Zurich University
of Applied Sciences

School of
Engineering

IAMP Institute of Applied
Mathematics and Physics

Tool Qualification Considerations for Tools Supporting STPA

Sven Stefan Krauss, Martin Rejzek, Christian Hilbes

Zurich University of Applied Sciences, Switzerland

Agenda

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Agenda

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Applied Research Project

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

CURTISS-WRIGHT

Integration of STPA as a safety analysis method in our partner's engineering development lifecycle, by

- industrial case study how STPA can be applied for **system components engineering** for **multiple safety domains** (confidential), and
- the **development and integration of an STPA tool in the partner's engineering toolchain** based on the experience gained from the case study and previous STPA projects [8], [9] and [10].

Safety Domains

CURTISS-WRIGHT

Industrial & Special Applications
IEC 61508 [15]

Railway
EN 50128 [16]

Aerospace & Defense
RTCA/DO-178C [17]
RTCA/DO-330 [18]
IEC 61508 [15]
MIL-STD 882 [29]

System and Safety Engineering

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

System / HW / SW-Engineer

Model based development

- Design with UML/SysML
- Documentation
- Simulation, Verification
- Code Generation

Safety Engineer

Hazard & Risk Analysis

- FMEA
- FTA
- HAZOP
- STAMP [1] & STPA [2]

UML Tools

- Sparx Systems Enterprise Architect [12]
- Many others…

Software Tools supporting STPA

- A-STPA [3] and XSTAMPP [4]
- SafetyHAT [5]
- MIT STPA Tool [6]

SAHRA [7]
STPA based hazard and risk analysis

SAHRA [7] – An Integrated STPA Tool

SAHRA – STPA based Hazard and Risk Analysis

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

STPA integrated into UML modeling tool

- Developed as extension (plugin) for UML tool Sparx Systems Enterprise Architect [12]
- Includes UML Profile for STPA data items

SAHRA Features

(1) Support for Multi Level Hierarchical Control Structures with diagram checks during modeling

(2) Context sensitive element editors for STPA data items and relationship analyzer to show related data for traceability

(3) Graphical safety net editor with drag'n'drop support and relationship analyzer for STPA Step 1

Fig.1: Hierarchical Control Structure Diagram

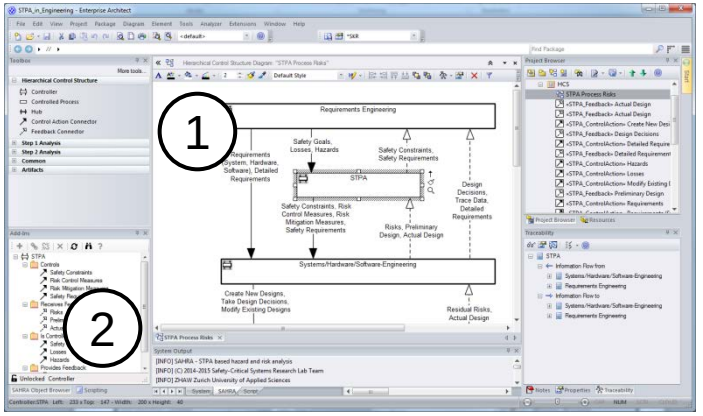
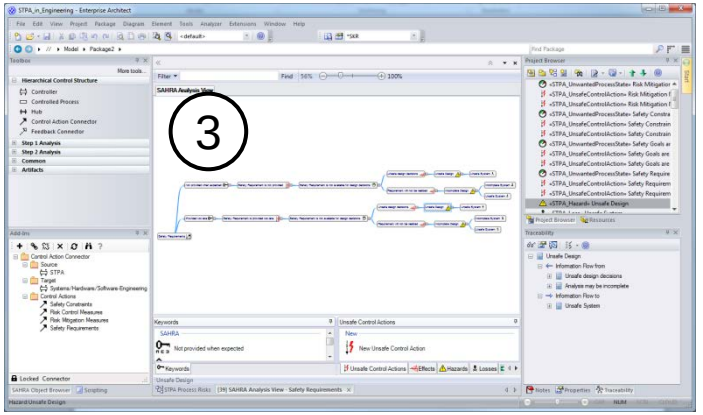


Fig.2: Graphical safety net editor for STPA Step 1



SAHRA
STPA based hazard and risk analysis

SAHRA [7] – An Integrated STPA Tool

SAHRA – STPA based Hazard and Risk Analysis

Integration Advantages

- Sparx System Enterprise Architect Corporate Edition provides multi user support with security permission system and configuration management integration for process control
- Requirements, Design and STPA data items are in one single repository which enables full end-to-end traceability

SAHRA
STPA based hazard and risk analysis

SAHRA [7] – An Integrated STPA Tool

SAHRA – STPA based Hazard and Risk Analysis

Research Questions

SAHRA is used for safety analysis of system components in multiple safety domains.

a) What are the tool qualification requirements in the respective safety standards?
b) What are the effects of tool errors in safety analysis tools like STPA tools?
c) Is tool qualification required or recommended and when yes to what level?

