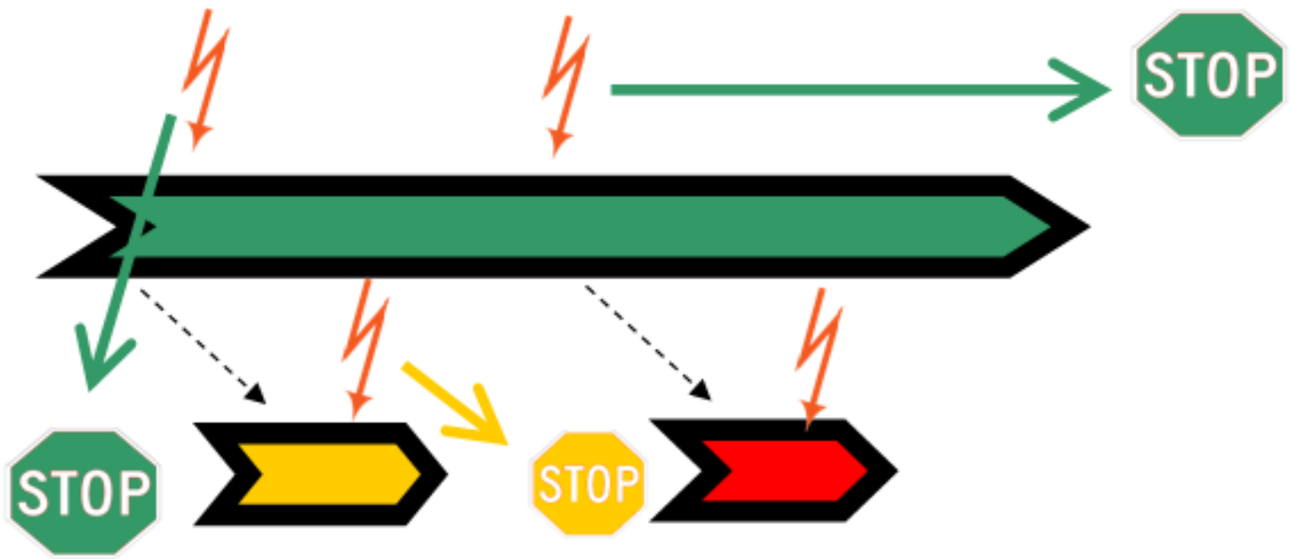
recomp
Reduced Certification Costs for trusted Multi-core Platforms

