AKAENE

STPAmaster Lite

The new STPA Automation Tool

4.6.2024

AKAENE

10+ research projects
in aviation safety and knowledge management

25+ STAMP and STPA-based case studies
50+ research papers

7 years in STAMP,
15 years in safety management systems

AKAENE

Can we beat the most popular STPA tools?

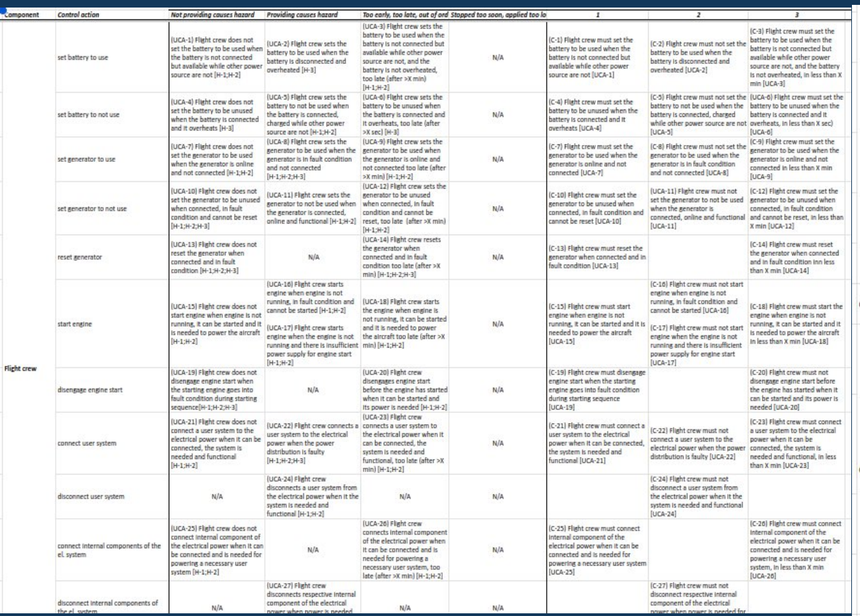
1. Pen and paper

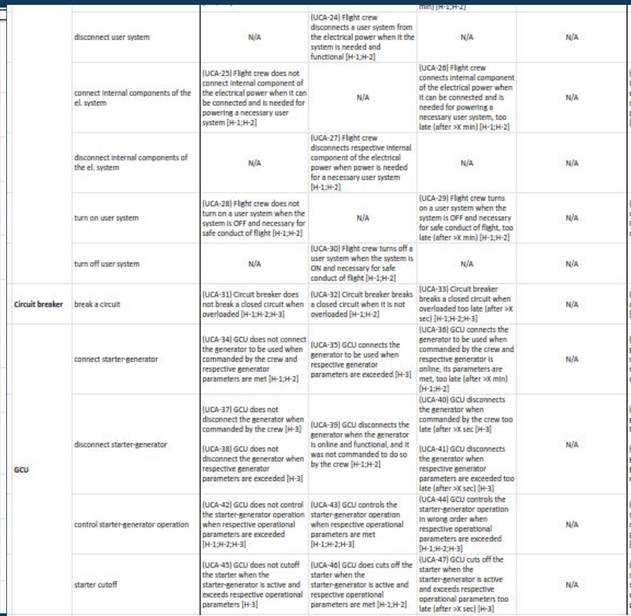
Image source: https://www.linkedin.com/pulse/messy-whiteboard-vs-clean-chad-j-willett/

