



Is my STPA tool *safe*?

STPA tool qualification with STPA

27.3.2025

The transition from STPA theory to practice is already supported by many tools



PASTA (STPA-DSL)
kieler | 245 installs | ★★★★★ (1) | Free

A DSL for STPA. Includes an automatic visualization of the defined relationships and control structure.

[Install](#) [Trouble Installing?](#)

[Overview](#) [Version History](#) [Q & A](#) [Rating & Review](#)

PASTA: Pragmatic Automated System-Theoretic Process Analysis

This extension offers a Domain-Specific-Language (DSL) for System-Theoretic Process Analysis (STPA) including an automatic visualization and validity checks.

Examples can be found in [pasta-examples](#).

Features

Validity Checks

Several validity checks are provided, for example

- for each control action at least one Unsafe Control Action (UCA) must be defined.
- for each UCA a constraint must be defined.

These checks can be turned off in the context menu of the editor.

STPAmaster Lite

STPAmaster Lite is a free STPA tool designed for anyone interested to learn & perform STPA

Automated ID generation & traceability
Adding losses, system-level hazards and constraints autogenerates IDs and references.

Automated import of your safety control structure
Both system components and interactions are automatically imported.

Pre-generation of unsafe control actions (UCA) & Loss Scenarios (LS)
Most of the text pre-generates, just edit the fields accordingly.

SEE HOW IT HELPS → SIMPLE WORKFLOW → EASY INPUT → PRE-GENERATED TEXT

T A C R This project is financed from the state budget by the Technology Agency of the Czech Republic and the Ministry of Industry and Trade within the I4I200 Programme.

We at AKAENE believe that systemic approach to safety is the next step to We devoted our efforts to its industry application/standardization, the like If you want to share your thoughts or suggestions on the tool do not hesitate

[Click here to send us an e-mail](#)

mailto:info@akaene.com

STPAmaster Lite Summary | 1. Define analysis purpose | 2. Control structure | 3. Unsafe control actions | 4. Loss scenarios | System-level