Applying ISO26262 to Tool Qualification



Dr. Oscar Slotosch, Validas AG
Marco Reiling, Wind River

WIND RIVER

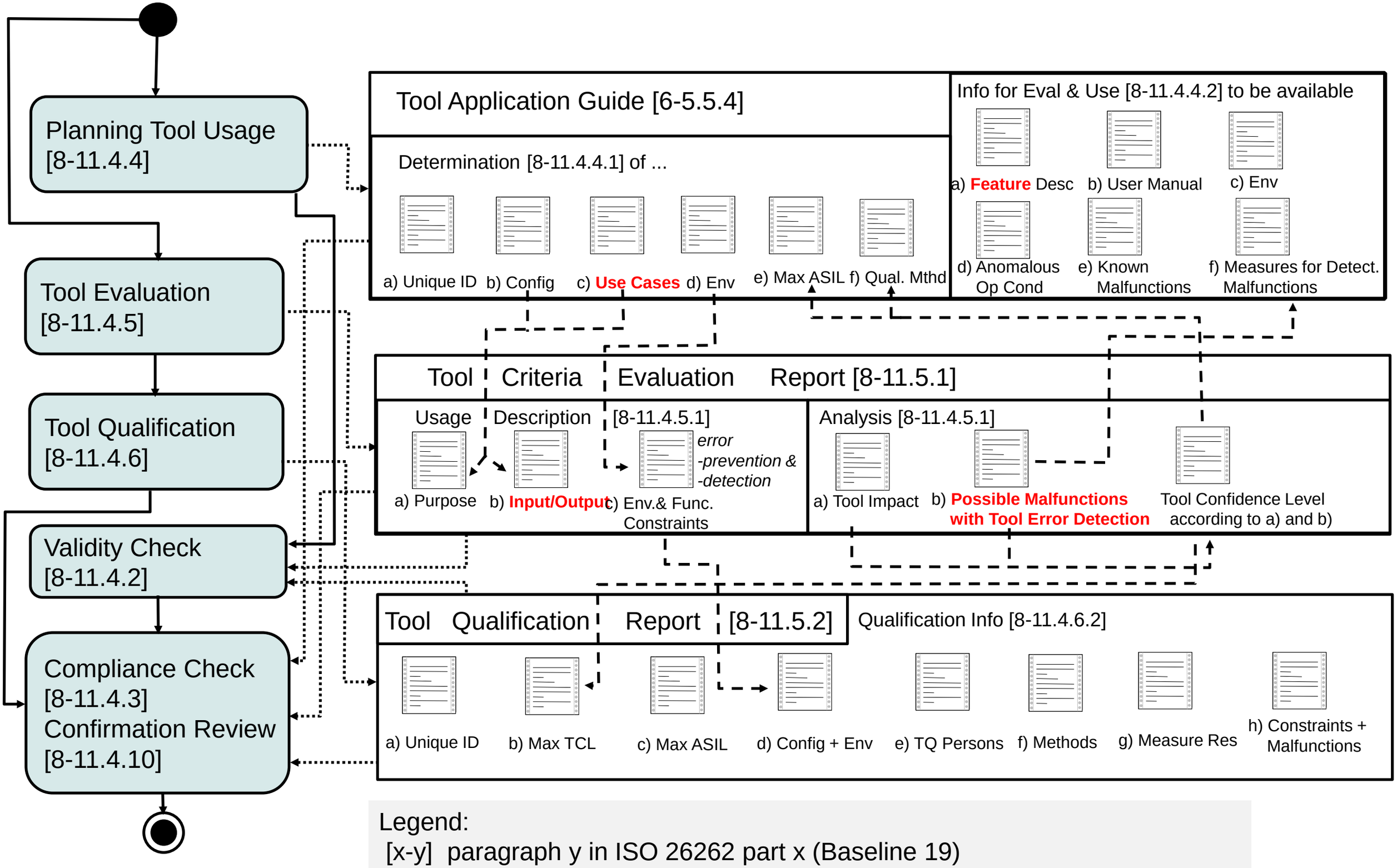
Content: Tool Chain Analysis

- Motivation: ISO 26262: Tool Confidence
- Method: Tool Chain Analysis
  - General Error Model
- Validas Tool Chain Analyzer
- Wind River Diab Compiler Qualification Kit

Content: Tool Chain Analysis

- **Motivation: ISO 26262: Tool Confidence**
- Method: Tool Chain Analysis
  - General Error Model
- Validas Tool Chain Analyzer
- Wind River Diab Compiler Qualification Kit

Confidence in Use of Tools 26262-8



Legend:
[x-y] paragraph y in ISO 26262 part x (Baseline 19)

ISO 26262-8, Chapter 11:
„Confidence in the use of software tools“

- **Classification in „Tool Confidence Level (TCL)“**
- **Tool Impact (TI)**
  - TI1: no impact => Tool is TCL1
  - TI2: some impact
- Tool Error Detection/prevention probability (TD)
  - TD1:high confidence => Tool is TCL1
  - TD2:medium confidence => Tool is TCL2
  - TD3: low/unkown confidence => Tool is TCL3
- **Justification? Dokumentation? Confirmation Review!**

