AKAENE

STPAmaster Lite

The new STPA Automation Tool

4.6.2024









10+ research projects in aviation safet and knowledge safety management

7 years in STAMP, 15 years in safety management systems

AKAENE

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



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/



Can we beat the most popular STPA tools?

2. Microsoft Office

(or equivalent)

ponent Co	ntrol action	Not providing causes hazard	roviding causes hazard	Too early, too late, out of ord Stopp	ed too soon, applied too lo	1	2	3	-		2019-02	(UCA-24) Flight crew	min) (H-1;H-2)			(C-24) Flight crew must not			not connected but available while	disconnected and overheated.	battery is not connected but available		ler that indicated the battery is connected			
set battery to use	batters to une	(UCA-1) Flight crew does not set the bettery to be used when	UCA-2) Flight crew sets the sattery to be used when the	(UCA-3) Flight crew sets the battery to be used when the battery is not connected but available while other power source are not, and the		(C-1) Flight crew must set the battery to be used when the battery is not connected but available while other power	(C-2) Flight crew must not set the battery to be used when the battery is disconnected and	(C-3) Flight crew must set the battery to be used when the battery is not connected but available while other power source are not, and the battery		disconnect user system		disconnects a user system from the electrical power when it the system is needed and functional [H-1;H-2]	e N/A	N/A		disconnect a user system from the electrical power when it th system is needed and functions [UCA-24]	e	Behavior Scenario Type 2: Unsafe + Feedback	(BS-1.2) Flight crew has no feedback	(BS-2.2) Flight crew has no feedbac that the battery is overheated. The battery is disconnected and	connected but available while other power sources are not. The battery	Scenario Type 2: Unsafe Feedbac	connected and overheats. The	crew does not indicate the ba connected, charged while oth source are not. The feedback		
		source are not (in 1,in 1)		battery is not overheated, too late (after >X min) [H-1;H-2] [UCA-0] Flight crew sets the		source are not [UCA-1]	overneated [UCA-2]	ed [UCA-2] source are not, and the battery is not overheated, in less than X min [UCA-3] ht crew must not set the [UCA-0] Flight crew must set the	x			ment of	(UCA-26) Flight crew connects internal component of the electrical power when it can be connected and is	N/A	(C-25) Flight crew must connect internal component of the electrical power when it can be		Internal component of the electrical power when it can b connected and is needed for	Path		(BS-2 3) Flight crew does not set th	e (BS-3.3) Flight crew sets the battery to	Path	from the battery. (BS-4.3) Flight crew does set the	In Information from the batte (BS-5.3) Flight crew does not		
		when the battery to be unused when the battery is connected	sattery to not be used when he battery is connected, harged while other power ource are not [H-1;H-2]	battery to be unused when the battery is connected and it overheats, too late (after >X sec) [H-3]	N/A	(C-4) Flight crew must set the battery to be unused when the battery is connected and it overheats [UCA-4]	battery to not be used when the battery is connected, charged while other power source are not [UCA-5]	battery to be unused when the battery is connected and it overheats, in less than X sec) [UCA-6]		el system	be connected and is needed for powering a necessary user system [H-1;H-2]	(UCA-27) Flight crew	necessary user system, too late (after >X min) [H-1;H-2]		connected and is needed for powering a necessary user system [UCA-25]	m (C-27) Flight crew must not	powering a necessary user system, in less than X min [UCA-26]	Type 3: Unsafe Control Pa	be used. The command is not received	to ed battery to be used. The command use the battery is received by the battery.	be used on time. The command is	Type 3: Unsafe Control	battery to be unused. The command			