Agenda

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Research Questions

a) What are the tool qualification requirements in the respective safety standards?

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Software Tool Qualification

- Risk assessment of whether an engineering software tool may have a negative impact on safety
- Malfunctioning engineering tools can influence the final safety-related system by
  - introducing errors or
  - failing to detect errors

Do you rely on software tools?

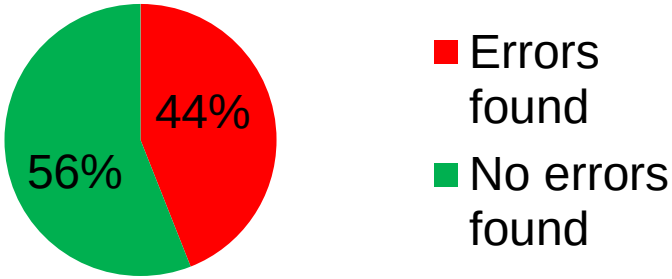
Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Software Tool Qualification

Survey about Tool Qualification according to DO-178B [20], Section J:

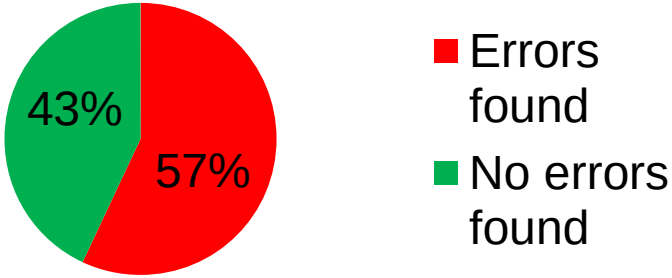
Development Tools

- ~44% of survey respondents with experience with tool qualification found errors in a development tool during tool qualification



Verification Tools

- 57% of survey respondents with experience with tool qualification found errors in a verification tool during tool qualification



Software Tool Qualification

Typical Tool Qualification Methods

Tool validation

- Requirements based testing of tool operational requirements which specify tool behavior

Increased confidence from use

- The software tool has a extensive history of successful use

Tool error detection means

- Built-in functionality to prevent or to detect tool errors like diverse redundant code

Tool development according to a safety standard

- Software tool was developed according to a safety standard to avoid systematic errors

Tool Qualification Overview

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Industrial / Generic

- IEC 61508 Part 3 [24]
- IEC 61508 Part 4 [23]

Railway

- EN 50128 [16]

Aerospace & Defense

- DO-178C [17]
- DO-330 [18]

Automotive

- ISO 26262 Part 8 [19]

For more details: [22]

Generic Safety Standard
IEC 61508

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Industrial / Generic

- IEC 61508 Part 3 [24]
- IEC 61508 Part 4 [23]

Tool classes

- T1 – Tool has no direct or indirect impact
- T2 – Tool may fail to detect errors
- T3 – Tool may Introduce errors

Qualification Requirements

- Mandatory for tools of class T3
- Recommended for tools of class T2
- Specification or manual which defines tool behavior
- Safety assessment and mitigation action

Tool Qualification Methods

- Increased confidence from use
- Tool validation

Railway
EN 50128

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Railway

- EN 50128 [16]

Tool classes

- T1 – Tool has no direct or indirect impact
- T2 – Tool may fail to detect errors
- T3 – Tool may introduce errors

Qualification Requirements

- Mandatory for tools of class T3
- Recommended for tools of class T2
- Specification or manual which defines tool behavior
- Safety assessment and mitigation action

Tool Qualification Methods

- Increased confidence from use
- Tool validation
- Tool error detection means

Aerospace & Defense
DO-178C [17], DO-330 [18]

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Aerospace & Defense

- DO-178C [17]
- DO-330 [18]

Tool Qualification Level

Tool Qualification Level TQL-1 to TQL-5 is defined by tool criteria and safety level:

- Criteria 1 – Tool may insert error
- Criteria 2 – Tool automates or eliminates verification or development process steps
- Criteria 3 – Tool may fail to detect an error
- Safety Level A (most critical) to Level D

Qualification Requirements

- Depend on Tool Qualification Level (TQL)
- DO-330 provides set of objectives for each TQL

Tool Qualification Methods

- Tool validation
- Tool development according to safety standard DO-330 (tool developers)

Automotive
ISO 26262-8 [19]

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Automotive

- ISO 26262 Part 8 [19]

Tool Confidence Level

Tool Confidence Level TCL1 to TCL3 is defined by tool impact TI and Tool error detection TD level:

- TI – Tool impact
- TD – Confidence level if tool error can be detected or prevented

Qualification Requirements

- Depend on Tool Confidence Level (TCL) and safety level
- Recommended and highly recommended qualification methods depending on safety level

Tool Qualification Methods

- Increased confidence from use
- Tool validation
- Evaluation of tool development process
- Tool development according to a safety standard (tool developers)

Agenda

Research Questions

b) What are the effects of tool errors in safety analysis tools like STPA tools?

c) Is tool qualification required or recommended and when yes to what level?