Table 2 — Qualification of software tools classified TCL3

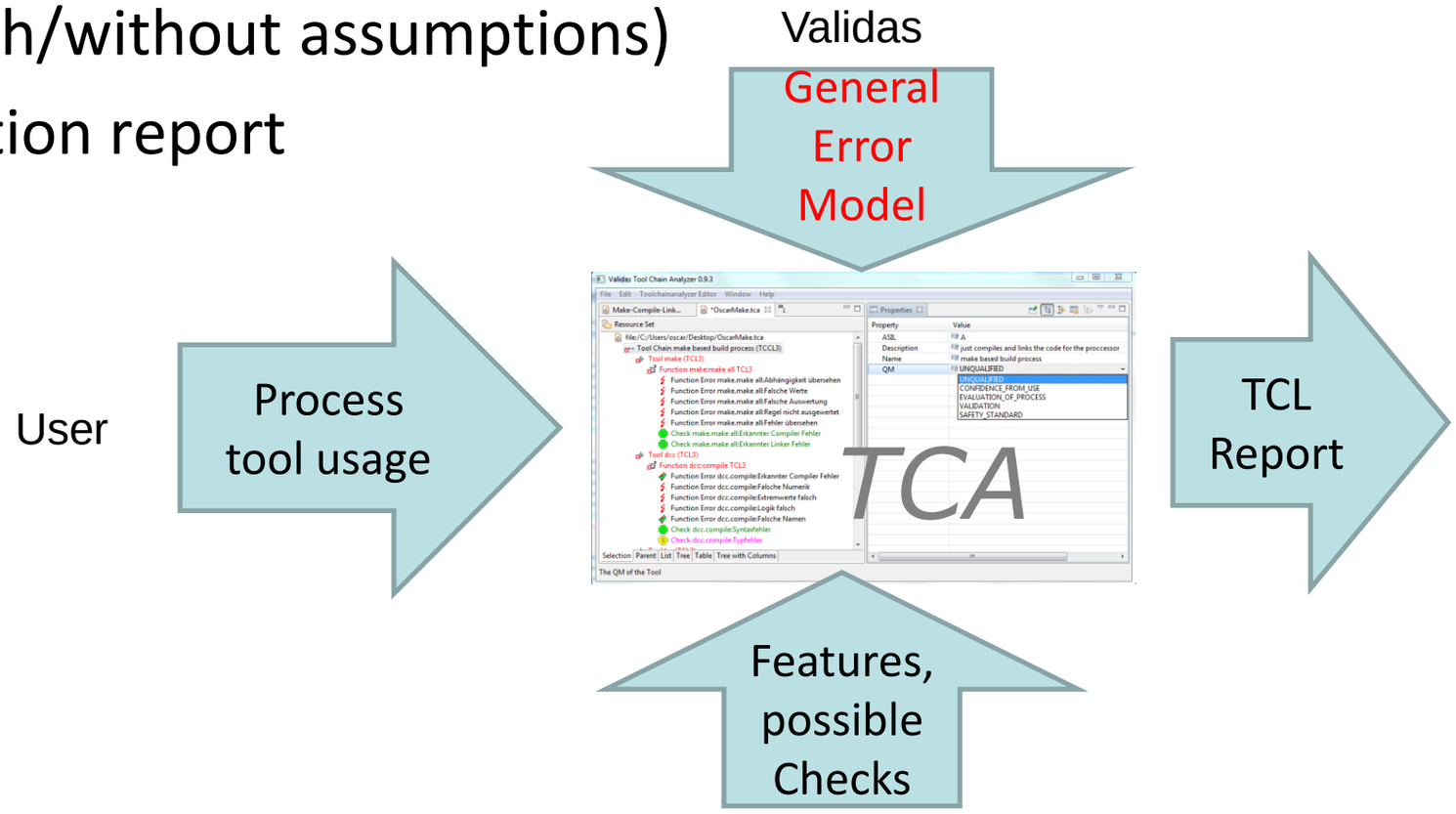
Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use according to 11.4.7	++	++	+	+
1b	Evaluation of the tool development process according to 11.4.8	++	++	+	+
1c	Validation of the software tool according to 11.4.9	+	+	++	++
1d	Development in compliance with a safety standard[a]	+	+	++	++

