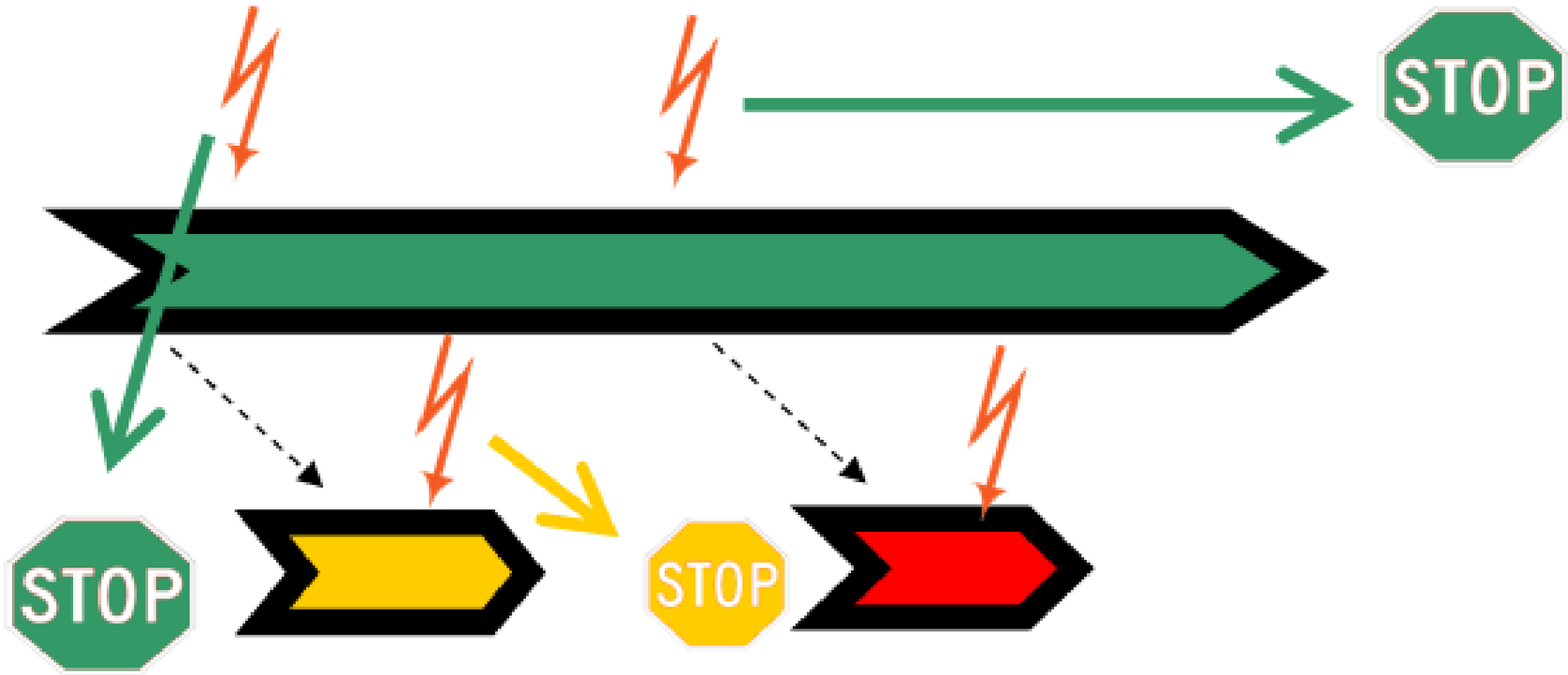
recomp
Reduced Certification Costs for trusted Multi-core Platforms



Dr. Oscar Slotosch, Validas AG

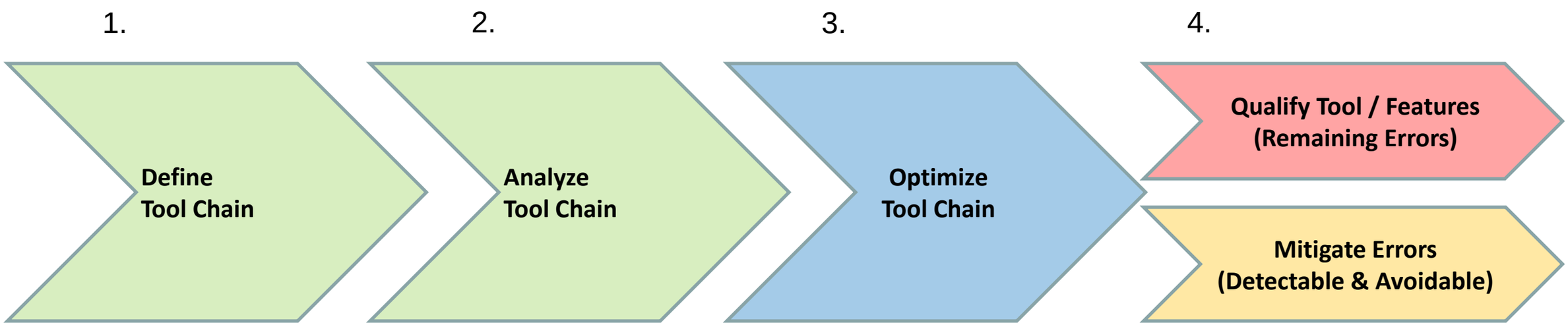
Tool Chain Analyzer: Method, Tool and Examples