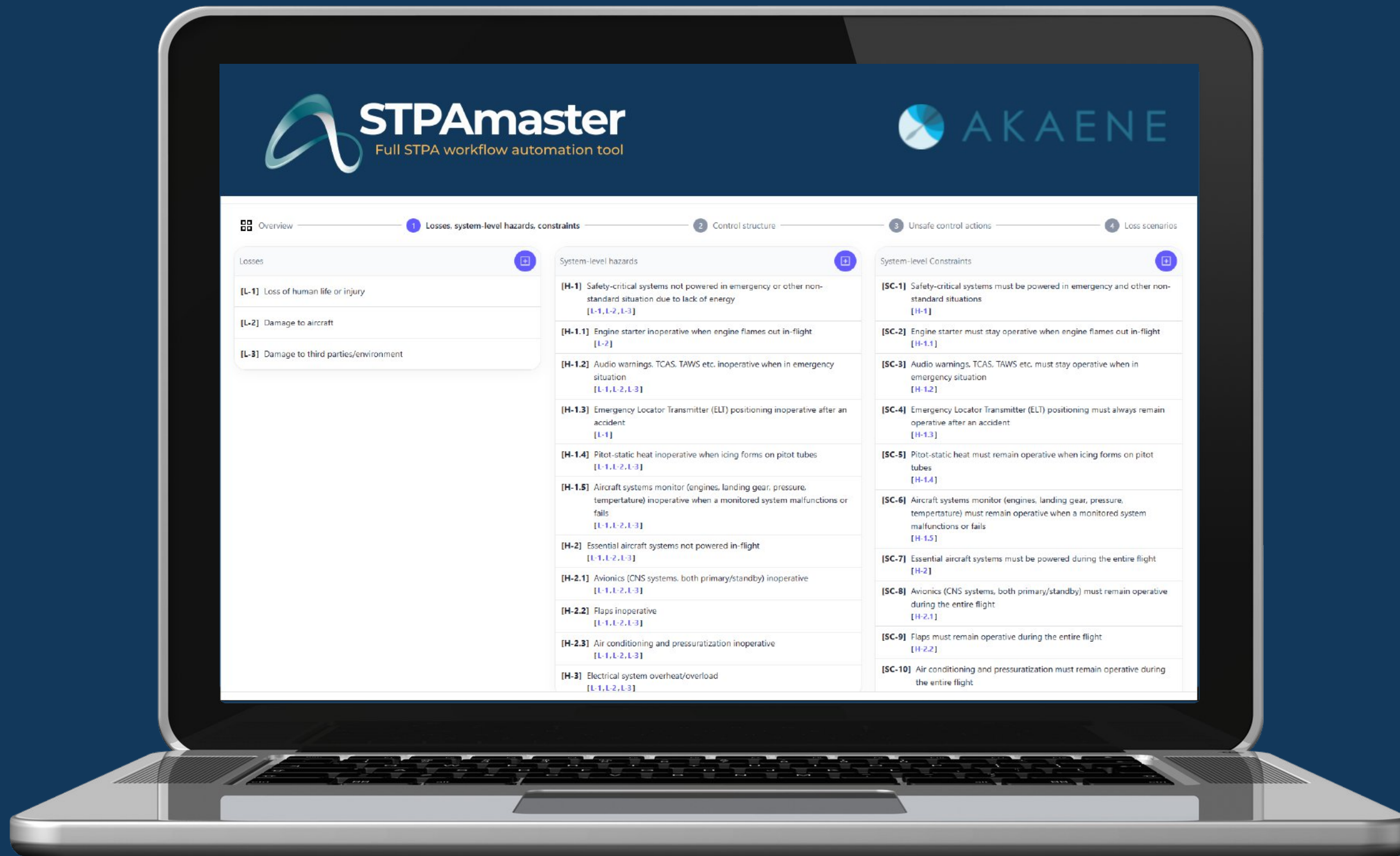
VWAY

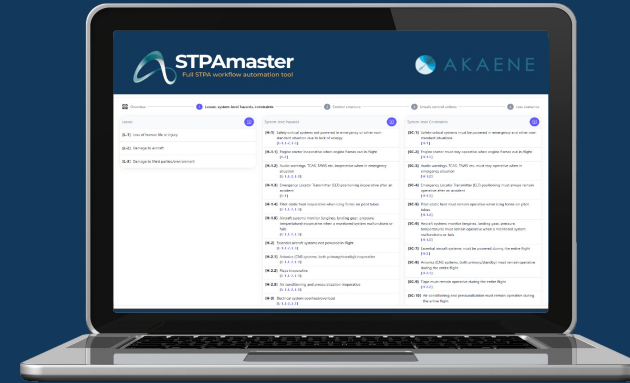
MIT STAMP WORKSHOP

VisualPro - Blended Analysis Software

(STPA & CAST, and Others)