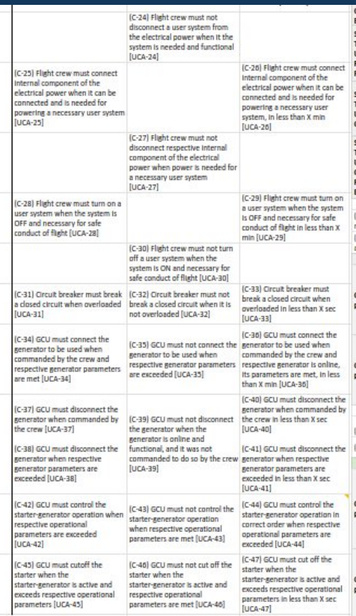
AKAENE

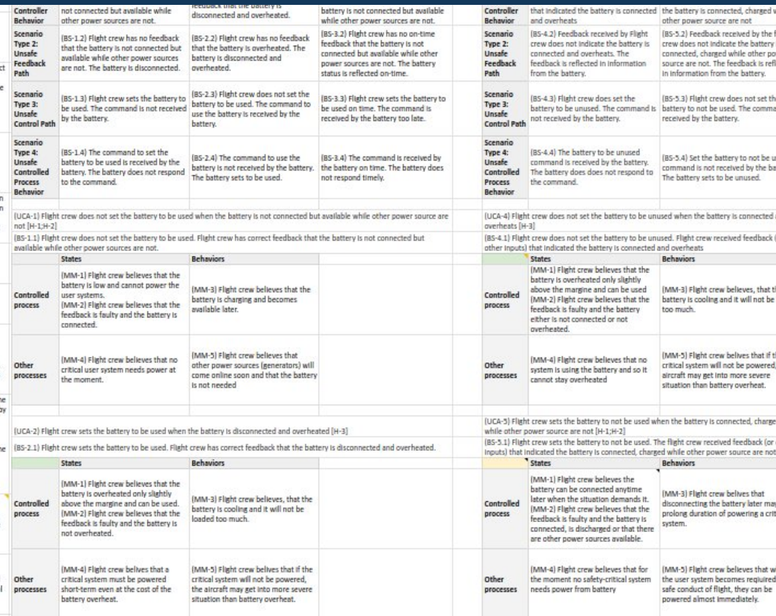
Can we beat the most popular STPA tools?

2. Microsoft Office (or equivalent)





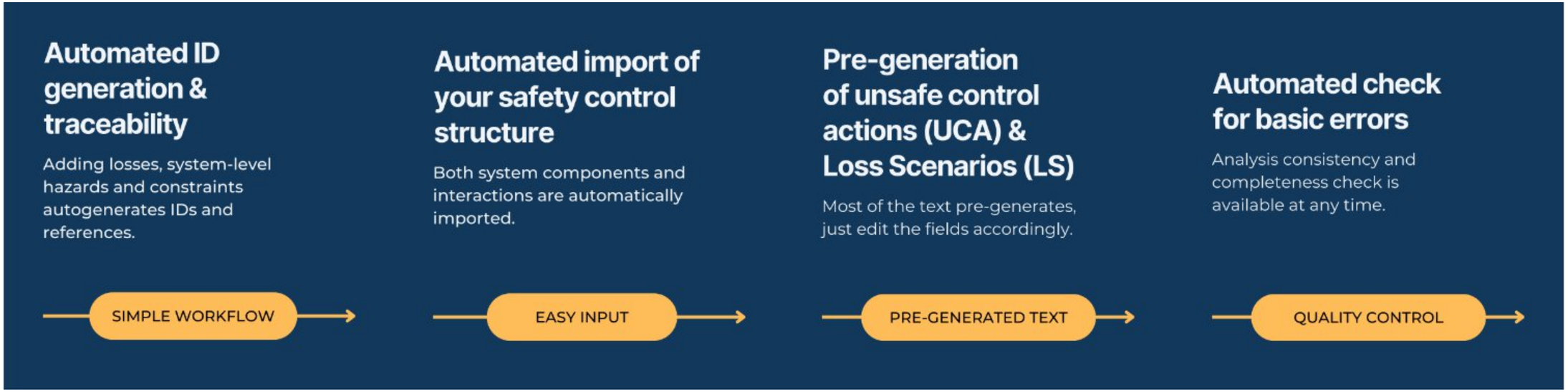




...and still have it

free for everyone?

STPAmaster Lite is easy, free, waiting for your feedback.



Google Sheets yEd draw.io

AKAENE

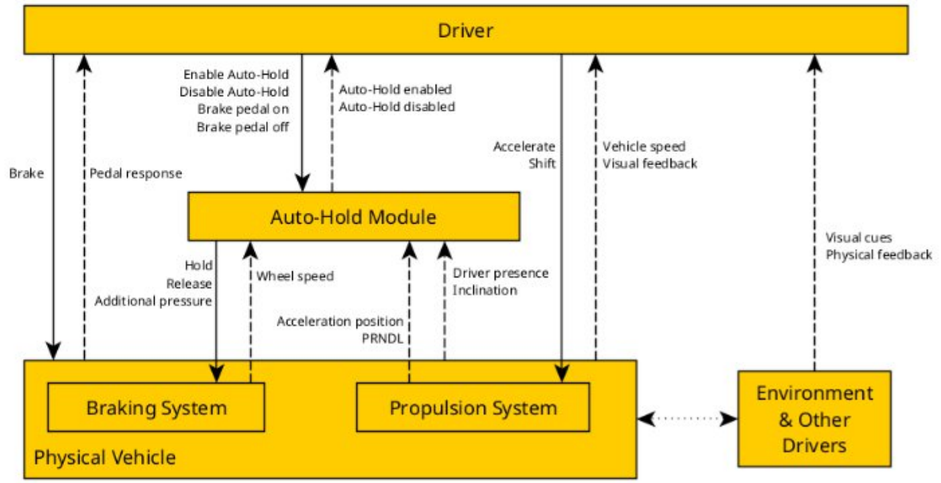
https://stpamaster.com/

STPAmaster Lite is easy, free, waiting for your feedback.