Content

- **Motivation**
- Tool Chain Analyzer
- Examples
  - RECOMP Tool Chain
  - Industrial
- Summary

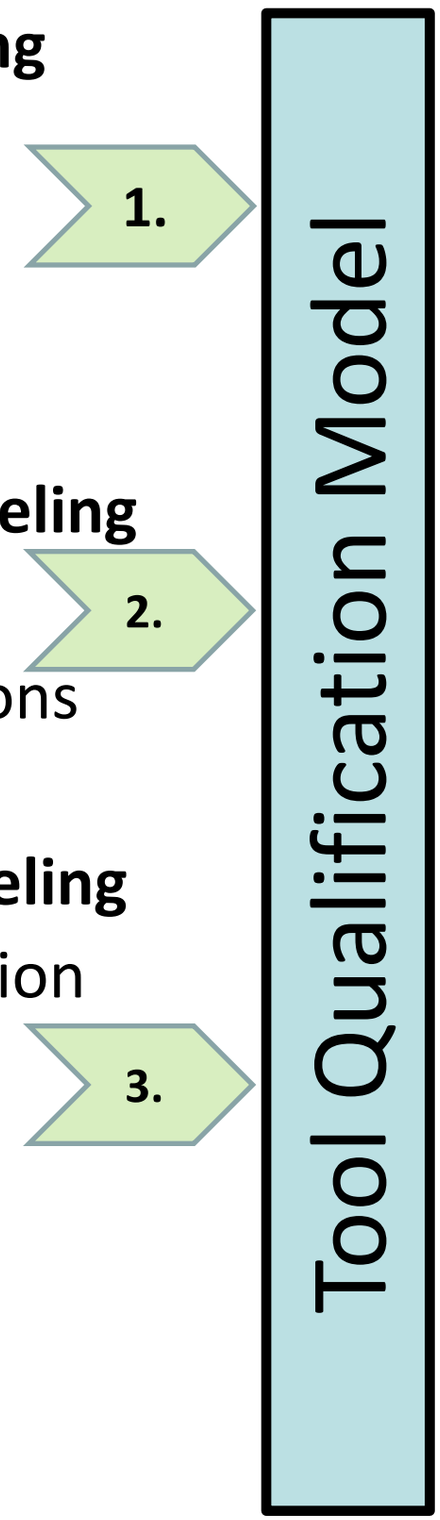
The Tool Qualification Process

1. **Definition: Tools in chain (process) with artifacts**
2. **Analysis: Determination of**
   - Required Confidence
   - Potential tool errors
     - Unused features
     - Detectable / avoidable
     - Remaining
3. **Optimization: tool chain improvements**
4. **Qualification: Once for each tool version**
4. **Mitigation: Every tool application**



Model-Based Tool Qualification

1. **Tool (Chain) definition modeling**
   - Use-Cases,
   - Relevant tool features,
   - Artifacts
   - Documentation
2. **Tool (Chain) classification modeling**
   - Potential errors
   - Available checks & restrictions
   - Documentation
3. **Tool (Chain) qualification modeling**
   - Qualification cost optimization
   - Qualification planning
   - Qualification tests:
     - Identification,
     - Validation Plan
     - Execution Plan
   - Documentation



Generated Qualification Documents

- Tool Impact
- Tool Confidence Level
- Tool Application Guide (TCL1)
- Tool Qualification Plan
- Test Plan
- Test Report
- Test V&V
- V&V Report
- Tool Qualification Report
- Tool Application Guide (TCL>1)

Cost Reduction by Model-based Tool Qualification

- **Tool Provider**
  - Provides a **scalable** tool qualification kit with
    - Model (Tool, Features, pot. Errors, Checks/Restrictions, Tests, ..)
    - Tests
    - Qualification environment to execute the required tests
    - Documentation
  - Has a priorization for further tests (risk-/user-cost-based)
- **Tool User**
  - Kit can be applied in different processes (no “Reference Process” required)
  - Model (of the current process) can be used
    - Determine required checks and restrictions to detect/avoid pot. errors
    - Determine the TCL of the tool in the use-case
    - Analyze variants of the process
    - Generate a report for the tool classification
    - Identify the required qualification test (“test plan generation”)
  - Models (of single tools) can be integrated to Tool-Chain models to reduce qualification need

Content

- Motivation
- **Tool Chain Analyzer**
- Examples
  - RECOMP Tool Chain
  - Industrial
- Summary

