Oscar Slotosch, Validas AG

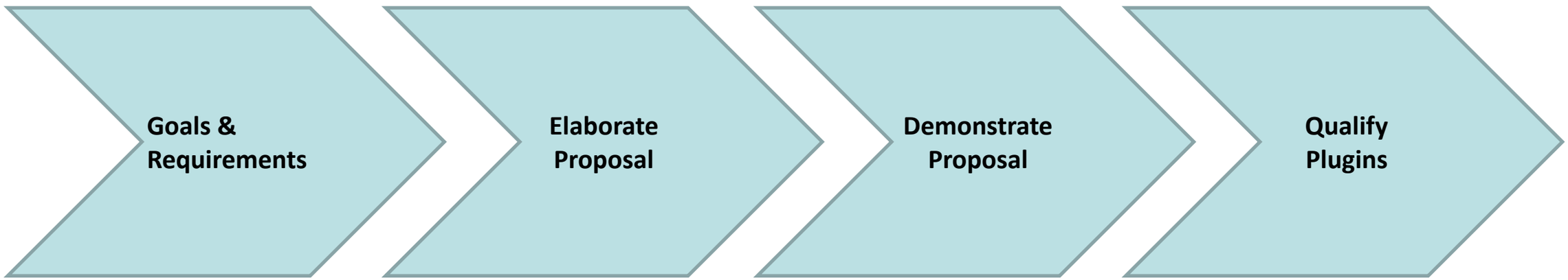
Proposal for a Roadmap towards Development of Qualifyable Eclipse Tools

Content

- **Roadmap**
- Requirements for Tool Qualification (Standards)
- Proposals for Goals for Eclipse
- Proposals for some steps towards Tool Qualification
- First steps on the road
- Summary

Roadmap

- Identify goals & requirements for tool qualification in Eclipse
- Propose process / project
- Demonstrate tool qualification & improve proposal
- Establish proposal: Qualify (selected) plugins



- Is this a Eclipse project? Not a typical ☺
- Is this an Industrial Working Group process?

Content

- Roadmap
- **Requirements for Tool Qualification (Standards)**
- Proposals for Goals for Eclipse
- Proposals for some steps towards Tool Qualification
- First steps on the road
- Summary

Tool Qualification (Summary)

- **Standards require tool qualification: ISO 26262, IEC 61508, DO, EN 50128**
- **Process:**
  - Classify all used tools (Impact, Use-Cases, Artifacts)
  - Qualify critical tools
  - Use tools
- **Qualification Methods ISO 26262**

Table 4 — Qualification of software tools classified TCL3

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

Here is a hole were the new DO-330 standard fits in

- **Some tools provide qualification kits for confidence with evidence into**
  - Correctness of functions by testing them “validatio
  - Development process by documentation
  - ….

Since DO-330 is scalable, here could also be a ++

Extension of the ISO 26262?

- **Possible extension / integration of DO-330 into ISO 26262 could look like:**

11.4.10 Development according to a Safety Standard

11.4.10.1 The DO-330 is the first safety standard that is fully applicable to the development of software tools. It is based on Tool Qualification Levels TQL where TQL-1 is the most rigorous level, while TQL-5 is the least one.

11.4.10.2 The mapping from the TCL to the TQL should depend on the SIL level of the system. The mapping is specified in table 4.

ASIL	TCL 1	TCL 2	TCL 3
D	TQL-5	TQL-2	TQL-1
C	TQL-5	TQL-3	TQL-2
B	TQL-5	TQL-4	TQL-3
A	TQL-5	TQL-5	TQL-4

Table 3: Determination of Tool Qualification Levels for DO-330

11.4.10.3 The tool operational requirements, which are the input for tool development according to DO-330, should cover the use cases analysed in clause 11.4.4

- **Similar chapters exist in DO-178C and DO-254**

Table 12-1 Tool Qualification Level Determination

Software Level	Criteria		
	1	2	3
A	TQL-1	TQL-4	TQL-5
B	TQL-2	TQL-4	TQL-5
C	TQL-3	TQL-5	TQL-5
D	TQL-4	TQL-5	TQL-5

- **Extension is not necessary to apply DO-330 in ISO 26262 but could clarify**

Content

- Roadmap
- Requirements for Tool Qualification (Standards)
- **Proposals for Goals for Eclipse**
- Proposals for some steps towards Tool Qualification
- First steps on the road
- Summary

Goals for Eclipse IWG

- **Exchange & share knowledge**
  - Motivate developers & community to provide qualifyable plugins
- **Provide classification support to users of Eclipse tools**
- **Support the development of qualifyable tools (“Qualification Kits”)**
  - Validation
  - Safety-Standard (DO-330)
- **Apply this to reference tools ARTOP, EMF,… ?**

