An STPA Centric Approach to Aerospace Certification

Dave Cummins, CEng, IntPE
Dr John Thomas, MIT

All Images - Public Domain / Stock



Regulations STPA could support

FOCUS OF THIS TALK

25.1309
Systems & Equipment

25.1302
Crew Error & Usability

25.1322
Alerting

ALSO APPLIES

25.1301 Function and installation
"Each item of installed equipment must be of a kind and design appropriate to its intended function"

OTHER POSSIBLE CANDIDATES

25.671 Control systems
Safe flight after failures, jams

25.672 Stability augmentation
Failure warning, safe control

25.1329 Flight guidance
Modes, disengagement, transients

25.1523 Minimum flight crew
Crew workload, ease of operation

25.703 Takeoff warning
Unsafe takeoff configuration

25.729(e) Gear warning
Landing with gear not locked down

25.901(c) Powerplant
Engines and APU must meet 25.1309

25.1585 Operating procedures
Normal, non-normal, emergency

25.1319 Security (proposed)
Unauthorized electronic access

Part 5 Safety management
Hazards and risk controls

SIMILAR RULES ELSEWHERE

FAA	23.2510, 27.1309, 29.1309, 33.75, 33.28(e), 35.15, PL.2510 (powered-lift)
EASA	CS 25.1309, CS 23.2510, CS 27.1309, CS 29.1309, CS-E 510, CS-P 150, SC-VTOL VTOL.2510
1301-style	23.2505, 27.1301, 29.1301, CS 25.1301

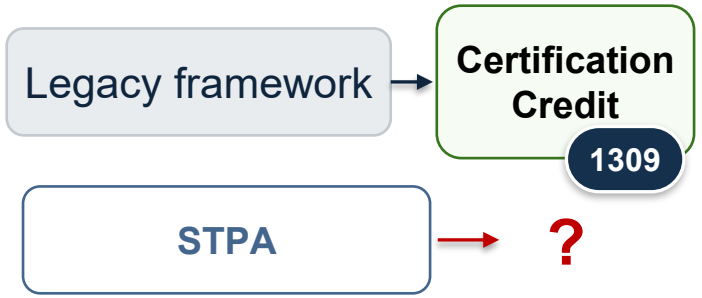
ARP4761 CITED ELSEWHERE

FAA	ACs 23.1309-1E, 27-1B, 29-2C, 33.28-3, 33.75-1A
EASA	AMC 25.1309, AMC 27.1309, AMC 29.1309, AMC E 510
Military	MIL-HDBK-516C/D airworthiness certification criteria

Not a complete list. Rule text from 14 CFR (as amended August 2024) and EASA Easy Access Rules. PL.2510 is from AC 21.17-4 (2025). 25.1319 is proposed: FAA NPRM, August 21, 2024 (FAA-2024-1398). Part 5 SMS applies to type and production certificate holders under the April 2024 final rule.

Different ways to use STPA

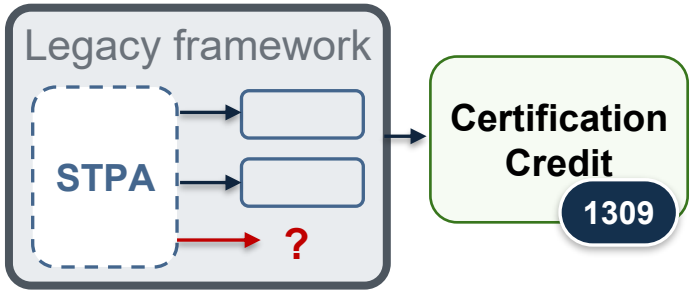
1 STPA on the side



Parallel approach
- STPA used alongside as an experiment
- STPA results not shared (voluntary)

Duplicated effort
No certification credit

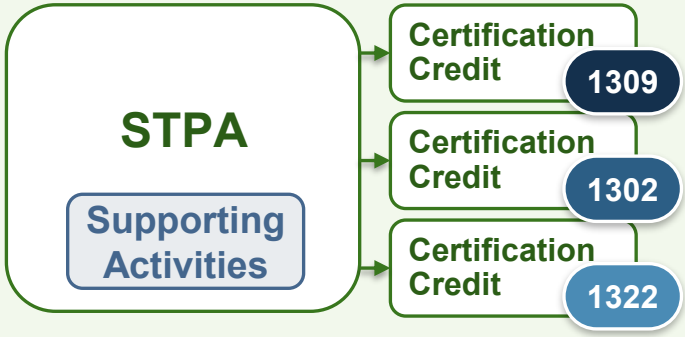
2 STPA inside legacy framework



STPA used as “secret sauce”
- Some results mapped to legacy outputs
- Some results have no home

STPA is helpful,
but used in a narrow way

3 STPA-Centric



STPA used directly
- A unified analysis: STPA
- Broader certification credit
- Some additions/extensions needed

Shared certification basis

The opportunity: lower cost and improved safety, from one analysis

What and why?

WHAT

STPA is a powerful hazard analysis method
Well suited to highly automated, software-intensive aircraft

We need to scale to new, more complex technologies
Technology is advancing, but certification hasn't. Certification gaps are known.

We need streamlined approach to satisfy existing regs
One multifaceted argument to satisfy 25.1309, 25.1302 and 25.1322

WHY

Modern hazards come from complex interactions
Includes control logic, automation behavior, and human-automation dynamics

STPA aligns well with performance-based rules
One approach can address 25.1309, 25.1302 and 25.1322

Performance-based rules are flexible
STPA results can be used directly in compliance matrix

EXAMPLES OF SAFETY CONCERNS TO ADDRESS

- Component failures and malfunctions
- Unsafe interactions between systems that all work as specified
- Automation behavior and control logic the crew did not expect
- How flight crew beliefs compare to actual system design

STPA: A unified analysis to address these and avoid gaps

Who would benefit?