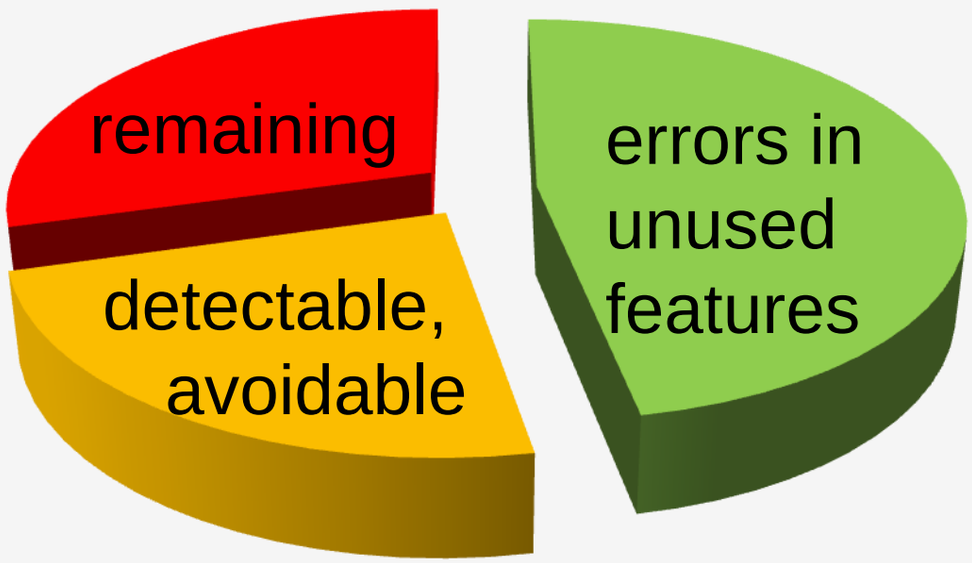
Tool Chain Analyzer (TCA)

- **Automatically determines the Impact and the TCLs of tools and tool chains**
- **Bases on a formal model of**
  - Tools & Use cases (and features)
  - Potential Errors
  - Detection/prevention mechanisms
  - Artifacts (inputs & outputs)
  - Qualifications for tools & features
  - Assumptions
- **Supports generic error models**
- **Checks the validity of qualifications with a given ASIL**
- **Generates reports (.docx)**
- **Developed from Validas AG within European research project** recomp
  Reduced Certification Costs for trusted Multi-core Platforms
  - Eclipse rich client based on EMF, docx4j and poi
- **Evaluation available at www.validas.de/TCA.htm**

