SafetyHAT

A Transportation Systems Safety Hazard Analysis Tool

March 26, 2014

Volpe The National Transportation Systems Center

Advancing transportation innovation for the public good

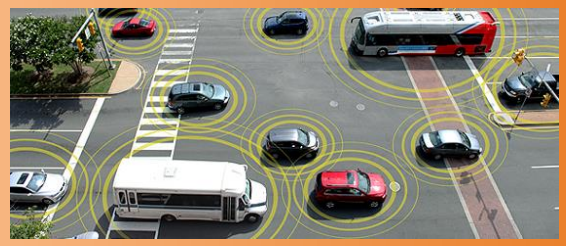
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
John A. Volpe National Transportation Systems Center

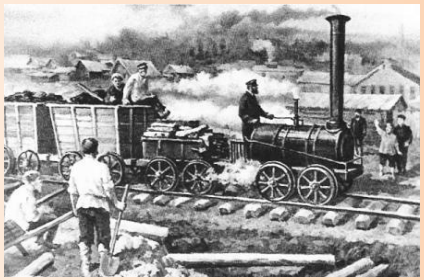
Overview

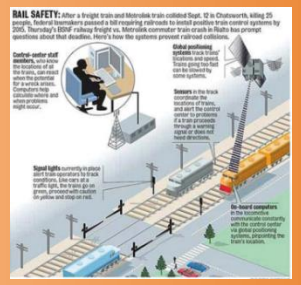
- Why SafetyHAT
- SafetyHAT Walkthrough
- Benefits from Using SafetyHAT
- How to get SafetyHAT
- Future Possibilities

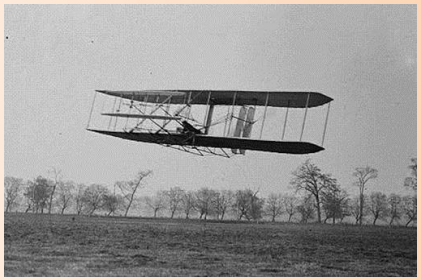
Simple Mechanical Systems

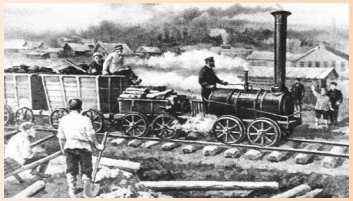
Distributed Complex Sociotechnical Systems