Professional STPA tools **might feel especially safe**



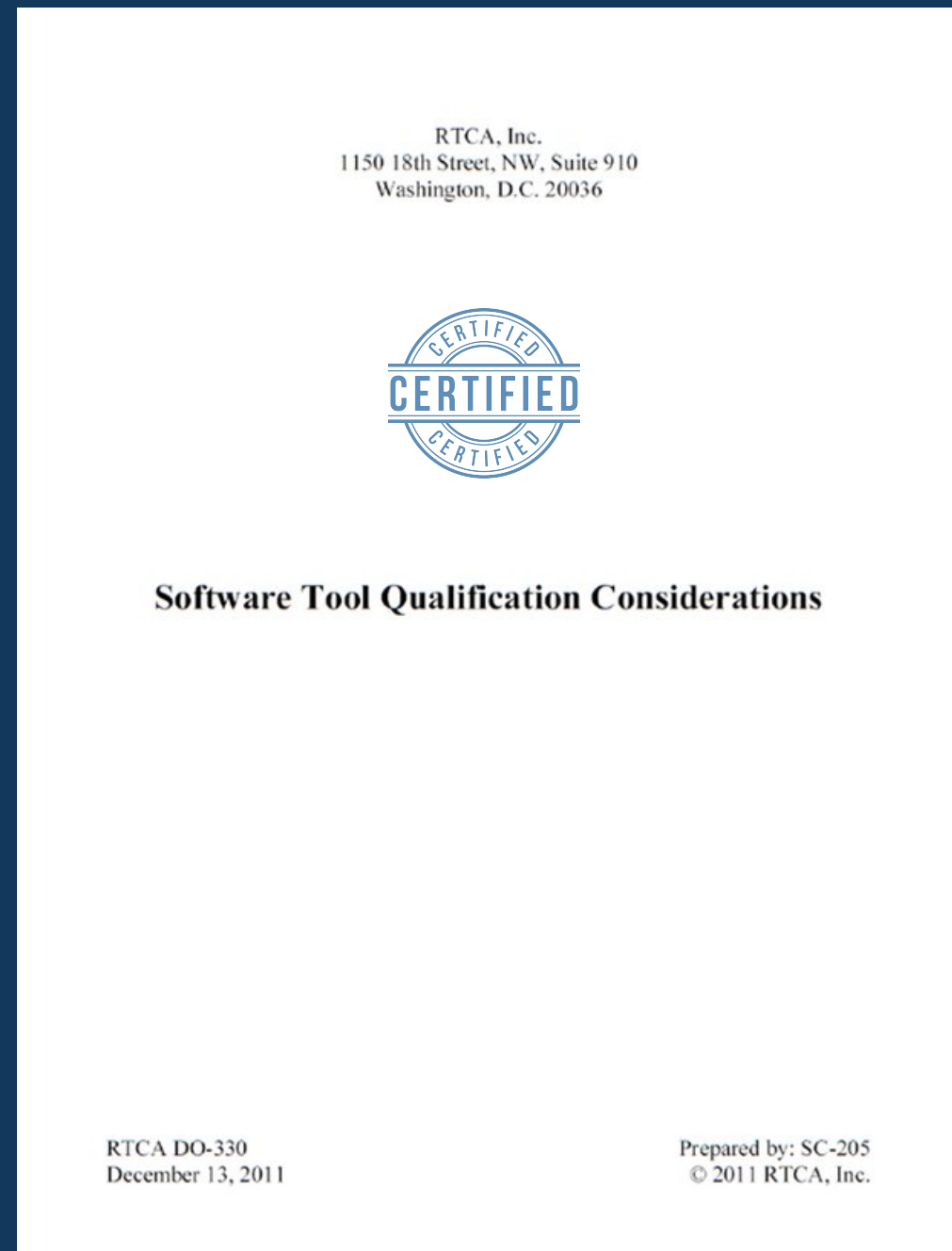


“

But are they?

”

The good news is,
there is a process to follow...