- **Current status (web-page):**

Auto IWG WP5

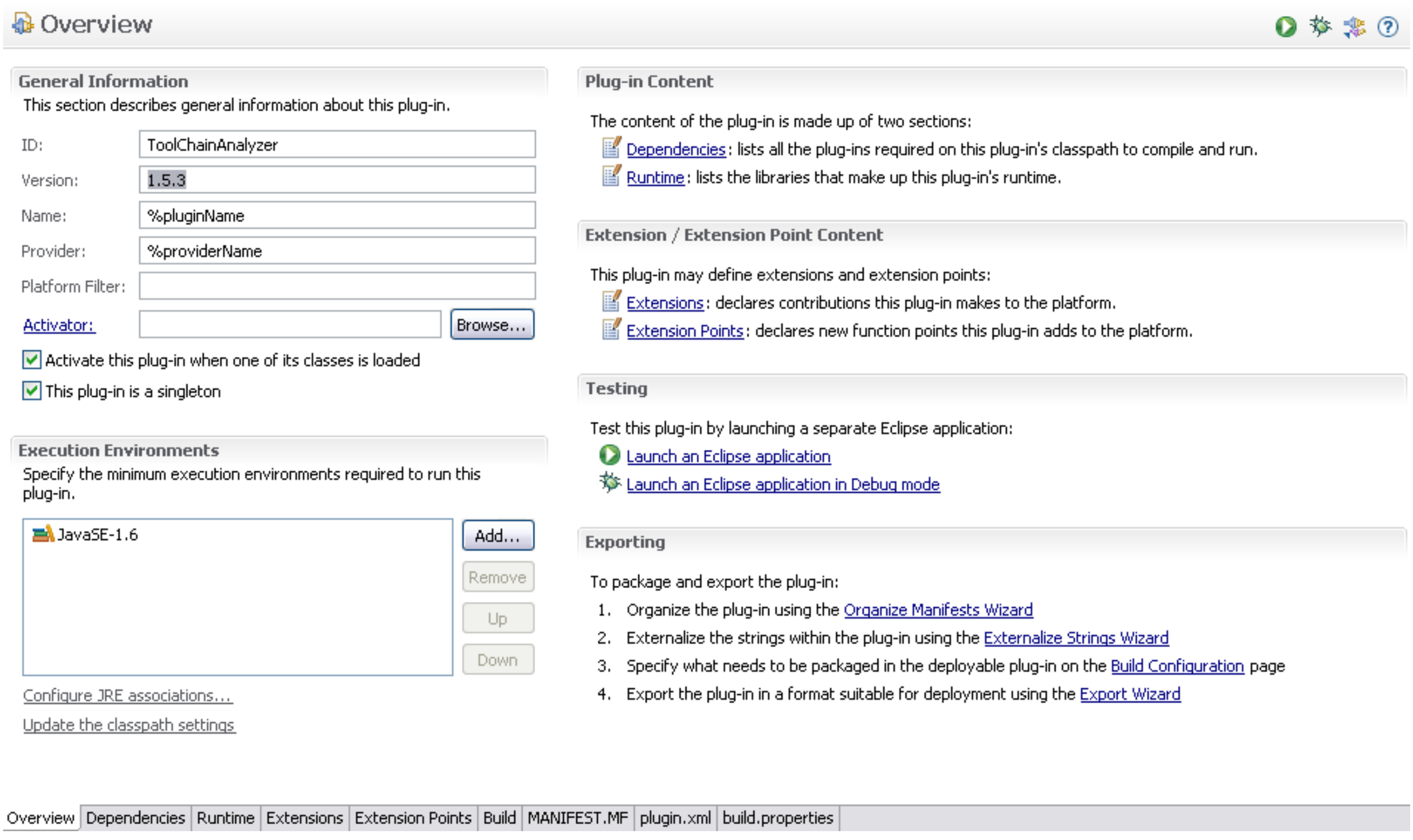
WP5: Eclipse Qualification Kit (ISO26262)

This is work package 5 of the Automotive Industry Working Group.