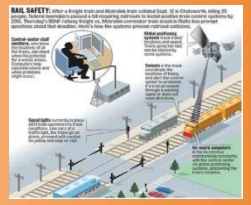


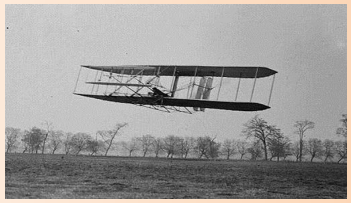


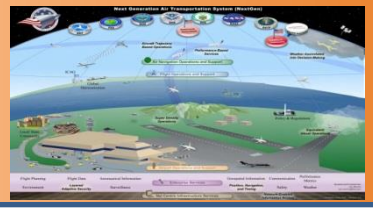












Component Failure

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

1931 Domino Model

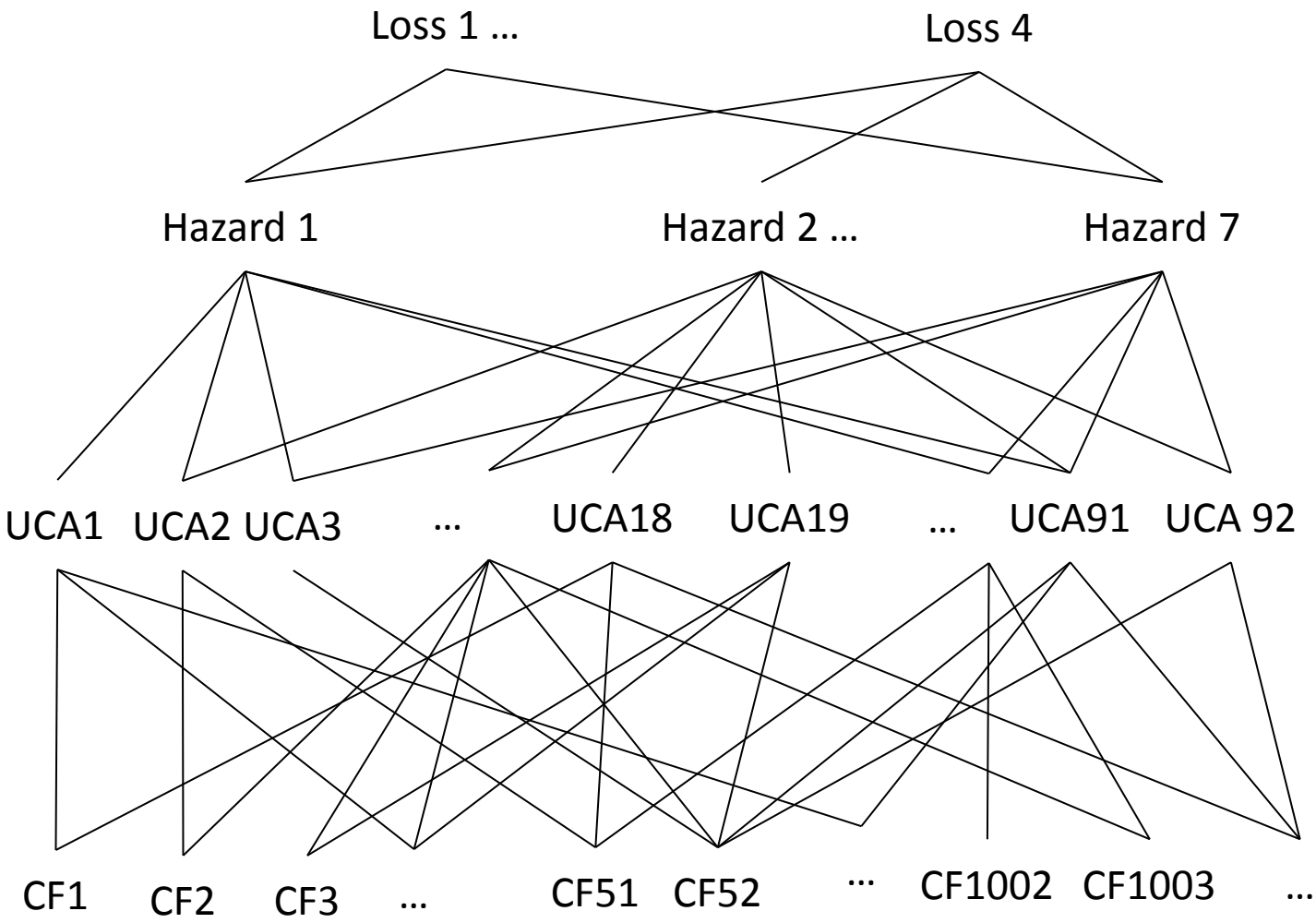
1949 Failure Modes and Effects Analysis

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

Transportation Systems
Safety HAT
Hazard Analysis Tool

- 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

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 Pre... The Preparatory Steps ca... Steps" button at the bottom of this screen. A control structure diagram ... 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

