# Innovation and Lessons Learned from Applying STPA for Medical Device

## Next Generation Automated External Defibrillator (AED)


Mark A. Vernacchia, MSES, INCOSE ESEP, PE
Principal and Co-Founder – SSE Group, LLC
Former Technical Fellow – General Motors Company
Chair – SAE STPA Task Force

Lawrence Wong, PhD
Postdoctoral Researcher, Department of Radiation Medicine and Applied Sciences,
UC San Diego Health
Member – SAE STPA Task Force

# Aim

- To facilitate wider application of STPA for medical device design
- To demonstrate the ability to advance medical device design with STPA
- To highlight key STPA analysis decisions and pitfalls

# Agenda

- Automated External Defibrillator (AED) -- the medical device of interest
- STPA of AED (cardiac arrest resuscitation) -- examples and shareable lessons
- Next-generation AED functions derived from AED STPA

# Automatic External Defibrillator (AED)




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 All AEDs

1. Power ON the AED
2. Attach electrode pads
3. Analyze the rhythm
4. Clear the victim and press SHOCK button

(American Heart Association, 2000)

# STPA Step 1 – Losses and Hazards

- Traceability

| Number | Losses |
|---|---|
| L1 | Loss of life |
| L2 | Injury to rescuers or bystanders |
| L3 | Unsuccessful resuscitation |
| L4 ?? | Damage to equipment |

| Hazard Number | Hazards | Relationship to Losses |
|---|---|---|
| H1 | 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 design (???) | L4 |

# STPA Step 1 – Losses and Hazards

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

| Number | Losses |
|---|---|
| L1 | Loss of life |
| L2 | Injury to rescuers or bystanders |
| L3 | Unsuccessful resuscitation |

| Hazard Number | Hazards | Relationship to Losses |
|---|---|---|
| H1 | 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 |

# STPA Step 1 – Losses and Hazards

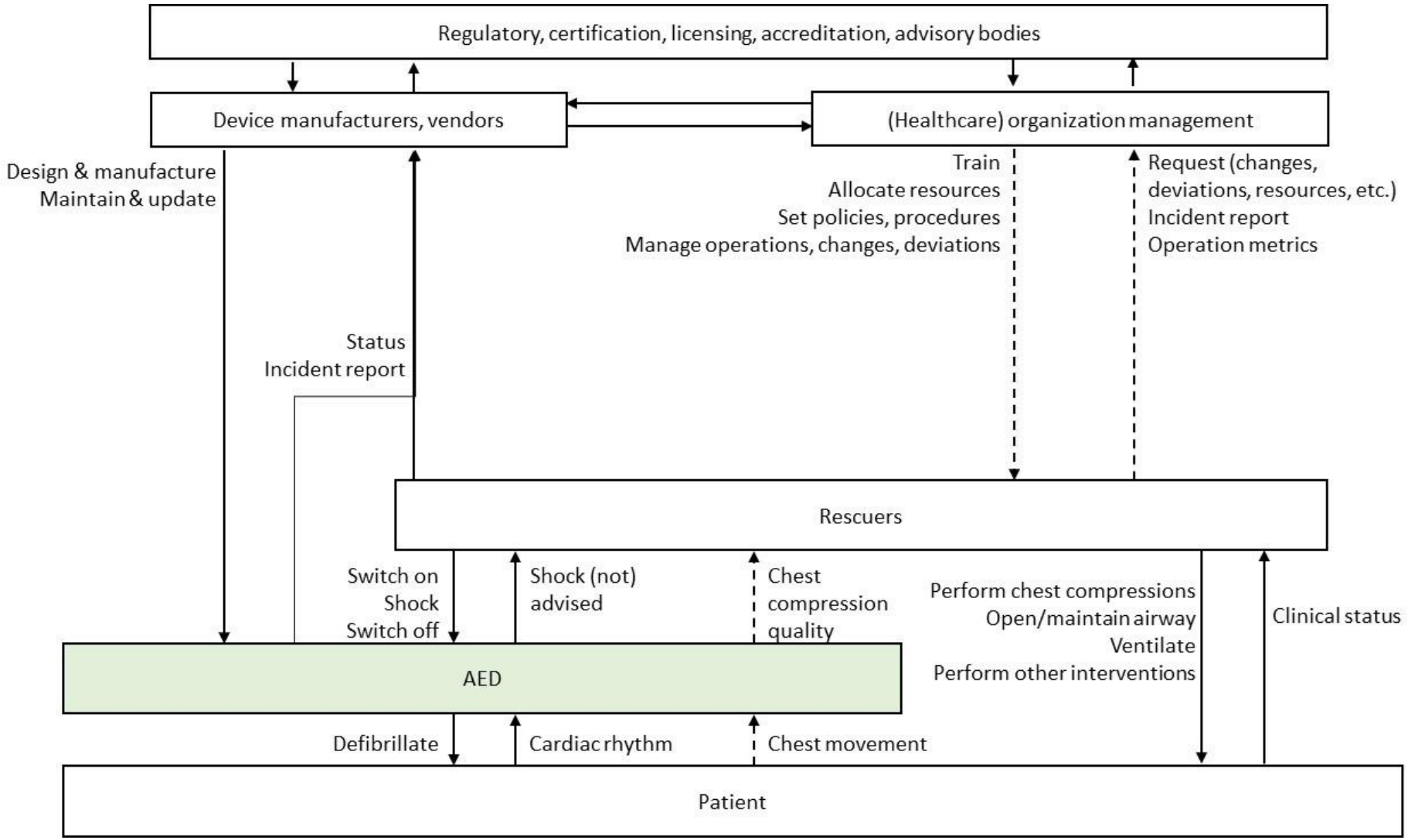
- Traceability
- Analysis scoping
  - L4, H4 omitted for this work
- Constraints
  - Keeping them at the system (vs. component) level

| Number | Losses |
|---|---|
| L1 | Loss of life |
| L2 | Injury to rescuers or bystanders |
| L3 | Unsuccessful resuscitation |

| Hazard Number | Hazards | Relationship to Losses | Constraint Number | Constraints |
|---|---|---|---|---|
| H1 | Exposure of human to electrical energy | L1 and L2 | C1 | The AED shall protect humans from exposure to electrical energy |
| H2 | Exposure of human to thermal or combustion events/energy | L1, L2, and L3 | C2 | The AED shall protect humans from exposure to electrical energy |
| H3 | Patient does not receive effective defibrillation, chest compression (or rescue breathing) | L3 | C3-1 | The AED shall provide effective defibrillation when operated |
| | | | C3-2 | The Rescuer shall provide effective chest compressions and/or rescue breathing when required |

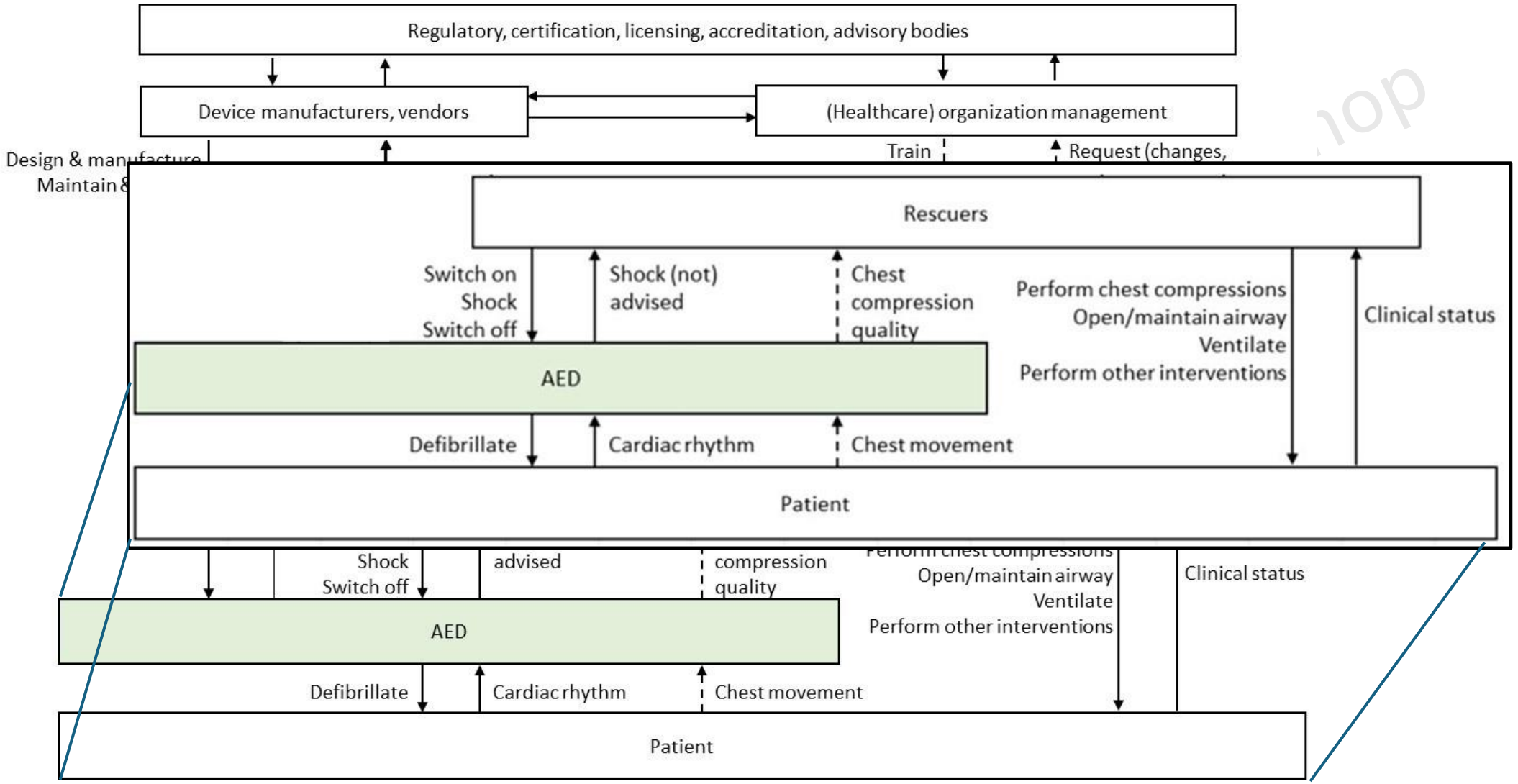
# STPA Step 2 – Control Structure

The entire cardiac arrest resuscitation system has many components



# STPA Step 2 – Control Structure

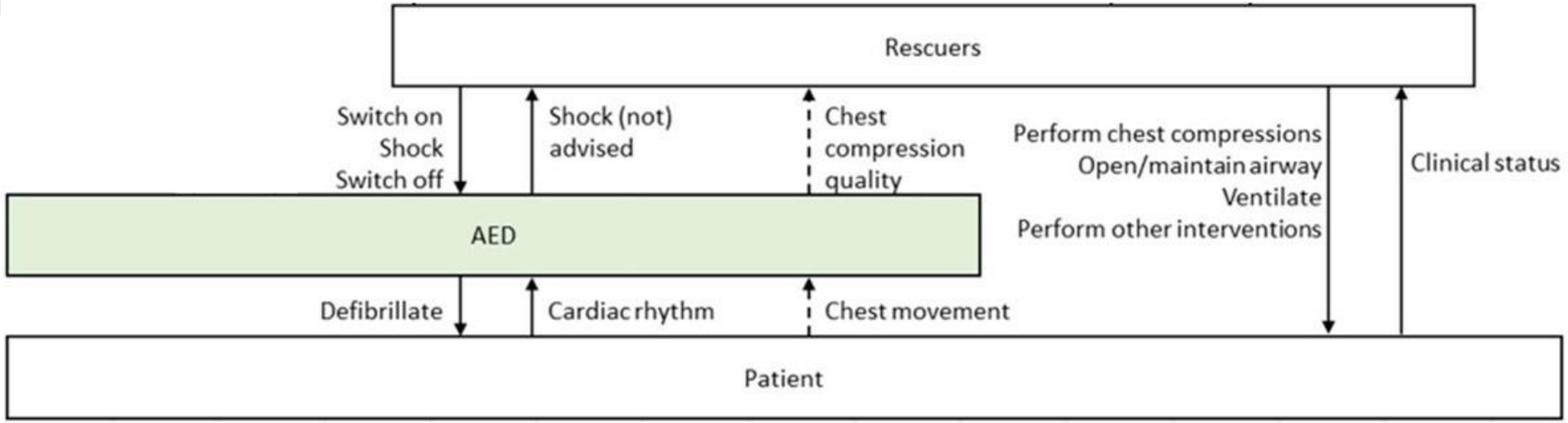
The entire cardiac arrest resuscitation system has many components



# STPA Step 2 – Control Structure

A comprehensive analysis should consider multiple aspects and perspectives. Rescuer as "controller" with its own mental model

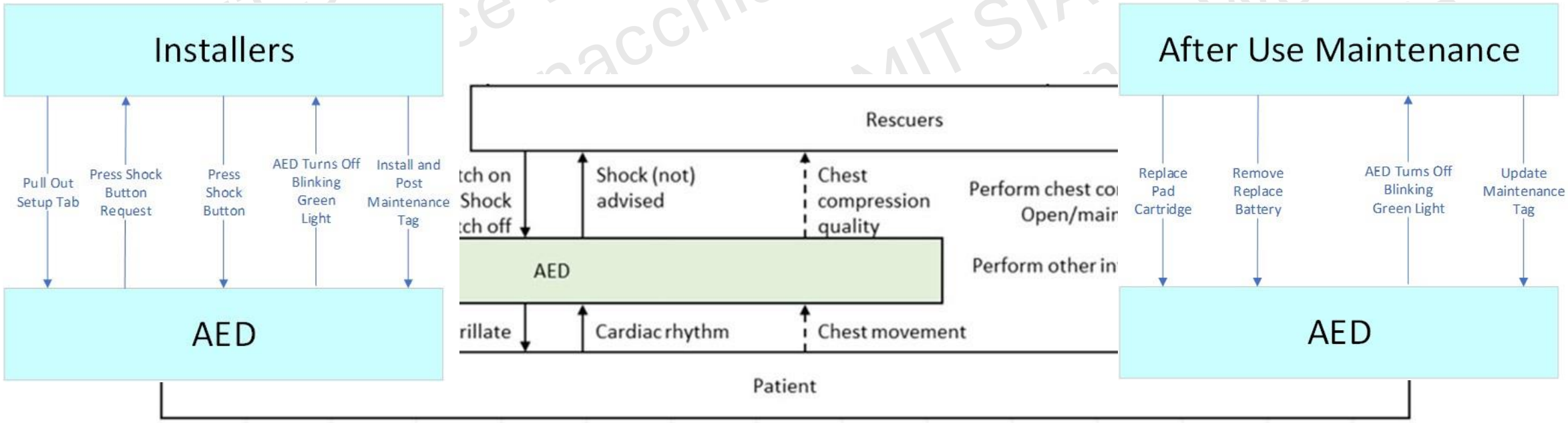




# STPA Step 2 – Control Structure

A comprehensive analysis should consider multiple aspects and perspectives. Rescuer as "controller" with its own mental model

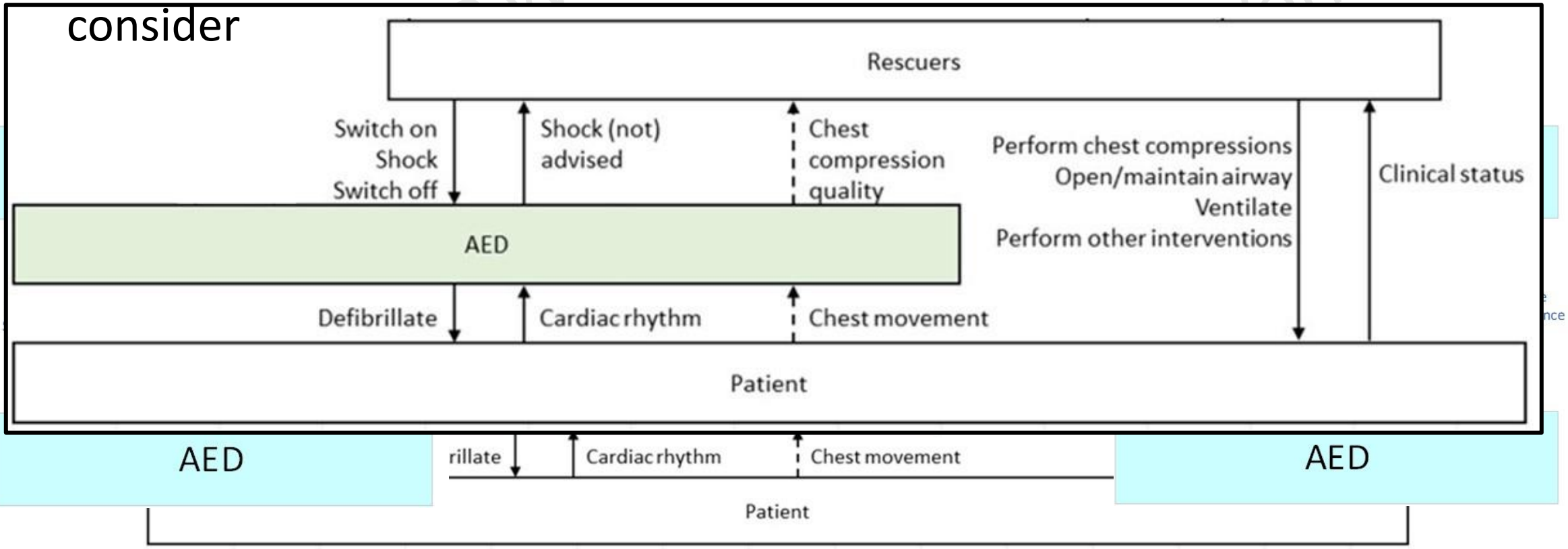
- Initial Installation, Using AED, and Post-Use Maintenance



# STPA Step 2 – Control Structure

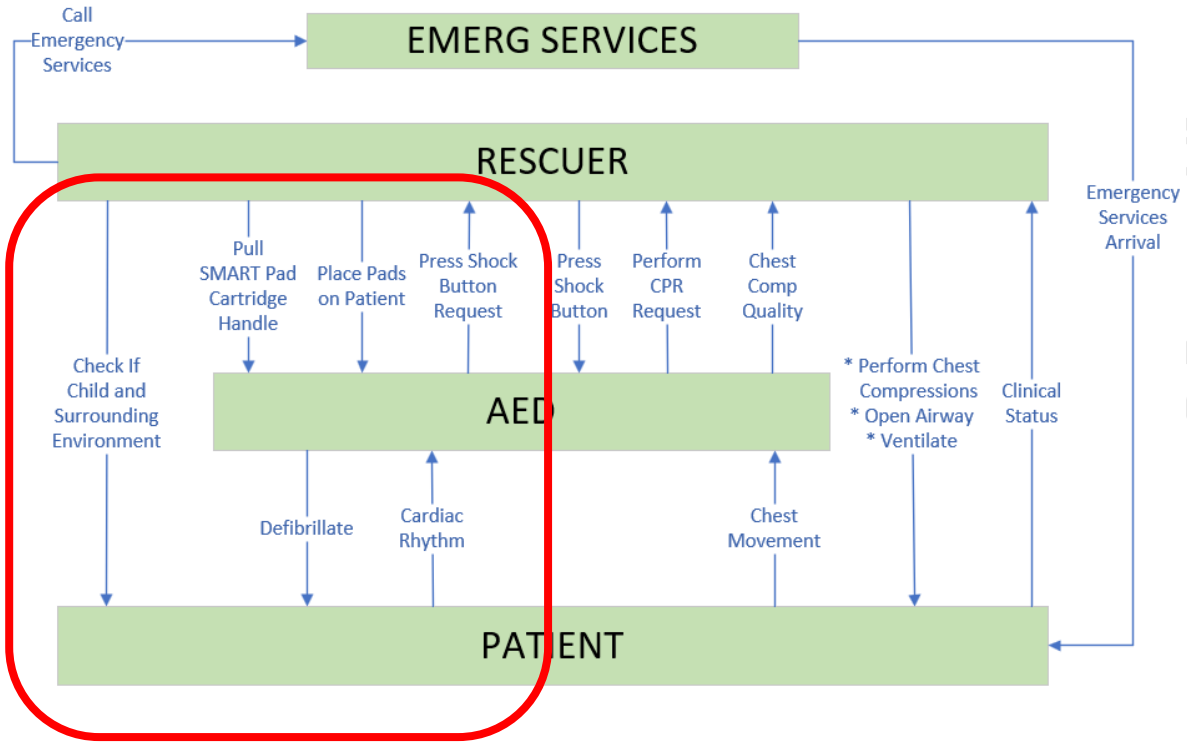
A comprehensive analysis should consider multiple aspects and perspectives. Rescuer as "controller" with its own mental model

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



# STPA Step 2 – Control Structure

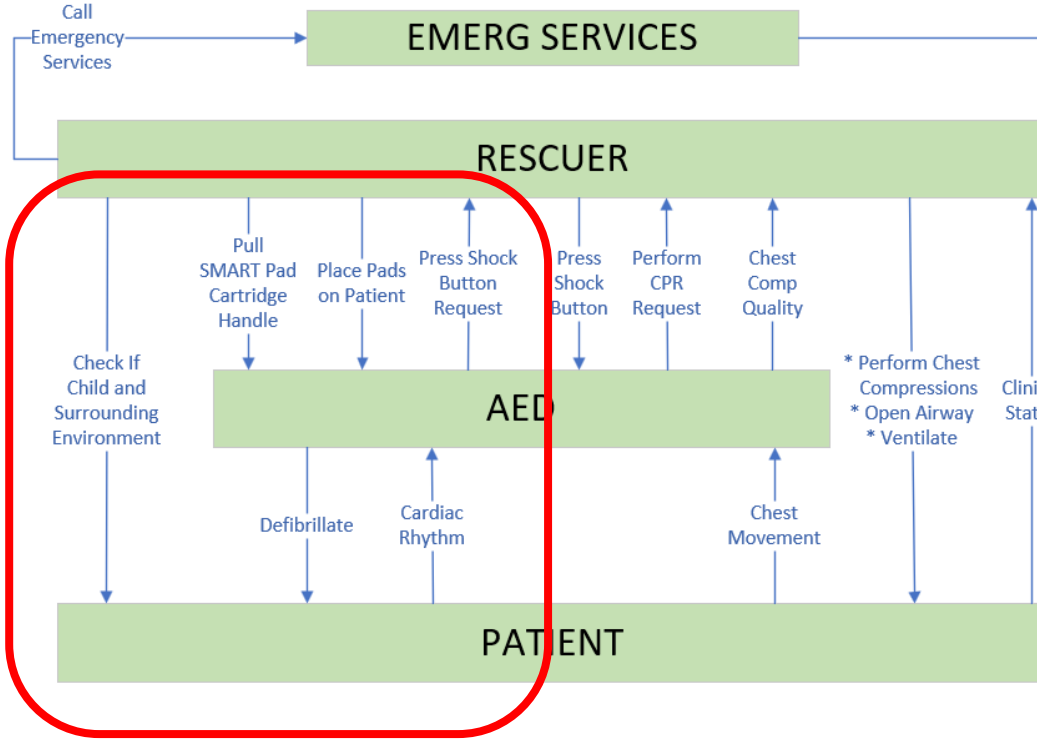
CS evolved based on understanding of actual uses and STAMP diagramming conventions

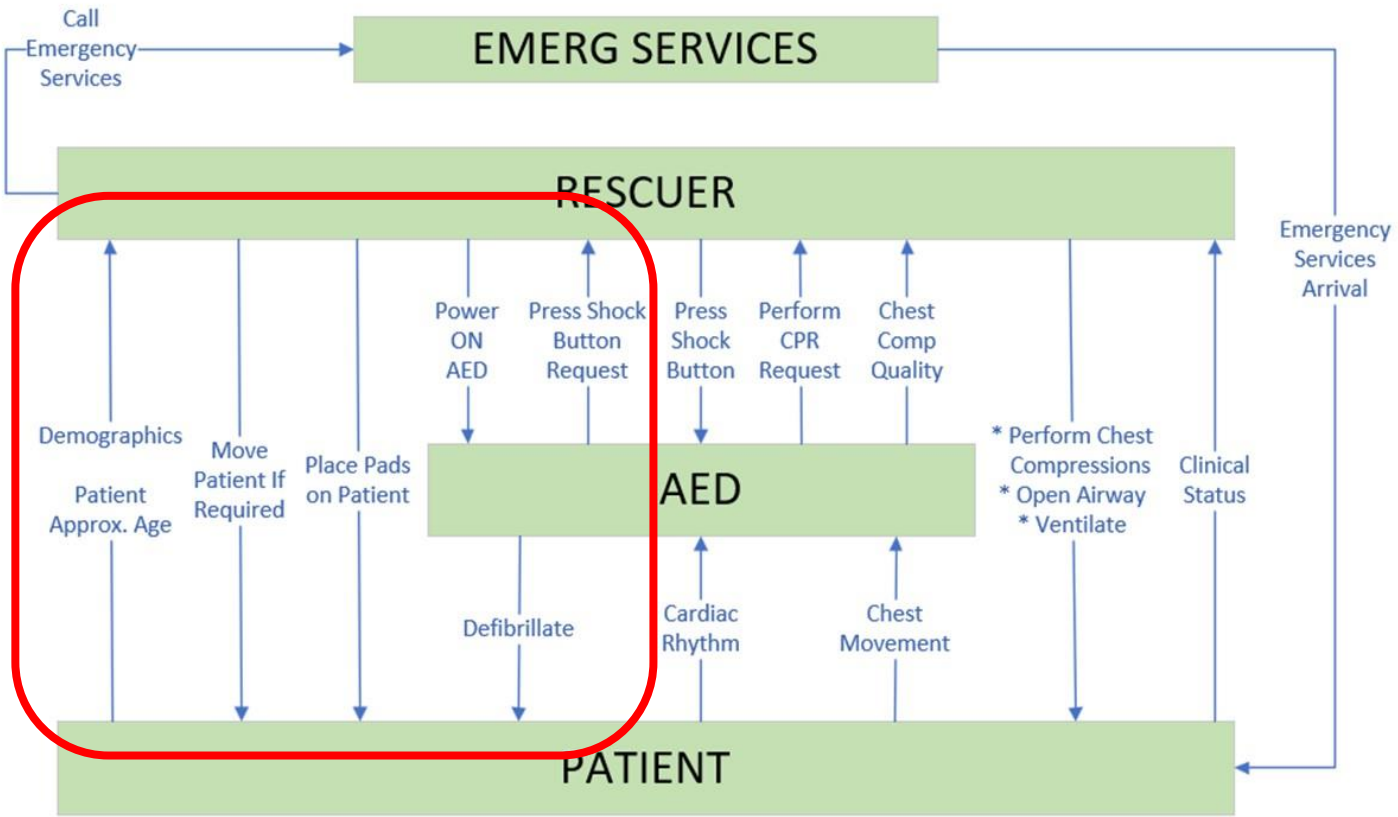


# STPA Step 2 – Control Structure

CS evolved based on understanding of actual uses and STAMP diagramming conventions

- Moving Patient if required
- Change to correct "Place Pads on Patient," as initial control action was predicated on the instruction sequence in the manual – Made us think: "Is that really how it works?"



# STPA Step 3 – Unsafe Control Actions

## Documenting "no hazard" statements

- Initially, these CAs do not seem to present a hazard, can be pruned 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 – Unsafe Control Actions

Documenting "no hazard" statements

- Initially, these CAs do not seem to present a hazard, can be pruned from analysis

Or Can 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 | |
| | | 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]<br><br>**(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?)** | | | |
| | | | | | | 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 4 – Loss (Causal) Scenarios

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 – Loss (Causal) Scenarios

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 | Cont... ...ses 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 | | | |

This UCA and causal scenario can be re-written into other UCAs and causal scenarios.

Ex. UCA: Rescuer does not move Patient to eliminate potential dangers before attempting defibrillation (i.e., when patient is in a position of danger (e.g., fire, traffic)) [H1, H2]
...

Ex. CS: 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

# STPA Evaluation – Loss (Causal) Scenarios

## Defining subcases to causal scenarios

- Whether to explicitly define these subcases is an analysis decision. The decision can be made from whether explicit statements will be useful, e.g., to identify solutions to eliminate/mitigate the causal scenarios



| | | | | | |
|---|---|---|---|---|---|
| | Also subcases to the causal scenarios for UCA-RES-02: Rescuer does not move Patient to eliminate potential dangers before attempting defibrillation<br><br>Illustrated below as an example | | | | |
| UCA-RES-35: Rescuer does perform CPR when patient is positioned on equipment not designed for the load/weight generated in the process of resuscitation [H3, H4] | | CS-RES-30a: The Rescuer does not recognize the patient is positioned on equipment not designed for the load/weight because the load/weight bearing capability of the equipment has been undermined since the assessment was made initially. The rescuer was not trained to repeat assessment over time. | | | SR-RES-240: The AED shall provide visual and aural feedback to the Rescuer that CPR compressions are insufficient and that the Patient may need to be moved to firmer ground |

# More Shareable Lessons While Doing this Analysis

- Reassigned UCAs from one UCA column to another as analysis proceeded (e.g., was Not Provided" but now "Incorrect Timing/Order")
- Handling UCAs that can be accommodated into existing UCAs
- Inclusion or exclusion of Causal Scenarios based on analysis scope
- Accommodating assumptions about possible Rescuer impairments (visual, aural, etc.)
- Relationship between Causal Scenarios where one provides a deeper level of understanding of another
- Assess different use cases – are there only two Rescuer types (child or adult)?  How to handle a person of short stature (Little People)

# Next-generation AED functions derived from AED STPA

- 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 |

# Next-generation AED functions derived from AED STPA

- 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-04: The Rescuer cannot find a safe area<br><br><This is a neat causal scenario of the "contextual factor" category> | | 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 |
| | | | | CS-RES-04: The Patient is not moveable | 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 |
| | | 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 | | | 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<br><br>SR_RES-22a: The AED shall display basic information for moving a 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. | | | SR-RES-01b: The AED shall broadcast audio/visual instructions to check surrounding environment at a regular interval prior to providing defibrillation shock |

# Next-generation AED functions derived from AED STPA

- 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 |

# Forthcoming J-3187-5: System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Healthcare APPENDIX – STPA and Medical Devices

Aims to provide expanded guidance to safety practitioners working in the healthcare device space to enable more effective and holistic system engineering outcomes

Supplements existing SAE guidance on applying STPA… provide a concise set of proven techniques practitioners have successfully applied when using STPA on safety-critical, human-interfacing healthcare systems

Interested STPA Practitioners are welcome to join the SAE STPA Task Force to help develop this planned Recommended Practice

**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

*Coming Fall 2024 - SAE J3307*

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

# QUESTIONS??

markv.ssegroup.011@gmail.com

L_wong@mit.edu

(Additional Slides Follow)

# STPA Evaluation – Loss (Causal) Scenarios

## Improving Loss (Causal) Scenarios as we proceeded with analysis

- Deciding if Loss (Casual) Scenario is well defined, or requires more thought
- Assess how to document potential redundancy with other UCAs

| | Why Would Malfunctions Occur? | | Why Might Control Actions Not be Executed or Executed Improperly? | | Initial Requirements and/or Constraints |
|---|---|---|---|---|---|
| UCA | Unsafe "Controller" Behavior (Human or Physical) | Causes of Inadequate Feedback/Input | Control Path Issues | Controlled Processes Issues | |
| UCA-RES-02: Rescuer does not move Patient to eliminate potential dangers before attempting defibrillation [H1, H2] | CS-RES-03: The Rescuer does not recognize a potential danger<br><br><This causal scenario seems under-specified because it only states a mental model flaw but does not relate it to the other aspects of the system. A question to enrich the content is "why does the rescuer not recognize a potential danger? See CS-RES-26 as an example> | | | | SR-RES-02: Information describing potential dangers shall be easily visible on the AED packaging<br><br>SR-RES-02a: The AED shall broadcast audio/visual descriptions of potential hazards upon initial Power <ON> sequence |
| | | CS-RES-27: The Rescuer does not recognize a potential danger because they do not know they should assess the surrounding environment due to the lack of training<br><br><This causal scenario incorporates the content originally described in CS-RES-01> | | | SR-RES-01a: The AED shall broadcast audio/visual instructions to check surrounding environment upon initial Power <ON> sequence |
| | | CS-RES-28: The Rescuer does not recognize a potential danger because they do not know they should assess the surrounding environment and did not receive any feedback or instruction telling them to assess the surrounding environment<br><br><This causal scenario incorporates content originally described in CS-RES-02> | | | SR-RES-01a: The AED shall broadcast audio/visual instructions to check surrounding environment upon initial Power <ON> sequence |

# STPA Evaluation – Loss (Causal) Scenarios

## Updating UCAs as we proceeded with Loss Scenario analysis

| | Why Would Malfunctions Occur? | | Why Might Control Actions Not be Executed or Executed Improperly? | | Initial Requirements and/or Constraints |
|---|---|---|---|---|---|
| **UCA** | **Unsafe "Controller" Behavior (Human or Physical)** | **Causes of Inadequate Feedback/Input** | **Control Path Issues** | **Controlled Processes Issues** | |
| ~~UCA-RES-08: Rescuer does not press Shock Button when patient is in cardiac arrest and has cardiac activity amenable to defibrillation (ventricular fibrillation or ventricular tachycardia) [H3]~~<br><br>UCA-RES-08: Rescuer does press Shock Button when patient is in cardiac arrest and has cardiac activity amenable to defibrillation but too late (> 5 seconds) after AED is charged [H3] | CS-RES-10: The Rescuer cannot find the Shock Button <because the AED is designed to have a Shock mechanism very different from what the rescuer expects, or the mechanism is inconspicuous> | | | | SR-RES-07: The AED shall provide feedback to the Rescuer for locating the Shock Button and informing them to push it |
| | CS-RES-11: The Rescuer thinks the AED will provide shock by itself <from training or feedback that the AED provides> | | | | SR-RES-07: The AED shall provide feedback to the Rescuer for locating the Shock Button and informing them to push it |
| | CS-RES-32: The Rescuer thinks the AED is still charging because the AED announces so | | | | SR-RES-40: The AED shall not announce it is charging without first having run a charging diagnostic to confirm charging |
| | | | CS-RES-34: AED does not shock even when the mechanism is triggered because of wiring failure, battery outage, circuit short, other device faults, or poor pad placement. | | SR-RES-33: The AED shall perform a self-diagnostic on shock defibrillation system upon initial Rescuer request |
| | | | | | SR-RES-34: The AED shall perform a self-diagnostic on shock defibrillation system upon any initial detected physical motion it senses prior to Rescuer request |
| | | | | | SR-RES-35: The AED shall provide feedback to the Rescuer informing them that the shock defibrillation system mechanism is not working |

# STPA Evaluation – Loss (Causal) Scenarios

## Assessed how to document potential redundancy with other UCAs

| | Why Would Malfunctions Occur? | | Why Might Control Actions Not be Executed or Executed Improperly? | | Initial Requirements and/or Constraints |
|---|---|---|---|---|---|
| **UCA** | **Unsafe "Controller" Behavior (Human or Physical)** | **Causes of Inadequate Feedback/Input** | **Control Path Issues** | **Controlled Processes Issues** | |
| UCA-RES-25: Rescuer places pads when pads also contact any human besides the patient [H1] | See CS-RES-40, CS-RES-17 | | | | |
| UCA-RES-28: Rescuer places pads when pads are not placed in a way that supports cardiac activity assessment or defibrillation (e.g., the heart is not along the conduction pathway between the pads) [H3] | See CS-RES-18, CS-RES-19, CS-RES-39, CS-RES-40, CS-RES-41, CS-RES-42 | | | | |
| | CS-RES-65: The rescuer thought pads are placed properly when not because they were given inappropriate pad placement information from the 911 call taker or another rescuer/bystander | | | | SR-RES-10: The AED shall provide audible or visual instructions to the Rescuer regarding how to attach pads to Patient properly |
| UCA-RES-29: Rescuer places pads when pads are in contact of any equipment [H4] | See CS-RES-40, CS-RES-17, CS-RES-58, CS-RES-59, CS-RES-60 | | | | |

# STPA Evaluation - Next Generation AED Impact

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 | | 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 |