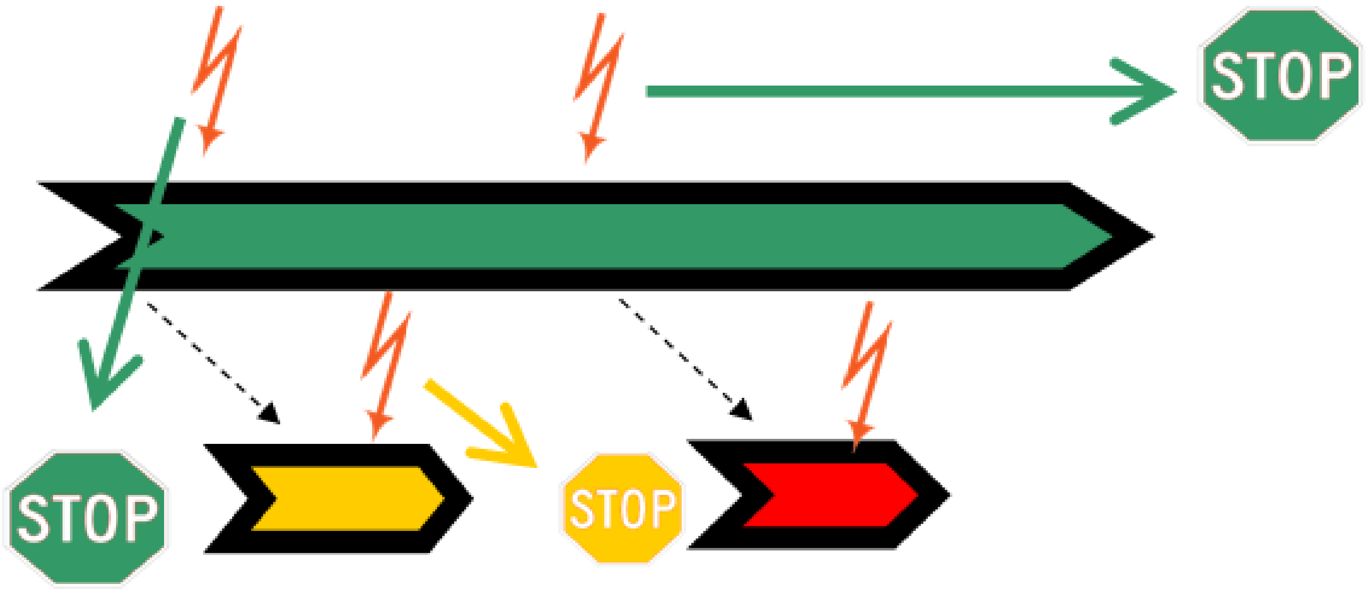
Applying ISO26262 to Tool Qualification



Dr. Oscar Slotosch, Validas AG

Marco Reiling, Wind River

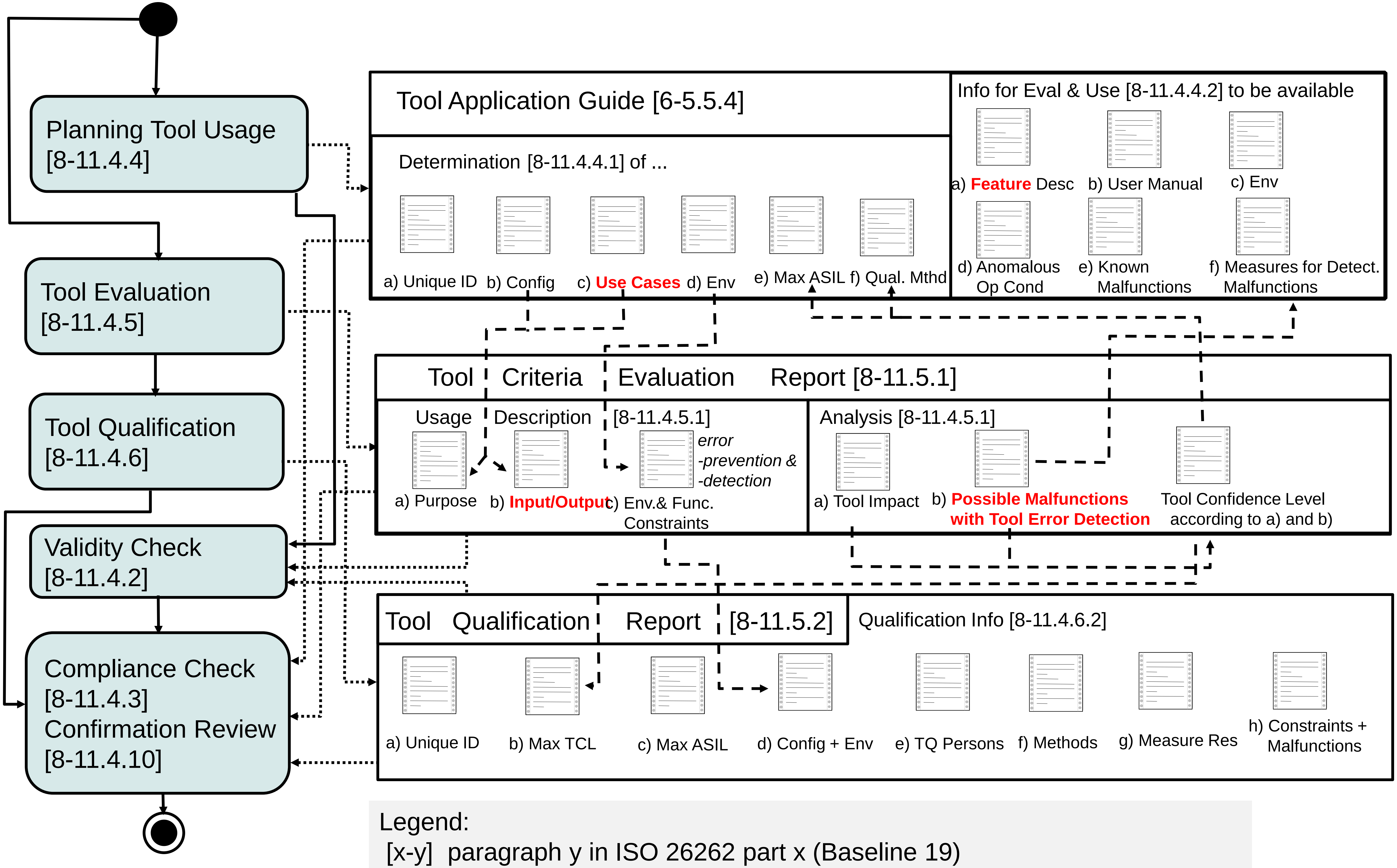
Content: Tool Chain Analysis

- 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



Planning Tool Usage [8-11.4.4]

Tool Evaluation [8-11.4.5]

Tool Qualification [8-11.4.6]

Validity Check [8-11.4.2]

Compliance Check [8-11.4.3] Confirmation Review [8-11.4.10]

Tool Application Guide [6-5.5.4]

Determination [8-11.4.4.1] of ...

a) Unique ID b) Config c) **Use Cases** d) Env e) Max ASIL f) Qual. Mthd

Info for Eval & Use [8-11.4.4.2] to be available

a) **Feature** Desc b) User Manual c) Env

d) Anomalous Op Cond e) Known Malfunctions f) Measures for Detect. Malfunctions

Tool Criteria Evaluation Report [8-11.5.1]

Usage Description [8-11.4.5.1]

a) Purpose b) **Input/Output** c) Env.& Func. Constraints

error -prevention & -detection

Analysis [8-11.4.5.1]

a) Tool Impact b) **Possible Malfunctions with Tool Error Detection**

Tool Confidence Level according to a) and b)

Tool Qualification Report [8-11.5.2]

Qualification Info [8-11.4.6.2]