Import your safety control structure. Click on the button to enter the URL of the file containing the control structure diagram. System components and interactions will be im

Import control structure *You can also drop and image here to see the control structure. Do not edit the "controller", "control action" and "controlled process" columns, changes may break the analysis.*

Controller	Control action	Controlled process
Auto-Hold Module	Hold	Braking System
	Release	Braking System
	Additional pressure	Braking System
Driver	Brake	Physical Vehicle
	Enable Auto-Hold	Auto-Hold Module
	Disable Auto-Hold	Auto-Hold Module
	Brake pedal on	Auto-Hold Module
	Brake pedal off	Auto-Hold Module
	Accelerate	Propulsion System
	Shift	Propulsion System

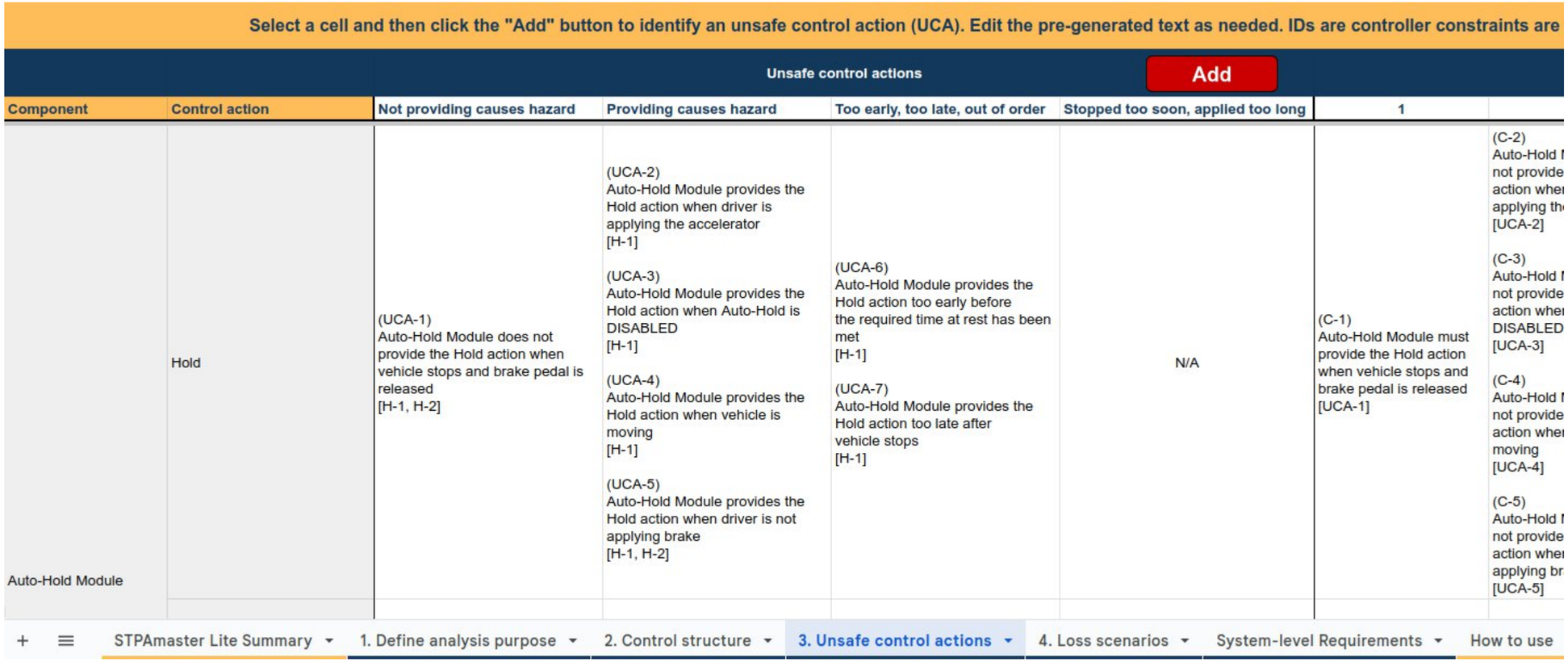


STPAmaster Lite Summary | 1. Define analysis purpose | 2. Control structure | 3. Unsafe control actions | 4. Loss scenarios | System-level Requirements | How to use

AKAENE

https://stpamaster.com/

STPAmaster Lite is easy, free, waiting for your feedback.