Generic Safety Standard
IEC 61508

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Industrial / Generic

- IEC 61508 Part 3 [24]
- IEC 61508 Part 4 [23]

Tool classes

- T1 – Tool has no direct or indirect impact* ✓
- T2 – Tool may fail to detect errors ✗
- T3 – Tool may introduce errors ✗

*Listed examples for T1:

- Requirement Management Tool
- Modeling tool without code generation

Really?

- Do tool errors in safety analysis tools have a direct or indirect impact on safety?
- Hypothesis: YES!
- Detailed analysis required!

Do we need to qualify STPA tools?
Effect of tool errors

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Tool classification problem

IEC 61508: Tool class is selected according to tool class description and listed examples (i.e. Requirements Management Tool, Modeling tool without code generation)

1. Selected tool class is T1
2. No tool qualification is required
3. No tool risk analysis is required
4. **No mitigation actions in place for risks caused by tool errors even when they would have an direct or indirect impact on safety!**

Do we need to qualify STPA tools?
Effect of tool errors

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Role of tool errors in safety analysis tools

To understand the effect of tool errors in safety analysis tools (here: STPA) we have to consider:

Process Risks

- Process risk analysis of safety analysis process (here: STPA) in the development lifecycle with STPA (Meta-Analysis)

Tool & Integration Risks

- Risk analysis of automating or supporting safety analysis process (here: STPA) with a tool

Tool Operational Scenarios

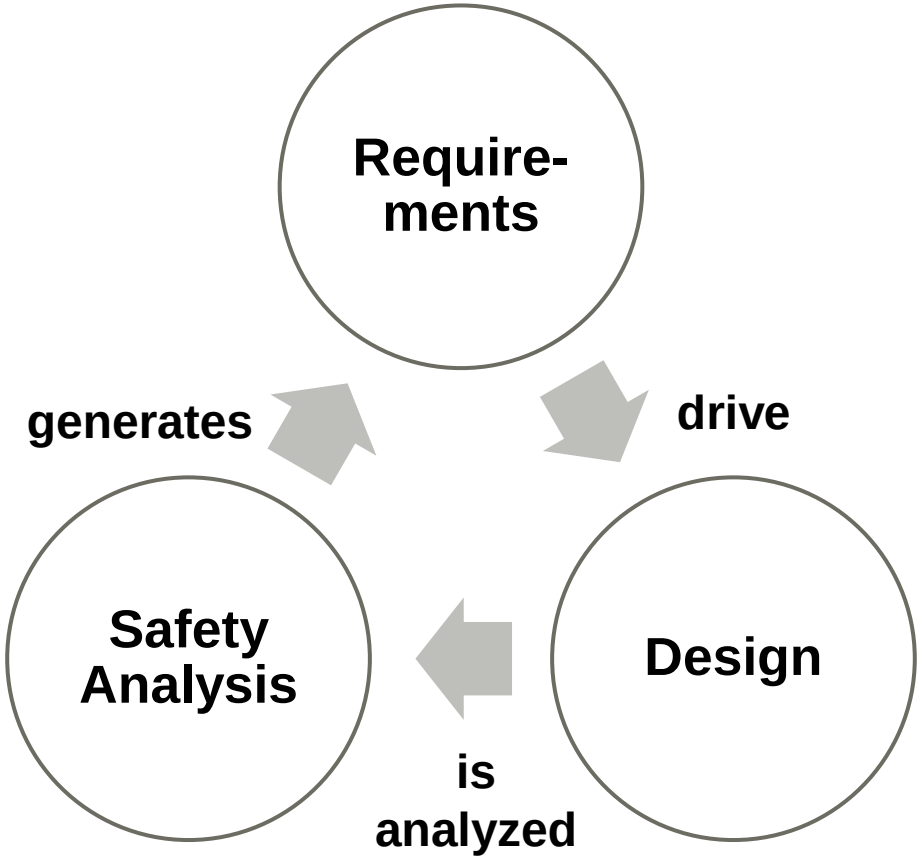
- Look at how the tool is used in the lifecycle (intended use)

Do we need to qualify STPA tools?
Process Risks

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Process Risks?