		set the generator to be used when the generator to a build generator to be used when the generator to a build generator to be used when the generator to a build generator generator to a build generator to a build generator generator to a build generator to a build generator generator to a build generator to a build generator generat		generator to be used when the generator is online and not	stator to be used when the generator to be used when the generator is online and not generator is in fault condition			disconnect internal components of the el. system	N/A	(UCA-27) Fight crew disconnects respective internal component of the electrical power when power is needed for a necessary user system [H-1:H-2]	N/A	N/A		(C-27) Fight crew must not disconnect respective internal component of the electrical power when power is needed f a necessary user system [UCA-27]	for	Scenario Type 4: Unsafe Controlled Process	(BS-1.4) The command to set the battery to be used is received by th battery. The battery does not respo to the command.	battenuis not received by the batte	(BS-3.4) The command is received by ry. the battery on time. The battery does not respond timely.	Unsafe Control Process	(BS-4.4) The battery to be unused command is received by the battery. led The battery does does not respond to the command.	(BS-5.4) Set the battery to not command is not received by t The battery sets to be unused				
	• • • •	(UCA-10) Flight crew does not set the energitar to be unused			-	(C-10) Flight crew must set the	(UCA-11) Flight crew must not set the generator to not be used						(UCA-29) Flight crew turns				(C-29) Flight crew must turn on	Behavior				Behavio	Behavior			
se	Renerator to not use	when connected in fault	he generator to not be used when the generator is connected, anline and functional [H-1;H-2]	when connected, in fault	N/A	generator to be unused when connected, in fault condition and cannot be reset [UCA-10]	when the generator is connected, online and functional	connected, in fault condition		turn on user system	(UCA-28) Flight crew does not turn on a user system when the system is OFF and necessary for	the N/A	on a user system when the system is OFF and necessary for safe conduct of flight, too	y N/A	(C-28) Flight crew must turn on a user system when the system is OFF and necessary for safe	a user system whe Is OFF and necessa	a user system when the system	(UCA-1) Fi	Flight crew does not set the battery to be used when the battery is not connected but available while other power source are 154-2]		(UCA-4) Flight crew does not set the battery to be unused when the battery is connecte overheats [H-3]					
		(UCA-13) Flight crew does not	light crew does not ULA-14 Flight crew rests [C-14] Flight crew must see the [C-14] Flight crew		(C-14) Flight crew must reset	-		safe conduct of flight [H-1;H-2]	(UCA-30) Flight crew turns off a	late (after >X min) [H-1;H-2]		conduct of flight [UCA-28]	min [UCA-29] (C-30) Flight crew must not turn	min [UCA-29]	(BS-1.1) Flight		e used. Flight crew has correct feedback that the battery is not connected but			Flight crew does not set the battery to be o pouts) that indicated the battery is connected						
re	et generator	reset the generator when connected and in fault		onnected and in fault N/A	d in fault N/A	nd in fault N/A	d in fault N/A	N/A genera	(C-13) Flight crew must reset the generator when connected and fault condition [UCA-13]		the generator when connected and in fault condition inn less		turn off user system	51/5	user system when the system is		N/A		off a user system when the	evenau/e v	States	Behaviors		uner in	States	Behaviors
start engine		condition [H-1;H-2;H-3]	UCA-16) Flight crew starts	condition too late (after >X min) [H-1;H-2;H-3]	-	Ideax condition [OCK-13]	(C-16) Flight crew must not start	than X min [UCA-14]		and an arrangements of the second sec		ON and necessary for safe conduct of flight [H-1;H-2]				system Is ON and necessary for safe conduct of flight [UCA-30]			(MIM-1) Flight crew believes that th battery is low and cannot power the	1 C			(MM-1) Flight crew believes that the battery is overheated only slightly			