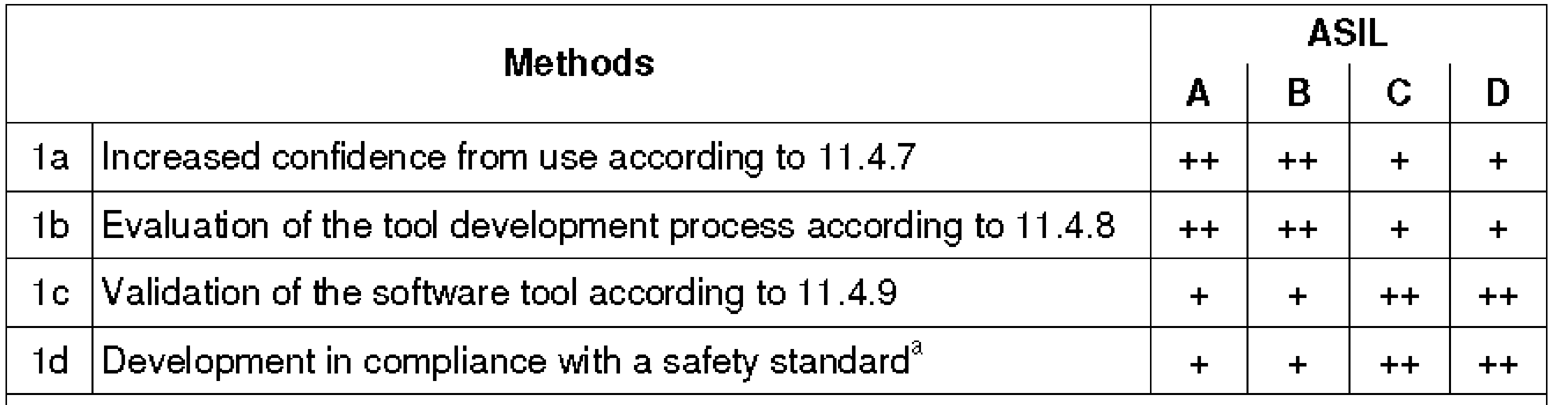
a) Unique ID b) Max TCL c) Max ASIL d) Config + Env e) TQ Persons f) Methods g) Measure Res h) Constraints + Malfunctions

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



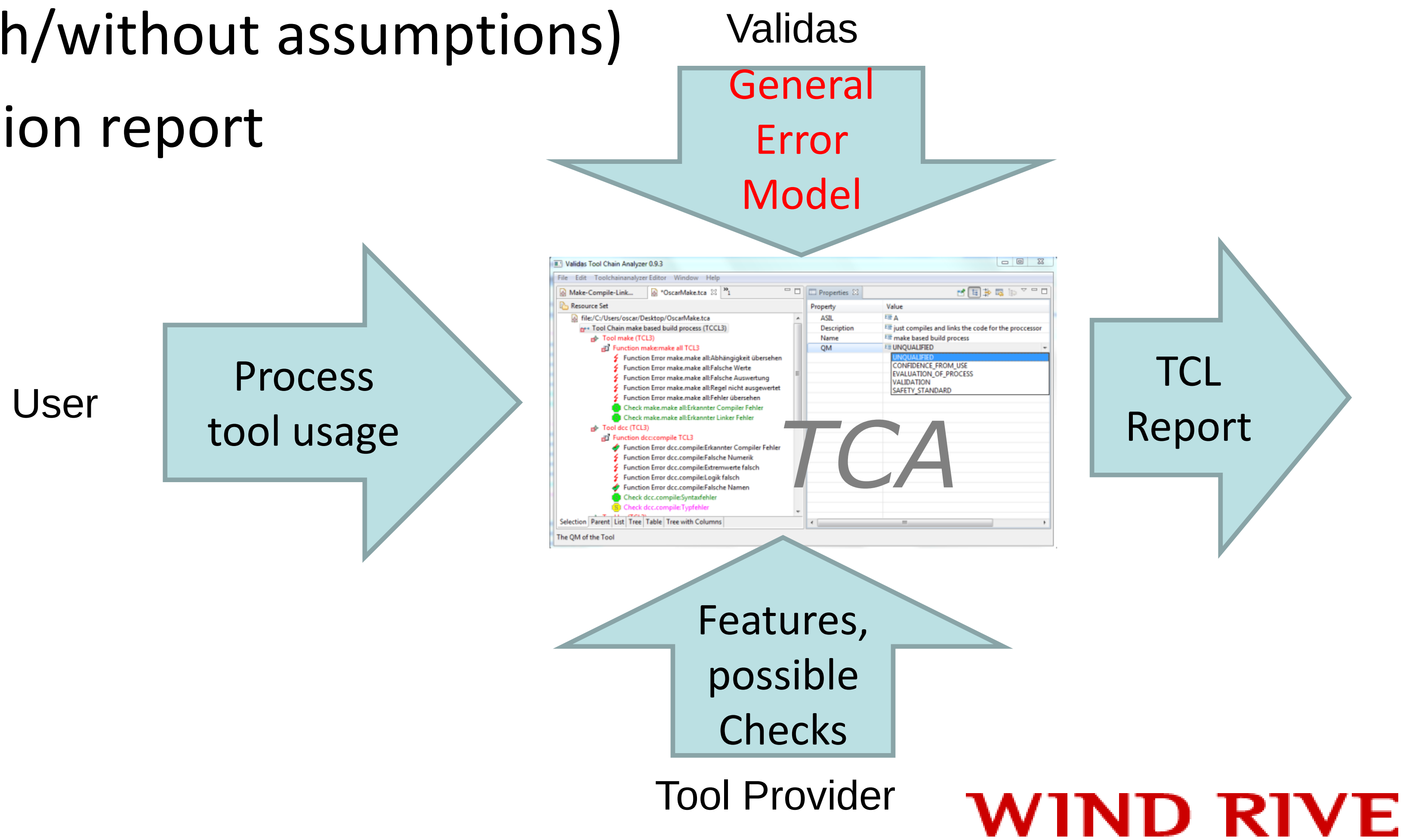
Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use according to 11.4.7	++	++	+	+
1b	Evaluation of the tool development process according to 11.4.8	++	++	+	+
1c	Validation of the software tool according to 11.4.9	+	+	++	++
1d	Development in compliance with a safety standard[a]	+	+	++	++

