Architecture-Supported Audit Processor

*Interactive, Query-Driven Assurance*

Sam Procter
Jerome Hugues

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
Document Markings

Copyright 2021 Carnegie Mellon University.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

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 SpO₂ displayed
The PulseOx Forwarding Example

• Safety problem to avoid: Incorrect SpO₂ displayed
The PulseOx Forwarding Example

- Safety problem to avoid: Incorrect SpO₂ displayed
- AADL’s “Error Modeling” (EMV2) annex can model these error propagations
Figure 2.1: Overview of the basic STPA Method

© John Thomas, Nancy Leveson, STPA Handbook, March 2018
https://psasscriptsmiteduhomegetfilephasenameSTPA_handbookpdf
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
**Viewpoint 1: Fundamentals (Hierarchy)**

```
<table>
<thead>
<tr>
<th>Accidents</th>
<th>Constraints</th>
<th>Hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accident 1-1</td>
<td>Constraint 1-1-1</td>
<td>Hazard 1-1-1</td>
</tr>
<tr>
<td>Accident 1-2</td>
<td>Constraint 1-1-1</td>
<td>Hazard 1-1-2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Accident 1-l</td>
<td>Constraint 1-1-1-n</td>
<td>Hazard 1-1-m</td>
</tr>
</tbody>
</table>
```

**Hazard BadInfoDisplayed**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accident PatientHarmened</td>
<td>☑</td>
</tr>
<tr>
<td>Constraint ShowGoodInfo</td>
<td>☑</td>
</tr>
<tr>
<td>Incorrect Information</td>
<td>☑</td>
</tr>
<tr>
<td>Abstract Patient</td>
<td>☑</td>
</tr>
<tr>
<td>Error Type SpO2ValueHigh</td>
<td>☑</td>
</tr>
<tr>
<td>BadInfoDisplayed</td>
<td>☑</td>
</tr>
<tr>
<td>Event Data Port DispSpO2</td>
<td>☑</td>
</tr>
</tbody>
</table>
Viewpoint 1: Fundamentals (Hierarchy)

Accident Level 1
- Accident 1-1
- Accident 1-2
- ... Accident 1-l

Hazard 1-1-1
- Hazard 1-1-2
- ... Hazard 1-1-m

Constraint 1-1-1-1
- Constraint 1-1-1-2
- ... Constraint 1-1-1-n

Hazard BadInfoDisplayed

<table>
<thead>
<tr>
<th>Semantic</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazard</td>
<td>BadInfoDisplayed</td>
<td></td>
</tr>
<tr>
<td>Accident</td>
<td></td>
<td>Accident PatientHarmend</td>
</tr>
<tr>
<td>Constraint</td>
<td></td>
<td>Constraint ShowGoodInfo</td>
</tr>
<tr>
<td>Description</td>
<td></td>
<td>Incorrect information is sent to the display</td>
</tr>
<tr>
<td>Environment</td>
<td>Element</td>
<td>Abstract patient</td>
</tr>
<tr>
<td>Error Type</td>
<td></td>
<td>Error Type SpO2ValueHigh</td>
</tr>
<tr>
<td>Explanations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hazardous Factor</td>
<td></td>
<td>SpO2 Information</td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td>BadInfoDisplayed</td>
</tr>
<tr>
<td>System Element</td>
<td></td>
<td>Event Data Port DispSpO2</td>
</tr>
</tbody>
</table>
Viewpoint 1: Fundamentals (Hierarchy)

Hazard BadInfoDisplayed

<table>
<thead>
<tr>
<th>Semantic</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazard BadInfoDisplayed</td>
<td>Accident</td>
<td>Accident PatientHarmed</td>
</tr>
<tr>
<td></td>
<td>Constraint</td>
<td>Constraint ShowGoodInfo</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Incorrect information is sent to the display</td>
</tr>
<tr>
<td></td>
<td>Environment Element</td>
<td>Abstract patient</td>
</tr>
<tr>
<td></td>
<td>Error Type</td>
<td>Error Type SpO2ValueHigh</td>
</tr>
<tr>
<td></td>
<td>Explanations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hazardous Factor</td>
<td>SpO2 Information</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>BadInfoDisplayed</td>
</tr>
<tr>
<td></td>
<td>System Element</td>
<td>Event Data Port DispSpO2</td>
</tr>
</tbody>
</table>
### Viewpoint 1: Fundamentals (Hierarchy)

