Transportation Systems

Safety HAT

Hazard Analysis Tool

Volpe
The National Transportation Systems Center
What is SafetyHAT?

• A software tool that facilitates hazard analysis using STPA

• Customized for transportation systems
Why Use SafetyHAT?

• Enter data using a streamlined, wizard-like format.

• Use a relational database to store, manage, and organize data.

• Facilitate documentation of your hazard analysis.
How Does SafetyHAT Work?

Welcome to the Transportation Systems Safety Hazard Analysis Tool (SafetyHAT). This tool will guide you through hazard analysis using the System-Theoretic Process Analysis (STPA) method.

Please complete the Preparatory Steps before accessing the forms below. The Preparatory Steps can be reviewed using the "Review Preparatory Steps" button at the bottom of this screen. A control structure diagram can be uploaded using the "Upload Control Structure Diagram" button at the bottom of this screen.

Complete the forms in the order presented below to ensure a complete analysis.

**Enter System Information**

1. **Components**
   - This form allows you to enter the components of your system.

2. **Connections**
   - This form allows you to enter connections between the components of your system.

3. **Control Actions**
   - This form allows you to enter specific Control Actions issued by controllers in your system.

**Conduct Analysis**

4. **Accidents or Losses**
   - This form will allow you to enter accidents (or losses) specific to your system.

5. **Hazards**
   - This form will allow you to enter hazards specific to your system.

6. **Unsafe Control Action Analysis**
   - This form will guide you through evaluating Unsafe Control Actions and potentially related system hazards.

7. **Causal Factor Analysis**
   - This form will guide you through evaluating Unsafe Control Actions and potential causal factors.

**Export Analysis**

8. **Export Data**
   - This will compile the STPA results and export the data to MS Excel.

---

Volpe The National Transportation Systems Center
SafetyHAT uses an eight step process to guide users through STPA

Main Menu

Welcome to the Transportation Systems Safety Hazard Analysis Tool (SafetyHAT). This tool will guide you through hazard analysis using the System-Theoretic Process Analysis (STPA) method.

Please complete the Preparatory Step by clicking on the "Next" button at the bottom of this screen. A control structure diagram will be uploaded using the "Upload Control Structure Diagram" button at the bottom of this screen.

Complete the forms in the order presented below to ensure a complete analysis.

1. **Describe your system**
   - **Components**
     - This form allows you to enter the components of your system.
   - **Connections**
     - This form allows you to enter connections between the components of your system.
   - **Control Actions**
     - This form allows you to enter specific Control Actions issued by controllers in your system.

2. **Analyze your system**
   - **Accidents or Losses**
     - This form will allow you to enter accidents (or losses) specific to your system.
   - **Hazards**
     - This form will allow you to enter hazards specific to your system.
   - **Unsafe Control Action Analysis**
     - This form will guide you through evaluating Unsafe Control Actions and potentially related system hazards.
   - **Causal Factor Analysis**
     - This form will guide you through evaluating Unsafe Control Actions and potential causal factors.

3. **Export your analysis**
   - **Export Data**
     - This will compile the STPA results and export the data to MS Excel.
   - **Advanced Options**
   - **Review Preparatory Steps**
   - **Upload Control Structure Diagram**
   - **Locate Additional STPA Resources**
SafetyHAT’s preloaded transportation-specific guide phrases can be customized for other domains.
Welcome to the Transportation Systems Safety Hazard Analysis Tool (SafetyHAT). This tool will guide you through hazard analysis using the System-Theoretic Process Analysis (STPA) method.

Please complete the Preparatory Steps before accessing the forms below. The Preparatory Steps can be reviewed using the "Review Preparatory Steps" button at the bottom of this screen. A control structure diagram can be uploaded using the "Upload Control Structure Diagram" button at the bottom of this screen.

Complete the forms in the order presented below to ensure a complete analysis.

1. **Components**
   - This form allows you to enter the components of your system.
2. **Connections**
   - This form allows you to enter connections between the components of your system.
3. **Control Actions**
   - This form allows you to enter specific Control Actions issued by controllers in your system.

