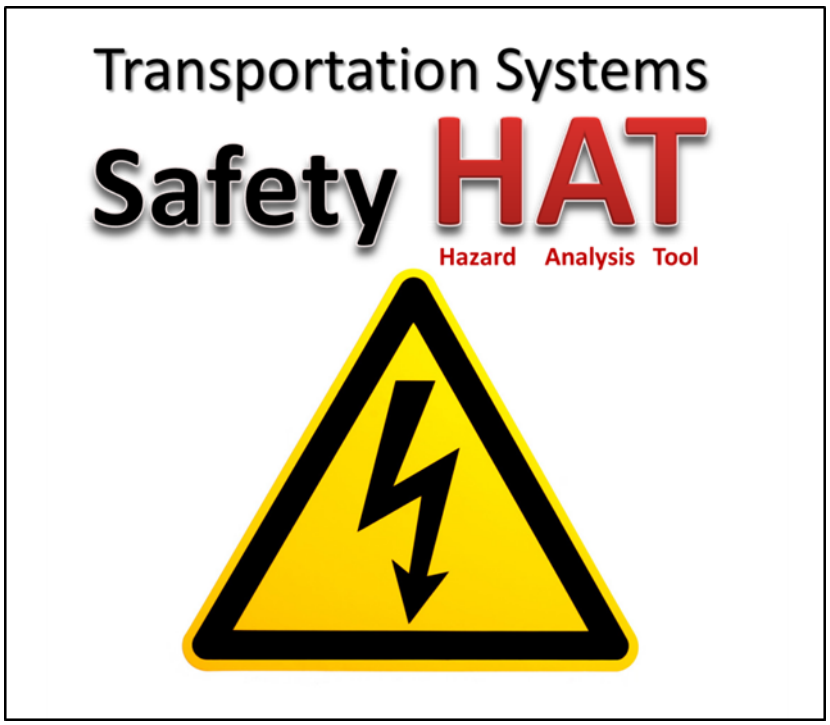
Transportation Systems Safety Hazard Analysis Tool (SafetyHAT)

User Guide (Version 1.0)



March 2014

DOT-VNTSC-14-01

Prepared for:

Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142

U.S. Department of Transportation
Research and Innovative Technology Administration
John A. Volpe National Transportation Systems Center

Volpe

Notice

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 24, 2014	

4. TITLE AND SUBTITLE	5a. FUNDING NUMBERS
Transportation Systems Safety Hazard Analysis Tool (SafetyHAT) User Guide (Version 1.0)	
6. AUTHOR(S)	5b. CONTRACT NUMBER
Christopher Becker, Qi Van Eikema Hommes	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Volpe National Transportation Systems Center 55 Broadway Cambridge, MA 02142	8. PERFORMING ORGANIZATION REPORT NUMBER DOT-VNTSC-14-01
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Volpe National Transportation Systems Center 55 Broadway Cambridge, MA 02142	10. SPONSORING/MONITORING AGENCY REPORT NUMBER NA
11. SUPPLEMENTARY NOTES	
12a. DISTRIBUTION/AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

This is a user guide for the transportation system Safety Hazard Analysis Tool (SafetyHAT) Version 1.0. SafetyHAT is a software tool that facilitates System Theoretic Process Analysis (STPA). This user guide provides instructions on how to download, install, and use SafetyHAT version 1.0.

14. SUBJECT TERMS	15. NUMBER OF PAGES
System Theoretic Process Analysis, STPA, Hazard Analysis, Hazard Identification, Safety Analysis, Safety Analysis Software, STPA Software, System Theoretic Process Analysis Software, SafetyHAT, STAMP, System Theoretic Accident Modeling Process, System Safety, Transportation System Safety	76
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18
298-102

Acknowledgments

The Transportation System Safety Hazard Analysis Tool (SafetyHAT) was funded by the Volpe National Transportation Systems Center (the Volpe Center) 2012 Innovation Challenge Grant. The project team includes Dr. Qi Van Eikema Hommes, Christopher Becker, Dr. Joanne Kang, Mike Razo, and Zale Anis. The software was primarily developed by Christopher Becker and Dr. Qi Van Eikema Hommes. Dr. Joanne King was the first user, and provided numerous valuable inputs for functionality improvements.

The team would like to thank the Volpe Center leadership Bob Johns, Director and Associate Administrator, and Anne Aylward, Deputy Associate Administrator for Research and Innovation, for establishing the Innovation Challenge grant. Technical Center Directors Gary Ritter and Dr. Steve Popkin have advised the team since the idea inception, guided the team through the pitch competition, and supported the team through the completion of the project. Their mentorship was instrumental for the success of this project. In addition, the team would like to thank the Volpe Center legal counsel Wendell Mah for his assistance and advice in the Intellectual Property decision for the software tool, and Matthew Isaacs for his help in providing suggestions on improving the user interface.

Furthermore, the team would like to thank the judges of the 2012 Volpe Center Innovation Challenge for selecting this project:

- Gregory Winfree, DOT OSTR Assistant Secretary,
- Jo Strang, Former Associate Administrator for Railroad Safety - Chief Safety Officer,
- Chris Bonanti, NHTSA Associate Administrator for Rulemaking, and
- Tony Fazio, FAA Director of the Office of Accident Investigation and Prevention.

Contents

List of Abbreviations

Abbreviation	Term
MS	Microsoft
SafetyHAT	Safety Hazard Analysis Tool
STAMP	System-Theoretic Accident Model Process
STPA	System-Theoretic Process Analysis
UCA	Unsafe Control Action
USDOT	United States Department of Transportation
The Volpe Center	Volpe, The National Transportation Systems Center

1. General Information

1.1 What Is SafetyHAT?

1.1.1 Overview

The Transportation Systems Safety Hazard Analysis Tool (SafetyHAT) is a software tool that facilitates System Theoretic Process Analysis (STPA). STPA is a hazard identification method based on a top-down system engineering approach and control systems theory [1]. While some familiarity with STPA is expected before using this tool, one of the primary goals of SafetyHAT is to help safety analysts become proficient with the STPA method. SafetyHAT includes transportation-oriented guide phrases and causal factors that tailor the STPA method to transportation systems.

STPA provides an algorithmic and well-guided analysis process that identifies the causes of system hazards, including:

- Hardware component failures
- Software errors
- Complex system interactions
- Human errors
- Inadequate organization management, policy, and procedures

STPA can be applied to technical control systems, as well as the social systems involved in the lifecycle of the technical system, as demonstrated by a number of published projects [2]. STPA enables users to identify and develop lower level safety design requirements to meet overall system safety constraints.

The benefits of SafetyHAT include:

1. Guiding analysts through the preparatory and analysis steps of STPA by:
   - Providing streamlined data entry process.
   - Directing analysts through STPA with a wizard-like format, with preloaded transportation-specific guidewords.
   - Enabling customization for other applications.
2. Leveraging the power of a relational database to organize and manage the large quantity of data that the analysis may produce. It can:
   - Efficiently store large quantity of analysis data (a small control system may generate over 10,000 entries).
   - Enforce data integrity when modifying or deleting data, reducing the analysts' burden during the iterations inherent to STPA.
3. Facilitating the documentation of hazard analysis. It can:

- Provide traceability from system-level hazards to component level causal factors.
- Generate auditable documentation.
- Further enable data sharing and reuse.
- Allow new system analysis to extend upon previous analysis models and results.

1.1.2 How Does SafetyHAT Differ from STPA

Although SafetyHAT is based on STPA, SafetyHAT incorporates two key differences.

1. STPA consists of two analysis steps and two preparatory steps that must be completed before beginning STPA. SafetyHAT uses an eight-step process to guide the user through the two STPA preparatory and two STPA analysis steps. Figure 1 illustrates how SafetyHAT steps correspond to STPA:

   - The first three steps guide you through STPA Preparatory Step 1, allowing you to input the description of the hierarchical control structure diagram. SafetyHAT will draw on this information throughout the analysis.

   - The next two steps (Steps 4-5) allow you to enter the system level accident/loss and hazards.

   - Step 6 and 7 are the two STPA steps.

   - Step 8 enables data export and generates an Excel spreadsheet.

   These steps are described in more detail in Section 3.5 and 3.6 of this user guide.

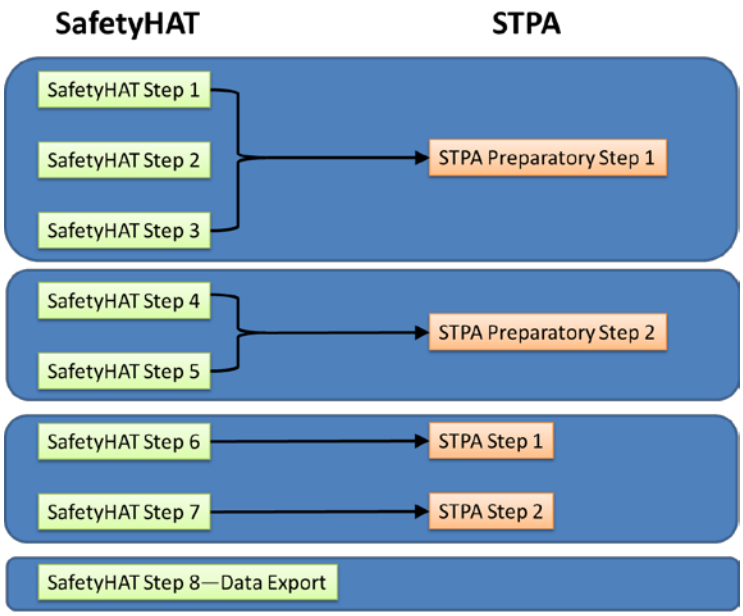


Figure 1: Mapping Between SafetyHAT Steps and STPA Steps

2. SafetyHAT comes preloaded with six unsafe control action (UCA) guide phrases and 26 causal factor guide phrases, compared to the four UCA guide phrases and 16 causal factor guide phrases traditionally used in STPA. The additional UCA and causal factor guide phrases were added based on the developers' experience in applying STPA to transportation systems. Please refer to Section 4 of this user guide for a list of the preloaded UCA and causal factor guide phrases.

   The pre-loaded UCA and causal factor guide phrases can be edited through the Advanced Options feature of SafetyHAT. This process is described in more detail in Section 4 of this user guide.

1.1.3 Developers

SafetyHAT was developed by the U.S. Department of Transportation John A. Volpe National Transportation Systems Center (Volpe) to assist in conducting system safety and hazard analyses.

1.2 Authorized Use Permission

SafetyHAT is available for public use and can be downloaded for free at http://www.volpe.dot.gov/SafetyHAT. Use and distribution of SafetyHAT is subject to the terms and conditions of the licensing agreement in the installation package.

1.3 Feedback and Suggestions

SafetyHAT is provided for free as an unsupported software tool. However, we do encourage users to provide feedback and suggested improvements by emailing SafetyHAT@dot.gov. Suggestions may be incorporated into future releases of SafetyHAT. If you wish to receive an email notification when updates or a new version of SafetyHAT is available, please register your email address at http://www.volpe.dot.gov/SafetyHAT.

2. Getting Started

2.1 About This User Guide

This user guide accompanies SafetyHAT Version 1.0 and provides instructions specific to this version of SafetyHAT. If are using a later version of SafetyHAT, please refer to the user guide that was included in your installation package.

2.1.1 Organization of the Guide

Section 2 of this user guide will help you set up SafetyHAT on your computer.

Section 3 of this user guide will walk you through performing an analysis using SafetyHAT, including how to use the various screens and input forms in SafetyHAT. Specifically:

- Section 3.1 explains the preparation work you must complete before you start using SafetyHAT.
- Section 3.2 explains how to open a SafetyHAT project.
- Section 3.3 provides an overview of the Main Menu screen and how to access each of the data entry forms in SafetyHAT.
- Section 3.4 provides an overview of the general layout of the data entry forms and key navigation features.
- Section 3.5 provides step-by-step instructions on how to enter data into each of the data entry forms.

Section 4 of this user guide explains how to customize SafetyHAT using the advanced options.

Throughout this guide, the following icons are used:

The exclamation icon marks critical information.

The light bulb icon shows helpful hints and information worth noting.

2.2 SafetyHAT Versions

There are two versions of SafetyHAT available for public use. The Microsoft (MS) Access Template Version is intended for individuals who plan on regularly using SafetyHAT and have MS Access software. The MS Access Runtime Version is an evaluation version intended for users without MS Access software. Both versions can be downloaded free of charge at http://www.volpe.dot.gov/SafetyHAT. The two versions are described in more detail below:

- **MS Access Template Version**: This version provides a reusable SafetyHAT template for Microsoft Access 2010 or later. You will be able to evaluate multiple systems using STPA by creating new instances of SafetyHAT directly from MS Access. This version allows the user to view or edit the underlying data tables, or database structure.

- **MS Access Runtime Version**: This is a single-use version of SafetyHAT intended for users without Microsoft Access 2010 or later. It uses MS Access 2010 Runtime to run SafetyHAT. This version of SafetyHAT allows the user to evaluate the software capability and complete an entire analysis for a single system. This version also does not allow the user to view or edit the underlying data tables, or database structure.

Check to see if you have MS Access installed on your machine by opening the Start Menu and typing "Microsoft Access" in the search bar.

2.3 Installation

SafetyHAT was developed using a Microsoft Windows operating system, and compatibility with other operating system environments, such as MacOS and Linux, has not been tested. There is no immediate plan for testing compatibility with other operating systems.

2.3.1 System Requirements

The minimum system requirements to run SafetyHAT are displayed in Table 1.

Table 1: SafetyHAT Minimum System Requirements

	Minimum Requirements
Operating System	Microsoft Windows XP, Microsoft Windows Vista, or Microsoft Windows 7
Processor Speed	500 MHz
Memory (RAM)	256 MB
Hard Disk Space †	10 MB (MS Access Template Version) 200MB (MS Access Runtime Version)
Display Resolution	1280 x 800
Software Requirements	Microsoft Access 2010 (or later) for the Template Version Microsoft Excel 2010 (or later) PDF Viewer
† Additional hard disk space will be required to save your analysis (approximately 5 to 10 MB for a 40-component system).	

2.3.2 MS Access Template Version Installation

If you do not have MS Access 2010 or later on your system, please refer to Section 2.3.3 for instructions on how to install the single-use MS Access Runtime Version.

To install the MS Access Template Version of SafetyHAT:

1. Download the installation package "SafetyHAT_Installer.zip" from http://www.volpe.dot.gov/SafetyHAT.

2. Extract the files to the directory where you would like to install SafetyHAT.

3. Double click the installation file "Setup.exe".

4. Follow the screen prompts.

SafetyHAT installs in the default template directory for MS Access. If you or your system administrator has changed this directory path, you will need to manually copy the "SafetyHAT.accdt" file from the installation directory into your MS Access template directory.

2.3.3 MS Access Runtime Version Installation

The MS Access Runtime Version of SafetyHAT uses MS Access 2010 Runtime. MS Access 2010 Runtime is a limited version of MS Access in which certain features have been disabled. To learn more about MS Access 2010 Runtime, please visit: http://www.microsoft.com/en-us/download/details.aspx?id=10910. You will be able to conduct a single complete analysis of a single system using SafetyHAT with the MS

Access Runtime Version.

To install the single-use MS Access Runtime Version of SafetyHAT:

1. Download the installation package “SafetyHAT_Runtime.zip” from http://www.volpe.dot.gov/SafetyHAT.

2. Extract the files to the directory where you would like to install SafetyHAT.

3. Double click the installation file “Setup.exe”.

4. Follow the screen prompts.

3. Using SafetyHAT

3.1 Preparing to Use SafetyHAT

SafetyHAT is a software tool that facilitates safety and hazard analysis using STPA. Before using SafetyHAT, two preparatory steps for STPA should be completed:

- **Preparatory Step 1:** Create a hierarchical control structure diagram of the system. The control structure diagram consists of blocks for each system component including controllers, actuators, sensors, and controlled processes. Interactions and information pathways between components are represented as lines between the blocks. Control actions issued by system controllers should be explicitly shown and labeled on the diagram. Figure 2 shows an example of a control structure diagram (automotive air bag control system).

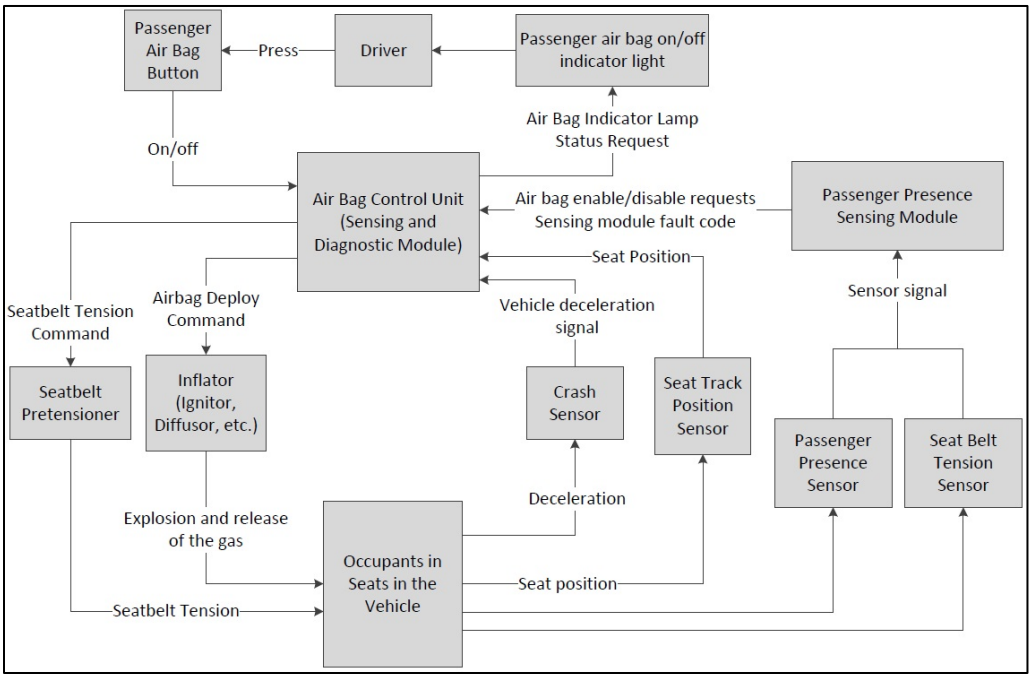


Figure 2: Example Control Structure Diagram (Automotive Air Bag Control System)

Saving a copy of your Control Structure Diagram as a PDF will enable you to create a link to the diagram in SafetyHAT. (See Section 3.3.2.)

- **Preparatory Step 2:** Identify system losses (accidents) and hazards. An accident is defined as "an undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc." [1]. STPA defines a hazard as "a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss)" [1].

3.2 Opening a SafetyHAT Project

3.2.1 Opening a New Project Using the MS Access Template Version

To open a new SafetyHAT project:

1. Open Microsoft Access.

2. Click the *My Templates* icon (see Figure 3)

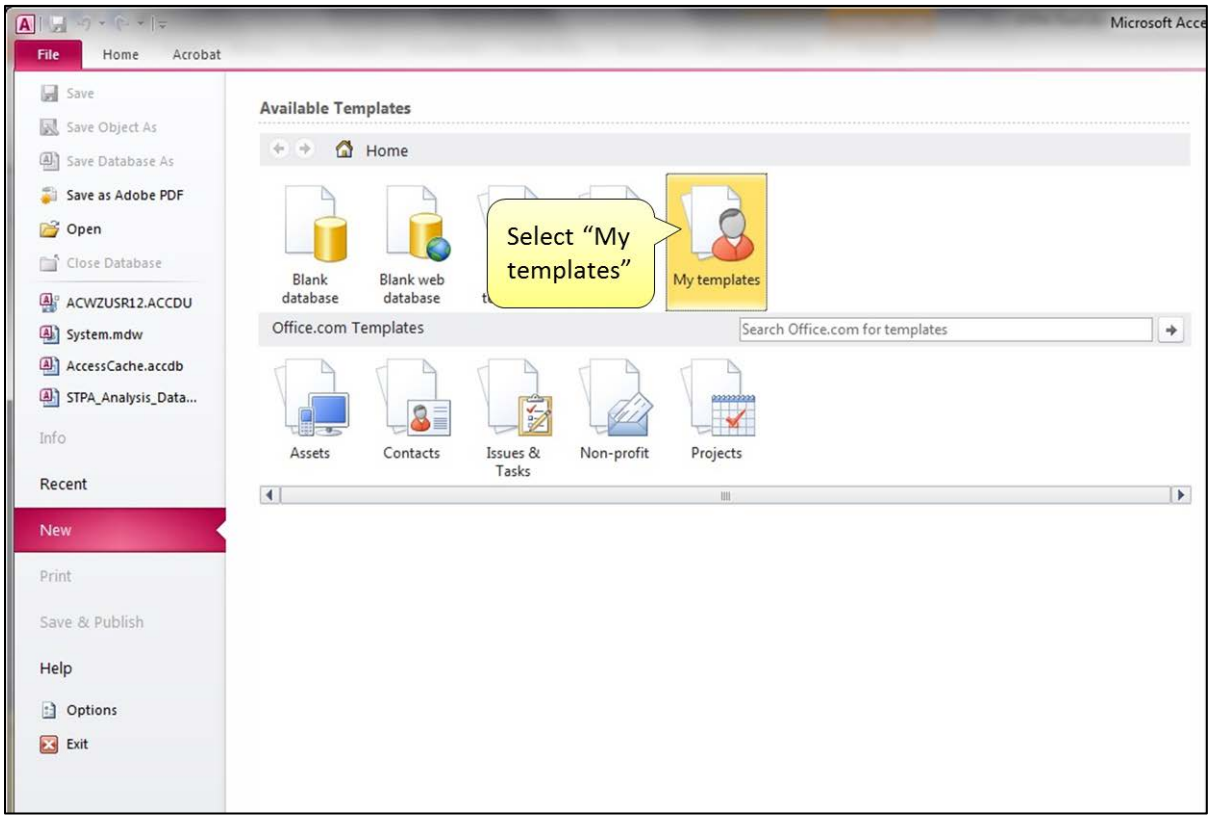


Figure 3: Opening the Custom Template Directory

3. Select the template called “SafetyHAT” (see Figure 4)

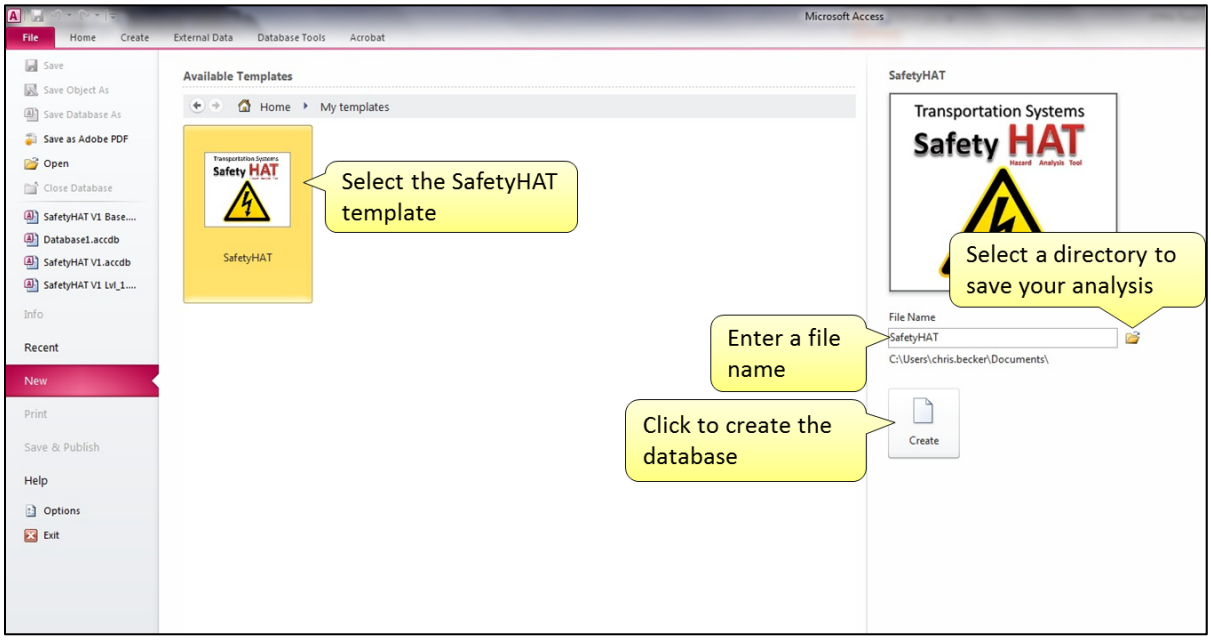


Figure 4: Creating a New SafetyHAT File

4. Click the folder icon on the right side of the screen to select the directory where you would like to save your SafetyHAT project file (see Figure 4).

5. Enter a new name for your SafetyHAT project file in the text box on the right side of the screen, or use the default “SafetyHAT” file name.

6. Click the *Create* button to create your SafetyHAT project file.

You will then see the screen shown in Figure 5. Click the *Enable Content* button at the top of this screen (see Figure 5).