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**


Validas
General Error Model
User
Process tool usage
TCA
TCL Report
Features, possible Checks
Tool Provider
Validas Tool Chain Analyzer 0.9.3
File Edit Toolchainanalyzer Editor Window Help
Make-Compile-Link...
*OscarMake.tca
Properties
Selection Parent List Tree Table Tree with Columns

Resource Set
- file:/C:/Users/oscar/Desktop/OscarMake.tca
  - Tool Chain make based build process (TCCL3)
    - Tool make (TCL3)
      - Function make:make all TCL3
        - Function Error make.make all:Abhängigkeit übersehen
        - Function Error make.make all:Falsche Werte
        - Function Error make.make all:Falsche Auswertung
        - Function Error make.make all:Regel nicht ausgewertet
        - Function Error make.make all:Fehler übersehen
        - Check make.make all:Erkannter Compiler Fehler
        - Check make.make all:Erkannter Linker Fehler
    - Tool dcc (TCL3)
      - Function dcc:compile TCL3
        - Function Error dcc.compile:Erkannter Compiler Fehler
        - Function Error dcc.compile:Falsche Numerik
        - Function Error dcc.compile:Extremwerte falsch
        - Function Error dcc.compile:Logik falsch
        - Function Error dcc.compile:Falsche Namen
        - Check dcc.compile:Syntaxfehler
        - Check dcc.compile:Typfehler

Property	Value
ASIL	A
Description	just compiles and links the code for the proccessor
Name	make based build process
QM	UNQUALIFIED

UNQUALIFIED
CONFIDENCE_FROM_USE
EVALUATION_OF_PROCESS
VALIDATION
SAFETY_STANDARD

The QM of the Tool

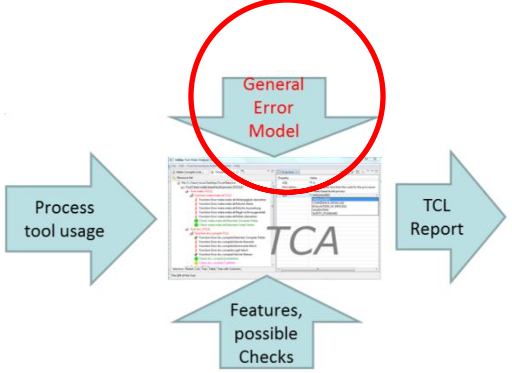
Tool Chain Analysis & Error Model

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

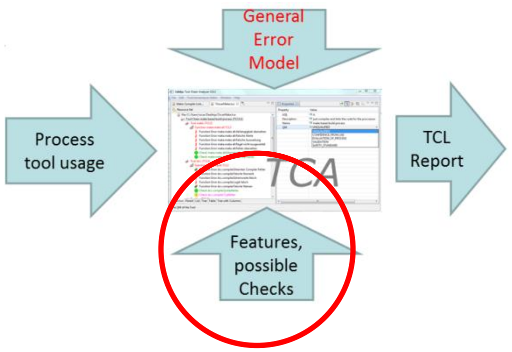


- **Creation Process**
  - Inductive: From known errors to classes of potential errors (“Observing”)
  - Deductive: From tool to potential errors (“Analytic Approach”)
    - Black-Box Approach: Consider Tool Outputs
      - Default errors for typical artifact attributes (XML, Code,…)
    - White-Box 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