Simplified development lifecycle model



Simplified model of development lifecycle:

- Requirements drive design
- Design is analyzed with safety analysis
- Safety analysis generates new requirements
- Requirements drive design
- …

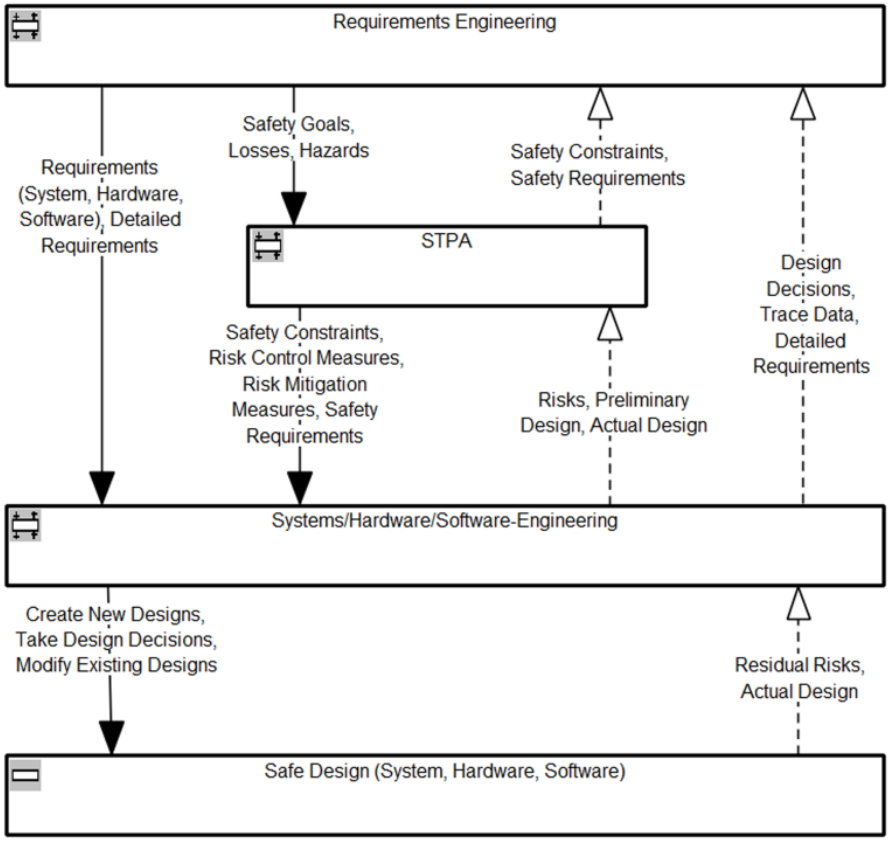
…until design is safe

Do we need to qualify STPA tools?
Process Risks

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Process Risks?

Detail analysis with STPA



Controller

- Requirements Engineering (Requirements)
- STPA (Safety Analysis)
- System/Hardware/Software Engineering (Design)

Controlled Process

- Safe Design (System, Hardware, Software)

Control Actions

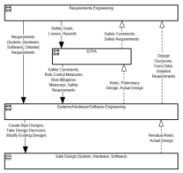
- Requirements (Safety, System, …)
- Safety Constraints
- Risk Control Measures
- Take Design Decisions
- Modify Existing Design
- …

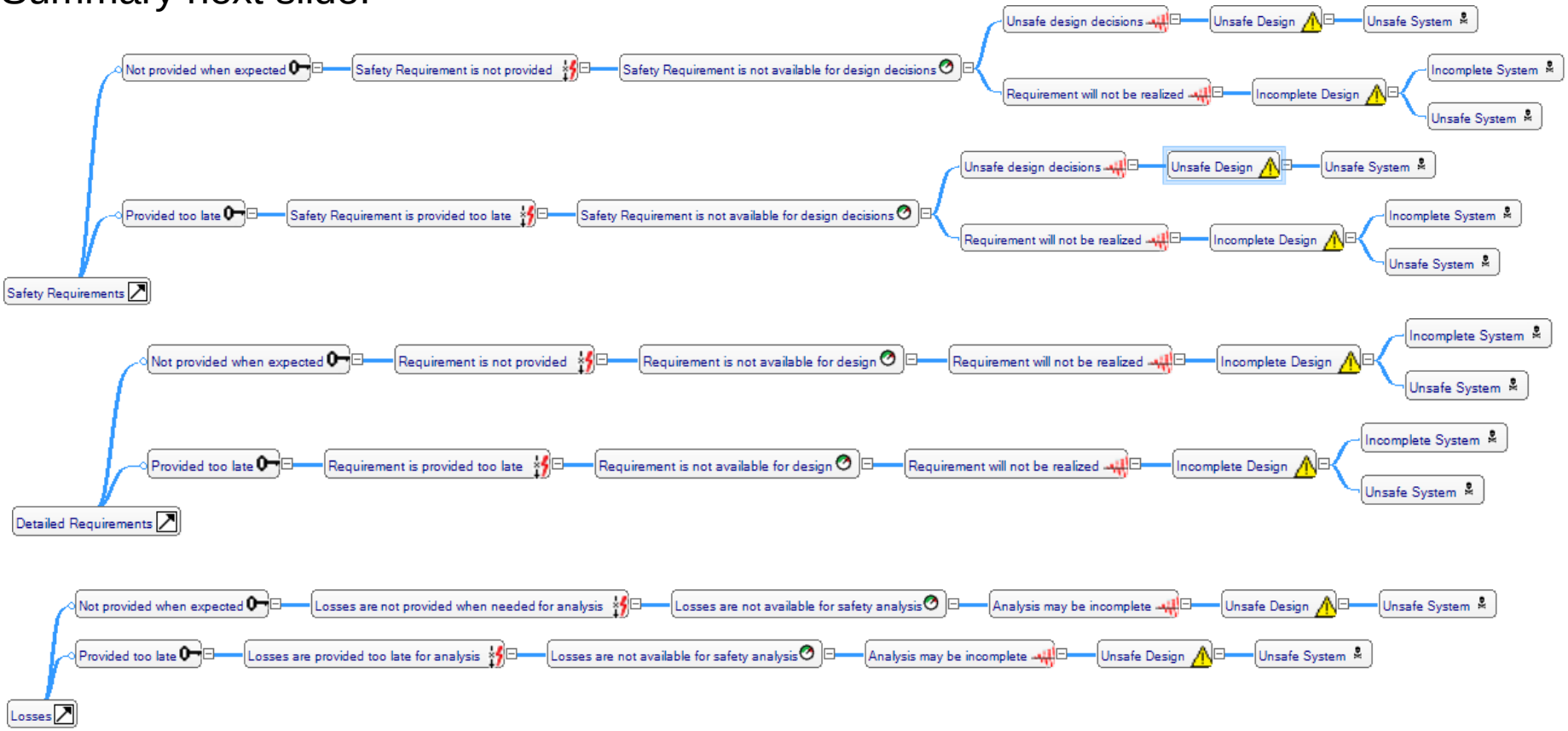
Do we need to qualify STPA tools?
Process Risks