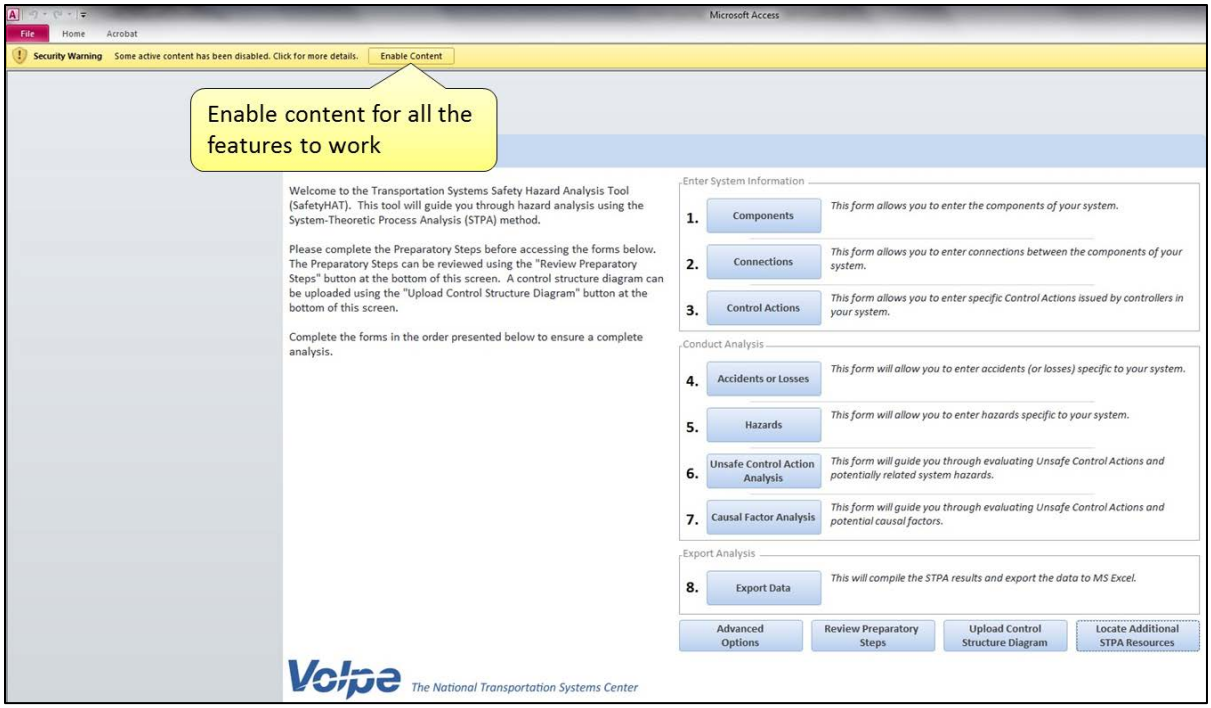


Figure 5: Enabling content in the Microsoft Security Warning banner.

You must click the Enable Content button to enable all of the features of SafetyHAT.

3.2.2 Opening an Existing Project

To open an existing SafetyHAT project file:

1. Navigate to the directory containing your project file.
2. Double click on the SafetyHAT project file icon.

3.2.3 Opening the MS Access Runtime Version of SafetyHAT

To open the MS Access Runtime Version of SafetyHAT:

1. Navigate to the directory where you installed the MS Access Runtime Version of SafetyHAT.
2. Double click on the SafetyHAT project file icon.

3.3 Main Menu Navigation

The Main Menu (Figure 6) automatically loads when you open a new or existing SafetyHAT project file. The numbered buttons on the right side of the main menu provide quick access to the seven data entry forms and the analysis export feature. The four buttons at the bottom of the main menu provide access to some additional features included in SafetyHAT.

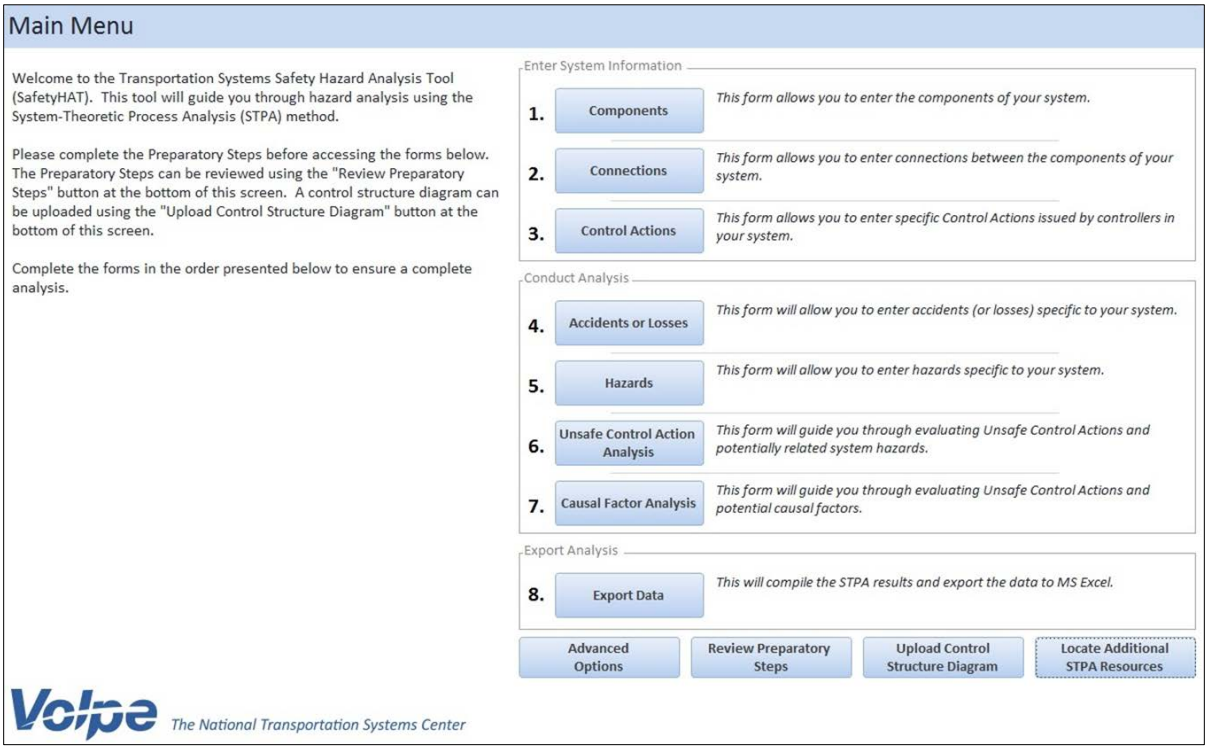


Figure 6: SafetyHAT Main Menu Screen

3.3.1 Accessing Data Entry Forms

SafetyHAT has eight numbered steps on the right hand side of the main menu. Steps 1 through 7 are data entry steps. Clicking any of these buttons will take you from the main menu directly to that data entry form. The final step (Step 8) is an export feature that compiles your analysis and generates a MS Excel spreadsheet.

To ensure the most complete analysis, begin with Step 1 in the Main Menu and proceed sequentially through Step 7.

3.3.2 Accessing Additional Features

Four buttons at the bottom of the main menu provide additional features. Button functionalities are described below.

The *Advanced Options* button enables you to alter the preloaded SafetyHAT guide phrases that underlie SafetyHAT. Use caution when modifying the guide phrases. Improper modification of the guide phrases could result in an incomplete or incorrect analysis. The advanced options feature is described in more detail in Section 4 of this user guide.

The *Review Preparatory Steps* button describes the steps in Section 3.1 of this User Guide. To review STPA's preparatory steps:

1. Click the *Review Preparatory Steps* button at the bottom of the Main Menu. This will open up the screen shown in Figure 7.

2. To return to the Main Menu screen, click the *Return to Main Menu* button in the lower right corner of the screen or the close button (*X)* in the upper right corner of the screen.

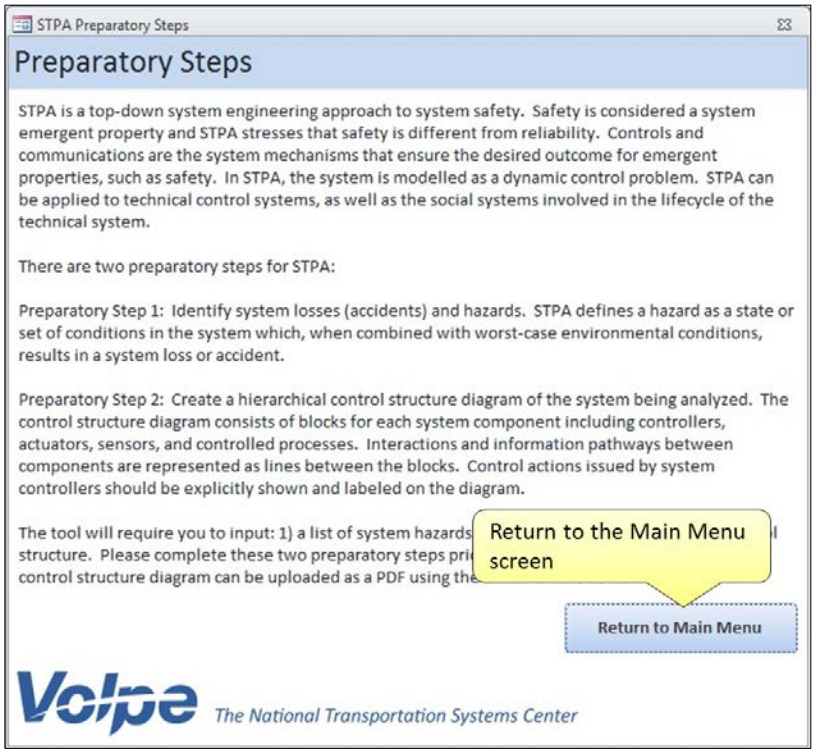


Figure 7: Preparatory Steps Overview Screen

The *Upload Control Structure Diagram* button allows you to create a link to the control structure diagram file on your computer using the following steps:

1. Click the *Upload Control Structure Diagram* button at the bottom of the Main Menu. This will open the dialogue box shown in Figure 8.

2. Use the sidebar or the navigation bar in the dialogue box to open the directory that contains your control structure diagram. This feature only supports control structure diagrams saved in PDF format.

3. Click the *Open* button to link the directory location of your control structure diagram with SafetyHAT.

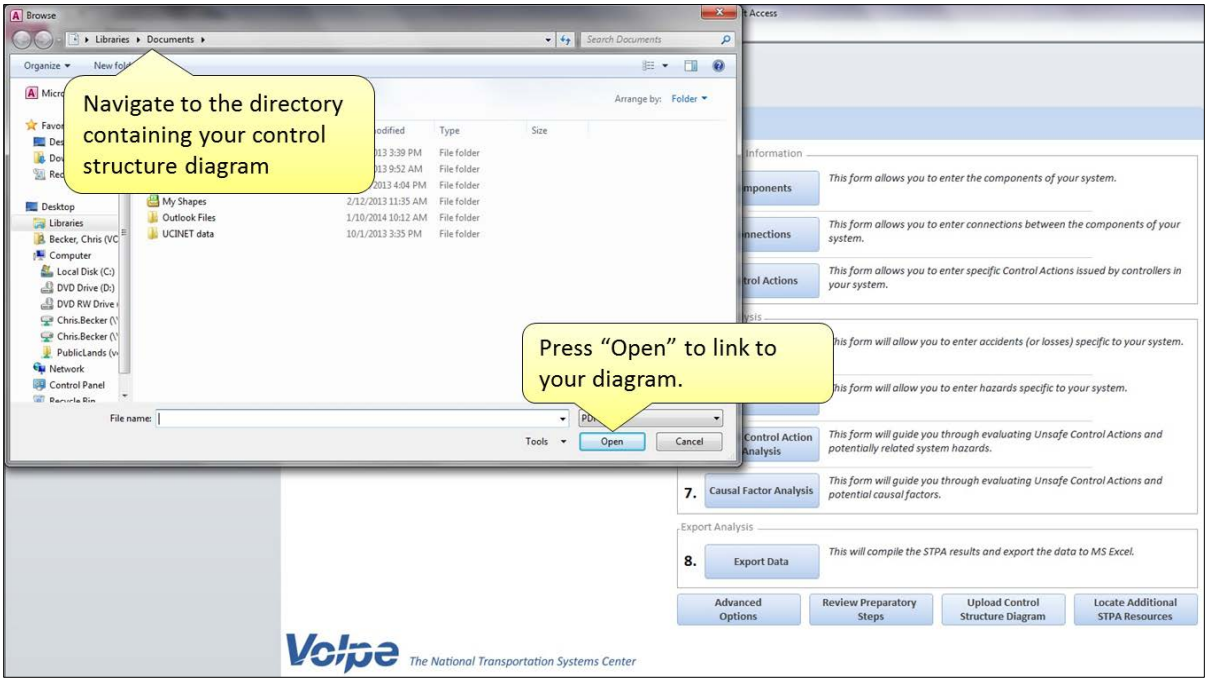


Figure 8: Control Structure Diagram Upload Screen

SafetyHAT only links to your diagram. If you change the file name or directory, you must re-establish the link between SafetyHAT and your diagram through the Main Menu.

The *Locate Additional STPA Resources* button allows you to learn more about STPA. These resources are for informational purposes and are not affiliated with the USDOT or the SafetyHAT software program.

3.4 General Form Navigation

The seven data entry forms (Steps 1-7) share similar layout. This section of the user guide will explain the general form layout and navigation features in SafetyHAT.

3.4.1 Navigation Bar

The navigation bar located at the bottom of each form allows you to move easily through SafetyHAT. The navigation bar contains five buttons, shown in Figure 9.

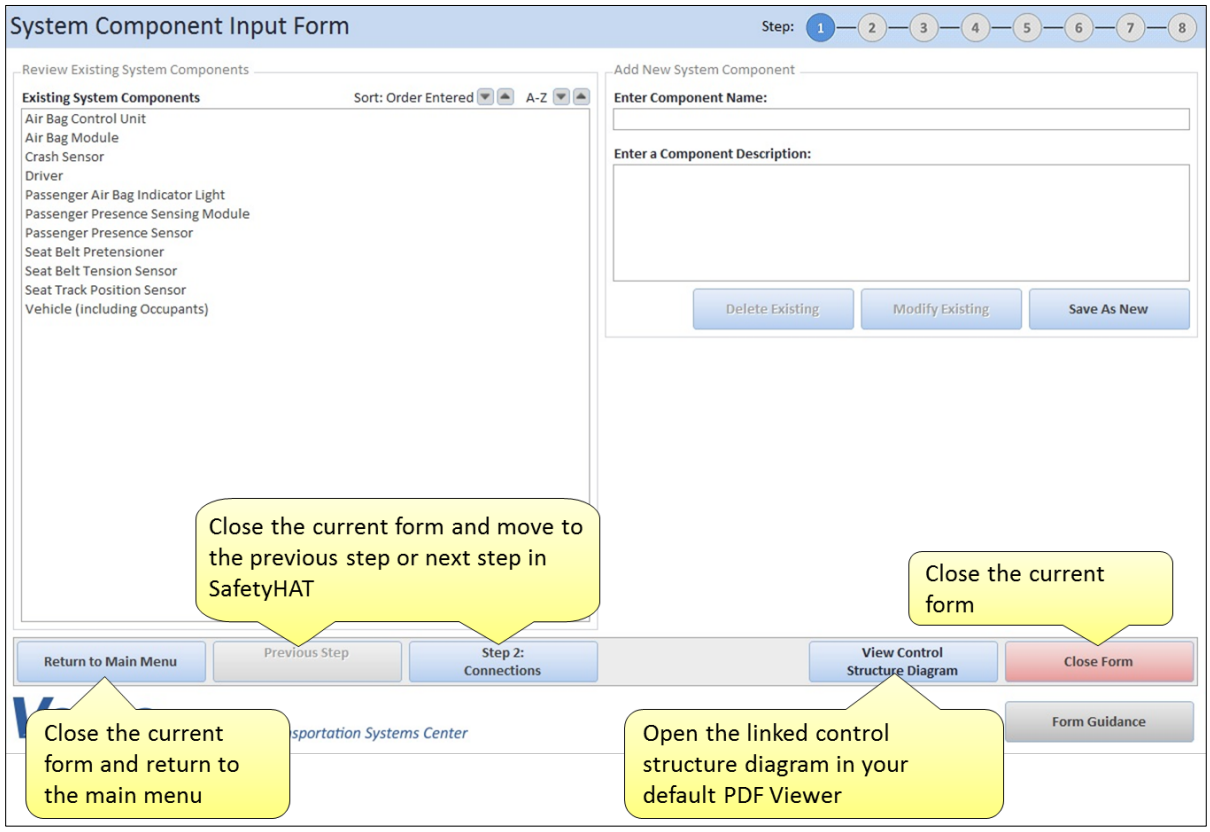


Figure 9: Navigation Bar Features

- Clicking the *Return to Main Menu* button will close the current form and open the Main Menu. If you entered data into the current form, you will receive a prompt to save the current entry before the form closes.

- Step buttons will close the current form and bring you to the next step (or previous step) in SafetyHAT. If you entered data into the current form, you will receive a prompt to save the current entry before the form closes. Note that when you are at the first data entry form in SafetyHAT, the *Previous Step* button is disabled.

- The *View Control Structure Diagram* will open the linked control structure diagram in your default PDF Viewer. SafetyHAT will remain open while viewing the control structure diagram.

  If you did not create a link to a control structure diagram from the Main Menu, the warning notification shown in Figure 10 will appear, providing instructions on how to link the control structure to the SafetyHAT.

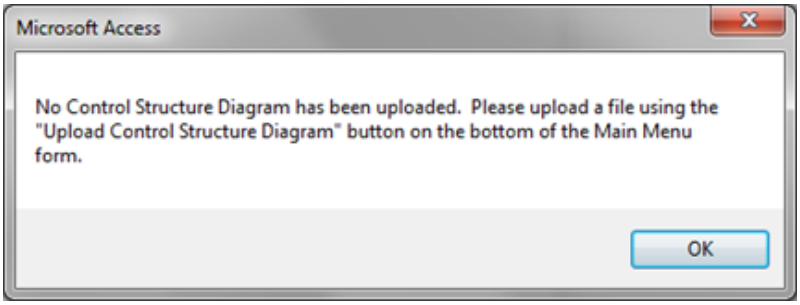


Figure 10: Warning Message If a Control Structure Diagram is Not Linked to SafetyHAT

- Clicking the *Close* button will close the current form. If you entered data into the current form, you will receive a prompt to save the current entry before the form closes.

3.4.2 Form Guidance

A *Form Guidance* button is available at the lower-right corner of each data entry form in SafetyHAT providing instruction on how to complete the current form. When appropriate, the form-specific guidance will also provide a brief description of how the current form relates to STPA.

Clicking the *Form Guidance* button in the lower right hand corner of your current form (see Figure 11) will bring up the screen shown in Figure 12. Clicking the *X* button in the upper right corner of the form guidance page will close the guide and return you to the input form.

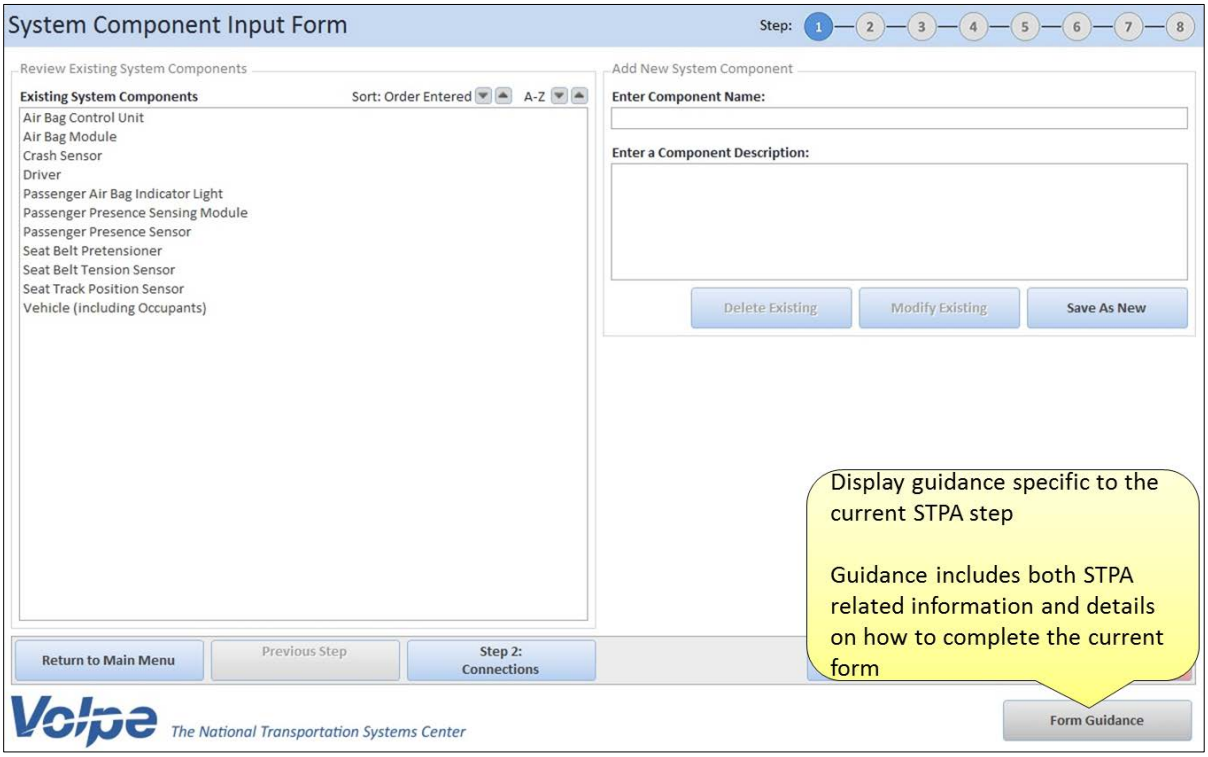


Figure 11: Accessing the Form-Specific Guidance Feature

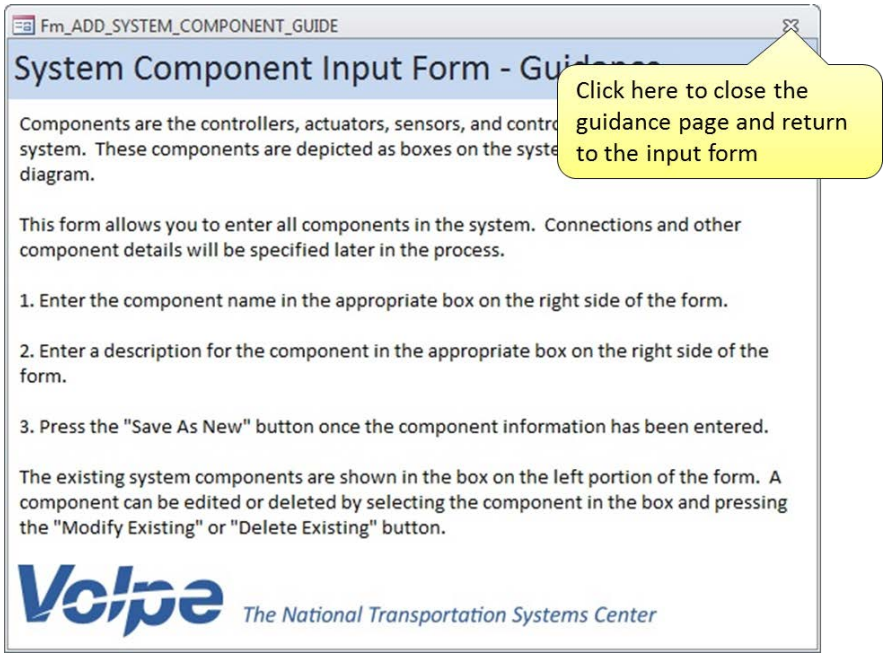


Figure 12: Closing the Form-Specific Guidance Page

3.4.3 Tracking Your Progress

You can track your progress in SafetyHAT using the colored circles in the upper right corner of the screen (see Figure 13). Each of the circles corresponds to one of the SafetyHAT steps; the order of these steps is identical to those shown on the main menu screen. Your current step is denoted by the blue circle.

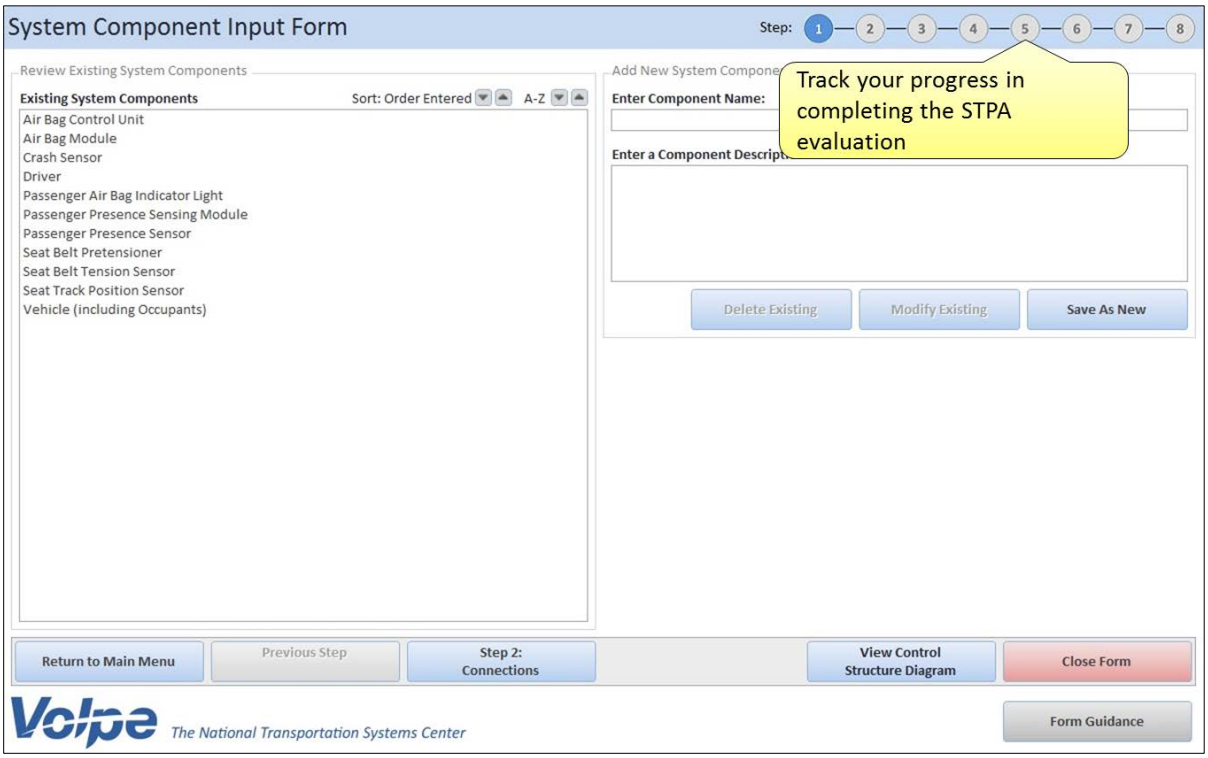


Figure 13: Progress Tracking Feature

3.4.4 Adding New Entries

SafetyHAT requires you to enter information about your system. Figure 14 shows a typical SafetyHAT data entry form. Data entry fields are shown on the right of each form and existing entries are shown on the left of each form.