Tool Safety Manuals
+ Extension by Qualification Results

Tool Evaluation Report

Potential Tool Errors



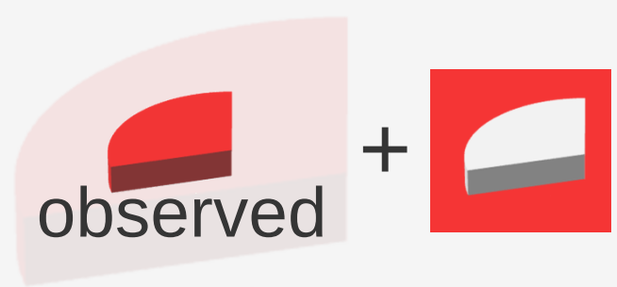
Tool Application Guide

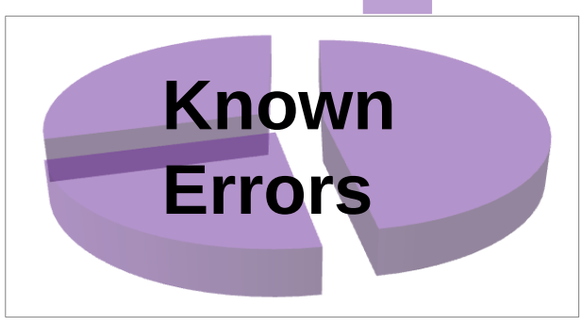
Modeling Guides

+ Error Mitigations

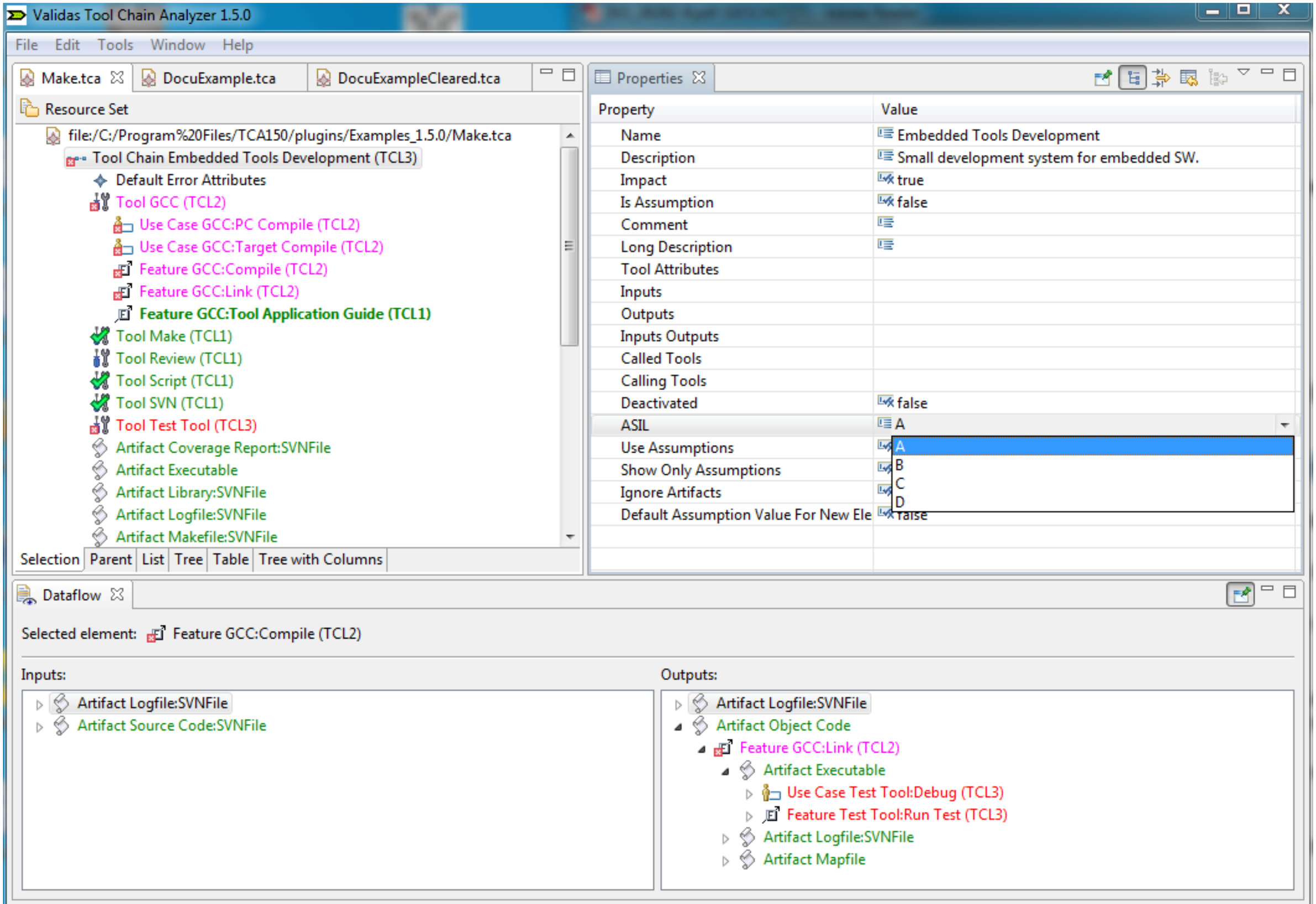
Tool Qualification Plan

Tool Qualification Report





TCA: Formal Model of Tool Chains



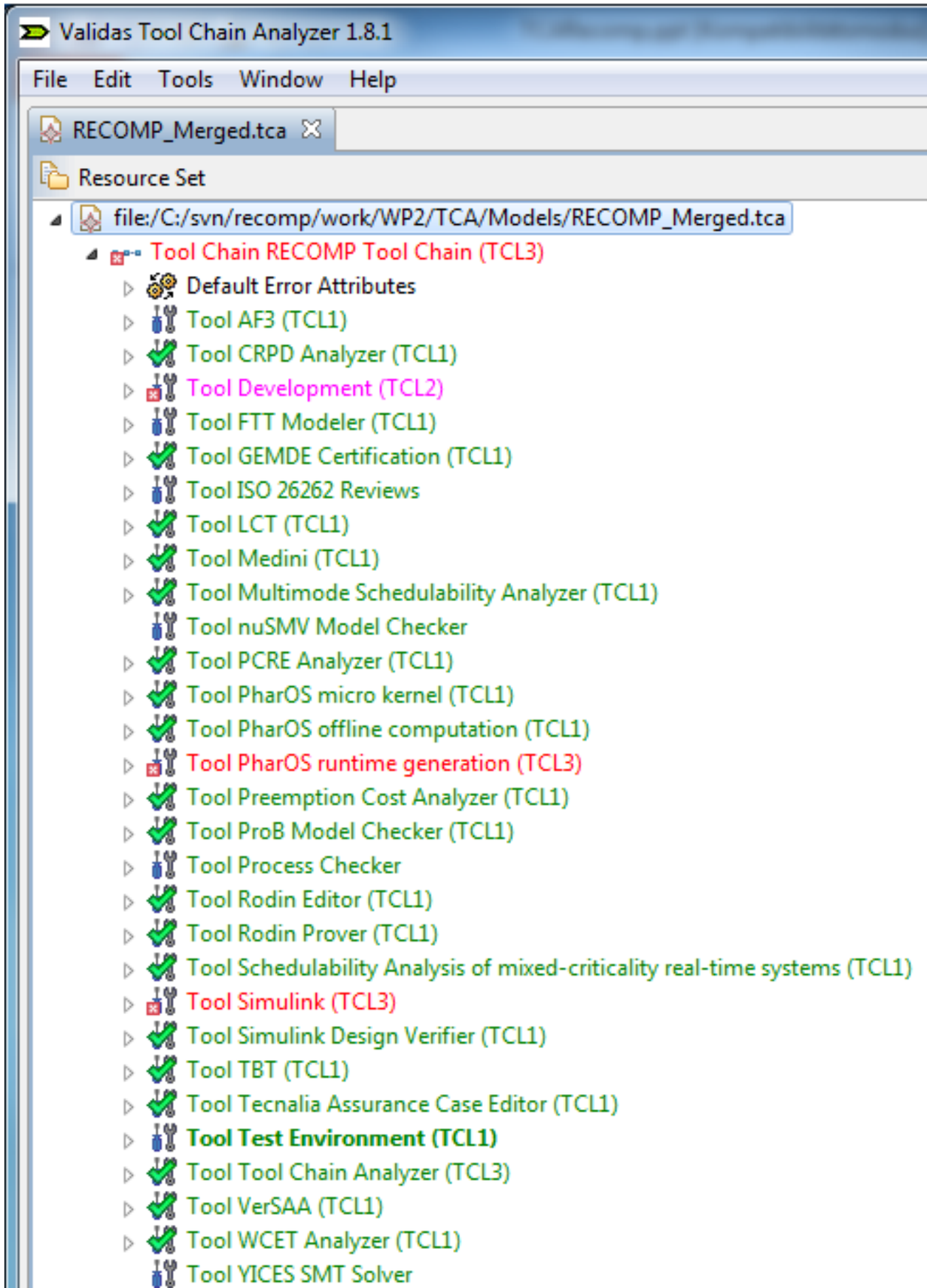
The ASIL of the Tool Chain

Content

- Motivation
- Tool Chain Analyzer
- **Examples**
  - **RECOMP Tool Chain**
  - **Industrial**
- Summary

RECOMP Tool Chain(s)

- **Most method/tool providing RECOMP partners have created models from their tools**
  - Tools
  - Use-Cases
  - Artifacts
  - Potential Errors
  - Mitigation Possibilities
- **Artifacts have been integrated & harmonized (Madrid-Workshop,..)**
- **Validas integrated the models**
- **TCA supports variants of chains for**
  - All Tools
  - Automotive
  - Avionics
  - Industrial
- **Reports have been generated (part of deliverables):**



RECOMP Tool Chain Overview

- **Generated picture from the model**

Medini
FTT Modeler
muSMV Model Checker
YICES SMT Solver
PCRE Analyzer
Rodin Editor
WCET Analyzer
ProB Model Checker
Development
PharOS offline computation
Rodin Prover
Simulink
PharOS runtime generation
LCT
Process Checker
AF3
VeriSAA
TBT
PharOS micro kernel
Tool Chain Analyzer
CRPD Analyzer
Schedulability Analysis of mixed-criticality real-time systems
Multimode Schedulability Analyzer
Simulink Design Verifier
Test Environment
ISO 26262 Reviews
Preemption Cost Analyzer
Tecnalia Assurance Case Editor
GEMDE Certification

RECOMP Tool Chain (Views)

- Artifact Evidence
- Artifact Evidence:Binary executable
- Artifact Evidence:Detailed System Architecture
- Artifact Evidence:Excel File
- Artifact Evidence:Failure rate catalog
- Artifact Evidence:FHA
- Artifact Evidence:FMEA
- Artifact Evidence:FTA
- Artifact Evidence:Functionalities