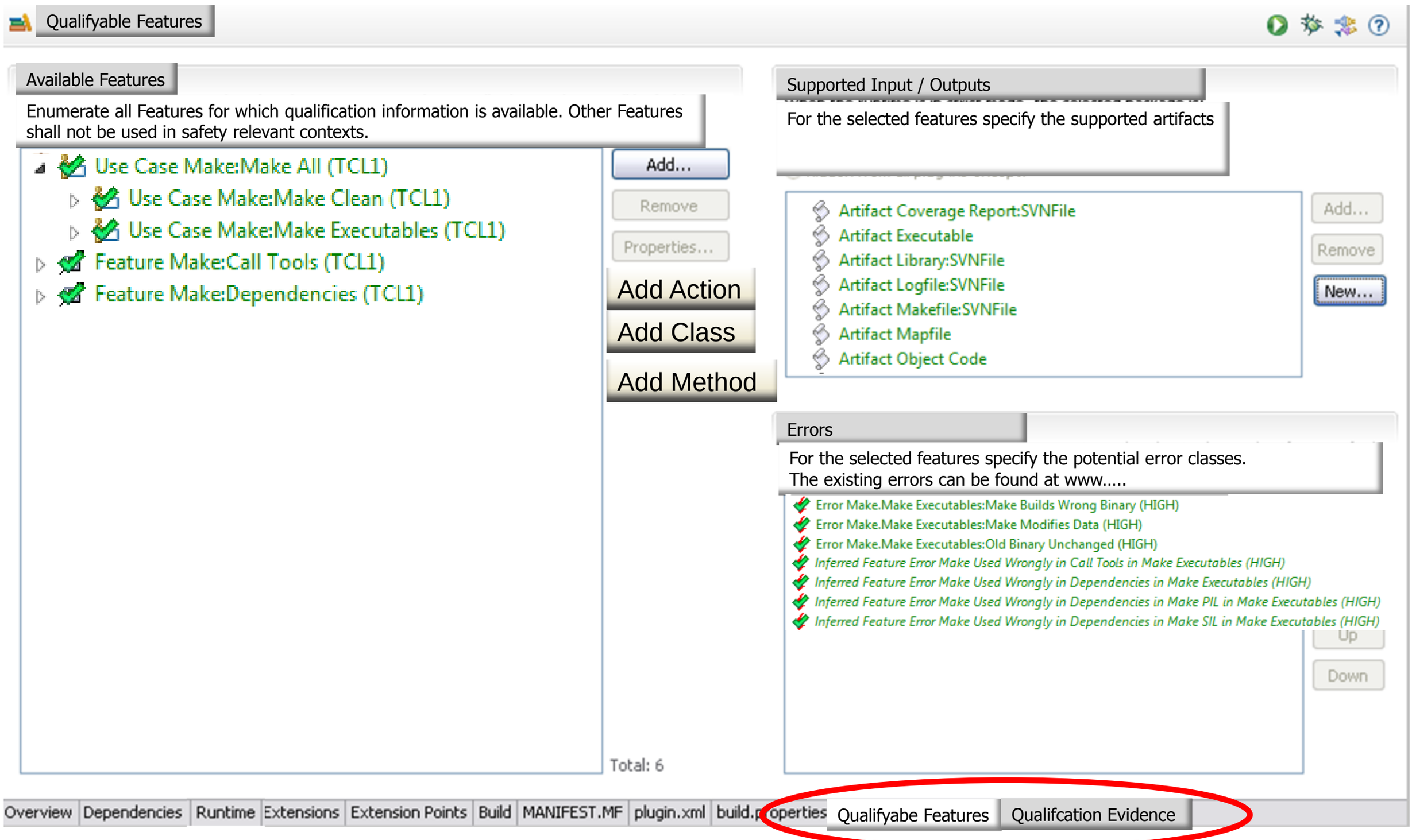
- WP Lead: Bredex (temporary)

Need to share knowledge and resources in the classification/qualification activities of eclipse related products.

Current Eclipse Metadata



Vision: Eclipse Classification Data



Proposed Role: Eclipse Validator

There is much (different) work to do such that we need a new kind of worker: The Validator

- **Should provide confidence**
- **Should be more formalized than a committer**
- **Should have qualifications e.g. by filling out questionnaires on**
  - Eclipse qualification process
  - DO-330
- **Should have responsibilities (answer to questions)**
- **Should earn "credits" for each successful validation action**
  - Executed reviews
  - Formulated requirements
  - Created use/test cases
  - Feedback
  - …
- **Comparable:**
  Confidence in ebay:

slotosch (25 ★)

Positive Bewertungen (der letzten 12 Monate): 100%
[Wie wird der Prozentsatz positiver Bewertungen berechnet?]