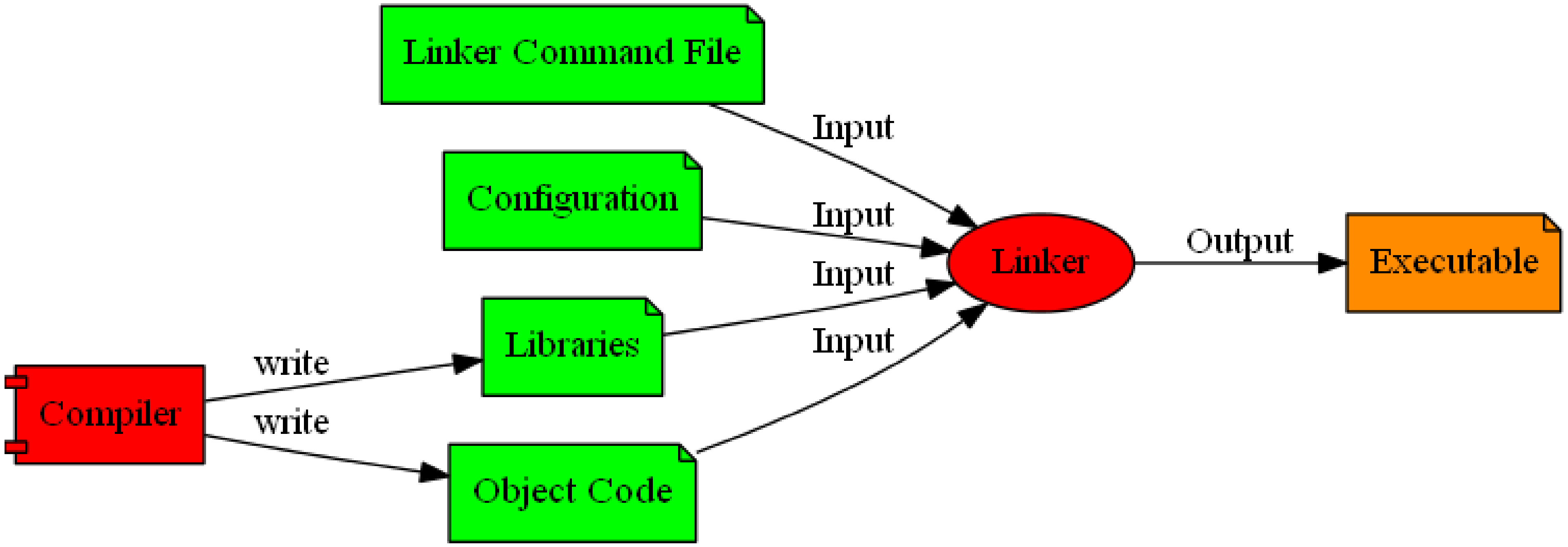
Validation of error model

error model with
Default Classes

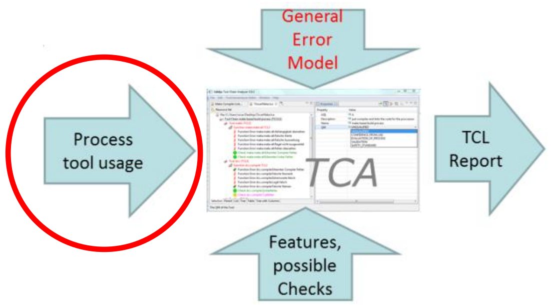
Tool / Feature Model



- 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

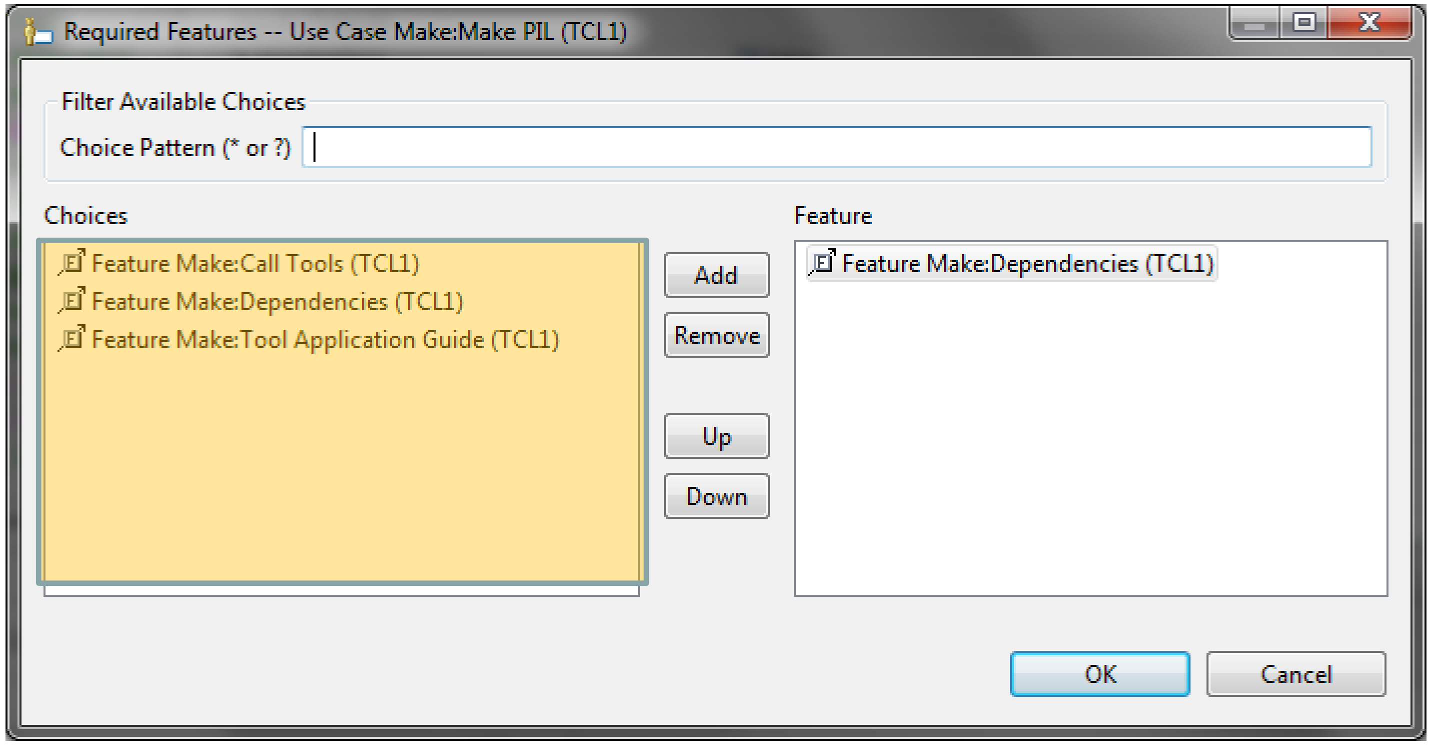