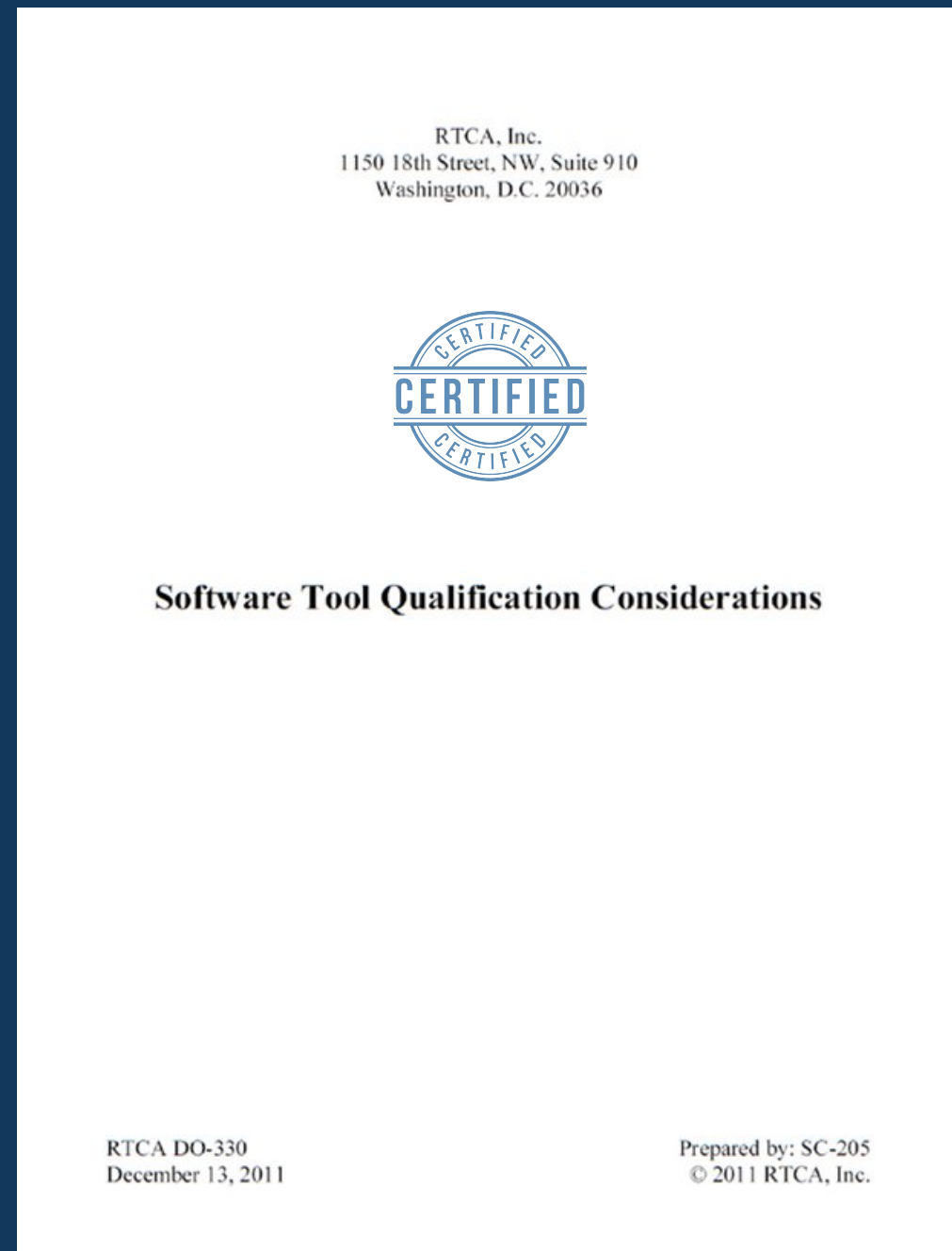


Applicable standard: *RTCA DO-330*

Tool qualification guidance

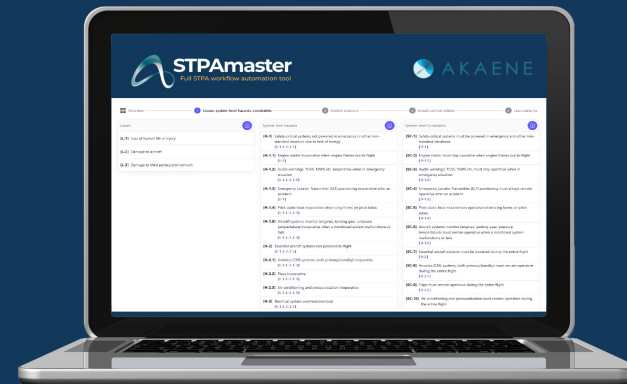
Covering the entire tool life cycle

...the bad news,
it relies on proper requirements definition

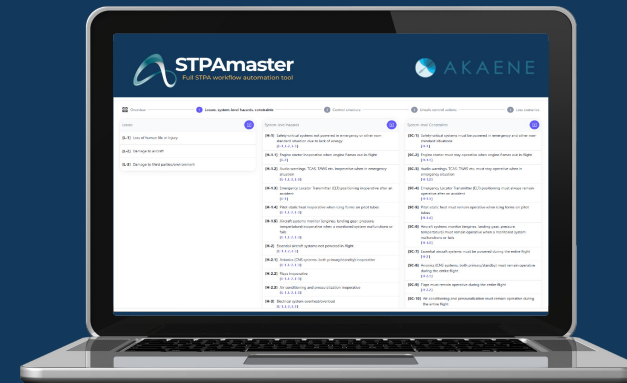


Applicable standard: *RTCA DO-330*

No guidance on which
methods to use



What if we used STPA
to qualify our STPA tool?