- Artifact Evidence:Malfunctions
- Artifact Evidence:Metrics
- Artifact Evidence:Overall Project Plan
- Artifact Evidence:Preliminary System Architecture
- Artifact Evidence:Report on Maximum CRPDs
- Artifact Evidence:Report on Schedulability (1 mode)
- Artifact Evidence:Report on Schedulability (all)
- Artifact Evidence:Review Protocol
- Artifact Evidence:Safety Goals List
- Artifact Evidence:Safety Manual
- Artifact Evidence:Safety Plan
- Artifact Evidence:Safety Requirements
- Artifact Evidence:SLDV verification report
- Artifact Evidence:Software Unit Design Specification
- Artifact Evidence:Software Unit Design Specification:Simulink Model
- Artifact Evidence:Source Code
- Artifact Evidence:Source Code:C/C++ Source Code
- Artifact Evidence:Source Code:Timing Parameters
- Artifact Evidence:TBT Data Model
- Artifact Evidence:TCA-Model
- Artifact Evidence:Test Cases
- Artifact Evidence:Test Specification
- Artifact Evidence:Tool Evaluation Report
- Artifact Evidence:WCET
- Artifact Evidence:WCRT
- Artifact Evidence:Word Document
- Artifact Execution Graph
- Artifact Mapping of tasks to processing elements

- 1 TCL Details of RECOMP Tool Chain
  - 8.1 TCL Result Overview
  - 8.2 AF3
  - 8.3 CRPD Analyzer
    - 8.3.1 Use Cases of CRPD Analyzer
      - 8.3.1.1 Use Case Compute All CR
      - 8.3.1.2 Use Case Compute single
    - 8.3.2 Features of CRPD Analyzer
      - 8.3.2.1 Feature Check input and
    - 8.3.3 Potential Errors in CRPD Analy
    - 8.3.4 Restrictions in CRPD Analyzer
    - 8.3.5 Checks in CRPD Analyzer
    - 8.3.6 Assumptions
    - 8.3.7 TCL Determination
      - 8.3.7.1 TCL Determination for Use Case: Compute All ...
      - 8.3.7.2 TCL Determination for Use Case: Compute sin...
  - 8.4 Developmen
  - 8.5 FTT Modeler
  - 8.6 GEMDE Certi
  - 8.7 ISO 26262 Re
  - 8.8 LCT
    - 8.8.1 Use Cas

8.1 TCL Result Overview

Table 4 shows the result of the tool evaluation, particulary the tool confidence levels.