Mitglied seit: 01.04.99 in Deutschland

Content

- Roadmap
- Requirements for Tool Qualification (Standards)
- Proposals for Goals for Eclipse
- **Proposals for some steps towards Tool Qualification**
- First steps on the road
- Summary

Proposals

Following activities are necessary to achieve goals:

- **Agree on focus, e.g. “Metadata extension for qualification information”**
- **Provide classification support to users of plugins**
  - Use case
  - Potential errors
  - Possible mitigations for errors
  - TCL inference
- **Provide qualification support**
  - Create checklist for DO-330 requirements (depending on the TQL)
    - Qualification data (general, plugin specific, user adaptable)
    - Requirements (general, development, operational)
  - Check Eclipse against the checklist, create
    - Mapping of Eclipse -> DO-330
    - Identify gaps: missing data/requirements
  - Provide model (EMF?) for the missing data
- **Demonstrate it: Small example e.g. EclipseCon**
- **Validate it: bigger example**

Content

- Roadmap
- Requirements for Tool Qualification (Standards)
- Proposals for Goals for Eclipse
- Proposals for some steps towards Tool Qualification
- **First steps on the road**
- Summary

First Steps on the Road

- **Create a checklist to show the DO-330 compliance**
- **Make a/some simple example tool(s) that shall comply with DO-330**
- **Work on selected topics: Requirements, Test, Code, …**
  - Analyze existing Eclipse process
  - Analyze possibilities for the topic e.g. RIF, tracing, tests,…
  - Create example document (eventually based on existing methods)
  - Check DO-330 compliance
  - Create model (for creation of document)
  - Review/Validate for:
    - Expressiveness
    - practicability
    - possible improvements
  - Make proposal for Eclipse integration (part)
- **Until DO-330 is completely satisfyable**
- **Make integrated proposal for Eclipse Extension (EMF,..)**

Checklist for DO-330 compliance

- **Create an Checklist for DO-330 compliance (unvalidated) draft:**

DO330.xlsx - Microsoft Excel

Datei | Start | Einfügen | Seitenlayout | Formeln | Daten | Überprüfen | Ansicht

Normal | Seitenlayout | Umbruchvorschau | Benutzerdef. Ansichten | Ganzer Bildschirm | Arbeitsmappenansichten

Lineal | Bearbeitungsleiste | Gitternetzlinien | Überschriften | Anzeigen

Zoom | 100 % | Fenster einfrieren | Zoom

Neues Fenster | Alle anordnen | Fenster einfrieren | Teilen | Ausblenden | Einblenden | Nebeneinander anzeigen | Synchroner Bildlauf | Fensterposition zurücksetzen | Aufgabenber. speichern | Fenster wechseln | Fenster

Makros | Makros

B46: The Tool Requirements should include all functional and interface-related requirements that will be implemented in the tool.

