Optimizing Tool Qualification Efforts

1st Tool Qualification Symposium

Dr. Jürgen Klarmann
Embedded Software and Safety Consulting

Optimizing Tool Qualification Efforts

Overview

- Company Background
- Introduction to Tool Qualification
- Tool Landscape
- Example: 7-zip
- Qualification Effort Optimization
  - Cost Modeling
  - Cost Optimization
  - Example: 7-zip
- Summary

Optimizing Tool Qualification Efforts

ETAS – Company Data

– ETAS – Locations Around the Globe

ETAS GmbH

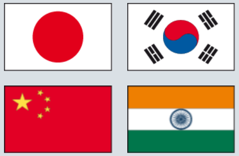
Founded	1994
Shareholder	100 % Robert Bosch GmbH
Headquarters	Stuttgart, Germany 18 additional offices worldwide

Europe

505 employees

Locations
Stuttgart/Germany, St. Ouen/France, Derby, York/UK, Trollhättan/Sweden, Turin/Italy, Moscow/Russian Federation

Asia-Pacific



127 employees

Locations
Yokohama, Nagoya/Japan, Seoul/Korea, Shanghai, Beijing, Wuhan, Chongqing, Changchun/P.R. China, Bangalore, Pune/India

Americas

52 employees

Locations
Ann Arbor/USA, São Paulo/Brazil

Optimizing Tool Qualification Efforts

ETAS – Software and Safety Consulting

- Independent Business Field of ETAS

- Offer Consulting and engineering services in the areas of:
  - Embedded SW development/AUTOSAR
  - Functional Safety
  - Embedded Security (in partnership with ESCRYPT and CoC-Security)
  - Systems Engineering
  - Process Improvement

- Serves Bosch internal and external customers

- Currently located in Feuerbach, York, Ann Arbor and Bangalore

Optimizing Tool Qualification Efforts

Overview

- Company Background
- Introduction to Tool Qualification
- Tool Landscape
- Example: 7-zip
- Qualification Effort Optimization
  - Cost Modeling
  - Cost Optimization
  - Example: 7-zip
- Summary

Optimizing Tool Qualification Efforts

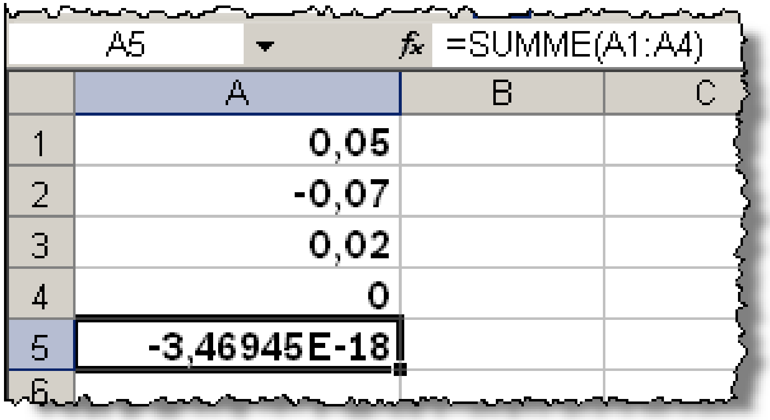
Introduction

- Tools consisting of software that are used in the development of safety relevant vehicle functions

Software Tool ≠ Tool for Software Development

- „*Confidence in the use of software tools*“ is described in **ISO 26262, part 8, chapter 11**

- **Objective**: A malfunction of a software tool must not lead to a violation of a safety goal.



A5 ▾ fx =SUMME(A1:A4)