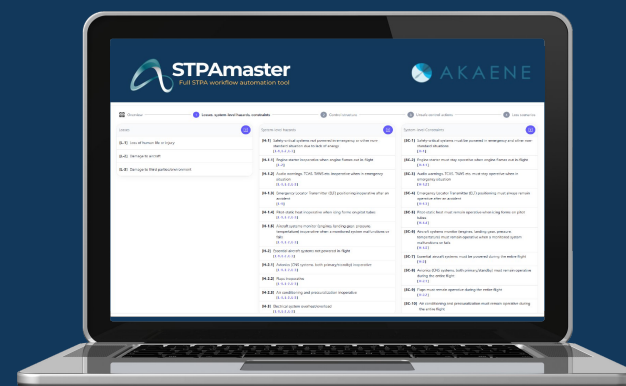
STPA can support ensuring SW safety



Most of the issues with SW relate to requirements flaws - applies on STPA tools as well!



STPA can be used to develop tool requirements with the DO-330 process



Overview — 1 Losses, system-level hazards, constraints — 2 Control structure — 3 Unsafe control actions — 4 Loss scenarios

Losses



[L-1] Loss of STPAmaster qualification

[L-2] Loss of trust in the STPAmaster

System-level hazards



[H-1] STPAmaster produces erroneous analysis
[L-1, L-2]

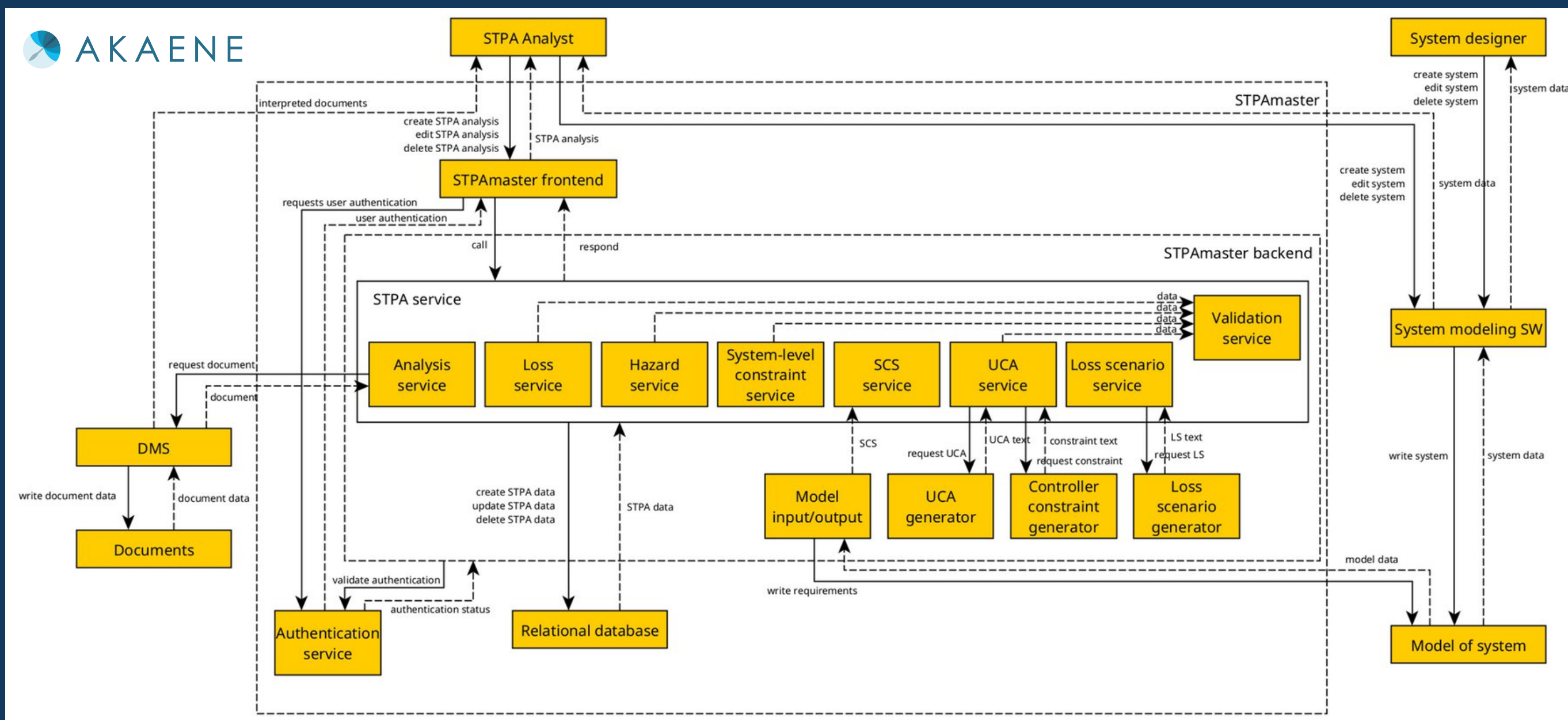
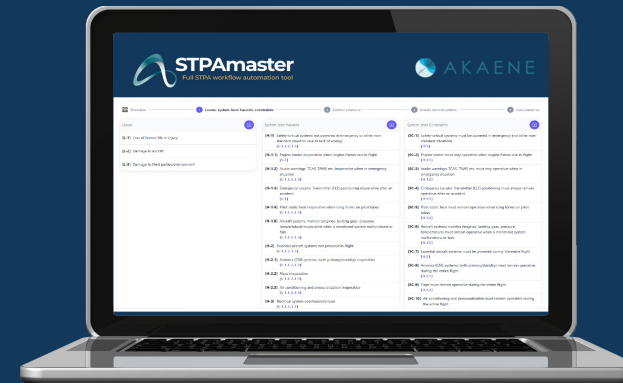
[H-2] STPAmaster does not detect user-induced critical errors
[L-1, L-2]