Name	Tool Impact (TI)	Tool Detection (TD)	Tool Confidence Level (TCL)	Assumptions
AF3	TI 2 (Impact)	TD 1 (HIGH)	TCL 1	-
CRPD Analyzer	TI 2 (Impact)	TD 1 (HIGH)	TCL 1	-
Development	TI 2 (Impact)	TD 2 (MEDIUM)	TCL 2	-
FTT Modeler	TI 2 (Impact)	TD 1 (HIGH)	TCL 1	-
GEMDE Certification	TI 2 (Impact)	TD 1 (HIGH)	TCL 1	-
ISO 26262 Reviews	TI 2 (Impact)	TD 1 (HIGH)	TCL 1	1
LCT	TI 2 (Impact)	TD 1 (HIGH)	TCL 1	-

Error: Cache-Related Preemption Cost Function - Computation Error
Description:
The computation of the artifact had errors such that the content is wrong.
From use case:
Compute All CRPD
Discovered by the following checks:
• Check input and output files and data.CRPD: check cohenrecy
Occurrences:
• in Compute All CRPD
Error View:

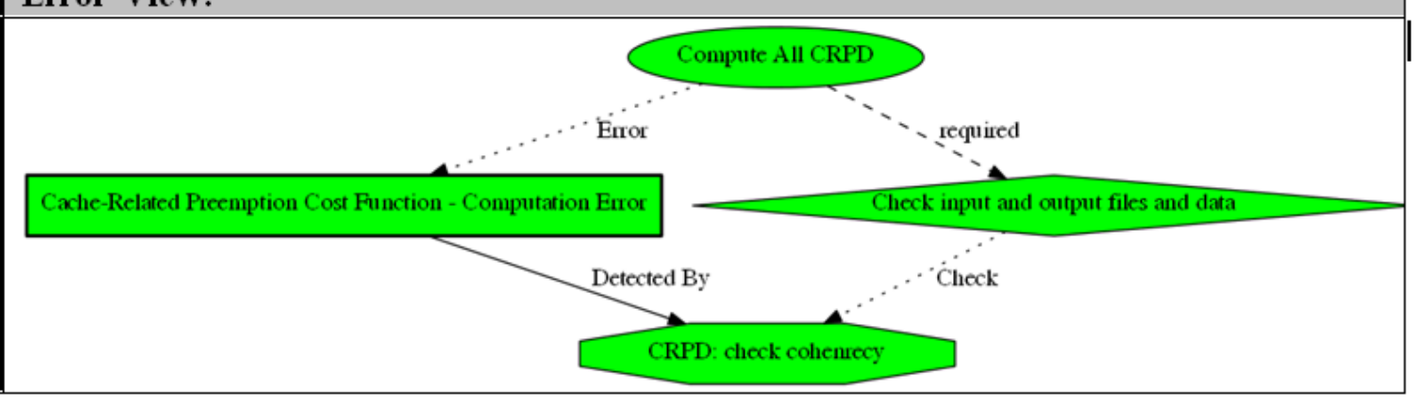
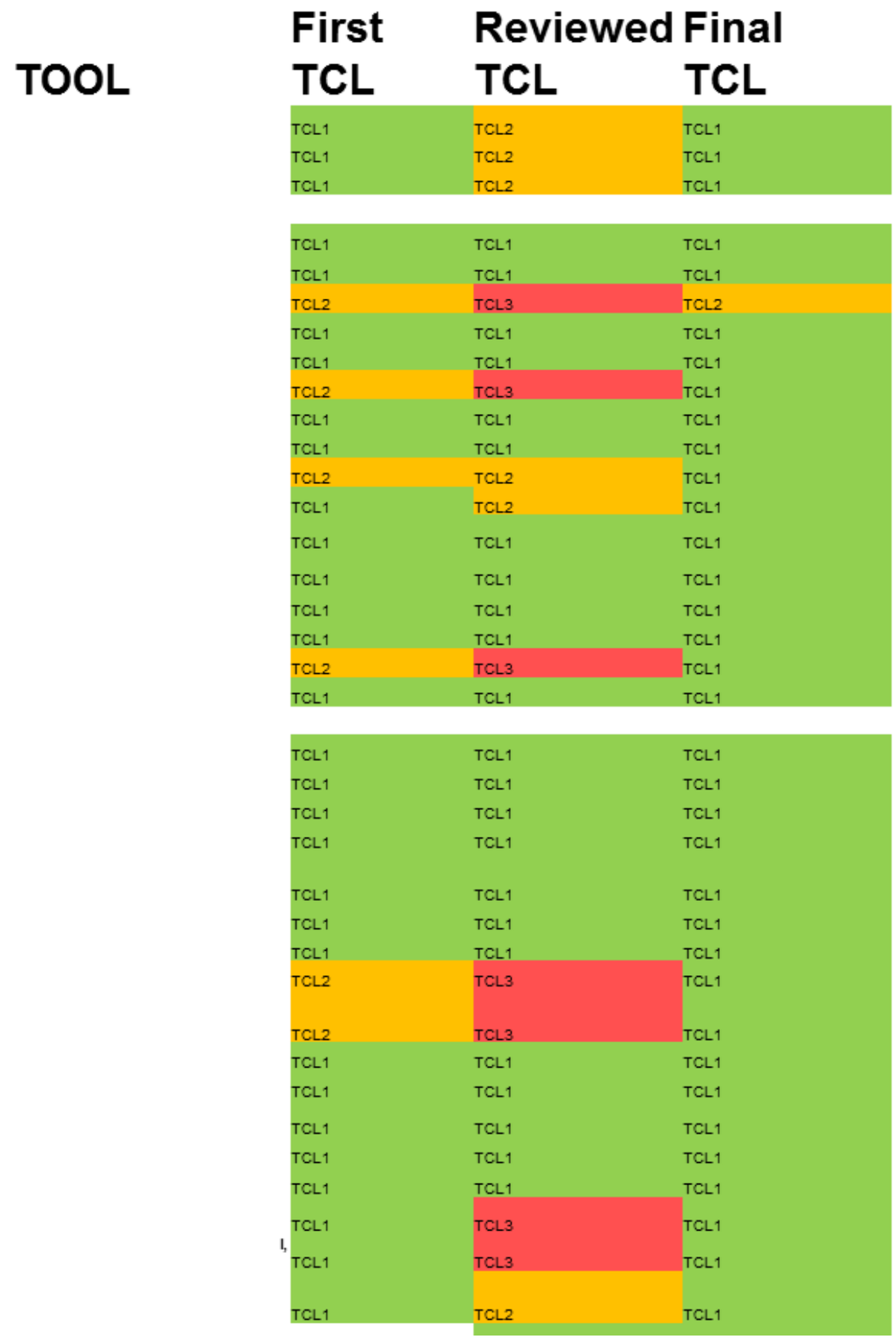