	rt engine	(UCA-15) Flight crew does not start engine when engine is not running, it can be started and it	engine when engine is not unning, in fault condition and cannot be started [H-1;H-2] UCA-17] Flight crew starts	the engine when engine is not running, it can be started and it is needed to power	N/A	(C-13) Flight crew must start engine when engine is not running, it can be started and it is needed to power the aircraft	engine when engine is not running, in fault condition and cannot be started [UCA-18] (C-17) Flight crew must not start	(C-18) Flight crew must start the engine when engine is not running, it can be started and it is needed to power the aircraft	d it	break a circuit		(UCA-32) Circuit breaker breaker a closed circuit when it is not overloaded [H-1;H-2]	UCA-33) Circuit breaker breaks a closed circuit when overloaded too late (after >X sec) [H-1;H-2;H-3] (UCA-36) GCU connects the	N/A		k [C-32] Orcuit breaker must not break a closed circuit when it is not overloaded [UCA-32]	overloaded In less than X sec [UCA-33]	Controlled process	trolled user systems.	battery is charging and becomes		Control process	led above the margine and can be used (MM-2) Flight crew believes that the feedback is faulty and the battery either is not connected or not overheated.	battery is cooling and it will n		
		[H-1;H-2]		eh the engine is not to be arrorar tob tate jarter >x [UCA-15] ply for engine start	[UCA-15] running and there is power supply for eny [UCA-17]	5] running and there is insufficient power supply for engine start [UCA-17]		connect starter-generator	commanded by the crew and	respective generator	generator to be used when commanded by the crew and respective generator is online its parameters are	N/A	[C-34] GCU must connect the generator to be used when commanded by the crew and respective generator parameters.	generator to be used when respective generator parameter	(C-38) GCU must connect the generator to be used when commanded by the crew and respective generator is online,		(MM-4) Flight crew believes that no critical user system needs power at		dl	Other	(MM-4) Flight crew believes that no system is using the battery and so it	(MM-5) Flight crew belives th critical system will not be pow				
		(UCA-19) Flight crew does not disengage engine start when the starting engine goes into fault condition during starting		(UCA-20) Flight crew disengages engine start before the engine has started when it can be started and	N/A	(C-19) Flight crew must disengage engine start when the starting engine goes into fault condition during starting sequence		(C-20) Flight crew must not disengage engine start before the engine has started when it can be started and its power is	-		parameters are met [H-1;H-2]	parameters are exceeded [H-3]	I met, too late (after >X min) [H-1;H-2] (UCA-40) GCU disconnects		are met [UCA-34]	are exceeded [UCA-35]	Its parameters are met, in less than X min [UCA-36] (C-40) GCU must disconnect the	e	processes the moment.	come online soon and that the battery is not needed	tery	process	processes system is using the pattern and so it cannot stay overheated	aircraft may get into more severe situation than battery overheat.		
		sequence[H-1;H-2;H-3]		s power is needed [H-1;H-2] JCA-23] Flight crew		[UCA-19]		needed [UCA-20]		disconnect starter-generator	(UCA-38) GCU does not	[0CA-39] GCD disconnects the generator when the generator is online and functional, and it was not comproved to do so	tor d it (UCA-41) GCU disconnects	21/2		(C-39) GCU must not disconnect the generator when the generator is online and	[UCA-40]	1¥				(UCA-3) Flight crew sets the battery to not be used when the battery is connecti		where the better is every - to do		
			(UCA-22) Flight crew connects a user system to the electrical		when It he N/A	(C-21) Flight crew must connect a user system to the electrical	a (C-22) Flight crew must not	(C-23) Flight crew must connect a user system to the electrical system to the power when it can be when the power connected, the system is	t									(UCA-2) Flight crew sets the battery to be used when the batter		the battery is disconnected and overheated [H-3]		(UCA-3) Fight crew sets the battery to not be used when t while other power source are not [H-1;H-2]		when the battery is connected, c		
	nnect user system		ower when the power	can be connected, the system is needed and		power when it can be connected, the system is needed and	electrical power when the power											(BS-2.1) Fi	ight crew sets the battery to be used. Fil	ght crew has correct feedback that the	battery is disconnected and overheated.	ated. (BS-3.1) Flight crew sets the battery to not be used. The flight crew received inputs) that indicated the battery is connected, charged while other power sets the battery is connected.				