Supplemental Type Certification (STC)

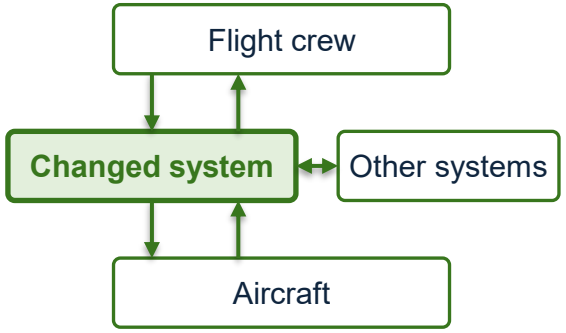
Changing an aircraft someone else designed

TRADITIONAL PATH



Rebuilt from scratch, even for small changes

STPA-CENTRIC PATH



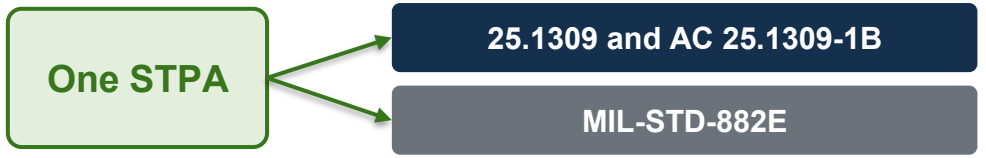
Start at the change

Follow each control loop it touches, out to the crew, other systems and the aircraft

A streamlined way to see everything a small change affects

Military programs

Hybrid 25.1309 and MIL-STD-882E requirements



Two safety processes today, each with its own severity terms and products. STPA could handle both together.

Part 25 OEMs

Large certification programs, with STPA run alongside



No certification credit for the STPA work, and the FAA does not see results that bear on safety

A traditional siloed approach

Systems & Equipment
14 CFR 25.1309



Failure conditions, probability budgets, redundancy

Crew Error & Usability
14 CFR 25.1302



Crew tasks, workload, error management

Alerting
14 CFR 25.1322



Alert detection, priority and format

FAA ADVISORY CIRCULAR

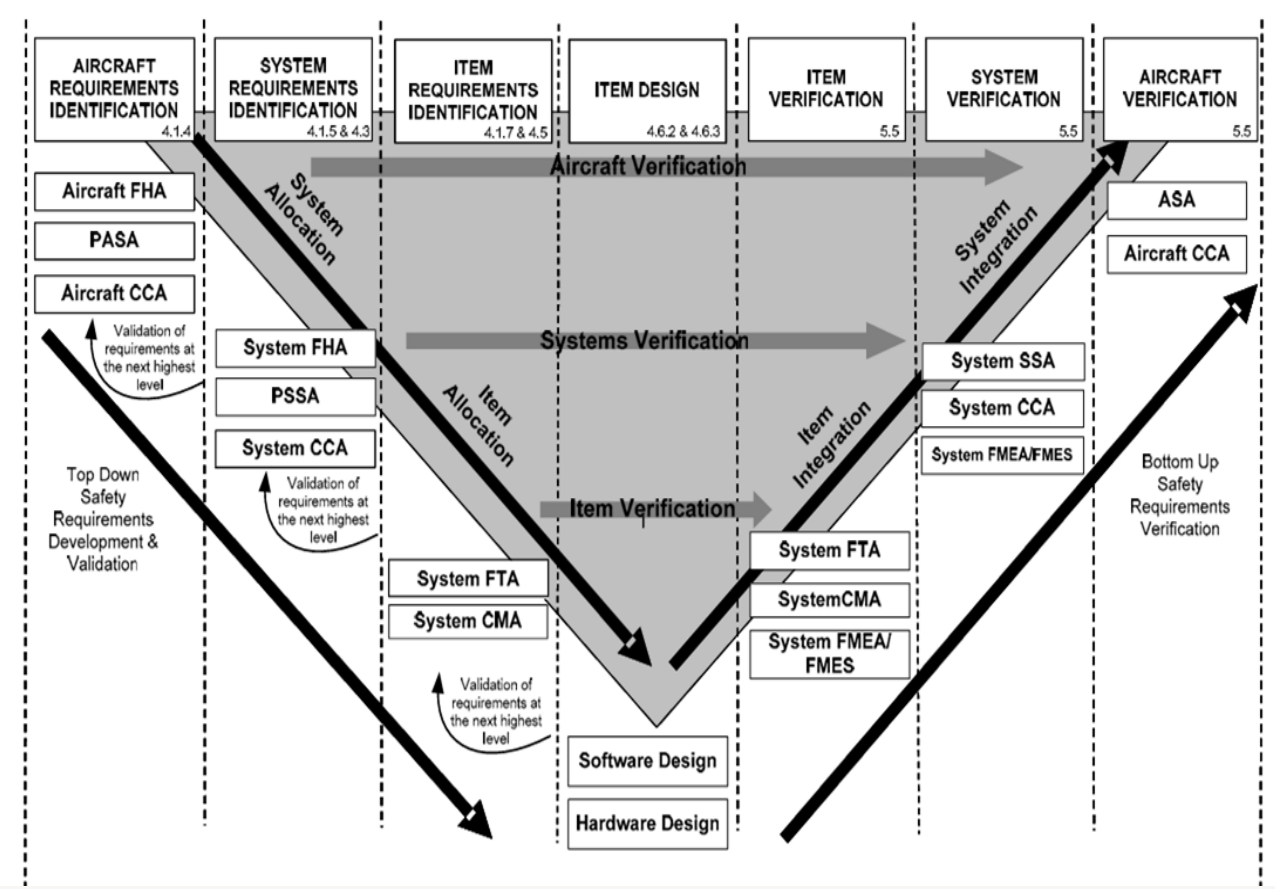
AC 25.1309-1B issued 2024	AC 25.1302-1 issued 2013	AC 25.1322-1 issued 2010

