SafetyHAT

A Transportation Systems Safety Hazard Analysis Tool

March 26, 2014

The National Transportation Systems Center
Advancing transportation innovation for the public good

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
John A. Volpe National Transportation Systems Center
Overview

- Why SafetyHAT
- SafetyHAT Walkthrough
- Benefits from Using SafetyHAT
- How to get SafetyHAT
- Future Possibilities
Simple Mechanical Systems

Distributed Complex Sociotechnical Systems
Component Failure, Software Errors, Unsafe System Interactions, Complex Dynamic Process, Human Factors

- 1931 Domino Model
- 1949 Failure Modes and Effects Analysis
- 1962 Fault Tree Analysis
- 1990 Swiss Cheese Model
- 2012 System Theoretic Process Analysis (STPA)
Analysis Statistics

STPA
- System Description
- System Level Loss - 4
- Hazards - 7
- Unsafe Control Actions - 92
- Causal Factors – 13,775 paths (299 unique causal factors)
What is SafetyHAT?

- A software tool that facilitates hazard analysis using the System Theoretic Process Analysis (STPA) method

SafetyHAT will:
- Guide users through STPA in a step-by-step process
- Store, manage, and organize your data
- Facilitate documentation of your analysis
- Include customization for transportation systems

SafetyHAT includes customized STPA guide phrases specific to transportation systems.
SafetyHAT Walkthrough
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 by clicking the "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.

### Describe your system

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.

### Analyze your system

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 your analysis

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

SafetyHAT

1. SafetyHAT Step 1
2. SafetyHAT Step 2
3. SafetyHAT Step 3
4. SafetyHAT Step 4
5. SafetyHAT Step 5
6. SafetyHAT Step 6
7. SafetyHAT Step 7
8. SafetyHAT Step 8—Data Export

STPA

1. STPA Preparatory Step 1
2. STPA Preparatory Step 2
3. STPA Step 1
4. STPA Step 2
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.

**Customizable guide phrases**

**Link to a PDF of your control structure diagram**
**System Component Input Form**

### Review Existing System Components

<table>
<thead>
<tr>
<th>Existing System Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air Bag Control Unit</td>
</tr>
<tr>
<td>Air Bag Module</td>
</tr>
<tr>
<td>Crash Sensor</td>
</tr>
<tr>
<td>Driver</td>
</tr>
<tr>
<td>Passenger Air Bag Indicator Light</td>
</tr>
<tr>
<td>Passenger Presence Sensing Module</td>
</tr>
<tr>
<td>Passenger Presence Sensor</td>
</tr>
<tr>
<td>Seat Belt Pretensioner</td>
</tr>
<tr>
<td>Seat Belt Tension Sensor</td>
</tr>
<tr>
<td>Seat Track Position Sensor</td>
</tr>
<tr>
<td>Vehicle (including Occupants)</td>
</tr>
</tbody>
</table>

### Add New System Component

**Enter Component Name:**

Passenger Air Bag Button

**Enter a Component Description:**

Dashboard button to enable or disable the passenger side air bag.

---

**Return to Main Menu**  **Previous Step**  **Step 2: Connections**  **View Control Structure Diagram**  **Close Form**  **Form Guidance**
The navigation bar allows you to move easily between data entry forms.
Review entered data ...