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Process Risks?

Detail analysis with STPA Step 1.
Summary next slide.



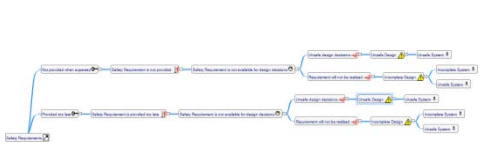


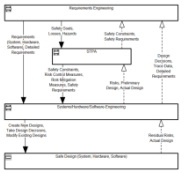
STPA Step 1 safety nets show only a small subset of complete analysis.

Do we need to qualify STPA tools?
Process Risks

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Identified Process Risks
Analysis Summary





Risk	Description	Hazard	Loss
PR1	safety constraints and safety requirements are **not provided** or **provided too late** either to the system, hardware and software engineering when needed to make **design decisions**	Unsafe Design, Incomplete Design	Unsafe System, Incomplete System
PR2	risk control measures and risk mitigation measures are **not provided** or **provided too late** to the system, hardware and software engineering when needed to make **design decisions**	Unsafe Design	Unsafe System
PR3	trace data is **incomplete** or **incorrect** when needed for modification **change impact analysis**	Unsafe Modification	Unsafe System

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Tool & Tool Integration Risks

Causal Factors [25-28]:

- Lack of Data Integrity
- Lack of Traceability for Completeness and Consistency
- …

Risk	Description
TR1	Analysis data items (i.e. safety requirements, safety constraints, risk control and mitigation measures) are incomplete or corrupt (→PR1, →PR2)
TR2	Trace data is incomplete or corrupt (→PR3)
TR3	Corrupt data items are used for verification (→PR1)
TR4	Corrupt data items are used for code generation (→PR1)

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Tool Operational Scenarios

TOS1 - Standalone STPA tool with manual verification

- Tool is used with manual verification of tool outputs for completeness and consistency → Manual **process quality assurance** is required

TOS2 - Integrated STPA tool without manual verification

- STPA data is automatically transferred to or integrated into another tool without manual verification for completeness and consistency → Tool requires **tool error detection or tool error prevention**

TOS3 - STPA data is used for verification

- STPA data is used for **verification** and may **fail to detect an error.**

TOS4 - STPA data is used for code generation

- STPA data is used for auto **code generation** may **introduce an error**

Do we need to qualify STPA tools?
Tool Qualification Overview

Zurich University of Applied Sciences
zh aw School of Engineering
IAMP Institute of Applied Mathematics and Physics

TOS	IEC 61508	EN 50128	ISO 26262			DO-330		
	Tool Class	Tool Class	Tool Impact	Tool error Detection	Tool Confidence Level	Tool Criterion	Safety Level	Tool Quali. Level
TOS1	T1	T1	TI2	TD3	TCL1	---	---	(TQL-5)
TOS2	T1 (T2)	T1 (T2)	TI2	TD1 TD2 TD3	TCL1 TCL2 TCL3	2	A B C D	TQL-3 TQL-4 TQL-5 TQL-5
TOS3	T2	T2	TI2	TD1 TD2 TD3	TCL1 TCL2 TCL3	2	A B C D	TQL-3 TQL-4 TQL-5 TQL-5
TOS4	T3	T3	TI2	TD1 TD2 TD3	TCL1 TCL2 TCL3	1	A B C D	TQL-1 TQL-2 TQL-3 TQL-4
	Tool class depends on intended use	Tool class depends on intended use	Tool class depends on Tool Detection confidence level (TD1, TD2, TD3) and Tool Impact (TI1,TI2)			Tool class depends on tool criterion (1,2,3) and safety level (A,B,C,D)		

Tool Qualification depends on many factors!