To add a new entry:

1. Type in the relevant information in the fields on the right side of each form. Some forms may have drop-down lists in addition to text entry fields.

2. Click the *Save As New* to add your entry. If your entry matches an existing entry, SafetyHAT will **not** create a duplicate entry.

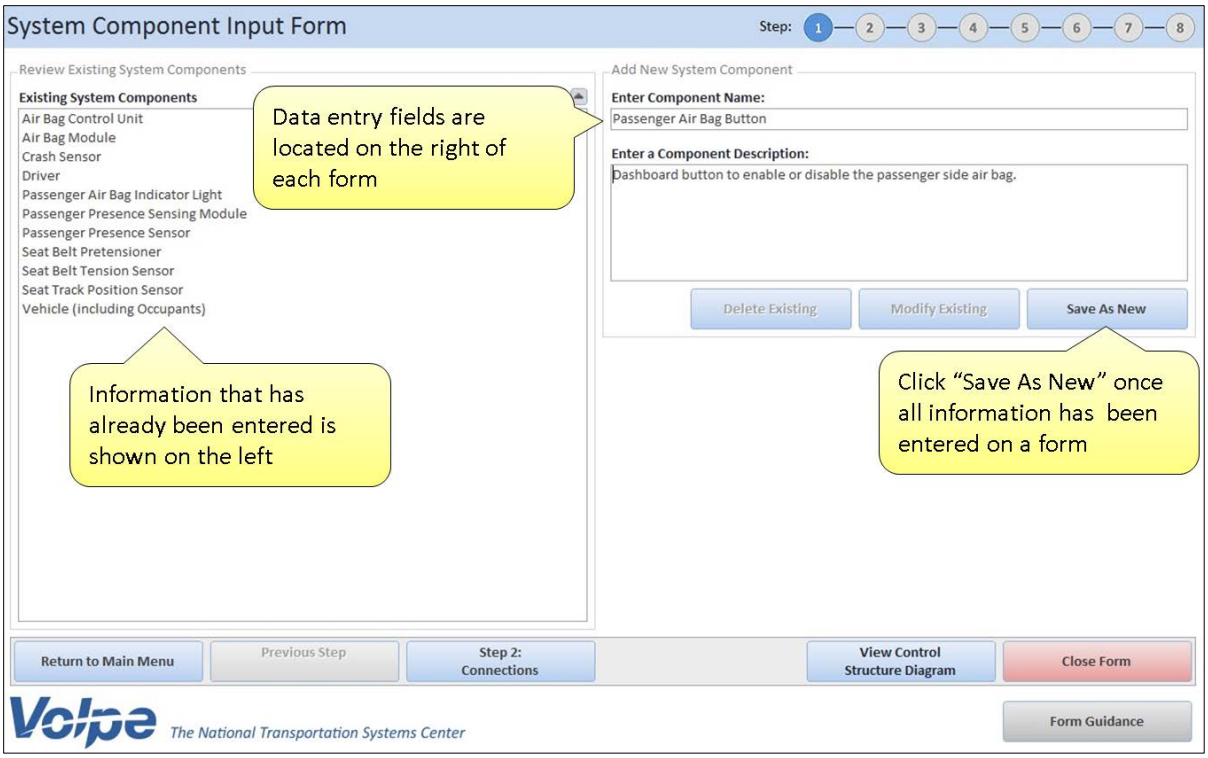


Figure 14: Entering New Data

The description fields allow you to enter references or more in-depth details. Information entered into these fields will appear in the final output file from SafetyHAT.

SafetyHAT does not allow duplicate entries (for example, tow components with the same name). Make sure each entry is unique.

3.4.5 Modifying and Deleting Existing Entries

SafetyHAT allows you to modify or delete existing entries directly from each form (see Figure 15). SafetyHAT will automatically propagate any changes you make throughout the analysis. For example, if you change a component name in Step 1, the component name will automatically be updated in any associated connections in Step 2. Likewise, deleting a component in Step 1 will delete any connections and analyses related to that component.

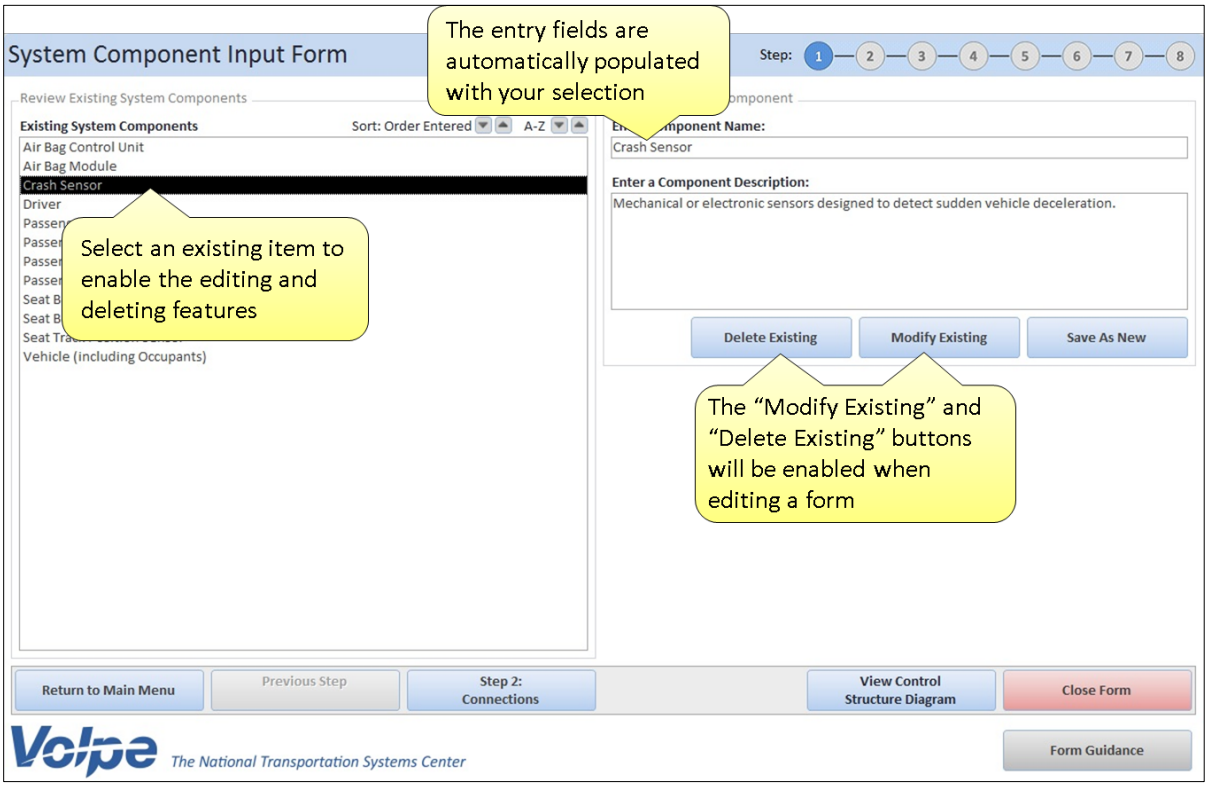


Figure 15: Modifying and Deleting Entries

To modify existing entries:

1. Select an existing entry from the left side of the form. The right side of the form will automatically be populated with your selection and the *Modify Existing* button will be enabled.

2. Make any necessary changes directly in the entry boxes on the right side of the form.

3. Click the *Modify Existing* button.

To delete an existing entry:

1. Select an existing entry from the left side of the form. The right side of the form will automatically be populated with your selection and the *Delete Existing* button will be enabled.

2. Click the *Delete Existing* button.

*SafetyHAT does not have an "undo" feature. Deleting an entry will **permanently** remove the entry and any associated analyses.*

3.4.6 Sorting Existing Entries

To help you review and locate existing entries, SafetyHAT allows you to sort the existing entries found on the left side of each form. Existing entries can be sorted alphabetically (A-Z) or by the order in which the entries were added (Order Entered). To sort entries, use the buttons located to the upper right of the box containing your existing entries, as shown in Figure 16.

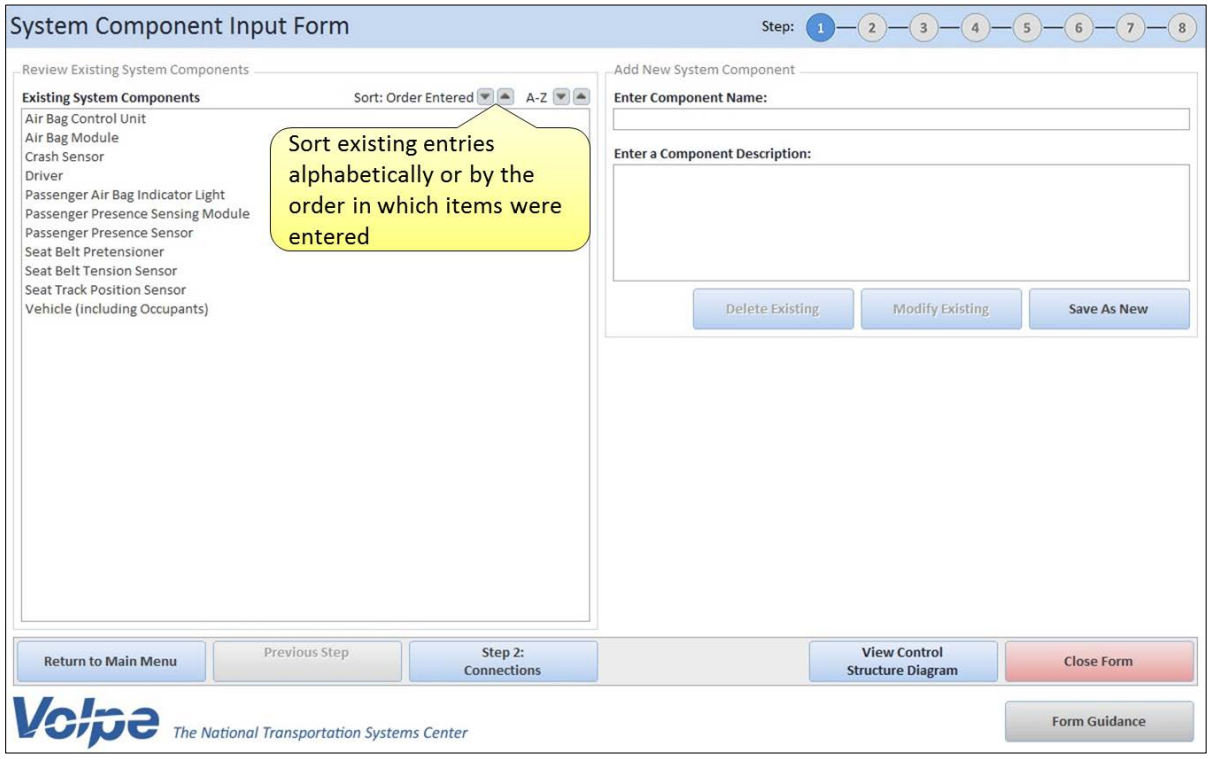


Figure 16: Sorting Existing Entries

3.5 Data Entry Forms

This section of the user guide will walk you through each of the seven data entry forms in SafetyHAT (Steps 1-7).

3.5.1 Step 1: System Component Input Form

Components are the controllers, actuators, sensors, and controlled processes of the system. These components are depicted as boxes on the system control structure diagram. The System Component Input Form allows you to enter, modify, and delete component information. Figure 17 shows the layout of the System Component Input Form.

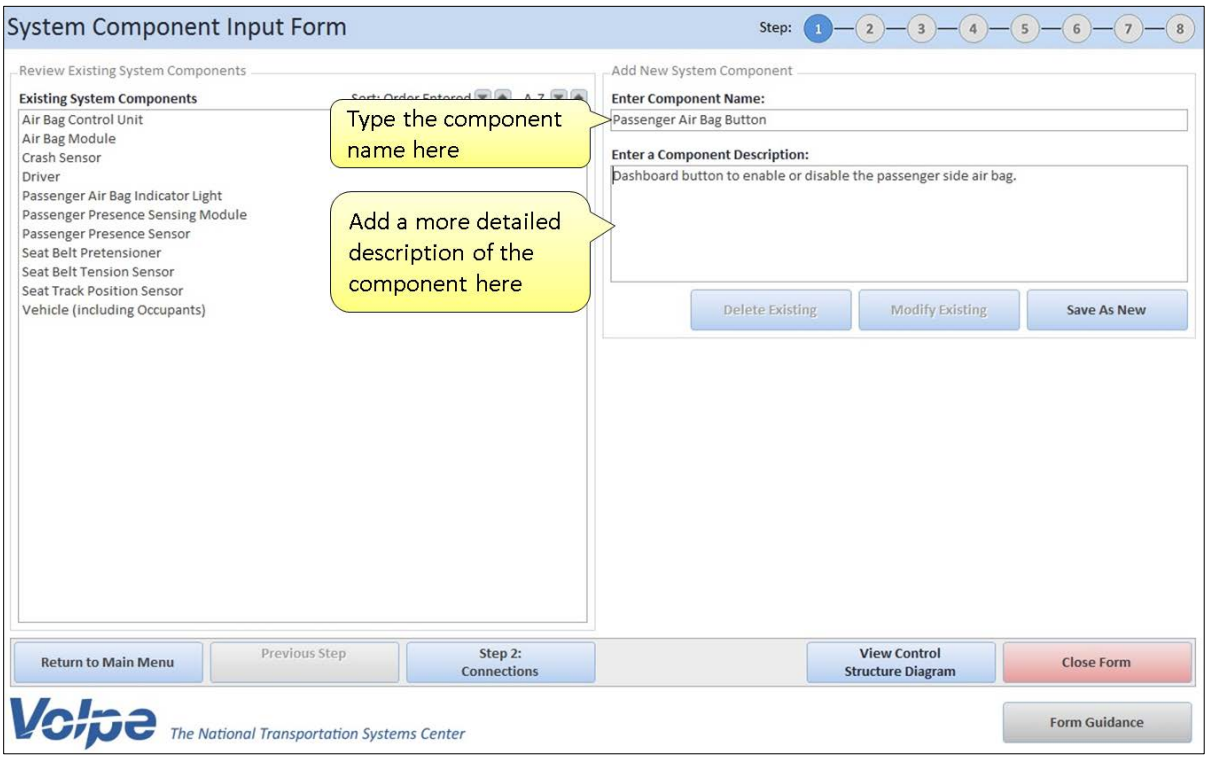


Figure 17: System Component Input Form

To enter a new component:

1. Enter the component name in the first entry field on the right side of the form.
2. Enter a detailed description for the component in the second entry field on the right side of the form.
3. Click the *Save As New* button.

To modify an existing component:

1. Select the component you want to edit from the box on the left side of the form.
2. Make the necessary changes in the fields on the right side of the form.
3. Click the *Modify Existing* button.
4. Click *Yes* to confirm your change(s).

To delete an existing component:

1. Select the component you want to delete from the box on the left side of the form.

2. Click the *Delete Existing* button.

3. Click *Yes* to confirm deletion.

3.5.2 Step 2: System Connections Input Form

System connections represent information or resource flows, or other interactions between system components. System connections are represented by the lines connecting the components on your system control structure diagram. The System Connections Input Form allows you to enter, modify, or delete connections between components in your system. Figure 18 shows the layout of the System Connections Input Form.

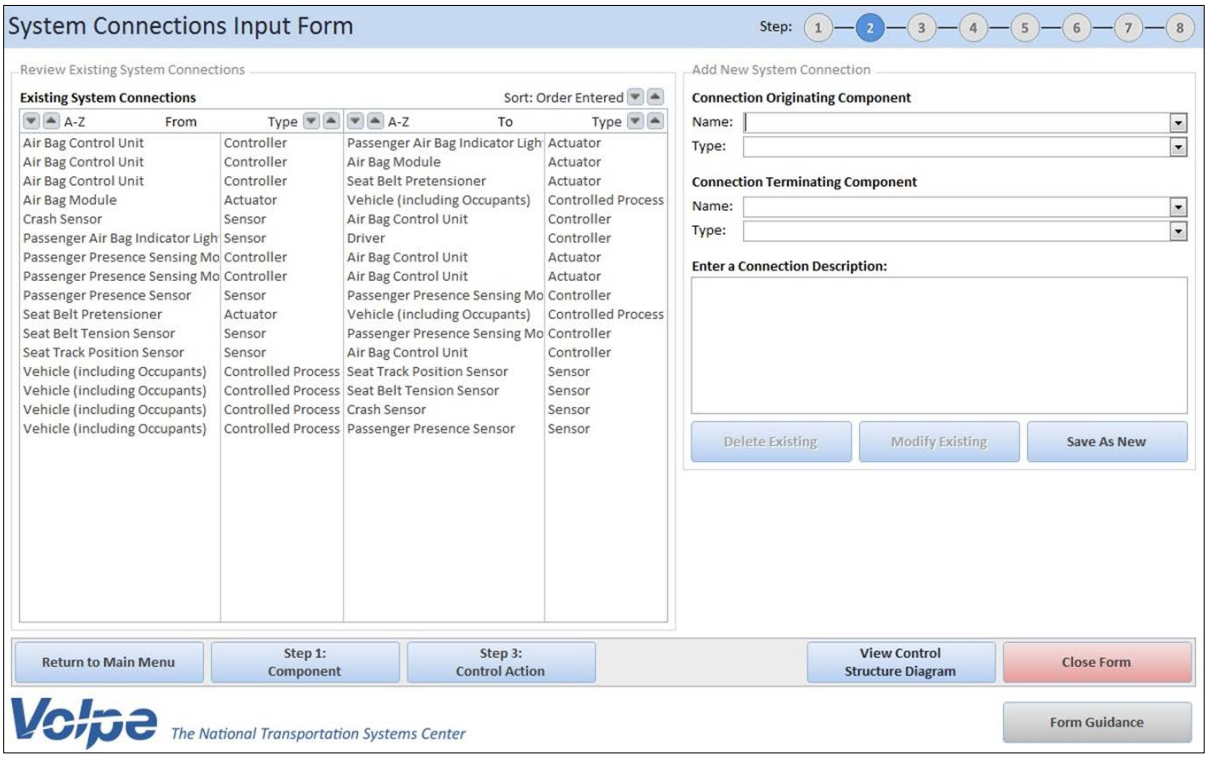


Figure 18: System Connections Input Form

SafetyHAT allows you to make connections between any two components. The component type drop-down list determines the role of each component in the connection. Components may be assigned different component types depending on the connection being defined. For example, in Figure 18, the Air Bag Control Unit represents an actuator with respect to the Passenger Presence Sensing Module, and represents a controller with respect to the Crash Sensor.

This step effectively defines the control system for your analysis. It is critical to ensure that the connections and component types accurately reflect your control structure.

To create a new connection:

1. Select the originating component for the connection from the first drop-down list on the right side of the form (see Figure 19).

   SafetyHAT generates the list of available components based on your entries in Step 1. If a component does not appear in the drop-down list, return to Step 1 and add the component.

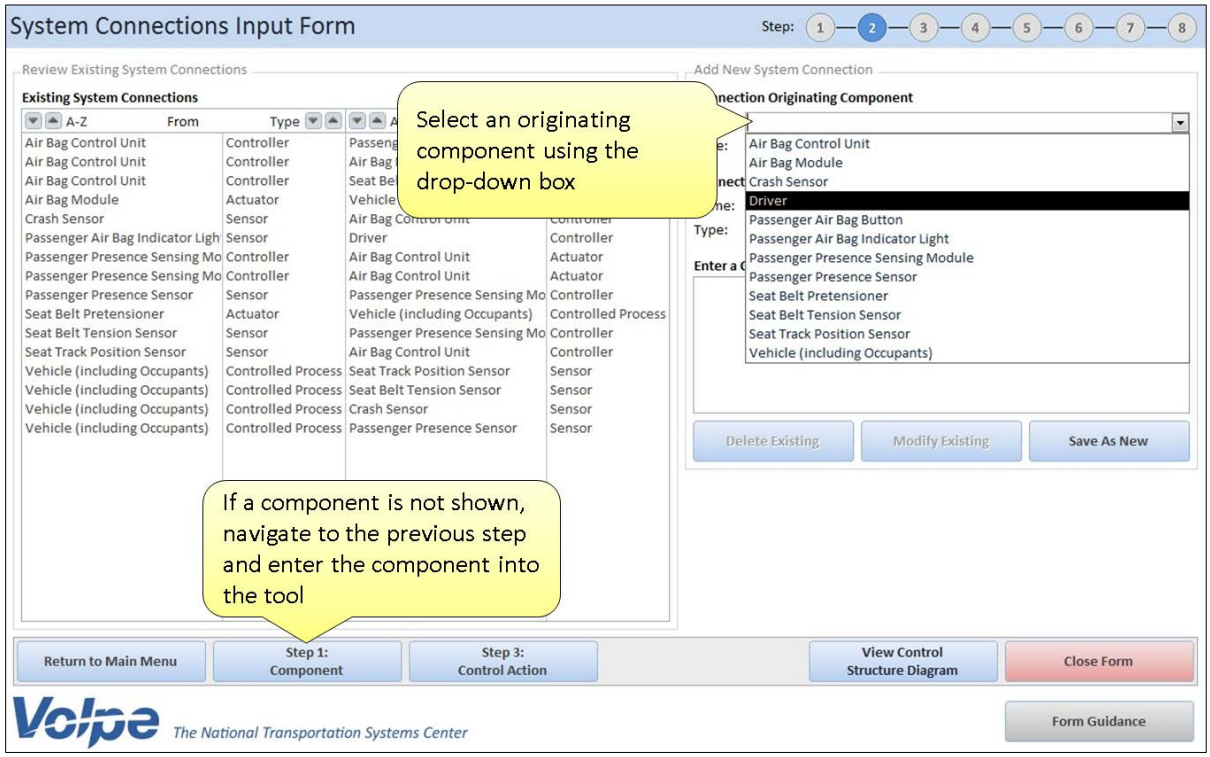


Figure 19: Selecting an Originating Component From the System Connections Input Form

2. Assign the originating component a type using the second drop-down list.

   SafetyHAT is preloaded with five component types, based on STPA. The preloaded component types are described below:

   - **Controllers** process information and issue control actions.
   - **Actuators** execute and implement control actions.
   - **Sensors** measure system states and report the information to controllers.
   - **Controlled Processes** modify behavior in response to an actuator input.
   - **Process Input Suppliers** provide resources to the Controlled Process.

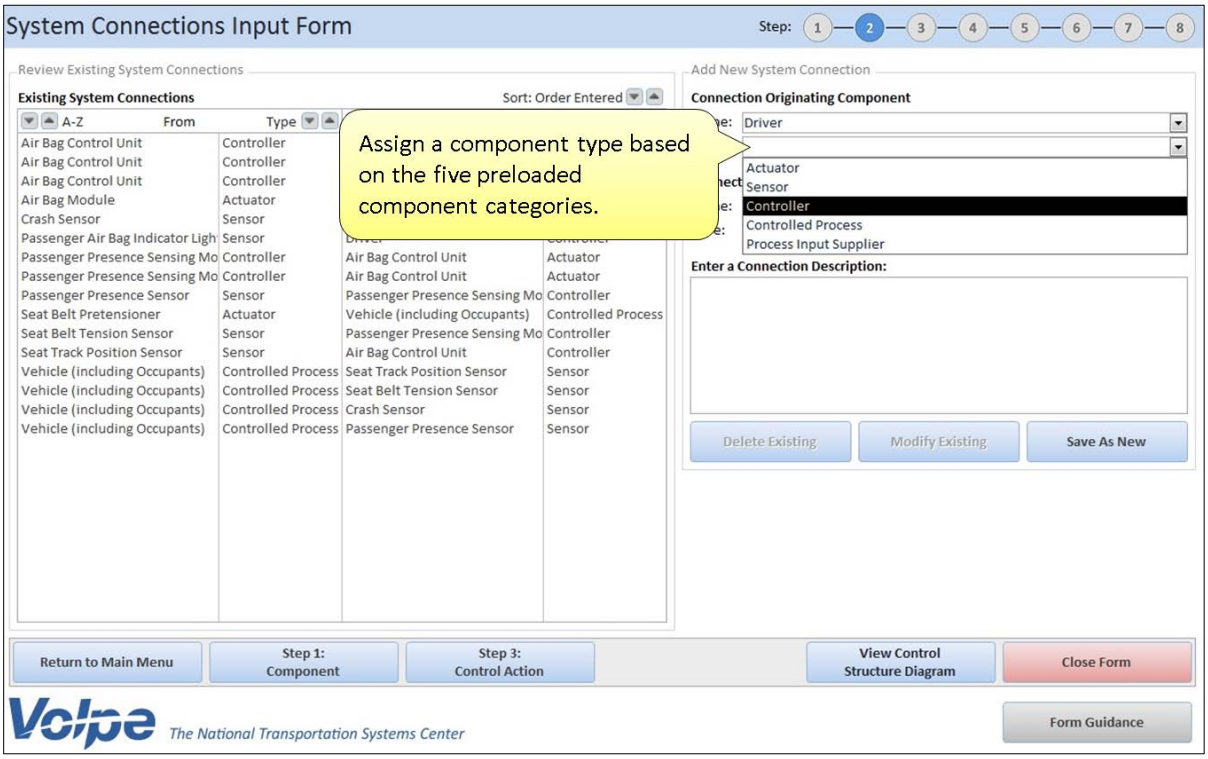


Figure 20: Selecting a Component Type From the System Connections Input Form

3. Repeat steps 1 and 2 to select a terminating component.

   SafetyHAT only allows certain connections between component types based on the STPA framework. Your available options for the terminating component type will be restricted based on the type you assigned to the originating component. For example, a connection originating from a sensor can only terminate at a controller.

4. Enter a detailed description for the connection.

5. Click the *Save As New* button.

SafetyHAT is preloaded with five component and five connection types described in STPA. These preloaded types can be modified through SafetyHAT's Advanced Options feature.

To modify an existing connection:

1. Select the connection you want to edit from the box on the left side of the form.

2. Make the necessary changes in the fields on the right side of the form.

   SafetyHAT will still restrict the allowed connection types when modifying an entry. If you attempt to create an invalid connection, the dialogue box shown in Figure 21 will appear.