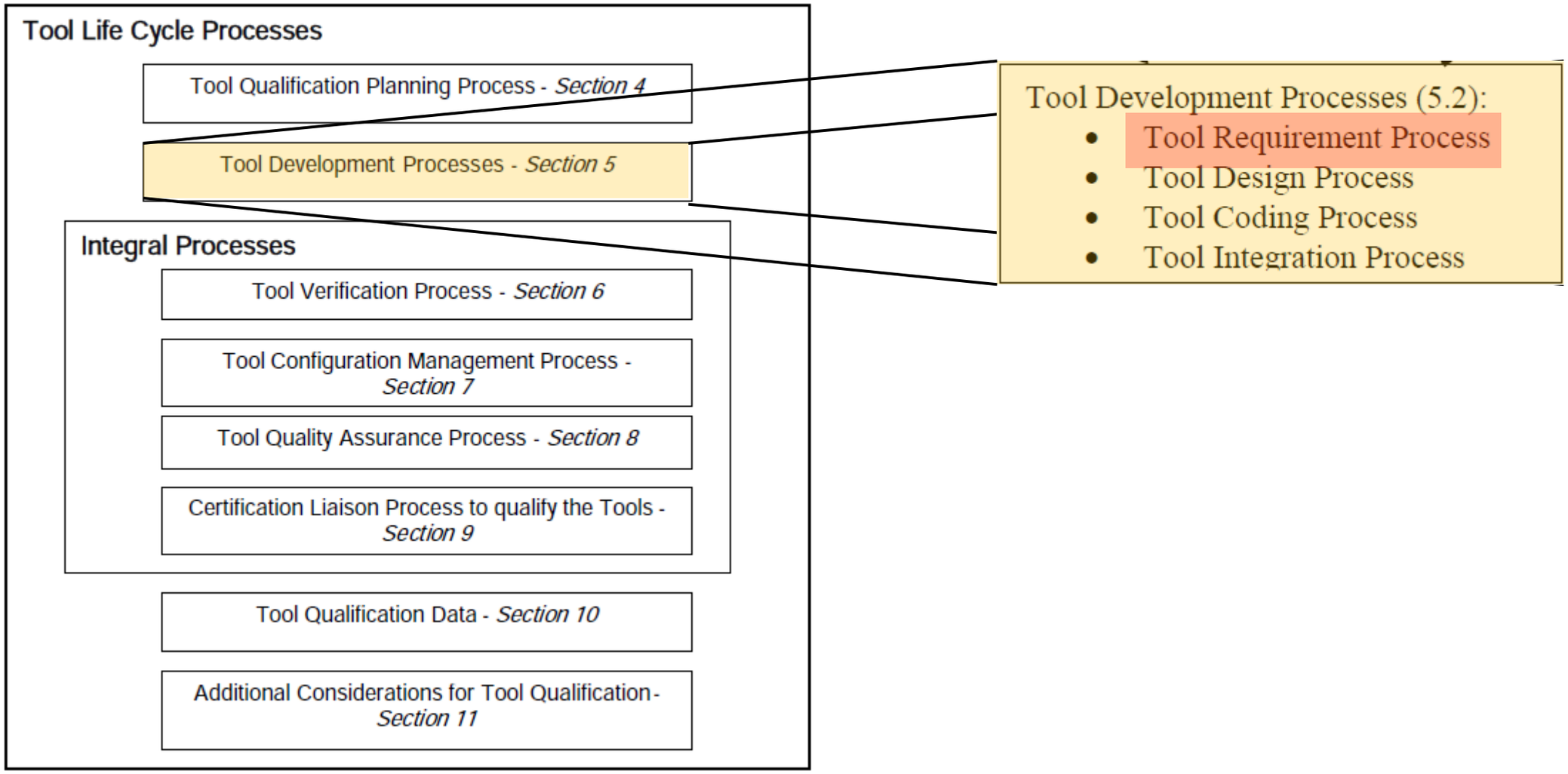
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	ID	Content	Process	Output	TQL1	TQL2	TQL3	TQL4	TQL5	TQL1	TQL2	TQL3	TQL4	TQL5
44	5.2.1.2	Tool Requirements Activities	Tool Development Life Cycle	see subitems										
45	5.2.1.2.a	The Tool Requirements should be developed and docu	Tool Development Life Cycle	Tool Requirements/ Trace Data	Sat	Sat	Sat	Sat	Private	CC1	CC1	CC1	CC1	Private
46	5.2.1.2.b	The Tool Requirements should include all functiona	Tool Development Life Cycle	Tool Requirements/ Trace Data	Sat	Sat	Sat	Sat	Private	CC1	CC1	CC1	CC1	Private
47	5.2.1.2.c	The Tool Requirements should be developed followin	Tool Development Life Cycle	Tool Requirements/ Trace Data	Sat	Sat	Sat	Sat	Private	CC1	CC1	CC1	CC1	Private
48	5.2.1.2.d	The Tool Requirements should be developed using th	Tool Development Life Cycle	Tool Requirements/ Trace Data	Sat	Sat	Sat	Sat	Private	CC1	CC1	CC1	CC1	Private
49	5.2.1.2.e	The Tool Requirements should be verifiable and consi	Tool Development Life Cycle	Tool Requirements/ Trace Data	Sat	Sat	Sat	Sat	Private	CC1	CC1	CC1	CC1	Private
50	5.2.1.2.f	The Tool Requirements should be defined such that al	Tool Development Life Cycle	Tool Requirements/ Trace Data	Sat	Sat	Sat	Sat	Private	CC1	CC1	CC1	CC1	Private
51	5.2.1.2.g	Each Tool Requirement should trace to one or more To	Tool Development Life Cycle	Tool Requirements/ Trace Data	Sat	Sat	Sat	Sat	Private	CC1	CC1	CC1	CC1	Private
52	5.2.1.2.h	Derived tool requirements are those not traceable to	Tool Development Life Cycle	Tool Requirements/ Trace Data	Sat	Sat	Sat	Sat	Private	CC1	CC1	CC1	CC1	Private
53	5.2.1.2.i	The Tool Requirements should provide user instructio	Tool Development Life Cycle	Tool Requirements/ Trace Data	Sat	Sat	Sat	Sat	Private	CC1	CC1	CC1	CC1	Private
54	5.2.1.2.j	The Tool Requirements should identify requirements	Tool Development Life Cycle	Tool Requirements/ Trace Data	Sat	Sat	Sat	Sat	Private	CC1	CC1	CC1	CC1	Private
55	5.2.1.2.k	The Tool Requirements should be defined to a level o	Tool Development Life Cycle	Tool Requirements/ Trace Data	Sat	Sat	Sat	Sat	Private	CC1	CC1	CC1	CC1	Private
56	5.2.2	Tool Design Process	Tool Development Life Cycle	see subitems, 10.2.2										