Analyze your system

Export your 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.*

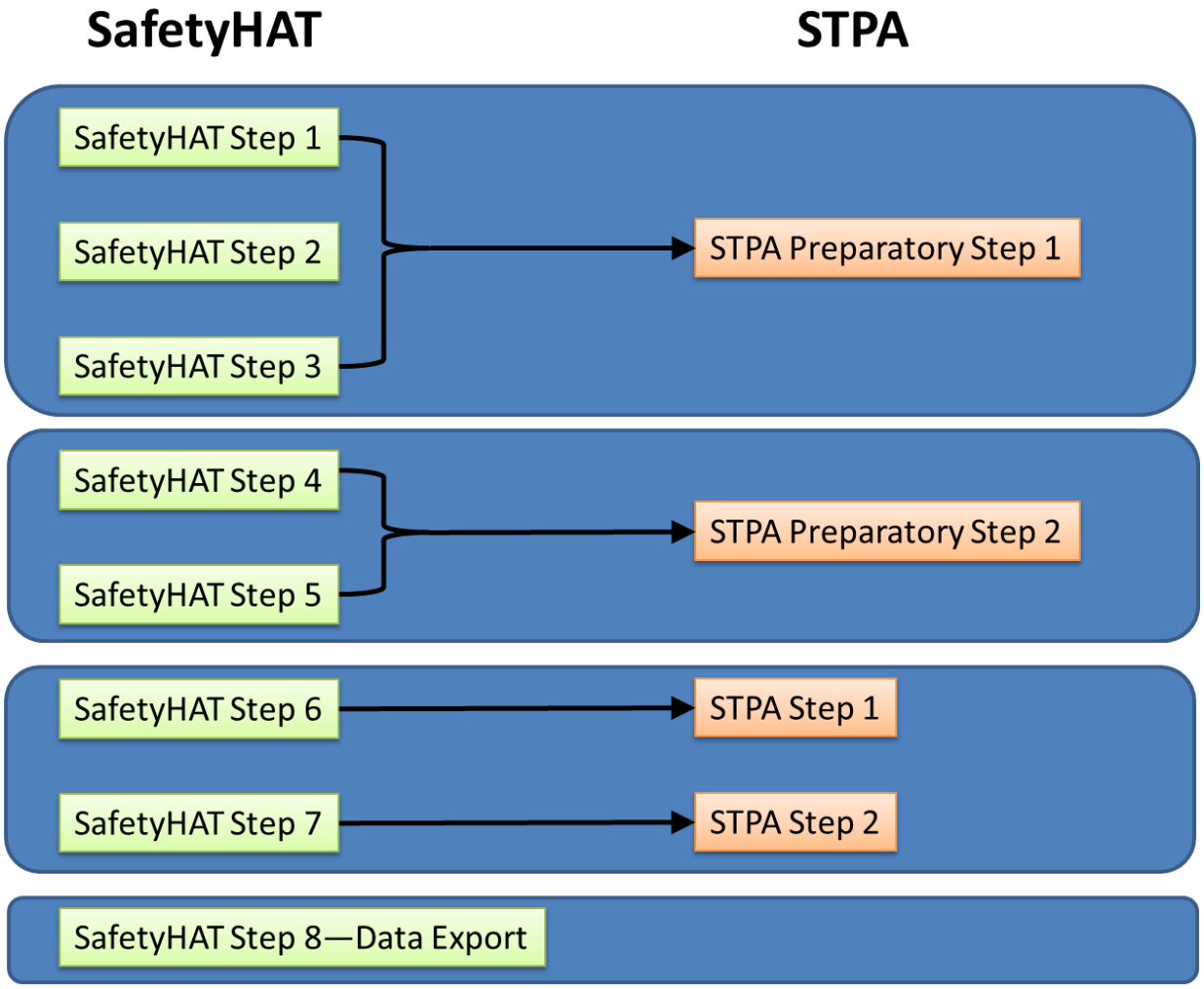
Export Analysis

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

Advanced Options | Review Preparatory Steps | Upload Control Structure Diagram | Locate Additional STPA Resources