Content: Tool Chain Analysis

- Motivation: ISO 26262: Tool Confidence
- **Method: Tool Chain Analysis**
  - **General Error Model**
- Validas Tool Chain Analyzer
- Wind River Diab Compiler Qualification Kit

Modeling Method / Process for TCA

1. **Planning:**
    1. Build a formal model of tool usage based on tool and process information
    2. Validate the model (Review, Checklists)
2. **Tool Evaluation**
    1. Systematically build an error model (black box / glass box)
    2. Model detection and prevention (including assumptions)
    3. Validate assumptions and error/detection/prevention model
    4. Compute the TCL (with/without assumptions)
    5. Generate tool evaluation report
3. **Tool Qualification**



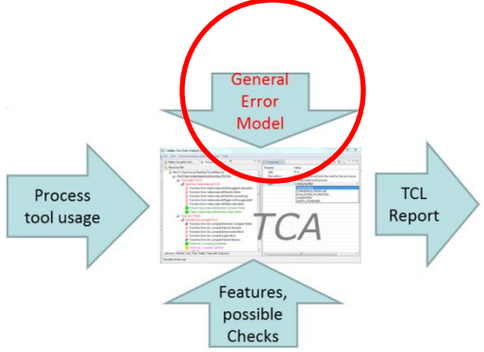
Tool Chain Analysis & Error Model

Motivation / Requirements for Error Model

- ***One*** **error model describes possible tool errors in** ***every*** **tool**
- **Error model should be extensible (for new kinds of tools)**
- **Error model should cover all potential errors**
- **Error model should be acceptable (agreeable and simple to apply)**
- **Error model should cover the existing (known) errors**

- **Systematic (“Repeatable”) approach needed**

General Error Model

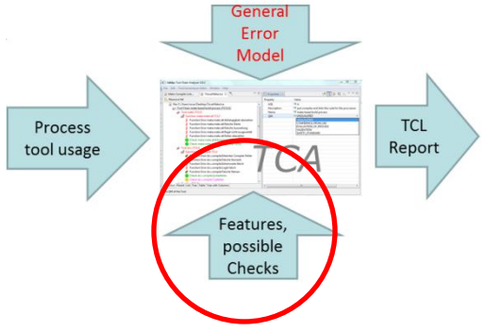


- **Creation Process**
  - Inductive: From known errors to classes of potential errors (“Observing”)
  - Deductive: From tool to potential errors (“Analytic Approach”)
    - Black-Box Approach: Consider Tool Outputs
      - Default errors for typical artifact attributes (XML, Code,…)
    - White-Box Approach: Consider Tool Structure (features & tool components)
      - Default errors for typical tool attributes (Optimizing / Parsing / Searching /…)
- **Management:**
  - Relation between errors: “Subsuming”
  - Assignment of errors to tool chain