Requirements & Activities | TCM Process Activities | Tabelle3

Bereit | 100 %

DO-330 Topics

- **Structure of DO-330**



Existing Methods: Requirements

- **Currently not practiced in Eclipse**
- **RMF / ProR (Incubation):**

ProR

Reqlf-Model.rif | Specification Document

Specification Document

	ID	Description	Link
1	REQ-1	Dies ist eine Demo von ProR	0 ▷ R ▷ 2
	▷		REQ-5
	▷	Links können auch Attribute haben.	REQ-6
1.1	REQ-2	Hierarchien beliebiger Tiefe werden unterstützt.	
1.2	REQ-3	Der Linke Rand hilft bei der Orientierung	
1.2.1	REQ-4	... und die erste Spalte wird eingerückt.	
2	REQ-5	Im Properties-View werden alle Attribute angezeigt.	1 ▷ R ▷ 0
3	REQ-6	Im Editor nur die, die man sehen will.	1 ▷ R ▷ 0

- **general approach, not tailored for tool requirements**
- **Adoptable to tool requirements by creating corresponding requirements types**
- **First Investigation**
  - Nice usability e.g. for creating new requirements
  - Polymorphic links (any requirement can be linked)
  - Extensible to design / test / …?
  - Do we need RIF within Eclipse?

Create DO-330 Conformant Example

Tool Requirements for Tool Chain Analyzer
Version 0.2
Validas AG

3 General Information

This section contains the general information on the Tool Chain Analyzer generated from the corresponding plugin metadata

- Name: Tool Chain Analyzer
- ID: de.validas.toolchainanalyzer
- Version: 1.5.3
- Provider: Validas AG
- Tool Qualification Level (TQL): TQL-1

from MANIFEST.MF

Overview

General Information

This section describes general information about this plug-in.

ID:	de.validas.toolchainanalyzer
Version:	1.5.3
Name:	Tool Chain Analyzer
Provider:	Validas AG
Qualification Level	TQL-1

?

From Tool Requirements Model

5.4 Customization Requirements

The tool shall be customized to the resources of the computer were it is executed.

5.4.1 Stack Size

The stack size shall be settable. The default stack size should be 400 MB

5.4.2 Heap Size

The heap size shall be settable. The default hap size should be 1000 MB.

5.5 Tool Interface Requirements

The tool chain analyzer shall have the following interfaces.

5.5.1 Graphical User Interface

The graphical user interface consists of different views and property dialogs.

5.5.1.1 Structure View

The structure view represents the tool chain models in a tree view with the structure how the elements are modeled. The structure views also contains the actions to created, move and delete elements. Furthermore it can be used to start actions like the im- and export of tool models.

5.5.1.2 Property View

The property view shows the properties (attributes and relations) of the elements selected in the tree view. They can be edited either directly in the view or in property dialogs the start when the elements are double-clicked.

5.5.1.3 Property Dialogs

The property dialogs are used to edit long text fields or complex relations in the modeled elements. They are started from the property view.

5.5.1.4 Flow View

The flow view shows the information flows within the model, e.g. from one tool to another via the artifact that is written and read. Furthermore the error derivation flow from the general error model to the features and use cases.