INDUSTRY RECOMMENDED PRACTICE

SAE ARP4761 SAE ARP4754	No end-to-end recommended practice*	No end-to-end recommended practice**

ARP7143, "Human Factors Recommended Practices for Showing Compliance to Regulation 25.1302", is in progress to fill this gap
**ARP4102/4 offers alerting design guidance, but no complete compliance process like ARP4754 and ARP4761*

How does the traditional MOC stack-up?



ARP4754A, Figure 5

MOC = Means of Compliance
FHA = Functional Hazard Assessment
PASA = Prelim Aircraft Safety Assessment
CCA = Common Cause Analysis
PSSA = Prelim System Safety Assessment
FTA = Fault Tree Analysis
CMA = Common Mode Analysis
FMEA = Failure Modes and Effects Analysis
FMES = Failure Modes and Effects Summary
SSA = System Safety Assessment
ASA = Aircraft Safety Assessment

ARP4761 is a common MOC for 25.1309 (Systems & Equipment)

- Looks at failure conditions: unintended function or functional loss
- Extensive, complex analysis
- Highly vulnerable to early assumptions, especially about human factors
- Bad assumptions surface late, forcing redesign or leaving a safety gap

...but at enormous effort

It does not satisfy 25.1302 (Crew Error & Usability)

- 25.1302 compliance treated as out of scope
- For known failures, identifies expected effect on flight crew
- Assumptions about crew are checked later, separately, and only for failures already found
- That check can invalidate failure conditions and derived requirements

It does not satisfy 25.1322 (Flight Crew Alerting)

- 25.1322 compliance treated as out of scope
- Monitoring requirements may be generated, but based on assumptions about expected crew response

Vulnerability example

Example of ARP4761 (Systems and Equipment)

Failure condition	Flight Phase	Failure Effects	Severity Classification	Remarks, Assumptions, and Rationale
Loss of control in yaw axis	All Phases	**Aircraft:** Significant reduction in safety margins due to inability to directly control yaw **Flight Crew:** Significant increase in workload to maintain safe control of aircraft using pitch and roll axis to compensate **Occupants:** May experience significant discomfort, possibly including injuries	MAJOR	We are assuming compensation in the pitch and roll axes is possible! It may not be in some conditions Can the flight crew reasonably compensate for this alongside their other duties? Is the workload increase manageable even if strenuous? Do the flight crew have a means to know, and therefore react immediately to a loss of yaw axis control?

Illustrative example of an early draft for review, not a finished worksheet

- ARP4761 asks for assumptions and rationale here, but thinking of them is left to the analyst
- Often builds the failure condition out of assumptions, bounding the engineering effort
- Validation usually comes later, which forces late re-design

How does STPA stack-up?