	A	B	C
1	0,05		
2	-0,07		
3	0,02		
4	0		
5	-3,46945E-18		
6			

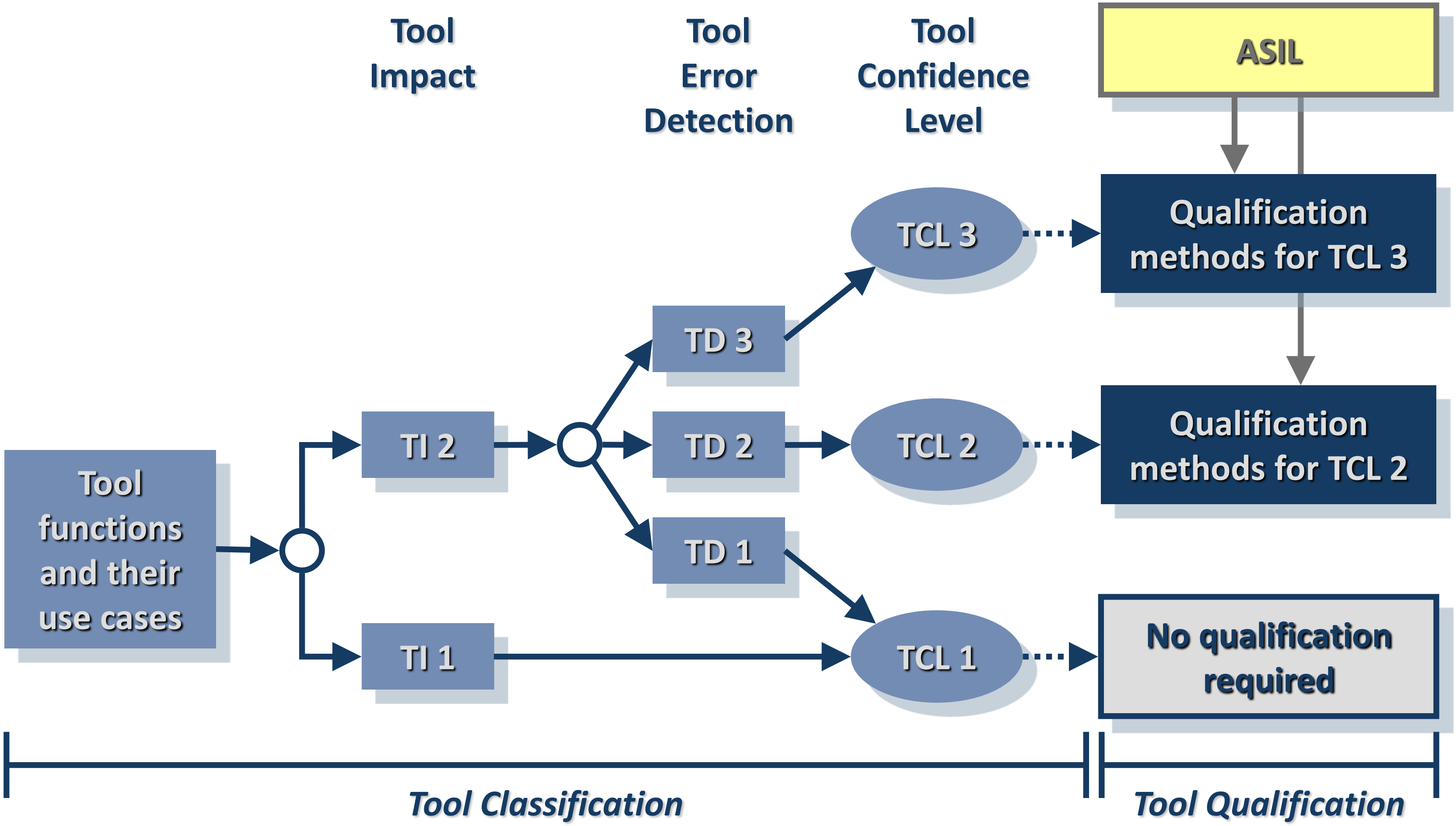
Experiences with qualification of software tools

Introduction

- 2 Steps: **Tool Classification** & **Tool-Qualification**
- Classification considers the software tool's **embedding in the product development process**
  - Use cases, Tool Impact: *What is being done with the tool?*
  - Tool Error Detection: *How well is erroneous tool output avoidable or detectable (e.g. tests, reviews)?*
- Consequence: Classification may only be done in the context of a tool use
- Responsibility lies with the tool users

Optimizing Tool Qualification Efforts

Introduction



Optimizing Tool Qualification Efforts

Overview

- Company Background
- Introduction to Tool Qualification
- Tool Landscape
- Example: 7-zip
- Qualification Effort Optimization
  - Cost Modeling
  - Cost Optimization
  - Example: 7-zip
- Summary