Do we need to qualify STPA tools?
Example: SAHRA

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

SAHRA (TOS2)

Standard	Qualification acc. Standard	Recommended Qualification	Comment
IEC 61508	T1	T2	Indirect Impact (process risks)
EN 50128	T1	T2	Indirect Impact (process risks)
ISO 26262	TCL1 TCL2 TCL3	TCL2	Tool Error Detection confidence level (TD) is high TD1, prevention of tool errors through safety tool development process (DO-330)
DO-178C / DO-330	TQL-3 TQL-4 TQL-5	TQL-3 Suitable for Level A	Automates development and verification process steps → Criteria 2

Do we need to qualify STPA tools?
Example: STPA Tool with Model Checker

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

STPA Tool with verification capabilities (TOS3)

STPA data items are used for Formal Model Checking

Standard	Qualification acc. Standard	Recommended Qualification	Comment
IEC 61508	T2	T2	Indirect (process risks) Tool may fail to detect an error
EN 50128	T2	T2	Indirect (process risks) Tool may fail to detect an error
ISO 26262	TCL1 TCL2 TCL3	TCL3	Tool Error Detection (TD) confidence level is unknown → TD3
DO-178C / DO-330	TQL-3 TQL-4 TQL-5	TQL-3 Suitable for Level A	Eliminates verification process steps → Criteria 2

Agenda

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Conclusion

Tool Qualification of tools supporting STPA

Tool Risk Analysis

Tool risk analysis of safety analysis tools (here: STPA) is required for proper tool classification and to determine Tool Qualification Requirements.

The tool risk analysis shall consider:

- process risks,
- tool and tool integration risks, and
- operational scenarios how the tool is used in the process.

For more details about tool and tool integration risks: [25-28]

Conclusion

Tool Qualification of tools supporting STPA

Effects of Tool Errors

- Tool errors in STPA tools (and safety analysis tools in general) might have an **negative impact** on the final safety related system and can be traced to process risks
- Tool Qualification based on **tool risk assessment** and **operational scenarios** of safety analysis tools is therefore **highly recommended**

Conclusion

Tool Qualification of tools supporting STPA

DO-330 provides detailed guidelines for multi domain tool qualification and

- can be used by tool users and tool developers as a guiding standard for tool qualification,
- can be used by tool developers as a guiding standard for safe tool development

SAHRA Development Lifecycle

- We use DO-330 as guiding safety standard for tool development of SAHRA with TQL-4 (suitable for Level B-D)

Tool Qualification Packages

- Tool developers can help tool users to qualify their tools with Tool Qualification Packages with tool operational requirements and predefined tool validation test cases and procedures.
- Tool developers should provide a safety manual including a reference workflow with operational scenarios for safe use of the tool.

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Problems

Limitation to Software Development Lifecycle Support Tools

The standards have a strong focus on tools that support the software development lifecycle and do not explicitly consider other tools for system or hardware engineering.

Safety Analysis Tools?

- Safety analysis tools are not addressed in the standards. What about errors in Fault Tree Tools, FMEA tools and others?

Simulation Tools?

- What about tool errors in tools for systems or hardware engineering like simulation tools which are used for verification?

Requirements Management Tools?

- Errors in Requirements Management Tools share the same process risks, hazards and losses: Unsafe Design and Unsafe System!

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Problems

Tool classification problems

- Tool classification is difficult, especially for integrated tools (like SAHRA) or combined tools (for example STPA tools with formal model checking capabilities) and depends on the operational scenarios, i.e. context and intended use.
- Wrong order of qualification steps in standards IEC 61508 and EN 50128. First demanding tool risk assessment, then tool classification would be better!

Stakeholder Scope

- Its in most reviewed standards unclear what are the requirements for tool users and what are requirements for tool developers (exception: DO-330).
- Most requirements can only be satisfied by tool developers. Example: Tool error detection confidence level TD in ISO 26262 cannot be selected correctly by tool users. When tool error detection function is used within the tool, then it should be validated by the tool developer!