Select a cell and then click the "Add" button to identify an unsafe control action (UCA). Edit the pre-generated text as needed. IDs are controller constraints are

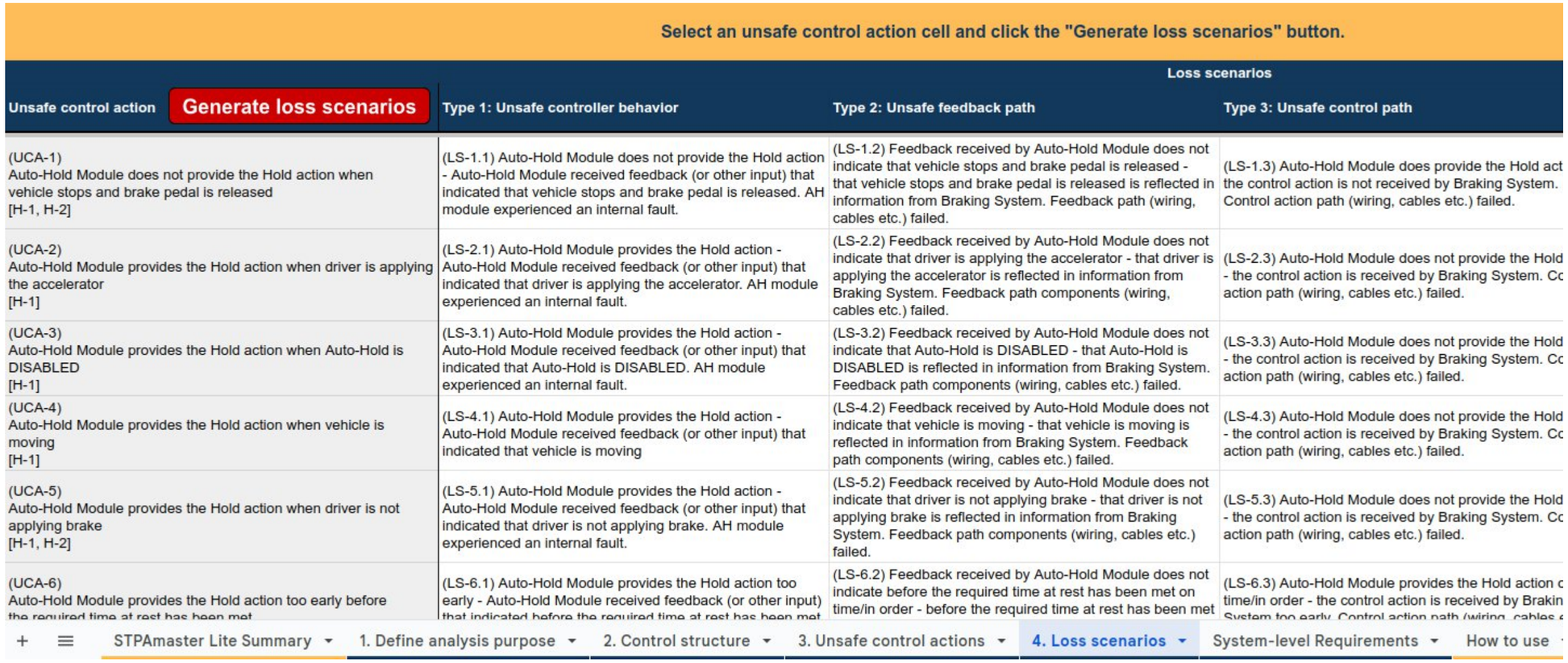
		Unsafe control actions				Add	
Component	Control action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long	1	
Auto-Hold Module	Hold	(UCA-1) Auto-Hold Module does not provide the Hold action when vehicle stops and brake pedal is released [H-1, H-2]	(UCA-2) Auto-Hold Module provides the Hold action when driver is applying the accelerator [H-1] (UCA-3) Auto-Hold Module provides the Hold action when Auto-Hold is DISABLED [H-1] (UCA-4) Auto-Hold Module provides the Hold action when vehicle is moving [H-1] (UCA-5) Auto-Hold Module provides the Hold action when driver is not applying brake [H-1, H-2]	(UCA-6) Auto-Hold Module provides the Hold action too early before the required time at rest has been met [H-1] (UCA-7) Auto-Hold Module provides the Hold action too late after vehicle stops [H-1]	N/A	(C-1) Auto-Hold Module must provide the Hold action when vehicle stops and brake pedal is released [UCA-1]	(C-2) Auto-Hold M not provide action wher applying th [UCA-2] (C-3) Auto-Hold M not provide action wher DISABLED [UCA-3] (C-4) Auto-Hold M not provide action wher moving [UCA-4] (C-5) Auto-Hold M not provide action wher applying br [UCA-5]

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

AKAENE

https://stpamaster.com/

STPAmaster Lite is easy, free, waiting for your feedback.