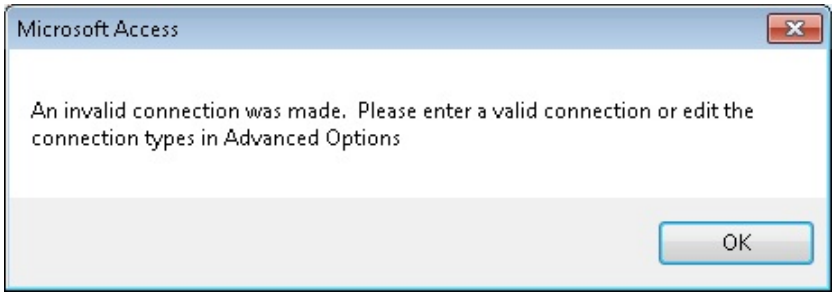


Figure 21: Invalid Connection Error Message

3. Click the *Modify Existing* button.

4. Click *Yes* to confirm your change(s).

To delete an existing component:

1. Select the component you want to delete from the box on the left side of the form.

2. Click the *Delete Existing* button.

3. Click *Yes* to confirm deletion.

3.5.3 Step 3: Control Action Input Form

A control action is the command issued by a controller that changes the system state. Control actions are necessary to ensure proper system function and ensure system safety. This form allows you to enter, modify, or delete control actions for components you designated as controllers in Step 2. The layout of the Control Action Input Form is shown in Figure 22.

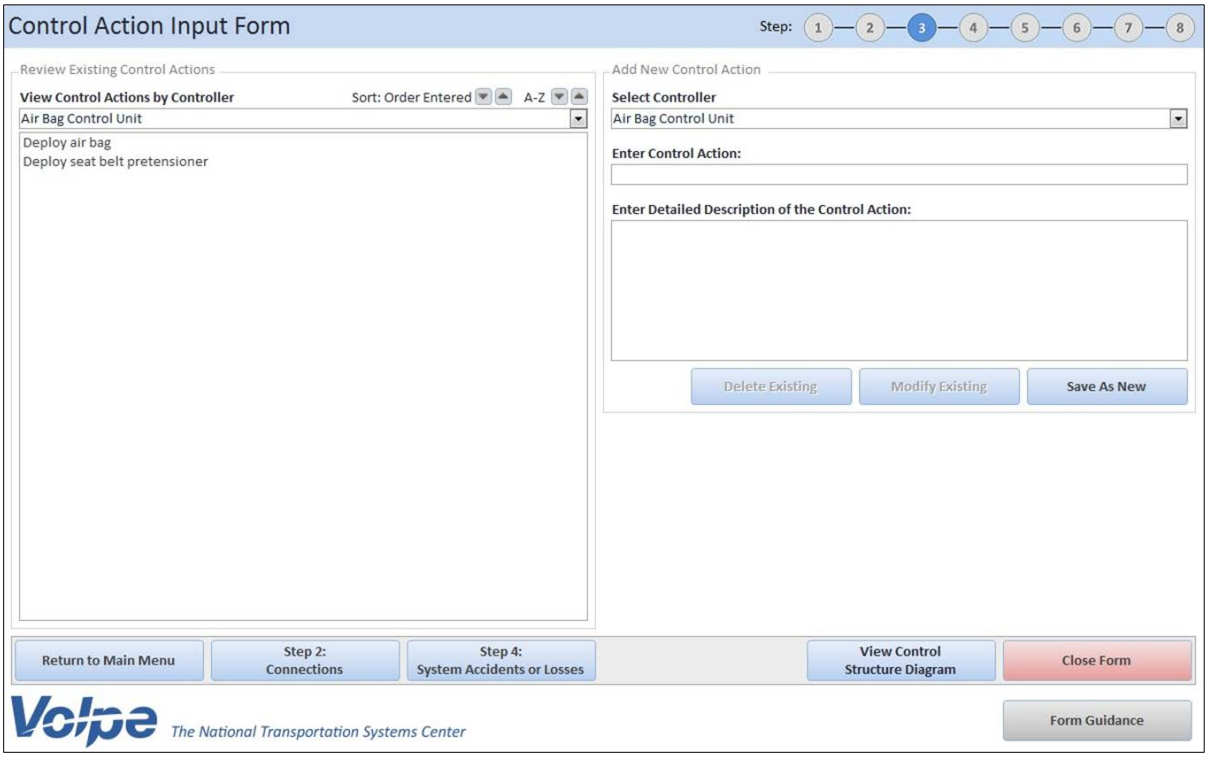


Figure 22: Control Action Input Form

Control actions are typically specific to the controller and system being analyzed, and should be clearly defined. For the air bag control example, the air bag controller may issue the control action "Deploy Air Bag". A single control action should not include more than one command. For example, the control action "Indicator Light On/Off" is ambiguous. Instead, input the separate control actions "Indicator Light On" and "Indicator Light Off". This will facilitate your analysis in later stages of SafetyHAT.

A control action should not include more than one command. For example, enter "Indicator Light On" and "Indicator Light Off" separately, instead of "Indicator Light On/Off".

To enter a new control action:

1. Select a controller using the drop-down list on the right side of this form (see Figure 23).

   Any component you designated as a controller in Step 2 will appear in this list. Once you select a controller, the list of existing control actions for that controller will be shown on the left side of the form. If a controller does not appear in the drop-down list, return to Step 2 and make sure the component was entered as a controller for at least one system connection.

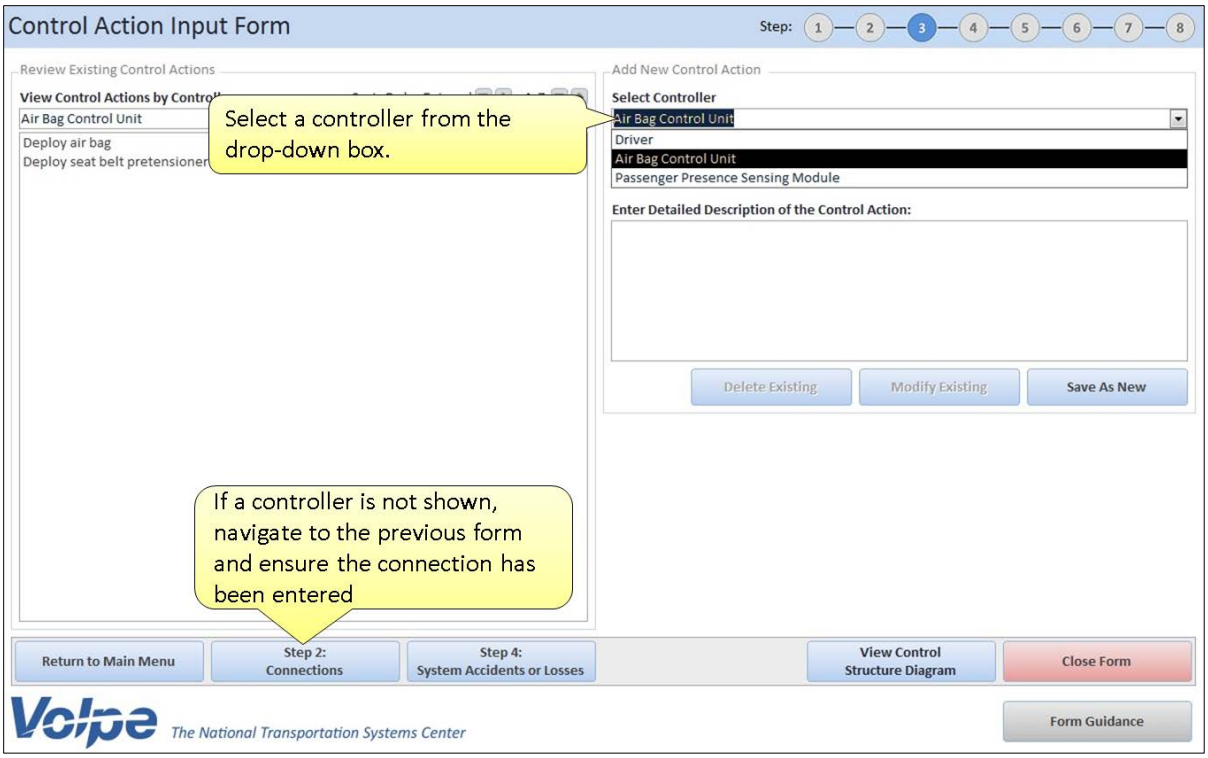


Figure 23: Selecting a Controller in the Control Action Input Form

2. Enter the control action phrase in the entry field below the controller (see Figure 24).

3. Enter a detailed description of the control action in the last entry field (see Figure 24).

4. Click the *Save As New* button.

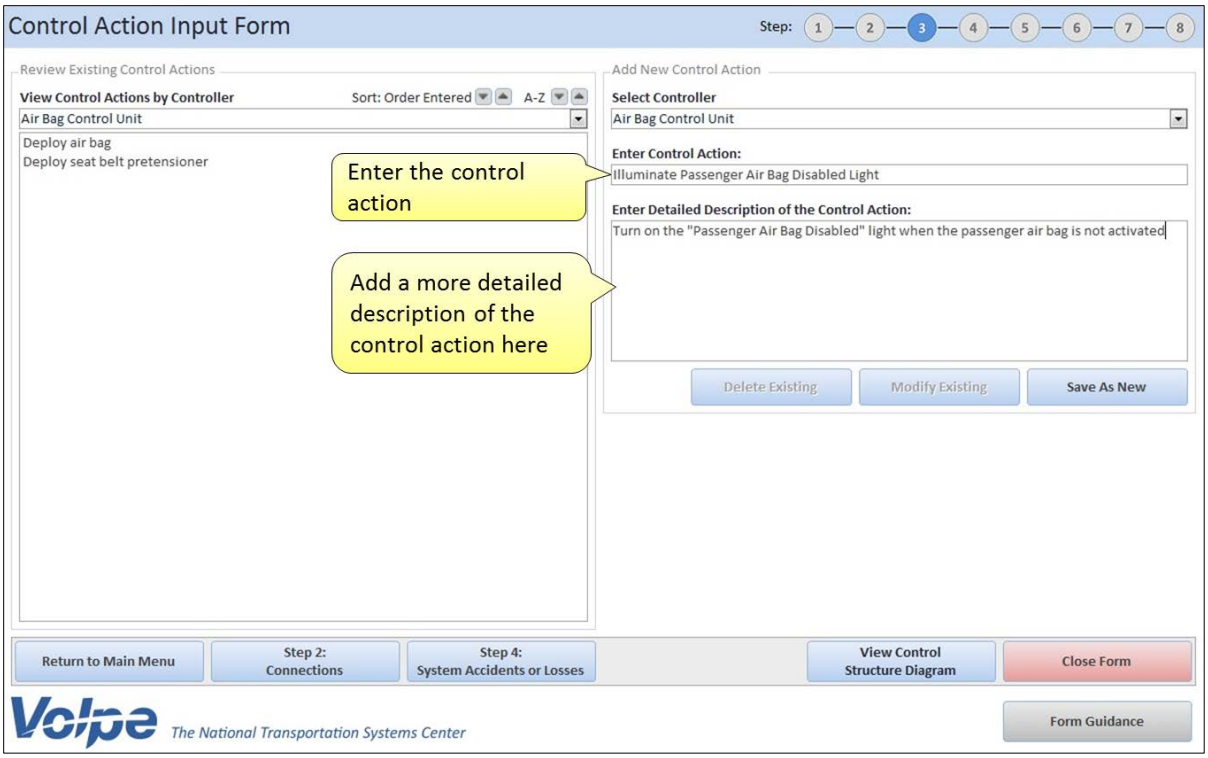


Figure 24: Entering a Control Action in the Control Action Input Form

To modify an existing control action:

1. Select a controller from the drop-down list on the left side of the form (see Figure 25).
2. Select the control action you want to edit from the box on the left side of the form.
3. Make the necessary changes in the fields on the right side of the form.
4. Click the *Modify Existing* button.
5. Click *Yes* to confirm your change(s).

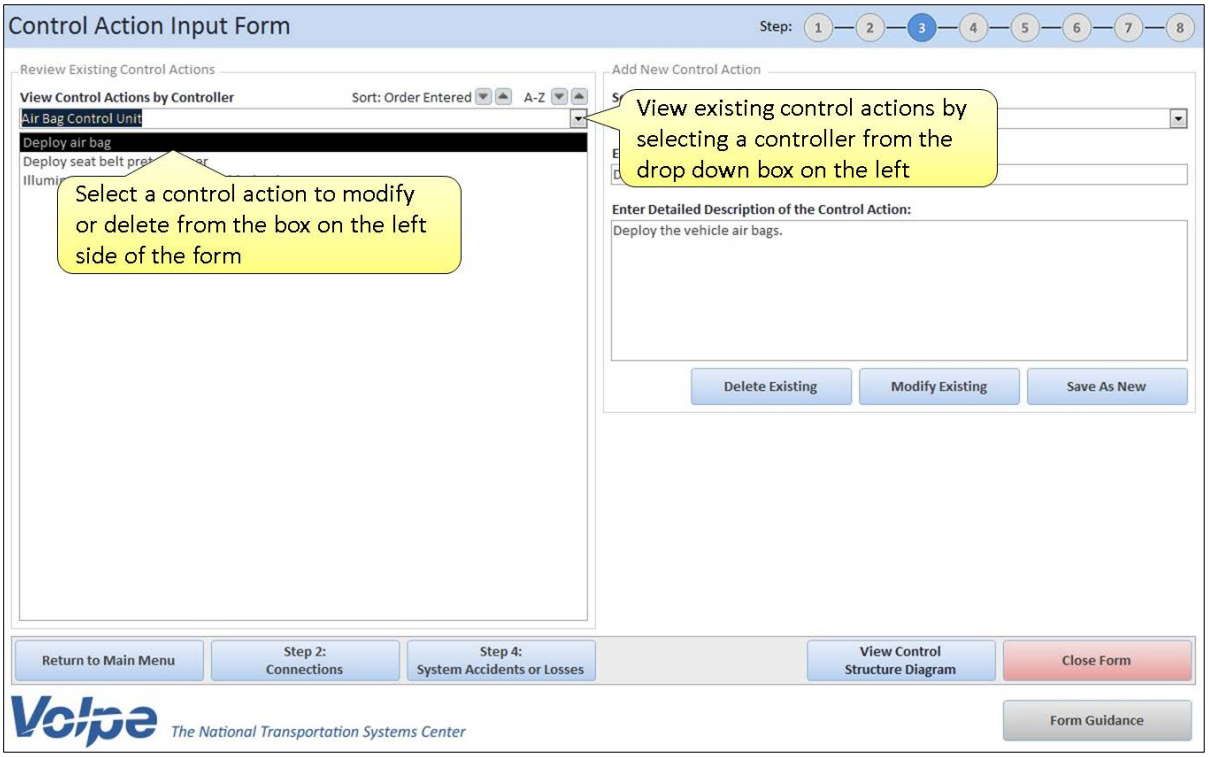


Figure 25: Selecting a Control Action to Modify or Delete in the Control Action Input Form

To delete an existing control action:

1. Select a controller from the drop-down list on the left side of the form (see Figure 25).
2. Select the control action you want to delete from the box on the left side of the form.
3. Click the *Delete Existing* button.
4. Click *Yes* to confirm deletion.

3.5.4 Step 4: Accident (or Losses) Input Form

In STPA an accident is defined as "an undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc." [1] For example, accidents may include loss of life, loss of property, or environmental contamination. The Accident (or Losses) Input Form allows you to enter, modify, or delete system-level accidents in SafetyHAT. The layout of the Accident (or Losses) Input Form is shown in Figure 26.

Accidents should not be confused with hazards. Accidents are undesired events and hazards are system states that lead to accidents in worst-case environmental conditions.

To enter a new system-level accident:

1. Enter the system-specific accident in the first field on the right side of the form (see Figure 26).
2. Enter a detailed description of the accident in the second field on the right side of the form.
3. Click the *Save As New* button.

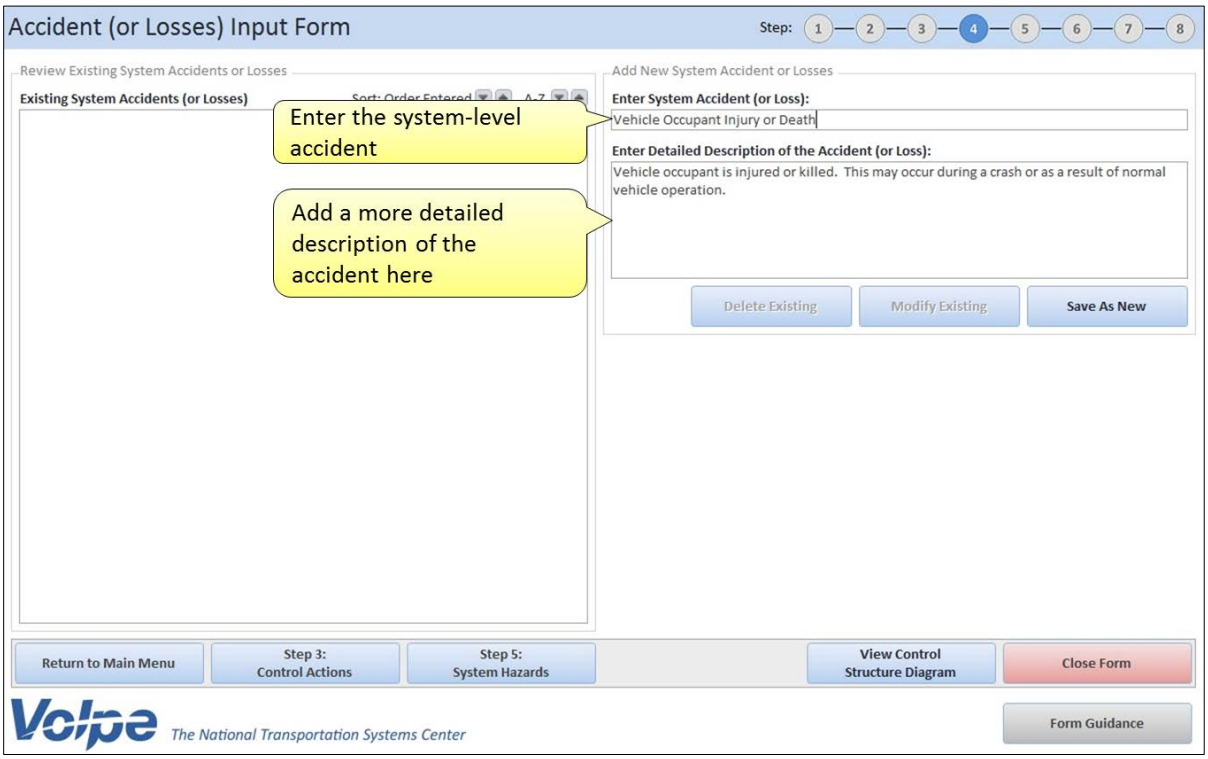


Figure 26: Accident (or Losses) Input Form

To modify an existing accident:

1. Select the accident you want to edit from the box on the left side of the form.
2. Make the necessary changes in the fields on the right side of the form.
3. Click the *Modify Existing* button.
4. Click *Yes* to confirm your change(s).

To delete an existing accident:

1. Select the accident you want to delete from the box on the left side of the form.

2. Click the *Delete Existing* button.

3. Click *Yes* to confirm deletion.

3.5.5 Step 5: Hazard Input Form

Hazards are defined as system states or conditions that lead to a system accident under a specific set of worst-case environmental conditions. Hazards are typically high-level and broadly defined conditions, such as "Vehicle Instability" or "Unexpected Deceleration". You should make sure not to confuse hazards with accidents (unwanted consequences from a hazard) or control actions (lower-level commands that could potentially lead to a hazard).

To enter a new system-level hazard:

1. Enter the hazard in the first field on the right side of the form (see Figure 27).

2. Add a detailed description of the hazard in the second field on the right side of the form.

3. Associate one or more of the system-level accidents with this hazard by clicking on the accident in the list box on the right side of the form.

   If an accident does not appear in the list on the right side of the form, return to Step 4 and add the accident.

4. Click the *Save As New* button.

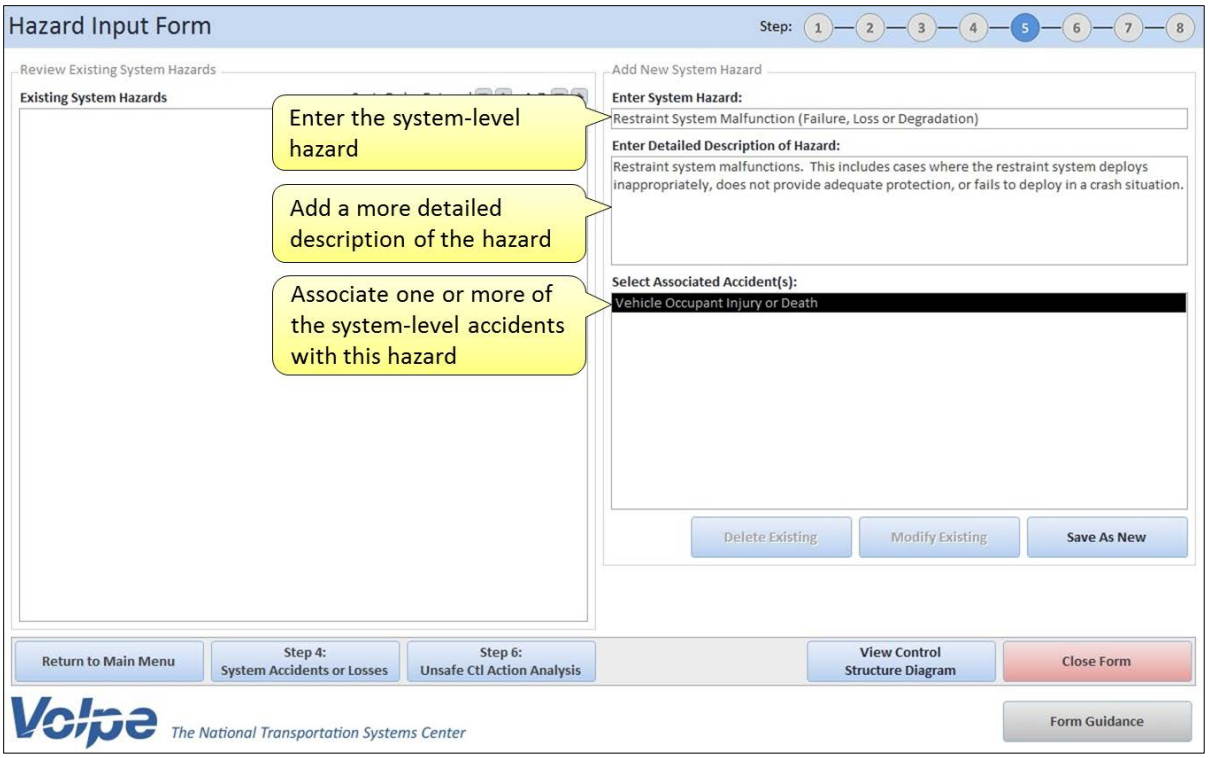


Figure 27: Hazard Input Form

To modify an existing hazard:

1. Select the hazard you want to edit from the box on the left side of the form.
2. Make the necessary changes in the fields on the right side of the form.
3. Click the *Modify Existing* button.
4. Click *Yes* to confirm your change(s).

To delete an existing hazard:

1. Select the hazard you want to delete from the box on the left side of the form.
2. Click the *Delete Existing* button.
3. Click *Yes* to confirm deletion.

3.5.6 Step 6: Unsafe Control Action (UCA) Analysis

The Unsafe Control Action (UCA) Analysis form will help you assess which of the potential unsafe control action scenarios may lead to the system-level hazards you entered in Step 5 of SafetyHAT. Figure 28 shows the general layout of the UCA Analysis form.

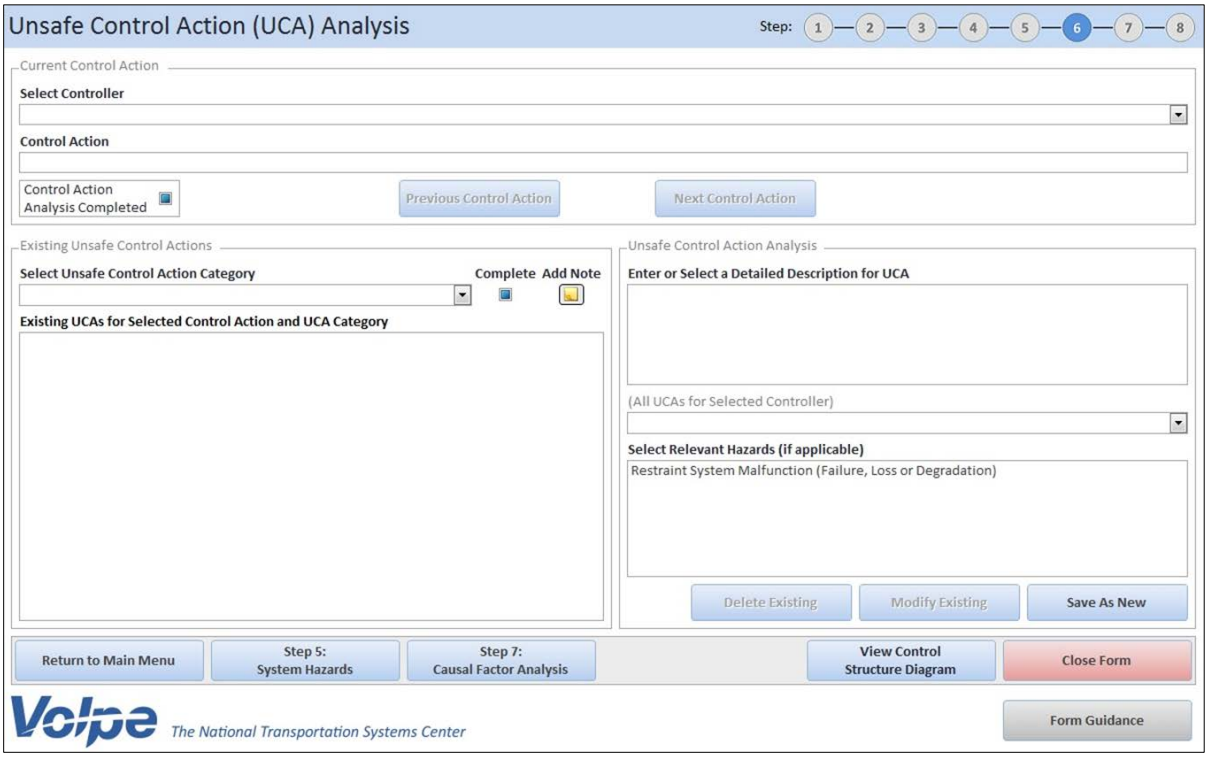


Figure 28: Unsafe Control Action (UCA) Analysis Form

The system will not enter a hazardous state unless an unsafe control action has been issued by a controller or a required control action to remain safe was not issued by a controller. Not all unsafe control action scenarios will lead to the hazardous system states you are evaluating with SafetyHAT. Conversely, some unsafe control action scenarios may lead to more than one hazardous state. Figure 29 shows a sample unsafe control action analysis.