System-level Constraints



[SC-1] STPAmaster must produce error-free analyses.
[H-1]

[SC-2] If the STPAmaster produces erroneous analysis, it must be detected.
[H-1, H-2]





Controller
STPA Analyst



Expand all Collapse all Show all constraints Hide all constraints

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
add loss scenario → STPA step 4 Show constraints	[UCA-1] STPA Analyst does not provide the add loss scenario action when a loss scenario exists. [H-1, H-2]	[UCA-2] STPA Analyst provides the add loss scenario action that violates the STPA guidance. [H-1, H-2]	[UCA-3] STPA Analyst provides the add loss scenario action too late, when the analysis outputs are already used by other engineers. [H-1] [UCA-4] STPA Analyst provides the add loss scenario action too early, before relevant unsafe control actions have been defined. [H-1, H-2]	
add loss, system-level hazard or system-level constraints → STPA step 1 Show more Show constraints	[UCA-5] STPA Analyst does not provide the add loss, system-level hazard or system-level constraints action when loss or system-level hazard exists, or when system-level constraints shall be defined [H-1, H-2]	[UCA-6] STPA Analyst provides the add loss, system-level hazard or system-level constraints action that violates the STPA guidance. [H-1, H-2]	[UCA-7] STPA Analyst provides the add loss, system-level hazard or system-level constraints action too late, when the analysis outputs are already used by other engineers. [H-1, H-2] [UCA-8] STPA Analyst provides the add loss, system-level hazard or system-level constraints action too early, before relevant referenced items have been defined. ...	
	[UCA-9] STPA Analyst does not provide the	[UCA-10] STPA Analyst provides the add	[UCA-11] STPA Analyst provides the add	

Controller Details

STPA Analyst

[← Back](#)

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
add loss scenario → STPA step 4	[C-1] STPA Analyst must add loss scenario when a loss scenario exists.	[C-2] STPA Analyst must add only loss scenario action that follows the STPA guidance.	[C-3] STPA Analyst must add loss scenario before the analysis outputs are used by other engineers. [C-4] STPA Analyst must add loss scenarios only after relevant unsafe control actions have been defined.	
add loss, system-level hazard or system-level constraints → STPA step 1	[C-5] STPA Analyst must add loss, system-level hazard or system-level constraints when loss or system-level hazard exists, or when system-level constraints shall be defined.	[C-6] STPA Analyst must add only loss, system-level hazard or system-level constraints action that meets the STPA guidance.	[C-7] STPA Analyst must add loss, system-level hazard or system-level constraints before the analysis outputs are used by other engineers. [C-8] STPA Analyst must add loss, system-level hazard or system-level constraints action only after relevant referenced items have been defined.	
add unsafe control action or controller constraint → STPA step 3	[C-9] STPA Analyst must add unsafe control action or controller constraint when unsafe control action exists, or when controller constraint shall be defined	[C-10] STPA Analyst must add unsafe control action or controller constraint that meets the STPA guidance.	[C-11] STPA Analyst must add unsafe control action or controller constraint before the analysis outputs are already used by other engineers [C-12] STPA Analyst must add unsafe control action or controller constraint only when all relevant referenced items have been defined.	