**Accident Level 1**

- Accident 1-1
- Accident 1-2...
- Accident 1-l

**Hazard 1-1-1**
- Hazard 1-1-2...
- Hazard 1-1-m

**Constraint 1-1-1-1**
- Constraint 1-1-1-2...
- Constraint 1-1-1-n

#### Hazard BadInfoDisplayed

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Incorrect information is sent to the display</td>
</tr>
<tr>
<td>Environment Element</td>
<td>Abstract patient</td>
</tr>
<tr>
<td>Error Type</td>
<td>Error Type SpO2ValueHigh</td>
</tr>
<tr>
<td>Explanations</td>
<td></td>
</tr>
<tr>
<td>Hazardous Factor</td>
<td>SpO2 Information</td>
</tr>
<tr>
<td>Name</td>
<td>BadInfoDisplayed</td>
</tr>
<tr>
<td>System Element</td>
<td>Event Data Port DispSpO2</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Semantic</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazard BadInfoDisplayed</td>
<td>Accident</td>
<td>Accident PatientHarmmed</td>
</tr>
<tr>
<td></td>
<td>Constraint</td>
<td>Constraint ShowGoodInfo</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Incorrect information is sent to the display</td>
</tr>
<tr>
<td></td>
<td>Environment Element</td>
<td>Abstract patient</td>
</tr>
<tr>
<td></td>
<td>Error Type</td>
<td>Error Type SpO2ValueHigh</td>
</tr>
<tr>
<td></td>
<td>Explanations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hazardous Factor</td>
<td>SpO2 Information</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>BadInfoDisplayed</td>
</tr>
<tr>
<td></td>
<td>System Element</td>
<td>Event Data Port DispSpO2</td>
</tr>
</tbody>
</table>

Hazard = System State + Environment State
(Error Type + Port) + (Component)

Sensor

Connection

Environment

Constraint

(Error Type + Port)
Viewpoint 1: Fundamentals (Link to system)

Hazard BadInfoDisplayed

<table>
<thead>
<tr>
<th>Semantic</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>Value</td>
</tr>
<tr>
<td>Hazard BadInfoDisplayed</td>
<td>Accident PatientHarmed</td>
</tr>
<tr>
<td>Accident</td>
<td>Constraint ShowGoodInfo</td>
</tr>
<tr>
<td>Constraint</td>
<td>Incorrect information is sent to the display</td>
</tr>
<tr>
<td>Description</td>
<td>Abstract patient</td>
</tr>
<tr>
<td>Environment Element</td>
<td>Error Type SpO2ValueHigh</td>
</tr>
<tr>
<td>Error Type</td>
<td>Explanations</td>
</tr>
<tr>
<td>Hazardous Factor</td>
<td>Name BadInfoDisplayed</td>
</tr>
<tr>
<td>System Element</td>
<td>Event Data Port DispSpO2</td>
</tr>
</tbody>
</table>

Hazard = System State + Environment State
(Error Type + Port) + (Component)
Viewpoint 1: Fundamentals (Link to system)

Hazard = System State + Environment State
(Error Type + Port) + (Component)
Viewpoint 2: Connected Neighbors

Figure 2.1: Overview of the basic STPA Method
© John Thomas, Nancy Leveson, STPA Handbook, March 2018
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
Viewpoint 3: Unsafe Control Actions

Communication Channels (ie, control actions and sensor feedback)

- patient.PatientFingercip \rightarrow pulseOx.SensorInput
- pulseOx.PO0utSpO2 \rightarrow electronicHealthRecord.ehrSpO2
- pulseOx.PO0utSpO2 \rightarrow appLogic.StoreSpO2Thread.incoming_spo2
- appDisplay.DispShowSpO2 \rightarrow clinician.ClinViewSpO2
- clinician.ClinTreatment \rightarrow patient.PatientTreatment
- appLogic.CheckSpO2Thread.Alarm \rightarrow appDisplay.HandleAlarmThread.Alar...
- pulseOx.PO0utSpO2 \rightarrow appDisplay.UpdateSpO2Thread.SpO2

Top-Level Errors (ie, abstract guidewords)

- ItemValueError
- ItemTimingError
- ViolatedConstraint
- ServiceError

X means one or more errors in this family can propagate on this channel
Interlude: The EMV2 Error Library

Timing Related Error

Item Timing Error
- Early Delivery
- Late Delivery
- Late SpO2

Sequence Timing Error
- High Rate
- Low Rate
- Rate Jitter
- Babbling Pulse Ox

Service Timing Error
- Early Service
- Delayed Service
Viewpoint 3: Unsafe Control Actions

**Communication Channels (ie, control actions and sensor feedback)**
- patient.PatientFingercip -> pulseOx.SensorInput
- pulseOx.POOutSpO2 -> electronicHealthRecord.ehrSpO2
- pulseOx.POOutSpO2 -> appLogic.StoreSpO2Thread.incoming_spO2
- appLogic.CheckSpO2Thread.Alarm -> appDisplay.HandleAlarmThread.Ala...
- pulseOx.POOutSpO2 -> appDisplay.UpdateSpO2Thread.SpO2

**Top-Level Errors (ie, abstract guidewords)**
- ItemValueError
- ItemTimingError
- ViolatedConstraint
- ServiceError

**Refined Errors (ie, domain / system-specific guidewords)**

- Early SpO2
  - Cause: ...
  - Compensation: ...

- Late SpO2
  - Cause: ...
  - Compensation: ...

Undocumented propagation!
Outline

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

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