5.5.2 File Interface

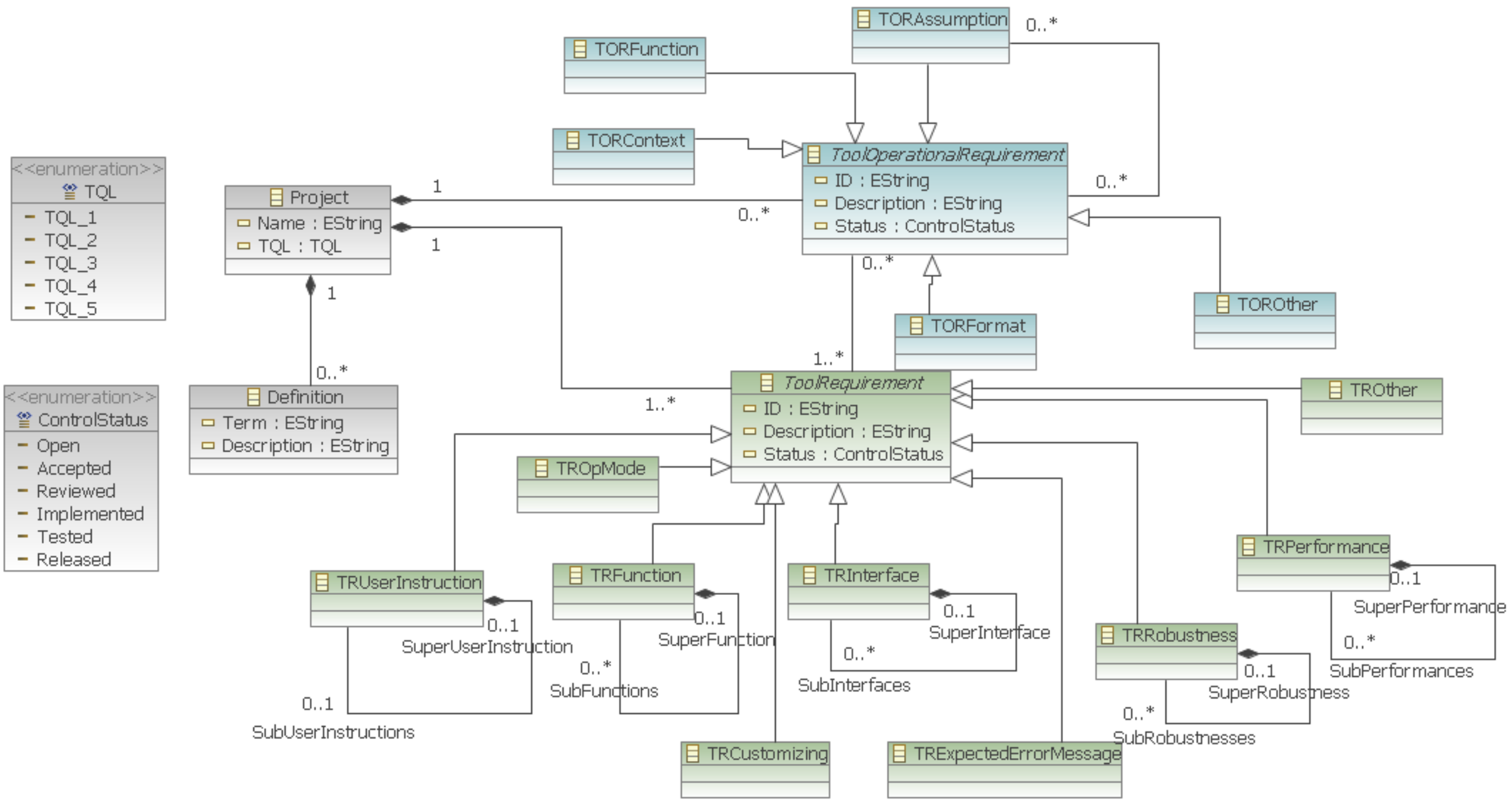
The tool chain models shall be persistent to files. The tool chain analyzer loads models from files and writes the back into files.

5.5.3 DOT Interface

For drawing the images to explain the error flow in the model the graphviz tool with the DOT language. The intermediate files are accessible and can be modified or integrated into other images.

