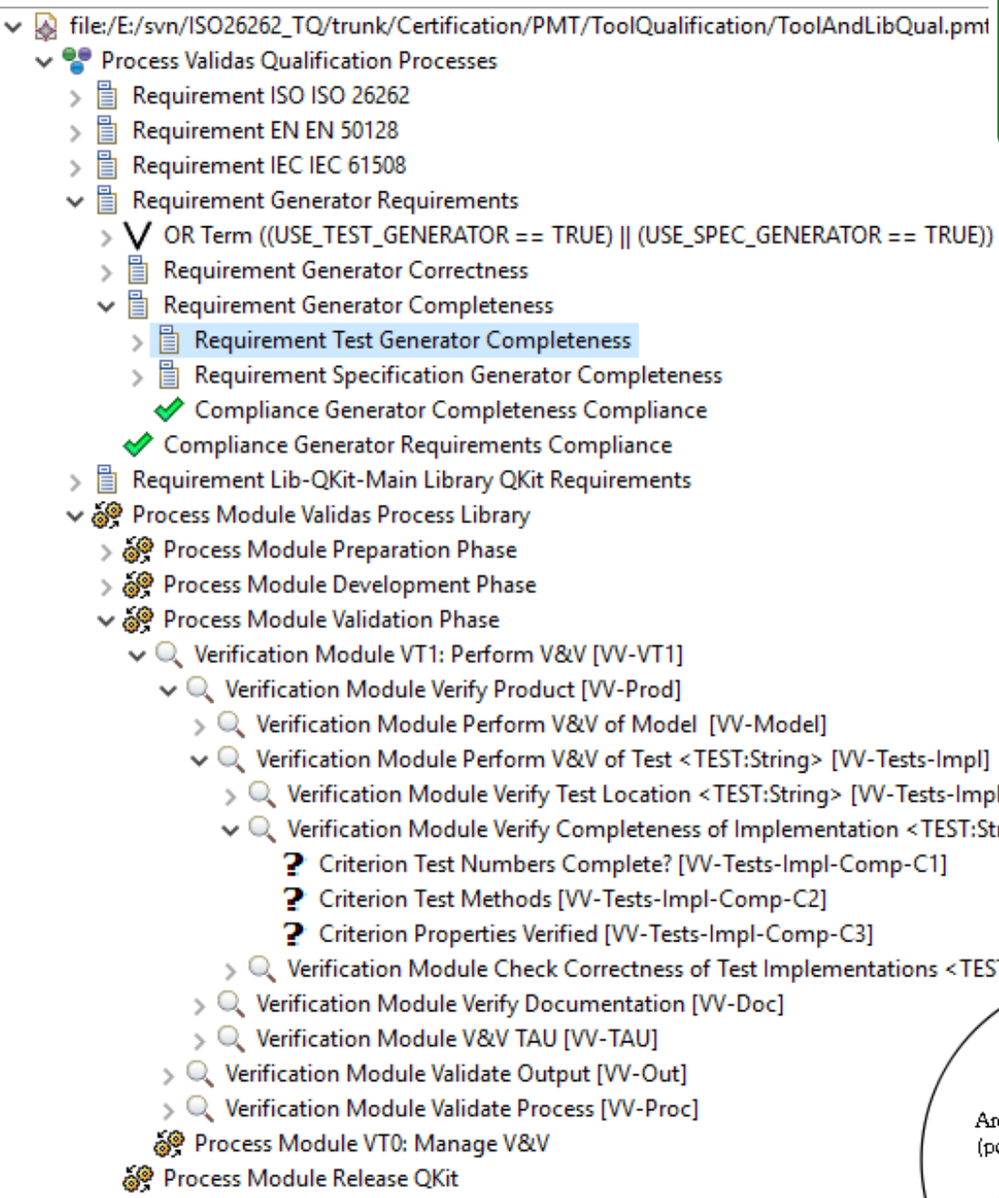
Safety Plan

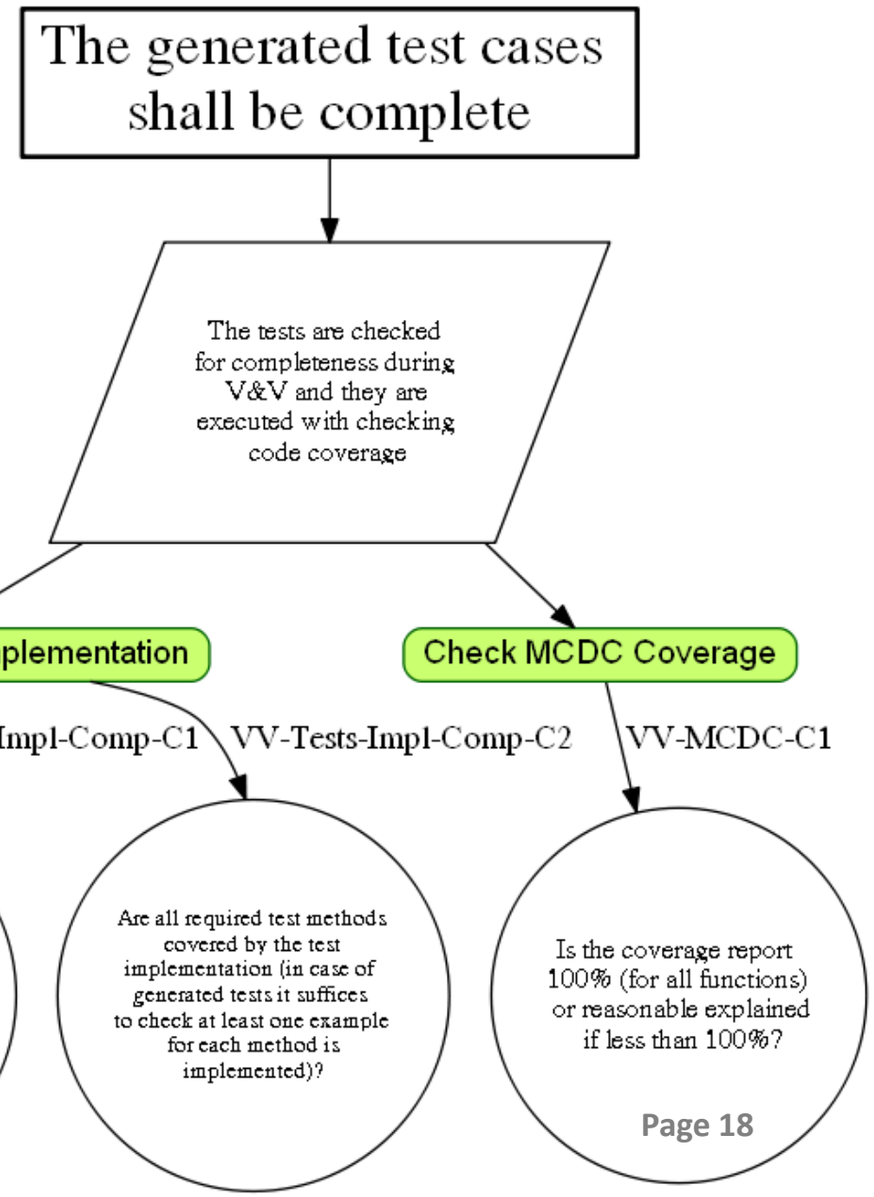
Safety Case

Example Compliane Argumentation

- We use Test Generators that have to generate complete test case
- We check this during V&V