An example Unsafe Control Action analysis:

Controller:	Air Bag Control Module
Control Action:	Deploy Air Bag
Unsafe Control Action Guide Phrase:	A control action is NOT PROVIDED WHEN NEEDED, causing hazard
Detailed UCA Description:	The air bag is deployed when the vehicle is not in a crash.
Associated System Hazard:	Restraint System Loss or Degradation

Figure 29: An Example Unsafe Control Action Analysis

To evaluate an unsafe control action:

1. Select a system controller from the drop-down list at the top of the form (see Figure 30).

   If a controller does not appear in the drop-down list, return to Step 3 and make sure you have entered at least one control action for that controller. The first control action for the selected controller will be shown in the field below the drop-down list.

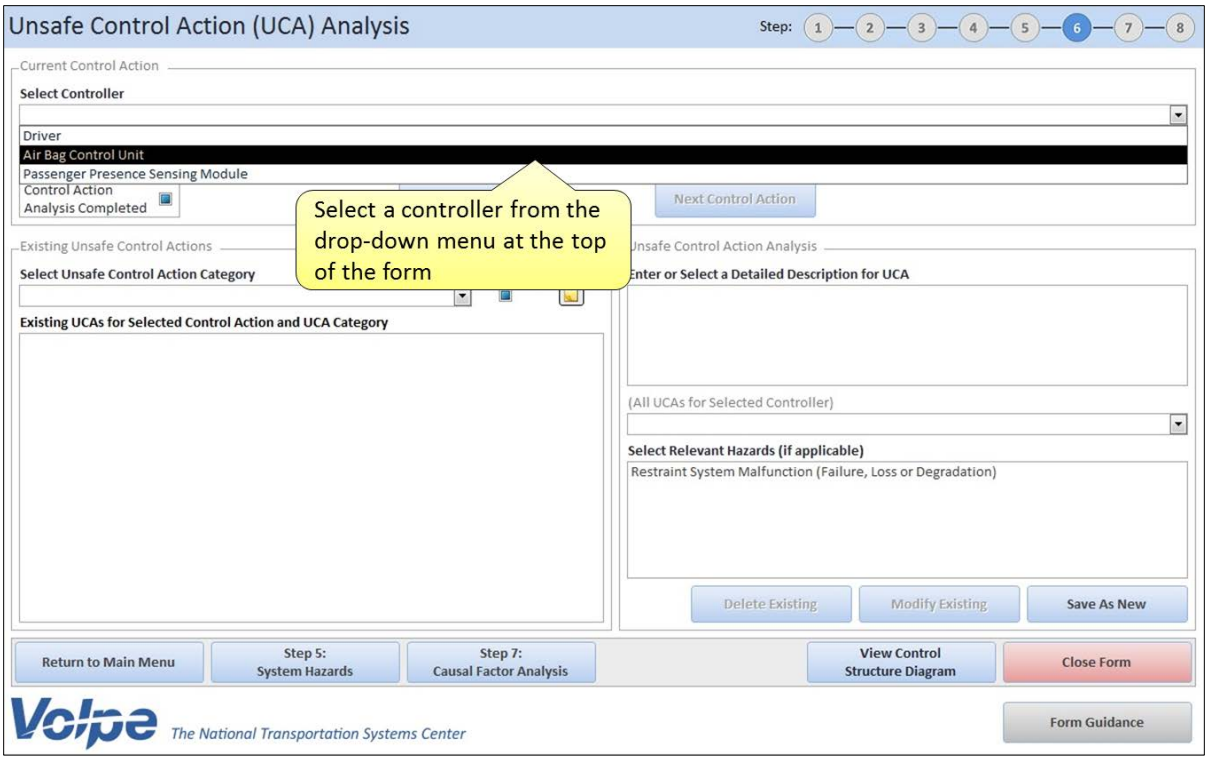


Figure 30: Selecting a Controller in the Unsafe Control Action (UCA) Analysis Form

2. Select one of the Unsafe Control Action guide phrases from the drop-down list on the left side of the form (see Figure 31).

   After selecting a UCA guide phrase, the existing descriptions for the current control action and UCA guide phrase will be shown in the below the drop-down list.

   SafetyHAT has six preloaded UCA guide phrases. These guide phrases are designed to help you consider ways in which the control action at the top of the form could lead to an unsafe condition.

   In the drop-down list, two columns are located to the right of the UCA guide phrase.

   - The first column corresponds to the "Complete" check box. A "Y" in this column indicates that you have already designated the analysis for that UCA guide phrase as complete.

   - The second column corresponds to the "Note" button. A "Y" in this column indicates that a note was entered for this UCA guide phrase.

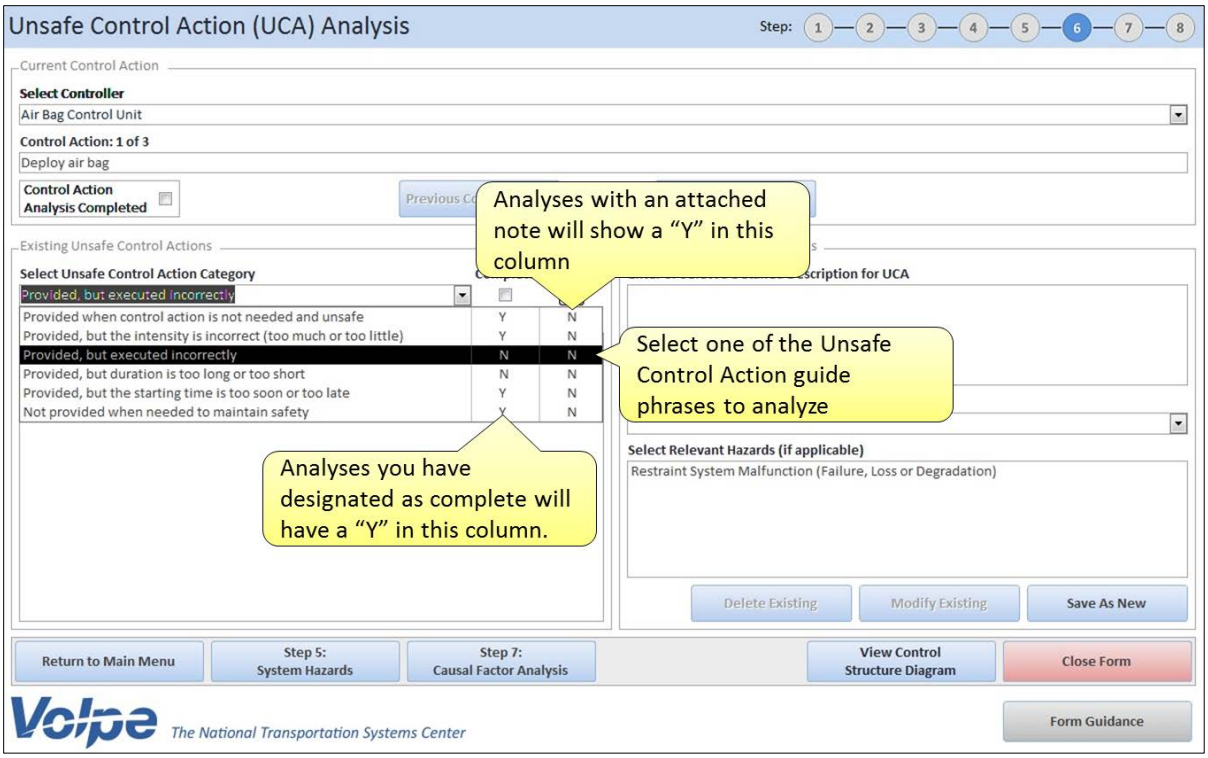


Figure 31: Selecting a UCA Guide Phrase to Analyze in the Unsafe Control Action (UCA) Analysis Form

3. Enter a more detailed description of the unsafe control action in the first field on the right side of the form.

    - Since the preloaded UCA guide phrases are generic, a system-specific description is necessary to explain how the UCA guide phrase affects your system.

    - If you want to re-use a detailed UCA description that already has been entered, the drop-down list on the right side of the form will provide you with a list of existing UCA descriptions for the current controller.

4. Associate one or more system hazards with the UCA description by selecting the hazards in the last field on the right side of the form. If a UCA description is not associated with a hazard, the description will be saved in SafetyHAT but will not appear in Step 7 for further analysis.

5. Click the *Save As New* button.

SafetyHAT is preloaded with six Unsafe Control Action guide phrases. These guide phrases can be modified through SafetyHAT's Advanced Options feature.

To ensure a complete analysis, each UCA guide phrase should be evaluated. However, not all UCAs may lead to the system hazards being considered in your project.

To modify an existing UCA description:

1. Select the UCA description you want to edit from the box on the left side of the form.

   If no UCA descriptions are shown, make sure a UCA guide phrase has been selected from the drop-down list on the left side of the form.

2. Make the necessary changes in the fields on the right side of the form.

3. Click the *Modify Existing* button.

4. Click *Yes* to confirm your change(s). The dialogue box shown in Figure 32 will appear.

   - Clicking *Yes* will apply your change to the current description. This change will also be applied anywhere else the current description appears for the current controller. Use this feature if you want to make your edit universal.

   - Clicking *No* will only apply your change to the current description. If the current description appears elsewhere, those entries will *not* be changed. Use this feature if you only want to edit a single entry.

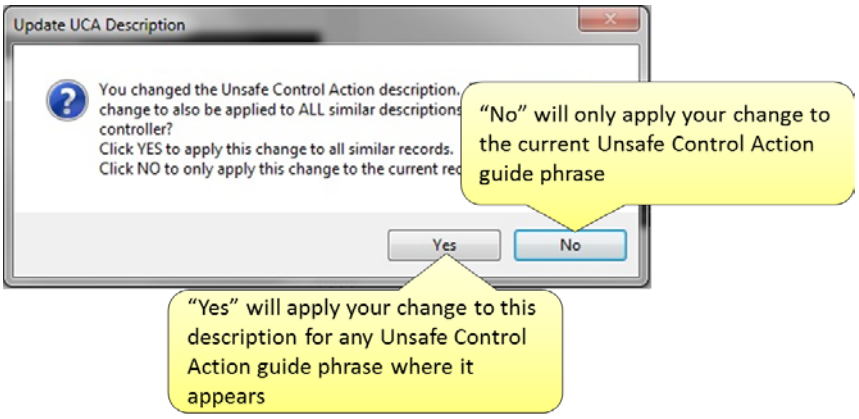


Figure 32: Confirming Modification of an Entry in the Unsafe Control Action (UCA) Analysis Form

To delete an existing UCA description:

1. Select the UCA description you want to delete from the box on the left side of the form.

   If no UCA descriptions are shown, make sure a UCA guide phrase has been selected from the drop-down list on the left side of the form.

2. Click the *Delete Existing* button.

3. Click *Yes* to confirm deletion.

More than one description can be entered for each UCA guide phrase. Continue adding new descriptions until all relevant unsafe control action descriptions have been added for a particular control action / unsafe control action guide phrase pairing. After you have completed entering the descriptions for a UCA guide phrase, you can mark the guide phrase as complete (see Figure 33).

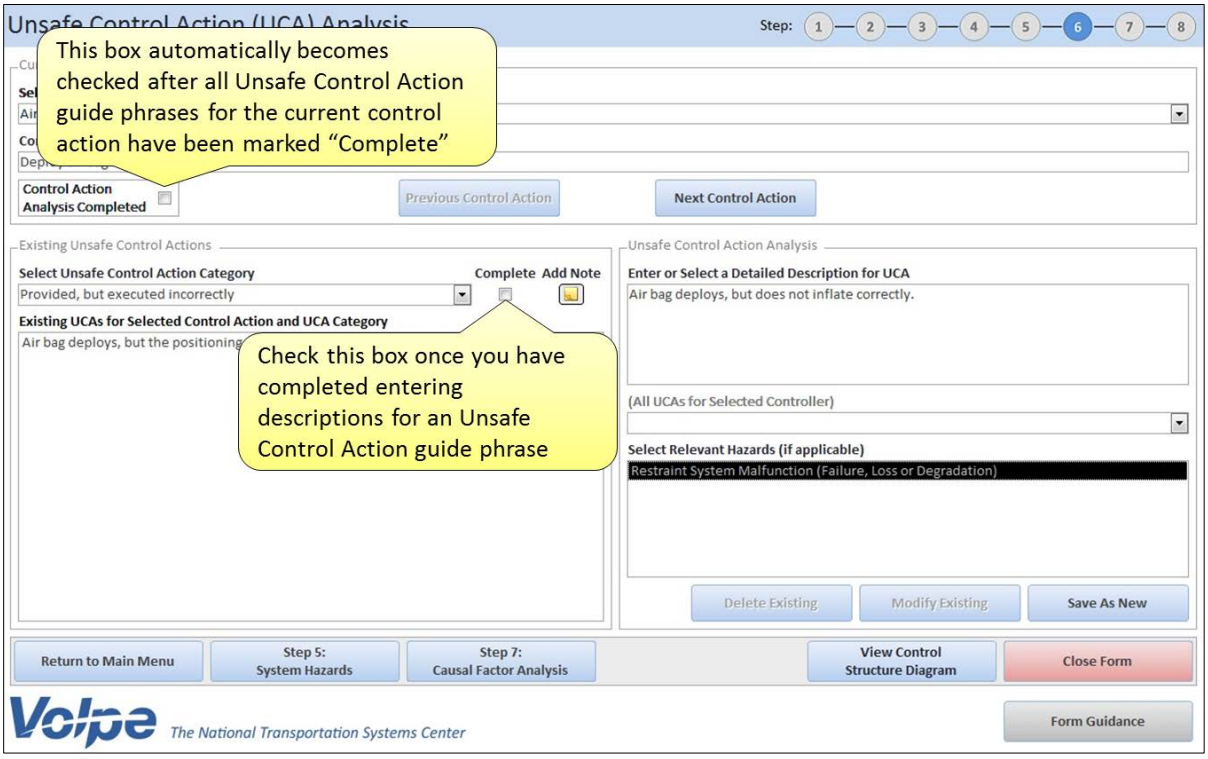


Figure 33: Marking a UCA Guide Phrase as "Complete" in the Unsafe Control Action (UCA) Analysis Form

For a complete analysis, each UCA guide phrase in the drop-down list on the left side of the screen should be evaluated for each control action. Likewise, each control action and controller should be fully analyzed.

After all UCA guide phrases for a control action have been designated as complete, the check box at the top of the form will automatically become marked. This will help you quickly identify control actions which still require unsafe control action analysis.

To navigate between control actions, there are two navigation buttons located at the top of the form (see Figure 34).

- The *Next Control Action* button will take you to the next control action for the current controller. This button will be disabled on the last control action for the current controller.

- The *Previous Control Action* button will take you to the previous control action for the current controller. This button will be disabled on the first control action for the current controller.

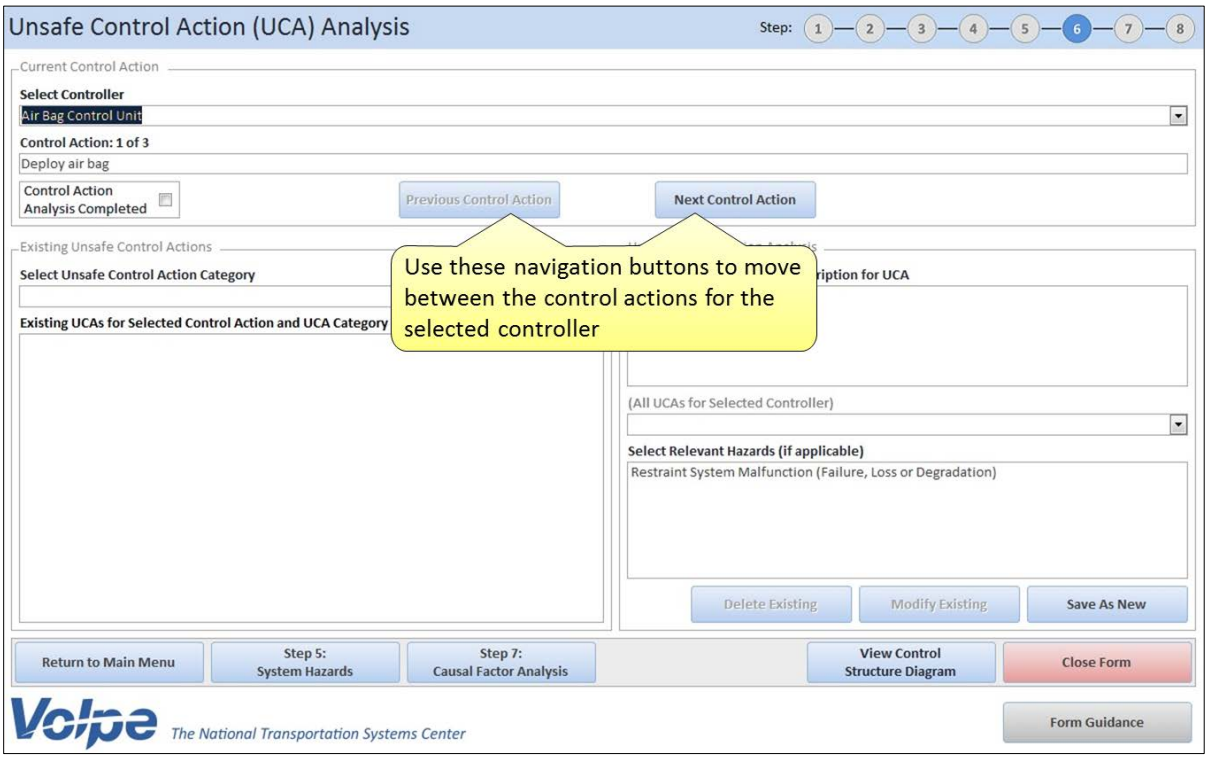


Figure 34: Navigating Between Control Actions in the Unsafe Control Action (UCA) Analysis Form

SafetyHAT allows you to attach a note to the selected UCA guide phrase for the current control action by clicking the *Add Note* button (see Figure 35). This feature lets you store personal notes for your analysis, similar to a "sticky-note". Information entered as a note does not appear in your final output from SafetyHAT.

The layout of the note entry screen is shown in Figure 36.

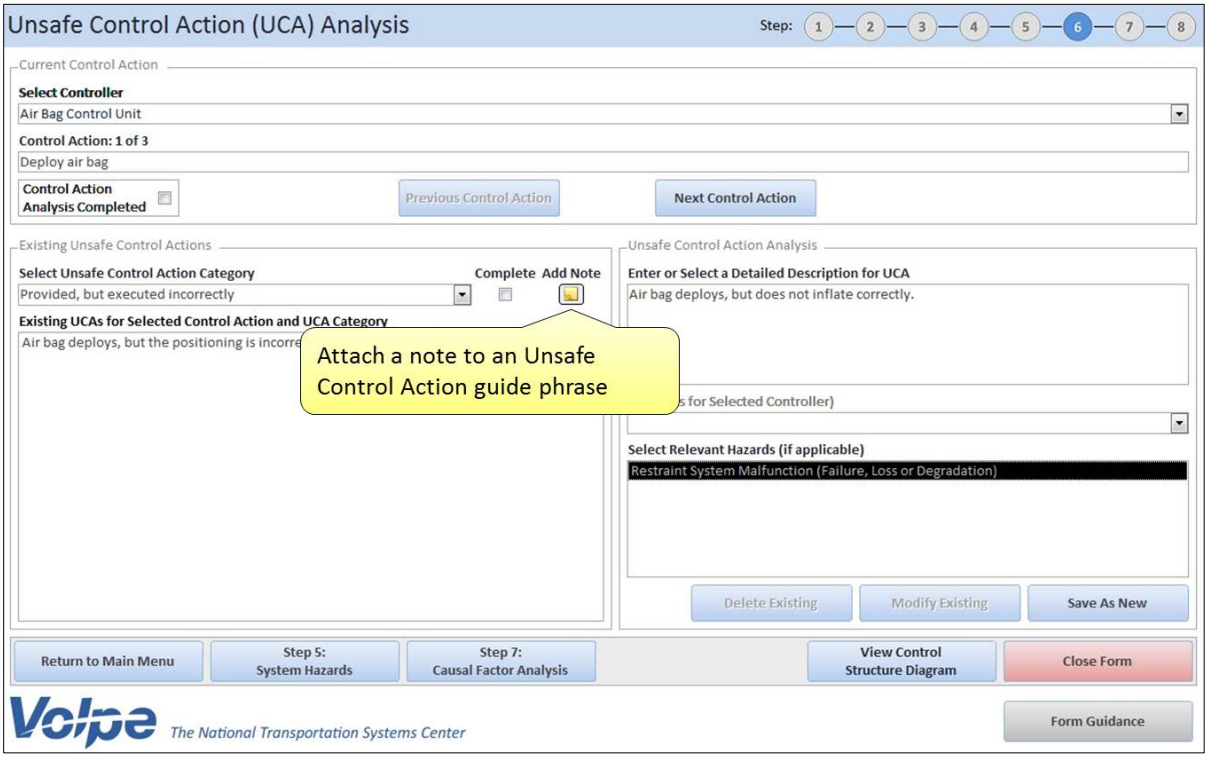


Figure 35: Adding a Note in the Unsafe Control Action (UCA) Analysis Form

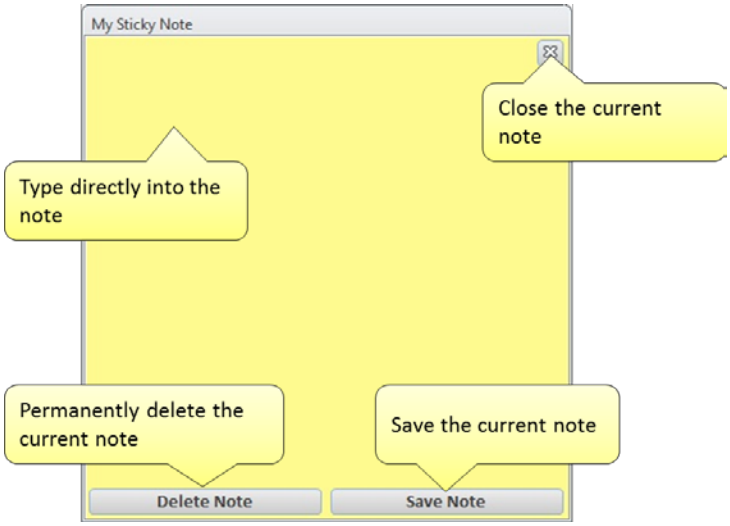


Figure 36: Note Form

To add a note:

1. Click the *Add Note* button on the Unsafe Control Action (UCA) Analysis Form.

2. Type your note directly into the note form.

3. Click the *Save Note* button on the note form.

To delete a note

1. Click the *Add Note* button on the Unsafe Control Action (UCA) Analysis Form.

2. Click the *Delete Note* button on the note form.

The background of the *Add Note* button will change to yellow after a note has been added. The corresponding column in the unsafe control action guide phrase drop-down list will also be marked with a "Y".

3.5.7 Step 7: Causal Factor Analysis

The Causal Factor Analysis form will guide you through analyzing how the components and connections in your system may lead to unsafe control actions. Figure 37 shows the general layout of the Causal Factor Analysis form.

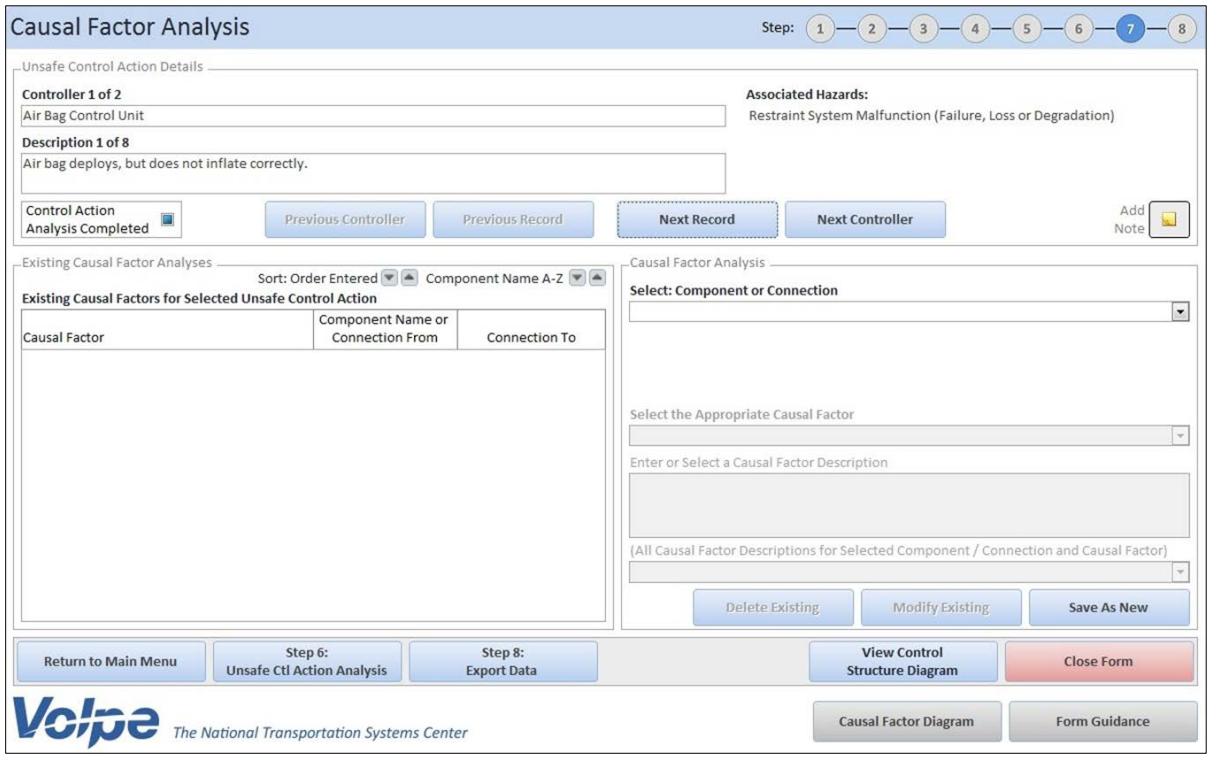


Figure 37: Causal Factor Analysis Form

SafetyHAT provides you with unsafe control actions to analyze based on the unsafe control action descriptions you associated with system hazards in Step 6. The details of each unsafe control action are shown at the top of the form. You can navigate between unsafe control action descriptions using the *Next Record* and *Previous Record* buttons (see Figure 38). The *Next Controller* and *Previous Controller* buttons let you move quickly between controllers.