**Conduct Analysis**

4. **Accidents or Losses**
   - This form will allow you to enter accidents (or losses) specific to your system.
5. **Hazard**
   - This form will allow you to enter hazards specific to your system.
6. **Unsafe Control Action Analysis**
   - This form will guide you through evaluating Unsafe Control Actions and potentially related system hazards.
7. **Causal Factor Analysis**
   - This form will guide you through evaluating Unsafe Control Actions and potential causal factors.

**Export Analysis**

8. **Export Data**
   - This will compile the STPA results and export the data to MS Excel.
All data entry and analysis forms share basic features.

The navigation bar allows you to move easily between data entry forms.
All data entry and analysis forms share basic features

Review entered data ...

...and add, modify, or delete data
All data entry and analysis forms share basic features.

Description boxes let you enter additional details about your system.
Step 1 allows you to enter and modify component information.

Use the navigation bar to move sequentially between steps.
Step 2 allows you to enter and modify connections between components.
Step 2 allows you to enter and modify connections between components.

SafetyHAT uses information about your system to simplify data entry.
Step 3 allows you to enter control actions issued by system controllers.
Step 4 allows you to enter system-level accidents.
Step 5 allows you to enter system-level hazards.

Hazards can be linked to one or more system-level accidents.
Step 6 guides you through analysis of Unsafe Control Actions.
Step 6 guides you through analysis of Unsafe Control Actions

SafetyHAT comes preloaded with six UCA guide phrases
Step 7 guides you through the causal factor analysis
Step 7 guides you through the causal factor analysis

SafetyHAT is preloaded with 26 causal factor guide phrases
Step 8 lets you export data to a Microsoft Excel spreadsheet.
The exported spreadsheet summarizes the data you entered into Safety HAT.

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>COMPONENT_NAME</th>
<th>COMPONENT_DESC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actuator</td>
<td>Air Bag Control Unit</td>
<td>Main controller for the system. Also referred to as the Sensing and Diagnostic Module.</td>
</tr>
<tr>
<td>Actuator</td>
<td>Air Bag Module</td>
<td>Includes squib, inflator, ignitor, diffusor, tether, bag, etc.</td>
</tr>
<tr>
<td>Actuator</td>
<td>Passenger Air Bag Button</td>
<td>Button that manually enables or disables the passenger air bag.</td>
</tr>
<tr>
<td>Actuator</td>
<td>Passenger Air Bag Indicator Light</td>
<td>Dashboard display alerting driver to the status of the passenger air bag.</td>
</tr>
<tr>
<td>Actuator</td>
<td>Seat Belt Pretensioner</td>
<td>Electrically ignited pyrotechnic charges that cause retraction of the seatbelt around the occupant.</td>
</tr>
<tr>
<td>Controlled Process</td>
<td>Vehicle (including Occupants)</td>
<td>Air bags are designed to protect the seated occupants.</td>
</tr>
<tr>
<td>Controller</td>
<td>Air Bag Control Unit</td>
<td>Main controller for the system. Also referred to as the Sensing and Diagnostic Module.</td>
</tr>
<tr>
<td>Controller</td>
<td>Driver</td>
<td>Driver of the vehicle</td>
</tr>
<tr>
<td>Controller</td>
<td>Passenger Presence Sensing Module</td>
<td>Calculates passenger weight and position, and determines whether passenger air bag should be disabled.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Crash Sensor</td>
<td>Mechanical or electronic sensors designed to detect sudden vehicle deceleration.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Passenger Air Bag Button</td>
<td>Button that manually enables or disables the passenger air bag.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Passenger Air Bag Indicator Light</td>
<td>Dashboard display alerting driver to the status of the passenger air bag.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Passenger Presence Sensor</td>
<td>Fluid bladder or strain gauge type sensors that detect occupants position and weight.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Seat Belt Tension Sensor</td>
<td>Secondary sensor used to help classify occupant's position and weight.</td>
</tr>
</tbody>
</table>
Automatically produce the spreadsheet that links accidents to causal factors