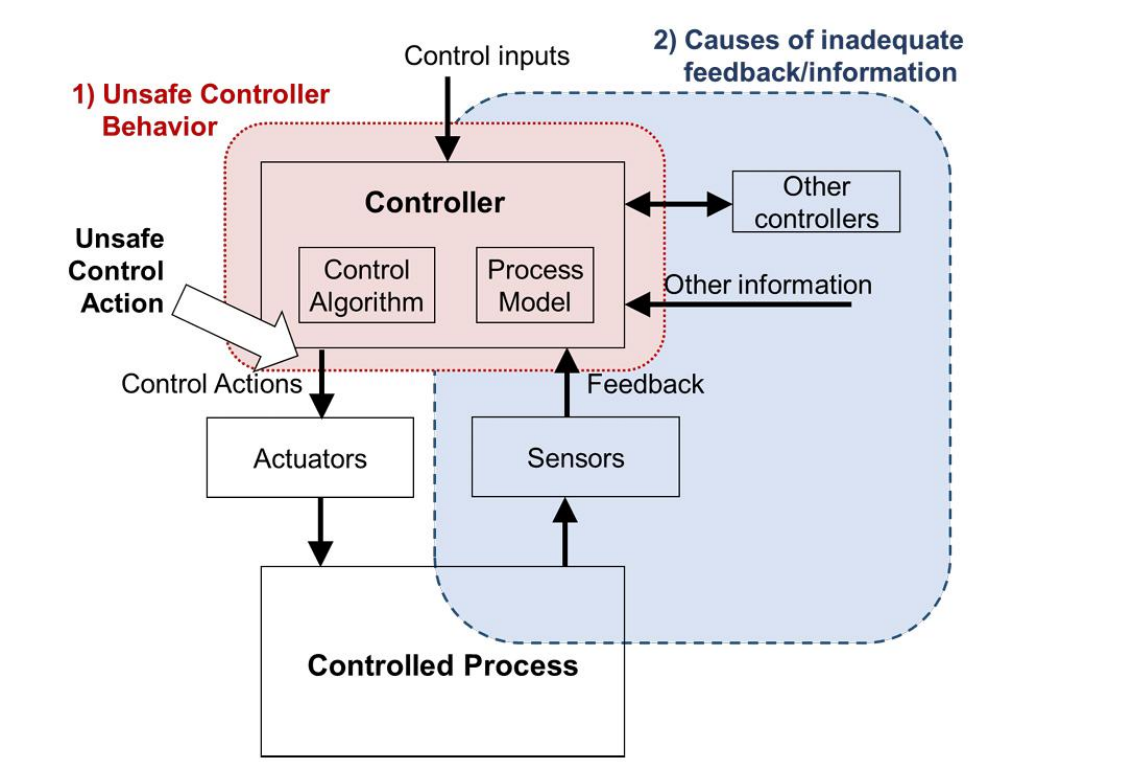


Figure: STPA Handbook 2018

STPA can support 25.1309 (Systems and Equipment)

- STPA directly supports most of 25.1309 already
- Shared goal to protect against the hazard
- Solutions to cover probability-related regulations are proposed

CHALLENGE

- **1309 has severity and probability requirements (risk)**
- **STPA has a different basis, no knowable probabilities**

STPA does support 25.1302 (Crew Error & Usability)

- STPA treats 25.1302 factors as in scope, as a core design consideration
- STPA uncovers hidden assumptions about human factors made elsewhere
- STPA identifies the crew tasks that the design will rely on

STPA does support 25.1322 (Flight Crew Alerting)

- Feedback is central to STPA's causal scenarios for a UCA
- Identifies which conditions need an alert (or other feedback)
- Analyzes information content, timing, contradictory information
- Analyzes crew's ability to respond to feedback given broader context of human decision-making
- Identifies scenarios that can be evaluated in a flight deck environment

Builds on prior work by Leveson, "Improving the Standard Risk Matrix: Part 1", MIT, 2019; Gregorian and Yoo, "A System-Theoretic Approach to Risk Analysis", MIT SM thesis, 2021; and MIL-STD-882E.

ARP4761 supplies risk-based info to 25.1309

PROCESS

ARP4761 PRODUCES

- Failure conditions
- A severity classification for each
- A probability of occurrence

PROBABILITY — FAILURE CONDITION SEVERITY

	Cata-strophic	Hazardous	Major	Minor
Probable				
Remote			✓	
Extremely Remote		✓		
Extremely Improbable	✓			

Acceptable Not acceptable ✓ Named in 25.1309

REGULATION

25.1309 REQUIRES

- Severity → Probability relationship
- Catastrophic failure conditions → extremely improbable
- No catastrophic failure condition from a single failure
- These probabilities are **qualitative** in the regulation*

ARP4761 produces severity and probability values
That's one approach to satisfy this Regulation

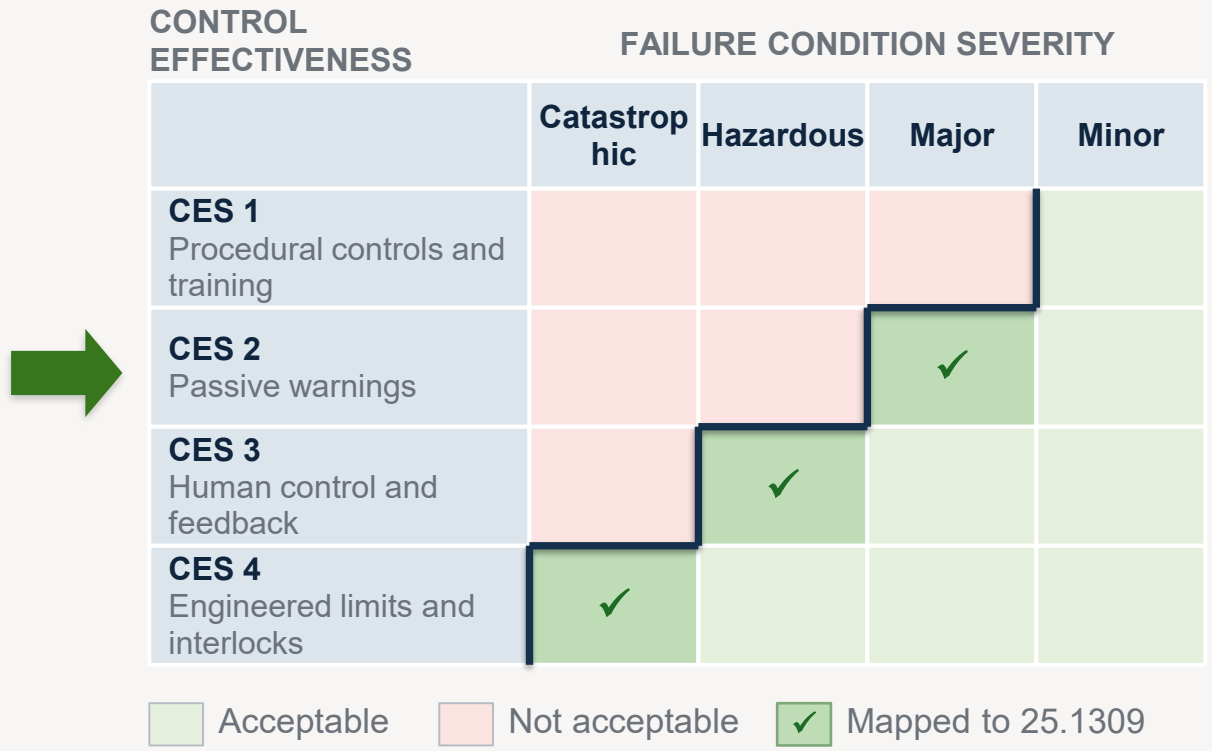
**AC 25.1309-1B:*
- *Provides quantitative probability limits, but uses language "on the order of" and as "aids to engineering judgement".*
- *Has disclaimer: "describes acceptable means, but not the only means, for showing compliance"*

CFR 25.1309 has only one number: 1/1000, the limit on latent failure probability when two failures together are catastrophic.