Optimizing Tool Qualification Efforts
Tool Landscape

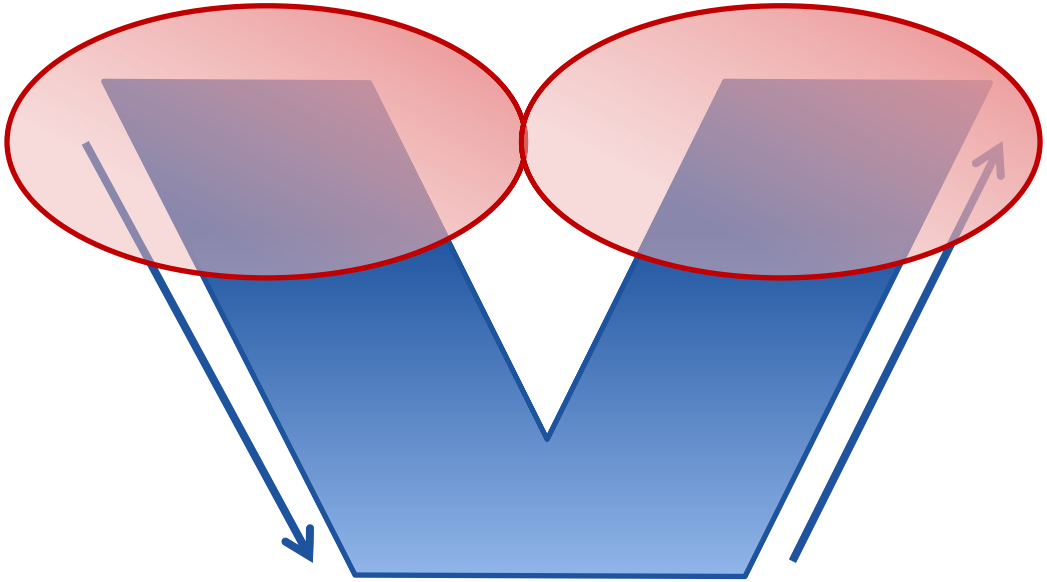
- **Safety relevant domains referring to tool qualification**
  - From the point of view of tool qualification, most safety relevant tools are located in the domains of the **upper left and of the upper right corner of the V-shaped development process**
  - It is hard to execute protection measures at the borders of the development process
  - Thus, the following domains are per se safety relevant for tool qualification:
    - Tools in the domain **REQM/RD**
    - Tools in the domain **series releases**

Optimizing Tool Qualification Efforts

Tool Landscape

- **Tools focus referring to tool qualification**

- Thus, **"classic tools" for REQM and RD** are affected
- Analogously, **delivery tools** are affected
- Besides, **standard tools** and **basis IT technology** are in focus, if they are used in terms of these domains
- **Examples:**
  - word processing
  - editors and viewers
  - spreadsheet programs
  - compression tools
    e.g. 7-zip
  - …



Optimizing Tool Qualification Efforts

Overview

- Company Background
- Introduction to Tool Qualification
- Tool Landscape
- Example: 7-zip
- Qualification Effort Optimization
  - Cost Modeling
  - Cost Optimization
  - Example: 7-zip
- Summary

Experiences with qualification of software tools

Example 7-zip

- Context of Robert Bosch GmbH
  - 130.000 installations
  - 3% usage in a safety relevant way

- Safety relevance 7-zip
  - Safety relevant in terms of **upper left corner** usage
    “compress/decompress specification of safety relevant requirements”
  - Safety relevant in terms of **upper right corner** usage
    “compressing/decompressing hex code for delivery”

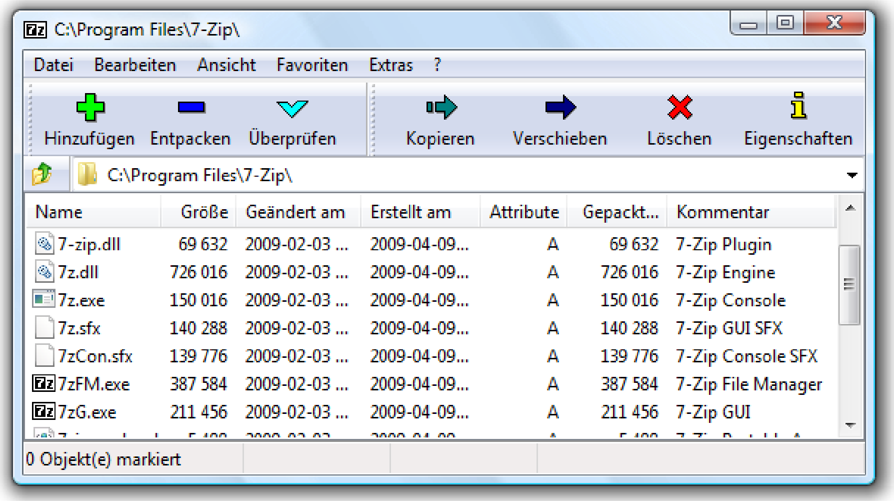
Experiences with qualification of software tools

Example 7-zip

- **Approach**
  - Feature based use case analysis
  - Goal: process independency for gaining reuse in the company
  - Thus: maximal benefit

Create a **7-zip model** with

- Use Cases
- Features
- Artifacts
- Errors
- Checks



Name	Größe	Geändert am	Erstellt am	Attribute	Gepackt...	Kommentar
7-zip.dll	69 632	2009-02-03 ...	2009-04-09...	A	69 632	7-Zip Plugin
7z.dll	726 016	2009-02-03 ...	2009-04-09...	A	726 016	7-Zip Engine
7z.exe	150 016	2009-02-03 ...	2009-04-09...	A	150 016	7-Zip Console
7z.sfx	140 288	2009-02-03 ...	2009-04-09...	A	140 288	7-Zip GUI SFX
7zCon.sfx	139 776	2009-02-03 ...	2009-04-09...	A	139 776	7-Zip Console SFX
7zFM.exe	387 584	2009-02-03 ...	2009-04-09...	A	387 584	7-Zip File Manager
7zG.exe	211 456	2009-02-03 ...	2009-04-09...	A	211 456	7-Zip GUI