Volpe *The National Transportation Systems Center*

Mapping SafetyHAT to STPA

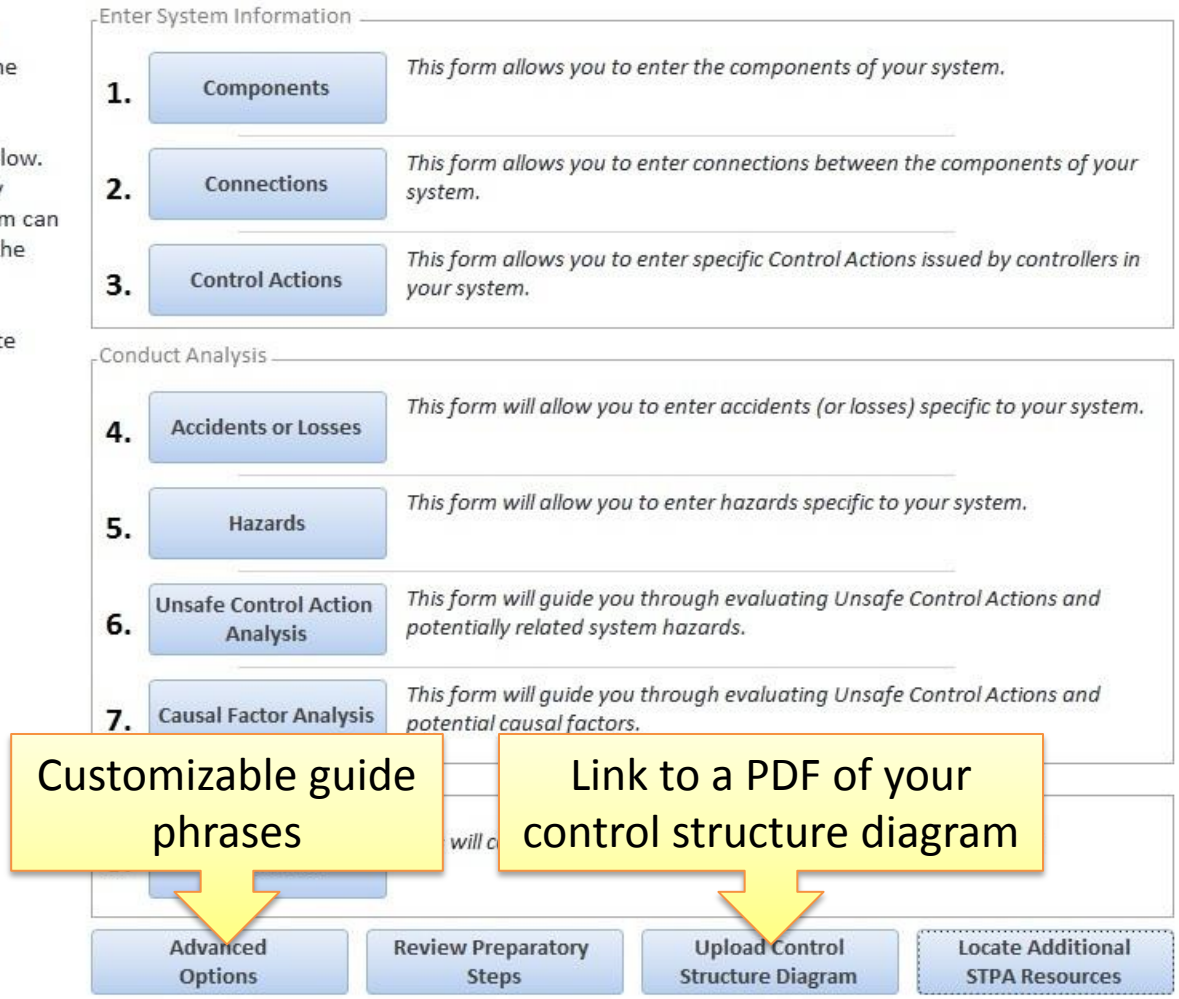


Main Menu

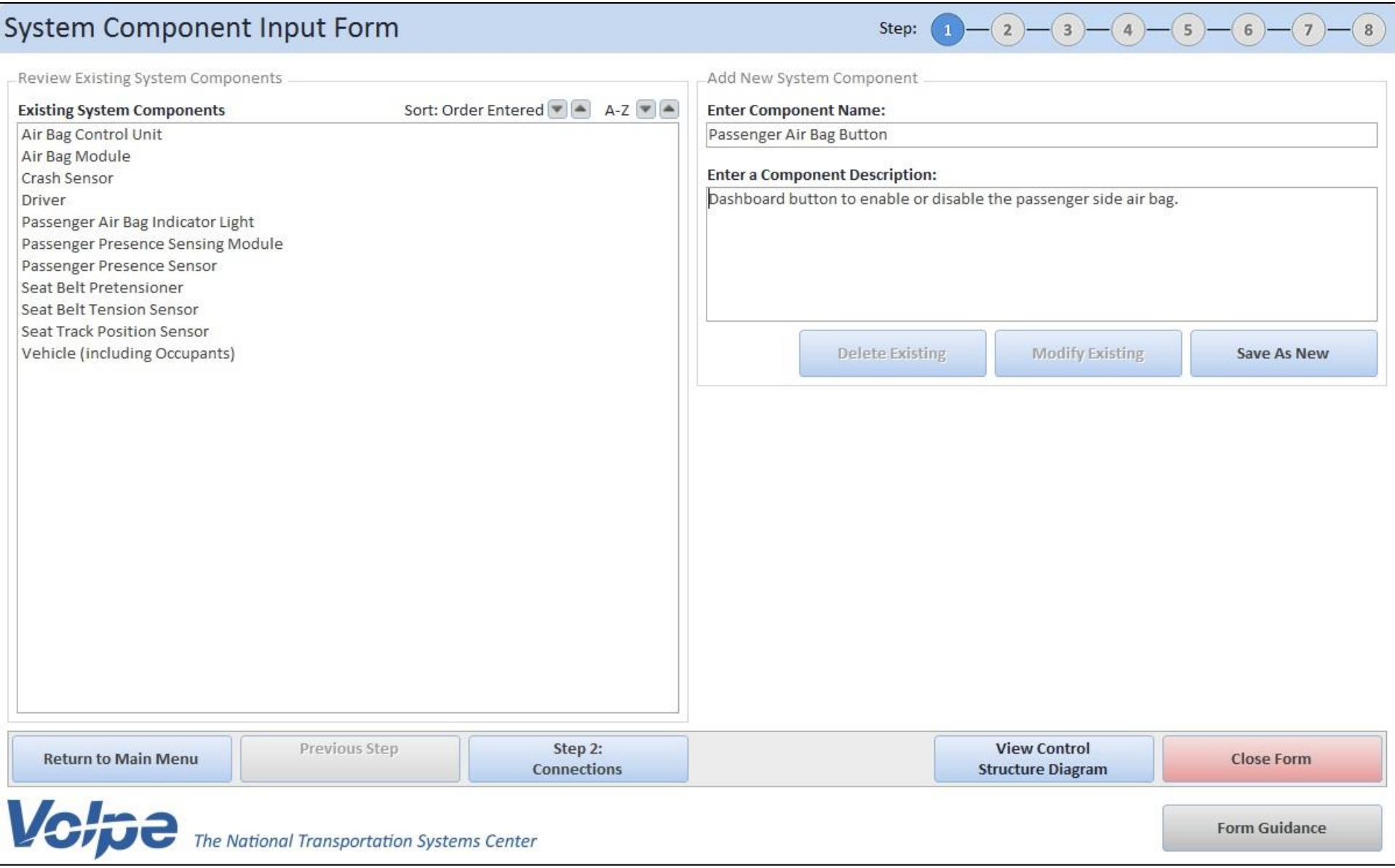
Welcome to the Transportation Systems Safety Hazard Analysis Tool (SafetyHAT). This tool will guide you through hazard analysis using the System-Theoretic Process Analysis (STPA) method.