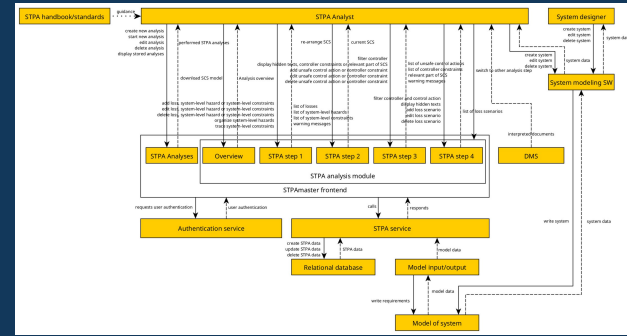
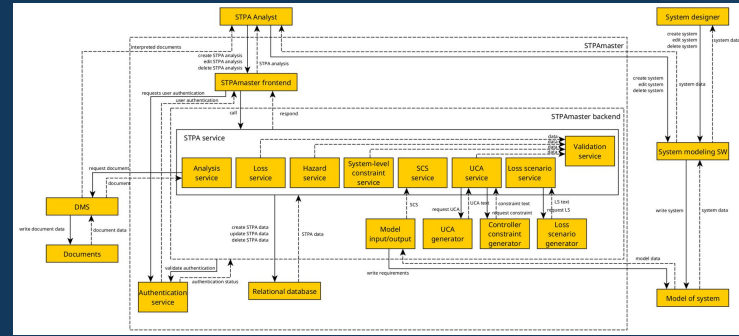


Controller
STPA Analyst

Control Action
All

Expand all Collapse all

Unsafe Control Action	Unsafe Controller Behavior	Unsafe Feedback Path	Unsafe Control Path	Unsafe Controlled Process Behavior
[UCA-1] STPA Analyst does not provide the add loss scenario action when a loss scenario exists.	[LS-1] STPA Analyst does not provide the add loss scenario action - STPA Analyst received feedback (or other inputs) that indicated that a loss scenario exists	[LS-2] Feedback (or other inputs) received by STPA Analyst does not adequately indicate that a loss scenario exists - it is true that a loss scenario exists	[LS-3] STPA Analyst does provide the add loss scenario action when a loss scenario exists - add loss scenario is not received by STPA step 4 when a loss scenario exists	[LS-4] The add loss scenario action is received by STPA step 4 when a loss scenario exists - STPA step 4 does not respond adequately (by adding loss scenario)
[UCA-2] STPA Analyst provides the add loss scenario action that violates the STPA guidance.	[LS-5] STPA Analyst provides the add loss scenario action - STPA Analyst received feedback (or other inputs) that indicated that a scenario violates the STPA guidance	[LS-6] Feedback (or other inputs) received by STPA Analyst does not adequately indicate that the scenario violates the STPA guidance - it is true that a scenario violates the STPA guidance	[LS-7] STPA Analyst does not provide the add loss scenario action when a scenario violates the STPA guidance - STPA step 4 receives add loss scenario when a scenario violates the STPA guidance	[LS-8] The add loss scenario action is not received by STPA step 4 when a scenario violates the STPA guidance - STPA step 4 responds (by adding loss scenario)
[UCA-3] STPA Analyst provides the add loss scenario action too late, when the analysis outputs are already used by other engineers.	[LS-9] STPA Analyst provides the add loss scenario action too late - STPA Analyst received feedback (or other inputs) that indicated on time that the analysis outputs are already used by other engineers	[LS-10] Feedback (or other inputs) received by STPA Analyst does not indicate on time the analysis outputs are already used by other engineers - it is true that the analysis outputs are already used by other engineers	[LS-11] STPA Analyst provides the add loss scenario action on time, before the analysis outputs will be used by other engineers - add loss scenario is received by STPA step 4 too late, after the analysis outputs are already used by other engineers	[LS-12] The add loss scenario action is received by STPA step 4 on time before the analysis outputs will be used by other engineers - STPA step 4 does not respond adequately (by adding loss scenario)(too late)