0 Objekt(e) markiert

- Identify **error sources and error sinks** (complexity handling)
- Cooperation project with Fa. Validas: Visualization & documentation with helps of **Tool Chain Analyzer (TCA)**

Optimizing Tool Qualification Efforts

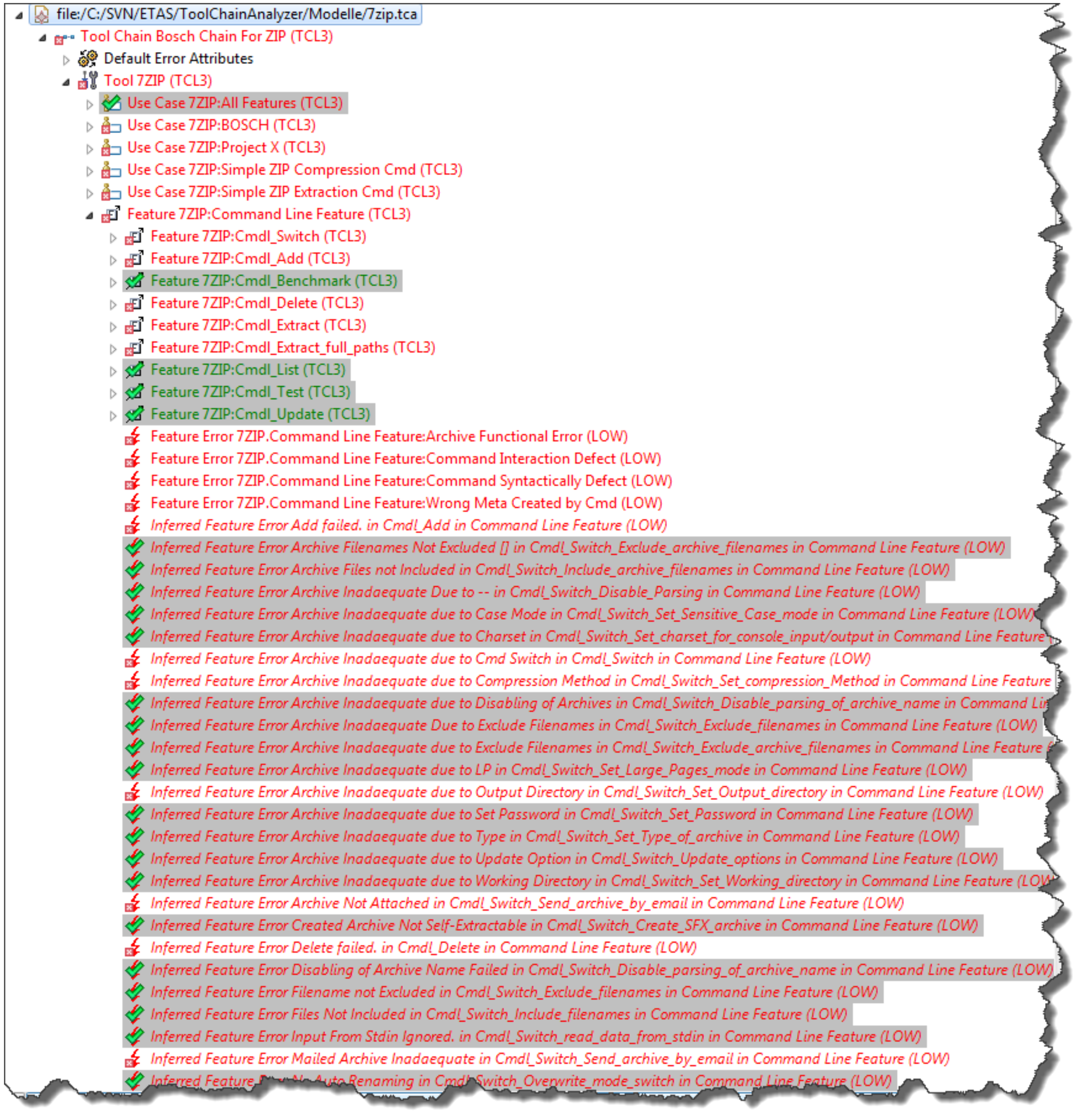
Example 7-zip

7-zip model

– Errors based on black-box strategy

– **Size of the model**

  - Features: 194
  - Proposed checks/restrictions: 26
  - Pot. errors:
    - Derived: ca. 2000 error
    - Subsumed: ca. 400 errors Status
  - TCL with assumptions: **TCL 1**
  - TCL without assumptions: **TCL 3**



```
◢ file:/C:/SVN/ETAS/ToolChainAnalyzer/Modelle/7zip.tca
  ◢ Tool Chain Bosch Chain For ZIP (TCL3)
    ▷ Default Error Attributes
    ◢ Tool 7ZIP (TCL3)
      ▷ Use Case 7ZIP:All Features (TCL3)
      ▷ Use Case 7ZIP:BOSCH (TCL3)
      ▷ Use Case 7ZIP:Project X (TCL3)
      ▷ Use Case 7ZIP:Simple ZIP Compression Cmd (TCL3)
      ▷ Use Case 7ZIP:Simple ZIP Extraction Cmd (TCL3)
      ◢ Feature 7ZIP:Command Line Feature (TCL3)
        ▷ Feature 7ZIP:Cmdl_Switch (TCL3)
        ▷ Feature 7ZIP:Cmdl_Add (TCL3)
        ▷ Feature 7ZIP:Cmdl_Benchmark (TCL3)
        ▷ Feature 7ZIP:Cmdl_Delete (TCL3)
        ▷ Feature 7ZIP:Cmdl_Extract (TCL3)
        ▷ Feature 7ZIP:Cmdl_Extract_full_paths (TCL3)
        ▷ Feature 7ZIP:Cmdl_List (TCL3)
        ▷ Feature 7ZIP:Cmdl_Test (TCL3)
        ▷ Feature 7ZIP:Cmdl_Update (TCL3)
          Feature Error 7ZIP.Command Line Feature:Archive Functional Error (LOW)
          Feature Error 7ZIP.Command Line Feature:Command Interaction Defect (LOW)
          Feature Error 7ZIP.Command Line Feature:Command Syntactically Defect (LOW)
          Feature Error 7ZIP.Command Line Feature:Wrong Meta Created by Cmd (LOW)
          Inferred Feature Error Add failed. in Cmdl_Add in Command Line Feature (LOW)
          Inferred Feature Error Archive Filenames Not Excluded [] in Cmdl_Switch_Exclude_archive_filenames in Command Line Feature (LOW)
          Inferred Feature Error Archive Files not Included in Cmdl_Switch_Include_archive_filenames in Command Line Feature (LOW)
          Inferred Feature Error Archive Inadaequate Due to -- in Cmdl_Switch_Disable_Parsing in Command Line Feature (LOW)
          Inferred Feature Error Archive Inadaequate due to Case Mode in Cmdl_Switch_Set_Sensitive_Case_mode in Command Line Feature (LOW)
          Inferred Feature Error Archive Inadaequate due to Charset in Cmdl_Switch_Set_charset_for_console_input/output in Command Line Feature