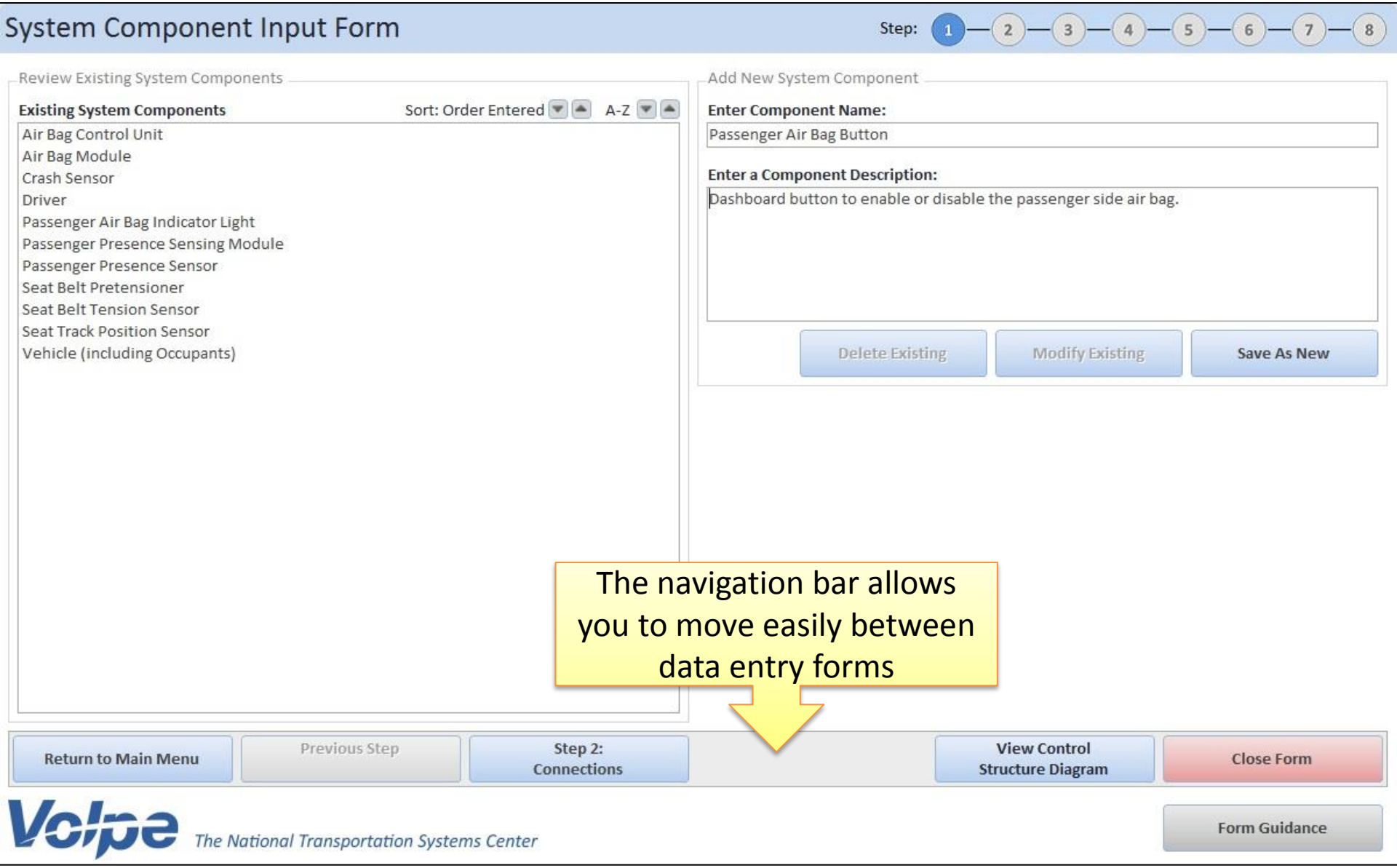
Please complete the Preparatory Steps before accessing the forms below. The Preparatory Steps can be reviewed using the "Review Preparatory Steps" button at the bottom of this screen. A control structure diagram can be uploaded using the "Upload Control Structure Diagram" button at the bottom of this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