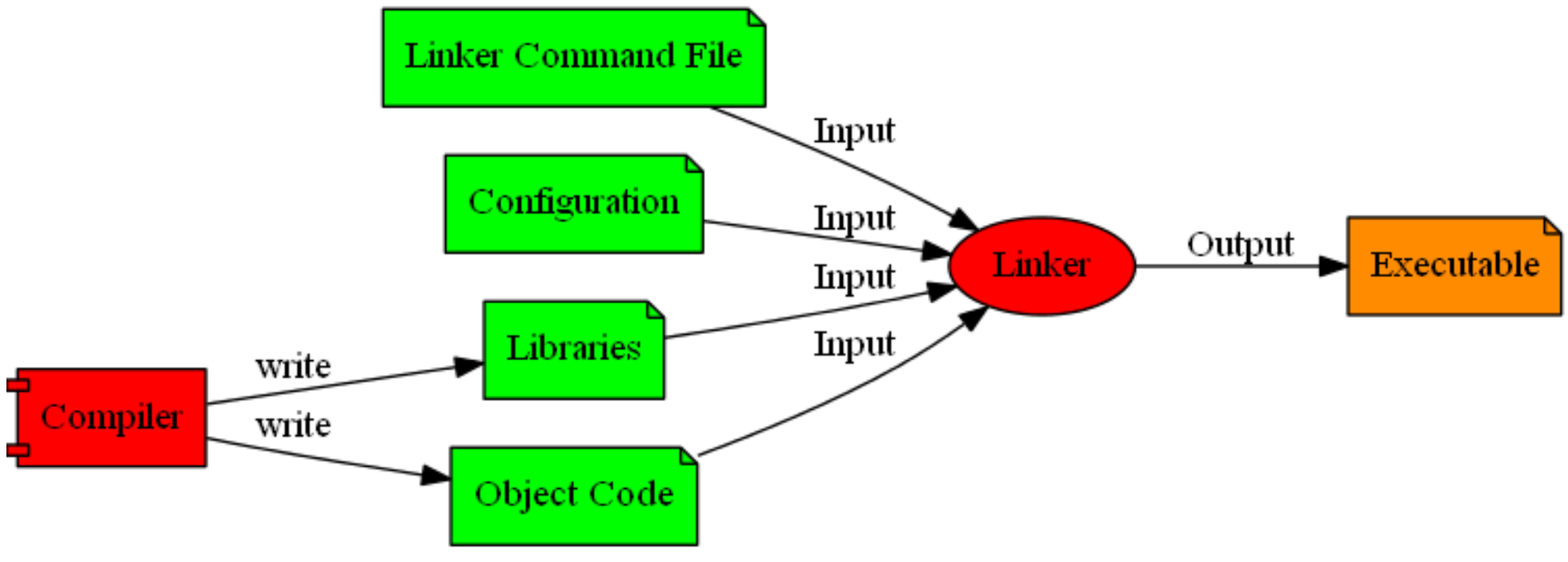
Validation of error model

error model with Default Classes

Tool / Feature Model

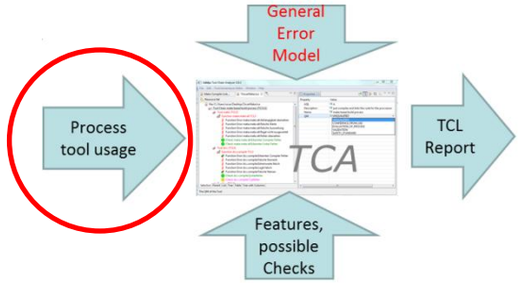


- **Tool provider / expert creates this model**
- **Based on tool analysis**
- **Consisting of**
  - Tools
  - Features with
    - input/output artifacts
    - Potential errors
    - Mitigation possibilities with probabilities (HIGH / MEDIUM / LOW)
      - Checks
      - Restrictions