Table 60 Error: Cache-Related Preemption Cost Function - Computation Error

Example: Industrial Tool Chain

- **Tool Chain: 39 tools**
- **Only one tool with TCL 2**
- **Improvement: Reviewed -> Final**
  - Added wins & quick wins (Process changes)
- **Input for tool qualification**
  - Critical features
  - Undetected errors
- **ISO 26262 compliant**
- **Better than**
  - Defaults (from literature)
  - IEC / DO classifications



Why Can we Trust?

- **Independent/external analysis performed from experts (Validas)**
- **TCLs are computed with a calculus (based on a formal model) from a dedicated tool for that purpose**
- **Systematic error model for tools applied (black-box & white-box)**
- **Tool chain model and error model have been validated and reviewed**
  - 157 error classes have been analyzed for 1556 potential errors
- **Analysis was tool supported (Tool Chain Analyzer)**
- **Detailed report (approx. 14 pages per tool) explaining every error and every check/restriction**

- **Note: ISO 26262 requires the following independence for the evaluation and qualification review (different person)**
  - I0: should for ASIL B
  - I1: shall for ASIL C,D

Confirmation measures	Degree of independency[a] applies to ASIL			
	A	B	C	D
Confirmation review of the software tool criteria evaluation report and the software tool qualification report[b] (see ISO 26262-8:2011, Clause 11) Independence with regard to the persons performing the qualification of the software tool	—	I0	I1	I1

- **You can extend it also within your team and review it by different persons**

Content

- Motivation
- Tool Chain Analyzer
- Examples
  - RECOMP Tool Chain
  - Industrial
- **Summary**

Summary

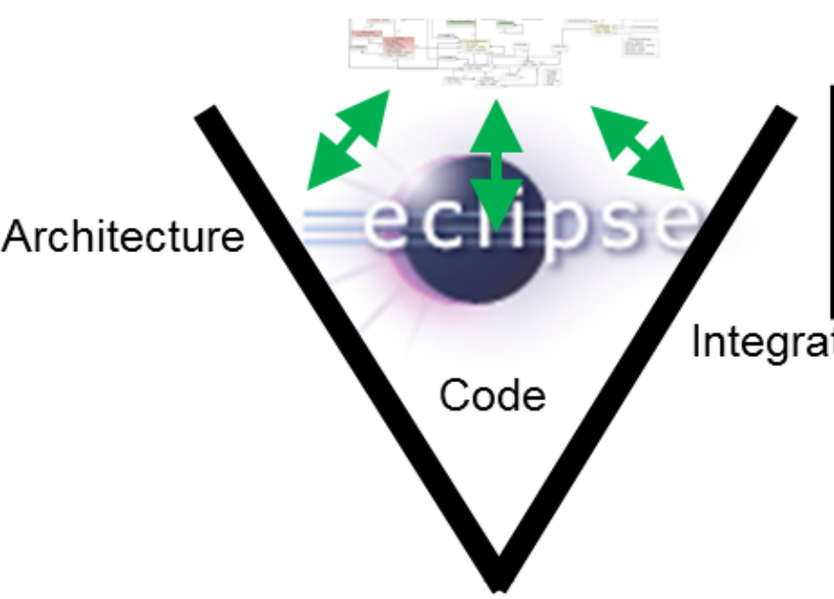
- **Tool Chain Analysis**
  - Satisfies requirements from Standards
  - Developed from Validas within RECOMP
  - Tool & Method applied in >10 commercial projects
- **Model-Based Tool Classification & Qualification reduces costs**
- **Tool Chain Analyzer has been used to integrate RECOMP tools**

Development With Eclipse?