Solution: Use control effectiveness

STPA PRODUCES

- Losses and hazards
- Unsafe control actions
- Causal scenarios for each UCA
- The controls that answer them



25.1309 REQUIRES

- Severity → Probability relationship
- Catastrophic failure conditions → extremely improbable
- No catastrophic failure condition from a single failure
- These probabilities are **qualitative** in the regulation

STPA → CES → 1309 Requirements

Based on prior work by Leveson, "Improving the Standard Risk Matrix: Part 1", MIT, 2019;
Gregorian and Yoo, "A System-Theoretic Approach to Risk Analysis", MIT SM thesis, 2021; and MIL-STD-882E.
This is a proposed mapping (needs FAA agreement)
Still required: Other 1309 rules, like single-failure and independence rules

Using STPA results for certification credit

Use AC 25.1309-1B severity classes inside a MIL-STD-882E risk framework
Aligned with 882E risk reduction precedence criteria.

Loss	Severity	Required CES
L1: Loss of life (2+)	CATASTROPHIC	CES4
L2: Loss of aircraft	CATASTROPHIC	CES4
L3: Serious injury	HAZARDOUS	CES3
L4: Physical distress to occupants	MAJOR	CES2
L5: Loss of cargo / mission*	[beyond 1309]	CES1

STPA already provides full traceability to hazards & losses.

The 25.1309 severity and likelihood objectives can be met with a CES requirement from STPA.

Hazard Likelihood	CES	Hazard Severity				
		(1) Catastrophic	(2) Hazardous	(3) Major	(4) Minor	(5) No Safety Effect
[A] Frequent	CES0	1A - HIGH	2A - HIGH	3A - SERIOUS	4A - MEDIUM	Eliminated
[B] Probable	CES1	1B - HIGH	2B - HIGH	3B - SERIOUS	4B - MEDIUM	
[C] Remote	CES2	1C - HIGH	2C - SERIOUS	3C - MEDIUM	4C - LOW	
[D] Ext. Remote	CES3	1D - SERIOUS	2D - MEDIUM	3D - MEDIUM	4D - LOW	
[E] Ext. Improbable	CES4	1E - MEDIUM	2E - MEDIUM	3E - MEDIUM	4E - LOW	
[F] Eliminated	CES5	Eliminated				

CES	Risk Reduction Control Type	Examples
CES5	Eliminate risk	Architecture removes every causal scenario for the UCA
CES4	Engineered limits and interlocks	Interlocks, limits on when a function can act, automatic shutdown or override
CES3	Human control and feedback	Alerts and annunciations sensed from the process, ability to take over effectively and in time
CES2	Passive warnings	Placards, signage, cautionary notes about hazards
CES1	Procedural controls and training	Manuals, procedures, checklists, and training
CES0	No controls	Do nothing

Proposed mapping (needs FAA agreement)
The controls still need to be reliable enough for its score
**Additional losses like L5 can optionally be included in same analysis, though out of scope for 1309*

Control effectiveness?

What?

Control Effectiveness Score (CES) is a means to measure how well a safety control prevents or mitigates Unsafe Control Actions (UCAs), and therefore Hazards and Losses

Is there pedigree to this?

Yes, in MIL-STD-882E we use the term ‘residual risk’ to illustrate the risk after controls are applied, explicitly taking credit for how effective the controls are at reducing hazard severity or likelihood

How would we measure whether we have the right CES?

Just like any approach, it depends on the consequences of loss and therefore the severity of your hazards, should they be realized

Should this always be used instead of probability?

Where probability cannot be used (non-failure scenarios), CES could be set by severity, standing in for the AC25.1309-1B likelihood terms. E.g., CES 4 for Extremely Improbable, etc.

Could also be used to complement probability where probability is viable, such as a well-known failure in a causal scenario

Hazard	Risk before new controls	Risk Objective	Controls	Risk after new controls	Status
H1: Aircraft lands uncontrolled	**1-D SERIOUS**	**1E-MEDIUM**	Req 1: CES 4 Req 2: CES 3	**1E-MEDIUM**	PASS

Risk reduction from this

To this

Is achieved by controls of a defined effectiveness score

Concept of control effectiveness from Leveson, "Improving the Standard Risk Matrix: Part 1", MIT, 2019; Gregorian and Yoo, "A System-Theoretic Approach to Risk Analysis", MIT SM thesis, 2021; and MIL-STD-882E.

Assigning Severity

Assign severity here?

Loss	Severity	Required CES
L1: Loss of life	CATASTROPHIC	4

AC 25.1309-1B: “A failure condition that would prevent continued safe flight and landing should be classified as catastrophic...”

In general, usually considered CATASTROPHIC

Hazard	Loss Link	Severity	Required CES
H1: Aircraft lands uncontrolled	L1: Loss of life	CATASTROPHIC	4

AC 25.1309-1B HAZARDOUS:

- “Serious or fatal injuries to a relatively small number of persons other than the flightcrew”
- “A large reduction in safety margins or functional capabilities”

Gear-up landing on runway is usually considered HAZARDOUS

UCA	Hazard Link	Severity	Required CES
U1: Flight crew lands when the gear is not down and locked	H1: Aircraft lands uncontrolled	CATASTROPHIC	4

An interlock is not always possible

UCA	Scenario	Identified Design Flaws	Requirement	Requirement Type	CES Credit
U1	X	Y	Z	Interlock	4
U1	X	Y	Z	Feedback	3

When UCAs provide more detail & context, can severity change?