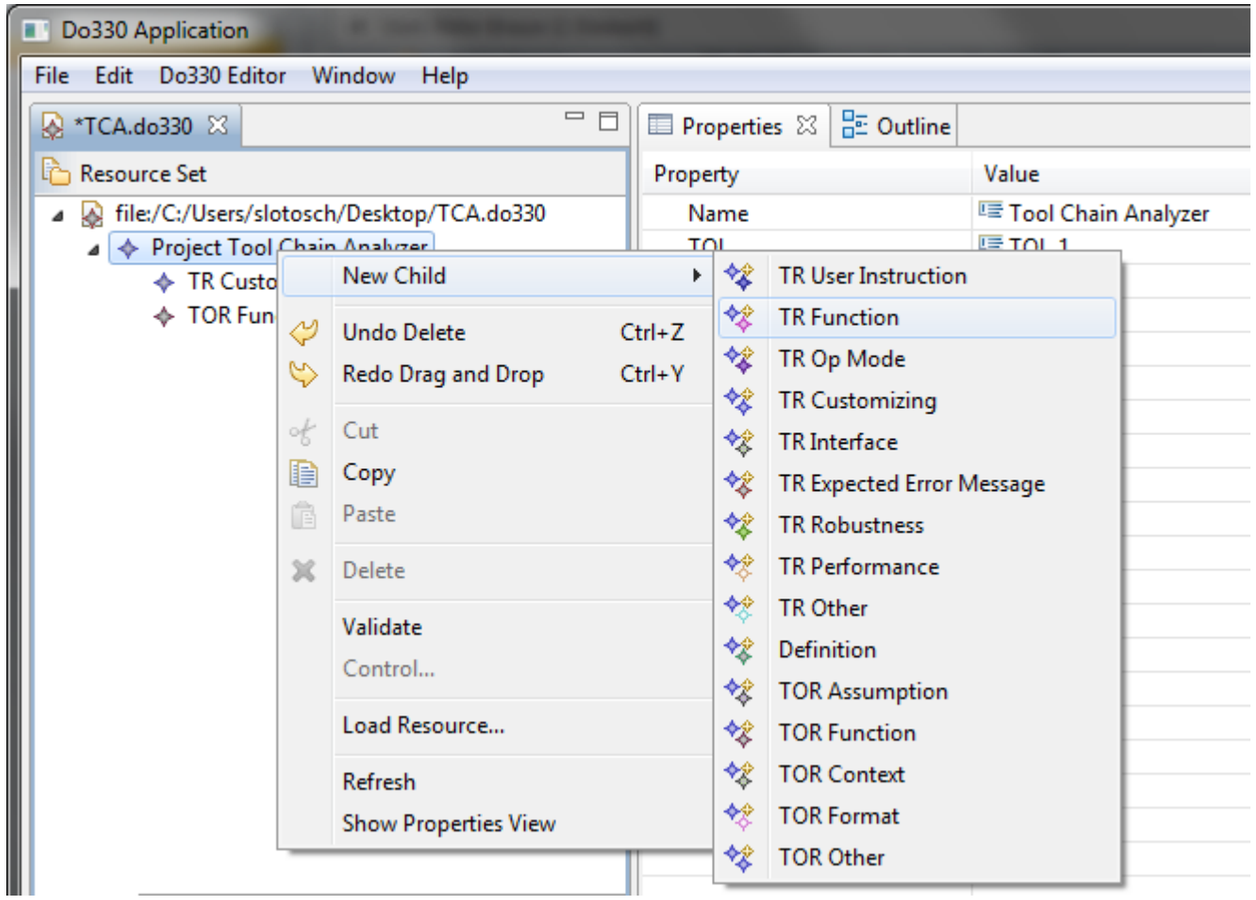
Create Model for Tool-Requirements

- **EMF-Metamodel (Draft) for Tool Requirements**

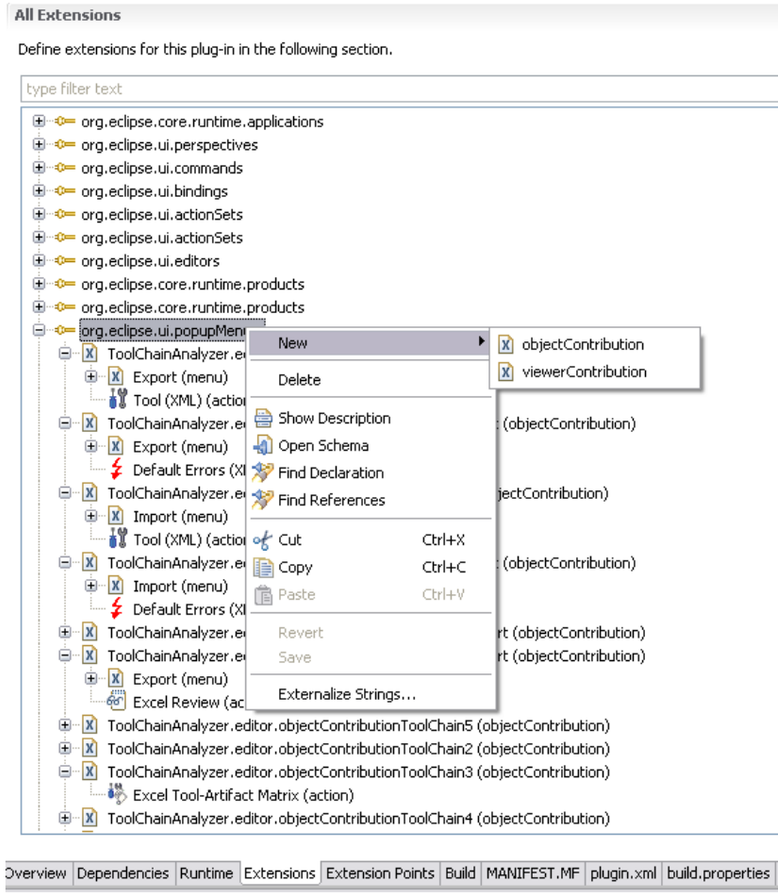


Create Example Model

- **Using the default EMF Editor**



Comparable: Plugin Extension



- **Shows how simple requirements could be created with Eclipse**
- **The example (DO-330 conforming) document can be generated completely from the model**
- **Tracing: TOR <-> TR is done using Eclipse association editors**

Content

- Roadmap
- Requirements for Tool Qualification (Standards)
- Proposals for Goals for Eclipse
- Proposals for some steps towards Tool Qualification
- First steps on the road
- **Summary**

Summary

- **Roadmap towards development of qualifyable Eclipse tools & plugins**
  - Classification
  - Qualification
  - Usage
- **Applicable to all relevant standards (ISO 26262, IEC 61508, DO-178C, EN 50128,..)**
- **Metadata extension for qualification information of plugins**
- **Much work to do**
  - Checklist
  - Gaps & Mapping
  - Extension of Eclipse processes, metadata, community
  - Improve eclipse plugins where needed
- **First steps started**
- **Proposed new role for that work: Eclipse Validator**
- **Validas will contribute**

Thank You!

VALIDAS

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