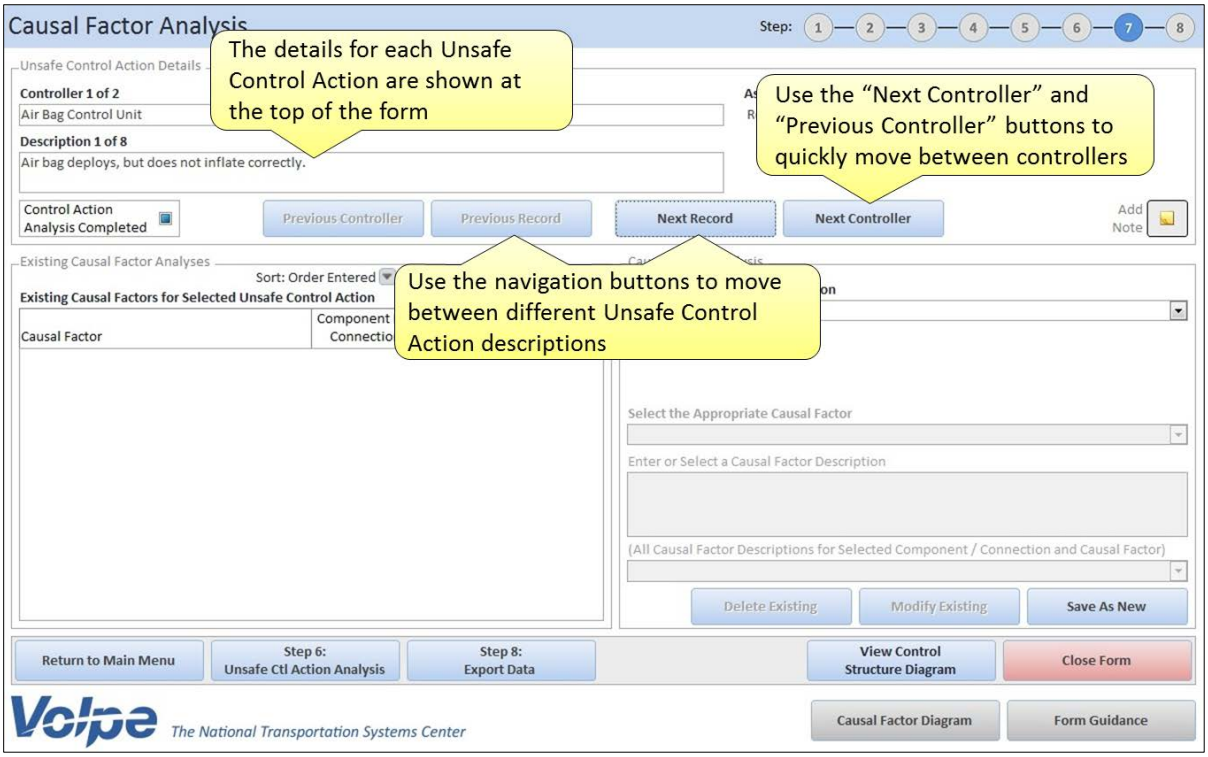


Figure 38: Navigating Between Controllers and Control Actions in the Causal Factor Analysis Form

STPA provides guidance in conducting the causal factor analysis through the use of "causal factor guide phrases", which provide generalized descriptions for how components or connections in the system could lead to an unsafe control action occurring. Since these causal factor guide phrases are generalized, it is incumbent on the user to provide the system-specific details. Multiple causal factors may exist for each unsafe control action description.

To evaluate causal factors related to system **components**:

1. Select “Component” from the first drop-down list on the right side of the form (see Figure 39).

   SafetyHAT will automatically limit your available options in subsequent steps to system components and component-related causal factors.

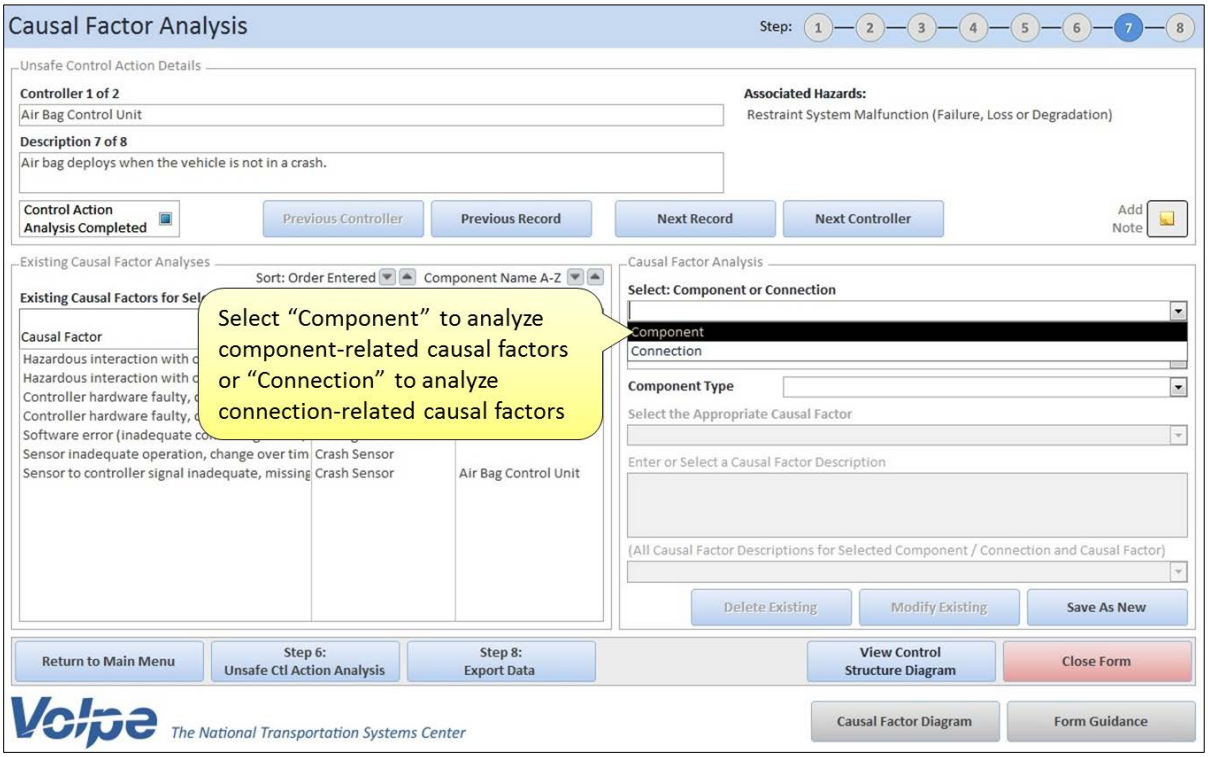


Figure 39: Selecting the Component or Connection Category in the Causal Factor Analysis Form

2. Select a component to analyze from the second drop-down list on the right side of the form (see Figure 40).

   SafetyHAT generates this list from the system components you entered in Step 1 of SafetyHAT.

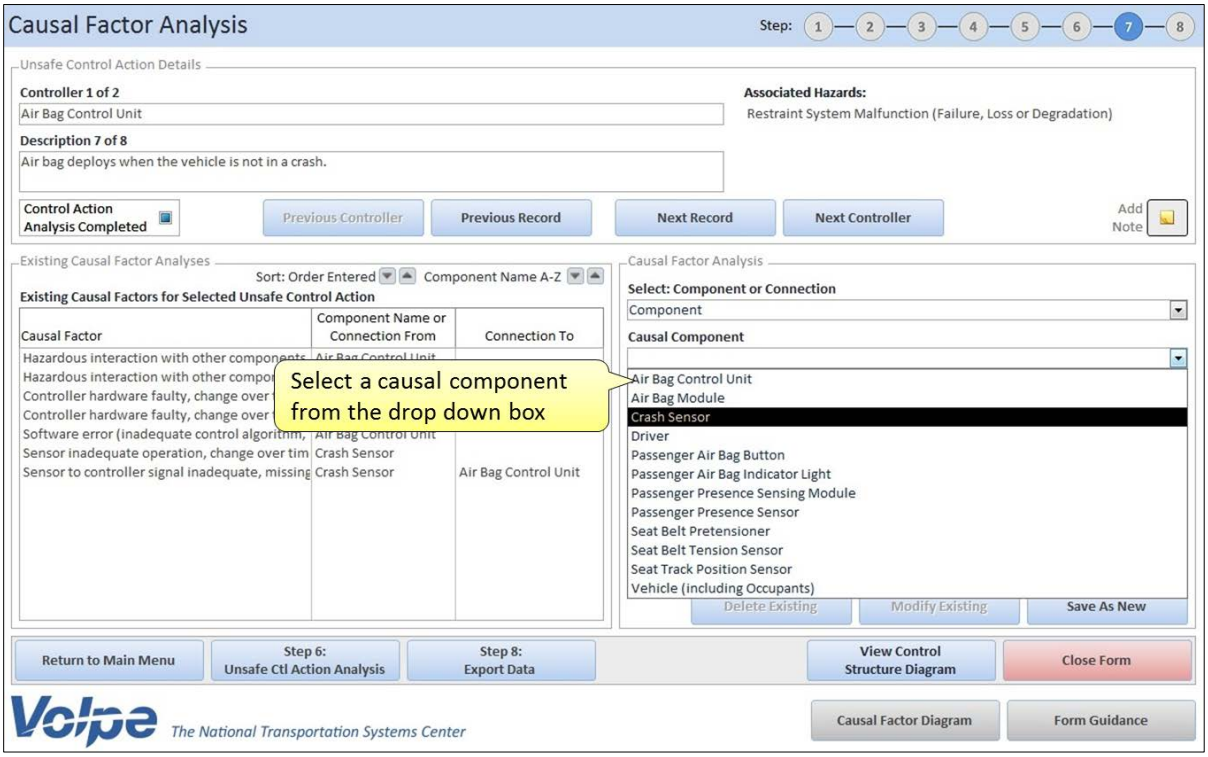


Figure 40: Selecting a System Component in the Causal Factor Analysis Form

3. Select a component type from the third drop-down list on the right side of the form (see Figure 41).

   The available options in this drop-down list are based on the types you assigned to the selected component when defining the system connections in Step 2 of SafetyHAT. SafetyHAT uses your selection in this drop-down list to generate a list of relevant causal factor guide phrases.

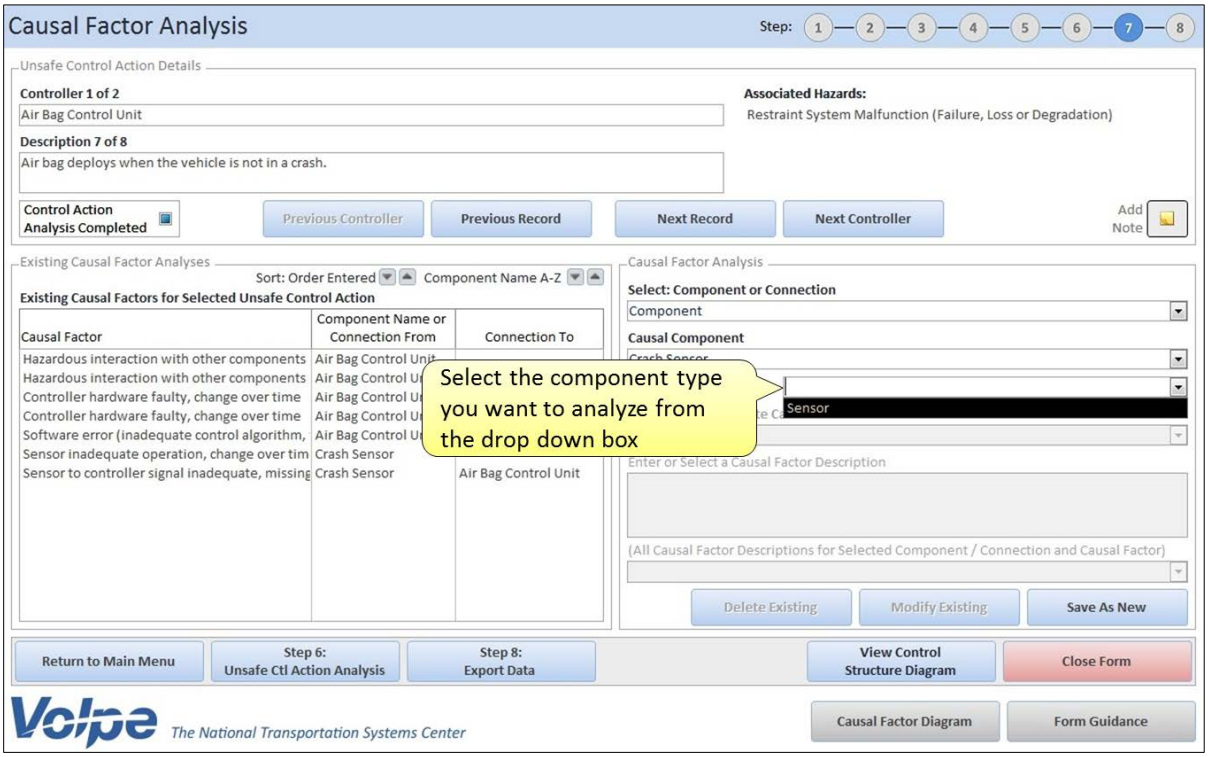


Figure 41: Selecting a Component Type in the Causal Factor Analysis Form

4. Select a generalized causal factor guide phrase from the fourth drop-down list on the right side of the form (see Figure 42).

   The available guide phrases are based on the component type you selected in the previous step. If you need additional guidance on selecting a causal factor, a graphical representation of the causal factors and their relation to a simplified control structure diagram can be accessed by clicking the *Causal Factor Diagram* button at the bottom of the Causal Factor Analysis form.

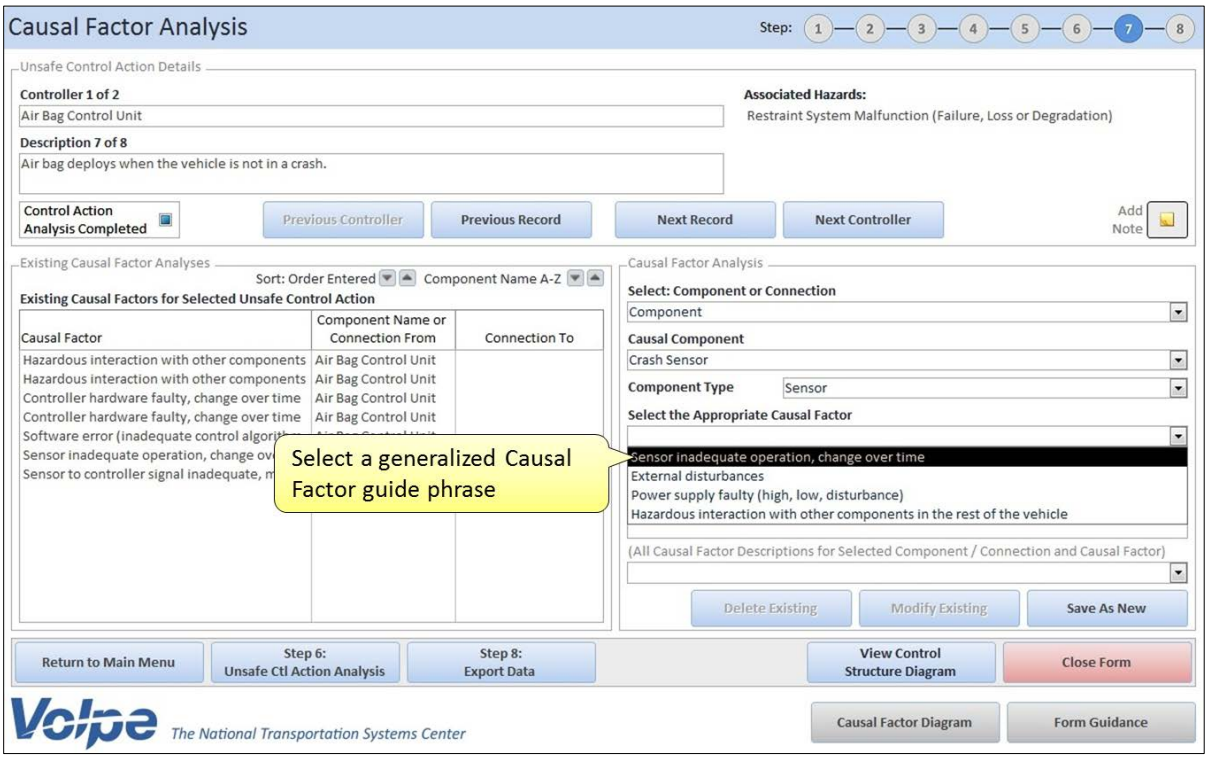


Figure 42: Selecting a Causal Factor Guide Phrase in the Causal Factor Analysis Form

5. Enter a system-specific description of the causal factor in the text field on the right side of the form (see Figure 43).

   Since the causal factor guide phrase is generalized, this description helps relate the causal factor to your specific system. You can also apply an existing description to your current selection using the last drop-down list on the right side of the form. The available selections in this drop-down list are based on your current component and causal factor guide phrase selection.

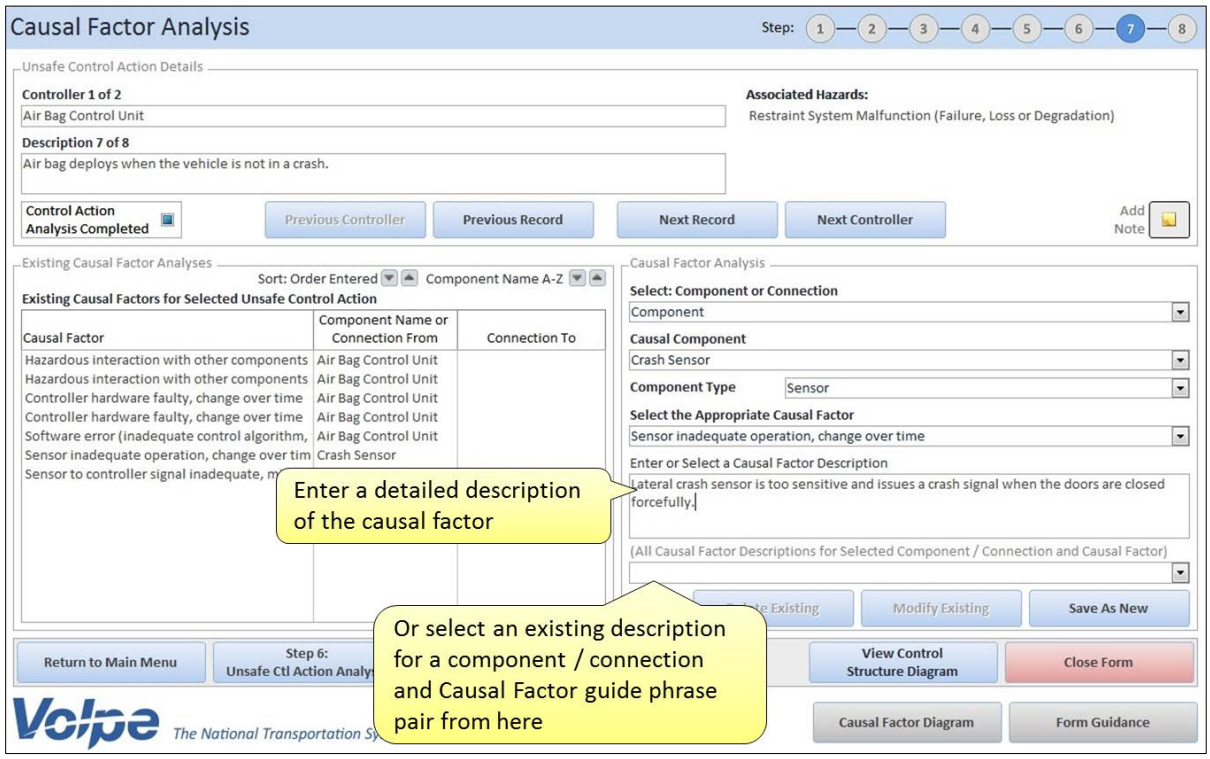


Figure 43: Entering a Causal Factor Description in the Causal Factor Analysis Form

6. Click the *Save As New* button.

Selecting an existing entry from the drop-down list is an efficient way to copy entries between unsafe control action descriptions.

To evaluate causal factors related to system connections:

1. Select “Connection” from the first drop-down list on the right side of the form (see Figure 39).

   This selection will cause SafetyHAT to limit your available options in subsequent steps to system connections and connection-related causal factors.

2. Select the originating component for the connection from the second drop-down list on the right side of the form (see Figure 44).

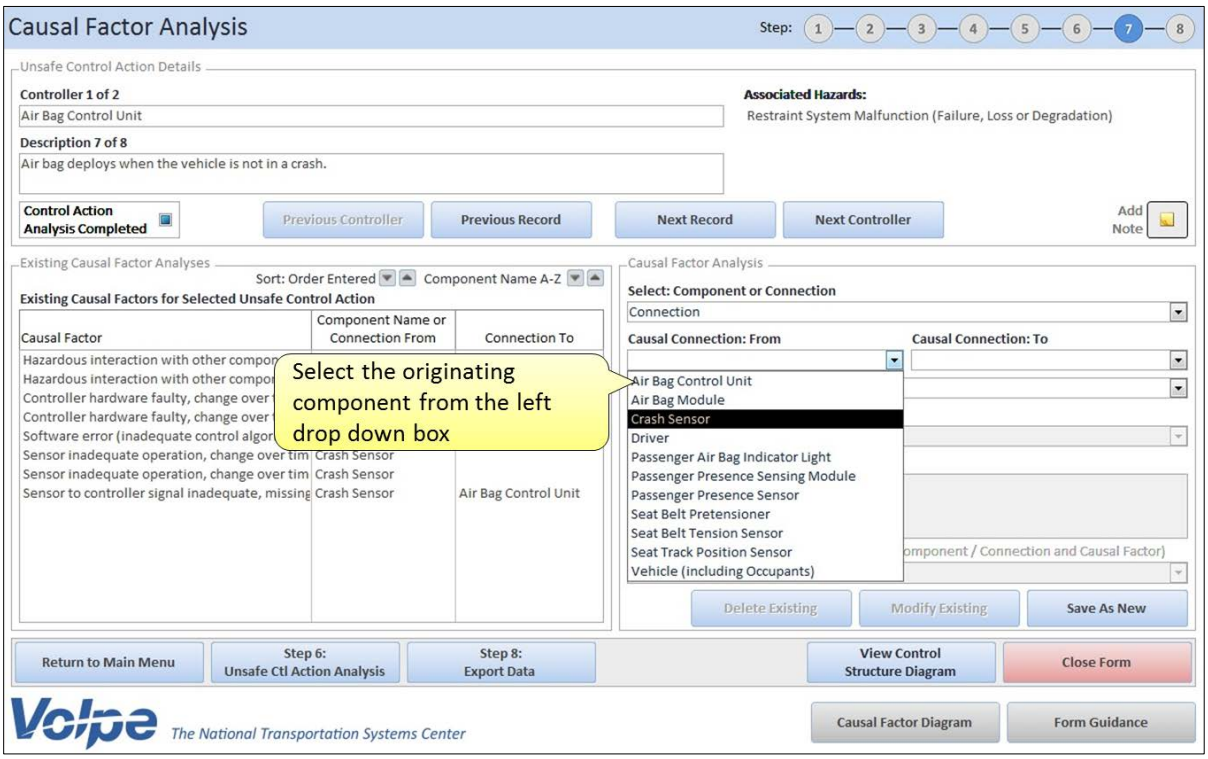


Figure 44: Selecting an Originating Component for Connection in the Causal Factor Analysis Form

3. Select the terminating component from the third drop-down list on the right side of the form (see Figure 45).

   SafetyHAT automatically filters the terminating components based on the system connections you defined in SafetyHAT Step 2. Only components you connected to the selected originating component will be shown in this drop-down list.