- Currently Eclipse does not support qualification
- There is a road towards tool qualification for Eclipse, see http://wiki.eclipse.org/Auto_IWG_WP5
- DO-330 is a safety standard for tools

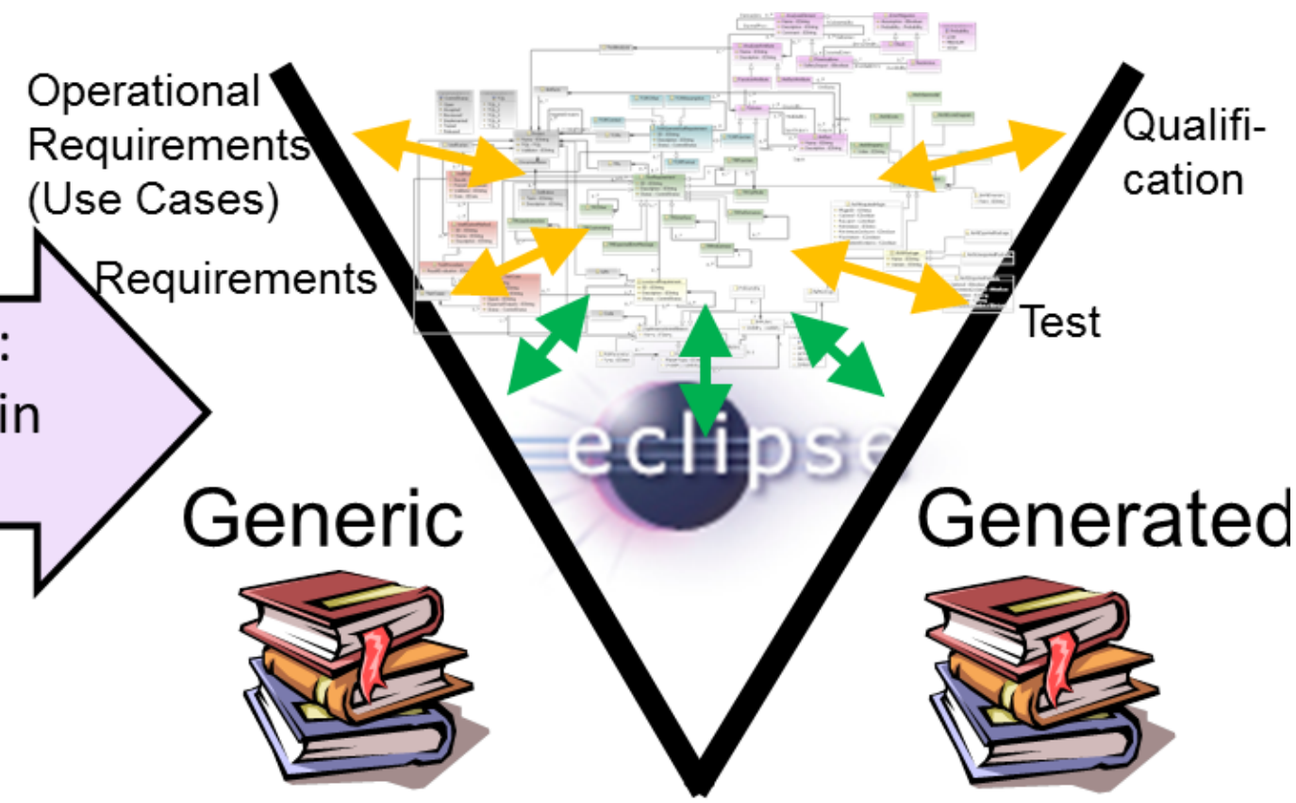
Model-based Tool Qualification

Current Metamodel



Eclipse Project: Qualifiable Plugin Projects (QPP)

New Extended Metamodel



Generic

How-To Qualify Tools according DO-330
Tool Development Plan
Tool Verification Plan
…

Generated

Requirements-Specificatio
Design-Specification
Test-Specification
Tool Analysis (TCL/PSAC)
…

First Tool Qualification Symposium

- **Presentations**
  - Tool user & tool provider
  - Qualification requirements & qualification kits
  - Experiences from different domains & different industries
  - Practical experiences & practical support
- **Keynote speech from F. Pothon**
  - Tool Qualification Considerations and Certification Credits of Qualified Code Generators
- **Location: Munich Airport**
- **Registration: http://toolqualification2013.eventbrite.com**
- **Agenda: http://www.validas.de/tqs.html**
- **Organization: Validas AG**
  - tqs@validas.de

Thank You!

VALIDAS

Arnulfstraße 27
80335 München
www.validas.de
info@validas.de