Process/Use Case Model



- 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)



Required Features -- Use Case Make:Make PIL (TCL1)

Filter Available Choices

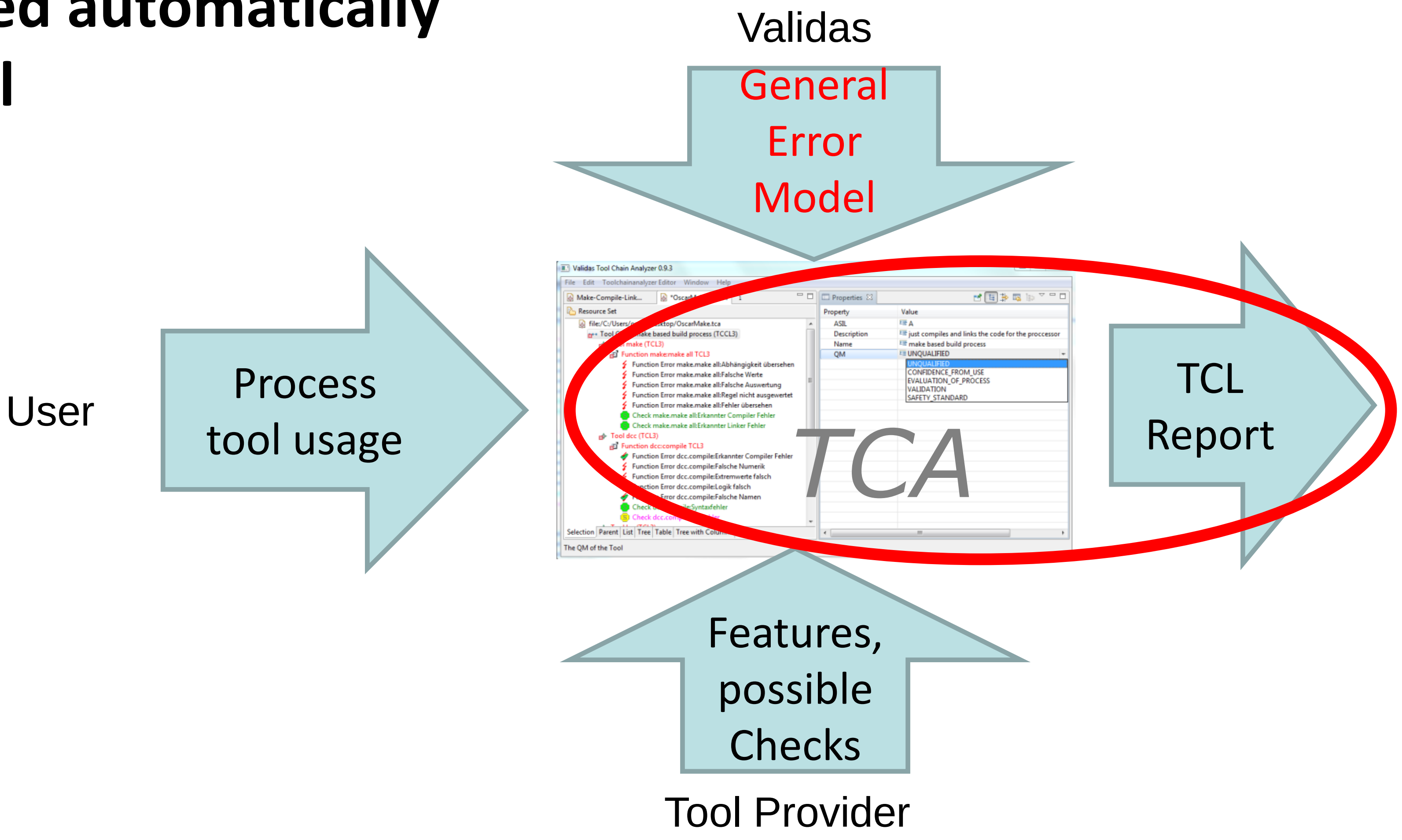
Choice Pattern (* or ?)