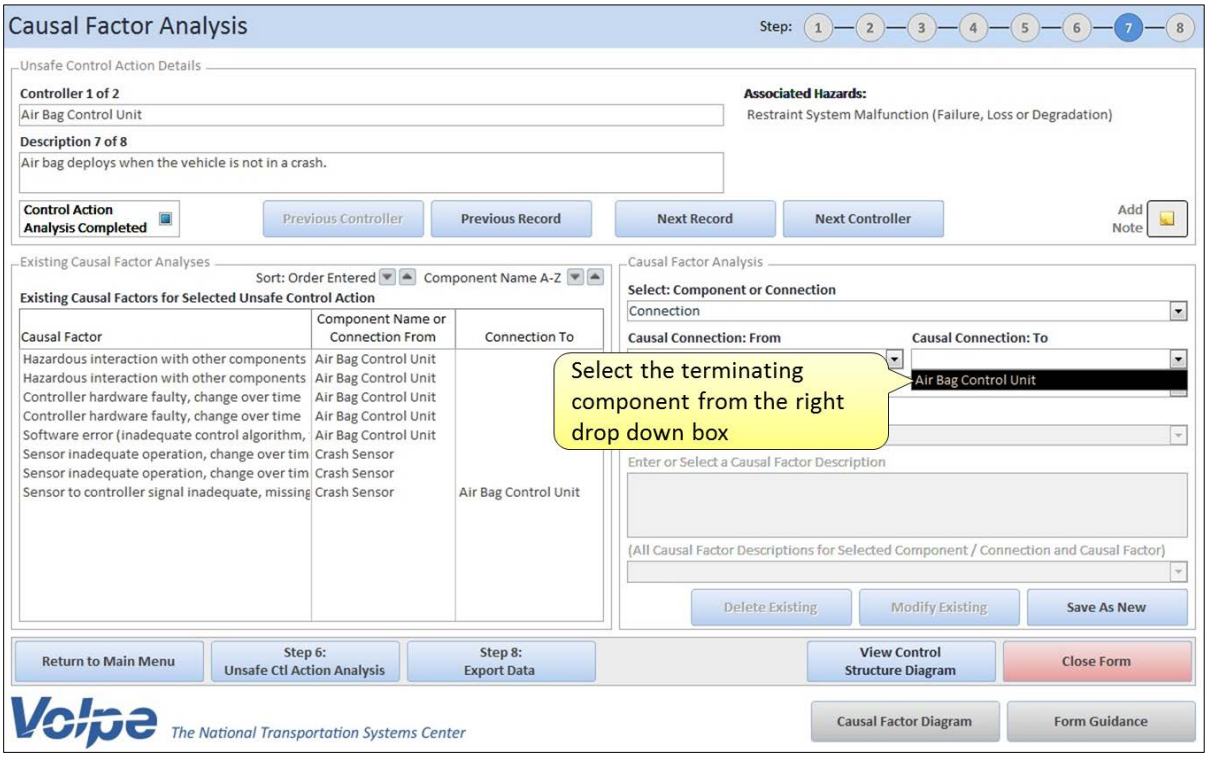


Figure 45: Selecting a Terminating Component for a Connection in the Causal Factor Analysis Form

4. Select the connection type from the fourth drop-down list on the right side of the form (see Figure 46).

   The available options in this drop-down list are based on the types you assigned to this connection when defining the system connections in Step 2 of SafetyHAT.

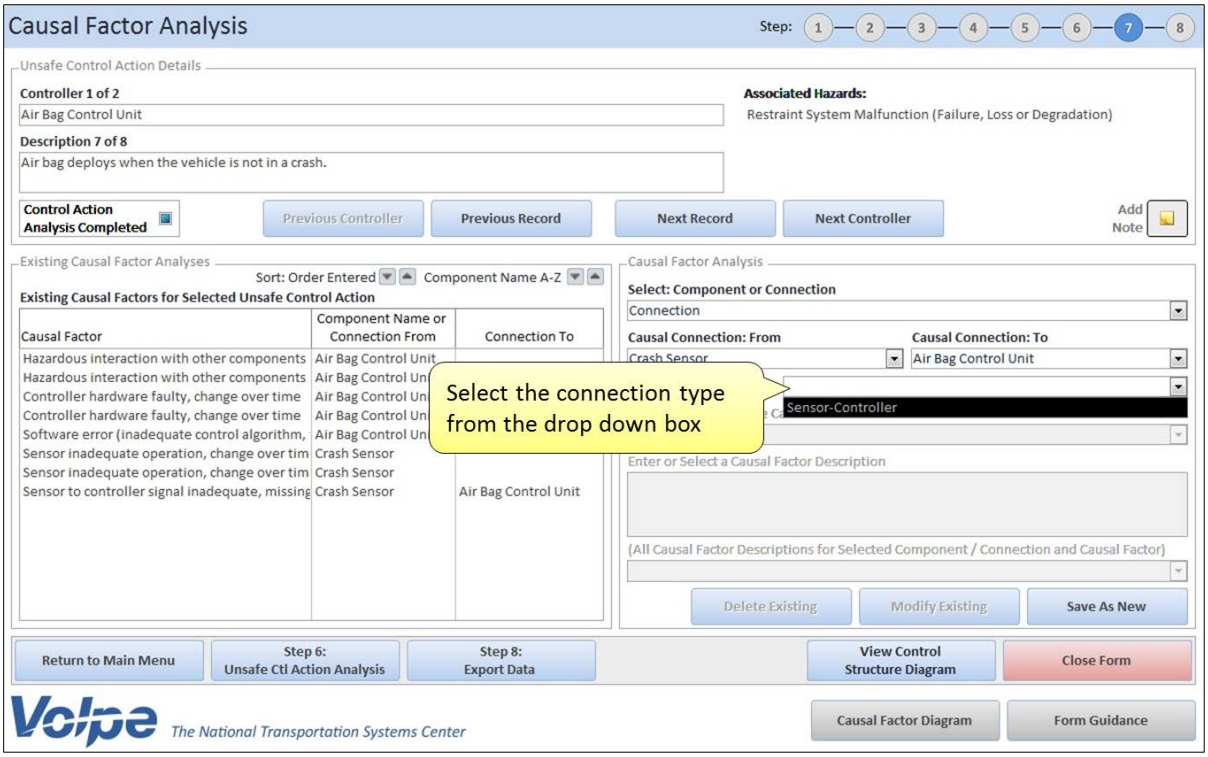


Figure 46: Selecting a Connection Type in the Causal Factor Analysis Form

5. Select a generalized causal factor guide phrase from the fourth drop-down list on the right side of the form (see Figure 42).

   The available guide phrases are based on the connection type you selected in the previous step.

6. Enter a system-specific description of the causal factor in the text field on the right side of the form (see Figure 43).

   You can also apply an existing description to your current selection using the last drop-down list on the right side of the form. The available selections in this drop-down list are based on your current component and causal factor guide phrase selection.

7. Click the *Save As New* button.

To modify an existing causal factor description:

1. Select the causal factor you want to edit from the box on the left side of the form.

2. Make the necessary changes in the fields on the right side of the form.

3. Click the *Modify Existing* button.

4. Click *Yes* to confirm your change(s). The dialogue box shown in Figure 47 will appear.

    - Clicking *Yes* will apply your change to causal factor descriptions for all analyses where the causal factor description appears. Use this feature if you want to make your edit universal.

    - Clicking *No* will only apply your change to the causal factor description for the current analysis. Use this feature if you only want to edit a single entry.

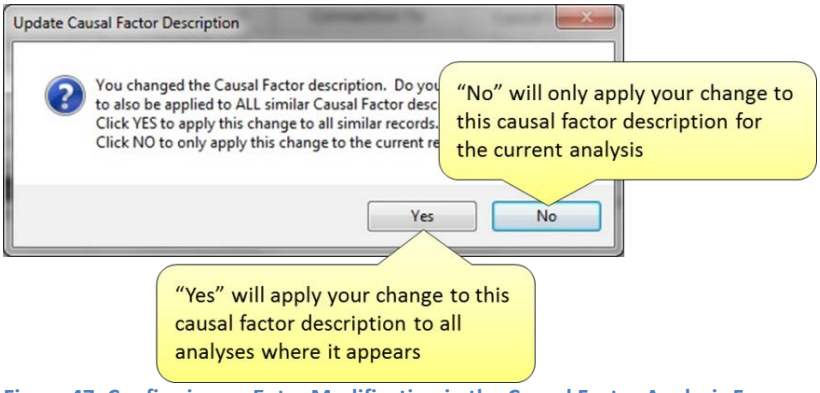


Figure 47: Confirming an Entry Modification in the Causal Factor Analysis Form

To delete an existing causal factor description:

1. Select the causal factor description you want to delete from the box on the left side of the form.

2. Click the *Delete Existing* button.

3. Click *Yes* to confirm deletion.

You can attach a note to the current UCA description by clicking the *Add Note* button (see Figure 48). The layout of the note entry screen is identical to the note screen shown in Figure 36 and entering notes follows the procedure outlined in Section 3.5.6.

Once you have completed adding causal factors for an unsafe control action description, check the box on the upper part of the form to record the completion status (see Figure 48).

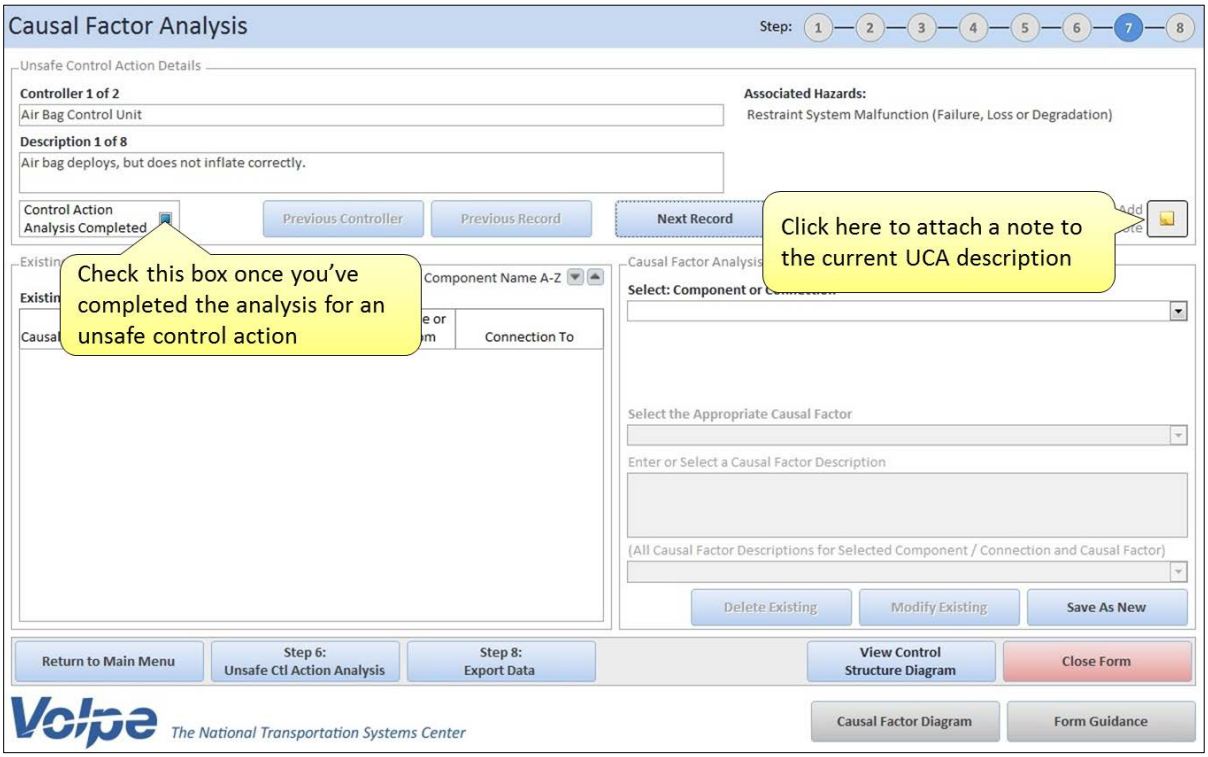


Figure 48: Marking an Analysis Complete and Adding Notes in the Causal Factor Analysis Form

3.6 Exporting Your Analysis

3.6.1 Starting the Export in SafetyHAT

Step 8 of SafetyHAT exports the completed analysis to MS Excel. You can begin the export either by selecting Step 8 from the main menu (see Figure 49) or by clicking the *Step 8: Export Data* button in the navigation bar on the Causal Factor Analysis Form (see Figure 50).

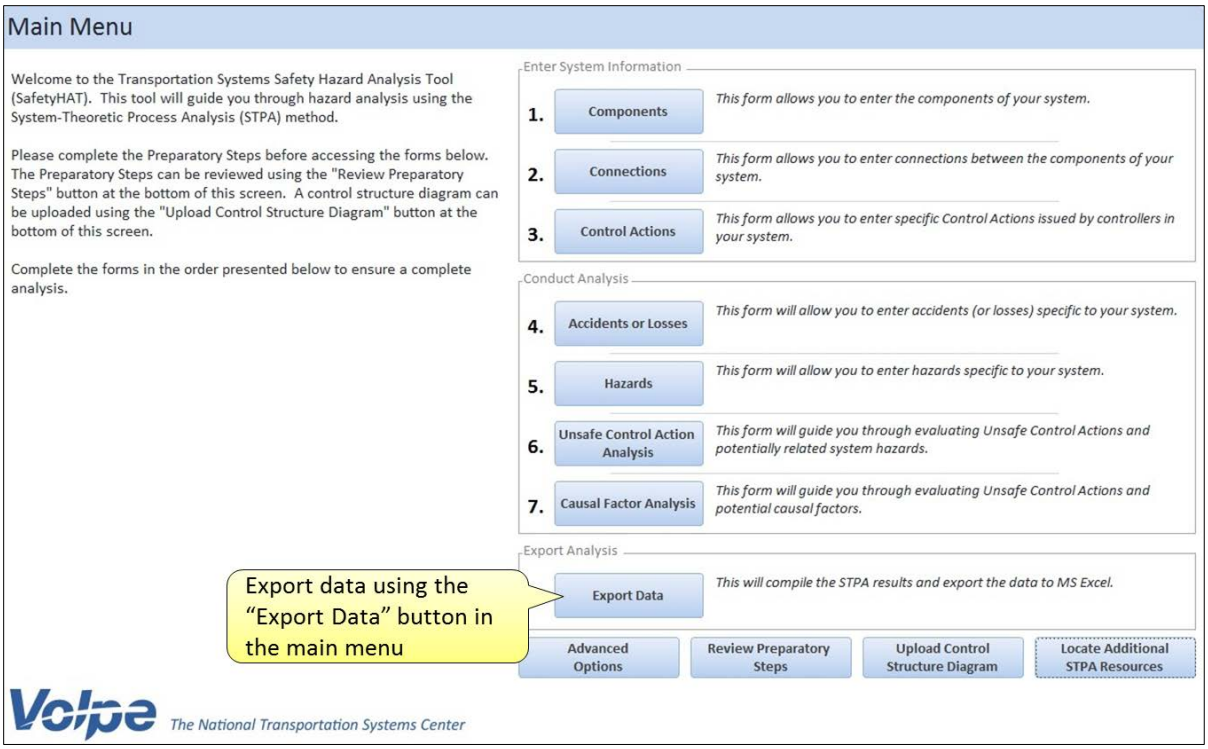


Figure 49: Exporting Your Analysis from the Main Menu

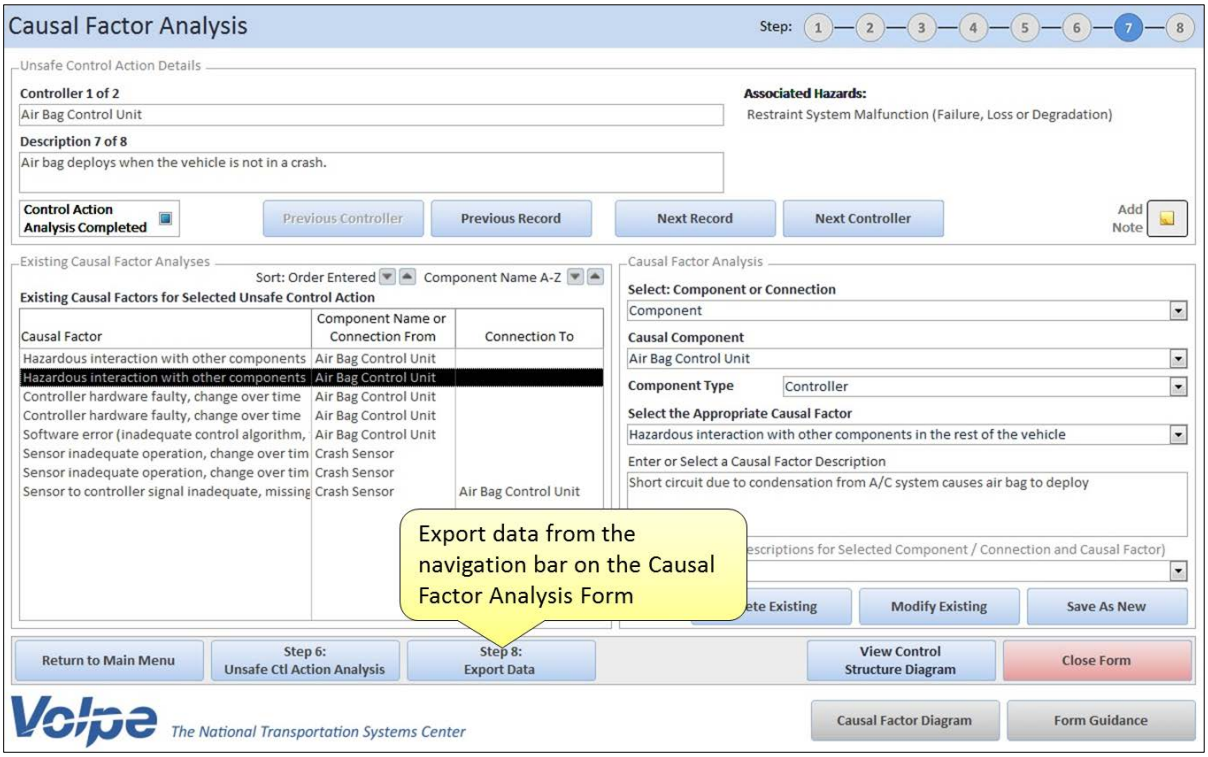


Figure 50: Exporting Your Analysis from the Navigation Bar

Once you begin the export process, SafetyHAT will integrate your analysis by combining your entries from Steps 4 through 7 into a many-to-many relationship. This many-to-many relationship maps out all possible pathways between causal factors and system-level accidents based on the information you provided in your analysis.

Depending on the complexity of the system you analyzed (*e.g.*, the number of causal factors, unsafe control actions, hazards, etc.), this process may take several minutes. Note that the screen may flicker briefly as SafetyHAT executes the integration.

After SafetyHAT completes integration of your analysis, a *Save As* dialogue box will appear. Specify the directory and file name for the spreadsheet that will contain your analysis (see Figure 51).

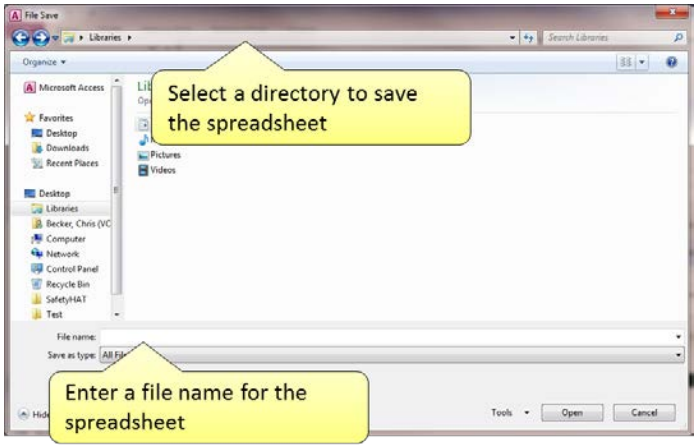


Figure 51: Export *Save As* Dialogue Box

Click the *Save* button to save the output of your analysis as a MS Excel spreadsheet.

3.6.2 Opening the Exported File

After SafetyHAT finishes saving your file, the dialogue box shown in Figure 52 will appear. This completes your analysis using SafetyHAT. You can open the file from the directly location shown in the dialogue box.

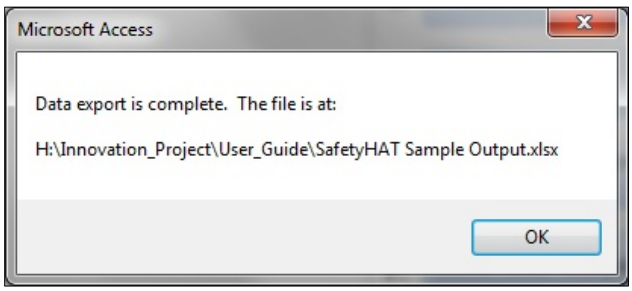


Figure 52: Export Complete Message

The exported file is an unformatted MS Excel spreadsheet. The spreadsheet contains seven tabs (see Figure 53). The first tab contains the fully integrated mapping between system-level accidents and causal factors. The remaining six tabs contain the data you entered into each of the forms in SafetyHAT. Note that the Accident and Hazard Input Forms are combined into a single tab; the seven input forms correspond to six tabs.

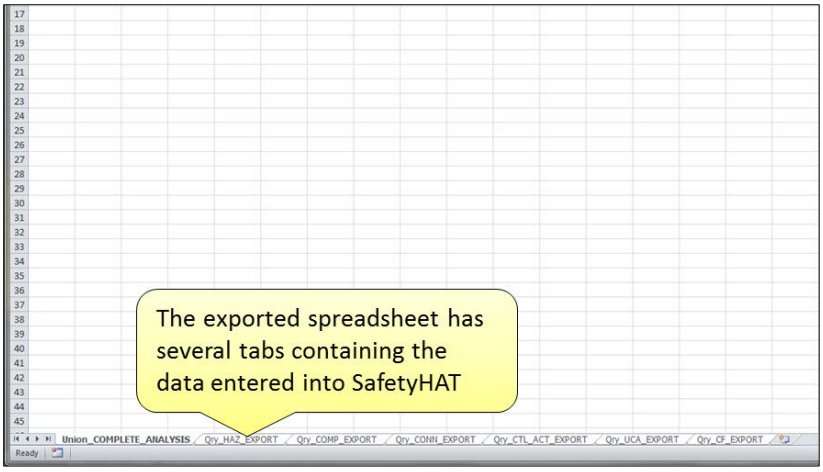


Figure 53: SafetyHAT MS Excel Output File

When you initially open the Excel output file, all tabs will be selected. Manually select a single tab before applying any formatting, filters, etc. to the spreadsheet.

4. Advanced Options

SafetyHAT is equipped with several advanced options that enable you to customize the STPA framework that underlies SafetyHAT. This section of the user guide walks you through each of the advanced options.

> *The advanced option feature is intended for experienced STPA practitioners. Improperly modifying the default information can result in an incomplete or incorrect analysis.*

To access the advanced options features, click the *Advanced Options* button on the main menu screen (Figure 54).

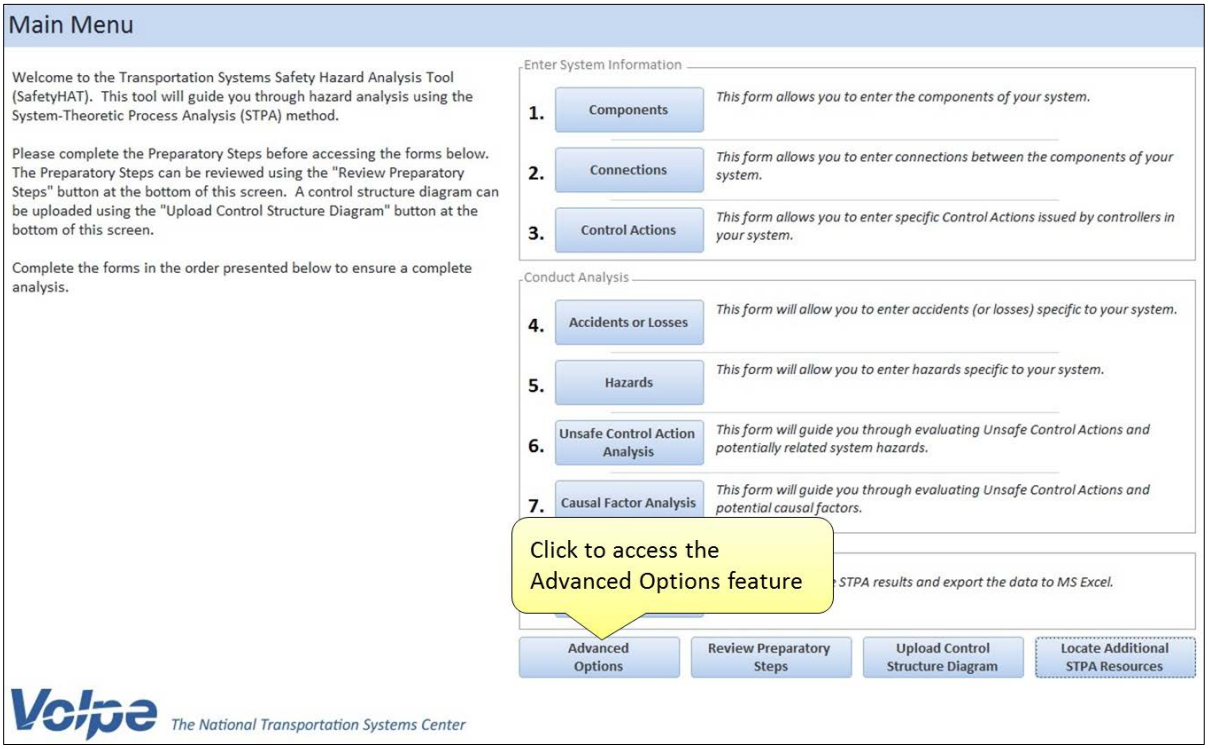


Figure 54: Accessing the Advanced Options

Clicking the *Advanced Options* button in the main menu screen will open a secondary menu with the three advanced options (see Figure 55).

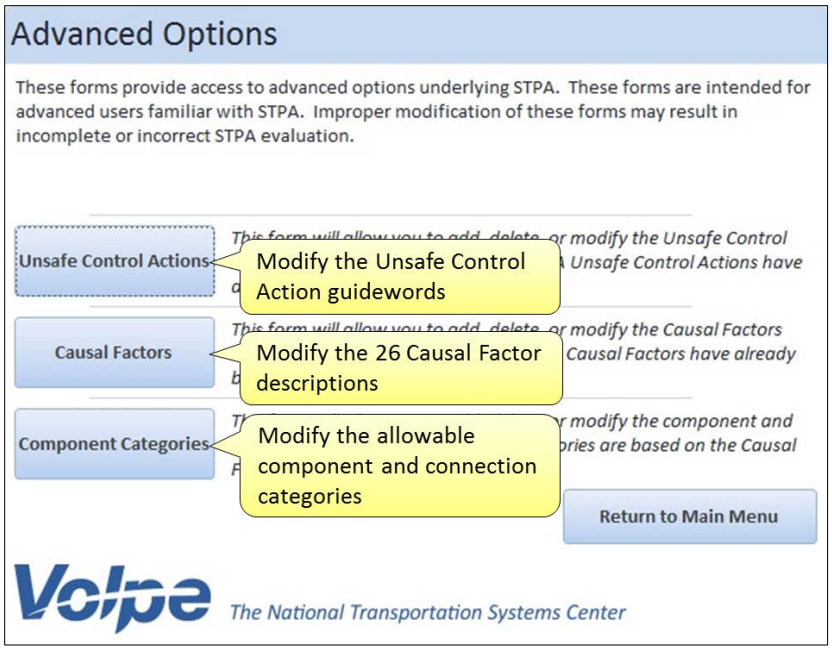


Figure 55: Advanced Options Menu Screen

4.1 Editing Unsafe Control Action Guide Phrases

SafetyHAT uses generalized unsafe control action (UCA) guide phrases to assist the user in completing the unsafe control action analysis. SafetyHAT has six pre-loaded guide phrases:

- Provided when control action is not needed and unsafe
- Provided, but the intensity is incorrect (too much or too little)
- Provided, but executed incorrectly [1]
- Provided, but duration is too long or too short
- Provided, but the starting time is too soon or too late
- Not provided when needed to maintain safety

The six UCA guide phrases included in SafetyHAT include the four guide phrases typically applied in STPA, plus two additional guide phrases. The additional guide phrases were added based on our experience in applying STPA to transportation systems.