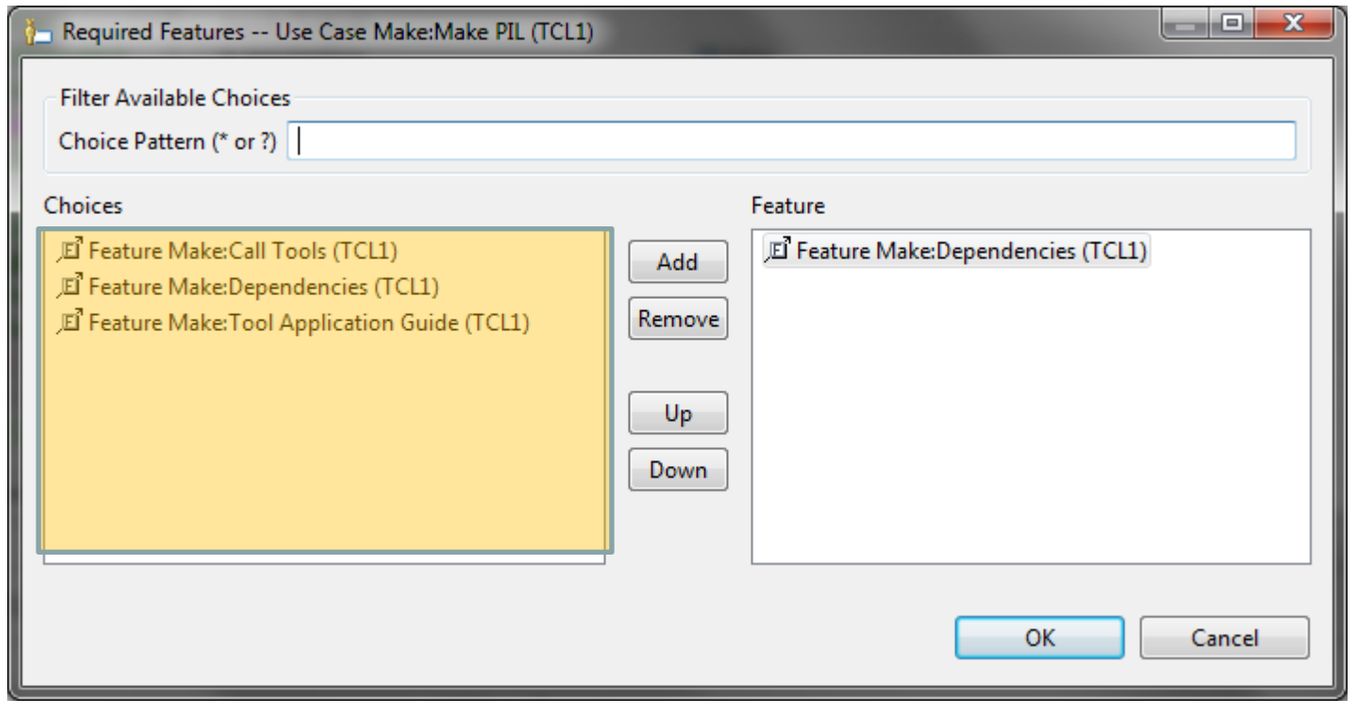
WIND RIVER

Process/Use Case Model



- **User creates this model**
- **Based on his process**
- **Consisting of**
  - Tools
  - Artifacts
  - Use-Cases with
    - input/output artifacts
    - Required features (available from Tool model)