Choices
- Feature Make:Call Tools (TCL1)
- Feature Make:Dependencies (TCL1)
- Feature Make:Tool Application Guide (TCL1)

Feature
- Feature Make:Dependencies (TCL1)

Determine Tool Confidence Level

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


Validas
General Error Model
User
Process tool usage
Validas Tool Chain Analyzer 0.9.3
File Edit Toolchainanalyzer Editor Window Help
Make-Compile-Link...
Resource Set
Properties
Selection Parent List Tree Table Tree with Colu
TCA
TCL Report
Features, possible Checks
Tool Provider

file:/C:/Users/o sktop/OscarMake.tca
Tool ake based build process (TCCL3)
make (TCL3)
Function make:make all TCL3
Function Error make.make all:Abhängigkeit übersehen
Function Error make.make all:Falsche Werte
Function Error make.make all:Falsche Auswertung
Function Error make.make all:Regel nicht ausgewertet
Function Error make.make all:Fehler übersehen
Check make.make all:Erkannter Compiler Fehler
Check make.make all:Erkannter Linker Fehler
Tool dcc (TCL3)
Function dcc:compile TCL3
Function Error dcc.compile:Erkannter Compiler Fehler
Function Error dcc.compile:Falsche Numerik
Function Error dcc.compile:Extremwerte falsch
nction Error dcc.compile:Logik falsch
Error dcc.compile:Falsche Namen
Check ile:Syntaxfehler
Check dcc.com

Property	Value
ASIL	A
Description	just compiles and links the code for the proccessor
Name	make based build process
QM	UNQUALIFIED