			[H-1;H-2;H-3]		H-1;H-2;H-3]	+1;H-2;H-3]	functional, too late (after >X min) [H-1:H-2]	late (after >X	functional [UCA-21]	distribution is faulty [UCA-22] needed an than X min	needed and functional, in less than X min [UCA-23] GCU	GCU		disconnect the generator when respective generator	was not commanded to do so by the crew [H-1;H-2]	so the generator when respective generator		generator when respective generator parameters are	commanded to do so by the crew [UCA-39]	rew generator when respective generator parameters are		States	Behaviors			States
	connect user system	N/A	UCA-24) Flight crew Ilsconnects a user system from he electrical power when it the		N/A		(C-24) Flight crew must not disconnect a user system from the electrical power when it the				parameters are exceeded [H-3]	t control UCA-43 GCU controls the poration statter-generator operation when respective operational parameters are met [H-1;H-2;H-3] t cutoff [UCA-40] GCU does cuts off the	parameters are exceeded too late (after >X sec) [H-3] (UCA-44) GCU controls the	s are exceeded too >X sec] [H-3]	exceeded [UCA-38] (C-42) GCU must control the starter-generator operation when respective operational parameters are exceeded [UCA-42] (C-45) GCU must cutoff the starter-generator is active and exceeds respective operational	(C-43) GCU must not control the starter-generator operation when respective operational parameters are del I/C-40 and appreciational orrect orde	exceeded in less than X sec [UCA-41]	Controlled	(MM-1) Flight crew believes that th battery is overheated only slightly above the margine and can be used	(a sha b) shake even believen shee she	he	Carterel		(MM-3) Flight crew belives th disconnecting the battery late		
			ystem is needed and unctional [H-1;H-2]				system is needed and functional [UCA-24]						starter-generator operation in wrong order when				(C-44) GCU must control the starter-generator operation in		(MM-2) Flight crew believes that th	bactery is cooling and it will not be		process	(MM-2) Flight crew believes that the feedback is faulty and the battery is	prolong duration of powering		
		(UCA-25) Flight crew does not connect internal component of the electrical power when it can		(UCA-26) Flight crew connects Internal component of the electrical power when it can be connected and is	N/A	(C-25) Flight crew must connect internal component of the electrical power when it can be		[C-26] Flight crew must connect internal component of the electrical power when it can be connected and is needed for		parat			onal respective operational parameters are exceeded [H-1:H-2:H-3]	operational N/A rs are exceeded			ational correct order when respective	ve fe	feedback is faulty and the battery is not overheated.	loaded too much.	connected, is faulty and the battery is connected, is discharged or that there are other power sources available.					
	system	be connected and is needed for powering a necessary user system [H-1;H-2]		needed for powering a necessary user system, too late (after >X min) [H-1;H-2]	170	connected and is needed for powering a necessary user system [UCA-25]		powering a necessary user system, in less than X min [UCA-28]		the	the starter when the		(UCA-47) GCU outs off the	suls.		(C-46) GCU must not cut off the starter when the	e (C-47) GCU must cut off the starter when the starter-generator is active and	Other	(MM-4) Flight crew belives that a critical system must be powered	(MM-5) Flight crew belives that if t critical system will not be powered		Other	(MM-4) Flight crew believes that for the moment no safety-critical system			
dis	connect internal components of		UCA-27) Flight crew disconnects respective internal component of the electrical	N/A	N/A		(C-27) Flight crew must not disconnect respective internal component of the electrical power when power is preded for		5	00	exceeds respective operational		and exceeds respective	N/A			nd exceeds respective operational	processes short-ter				process	other the moment no safety-critical syst processes needs power from battery	em the user system becomes require safe conduct of flight, they can be powered almost immediately.		