...and add, modify, or delete data
### System Connections Input Form

#### Review Existing System Connections

<table>
<thead>
<tr>
<th>Existing System Connections</th>
<th>Type</th>
<th>To</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air Bag Control Unit</td>
<td>Controller</td>
<td>Passenger Air Bag Indicator Light</td>
<td>Actuator</td>
</tr>
<tr>
<td>Air Bag Control Unit</td>
<td>Controller</td>
<td>Air Bag Module</td>
<td>Actuator</td>
</tr>
<tr>
<td>Air Bag Control Unit</td>
<td>Controller</td>
<td>Seat Belt Pretensioner</td>
<td>Actuator</td>
</tr>
<tr>
<td>Air Bag Control Unit</td>
<td>Controller</td>
<td>Vehicle (including Occupants)</td>
<td>Controlled Process</td>
</tr>
<tr>
<td>Air Bag Module</td>
<td>Actuator</td>
<td>Air Bag Control Unit</td>
<td>Controller</td>
</tr>
<tr>
<td>Crash Sensor</td>
<td>Sensor</td>
<td>Driver</td>
<td>Controller</td>
</tr>
<tr>
<td>Passenger Air Bag Indicator Light</td>
<td>Sensor</td>
<td>Air Bag Control Unit</td>
<td>Actuator</td>
</tr>
<tr>
<td>Passenger Presence Sensing Module</td>
<td>Controller</td>
<td>Air Bag Control Unit</td>
<td>Controller</td>
</tr>
<tr>
<td>Passenger Presence Sensor</td>
<td>Sensor</td>
<td>Passenger Presence Sensing Module</td>
<td>Controller</td>
</tr>
<tr>
<td>Seat Belt Pretensioner</td>
<td>Actuator</td>
<td>Vehicle (including Occupants)</td>
<td>Controlled Process</td>
</tr>
<tr>
<td>Seat Belt Tension Sensor</td>
<td>Sensor</td>
<td>Passenger Presence Sensing Module</td>
<td>Controller</td>
</tr>
<tr>
<td>Seat Track Position Sensor</td>
<td>Sensor</td>
<td>Air Bag Control Unit</td>
<td>Controller</td>
</tr>
<tr>
<td>Vehicle (including Occupants)</td>
<td>Controlled Process</td>
<td>Seat Track Position Sensor</td>
<td>Sensor</td>
</tr>
<tr>
<td>Vehicle (including Occupants)</td>
<td>Controlled Process</td>
<td>Seat Belt Tension Sensor</td>
<td>Sensor</td>
</tr>
<tr>
<td>Vehicle (including Occupants)</td>
<td>Controlled Process</td>
<td>Crash Sensor</td>
<td>Sensor</td>
</tr>
<tr>
<td>Vehicle (including Occupants)</td>
<td>Controlled Process</td>
<td>Passenger Presence Sensor</td>
<td>Sensor</td>
</tr>
</tbody>
</table>

#### Add New System Connection

**Connection Originating Component**

- **Name:**
- **Type:**

**Connection Terminating Component**

- **Name:**
- **Type:**

**Enter a Connection Description:**

- [Connection Description Field]

[Buttons: Delete Existing, Modify Existing, Save As New, Return to Main Menu, Step 1: Component, Step 3: Control Action, View Control Structure Diagram, Close Form, Form Guidance]
SafetyHAT uses information about your system to simplify data entry.
SafetyHAT identifies controllers based on your system connections.
**Accident (or Losses) Input Form**

**Review Existing System Accidents or Losses**

 existing system accidents (or losses)  

**Add New System Accident or Losses**

**Enter System Accident (or Loss):**
- Vehicle Occupant Injury or Death

**Enter Detailed Description of the Accident (or Loss):**
- Vehicle occupant is injured or killed. This may occur during a crash or as a result of normal vehicle operation.

**Buttons:**
- Delete Existing
- Modify Existing
- Save As New

**Buttons for Next Steps:**
- Step 3: Control Actions
- Step 5: System Hazards

**View Control Structure Diagram**

**Close Form**

**Return to Main Menu**

**Form Guidance**
Add New System Hazard

Enter System Hazard:
Restrainment System Malfunction (Failure, Loss or Degradation)

Enter Detailed Description of Hazard:
Restrainment system malfunctions. This includes cases where the restraint system deploys inappropriately, does not provide adequate protection, or fails to deploy in a crash situation.

Select Associated Accident(s):
Vehicle Occupant Injury or Death
Unsafe Control Action (UCA) Analysis

Current Control Action

Select Controller
Air Bag Control Unit

Control Action: 1 of 3
Deploy air bag

Control Action
Analysis Completed

Previous Control Action
Next Control Action

Existing Unsafe Control Actions

Select Unsafe Control Action Category
Provided, but executed incorrectly

Complete
Add Note

Existing UCA for Selected Control Action and UCA Category
Air bag deploys, but the positioning is incorrect and does not adequately protect occupants.