Discussion & Questions

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Word cloud generated with http://www.jasondavies.com/wordcloud/

Contact:

Sven Stefan Krauss
svenstefan.krauss@zhaw.ch

Martin Rejzek
martin.rejzek@zhaw.ch

Christian Hilbes
christian.hilbes@zhaw.ch

http://www.zhaw.ch
http://www.sahra.ch

Annex

Generic Safety Standard
IEC 61508 Part 4 [23]

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Class	Definition	Examples	Ref.
T1	Tool that generates **no outputs that can directly or indirectly contribute to the executable code (including data)** of the safety related system	Text Editor Requirements Management Tool Modeling Tool without Code Generation Configuration Management Tool	3.2.11
T2	Tool that **supports the test or verification of the design or executable code**, where errors in the tool **can fail to reveal defects** but cannot directly create errors in the executable software	Test Generator Code Coverage Tool Static Code Analysis Tool	3.2.12
T3	Tool that **generates outputs** that **can directly** or **indirectly contribute to the executable code** of the safety related system	Optimizing Compiler Compiler with Runtime Package	3.2.13

Generic Safety Standard
IEC 61508 Part 3 [24]

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Requirements	Ref.	T1	T2	T3
Tools shall be selected in accordance with all development activities	7.4.4.2	●	●	●
Selection of tool shall be justified	7.4.4.3		●	●
Tools shall have documentation or specification which specifies behavior and restrictions on use	7.4.4.4		●	●
Safety assessment required + mitigation actions	7.4.4.5		●	●
Evidence for conformance to specification or manual required, by • Increased confidence from use • Tool validation	7.4.4.6		○	●
Tool validation & report	7.4.4.7		○	●

Summary only, not all requirements are shown. ● Mandatory, ○ Recommended

Railway
EN 50128 [16]

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Class	Definition	Examples	Ref.
T1	Tool that generates **no outputs that can directly or indirectly contribute to the executable code (including data)** of the safety related system	Text Editor Requirements Management Tool Modeling Tool without Code Generation Configuration Management Tool	3.1.42
T2	Tool that **supports the test or verification of the design or executable code**, where errors in the tool **can fail to reveal defects** but cannot directly create errors in the executable software	Test Generator Code Coverage Tool Static Code Analysis Tool	3.1.43
T3	Tool that **generates outputs** that **can directly** or **indirectly contribute to the executable code** of the safety related system	Optimizing compiler Compiler with runtime package Data/Algorithm compiler Tool for changing reference values during operation	3.1.44

Railway
EN 50128 [16]

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Requirements	Ref.	T1	T2	T3
Tools shall be selected in accordance with all development activities	6.7.4.1	●	●	●
Selection of tool shall be justified	6.7.4.2		●	●
Tools shall have documentation or specification which specifies behavior and restrictions on use	6.7.4.3		●	●
Safety assessment required + mitigation actions	6.7.4.4		●	●
Evidence for conformance to specification or manual required by: • Increased Confidence from use • Tool validation • Tool detection means	6.7.4.4		○	●
Tool validation & report	6.7.4.5		○	●

Summary only, not all requirements are shown. ● Mandatory, ○ Recommended

Aerospace & Defense
DO-178C [17] / DO-330 [18]

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

C	Definition	Level D	Level C	Level B	Level A
1	A tool whose output is **part of the airborne software** and thus **could insert an error**.	TQL-4	TQL-3	TQL-2	TQL-1
2	A tool that **automates verification process(es)** and thus could **fail to detect an error**, and whose output is used to **justify the elimination or reduction** of: 1. **Verification process(es)** other than that automated by the tool, or 2. **Development process(es)** that could have an impact on the airborne software	TQL-5	TQL-5	TQL-4	TQL-3
3	A tool that, within the scope of its intended use, could **fail to detect an erro**r	TQL-5	TQL-5	TQL-5	TQL-4

Automotive
ISO 26262-8 [19]

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

Tool Impact		Tool Error Detection		
The possibility that a malfunction of a particular software tool can introduce or fail to detect errors in a safety-related item or element being developed.		High confidence to prevent/detect erroneous outputs	Medium confidence to prevent/detect erroneous outputs	Other cases
		TD1	TD2	TD3
TI1 shall be selected when there is an argument that there is no such possibility	TI1	TCL1	TCL1	TCL1
TI2 shall be selected in all other cases	TI2	TCL1	TCL2	TCL3

Automotive
ISO 26262-8 [19]

Zurich University of Applied Sciences
School of Engineering
IAMP Institute of Applied Mathematics and Physics

			ASIL			
	Methods	**TCL**	**A**	**B**	**C**	**D**
1a	Increased confidence from use in accordance with 11.4.7	TCL3	++	++	+	+
		TCL2	++	++	++	+
		TCL1				
1b	Evaluation of the tool development process in accordance with 11.4.8	TCL3	++	++	+	+
		TCL2	++	++	++	+
		TCL1				
1c	Validation of the software tool in accordance with 11.4.9	TCL3	+	+	++	++
		TCL2	+	+	+	++
		TCL1				
1d	Development in accordance with a safety standard [a]	TCL3	+	+	++	++
		TCL2	+	+	+	++
		TCL1				

[a] No safety standard is fully applicable to the development of software tools. Instead, a relevant subset of requirements of the safety standard can be selected.
EXAMPLE Development of the software tool in accordance with ISO 26262, IEC 61508 or RTCA DO-178.