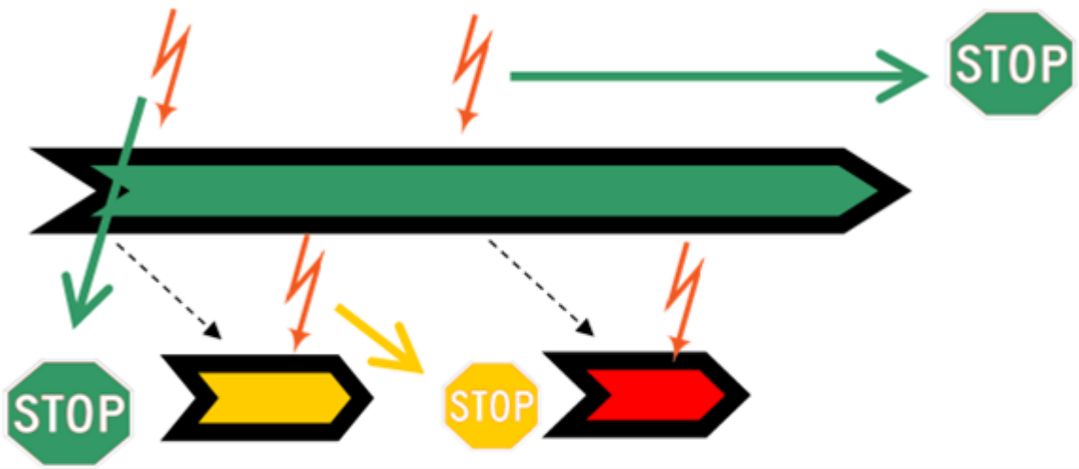






Generated Compliance Report

Compliance Report
for
AutoFOCUS3 Modeling Process



Version:	Template 0.2 / Document 0.3
Date:	2018-10-30
Status:	Generic / **Generated** / Reviewed / Final
Author:	Dr. Oscar Slotosch
File:	CR.docm
Size:	11 Pages

3.1 Requirement Specification Quality

This section describes requirement Specification Quality.

Requirement: Specification Quality
Name:
Specification Quality
Description:
Consistent documentation, i.e., Auto-generation of documentation.
Recommended From:
ASIL_A
Recommended To:
ASIL_D
Implementing Process (Satisfying this claim):
• Building Functional Black Box Model

Table 9 Requirement: Specification Quality

VerificationModule: Check Model Consistency
Name:
Check Model Consistency
Description:
The consistency of the model is statically checked using the tools. Consistency checks of black box models automatically detect - empty interfaces - empty descriptions - undefined types - non-matching types The result of the consistency check is a consi successfully checked".
Relevant Parameter:
• FUNCTION, see Table 7
Owner:
Model Validator
Input Artefacts:
• BlackBoxModel, see
Output Artefacts:
• Validation Report, see
Verifies:
• Model: BlackBoxModel, see • ProcessModule: Building Functional Black Box Model, see

