System Theoretic Process Analysis (STPA) in Medical Systems Risk Management

Mark A Vernacchia, Principal and Co-Founder - SSE Group, LLC
INCOSE Expert Systems Engineering Professional (ESEP)
Chair - SAE STPA Task Force

Presentation Outline

What is System Safety?

What is Risk and How to Find Risk?

Risk Analysis Process and Techniques

How Can We Improve Our Approach?

System Theoretic Process Analysis (STPA) Overview

How to Manage Risk and How STPA Supports that Effort

Automated External Defibrillator (AED) - STPA Example

Summary of How STPA Supports Risk Management Process

First STPA Standard for All Industries – SAE J3307_202503

STPA Recommended Practices for All Industries – SAE J3187_202305

What is System Safety?

System Safety is a specialty within systems engineering that supports program risk management. It is the application of engineering and management principles to optimize safety.

MIL-STD-882E [1]

- The application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system life-cycle

FAA Systems Safety Handbook [5]

- The application of engineering and management principles, criteria, and techniques to optimize safety within constraints of operational effectiveness, time, & cost throughout all phases of system life cycle

What is RISK?

Risk – Basic Definition

- A situation involving exposure to danger, harm, or loss, where the level of risk reflects the likelihood of the unwanted event and the potential consequences of the unwanted event

ARP-4761 [6]

- The combination of frequency (probability) of an occurrence and its associated level of severity (“Probability” implies quantitative)

ISO-26262 [4]

- Combination of the severity, the likelihood of occurrence of a hazard, and potential controllability of hazard that could potentially lead to harm (“Likelihood” implies qualitative – being in a certain operating condition)

What is RISK?

NASA System Safety Handbook [7]

- Risk is characterized by a set of triplets:
  - the scenario(s) leading to degraded performance in one or more performance measures
  - the likelihood(s) of those scenarios, and
  - the consequence(s) of impact on performance that would result if those scenarios occur

FAA System Safety Handbook [5]

- Risk is an expression of possible loss over a specific period of time or number of operational cycles. It may be indicated by the probability of an accident times the damage in dollars, lives, and / or operating units. Hazard Probability and Severity are measurable and, when combined, give us risk. Total risk is the sum of identified and unidentified risks.

Risk Analysis Process - ISO/TR 24971:2020 [9]

5.1 *Risk analysis process*

The *risk analysis process* consists of the following steps, which are explained in further detail in the next subclauses:

- description of the *intended use* of the *medical device* and *reasonably foreseeable misuse*;
- identification of the characteristics of the *medical device* that are related to *safety*;
- identification of *hazards* and *hazardous situations* associated with the *medical device*;
- estimation of *risks* for each *hazardous situation*.

Familiar Techniques that Support Risk Analysis

- Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) are useful in safety engineering, early in the development process. FTAs are primarily used as means for analyzing the causes of hazards, not identifying hazards.[10] ETAs are a general decision tree formulation to break up large complex systems into smaller parts to which FTA could be applied.[10]
- Failure Mode and Effects Analysis (FMEA) is a technique by which effects or consequences of individual components failures are systematically identified and is more appropriate as design matures and failure modes are better understood
- Both techniques typically focus on failure-based losses

How Can We Improve Our Approach?

- As systems become increasing complex we should explore additional analysis techniques in addition to those existing methodologies we have been using
- An option is System Theoretic Process Analysis (STPA) that leverages a “control loop” approach
- STPA is not a replacement for FMEAs or FTAs
- It is a complementary approach allowing evaluation of system element interactions (e.g., system has not failed but still produces unwanted behaviors)

Overview of System Safety Engineering [12]

1920 1940 1950 1960 1970 1980 1990 2000 2010 2020 ???

Reduce human errors

FMEA

FTA HAZOP ETA

STPA

➢ Mechanical systems

➢ Electro-mechanical systems

➢ Introduction of computer controls
➢ Exponential increases in complexity
➢ New technologies
➢ Changes in human roles

Assume accidents caused by **human errors**

Assume accidents caused by **component failures, component reliability** problems, and **human errors**

Leveson, 2017)

Component Interaction Losses Techniques [11]

Harm may be caused by **interactions** between components

- May not involve any component failures
- May be caused when all components operate exactly as designed or specified
  - But the design may be wrong
  - Requirements may be flawed
  - Assumptions about context / environment are incorrect or overlooked
- Related to complexity
  - Becoming increasingly common in complex systems
  - Complexity of interactions leads to unexpected system behavior
    - (e.g., Emergent Behavior)
  - Difficult to anticipate unsafe interactions
- Especially problematic for software

Hazard Analysis Methodologies Comparison

FMEA

Start with the known causes

Inductive Reasoning → Possible effects

Possible causes ← **Deductive Reasoning**

FTA

Start with the known effects

Possible causes ← **Exploratory Reasoning**

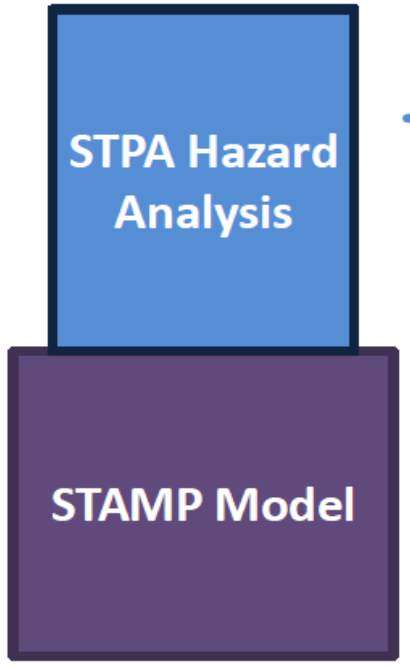
Interactions between elements

Exploratory Reasoning → Possible effects

STPA

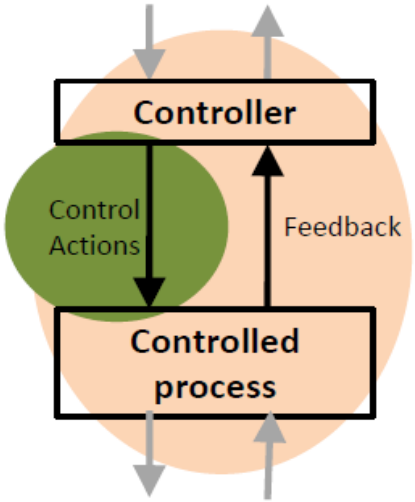
System-Theoretic Process Analysis (STPA) Overview [3]

STPA
(System-Theoretic Process Analysis)



Systems Theoretic Accident Model and Process
(Leveson, 2012)

- System engineering foundation
  - Define accidents, hazards, constraints
  - Control structure
- Identify Unsafe Control Actions
- Identify Causal Scenarios



11
1

STPA views system from a "controls-based" perspective using control loops

STPA incorporates human/operators as part of control system

STPA assesses where unwanted system behaviors occur due to poor system design when nothing has failed

How to Approach a STPA Hazard Evaluation

Key steps associated with a useful and effective system safety approach may be described as follows:

- Define what “losses” or harm you are concerned with
- Identify what hazards (hazardous conditions) could lead to losses
- Evaluate how functional aspects of system elements might behave, or misbehave, leading to unwanted behaviors that lead to hazards
- Determine causes or reasons allowing unwanted behaviors to occur
- Define appropriate requirements to prevent or manage causes or reasons that would allow unwanted behaviors to occur

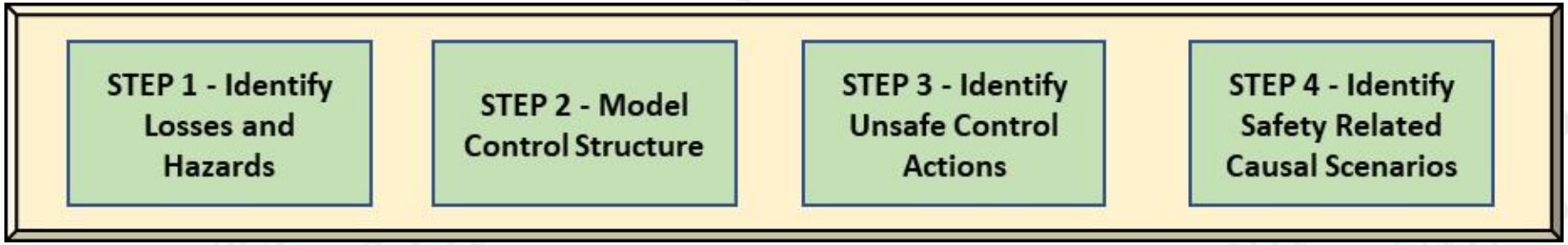
STPA Major Steps

Step 1 – Identify Losses and Hazards

Step 2 – Model Control Structure

Step 3 – Identify Unsafe Control Actions

Step 4 – Identify Safety Related Causal Scenarios



Use STPA results to generate safety requirements to prevent or manage related causal scenarios (causes)

How STPA Supports STPA Risk Management

- Risk (Basic Definition) - A situation involving exposure to danger, harm, or loss, where level of risk reflects the likelihood of the unwanted event and potential consequences of the unwanted event
- Risk Management is a disciplined approach to dealing with the uncertainty that is present throughout the entire system life cycle
- Issue is: "How to identify 'Risk' in the system of interest"
- STPA can identify safety-related risk as:
  - It identifies losses (harm) and hazardous conditions where losses may occur early in the process when the design is still being developed
  - It determines which control actions lead to hazardous conditions (UCAs)
- STPA can develop safety-related requirements to prevent/manage risk
  - It identifies why unsafe control actions (UCAs) occur
  - It identifies why control actions may not be executed or executed improperly

STPA Applied to Automatic External Defibrillator (AED) [8]

An AED . . .

- helps people who have a sudden cardiac arrest, which occurs when the heart suddenly stops beating regularly
- detects an abnormal rhythm
- delivers an electric shock through the chest to the heart

(American Heart Association, 2023)

Common Steps to Operate AEDs

- Power ON the AED
- Attach electrode pads
- Analyze the rhythm
- Clear victim and press SHOCK button

(American Heart Association, 2000)

STPA Step 1 – Identify Losses (Harm) and Hazards [8]

- Traceability

Number	Losses
L1	Loss of life
L2	Injury to patient, rescuers or bystanders
L3	Unsuccessful resuscitation
L4	Damage to equipment

Hazard Number	Hazards	Relationship to Losses
H1	Unintended exposure of human to electrical energy	L1 and L2
H2	Exposure of human to thermal or combustion events/energy	L1, L2, and L3
H3	Patient does not receive effective defibrillation, chest compression (or rescue breathing)	L3
H4	Exposure of equipment to forces, energies, or conditions that are beyond designed tolerances	L4

STPA Step 1 – Identify Losses (Harm) and Hazards [8]

- Traceability
- Analysis scoping
  - L4, H4 omitted for this work

Number	Losses	Hazard Number	Hazards	Relationship to Losses
L1	Loss of life	H1	Unintended exposure of human to electrical energy	L1 and L2
L2	Injury to patient, rescuers or bystanders	H2	Exposure of human to thermal or combustion events/energy	L1, L2, and L3
L3	Unsuccessful resuscitation	H3	Patient does not receive effective defibrillation, chest compression (or rescue breathing)	L3
L4	Damage to equipment	H4	Exposure of equipment to forces, energies, or conditions that are beyond designed tolerances	L4

STPA Step 1 – Identify Losses (Harm) and Hazards [8]

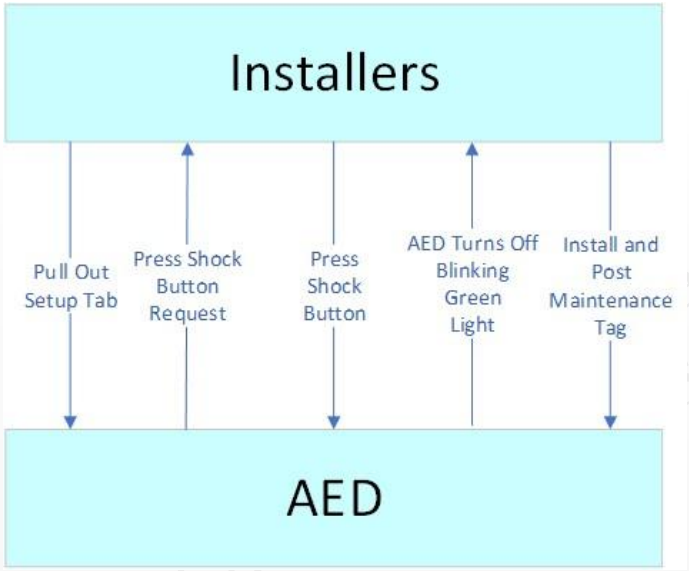
- Traceability
- Analysis scoping
  - L4, H4 omitted for this work
- Constraints - Keeping them at the system (vs. component) level

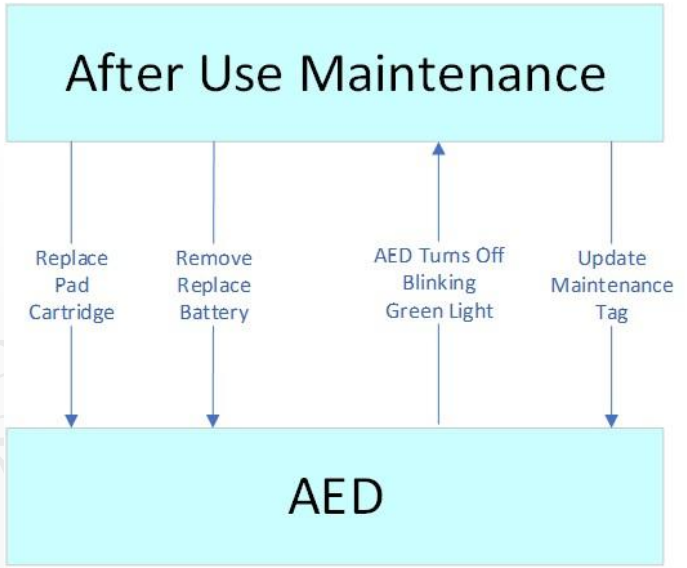
Number	Losses	Hazard Number	Hazards	Relationship to Losses	Constraint Number	Constraints
L1	Loss of life	H1	Unintended exposure of human to electrical energy	L1 and L2	SC1	The AED shall protect humans from unintended exposure to electrical energy
L2	Injury to patient, rescuers or bystanders	H2	Exposure of human to thermal or combustion events/energy	L1, L2, and L3	SC2	The AED shall protect humans from exposure to thermal energy
L3	Unsuccessful resuscitation	H3	Patient does not receive effective defibrillation, chest compression (or rescue breathing)	L3	SC3-1	The AED shall provide effective defibrillation when operated
					SC3-2	The Rescuer shall provide effective chest compressions and/or rescue breathing when required

STPA Step 2 – Model Control Structure [8]

A comprehensive analysis considers multiple aspects and perspectives

- Initial Installation, Using AED, and Post-Use Maintenance



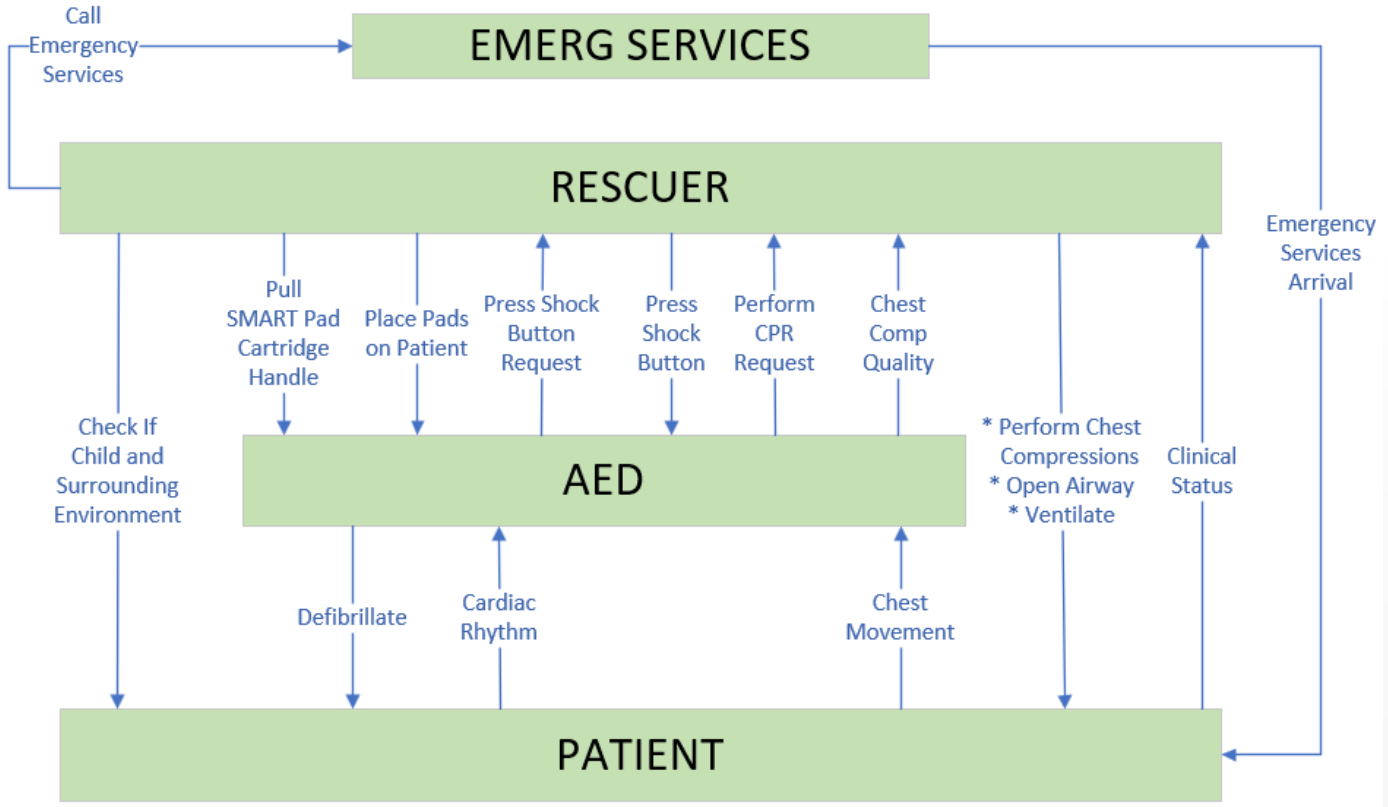


STPA Step 2 – Model Control Structure [8]

A comprehensive analysis considers multiple aspects and perspectives

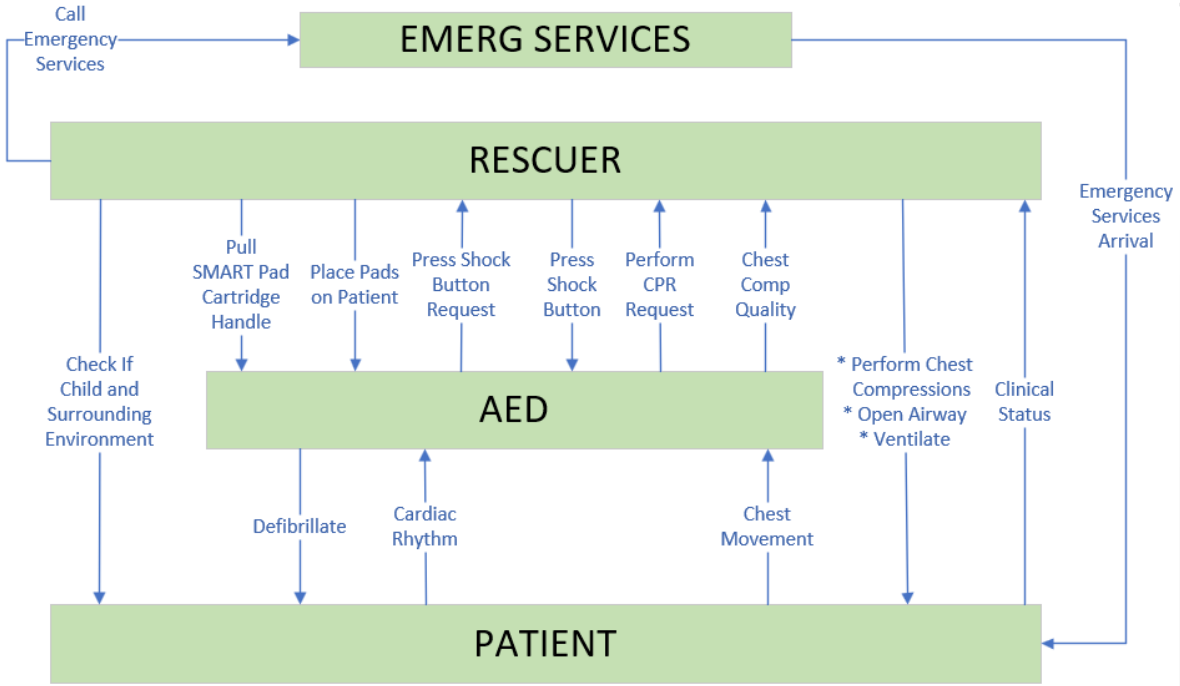
- Initial Installation, Using AED, and Post-Use Maintenance
- Selected Rescuer, AED, and Patient perspective as it has more interactions to consider

"Rescuer" as a "controller"



STPA Step 2 – Model Control Structure (CS) [8]

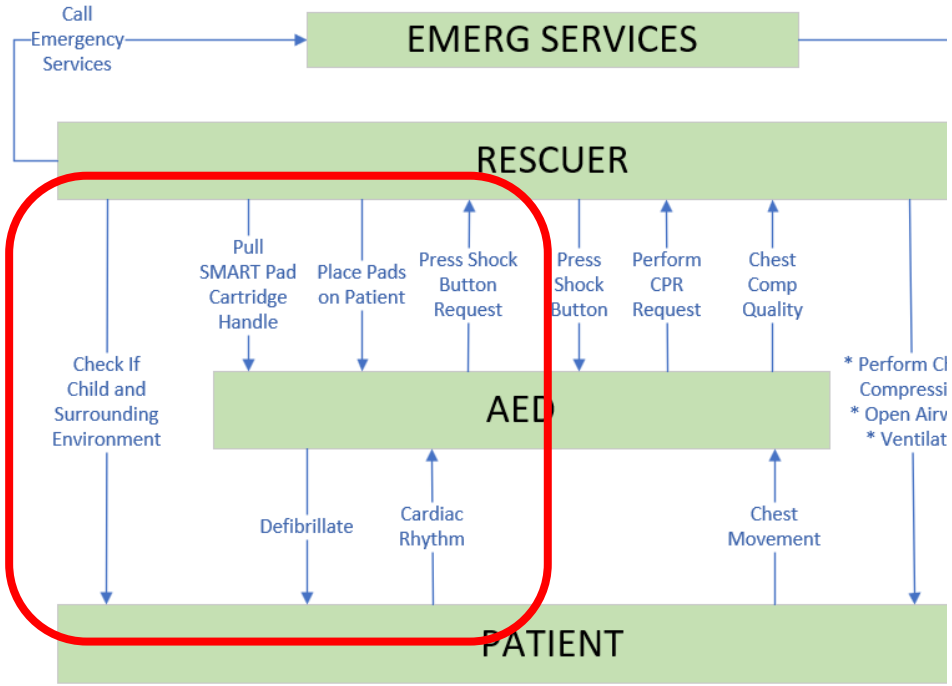
CS evolved by understanding of actual uses and STAMP diagramming conventions

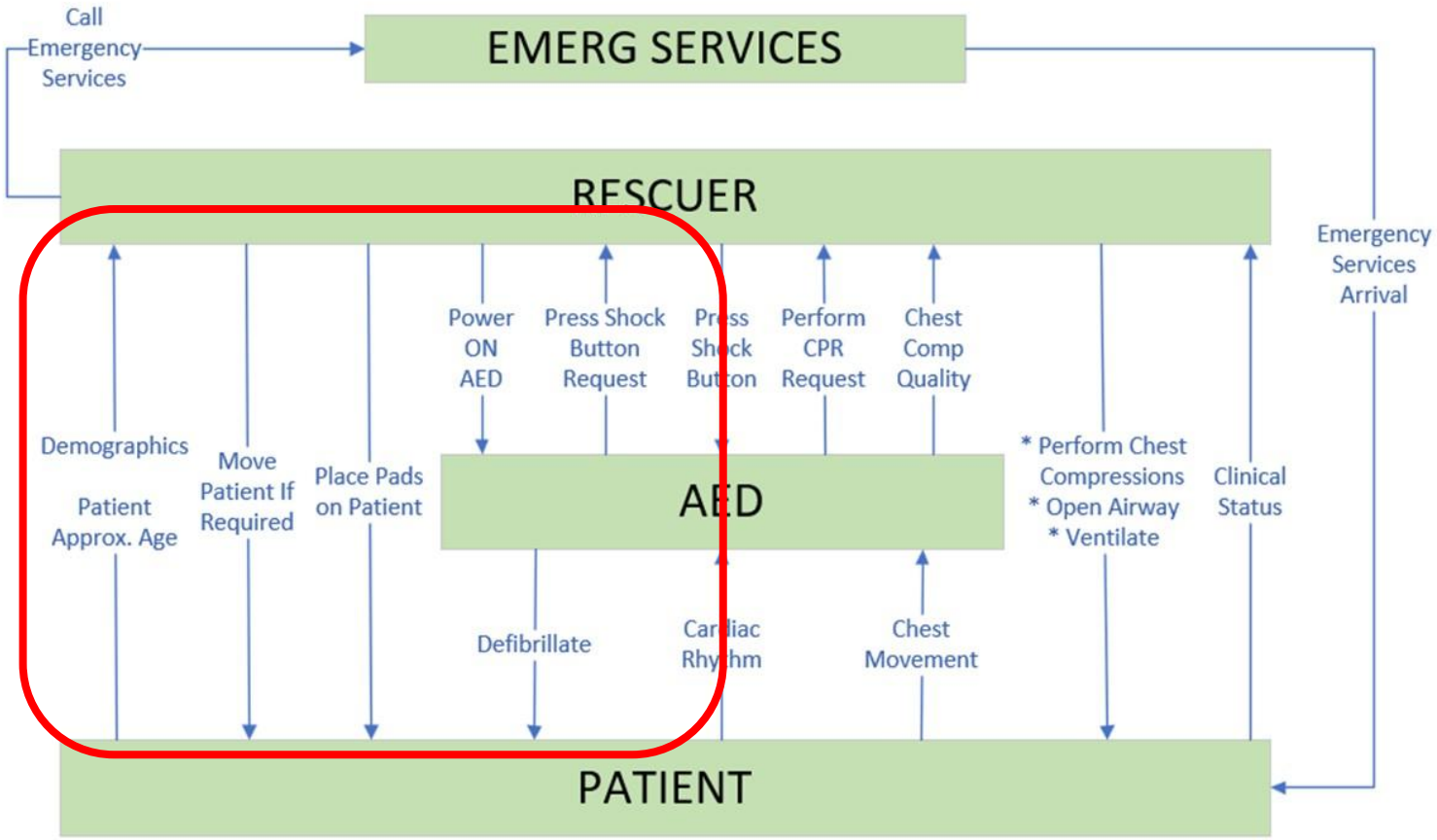


STPA Step 2 – Model Control Structure (CS) [8]

CS evolved by understanding of actual uses and STAMP diagramming conventions

- What about moving patient if required?
- Change CS to correct “Place Pads on Patient,” as initial control actions were predicated on the instruction sequence in the manual – Made us think: “Is that really how it works?”





STPA Step 3 – Identify Unsafe Control Actions [8]

Documenting "no hazard" statements

- Initially, these CAs did not seem to present a hazard, so why not prune them from analysis . . .

Element Functions					STPA Evaluation				
CONTEXT: USING THE AED ONSITE					UCAs (Unsafe/Unwanted Control Actions)				UCA Constraints
Element Number	Element Name	Rescuer "Execution" Perspective (per manual)	Input and/or Feedback	Control Action Issued	Not provided	Provided But Unsafe	Incorrect Timing/Order	Stopped Too Soon Applied Too Long	
		Rescuer Powers <ON> the AED	Patient Ready	Power <ON> AED		UCA-RES-05: Rescuer does Power <ON> AED when patient is not in cardiac arrest [No Hazard]			
						UCA-RES-06: Rescuer does Power <ON> AED when patient is in cardiac arrest but does not have cardiac activity amenable to defibrillation (e.g., asystole) [No Hazard]			
						UCA-RES-07: Rescuer does Power <ON> AED when Patient is in contact with a rescuer or bystander [No Hazard]			

STPA Step 3 – Identify Unsafe Control Actions [8]

Documenting "no hazard" statements

- Initially, these CAs did not seem to present a hazard, so why not prune them from analysis . . .

Or Do They???? Easy to give up to quickly with analysis

Element Functions					STPA Evaluation				
CONTEXT: USING THE AED ONSITE					UCAs (Unsafe/Unwanted Control Actions)				UCA Constraints
Element Number	Element Name	Rescuer "Execution" Perspective (per manual)	Input and/or Feedback	Control Action Issued	Not provided	Provided But Unsafe	Incorrect Timing/Order	Stopped Too Soon Applied Too Long	
						UCA-RES-05: Rescuer does Power <ON> AED			
		Rescuer Powers <ON> the AED	Patient Ready	Power <ON> AED					
						UCA-RES-07: Rescuer does Power <ON> AED when Patient is in contact with a rescuer or bystander [No Hazard]			

(May be hazard [H1] where AED once powered up may have a fault or issue that it provides an unwanted shock. Should it be covered here or assume the risk is really after the pads are placed on Patient?)

STPA Step 4 - Identify Safety Related Causal Scenarios [8]

Capturing intuitive "causal scenarios"; enriching them based on STAMP conventions

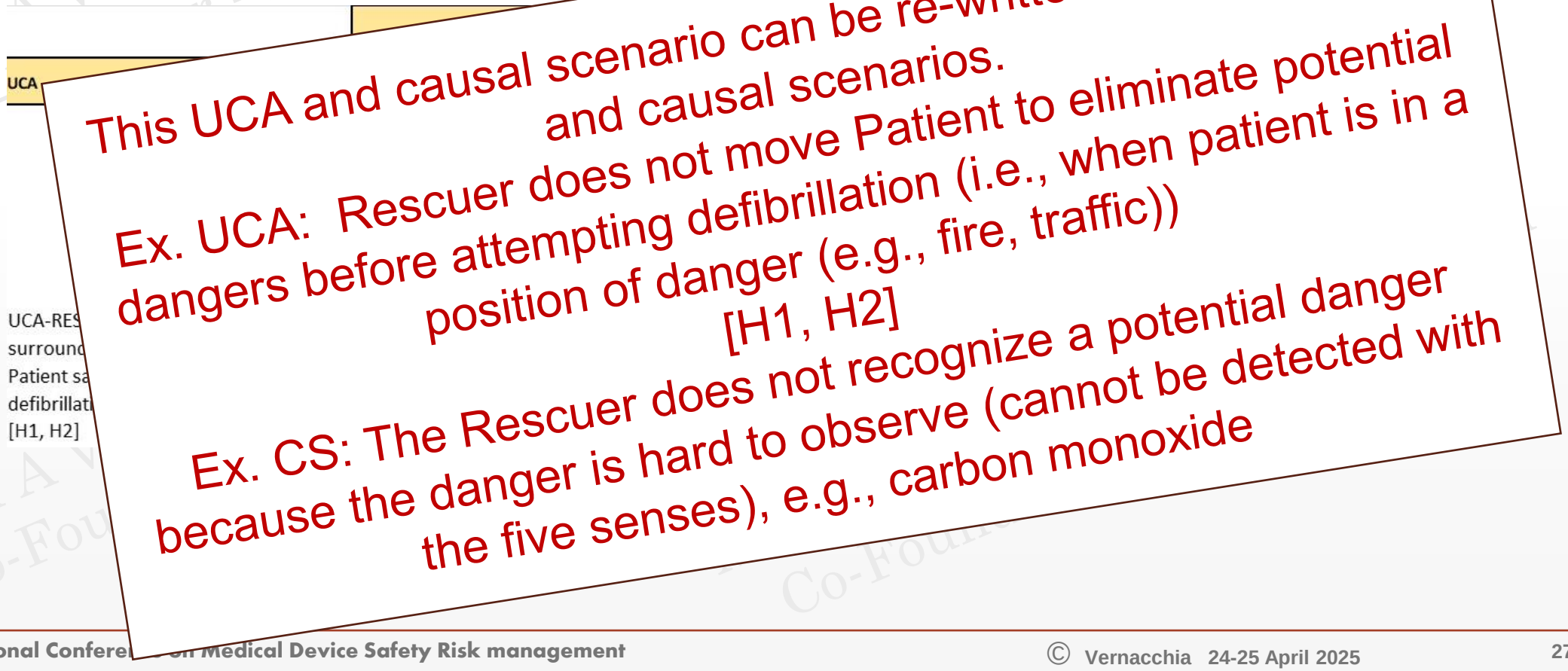
- Assessed how to document potential redundancy with other UCAs

	Why Would Malfunctions Occur?		Why Might Control Actions Not be Executed or Executed Improperly?	
UCA	Unsafe "Controller" Behavior (Human or Physical)	Causes of Inadequate Feedback/Input	Control Path Issues	Controlled Processes Issues
UCA-RES-01: Rescuer does not assess surrounding environment to determine Patient safety before attempting defibrillation [H1, H2]	CS-RES-01: The Rescuer does not know they should assess the surrounding environment			

STPA Step 4 - Identify Safety Related Causal Scenarios [8]

Capturing intuitive "causal scenarios"; enriching them based on STAMP conventions

- Assessed how to document potential redundan… UCAs



STPA AED Evaluation - Assumptions [8]

This evaluation considered future requirements associated with the Rescuer and AED interactions based on assumptions such as:

- Discussion regarding level of assumptions of Rescuer capabilities and training
- English not first language for Rescuer
- No Rescuer CPR capability
- Rescuer panic

STPA Next Generation AED Requirements [8]

These assumptions lead to an opportunity to have new future requirements that provide:

- Use of Artificial Intelligence (AI) for new req'mts
  - Interactive dialogue between AED and Rescuer
  - Multi-lingual AED capability
- New AED capabilities such as:
  - New sensors with enhanced pad location determination capability
  - Motion detection in AED unit
  - Enhanced visual and aural feedback

STPA Next Generation AED Requirements [8]

Additional functions that can be fulfilled with AED

	Why Would Malfunctions Occur?		Why Might Control Actions Not be Executed or Executed Improperly?		Initial Requirements and/or Constraints
UCA-RES-02: Rescuer does not move Patient to eliminate potential dangers before attempting defibrillation [H1, H2]		CS-RES-26: The Rescuer does not recognize a potential danger because the danger is hard to observe (cannot be detected with the five senses), e.g., carbon monoxide			SR-RES-21: The AED shall contain a CO monitor and shall alert the Rescuer of potential danger
		CS-RES-30: The Rescuer does not recognize a potential danger because the potential danger was not present when the assessment was made initially. The rescuer was not trained to repeat assessment over time.			SR-RES-01b: The AED shall broadcast audio/visual instructions to check surrounding environment at a regular interval prior to providing defibrillation shock

STPA Next Generation AED Requirements [8]

Additional functions that can be fulfilled with AED

	Why Would Malfunctions Occur?	Why Might Control Actions Not be Executed or Executed Improperly?	Initial Requirements and/or Constraints
UCA-RES-02: Rescuer does not move Patient to eliminate potential dangers before attempting defibrillation [H1, H2]	CS-RES-26: The Rescuer does not recognize a potential danger because the danger is hard to observe (cannot be detected with the five senses), e.g., carbon monoxide		ıall contain a CO the Rescuer of
	CS-RES-30: The Rescuer does not recognize a potential danger because the potential danger was not present when the assessment was made initially. The rescuer was not trained to repeat assessment over time.		all broadcast to check t at a regular g defibrillation

SR-RES-21: The AED shall contain a CO monitor and shall alert the Rescuer of potential danger

SR-RES-01b: The AED shall broadcast audio/visual instructions to check surrounding environment at a regular interval prior to providing defibrillation shock

STPA Next Generation AED Requirements [8]

Additional functions that can be fulfilled with AED

	Why Would Malfunctions Occur?		Why I	nts and/or ts
UCA-RES-02: Rescuer does not move Patient to eliminate potential dangers before attempting defibrillation [H1, H2]		CS-RES-26: The Rescuer does not recognize a potential danger because the danger is hard to observe (cannot be detected with the five senses), e.g., carbon monoxide		ll contain a CO he Rescuer of
		CS-RES-30: The Rescuer does not recognize a potential danger because the potential danger was not present when the assessment was made initially. The rescuer was not trained to repeat assessment over time.		all broadcast to check t at a regular g defibrillation

SR-RES-03: Instructions not to move Patient and to call Emergency Services if no safe area is available shall be included on AED packaging

SR-RES-03: Instructions not to move Patient and to call Emergency Services if no safe area is available shall be included on AED packaging

SR-RES-22: Personnel within the facility the AED is located shall receive appropriate training for assessing surround environment for hazards and moving the Patient if necessary

SR_RES-22a: The AED shall display basic information for moving a patient safely

STPA Next Generation AED Requirements [8]

Additional functions that can be fulfilled with AED

	Why Would Malfunctions Occur?		Why I	nts and/or ts
UCA-RES-02: Rescuer does not move Patient to eliminate potential dangers before attempting defibrillation [H1, H2]		CS-RES-26: The Rescuer does not recognize a potential danger because the danger is hard to observe (cannot be detected with the five senses), e.g., carbon monoxide		ll contain a CO he Rescuer of
			CS-RES find a s <This is the "co	not to move gency Services if shall be ing
				not to move gency Services if shall be ing
		CS-RES-29: The Rescuer believes the patient can be harmed from movement (e.g., spinal concern) and does not know how to perform a safe movement due to lack of training		ithin the facility eceive assessing or hazards and essary all display basic patient safely
		CS-RES-30: The Rescuer does not recognize a potential danger because the potential danger was not present when the assessment was made initially. The rescuer was not trained to repeat assessment over time.		all broadcast to check t at a regular g defibrillation

SR-RES-03: Instructions not to move Patient and to call Emergency Services if no safe area is available shall be included on AED packaging

SR-RES-03: Instructions not to move Patient and to call Emergency Services if no safe area is available shall be included on AED packaging

SR-RES-22: Personnel within the facility the AED is located shall receive appropriate training for assessing surround environment for hazards and moving the Patient if necessary

SR_RES-22a: The AED shall display basic information for moving a patient safely

STPA Next Generation AED Requirements [8]

- Additional functions that can be fulfilled with AED

UCA-RES-18: Rescuer moves patient when patient is NOT in a position of danger [H3]		CS-RES-35: The rescuer mistakes that patient is in a position of danger because the rescuer observed conditions mimicking danger (e.g., screams, shouting nearby)			SR-RES-70: The AED shall provide information to help the Rescuer assess danger potential
					SR-RES-71: The AED shall interact with the Rescue to determine surrounding danger
		CS-RES-36: The rescuer does not know that the hazard is handled by a different means (e.g., patient is in the different of the road, but road access has been blocked by police up and downstream) because 911 call taker is unreachable or focuses on providing resuscitation instructions			SR-RES-73: The AED shall provide communication capability to connect Rescuer to 911 services
					SR-RES-74: The AED shall provide information regarding surrounding Emergency Services activities

STPA Next Generation AED Requirements [8]

- Additional functions that can be fulfilled with AED

UCA-RES-18: Rescuer moves patient when patient is NOT in a position of danger [H3]		CS-RES-35: The rescu position of danger be conditions mimicking nearby)
		CS-RES-36: The rescu handled by a differen different of the road, police up and downst unreachable or focus instructions

SR-RES-70: The AED shall provide information to help the Rescuer assess danger potential
SR-RES-71: The AED shall interact with the Rescue to determine surrounding danger
SR-RES-73: The AED shall provide communication capability to connect Rescuer to 911 services
SR-RES-74: The AED shall provide information regarding surrounding Emergency Services activities

\ED shall provide information to assess danger potential
\ED shall interact with the ine surrounding danger
\ED shall provide apability to connect Rescuer to
\ED shall provide information nding Emergency Services

Future AI Design Aspects [8]

What to assume about

- Rescuer training and capabilities
- AED Capabilities

How can AI help in future design?

	Why Would Malfunctions Occur?		Why Might Control Actions Not be Executed or Executed Improperly?		Initial Requirements and/or Constraints	Future Capability
UCA-RES-36: Rescuer does perform CPR too late after a shock is provided by the AED [H3]	CS-RES-71: The rescuer is fatigued and cannot resume CPR immediately after a shock					
	CS-RES-72: The rescuer does not know that a shock has been provided by the AED because no enunciation was made or the enunciation is ineffective given the environmental and user conditions					
	CS-RES-73: The rescuer believes that CPR should be delayed (e.g., the AED is performing another round of analysis) because the prompt to resume CPR from the AED was delayed					
	CS-RES-74: The rescuer does not know that CPR should be resumed promptly after a shock because the need was not covered or incorrectly covered in training					

Future AI Design Aspects [8]

What to assume about

- Rescuer training and capabilities
- AED Capabilities

	Why Would Malfunctions Occur?		Why Might Control Actions Not be Executed or Executed Improperly?		Initial Requirements and/or Constraints	Future Capability
UCA-RES-36: Rescuer does perform CPR too late after a shock is provided by the AED [H3]	CS-RES-71: The rescuer is fatigued and cannot resume CPR immediately after a shock				SR-RES-233: The AED shall remind Rescuer to survey scene to recruit additional help	Y
					What is alternative if no other person is around? Should AED try to shock again? How would Rescuer Know?	Y
	CS-RES-72: The rescuer does not know that a shock has been provided by the AED because no enunciation was made or the enunciation is ineffective given the environmental and user conditions				SR-RES-250: The AED shall adjust aural output based on ambient sound level	Y
					SR-RES-221: The AED shall provide visual and aural feedback to the Rescuer that it is performing each step of the AED process so the Rescuer knows AED state	Y
	CS-RES-73: The rescuer believes that CPR should be delayed (e.g., the AED is performing another round of analysis) because the prompt to resume CPR from the AED was delayed				SR-RES-221: The AED shall provide visual and aural feedback to the Rescuer that it is performing each step of the AED process so the Rescuer knows AED state	Y
	CS-RES-74: The rescuer does not know that CPR should be resumed promptly after a shock because the need was not covered or incorrectly covered in training				SR-RES-251: AED Training shall address proper resumption of CPR after shock has been delivered	Y

STPA Next Generation AED Requirements [8]

Examples of AI-based requirements include:

SR-RES-106: The AED shall have multilingual voice recognition capabilities

SR-RES-104: The AED shall have microphone capabilities to listen to verbal Rescuer input

SR-RES-232: The AED shall communicate with Emergency Services dispatch centers conveying critical information

SR-RES-71: The AED shall interact with the Rescuer to determine surrounding danger

SR-RES-74: The AED shall provide information regarding Emergency Services activities

SR-RES-201: The AED shall determine Patient stature through pad location diagnostics and adjust shock accordingly

Next-generation AI Driven AED – Questions [8]

- Can an AI driven AED interaction be developed with sufficient capability to address all scenarios?
- Should the design constraints assume only a limited number of scenarios?
- How much should the design assume about Rescuer capabilities?
- Can an AI driven AED be made affordable (cost)?
- How should AED training be modified?
- What capabilities will the public assume when they hear about an AI-driven AED?

Summary - STPA and Risk Management Process

System Safety supports Risk Management as its goal is to optimize safety

Exposure to harm, danger, and loss (risk) is a function of likelihood and consequences

Risk Management (ISO-14971) – identify hazards and hazardous situations associated with medical devices and then control risk

Risk Control (ISO-14971) – risk at acceptable level

Summary - STPA and Risk Management Process

Fault Tree Analysis (FTA) – a failure-based approach starting with known effects to determine causes (deductive reasoning)

Failure Mode and Effects Analysis (FMEA) - a failure-based approach starting with known causes to determine potential effects (inductive inductive)

System Theoretic Process Analysis (STPA) – controls-based approach that evaluates system behavior to determine both possible effects and causes (exploratory reasoning). Easily accommodates human interactions as part of control structure and evaluates non-failure scenarios resulting from poor or improper design. (*Compliments* FTAs and FMEAs)

Summary - STPA and Risk Management Process

- STPA can identify safety-related risk:
  - Identifies losses and hazardous conditions where losses may occur. Can be used early in design process while system is under development to shape system design.
  - Determines which unsafe control actions (UCAs) lead to hazardous conditions
- STPA can develop safety-related requirements to prevent/manage risk
  - Identifies causes or scenarios for unsafe control actions
  - Determines why control actions may not be executed or executed improperly

First Cross-Industry STPA Standard

- SAE J3307_202503 documents what is required to execute a System Theoretic Process Analysis (STPA) of safety-critical products or systems in all industries. The standard defines the terminology, the steps in using STPA, activities flow and expected deliverables.
- This standard may be used when addressing compliance with contractual or regulatory requirements regarding risk assessments, safety assessments, development assurance, system security engineering, or other similar requirements
- In addition, this standard can be used to demonstrate that an effective STPA evaluation has been conducted when compliance is not of paramount concern

First Cross-Industry STPA Standard – SAE J3307

CURRENT ISSUED 2025-03-25

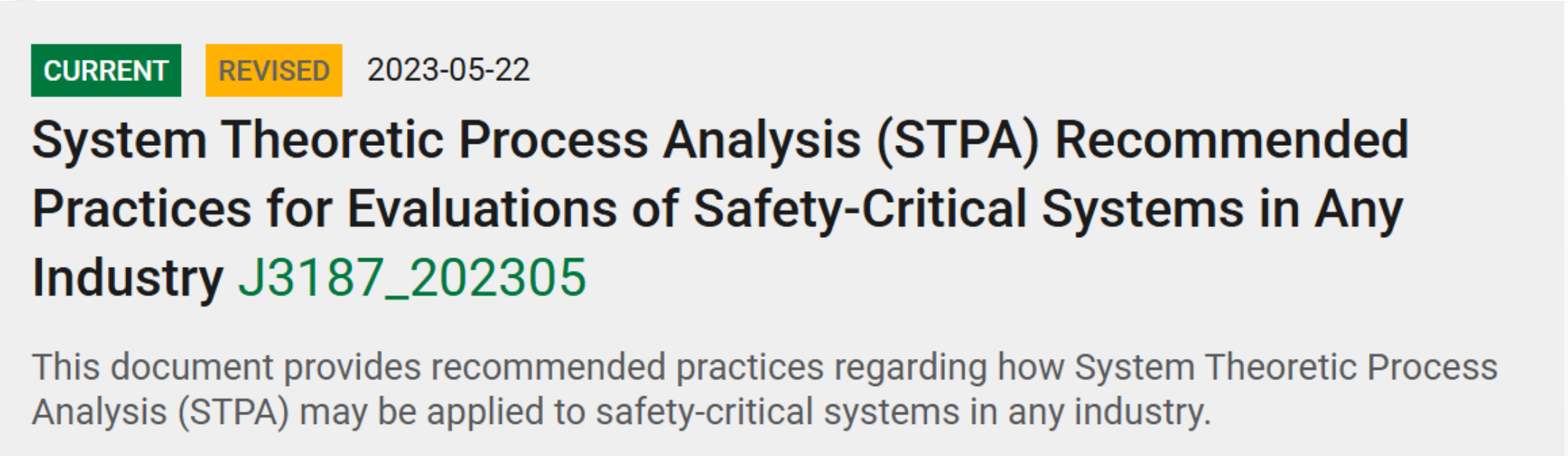
System Theoretic Process Analysis (STPA) Standard for All Industries J3307_202503

This standard documents what is required to execute a System Theoretic Process Analysis (STPA) of safety-critical products or systems in all industries. This standard defines the terminology, the steps in using STPA, the activities flow, and the expected deliverables. This standard may be used when addressing compliance with contractual or regulatory requirements regarding risk assessments, safety assessments, development assurance, system security engineering, or other similar requirements as appropriate. In addition, this standard can be used to demonstrate that an effective STPA evaluation has been conducted when compliance is not of paramount concern.

This standard is applicable to a broad set of uses including, but not limited to, corporate product development processes, organizational processes, regulatory groups, supplier processes, defense programs (e.g., government awards a contract to a company and the contract mandates STPA), defense program office (e.g., government safety group applies STPA during a safety review on a project), healthcare safety researchers (not engineers), and site reliability engineering (e.g., Google Maps, where the “controlled process” is a virtual map - pure data rather than a physical process) to name a few.

STPA Recommended Practices All Industries

- SAE J3187_202305 describes how to execute a System Theoretic Process Analysis (STPA) of safety-critical products or systems in all industries. It provides recommended practices regarding how System Theoretic Process Analysis (STPA) may be applied to safety-critical systems in any industry.



STPA Recommended Practices All Industries

- SAE J3187_202305 has published appendices
- The STPA Task Force is currently developing appendices for:
  - STPA and Security Engineering
  - STPA and Medical Devices

Existing STPA Recommended Practices

CURRENT REVISED 2023-05-22
System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry J3187_202305

CURRENT ISSUED 2023-09-06
System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry - Appendix: STPA and Human Machine Interactions (HMIs) J3187-1_202309

CURRENT ISSUED 2023-09-06
System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry - Appendix: STPA and Safety of the Intended Functionality J3187-2_202309

CURRENT ISSUED 2023-09-06
System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry - Appendix: STPA and Model-Based Systems Engineering (MBSE) J3187-3_202309

References

[1] MIL-STD-882E - Department of Defense Standard Practice System Safety

[2] ISO 14971 Medical devices - Application of Risk Mgmt to Medical Devices

[3] STPA Handbook 2018, Leveson, Nancy; Thomas John, MIT

[4] ISO-26262 – Version 1 2011

[5] FAA Systems Safety Handbook - December 30, 2000

[6] ARP-4761 - Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

[7] NASA System Safety Handbook - NASA/SP-2014-612 Version 1.0, November 2014

[8] Innovation and Lessons Learned from Applying STPA for Medical Devices, Next Generation Automated External Defibrillator (AED), MIT STAMP Virtual Conference Sept 2024, Vernacchia, Wong

[9] ISO/TR 24971 - Medical devices — Guidance on the Application of ISO 14971

[10] Introduction to System Safety Engineering; Leveson, Nancy; 2023 MIT

[11] STPA Overview, MIT STAMP Workshop; Leveson, Nancy; 2017 MIT

[12] System Safety and STPA Class; Thomas, John; STAMP-Institute; 2024

NOTE: SAE STPA Standard and Recommended Practices may be found at: https://saemobilus.sae.org/

QUESTIONS??

markv.ssegroup.011@gmail.com