Select an unsafe control action cell and click the "Generate loss scenarios" button.

Unsafe control action	Generate loss scenarios	Loss scenarios: Type 1: Unsafe controller behavior	Type 2: Unsafe feedback path	Type 3: Unsafe control path
(UCA-1) Auto-Hold Module does not provide the Hold action when vehicle stops and brake pedal is released [H-1, H-2]		(LS-1.1) Auto-Hold Module does not provide the Hold action - Auto-Hold Module received feedback (or other input) that indicated that vehicle stops and brake pedal is released. AH module experienced an internal fault.	(LS-1.2) Feedback received by Auto-Hold Module does not indicate that vehicle stops and brake pedal is released - that vehicle stops and brake pedal is released is reflected in information from Braking System. Feedback path (wiring, cables etc.) failed.	(LS-1.3) Auto-Hold Module does provide the Hold act the control action is not received by Braking System. Control action path (wiring, cables etc.) failed.
(UCA-2) Auto-Hold Module provides the Hold action when driver is applying the accelerator [H-1]		(LS-2.1) Auto-Hold Module provides the Hold action - Auto-Hold Module received feedback (or other input) that indicated that driver is applying the accelerator. AH module experienced an internal fault.	(LS-2.2) Feedback received by Auto-Hold Module does not indicate that driver is applying the accelerator - that driver is applying the accelerator is reflected in information from Braking System. Feedback path components (wiring, cables etc.) failed.	(LS-2.3) Auto-Hold Module does not provide the Hold - the control action is received by Braking System. Cc action path (wiring, cables etc.) failed.
(UCA-3) Auto-Hold Module provides the Hold action when Auto-Hold is DISABLED [H-1]		(LS-3.1) Auto-Hold Module provides the Hold action - Auto-Hold Module received feedback (or other input) that indicated that Auto-Hold is DISABLED. AH module experienced an internal fault.	(LS-3.2) Feedback received by Auto-Hold Module does not indicate that Auto-Hold is DISABLED - that Auto-Hold is DISABLED is reflected in information from Braking System. Feedback path components (wiring, cables etc.) failed.	(LS-3.3) Auto-Hold Module does not provide the Hold - the control action is received by Braking System. Cc action path (wiring, cables etc.) failed.
(UCA-4) Auto-Hold Module provides the Hold action when vehicle is moving [H-1]		(LS-4.1) Auto-Hold Module provides the Hold action - Auto-Hold Module received feedback (or other input) that indicated that vehicle is moving	(LS-4.2) Feedback received by Auto-Hold Module does not indicate that vehicle is moving - that vehicle is moving is reflected in information from Braking System. Feedback path components (wiring, cables etc.) failed.	(LS-4.3) Auto-Hold Module does not provide the Hold - the control action is received by Braking System. Cc action path (wiring, cables etc.) failed.
(UCA-5) Auto-Hold Module provides the Hold action when driver is not applying brake [H-1, H-2]		(LS-5.1) Auto-Hold Module provides the Hold action - Auto-Hold Module received feedback (or other input) that indicated that driver is not applying brake. AH module experienced an internal fault.	(LS-5.2) Feedback received by Auto-Hold Module does not indicate that driver is not applying brake - that driver is not applying brake is reflected in information from Braking System. Feedback path components (wiring, cables etc.) failed.	(LS-5.3) Auto-Hold Module does not provide the Hold - the control action is received by Braking System. Cc action path (wiring, cables etc.) failed.
(UCA-6) Auto-Hold Module provides the Hold action too early before the required time at rest has been met		(LS-6.1) Auto-Hold Module provides the Hold action too early - Auto-Hold Module received feedback (or other input) that indicated before the required time at rest has been met	(LS-6.2) Feedback received by Auto-Hold Module does not indicate before the required time at rest has been met on time/in order - before the required time at rest has been met	(LS-6.3) Auto-Hold Module provides the Hold action c time/in order - the control action is received by Brakin System too early. Control action path (wiring, cables

+ ≡ STPAmaster Lite Summary | 1. Define analysis purpose | 2. Control structure | 3. Unsafe control actions | 4. Loss scenarios | System-level Requirements | How to use

AKAENE

https://stpamaster.com/