          Inferred Feature Error Archive Inadaequate due to Cmd Switch in Cmdl_Switch in Command Line Feature (LOW)
          Inferred Feature Error Archive Inadaequate due to Compression Method in Cmdl_Switch_Set_compression_Method in Command Line Feature
          Inferred Feature Error Archive Inadaequate due to Disabling of Archives in Cmdl_Switch_Disable_parsing_of_archive_name in Command Li
          Inferred Feature Error Archive Inadaequate Due to Exclude Filenames in Cmdl_Switch_Exclude_filenames in Command Line Feature (LOW)
          Inferred Feature Error Archive Inadaequate due to Exclude Filenames in Cmdl_Switch_Exclude_archive_filenames in Command Line Feature
          Inferred Feature Error Archive Inadaequate due to LP in Cmdl_Switch_Set_Large_Pages_mode in Command Line Feature (LOW)
          Inferred Feature Error Archive Inadaequate due to Output Directory in Cmdl_Switch_Set_Output_directory in Command Line Feature (LOW)
          Inferred Feature Error Archive Inadaequate due to Set Password in Cmdl_Switch_Set_Password in Command Line Feature (LOW)
          Inferred Feature Error Archive Inadaequate due to Type in Cmdl_Switch_Set_Type_of_archive in Command Line Feature (LOW)
          Inferred Feature Error Archive Inadaequate due to Update Option in Cmdl_Switch_Update_options in Command Line Feature (LOW)
          Inferred Feature Error Archive Inadaequate due to Working Directory in Cmdl_Switch_Set_Working_directory in Command Line Feature (LO
          Inferred Feature Error Archive Not Attached in Cmdl_Switch_Send_archive_by_email in Command Line Feature (LOW)
          Inferred Feature Error Created Archive Not Self-Extractable in Cmdl_Switch_Create_SFX_archive in Command Line Feature (LOW)
          Inferred Feature Error Delete failed. in Cmdl_Delete in Command Line Feature (LOW)
          Inferred Feature Error Disabling of Archive Name Failed in Cmdl_Switch_Disable_parsing_of_archive_name in Command Line Feature (LOW)
          Inferred Feature Error Filename not Excluded in Cmdl_Switch_Exclude_filenames in Command Line Feature (LOW)
          Inferred Feature Error Files Not Included in Cmdl_Switch_Include_filenames in Command Line Feature (LOW)
          Inferred Feature Error Input From Stdin Ignored. in Cmdl_Switch_read_data_from_stdin in Command Line Feature (LOW)
          Inferred Feature Error Mailed Archive Inadaequate in Cmdl_Switch_Send_archive_by_email in Command Line Feature (LOW)
          Inferred Feature [illegible] No Auto Renaming in Cmdl_Switch_Overwrite_mode_switch in Command Line Feature (LOW)
```