Assigning severity

Potential sub-hazards:
- H1.1: Aircraft lands on runway with gear up
- H1.2: Aircraft lands outside a runway

Could sub-hazards have different severities?

Loss	Severity	Required CES
L1: Loss of life	CATASTROPHIC	4

Hazard	Loss Link	Severity	Required CES
H1: Aircraft lands uncontrolled	L1: Loss of life	CATASTROPHIC	4

UCA	Hazard Link	Severity	Required CES
U1: Flight crew lands when the gear is not down and locked	H1: Aircraft lands uncontrolled	CATASTROPHIC	4

An interlock is not always possible

UCA	Scenario	Identified Design Flaws	Requirement	Requirement Type	CES Credit
U1	X	Y	Z	Interlock	4
U1	X	Y	Z	Feedback	3

Note: 25.1309 common practice uses alleviating factors, such as backup systems or crew action, to lower severity

Assigning severity

Assign severity here?

Loss	Severity	Required CES
L1: Loss of life	CATASTROPHIC	4

Loss to Hazard

Does Severity ever change here?

Hazard	Loss Link	Severity	Required CES
H1: Aircraft lands uncontrolled	L1: Loss of life	CATASTROPHIC	4

Hazard to UCA

Does Severity ever change here?

UCA	Hazard Link	Severity	Required CES
U1: Flight crew lands when the gear is not down and locked	H1: Aircraft lands uncontrolled	CATASTROPHIC	4

UCA to causal scenarios

Does Severity ever change here?

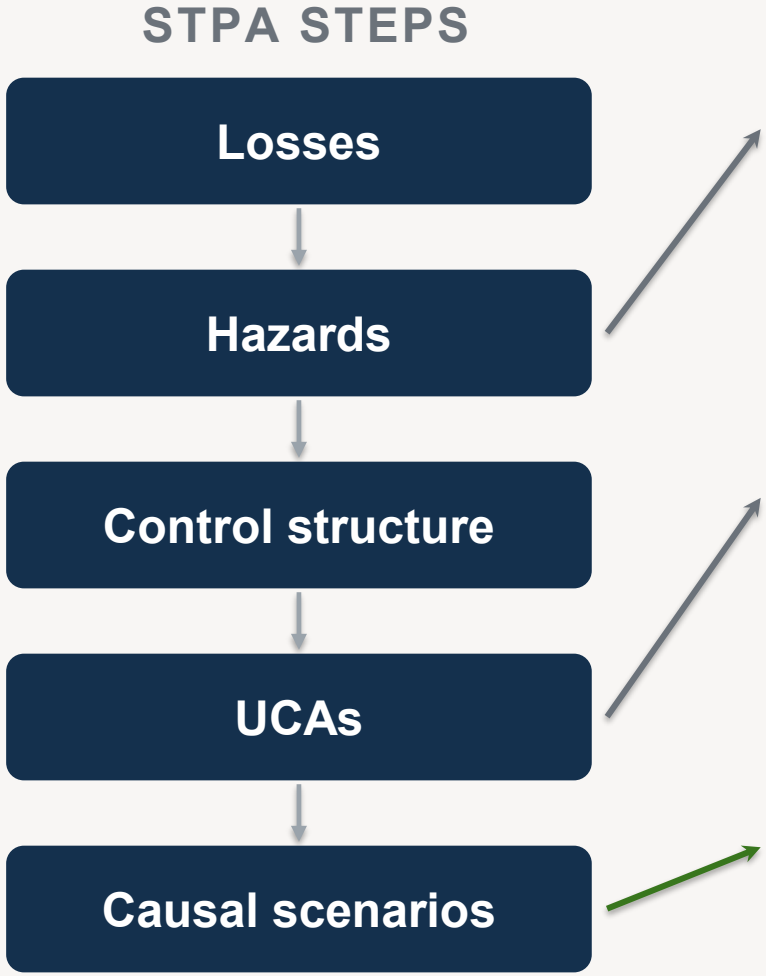
An interlock is not always possible

UCA	Scenario	Identified Design Flaws	Requirement	Requirement Type	CES Credit
U1	X	Y	Z	Interlock	4
U1	X	Y	Z	Feedback	3

How would you apportion a high UCA CES across its causal scenarios?

Note: 25.1309 common practice uses alleviating factors, such as backup systems or crew action, to lower severity

Where to assign Severity & CES requirements?



Potential options:

1 Add sub-hazards, some with lower severity

The MIL-STD-882E move: tag the UCAs to lower-level child hazards.

- × Inserts a middle-man between UCAs and hazards
- × Rests on assumptions that are vulnerable to being invalid
- × Somewhat decompositional approach

2 Develop lower-level UCAs

The reductionist view: split the unsafe interaction into constituent parts.

- × Same middle-man, one level down
- × Same reliance on assumptions
- × Somewhat of a decomposition approach

3 Refine the causal scenarios

LET'S TRY THIS

The natural place to show detailed causes and requirements.

- ✓ No middle-man, so the STPA model stays intact
- ✓ Keeps the initial CES scoring
- ✓ Assigns the score when the causes are identified / known

Still needs a systematic rule for allocating the CES

CS = causal scenario, the specific ways a UCA can come about. CES = control effectiveness score.