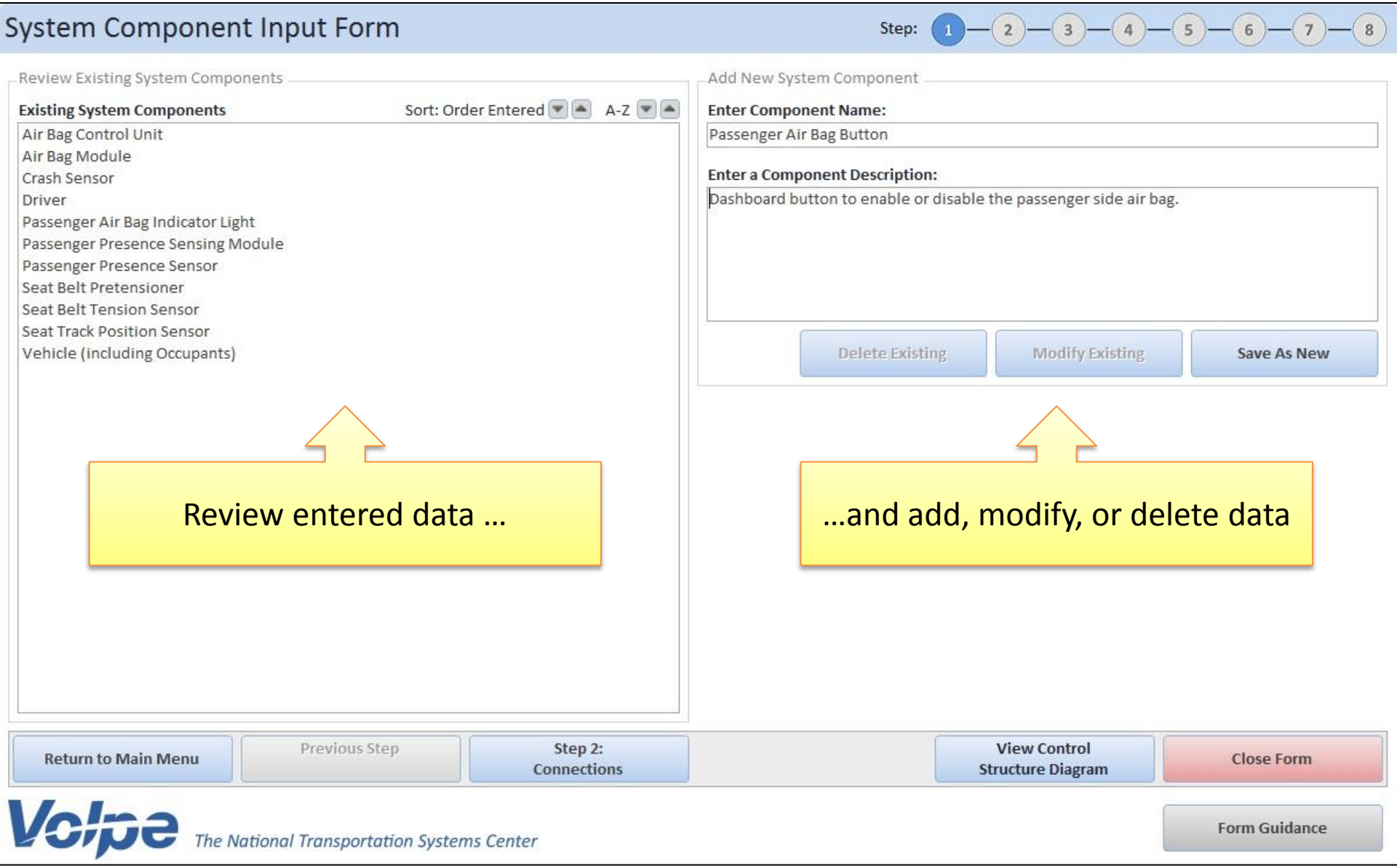
Complete the forms in the order presented below to ensure a complete analysis.