<table>
<thead>
<tr>
<th>ACC_NO</th>
<th>ACCIDENT</th>
<th>HAZ_NO</th>
<th>UCA_NO</th>
<th>COMPONENT_NAME</th>
<th>UCA_DESC</th>
<th>CAUSAL_FACT_NO</th>
<th>CF_USER_DESC</th>
<th>FROM_COMP</th>
<th>TO_COMP</th>
<th>CATEGORY</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Vehicle Occupant Injury or Death</td>
<td>H1</td>
<td>UCA2</td>
<td>Air Bag Control Unit</td>
<td>Air bag does not deploy when the vehicle is in a sufficiently severe crash.</td>
<td>CF1</td>
<td>Interaction with electrical system causes air bag to deploy when key is turned to “on” position.</td>
<td>Air Bag Control Unit</td>
<td></td>
<td>Controller</td>
</tr>
<tr>
<td>A2</td>
<td>Vehicle Occupant Injury or Death</td>
<td>H1</td>
<td>UCA2</td>
<td>Air Bag Control Unit</td>
<td>Air bag does not deploy when the vehicle is in a sufficiently severe crash.</td>
<td>CF2</td>
<td>Short circuit due to condensation from A/C system.</td>
<td>Air Bag Control Unit</td>
<td></td>
<td>Controller</td>
</tr>
<tr>
<td>A3</td>
<td>Vehicle Occupant Injury or Death</td>
<td>H1</td>
<td>UCA2</td>
<td>Air Bag Control Unit</td>
<td>Air bag does not deploy when the vehicle is in a sufficiently severe crash.</td>
<td>CF3</td>
<td>Manufacturing error with Application Specific Integrated Circuit (ASIC) causes air bag to deploy.</td>
<td>Air Bag Control Unit</td>
<td></td>
<td>Controller</td>
</tr>
<tr>
<td>A4</td>
<td>Vehicle Occupant Injury or Death</td>
<td>H1</td>
<td>UCA2</td>
<td>Air Bag Control Unit</td>
<td>Air bag does not deploy when the vehicle is in a sufficiently severe crash.</td>
<td>CF4</td>
<td>Delamination of internal subcomponents causes air bag to deploy.</td>
<td>Air Bag Control Unit</td>
<td></td>
<td>Controller</td>
</tr>
<tr>
<td>A5</td>
<td>Vehicle Occupant Injury or Death</td>
<td>H1</td>
<td>UCA2</td>
<td>Air Bag Control Unit</td>
<td>Air bag does not deploy when the vehicle is in a sufficiently severe crash.</td>
<td>CF5</td>
<td>Short circuit in wiring between crash sensor and the Air Bag Control Unit causes air bag to deploy.</td>
<td>Air Bag Control Unit</td>
<td></td>
<td>Controller</td>
</tr>
<tr>
<td>A6</td>
<td>Vehicle Occupant Injury or Death</td>
<td>H1</td>
<td>UCA2</td>
<td>Air Bag Control Unit</td>
<td>Air bag does not deploy when the vehicle is in a sufficiently severe crash.</td>
<td>CF6</td>
<td>Shear forces on component causes air bag to deploy.</td>
<td>Air Bag Control Unit</td>
<td></td>
<td>Controller</td>
</tr>
<tr>
<td>A7</td>
<td>Vehicle Occupant Injury or Death</td>
<td>H1</td>
<td>UCA2</td>
<td>Air Bag Control Unit</td>
<td>Air bag does not deploy when the vehicle is in a sufficiently severe crash.</td>
<td>CF7</td>
<td>Short circuit in wiring between crash sensor and the Air Bag Control Unit causes air bag to deploy.</td>
<td>Air Bag Control Unit</td>
<td></td>
<td>Controller</td>
</tr>
<tr>
<td>A8</td>
<td>Vehicle Occupant Injury or Death</td>
<td>H1</td>
<td>UCA2</td>
<td>Air Bag Control Unit</td>
<td>Air bag does not deploy when the vehicle is in a sufficiently severe crash.</td>
<td>CF8</td>
<td>Shear forces on component causes air bag to deploy.</td>
<td>Air Bag Control Unit</td>
<td></td>
<td>Controller</td>
</tr>
</tbody>
</table>

The spreadsheet is currently produced by hand!
How Do I Get SafetyHAT?

• SafetyHAT is available for public use and can be downloaded for free

• Visit [http://www.volpe.dot.gov/SafetyHAT](http://www.volpe.dot.gov/SafetyHAT) and register to receive a download link