Example: Assigning CES requirements

2 DECISION MAKING

If flaps are set, it is safe to take off

TASKS THE DESIGN MUST SUPPORT

- CES 1 — Confirm flap lever and gauge before takeoff
- CES 1 — Cross-check flaps against the takeoff data
- CES 1 — Reject the takeoff if the warning sounds

1 UNSAFE CONTROL ACTION

Flight crew starts takeoff when the flaps and slats are not set

NEEDS CES 4

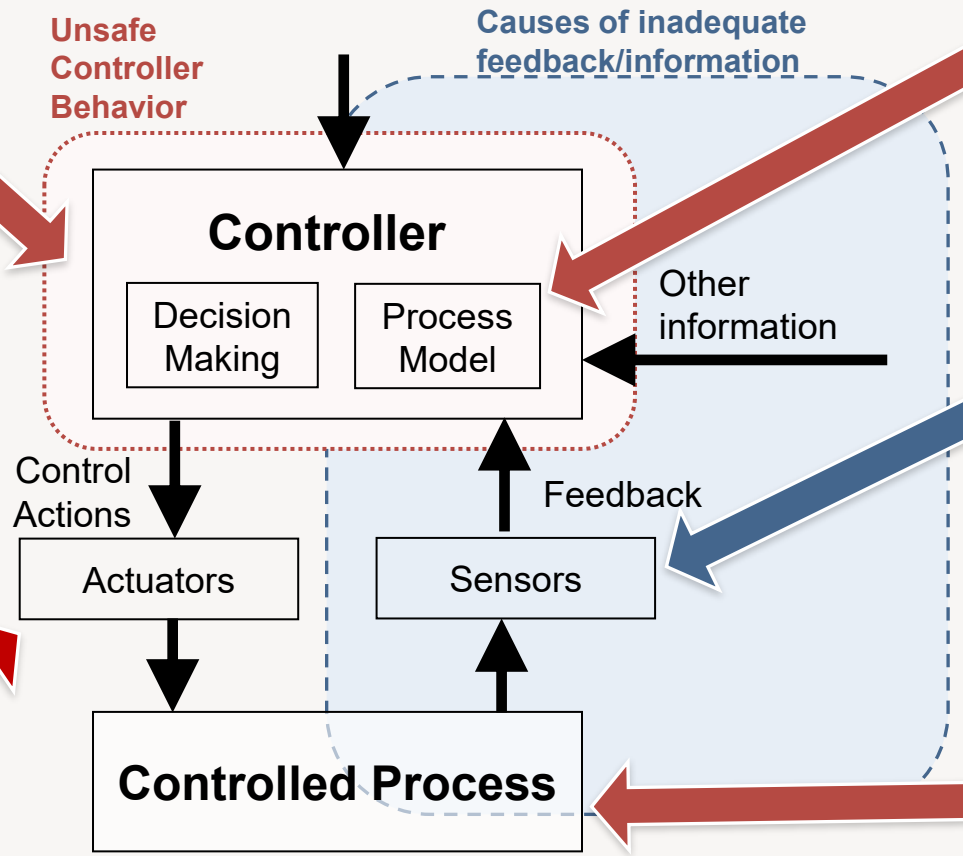


Figure: STPA Handbook 2018

3 PROCESS MODEL

Flight crew believes the flaps and slats are set for takeoff

FEEDBACK TO CREW

- CES 3 — Flap setting is shown with the takeoff speeds
- CES 3 — Aural and visual warning if thrust set without takeoff flaps
- CES 3 — Takeoff warning not driven by single air/ground relay

4 CONTROLLED PROCESS

Flaps and slats stay retracted, as last commanded
OR: Flaps and slats do not extend due to failure

The UCA needs CES 4. Can multiple mitigations combine to increase total protection against the UCA?
Only if they don't share a cause: some of these do!

Multiple regulations covered

2 DECISION MAKING

If flaps are set, it is safe to take off

TASKS THE DESIGN MUST SUPPORT

- 25.1302 — Confirm flap lever and gauge before takeoff
- 25.1302 — Cross-check flaps against the takeoff data
- 25.1302 — Reject the takeoff if the warning sounds