Optimizing Tool Qualification Efforts

Overview

- Company Background
- Introduction to Tool Qualification
- Tool Landscape
- Example: 7-zip
- Qualification Effort Optimization
  - Cost Modeling
  - Cost Optimization
  - Example: 7-zip
- Summary

Cost Modeling

- **Enforcement of checks** (process measure) reduces the number of TCL3 features

- **But:** Checks entail additional efforts

- **Selection of checks:**
  - It is not necessary to enforce all predefined checks because one check may detect more than one error
  - It is not necessary to cover all TCL3 features by checks, because it may be more effective to validate some TCL3 features

- **How to express this effectiveness?**

- Model enhancement:
  Introduction of a **cost parameter**

Optimizing Tool Qualification Efforts

Cost Modeling

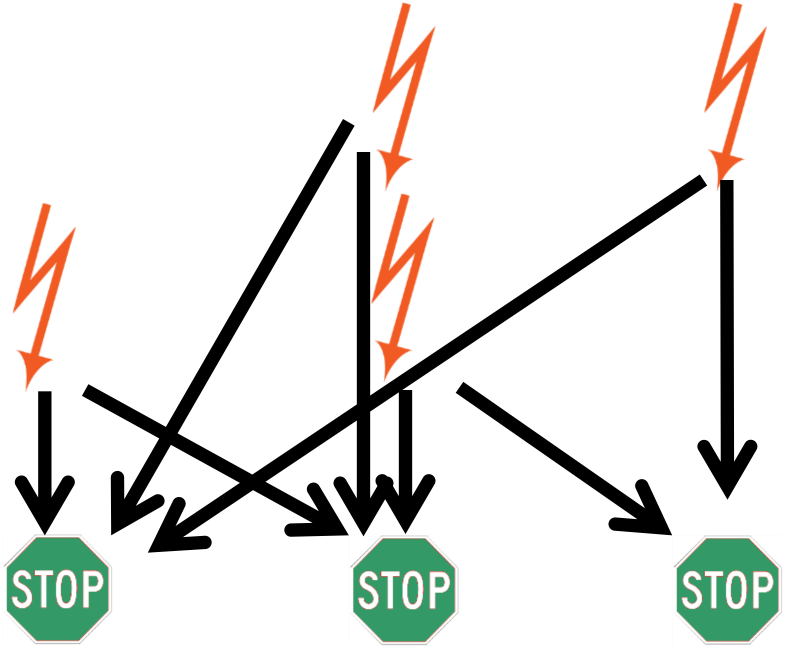
Shall consider different type of costs

- **Cost Units**
  - Money
  - User Time
  - Computer-Ressources (CPU-Time, RAM, Disk, Other)
- **Fix costs**
  - Only once per company, e.g. creation of a script, tool qualification kit
- **Variable costs**
  - Support per Tool (e.g. Known-Bugs Analysis, Upgrades, tool qualification) * UsageTime
  - Number of Licences * Price+SupportPerLicence
  - Number of Installtions (Clients+Server)*Installation effort
  - Manual Work with the tool
  - Automatic Work („CPU Usage“)

Optimizing Tool Qualification Efforts

Cost Optimization

- Use Case A (Inst #: N)
- Features:
  - Feature 1 (Inst #: 1)
  - Feature 2 (Inst #:3)
- Safety Guide (Checks & Costs):
  - Check 1
    (variable costs: 3,
    fix cost: 1)
  - Check 2
    (variable costs: 2,
    fix costs: 4)
  - Check 3
    (variable cost: 1,
    fix costs: 5)