Tool architecture

Monitoring STPA workflow

Tracking analysis conflicts, inconsistency or incompleteness

Tracking changes to the analysis and their inputs / outputs

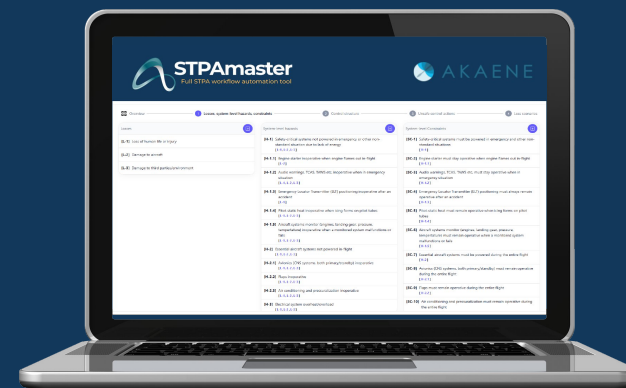
Supporting the user for common mistakes



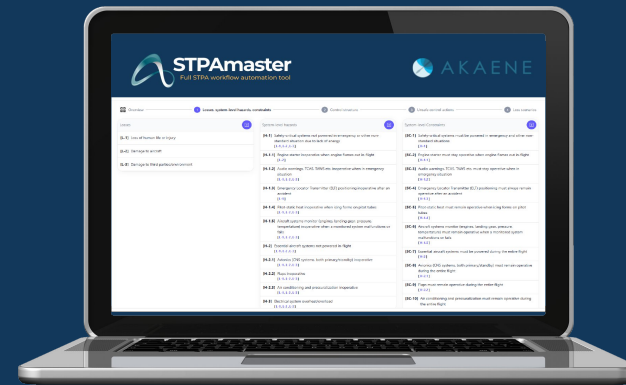
User interaction

Be properly trained in STPA

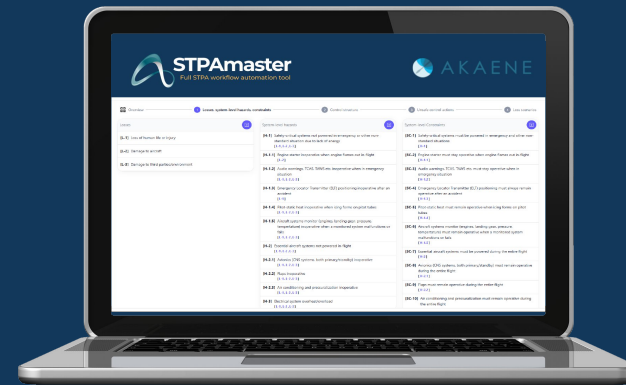
Indicate their actions & intentions



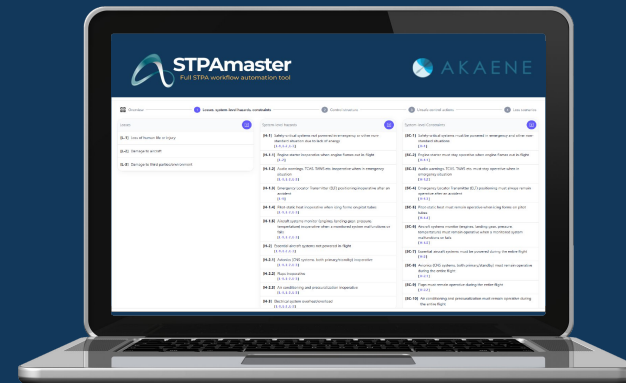
...so is the STPAmaster
safe to use?



STPAmaster is **ready to be qualified**
for safety-critical applications



Joint efforts will be needed



AKAENE provides **full support**
of **DO-330**, while using the STPA