Unsafe Control Action Analysis

Enter or Select a Detailed Description for UCA
Air bag deploys, but does not inflate correctly.

(All UCAs for Selected Controller)

Select Relevant Hazards (If applicable)
Restrainment System Malfunction (Failure, Loss or Degradation)

Delete Existing
Modify Existing
Save As New

Return to Main Menu
Step 5: System Hazards
Step 7: Causal Factor Analysis

View Control Structure Diagram
Close Form

Volpe The National Transportation Systems Center

Form Guidance
SafetyHAT comes preloaded with six UCA guide phrases.
### Causal Factor Analysis

**Unsafe Control Action Details**

- **Controller 1 of 2**
  - Air Bag Control Unit

**Description 7 of 8**

Air bag deploys when the vehicle is not in a crash.

**Associated Hazards:**

- Restraint System Malfunction (Failure, Loss or Degradation)

**Control Action Analysis Completed**

### Existing Causal Factor Analyses

**Existing Causal Factors for Selected Unsafe Control Action**

<table>
<thead>
<tr>
<th>Causal Factor</th>
<th>Component Name or Connection From</th>
<th>Connection To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hazardous interaction with other components</td>
<td>Air Bag Control Unit</td>
<td>Air Bag Control Unit</td>
</tr>
<tr>
<td>Hazardous interaction with other components</td>
<td>Air Bag Control Unit</td>
<td>Air Bag Control Unit</td>
</tr>
<tr>
<td>Controller hardware faulty, change over time</td>
<td>Air Bag Control Unit</td>
<td>Air Bag Control Unit</td>
</tr>
<tr>
<td>Controller hardware faulty, change over time</td>
<td>Air Bag Control Unit</td>
<td>Air Bag Control Unit</td>
</tr>
<tr>
<td>Software error (inadequate control algorithm)</td>
<td>Air Bag Control Unit</td>
<td>Crash Sensor</td>
</tr>
<tr>
<td>Sensor inadequate operation, change over time</td>
<td>Air Bag Control Unit</td>
<td>Crash Sensor</td>
</tr>
<tr>
<td>Sensor to controller signal inadequate, missing</td>
<td>Crash Sensor</td>
<td>Air Bag Control Unit</td>
</tr>
</tbody>
</table>

**Select: Component or Connection**

- **Component**
  - **Causal Component**
    - Crash Sensor
  - **Component Type**  Sensor

**Select the Appropriate Causal Factor**

- Sensor inadequate operation, change over time

Enter or Select a Causal Factor Description

- Lateral crash sensor is too sensitive and issues a crash signal when the doors are closed forcefully.

(All Causal Factor Descriptions for Selected Component / Connection and Causal Factor)
SafetyHAT is preloaded with 26 causal factor guide phrases.
SafetyHAT outputs a Microsoft Excel spreadsheet mapping causal factors to system-level losses.
Benefits of Safety HAT

- Novice practitioners can learn the STPA method quickly
- Ensures completeness of the hazard analysis
- Expedites the analysis
- Provides data integrity and consistency checks
- Exportable output table provides documentation straight from database
- Pre-loaded with guidewords developed for transportation systems
- Can easily modify the guidewords for other domains
How Can I get SafetyHAT?

- SafetyHAT can be downloaded free of charge from: [http://www.volpe.dot.gov/SafetyHAT](http://www.volpe.dot.gov/SafetyHAT)

- Use is subject to license terms and conditions:
  - Citation of the Volpe Center in published work involving SafetyHAT
  - Limited to personal use; distribution and/or commercialization is prohibited

Future Possibilities

- Registered SafetyHAT users will be notified of updates and enhancements.

- Users are invited to report good (and other) experiences in an effort to identify possible improvements via email to: SafetyHAT@dot.gov.

- Those who may wish to collaborate on further SafetyHAT development are encouraged to contact the Volpe Center at: SafetyHAT@dot.gov.
Questions