Clicking on the *Unsafe Control Actions* button in the advanced options menu screen will open the Unsafe Control Action Input Form (see Figure 56). You can add, modify, or delete the UCA guide phrases through the Unsafe Control Action Input Form.

[1] New unsafe control action guide phrase added in SafetyHAT.

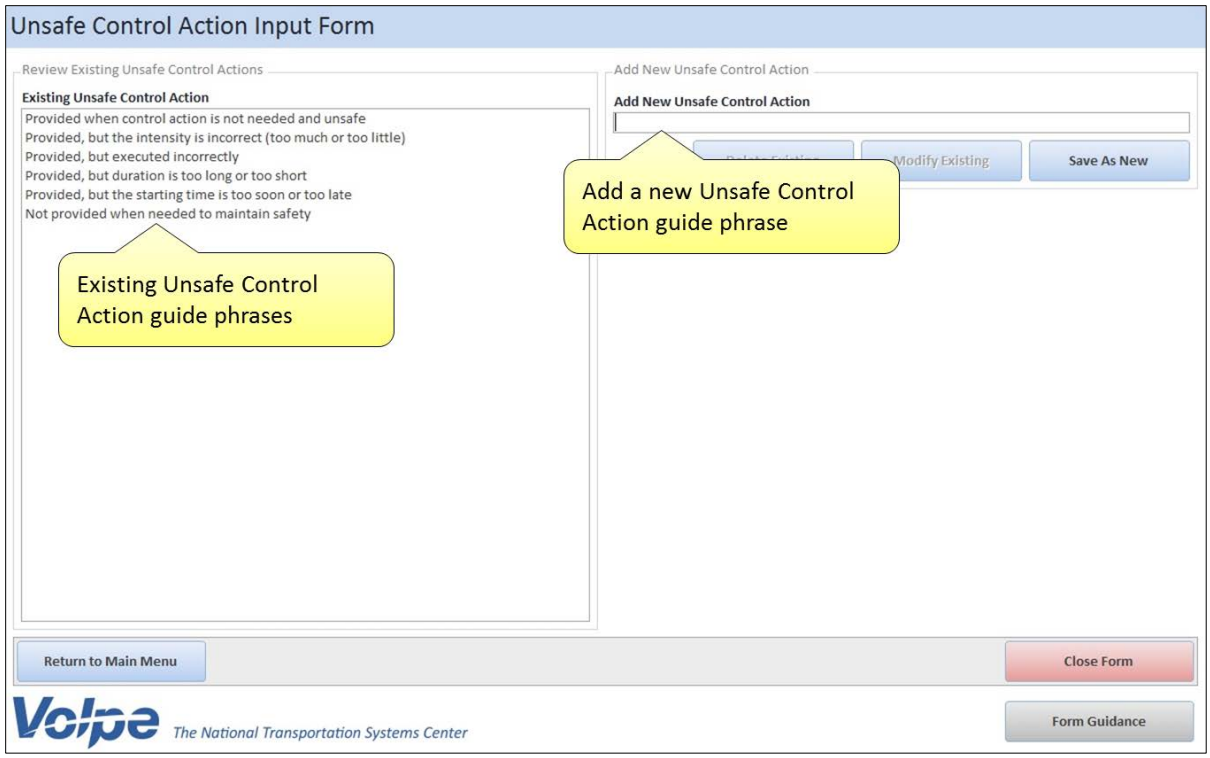


Figure 56: Unsafe Control Action Guide Phrase Input Form

To enter a new UCA guide phrase:

1. Enter the UCA guide phrase in the first entry field on the right side of the form.
2. Click the *Save As New* button.

To modify an existing UCA guide phrase:

1. Select the UCA guide phrase you want to edit from the box on the left side of the form.
2. Make the necessary changes in the fields on the right side of the form.
3. Click the *Modify Existing* button.
4. Click *Yes* to confirm your change(s).

To delete an existing UCA guide phrase:

1. Select the UCA guide phrase you want to delete from the box on the left side of the form.
2. Click the *Delete Existing* button.

3. Click *Yes* to confirm deletion.

4.2 Editing Causal Factor Guide Phrases

SafetyHAT uses generalized causal factor guide phrases to assist the user in completing the causal factor analysis. SafetyHAT has twenty-six pre-loaded causal factor guide phrases which correspond to the causal factor diagram shown in Figure 57.

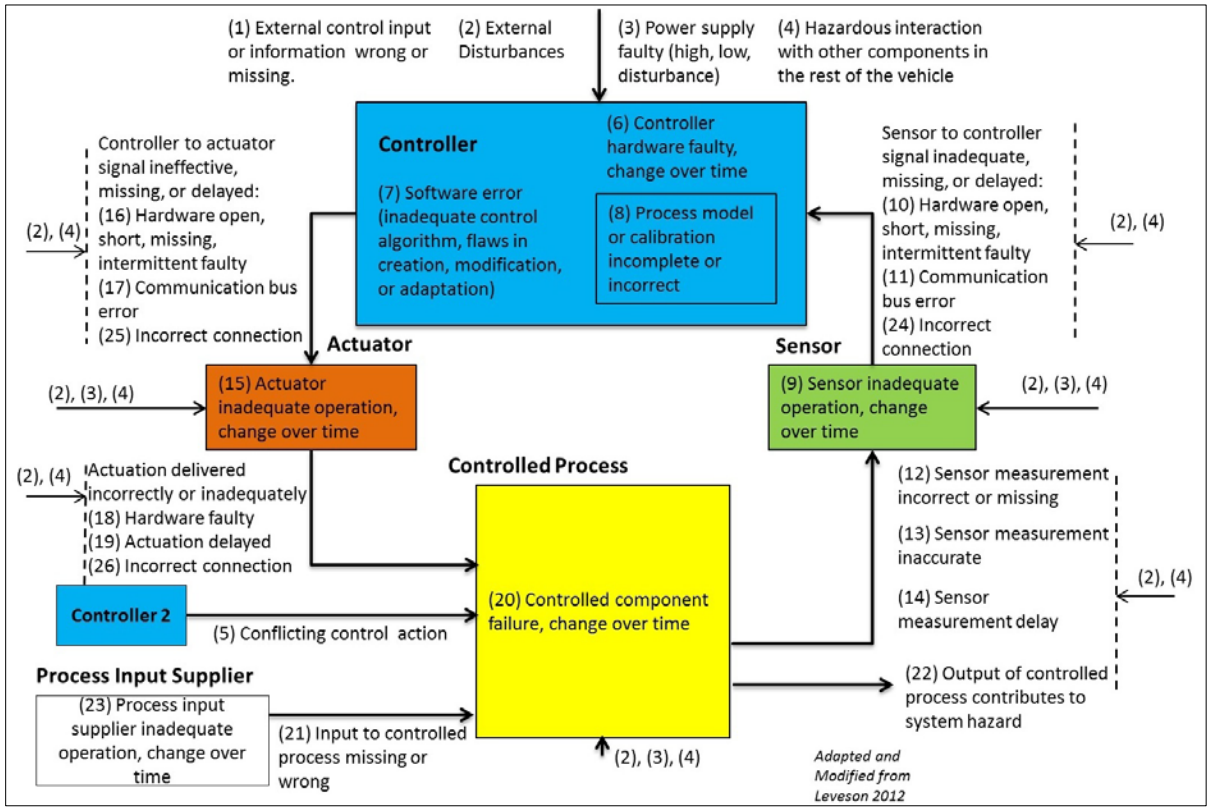


Figure 57: Causal Factor Diagram Showing the Default SafetyHAT Causal Factors

The pre-loaded guide phrases are:

1) External control input or information wrong or missing
2) External disturbances
3) Power supply faulty (high, low, disturbance) [2]
4) Hazardous interaction with other components in the rest of the vehicle
5) Conflicting control action
6) Controller hardware faulty, change over time
7) Software error (inadequate control algorithm, flaws in creation, modification, or adaptation)

[2] New causal factor guide phrase added in SafetyHAT.

8) Process model or calibration incomplete or incorrect
9) Sensor inadequate operation, change over time
10) Sensor to controller signal inadequate, missing, or delayed: Hardware open, short, missing, intermittent faulty
11) Sensor to controller signal inadequate, missing, or delayed: Communication bus error
12) Sensor measurement incorrect or missing
13) Sensor measurement inaccurate
14) Sensor measurement delay
15) Actuator inadequate operation, change over time
16) Controller to actuator signal ineffective, missing, or delayed: Hardware open, short, missing, intermittent faulty
17) Controller to actuator signal ineffective, missing, or delayed: Communication bus error
18) Actuation delivered incorrectly or inadequately: Hardware faulty
19) Actuation delivered incorrectly or inadequately: Actuation delayed
20) Controlled component failure, change over time
21) Input to controlled process missing or wrong
22) Output of controlled process contributes to system hazard
23) Process input supplier inadequate operation, change over time
24) Sensor to controller signal inadequate, missing, or delayed: Incorrect connection
25) Controller to actuator signal ineffective, missing, or delayed: Incorrect connection
26) Actuation delivered incorrectly or inadequately: Incorrect connection

The 26 causal factor guide phrases included in SafetyHAT include the 16 guide phrases typically applied in STPA, plus ten additional guide phrases. The original STPA guide phrases were modified and additional guide phrases were added based on the Volpe Center staff's experience in applying STPA to transportation systems.

Clicking on the *Causal Factors* button in the advanced options menu screen will open the Causal Factor Input Form (see Figure 58). You can add, modify, or delete the causal factor guide phrases through the Causal Factor Input Form.

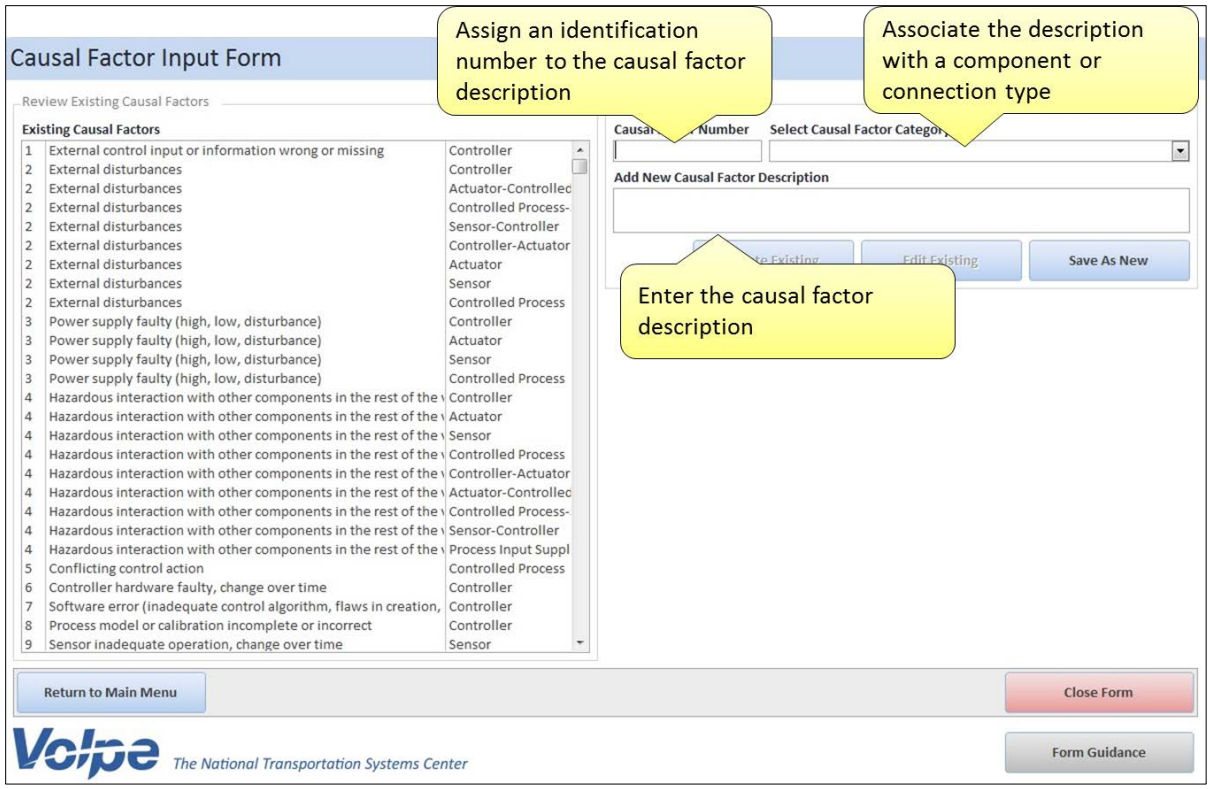


Figure 58: Causal Factor Guide Phrase Input Form

To enter a new causal factor guide phrase:

1. Enter a numerical identifier for the causal factor description in the first entry field on the right side of the form.

   Figure 57 illustrates how numerical identifiers are associated with each causal factor description. Each causal factor description should have a unique numerical identifier. If a causal factor description applies to multiple component or connection types, the same numerical identifier should be used. For example, in Figure 58 the numerical identifier "2" is associated with the "External disturbances" causal factor for all component and connection types.

2. Select a component or connection type from the drop-down list on the right side of the form to associate with the causal factor description

   A causal factor description can be associated with multiple component or connection types by creating a new entry. In Figure 57, several causal factor descriptions, such as "(2) External Disturbances", are associated with multiple components and connections.

3. Enter a description for the causal factor in the last entry field on the right side of the form.

4. Click the *Save As New* button.

To modify an existing causal factor guide phrase:

1. Select the causal factor guide phrase you want to edit from the box on the left side of the form.
2. Make the necessary changes in the fields on the right side of the form.
3. Click the *Modify Existing* button.
4. Click *Yes* to confirm your change(s).

To delete an existing causal factor guide phrase:

1. Select the causal factor guide phrase you want to delete from the box on the left side of the form.
2. Click the *Delete Existing* button.
3. Click *Yes* to confirm deletion.

Modifying or deleting a causal factor description will only affect the selected entry. Each separate occurrence of a causal factor description will need to be modified or deleted.

4.3 Editing Component / Connection Categories

In order to develop a representation of your system, SafetyHAT relies on component and connection categories. These categories are used to assign component and connection types in Step 2 of SafetyHAT. There are five pre-set component categories and five pre-set connection categories.

Components:

- Actuator
- Controlled Process
- Controller
- Process Input Supplier
- Sensor

Connections:

- Actuator-Controlled Process
- Controlled Process-Sensor
- Controller-Actuator
- Process Input Supplier-Controlled Process
- Sensor-Controller

Each of the components and connections listed above corresponds to components and connections shown in Figure 57.

The Component / Connection Type Input Form allows you to enter, modify, or delete the component and connection types used by SafetyHAT. The general layout of the Component / Connection Type Input Form is shown in Figure 59.

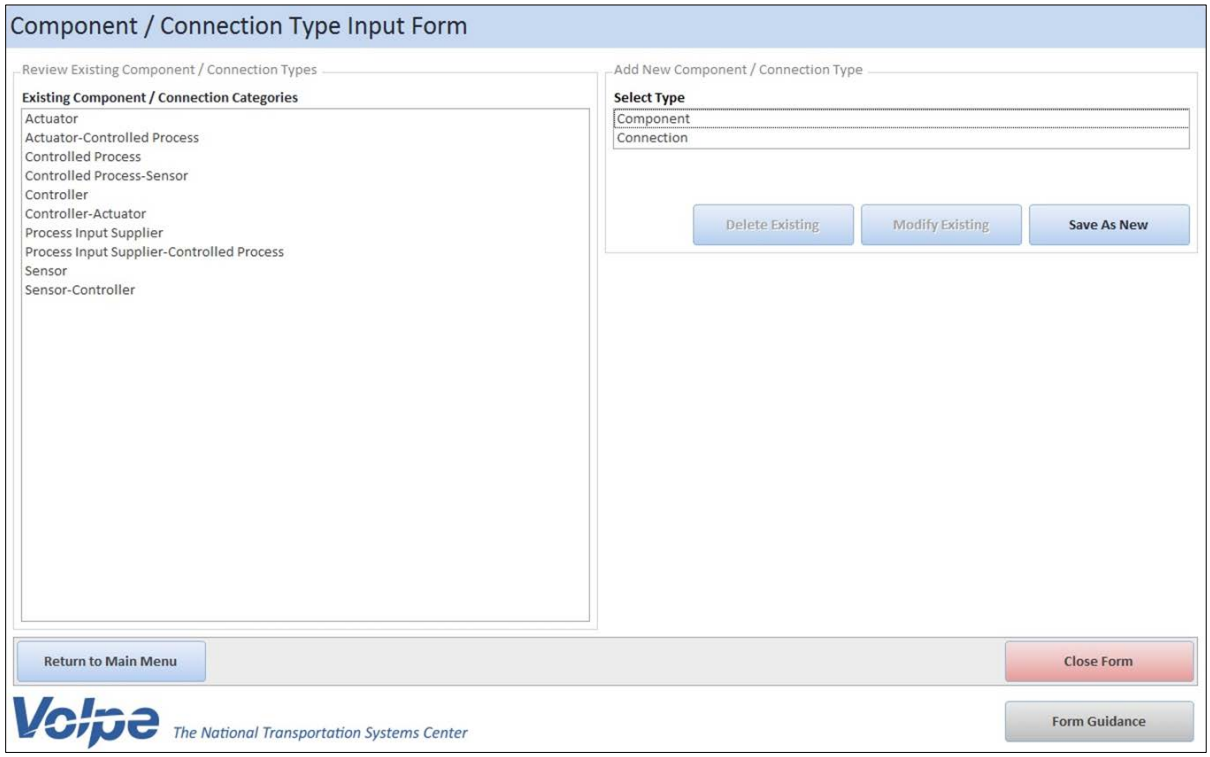


Figure 59: Component and Connection Type Input Form

To add a new component type:

1. Select “Component” from the selection box on the right side of the form.

2. Enter a name for the component type in the entry field on the right side of the form (see Figure 60).

3. Click the *Save As New* button.

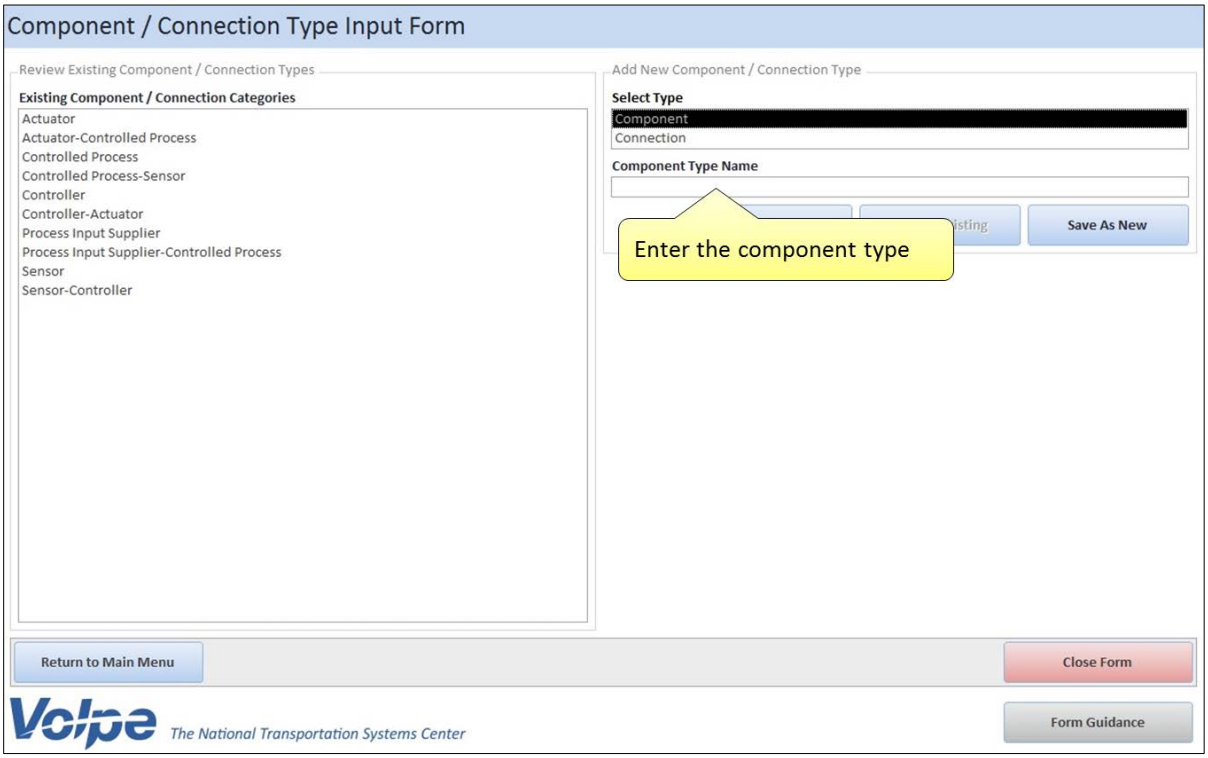


Figure 60: Entering a New Component Type in the Component and Connection Type Input Form

To add a new connection type:

1. Select "Connection" from the selection box on the right side of the form.

2. Select an originating component type from the first drop-down list on the right side of the form (see Figure 61).

3. Select a terminating component type from the second drop-down list on the right side of the form.

4. Click the *Save As New* button.

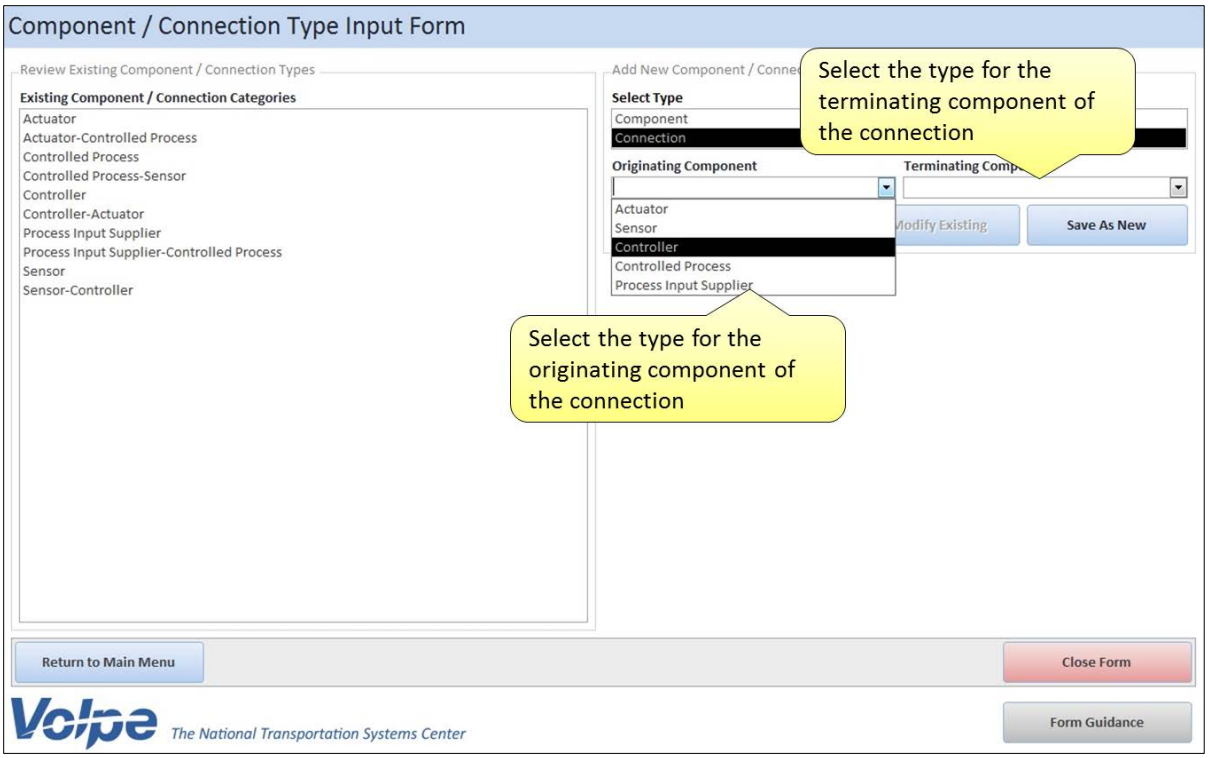


Figure 61: Entering a New Connection Type in the Component / Connection Type Input Form

Before a connection can be established, both the originating and terminating component types must be added using the "add a new component type" *procedure outlined above.*

To modify an existing component or connection type:

1. Select the component or connection type you want to edit from the box on the left side of the form.

2. Make the necessary changes in the fields on the right side of the form.

3. Click the *Modify Existing* button.

4. Click *Yes* to confirm your change(s).

To delete an existing component or connection type:

1. Select the component or connection type you want to delete from the box on the left side of the form.

2. Click the *Delete Existing* button.

3. Click *Yes* to confirm deletion.

5. References

[1] Leveson, N. Engineering a Safer World. MIT Press. Cambridge MA. 2012.

[2] MIT Partnership for a Systems Approach to Safety (PSAS). http://psas.scripts.mit.edu/home/ [Accessed February 21, 2014].

U.S. Department of Transportation
John A. Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142-1093

(617) 494-2000
www.volpe.dot.gov

DOT-VNTSC-14-01