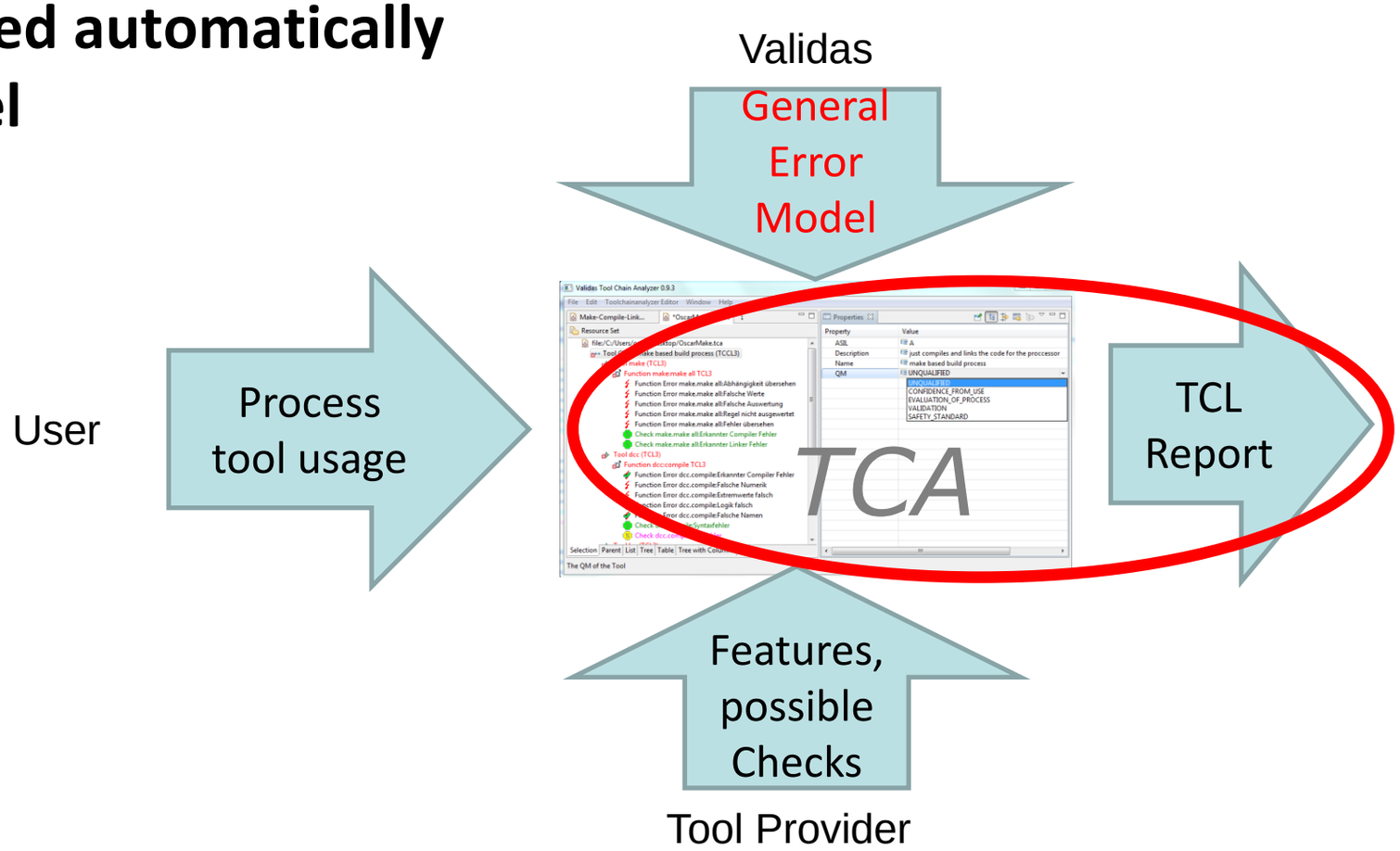
Potential errors are inferred from required features (including proposals for mitigations)