Summary only, not all requirements are shown. ++ Highly recommended, + Recommended

References

1. Leveson NG. Engineering a safer world: Systems thinking applied to safety. MIT Press, Cambridge MA, USA; 2012.
2. Leveson NG. A new accident model for engineering safer systems. Safety Science. 2004; 42: p. 237-70.
3. Abdulkhaleq A, Wagner S. A-STPA: Open Tool Support for System-Theoretic Process Analysis. STAMP Workshop 2014. MIT, Boston; 2014.
4. Abdulkhaleq A, Wagner S. XSTAMPP: An eXtensible STAMP Platform As Tool Support for Safety Engineering. STAMP Workshop 2015. MIT, Boston; 2015.
5. Hommes Q. The Volpe STPA Tool. STAMP Workshop 2014. MIT, Boston; 2014.
6. Suo D, Thomas J. An STPA Tool. STAMP Workshop 2014. MIT, Boston; 2014.
7. Safety-Critical Systems Research Lab Team of ZHAW Zurich University of Applied Sciences. SAHRA - STPA based Hazard and Risk Analysis. http://www.sahra.ch. Last access: 01.08.2015
8. Antoine B. Systems Theoretic Hazard Analysis (STPA) applied to the risk review of complex systems: an example from the medical device industry: Massachusetts Institute of Technology; 2013.
9. Rejzek M. Evaluation of STPA in the Safety Analysis of the Gantry 2 Proton Radiation Therapy System. STAMP Workshop 2012. MIT, Boston; 2012.
10. Rejzek M. Use of STPA in digital instrumentation and control systems of nuclear power plants. 2nd European STAMP Workshop. Stuttgart; 2014.
11. IEC 61508-7 Ed. 2 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures. 2010.
12. Sparx Systems Pty Ltd. Enterprise Architect - UML Modeling and Lifecycle Tool Suite. 2015. http://www.sparxsystems.com/. Last access: 01.08.2015
13. Sparx Systems Pty Ltd. Model Driven Generation (MDG) Technologies. 2015. http://www.sparxsystems.com.au/resources/mdg_tech/. Last access: 27.07.2015

References

14. Rejzek M, Hilbes C, Krauss SS. Safety Driven Design with UML and STPA. STAMP Workshop 2015. MIT, Boston; 2015.
15. IEC 61508 Ed. 2 - Functional safety of electrical/electronic/programmable electronic safety-related systems. 2010.
16. CENELEC. EN 50128 - Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems. 2011: p.
17. DO-178C - Software Considerations in Airborne Systems and Equipment Certification. 2011.
18. DO-330 - Software Tool Qualification Considerations. 2011.
19. ISO 26262-8 - Road Vehicles - Functional Safety - Part 8: Supporting processes. 2011.
20. Hayhurst KJ, Dorsey CA, Knight JC, Leveson NG, McCormick GF. Streamlining software aspects of certification: Report on the SSAC survey. NASA/TM-1999-209519. Citeseer; 1999.
21. DO-178B - Software Considerations in Airborne Systems and Equipment Certification. 1992.
22. Camus J-L, Dewalt MP, Pothon F, Ladier G, Boulanger J-L, Blanquart J-P, et al. Tool Qualification in Multiple Domains: Status and Perspectives. ERTS2 Embedded Real Time Software and System. Toulouse, France; 2014.
23. IEC 61508-4 Ed. 2 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations. 2010.
24. IEC 61508-3 Ed. 2 - Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements. 2010.
25. Asplund F, Biehl M, El-khoury J, Frede D, Törngren M. Tool Integration, from Tool to Tool Chain with ISO 26262. SAE 2012 World Congress & Exhibition SAE Technical Paper 2012-01-0026. 2012.
26. Asplund F. Risks Related to the Use of Software Tools when Developing Cyber-Physical Systems. PhD Thesis. KTH Royal Institute of Technology, Stockholm, Sweden; 2014.
27. Asplund F. Safety and Tool Integration, A System-Theoretic Process Analysis. Technical Report ISRN/KTH/MMK-R-12/01-SE. KTH Royal Institute of Technology, Stockholm, Sweden; 2012.
28. Asplund F, El-khoury J, Törngren M. Qualifying Software Tools, a Systems Approach. In: Ortmeier F, Daniel P, editors. Computer Safety, Reliability, and Security: Springer Berlin Heidelberg; 2012. p. 340-51.
29. US Department of Defense. MIL-STD-882E - System safety program requirements; 2012