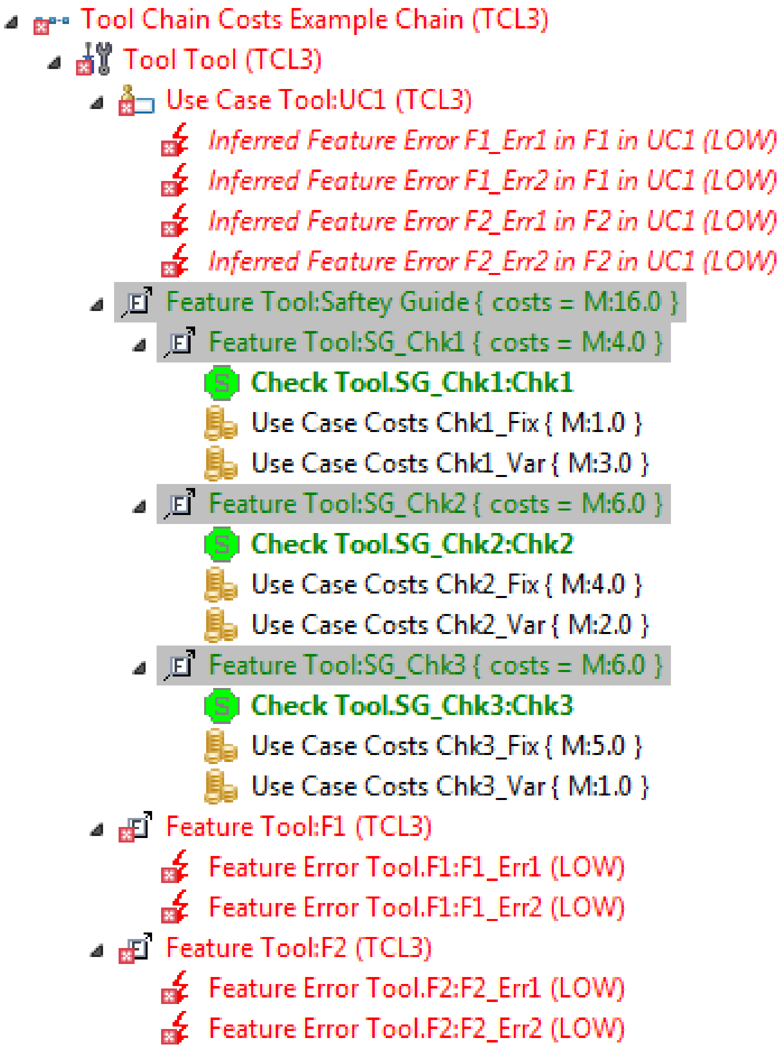


Solution A:	1+3N	+ 4+2N	+ 5+N	= 10+6N
Solution B:		4+2N	+ 5+N	= 9+3N
Solution C:			5+N	= 5+ N
Solution D:	1+3N	+ 4+2N		= 5+5N
Solution E:	1+3N			= 1+3N
Solution F:		4+2N		= 4+ 2N
Solution G:	1+3N		+ 5+N	= 6+4N

Optimizing Tool Qualification Efforts

Cost Optimization

- **Realization with Tool Chain Analyzer TCA**
  - Checks are Assumptions and contained in „Safety Guidelines“ (modeled as virtual Features)
  - Safety Guidelines contain Costs
  - Use Case requires Features
  - Safety Guidelines to be selected (from the Tool) in an optimal way