Flight cr

...and still have it free for everyone?



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.

EASY INPUT

Pre-generation of unsafe control actions (UCA) & Loss Scenarios (LS)

Most of the text pre-generates, just edit the fields accordingly.

PRE-GENERATED TEXT

SIMPLE WORKFLOW

Google Sheets







Automated check for basic errors

Analysis consistency and completeness check is available at any time.

QUALITY CONTROL

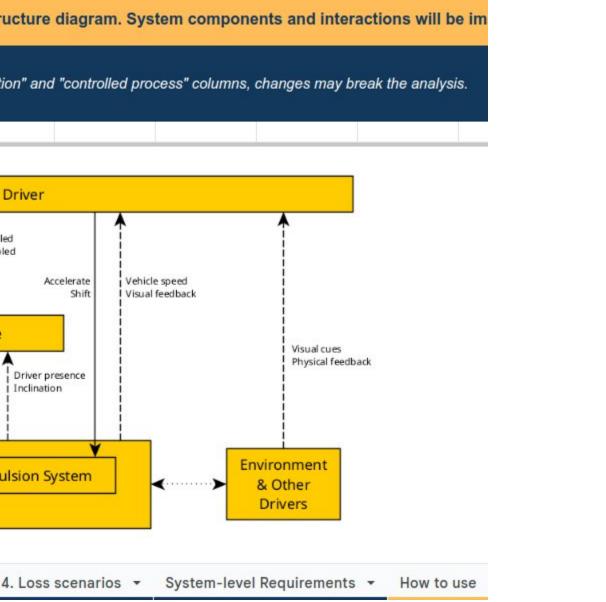
draw.io

Controller	Control action	Controlled process					
Controller	Hold	Braking System					
Auto-Hold Module	Release						
Auto-Hold Module		Braking System					
	Additional pressure Brake	Braking System Physical Vehicle					
	Enable Auto-Hold	Auto-Hold Module		Enable Auto-Hold Disable Auto-Hold Auto-Hold			
	Disable Auto-Hold	Auto-Hold Module		Bra	ke pedal on Auto-Hold disab		
Driver	Brake pedal on	Auto-Hold Module		Brake pedal off			
Dilver	Brake pedal off	Auto-Hold Module	Brake	Pedal response	J i		
	Accelerate	Propulsion System			i		
	Shift	Propulsion System			Auto-Hold Module		
				Hold Release Additional pressure	Wheel speed Acceleration position PRNDL		
				Braking System			









		Add	control actions	Unsafe						
	1	Stopped too soon, applied too long	Too early, too late, out of order	Providing causes hazard	Not providing causes hazard	Control action	omponent			
(C-2) Auto-H not pro action f applyin [UCA-2 (C-3) Auto-H not pro action f DISAB [UCA-3 (C-4) Auto-H not pro action f moving [UCA-4 (C-5) Auto-H not pro action f action f moving [UCA-4	(C-1) Auto-Hold Module must provide the Hold action when vehicle stops and brake pedal is released [UCA-1]	N/A	(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]	(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-1) Auto-Hold Module does not provide the Hold action when vehicle stops and brake pedal is released [H-1, H-2]	Hold	ito-Hold Module			





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

	scenarios				
Type 1: Unsafe controller behavior	Type 2: Unsafe feedback path	Type 3: Unsafe control path			
- Auto-Hold Module received feedback (or other input) that	that vehicle stops and brake pedal is released -	(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.			
(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. Co action path (wiring, cables etc.) failed.			
(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. Co action path (wiring, cables etc.) failed.			
(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. Co action path (wiring, cables etc.) failed.			
(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. Co action path (wiring, cables etc.) failed.			
(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 of time/in order - the control action is received by Brakin System too early. Control action path (wiring, cables of			
	(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-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-3.1) Auto-Hold Module provides the Hold action - Auto-Hold Module received feedback (or other input) that indicated that 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-4.1) Auto-Hold Module provides the Hold action - Auto-Hold Module received feedback (or other input) that indicated that vehicle is moving (LS-5.1) Auto-Hold Module provides the Hold action - Auto-Hold Module received feedback (or other input) that indicated that vehicle is moving (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-6.1) Auto-Hold Module provides the Hold action too early - Auto-Hold Module received feedback (or other input)	 (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-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-3.1) 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-3.1) Auto-Hold Module provides the Hold action - Auto-Hold Module provides the Hold action -			