UNQUALIFIED
CONFIDENCE_FROM_USE
EVALUATION_OF_PROCESS
VALIDATION
SAFETY_STANDARD

The QM of the Tool

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

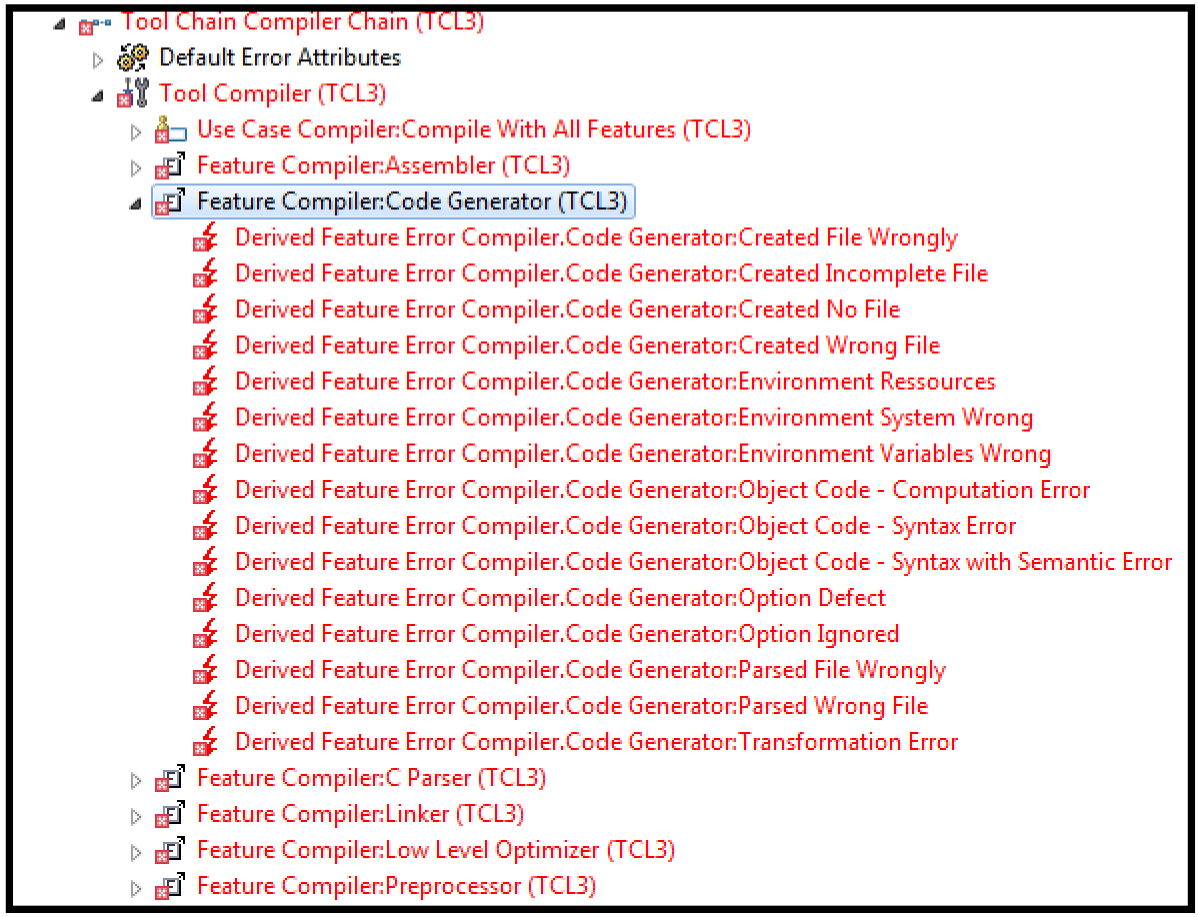
Content: Tool Chain Analysis

- 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



- Tool Chain Compiler Chain (TCL3)
  - Default Error Attributes
  - Tool Compiler (TCL3)
    - Use Case Compiler:Compile With All Features (TCL3)
    - Feature Compiler:Assembler (TCL3)
    - Feature Compiler:Code Generator (TCL3)
      - Derived Feature Error Compiler.Code Generator:Created File Wrongly
      - Derived Feature Error Compiler.Code Generator:Created Incomplete File
      - Derived Feature Error Compiler.Code Generator:Created No File
      - Derived Feature Error Compiler.Code Generator:Created Wrong File
      - Derived Feature Error Compiler.Code Generator:Environment Ressources
      - Derived Feature Error Compiler.Code Generator:Environment System Wrong
      - Derived Feature Error Compiler.Code Generator:Environment Variables Wrong
      - Derived Feature Error Compiler.Code Generator:Object Code - Computation Error
      - Derived Feature Error Compiler.Code Generator:Object Code - Syntax Error
      - Derived Feature Error Compiler.Code Generator:Object Code - Syntax with Semantic Error
      - Derived Feature Error Compiler.Code Generator:Option Defect
      - Derived Feature Error Compiler.Code Generator:Option Ignored
      - Derived Feature Error Compiler.Code Generator:Parsed File Wrongly
      - Derived Feature Error Compiler.Code Generator:Parsed Wrong File
      - Derived Feature Error Compiler.Code Generator:Transformation Error
    - Feature Compiler:C Parser (TCL3)
    - Feature Compiler:Linker (TCL3)
    - Feature Compiler:Low Level Optimizer (TCL3)
    - Feature Compiler:Preprocessor (TCL3)

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/

WIND RIVER

Embedded Konferenz 2012

- Sichere Geräte entwickeln
- Android einsetzen
- Entwicklungseffizienz steigern

3. Juli 2012

Stuttgart, Mövenpick Airport Hotel

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