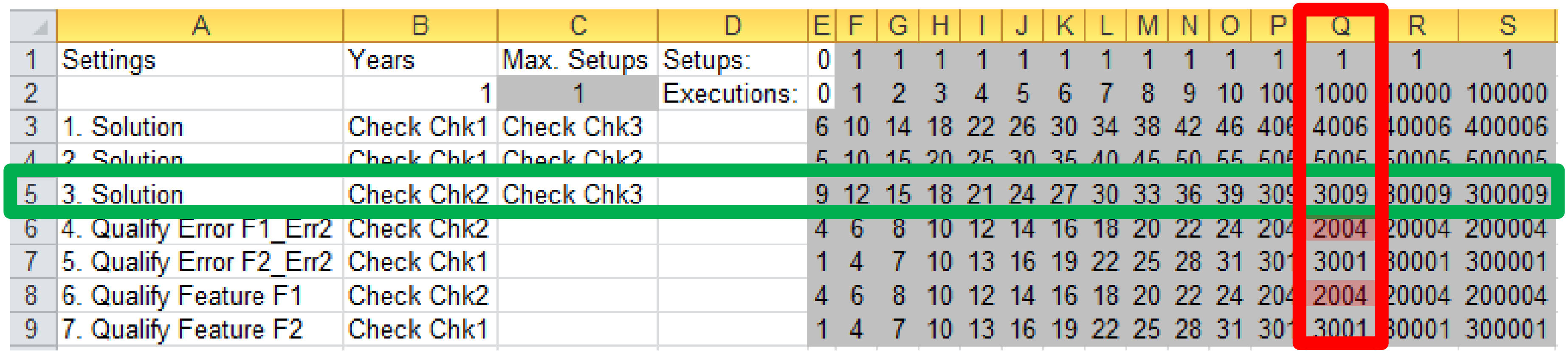
- Tool Chain Costs Example Chain (TCL3)
  - Tool Tool (TCL3)
    - Use Case Tool:UC1 (TCL3)
      - *Inferred Feature Error F1_Err1 in F1 in UC1 (LOW)*
      - *Inferred Feature Error F1_Err2 in F1 in UC1 (LOW)*
      - *Inferred Feature Error F2_Err1 in F2 in UC1 (LOW)*
      - *Inferred Feature Error F2_Err2 in F2 in UC1 (LOW)*
    - Feature Tool:Saftey Guide { costs = M:16.0 }
      - Feature Tool:SG_Chk1 { costs = M:4.0 }
        - **Check Tool.SG_Chk1:Chk1**
        - Use Case Costs Chk1_Fix { M:1.0 }
        - Use Case Costs Chk1_Var { M:3.0 }
      - Feature Tool:SG_Chk2 { costs = M:6.0 }
        - **Check Tool.SG_Chk2:Chk2**
        - Use Case Costs Chk2_Fix { M:4.0 }
        - Use Case Costs Chk2_Var { M:2.0 }
      - Feature Tool:SG_Chk3 { costs = M:6.0 }
        - **Check Tool.SG_Chk3:Chk3**
        - Use Case Costs Chk3_Fix { M:5.0 }
        - Use Case Costs Chk3_Var { M:1.0 }
    - Feature Tool:F1 (TCL3)
      - Feature Error Tool.F1:F1_Err1 (LOW)
      - Feature Error Tool.F1:F1_Err2 (LOW)
    - Feature Tool:F2 (TCL3)
      - Feature Error Tool.F2:F2_Err1 (LOW)
      - Feature Error Tool.F2:F2_Err2 (LOW)

Optimizing Tool Qualification Efforts

Cost Optimization

- **Results**
  - generated calculation table from the TCA model by TCA & SAT Solver
  - shows the costs for applying the mitigations required for the use cases
  - depending on their multiplicity N (N=number of executions)

For 1000 executions:
Solution 3 (B) is optimal
and qualifying against
Error F1E2 (or feature F1)
could save 3009-
2004=1005 costs



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	Settings	Years	Max. Setups	Setups:	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2		1	1	Executions:	0	1	2	3	4	5	6	7	8	9	10	100	1000	10000	100000
3	1. Solution	Check Chk1	Check Chk3		6	10	14	18	22	26	30	34	38	42	46	406	4006	40006	400006
4	2. Solution	Check Chk1	Check Chk2		5	10	15	20	25	30	35	40	45	50	55	505	5005	50005	500005
5	3. Solution	Check Chk2	Check Chk3		9	12	15	18	21	24	27	30	33	36	39	309	3009	30009	300009
6	4. Qualify Error F1_Err2	Check Chk2			4	6	8	10	12	14	16	18	20	22	24	204	2004	20004	200004
7	5. Qualify Error F2_Err2	Check Chk1			1	4	7	10	13	16	19	22	25	28	31	301	3001	30001	300001
8	6. Qualify Feature F1	Check Chk2			4	6	8	10	12	14	16	18	20	22	24	204	2004	20004	200004
9	7. Qualify Feature F2	Check Chk1			1	4	7	10	13	16	19	22	25	28	31	301	3001	30001	300001

Optimizing Tool Qualification Efforts

Example 7-zip

- **Solution of an Optimization Problem**
  - Finding all minimal solutions is a ***NP* hard problem**
  - Solving can take an exploding amount of time
  - Human help by mitigating some errors to reduce the search space
  - **Compare** costs (cost reductions) with qualification costs
    (for your number N of expected use-cases)
  - Derive the **optimum** between **check costs** and **qualification costs**

- **Result for 7-zip**
  - In our context, we enforce checks like syntax check, logfile verification, and default option setting as a safety guideline
  - On the other hand, we qualify selected command line features

Optimizing Tool Qualification Efforts

Overview

- Company Background
- Introduction to Tool Qualification
- Tool Landscape
- Example: 7-zip
- Qualification Effort Optimization
  - Cost Modeling
  - Cost Optimization
  - Example: 7-zip
- Summary

Optimizing Tool Qualification Efforts

Summary

- Identification of the **upper left** and of the **upper right corner of the V-shaped development process** as a domain where most **safety relevant tools** are located in
- Focus also on **Standard tools** and **basis IT technology** are in focus, if they are used in terms of these domains
- Consideration of **7-zip** as a representative of those tool class
- Performing a feature based **use case analysis** of 7-zip, including a **cost analysis**
- Modeling with help of **Tool Chain Analyzer TCA**
- Solving an NP hard **optimizing problem** with the proposed approach

Discussion