1 UNSAFE CONTROL ACTION

Flight crew starts takeoff when the flaps and slats are not set

NEEDS CES 4

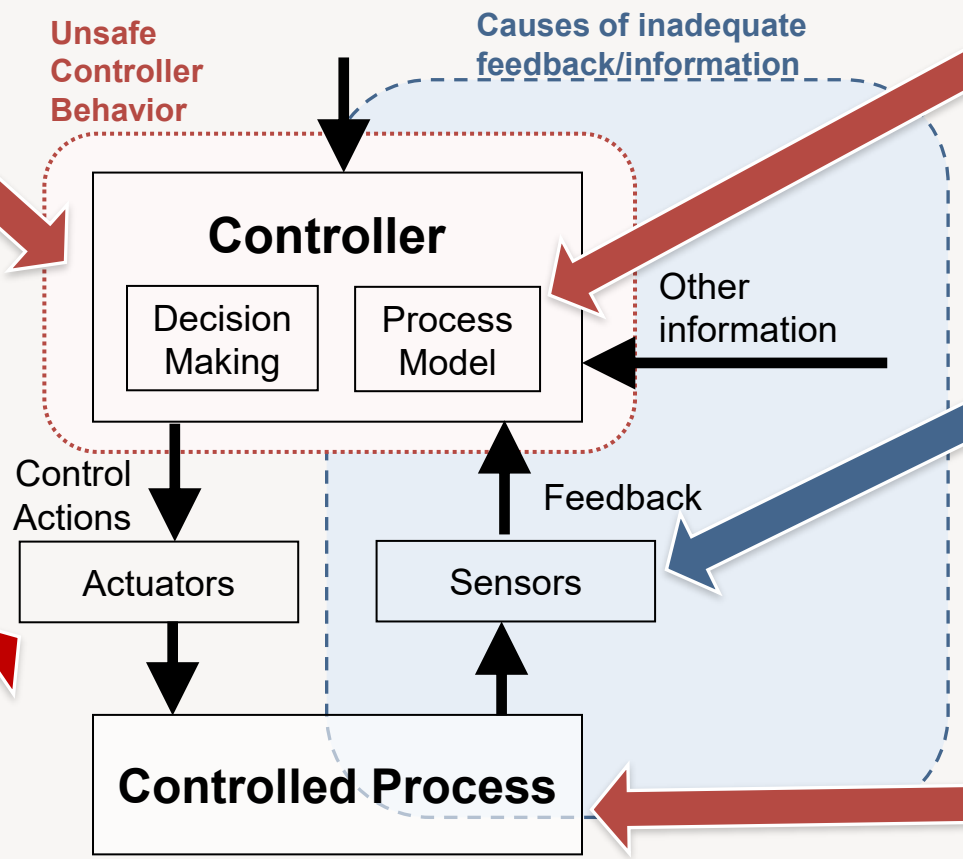


Figure: STPA Handbook 2018

3 PROCESS MODEL

Flight crew believes the flaps and slats are set for takeoff

FEEDBACK TO CREW

- 25.1302 — Flap setting is shown with the takeoff speeds
- 25.1322 — Aural and visual warning if thrust set without takeoff flaps
- 25.1309 — Takeoff warning not driven by single air/ground relay

4 CONTROLLED PROCESS

Flaps and slats stay retracted, as last commanded
OR: Flaps and slats do not extend due to failure

25.1302 25.1309

25.1309 Safety Assessment
Takeoff warning faults flagged before the next flight

25.1302 Crew Error & Usability
The crew can confirm the flap setting and act on it

25.1322 Alerting
Aural and visual takeoff configuration warning when thrust is set

Ideas on human CES decomposition principles

3 Refine the causal scenarios

Emphasis on CES stacking in the feedback loop

A Seek independent feedback

The confidence booster for situation awareness

- ✓ Provide multi-source, multi-haptic, high-integrity feedback
- ✓ Prevent single-strand decision making
- ✓ Seek alignment to procedure that fits the safe PM

Confidence in the correct (safe) process model

B Measure feedback quality

Feedback aligned with the safe PM and intended DM

- ✓ Provide timely feedback that supports right action, right time – align with safe PM
- ✓ Avoid misinformation or nuisance feedback
- ✓ Evaluate alignment to procedure

Enhance correct human control action via high-quality feedback

C Don't rely on procedure alone

Feedback that is directly aligned with high-quality procedure

- ✓ Don't rely on a correct response by chance
- ✓ Focus on high-quality procedure aligned to feedback
- ✓ Don't stack procedure and workload

Augment procedure with useful feedback

CES = control effectiveness score
DM = decision making (the controller's decision model e.g., "if X then do Y")
PM = process model (the controller's beliefs informed by feedback training)

How could this work as a process?

Traditional assessment	Traditional approach
Preliminary Aircraft Safety Assessment (PASA)	• Review aircraft-level failure conditions • Identify aircraft-level causes of failure conditions • Define safety objectives, probability budgets • Requirements for allocation to systems
Preliminary System Safety Assessment (PSSA)	• Same as PASA, but at system level
System Safety Assessment (SSA)	• Verify the system-level safety requirements
Aircraft Safety Assessment (ASA)	• Verify the aircraft-level safety requirements

New approach

Preliminary Aircraft-level STPA

- Informs aircraft design
- Informs flight-deck design and crew tasks
- Informs which alerts are needed

25.1309 25.1302 25.1322

Preliminary System-level STPA

- Informs system design
- Informs crew tasks and information
- Informs system-level alerting

25.1309 25.1302 25.1322

STPA-based System Safety Assessment

- Verify safety requirements from System-level STPA
- Confirms the control effectiveness score of each

STPA-based Aircraft Safety Assessment

- Verify safety constraints from the Aircraft-level STPA
- Confirms residual risk is acceptable aircraft-wide

STPA as a unifying approach supporting multiple regulations

How could this work as a process?

STPA ANALYSIS

New Process	STPA Basis
Preliminary Aircraft-level STPA (PASA)	• Losses • Hazards • System-level constraints • Control structure • Unsafe control actions • Controller constraints
Preliminary System-level STPA (PSSA)	• UCA causal scenarios • Safety requirements • Requirements validation
System Safety Assessment (SSA)	• Verify the safety requirements from the STPA PSSA
Aircraft Safety assessment (ASA)	• Verify the safety constraints from the STPA PASA

Supporting activities

Certification Credit
Systems & Equipment
14 CFR 25.1309

Certification Credit
Crew Error & Usability
14 CFR 25.1302

Certification Credit
Alerting
14 CFR 25.1322



Thank you!

We have a lot more we could have presented on this subject with more time. While a future talk in a dedicated format to this subject will likely provide that forum, if you found this talk interesting, have feedback, or suggestions, please reach out to us and share your comments!

- Jthomas4@mit.edu
- David.cummins2@baesystems.us