WIND RIVER

Determine Tool Confidence Level

- **Can be computed automatically from the model**



- **Create a report to document the results**

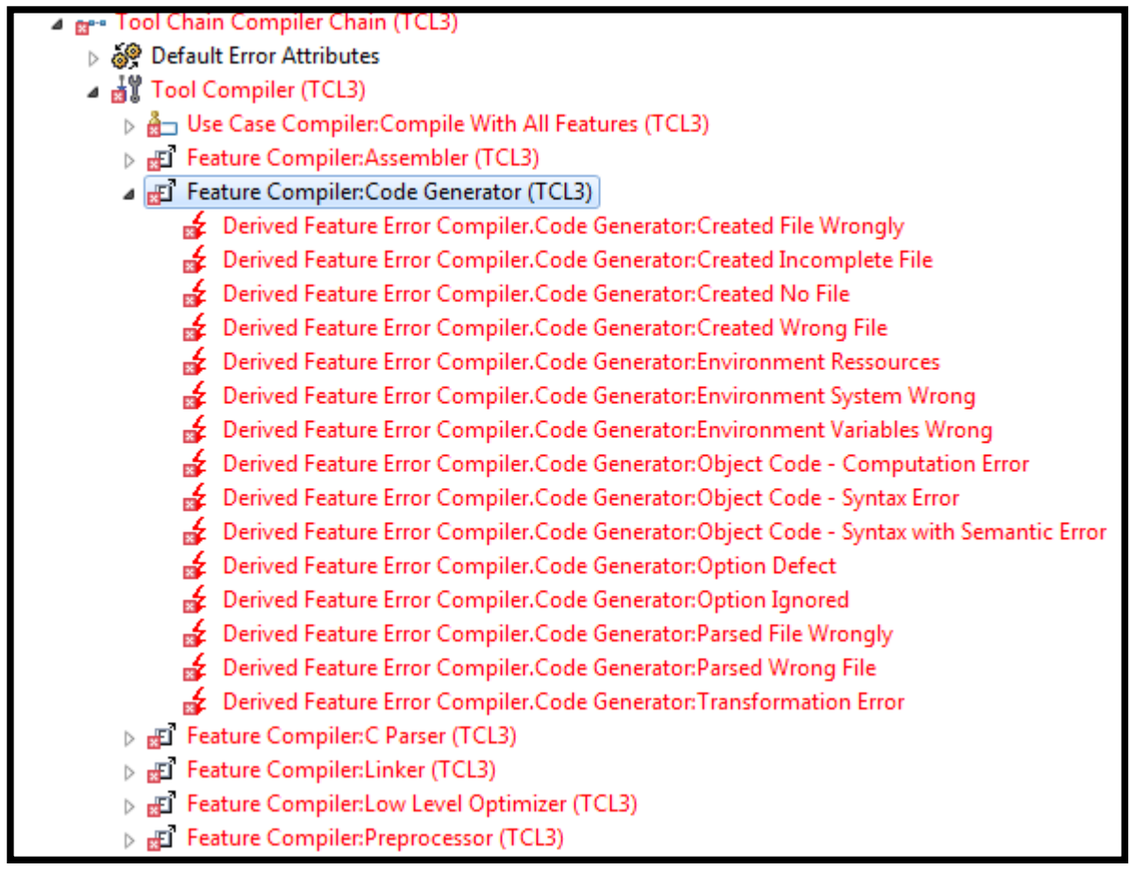
Content: Tool Chain Analysis

- Motivation: ISO 26262: Tool Confidence
- Method: Tool Chain Analysis
  - General Error Model
- **Validas Tool Chain Analyzer**
- Wind River Diab Compiler Qualification Kit

Tool Chain Analyzer (TCA)

- **Automatically determines the TCLs of tools and tool chains**
- **Bases on a formal model of**
  - Tools
  - Use cases (and features)
  - Errors
  - Detection/prevention mechanisms
  - Artifacts (inputs & outputs)
  - Qualifications for tools & features
- **Supports generic error models**
- **Checks the validity of qualifications with a**
- **Generates reports (.docx)**
- **Developed from Validas AG within European research project RECOMP**
  - Rich client, based on Eclipse modeling framework
- **Evaluation available at www.validas.de/TCA152.zip**

Derived Error Model in TCA



recomp
Reduced Certification Costs for trusted Multi-core Platforms

Content: Tool Chain Analysis

- Motivation: ISO 26262: Tool Confidence
- Method: Tool Chain Analysis
  - General Error Model
- Validas Tool Chain Analyzer
- **Wind River Diab Compiler Qualification Kit**

Wind River Diab Compiler

- **Provides Classification Information**
  - Features
  - Potential Errors
- **Provides Qualification Support (Qualification Kit)**
  - Instrumented Compiler
  - Tests
  - Application Method

- **More Details will be presented at http://www.embedded-konferenz.de/**

Summary

- Systematic method to fulfill the ISO 26262 tool requirements
- Generic Error Model for repeatable results
- Validas Tool Chain Analyzer
- Wind River Diab Compiler Qualification Kit

Thank You!

VALIDAS

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

WIND RIVER