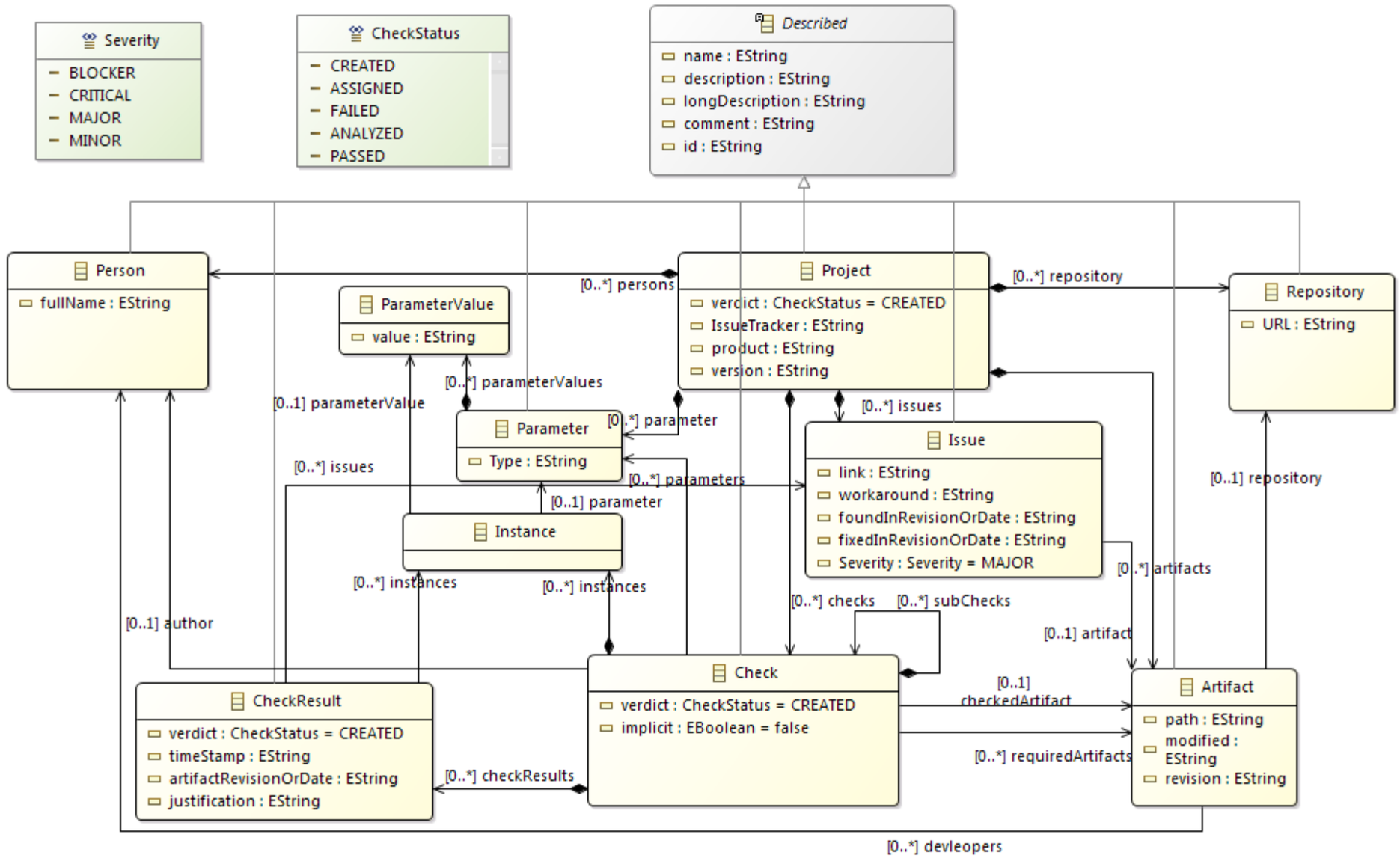
Table 11 VerificationModule: Check Model Consistency

Compliance Black Box Model Compliance
Name:
Black Box Model Compliance
Description:
By creating functional black box models the specification quality is increased. One obvious benefit of the models is that they can be automatically validated, i.e. if Validation has been performed the quality increased.
Requirement:
• Specification Quality, see Table 9
Implementing Process Module:
• Building Functional Black Box Model
V&V Check:
• Check Model Consistency, see Table 11

Table 12 Compliance Black Box Model Compliance

Verification and Validation Model

- V&V Model documents Verification and Validation (for all instances of the parameters)
- V&V Model is basis for Verification and Validation Tool (VVT)
- VVT Model is generated from PMT (based on Process and Planning parameters)
- Meta Model of VVT:



Example: Corresponding Checklist

	A	B	C	D	E	N	O	P	Q
1	Parameters	Result: Combinations Considered in Test Strategy	Date: Combinations Considered in Test Strategy	Issues: Combinations Considered in Test Strategy	Explain: Combinations Considered in Test Strategy	Result: NaNOK=0	Date: NaNOK=0	Issues: NaNOK=0	
155	TEST=test___aeabi_fsub	PASS	17/02/2019		Yes, 6 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 66 tests of __aeabi_fsub have been analyzed comp
156	TEST=test___aeabi_idiv	PASS	17/02/2019		Yes, 6 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 55 tests of __aeabi_idiv have been analyzed compl
157	TEST=test___aeabi_idiv0	PASS	17/02/2019		Yes, 4 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 36 tests of __aeabi_idiv0 have been analyzed comp
158	TEST=test___aeabi_ldiv0	PASS	17/02/2019		Yes, 4 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 36 tests of __aeabi_ldiv0 have been analyzed comp
159	TEST=test___aeabi_lmul	PASS	17/02/2019		Yes, 6 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 52 tests of __aeabi_lmul have been analyzed comp
160	TEST=test___aeabi_uidiv	PASS	17/02/2019		Yes, 6 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 55 tests of __aeabi_uidiv have been analyzed comp
161	TEST=test_abs	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019	#316	Yes, all 34 tests of abs have been analyzed completly durir
162	TEST=test_acos	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 55 tests of acos have been analyzed completly dur
163	TEST=test_acosf	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 55 tests of acosf have been analyzed completly du
164	TEST=test_asin	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 52 tests of asin have been analyzed completly duri
165	TEST=test_asinf	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 52 tests of asinf have been analyzed completly dur
166	TEST=test_atan	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 55 tests of atan have been analyzed completly duri
167	TEST=test_atan2	PASS	17/02/2019		Yes, 4 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 58 tests of atan2 have been analyzed completly du
168	TEST=test_atan2f	PASS	17/02/2019		Yes, 4 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 59 tests of atan2f have been analyzed completly du
169	TEST=test_atanf	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 56 tests of atanf have been analyzed completly dur
170	TEST=test_ceil	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 52 tests of ceil have been analyzed completly durir
171	TEST=test_ceilf	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 52 tests of ceilf have been analyzed completly duri
172	TEST=test_cos	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 53 tests of cos have been analyzed completly durir
173	TEST=test_cosf	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 53 tests of cosf have been analyzed completly duri
174	TEST=test_cosh	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 51 tests of cosh have been analyzed completly dur
175	TEST=test_coshf	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 51 tests of coshf have been analyzed completly du
176	TEST=test_exp	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 51 tests of exp have been analyzed completly durir
177	TEST=test_expf	PASS	17/02/2019		Yes, 2 combinations with other functions have been specified & tested (terms)	PASS	17/02/2019		Yes, all 54 tests of expf have been analyzed completly duri

... | Artifact Description | Issue Description | Check Description | CR_ERROR | CR_FEATURE | CR_TEST

Contents

- Reference Process
  - Motivation
  - Solution
  - Process Modelling Tool (PMT)
- Tool Qualification Processes
- Process Compliance
- **Summary**

Summary

- **SPEDIT-Reference process**
  - Is generic & model-based
  - Can be adapted to any project & company using PMT
  - Can be validated (syntactically & semantically)
  - Can be safe & compliant with ISO 26262, IEC 61508,..
- **PMT Prototype**
  - Is freely available from http://www.validas.de/tools/
- **VVT Prototype**
  - Is freely available from http://www.validas.de/tools/
- **Approach has been applied to certify Validas tool qualification process**

ZERTIFIKAT ◆ CERTIFICAT ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE

No. Q4B 18 01 03748 001

Holder of Certificate: Validas AG
Arnulfstr. 27
80335 Munich
GERMANY

Factory(ies): Validas AG
Arnulfstr. 27, 80335 Munich, GERMANY

Certification Mark:

Scope of Certificate: QKit development process for software support tools

Applied Standard(s): IEC 61508-1:2010
IEC 61508-3:2010
IEC 61508-4:2010
ISO 26262-1:2011
ISO 26262-2:2011
ISO 26262-8:2011

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No.: VMS2017C

Valid until: 2021-01-30

Date, 2018-01-31
(Jiayi Dong)
Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany