Architecture-Supported Audit Processor

Interactive, Query-Driven Assurance

Sam Procter

Jerome Hugues

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

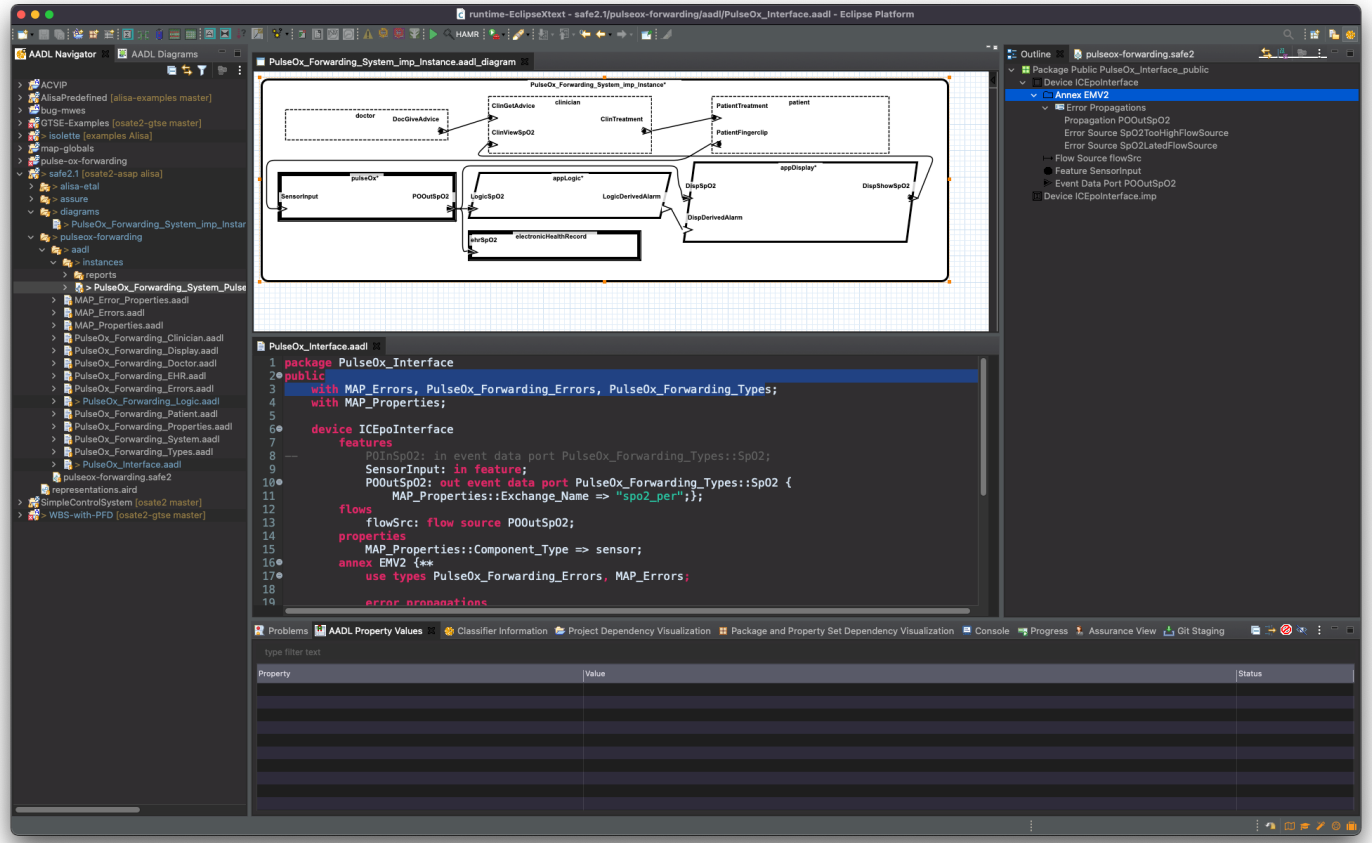
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0766

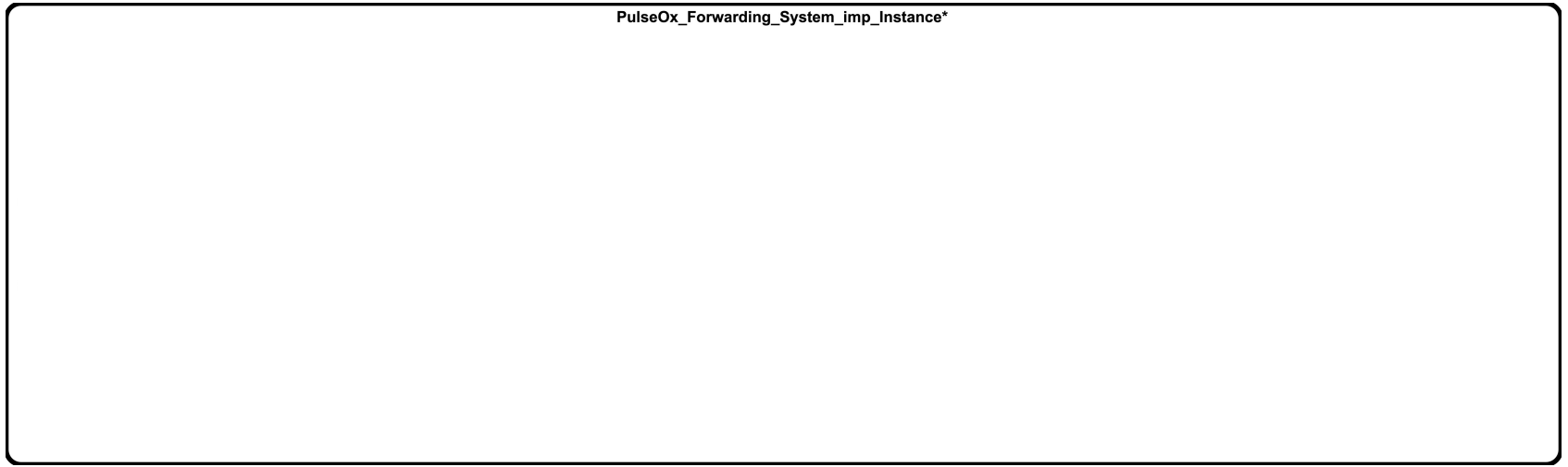
Outline

1. **Background**
    1. AADL / OSATE
    2. PulseOx Forwarding
    3. STPA, SAFE
2. ASAP: Three Viewpoints
3. Future Work

AADL & OSATE

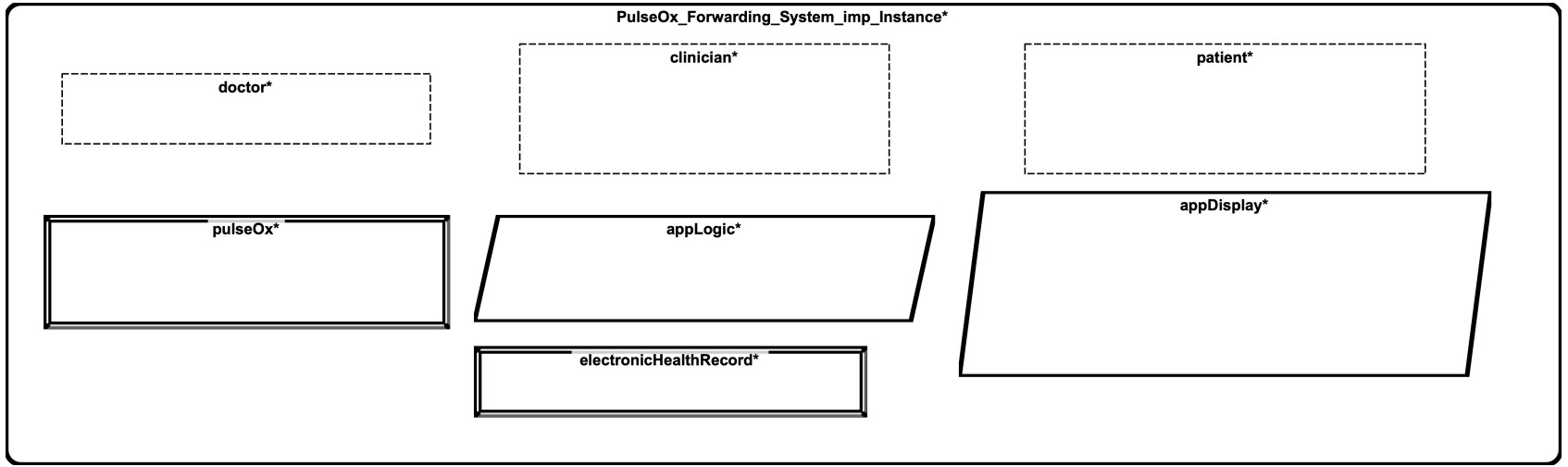


The PulseOx Forwarding Example

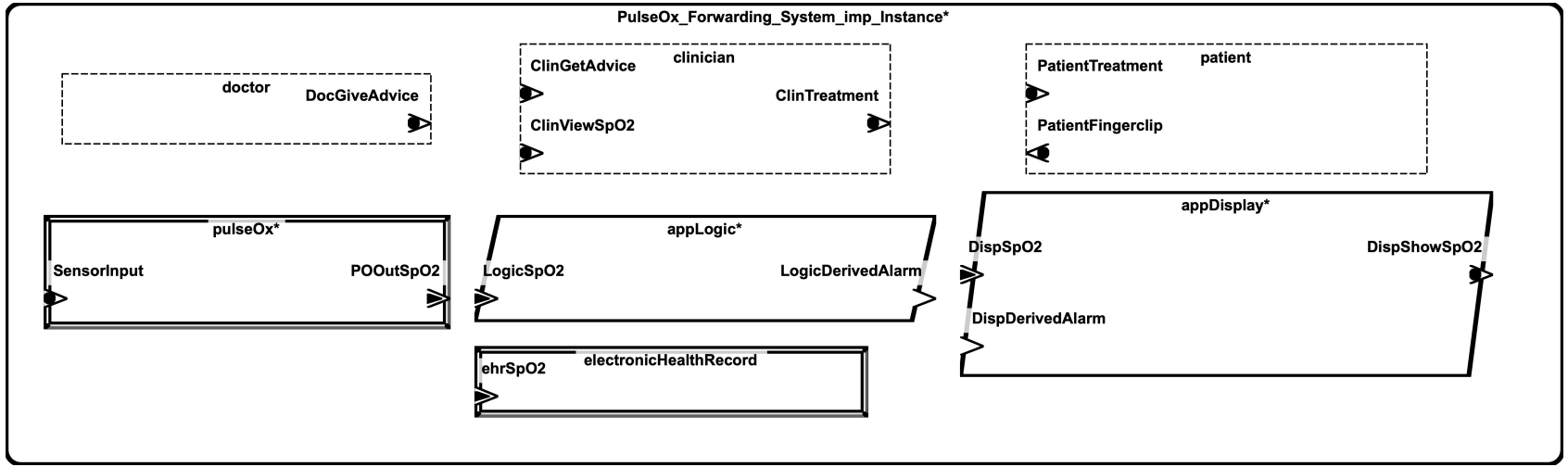


Pulse oximeter reads blood-oxygen saturation from a patient, monitoring software displays an alarm if values are out of expected range

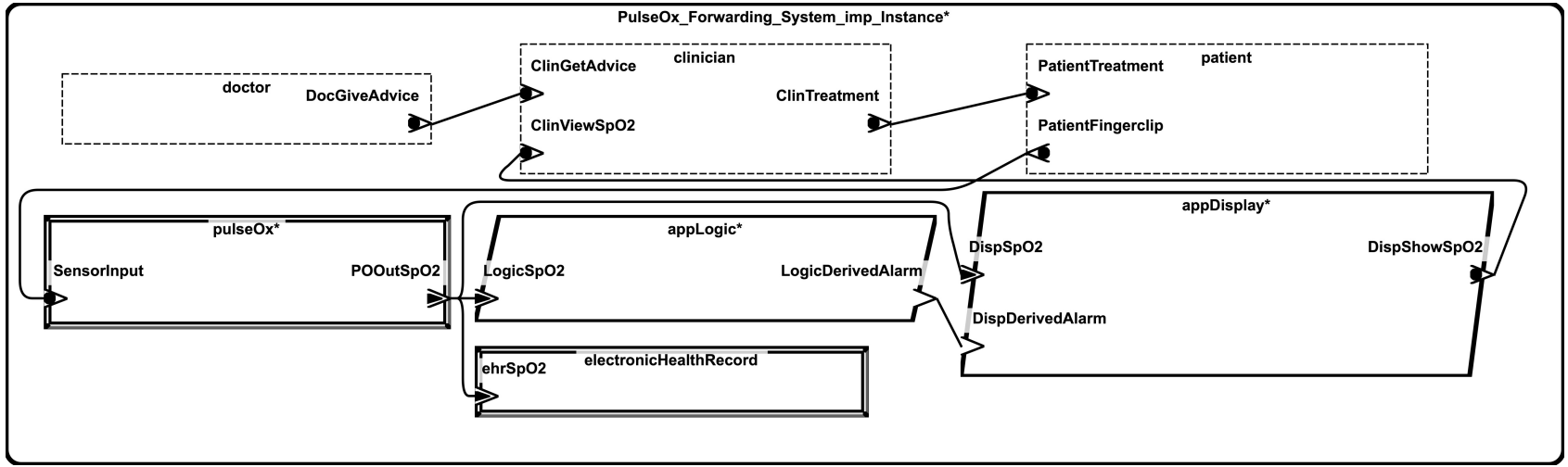
The PulseOx Forwarding Example



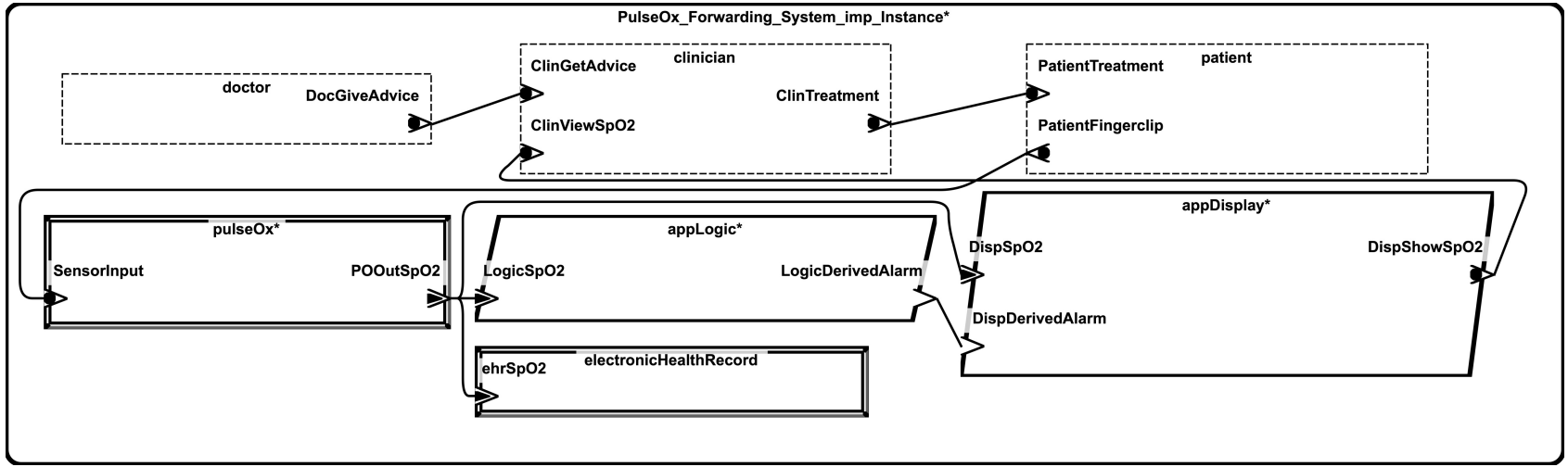
The PulseOx Forwarding Example



The PulseOx Forwarding Example

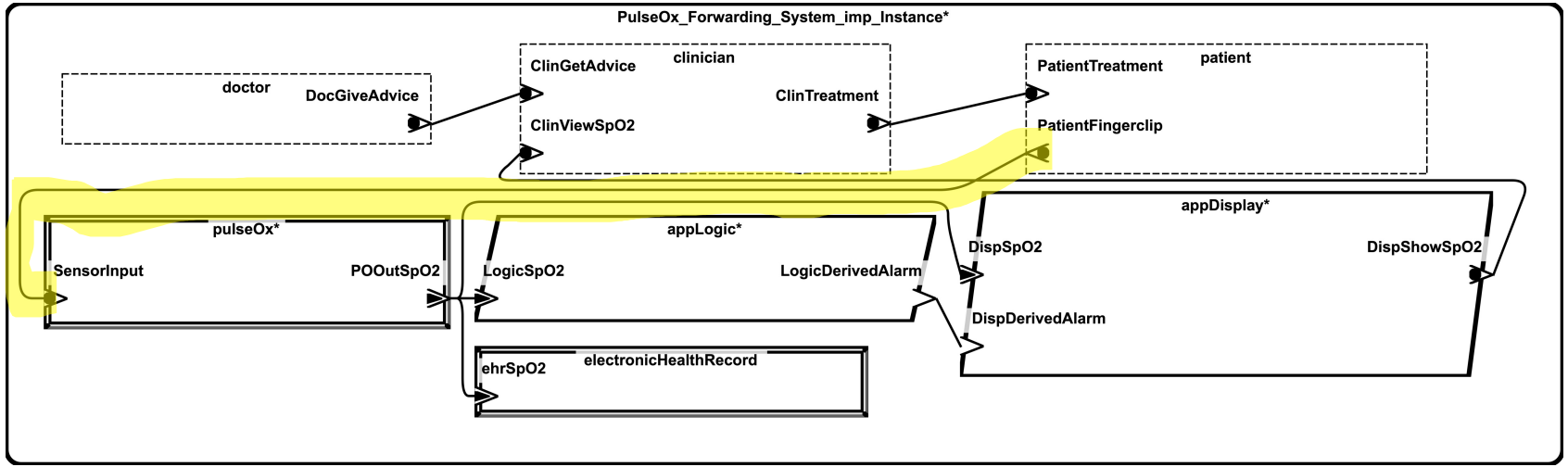


The PulseOx Forwarding Example



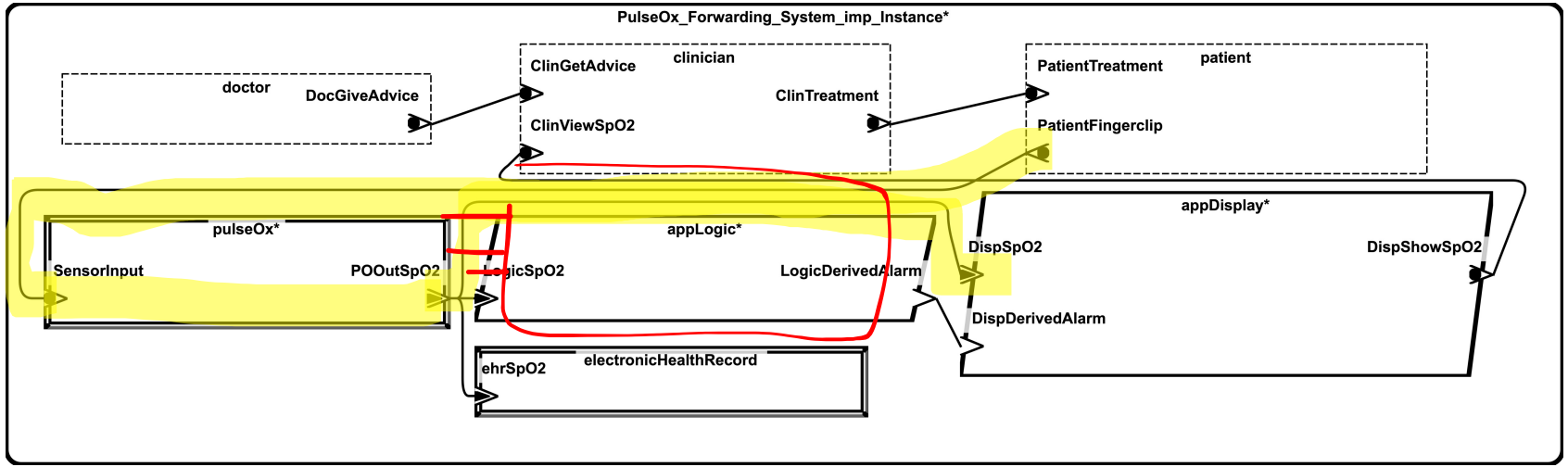
- Safety problem to avoid: Incorrect SpO_2 displayed

The PulseOx Forwarding Example



- Safety problem to avoid: Incorrect SpO_2 displayed

The PulseOx Forwarding Example



- Safety problem to avoid: Incorrect SpO_2 displayed
- AADL's "Error Modeling" (EMV2) annex can model these error propagations

STPA & SAFE

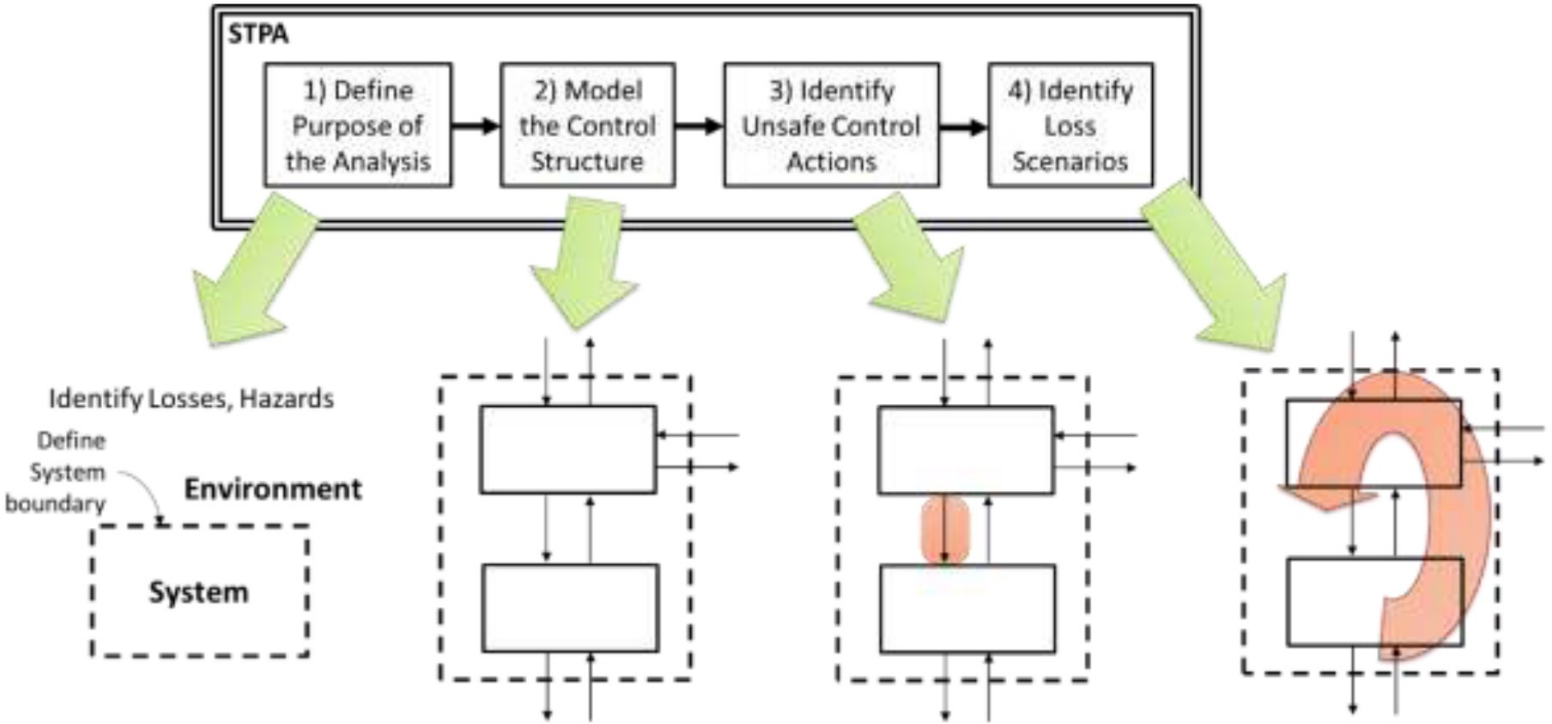


Figure 2.1: Overview of the basic STPA Method

© John Thomas, Nancy Leveson, STPA Handbook, March 2018
https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Outline

1. Background
2. **ASAP: Three Viewpoints**
    1. Fundamentals
    2. Connected Neighbors
    3. Unsafe Control Actions
3. Future Work

Viewpoint 1: Fundamentals

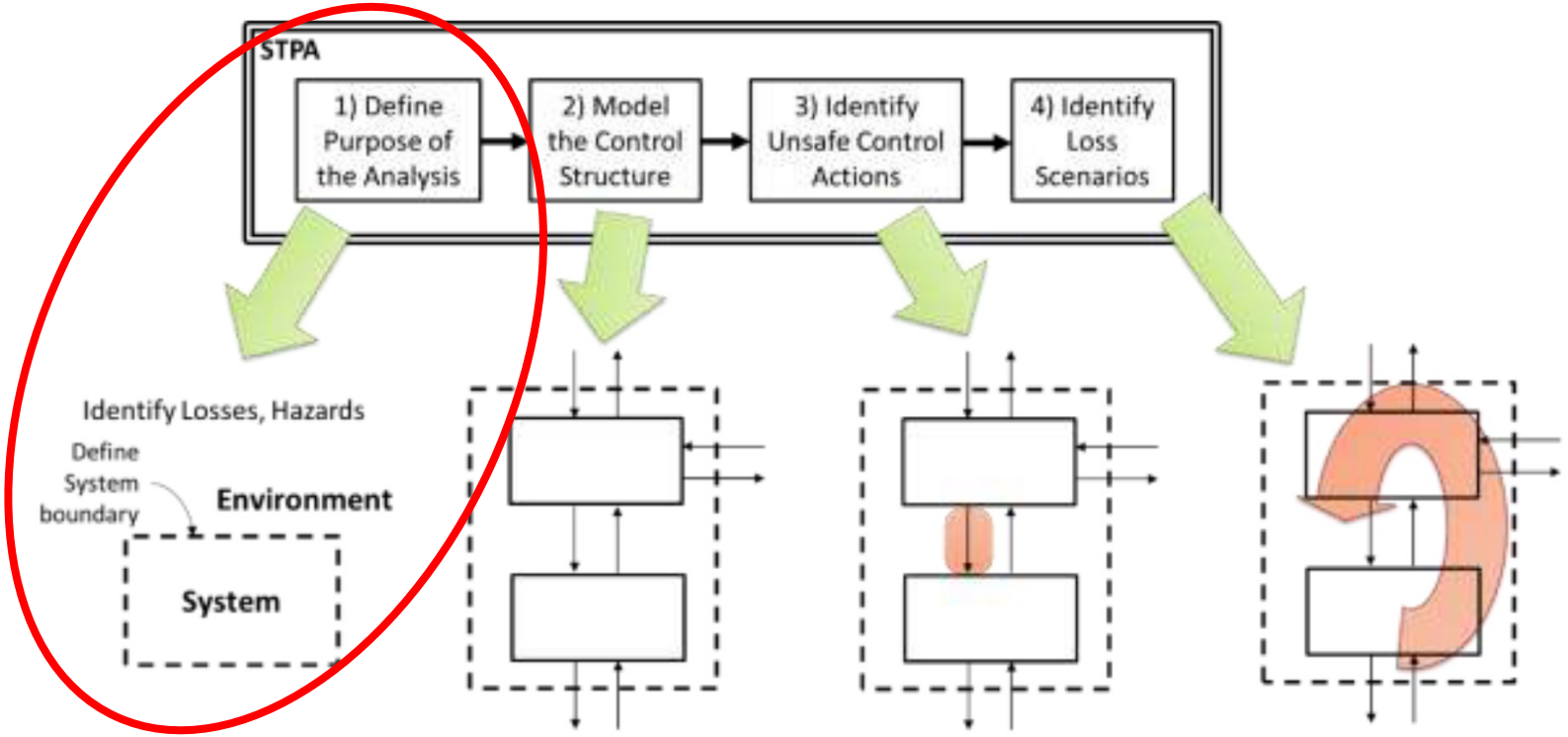


Figure 2.1: Overview of the basic STPA Method

© John Thomas, Nancy Leveson, STPA Handbook, March 2018
https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Viewpoint 1: Fundamentals (Hierarchy)

representations.aird | pulseox-forwarding.safe2 | new Fundamentals

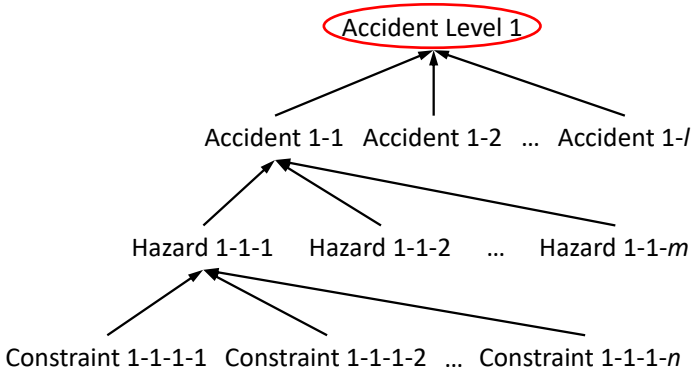
- DeathOrInjury
  - PatientHarmed
    - BadInfoDisplayed
      - ShowGoodInfo
    - InfoLate
      - ShowInfoOnTime

Problems | Properties | AADL Prop | Classifier In | Progress | Error Log

Hazard BadInfoDisplayed

Semantic

Property	Value
Hazard BadInfoDisplayed	
Accident	Accident PatientHarmed
Constraint	Constraint ShowGoodInfo
Description	Incorrect information is sent to the display
Environment Element	Abstract patient
Error Type	Error Type SpO2ValueHigh
Explanations	
Hazardous Factor	SpO2 Information
Name	BadInfoDisplayed
System Element	Event Data Port DispSpO2



Viewpoint 1: Fundamentals (Hierarchy)

representations.aird | pulseox-forwarding.safe2 | new Fundamentals

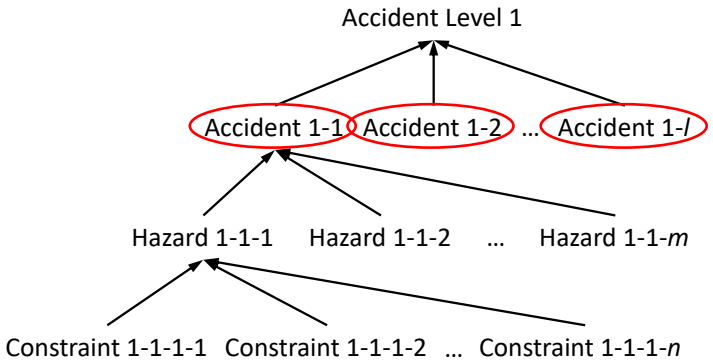
- DeathOrInjury
  - PatientHarmed
    - BadInfoDisplayed
      - ShowGoodInfo
    - InfoLate
      - ShowInfoOnTime

Problems | Properties | AADL Prop | Classifier In | Progress | Error Log

Hazard BadInfoDisplayed

Semantic

Property	Value
Hazard BadInfoDisplayed	
Accident	Accident PatientHarmed
Constraint	Constraint ShowGoodInfo
Description	Incorrect information is sent to the display
Environment Element	Abstract patient
Error Type	Error Type SpO2ValueHigh
Explanations	
Hazardous Factor	SpO2 Information
Name	BadInfoDisplayed
System Element	Event Data Port DispSpO2



Viewpoint 1: Fundamentals (Hierarchy)

representations.aird | pulseox-forwarding.safe2 | new Fundamentals

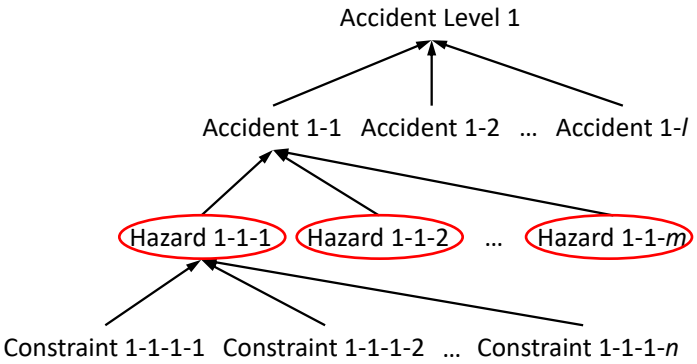
- DeathOrInjury
  - PatientHarmed
    - BadInfoDisplayed
      - ShowGoodInfo
    - InfoLate
      - ShowInfoOnTime

Problems | Properties | AADL Prop | Classifier In | Progress | Error Log

Hazard BadInfoDisplayed

Semantic

Property	Value
Hazard BadInfoDisplayed	
Accident	Accident PatientHarmed
Constraint	Constraint ShowGoodInfo
Description	Incorrect information is sent to the display
Environment Element	Abstract patient
Error Type	Error Type SpO2ValueHigh
Explanations	
Hazardous Factor	SpO2 Information
Name	BadInfoDisplayed
System Element	Event Data Port DispSpO2



Viewpoint 1: Fundamentals (Hierarchy)

representations.aird | pulseox-forwarding.safe2 | new Fundamentals

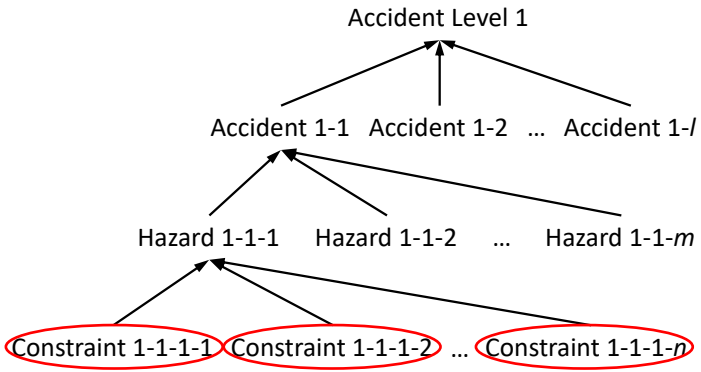
- DeathOrInjury
  - PatientHarmed
    - BadInfoDisplayed
      - ShowGoodInfo
    - InfoLate
      - ShowInfoOnTime

Problems | Properties | AADL Prop | Classifier In | Progress | Error Log

Hazard BadInfoDisplayed

Semantic

Property	Value
Hazard BadInfoDisplayed	
Accident	Accident PatientHarmed
Constraint	Constraint ShowGoodInfo
Description	Incorrect information is sent to the display
Environment Element	Abstract patient
Error Type	Error Type SpO2ValueHigh
Explanations	
Hazardous Factor	SpO2 Information
Name	BadInfoDisplayed
System Element	Event Data Port DispSpO2

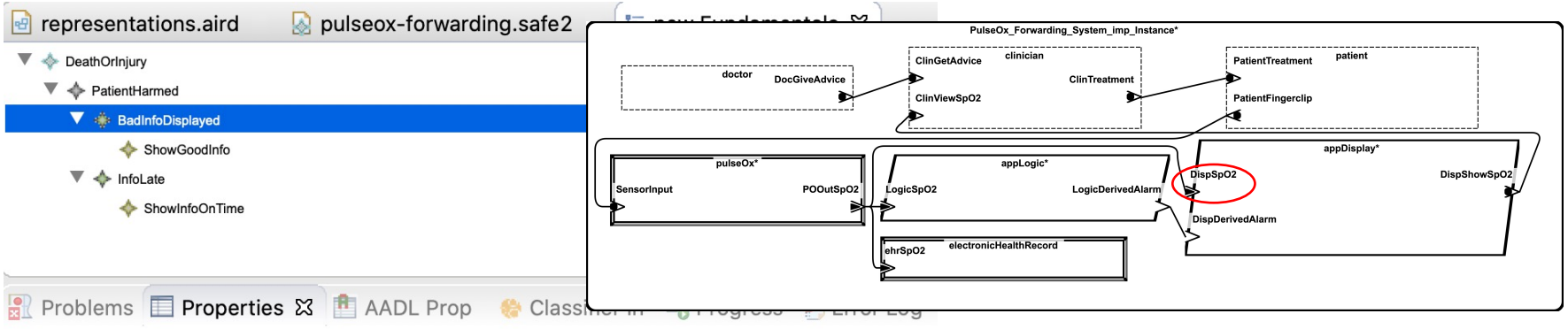


Viewpoint 1: Fundamentals

How can we tie our rather abstract fundamentals hierarchy to our very concrete system architecture?

SAFE (paraphrased, via STPA) uses the definition of a hazard: a system state, and a worst-case environment state.

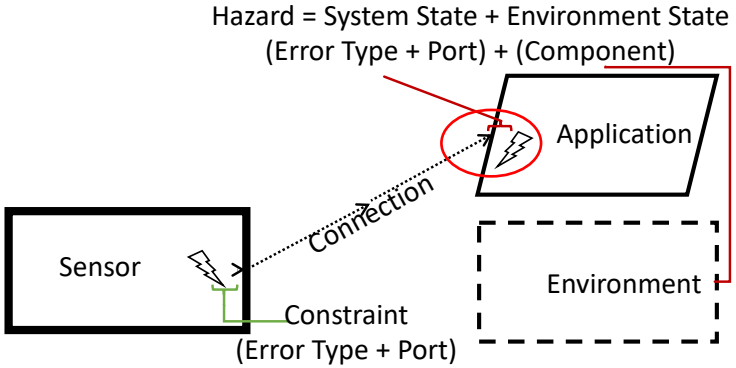
Viewpoint 1: Fundamentals (Link to system)



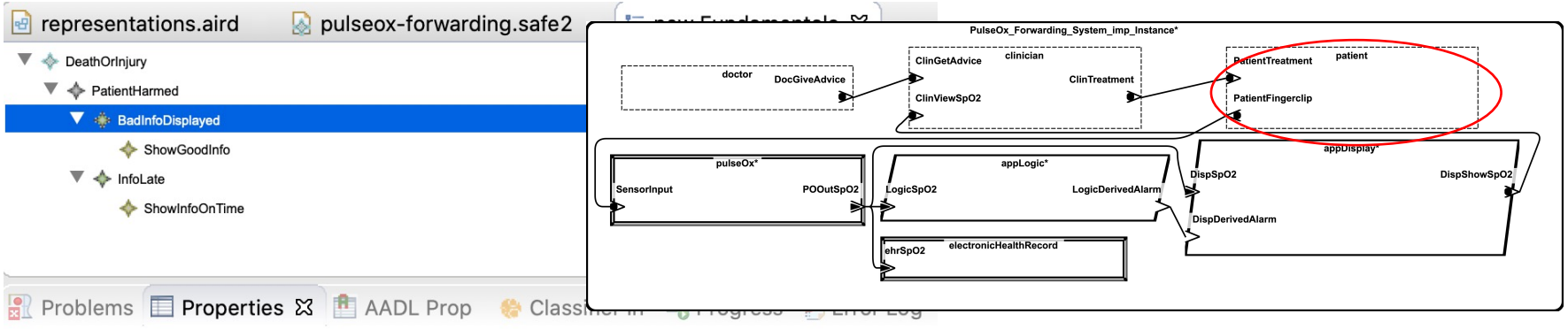
Hazard BadInfoDisplayed

Semantic

Property	Value
Hazard BadInfoDisplayed	
Accident	Accident PatientHarmed
Constraint	Constraint ShowGoodInfo
Description	Incorrect information is sent to the display
Environment Element	Abstract patient
Error Type	Error Type SpO2ValueHigh
Explanations	
Hazardous Factor	SpO2 Information
Name	BadInfoDisplayed
System Element	Event Data Port DispSpO2



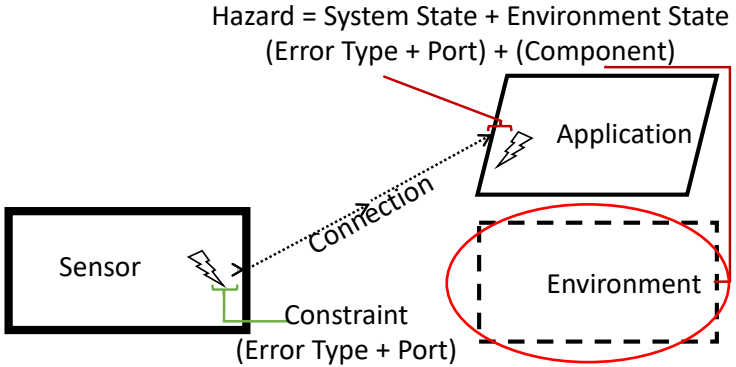
Viewpoint 1: Fundamentals (Link to system)



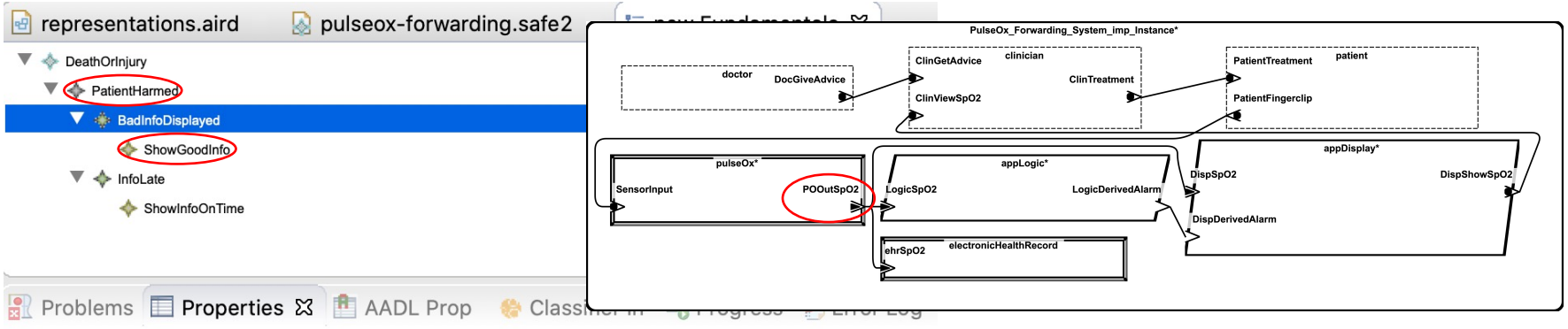
Hazard BadInfoDisplayed

Semantic

Property	Value
Hazard BadInfoDisplayed	
Accident	Accident PatientHarmed
Constraint	Constraint ShowGoodInfo
Description	Incorrect information is sent to the display
Environment Element	Abstract patient
Error Type	Error Type SpO2ValueHigh
Explanations	
Hazardous Factor	SpO2 Information
Name	BadInfoDisplayed
System Element	Event Data Port DispSpO2



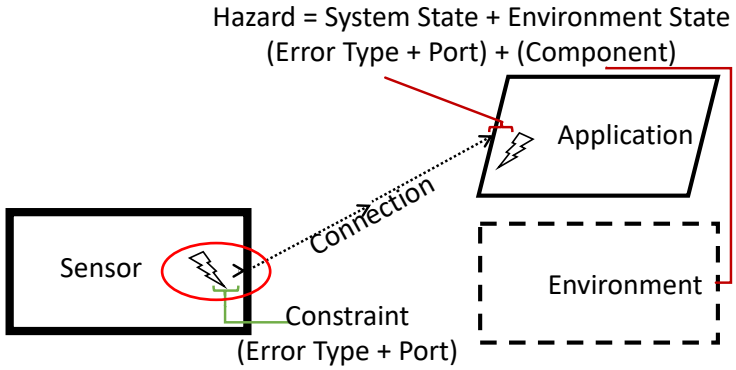
Viewpoint 1: Fundamentals (Link to system)



Hazard BadInfoDisplayed

Semantic

Property	Value
Hazard BadInfoDisplayed	
Accident	Accident PatientHarmed
Constraint	Constraint ShowGoodInfo
Description	Incorrect information is sent to the display
Environment Element	Abstract patient
Error Type	Error Type SpO2ValueHigh
Explanations	
Hazardous Factor	SpO2 Information
Name	BadInfoDisplayed
System Element	Event Data Port DispSpO2



Viewpoint 2: Connected Neighbors

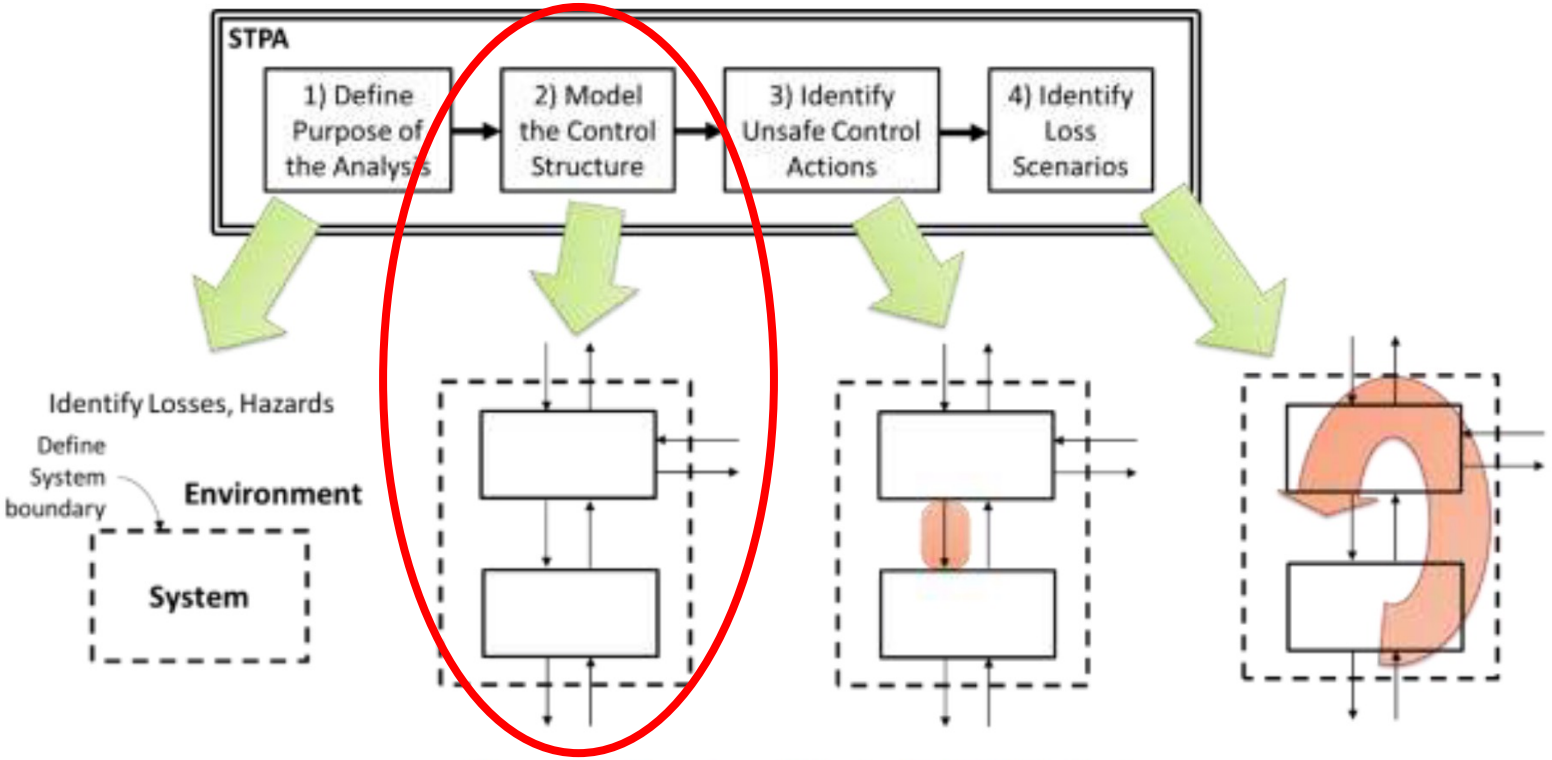
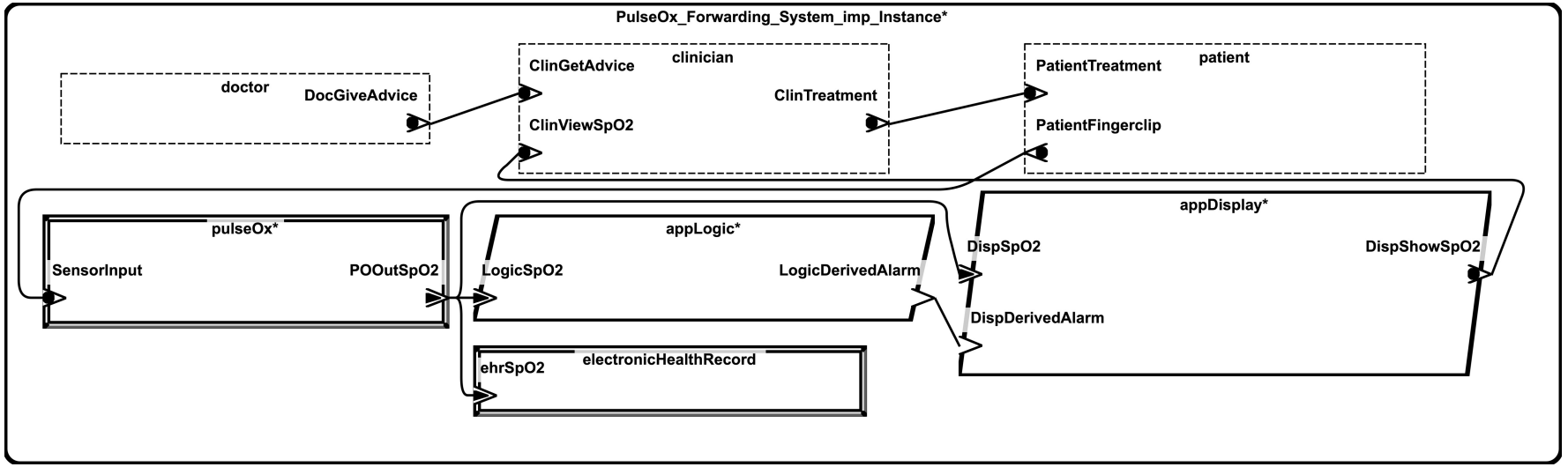


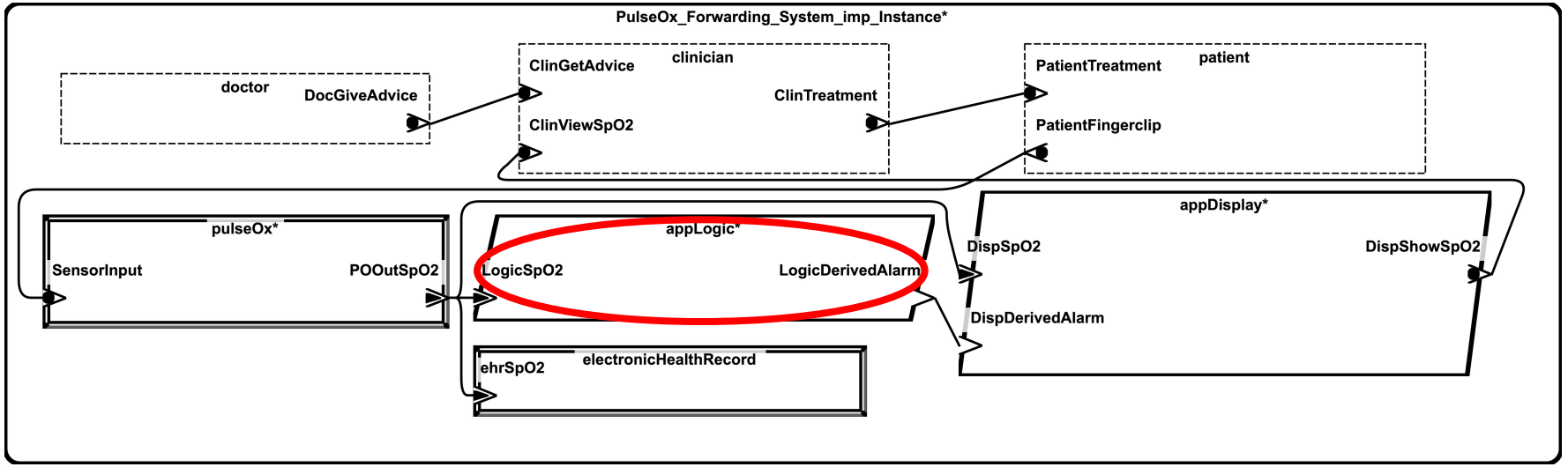
Figure 2.1: Overview of the basic STPA Method

© John Thomas, Nancy Leveson, STPA Handbook, March 2018
https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

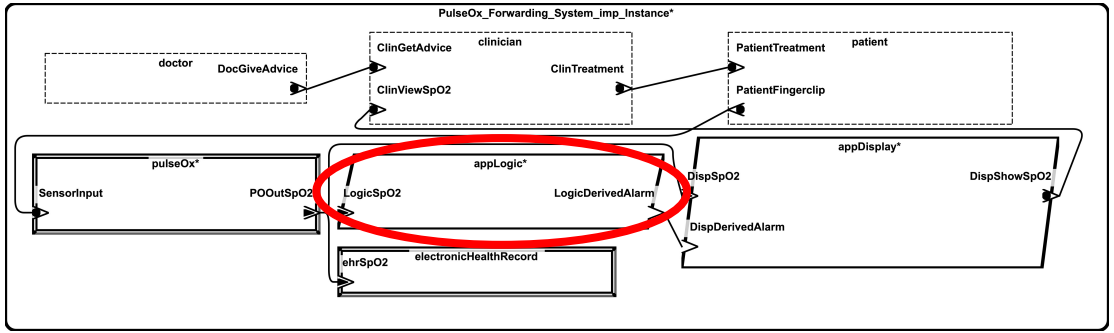
Viewpoint 2: Connected Neighbors

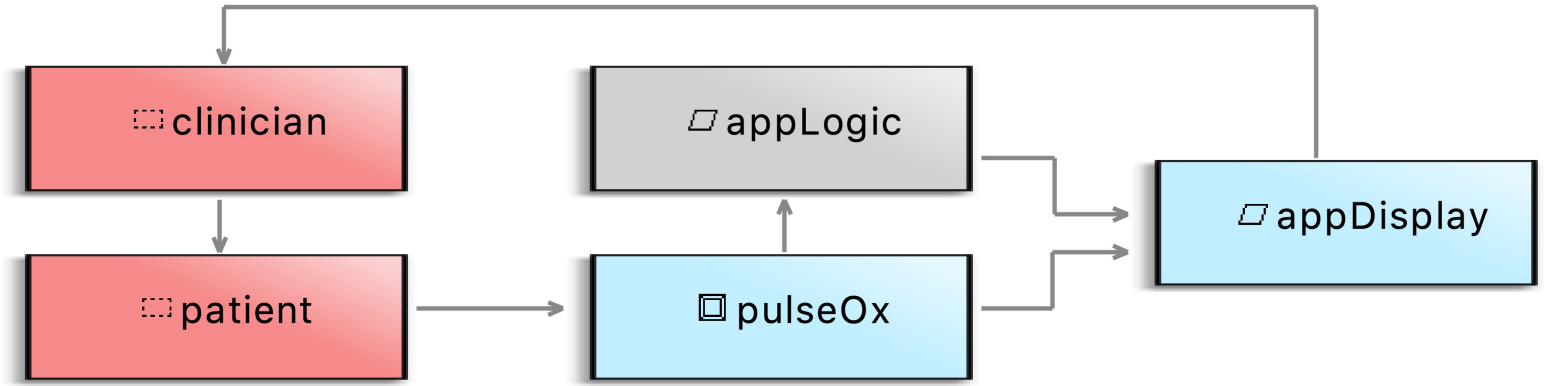


Viewpoint 2: Connected Neighbors



Viewpoint 2: Connected Neighbors





Viewpoint 3: Unsafe Control Actions

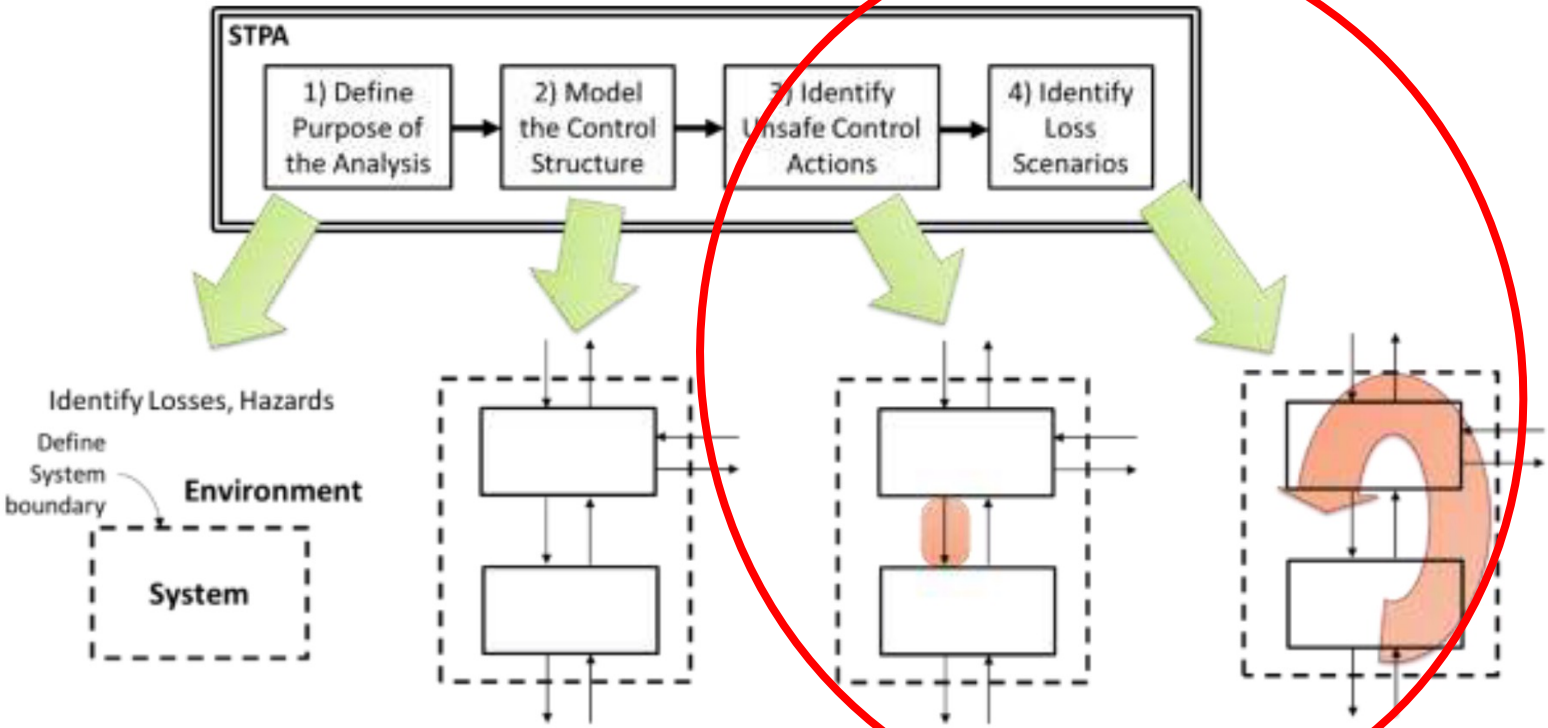
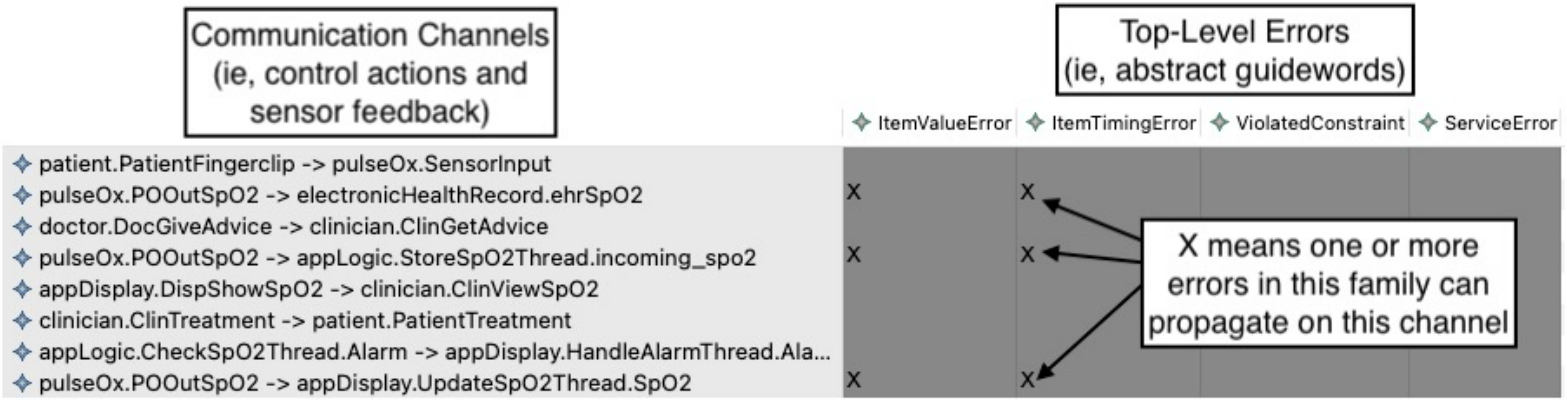


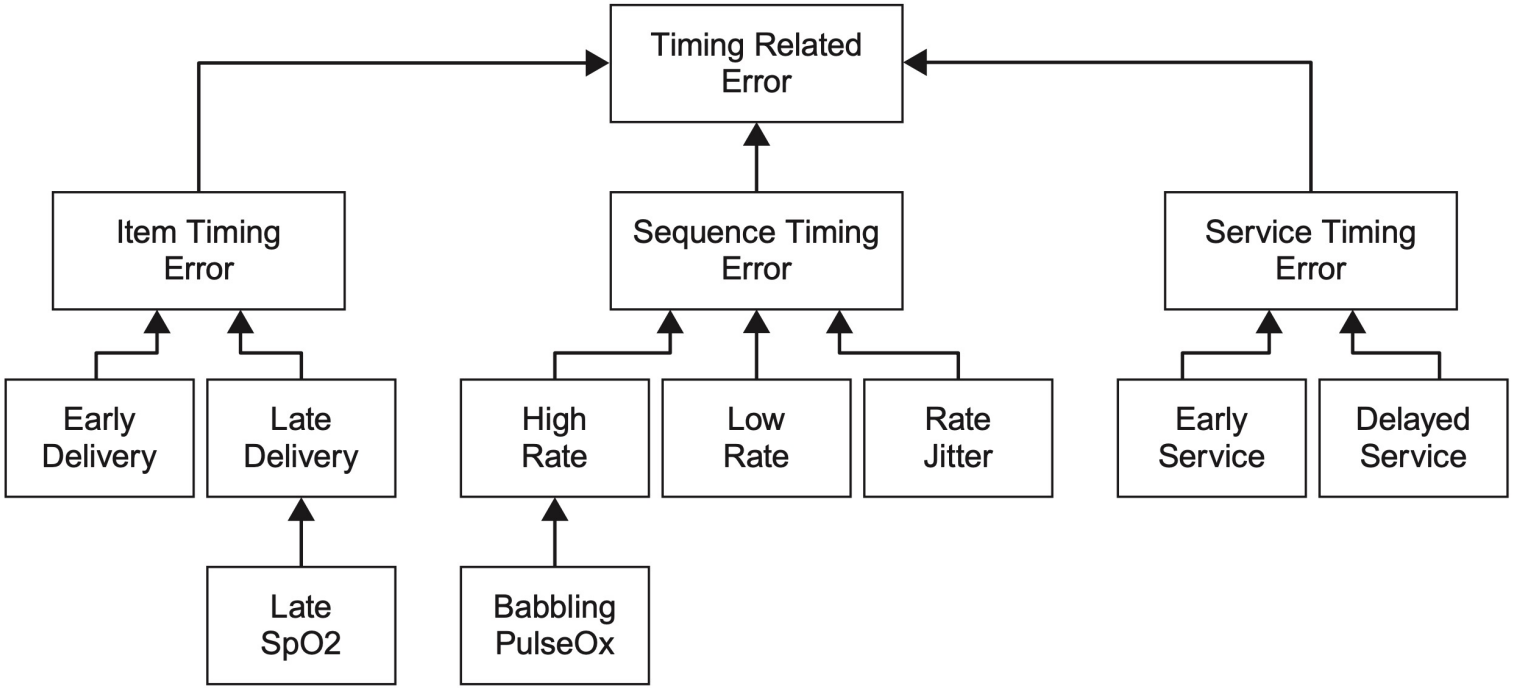
Figure 2.1: Overview of the basic STPA Method

© John Thomas, Nancy Leveson, STPA Handbook, March 2018
https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

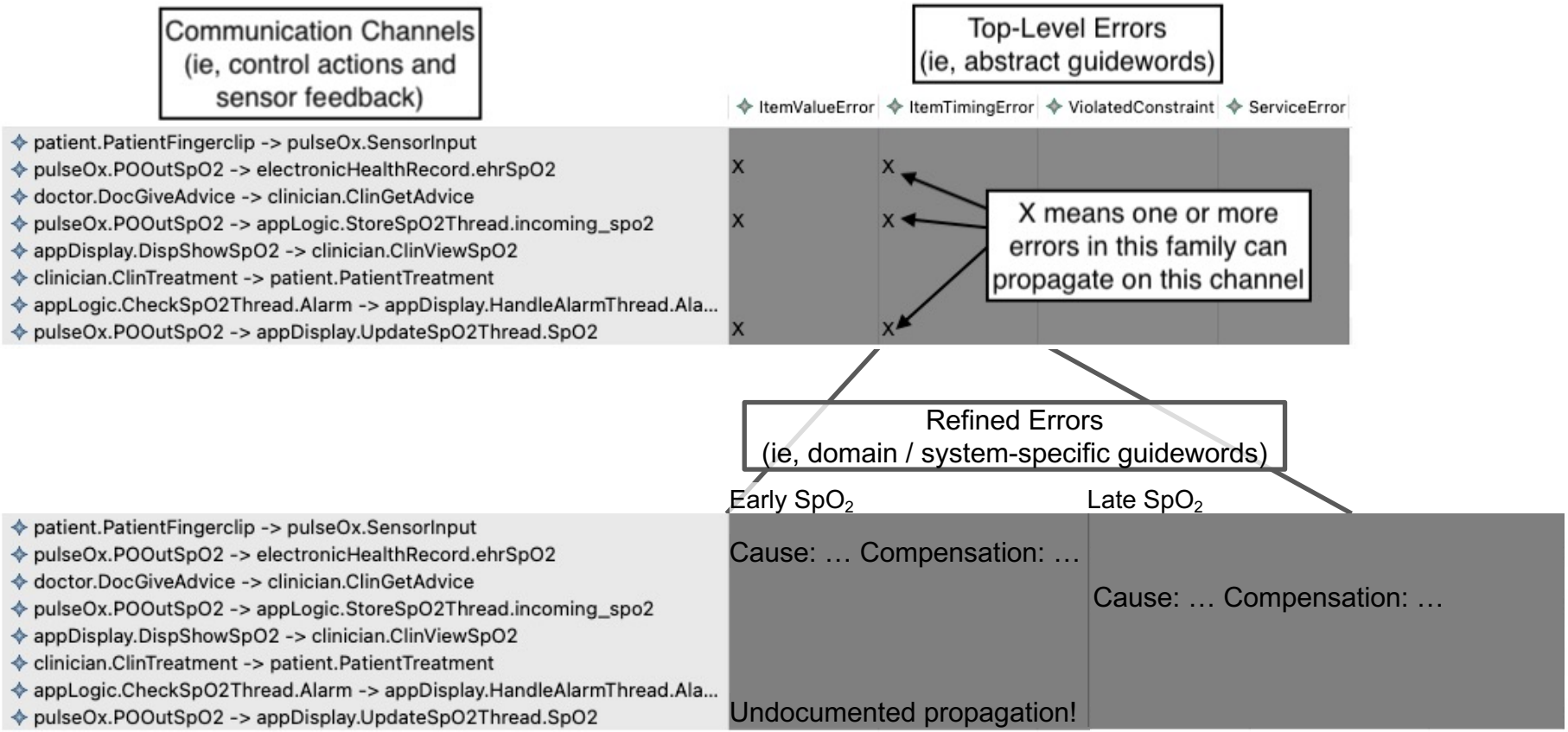
Viewpoint 3: Unsafe Control Actions



Interlude: The EMV2 Error Library



Viewpoint 3: Unsafe Control Actions



Outline

1. Background
2. ASAP: Three Viewpoints
3. **Future Work**

Future Work

1. The “Focus” Action
2. Discovering accident causation