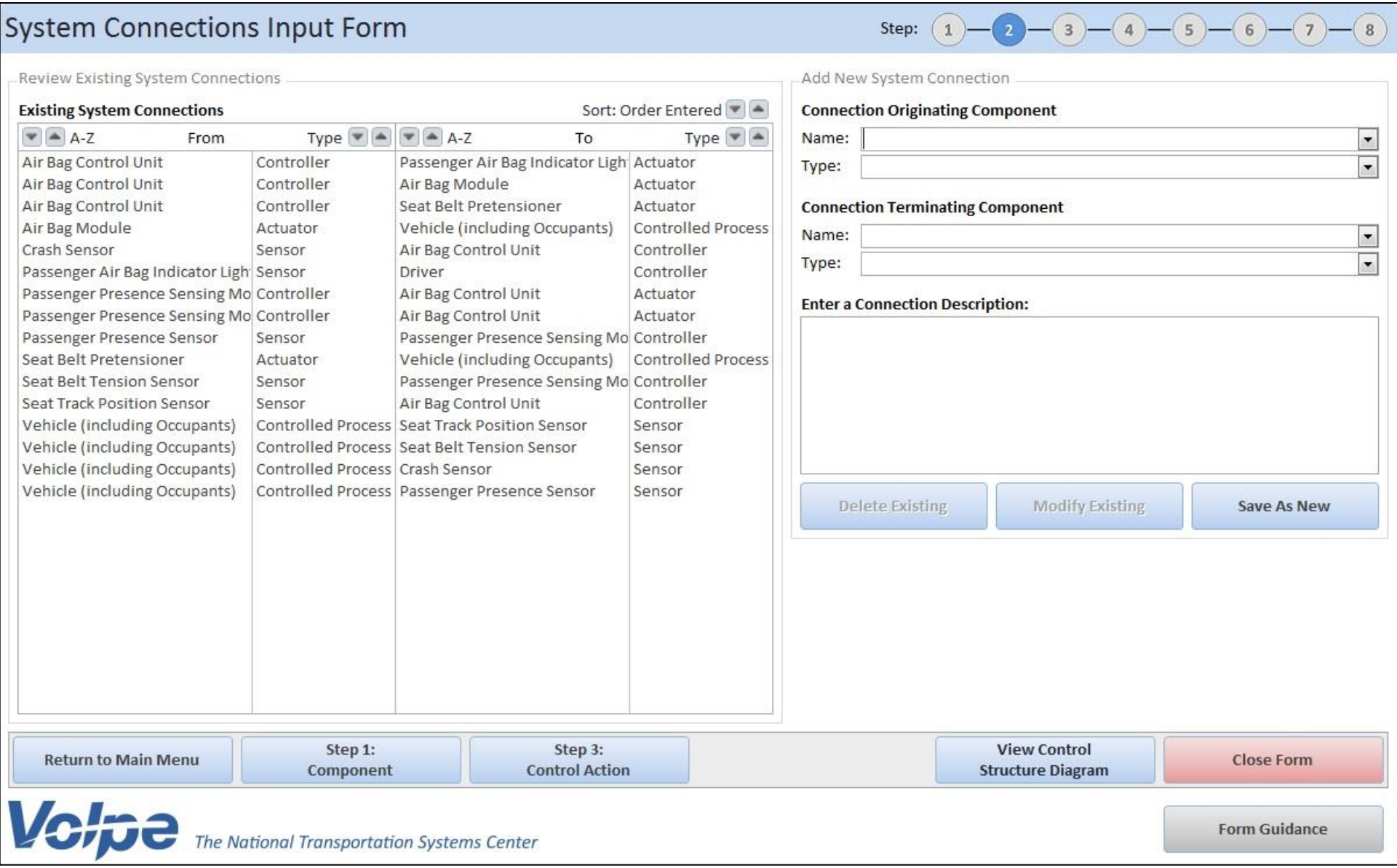


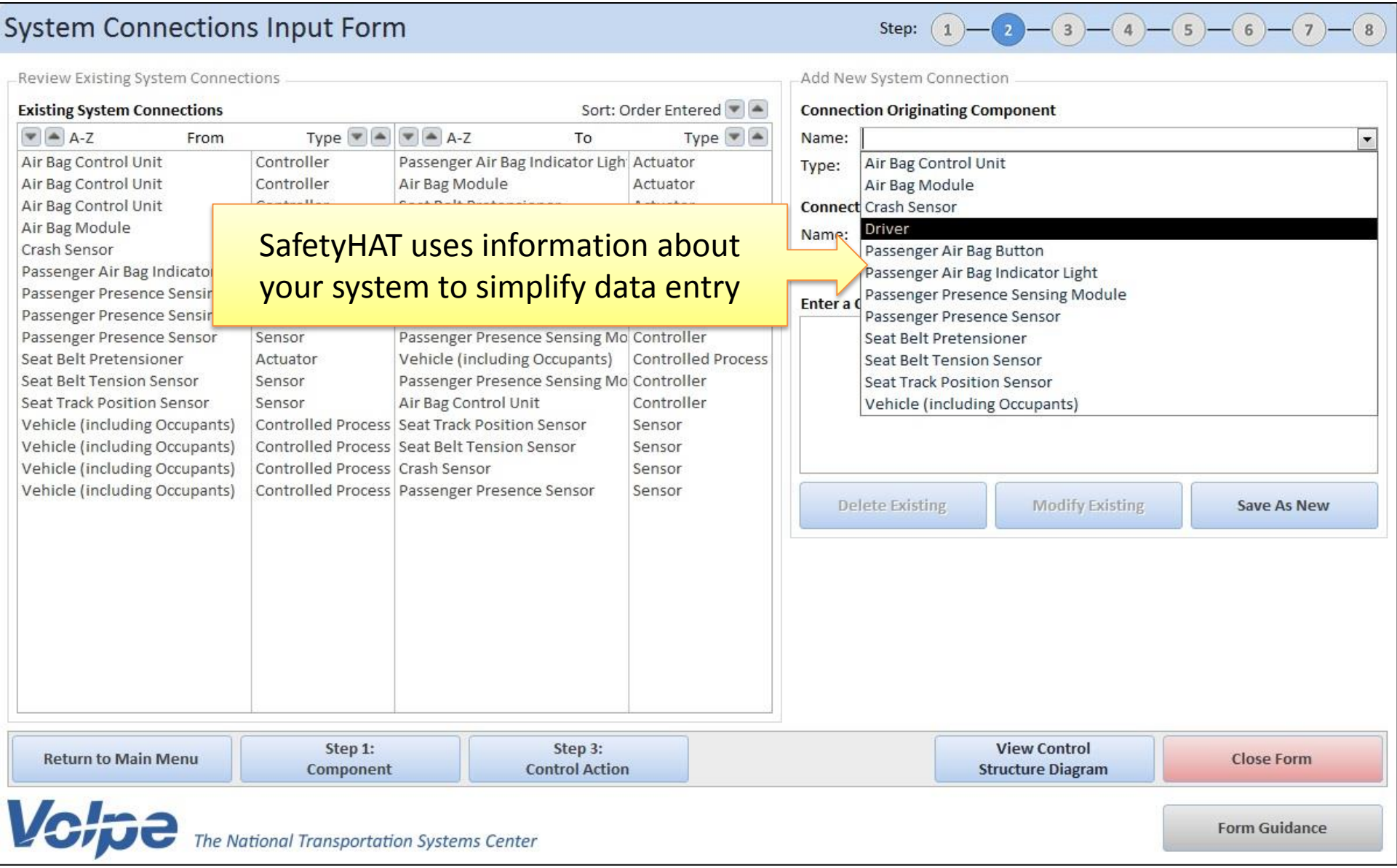
Volpe The National Transportation Systems Center

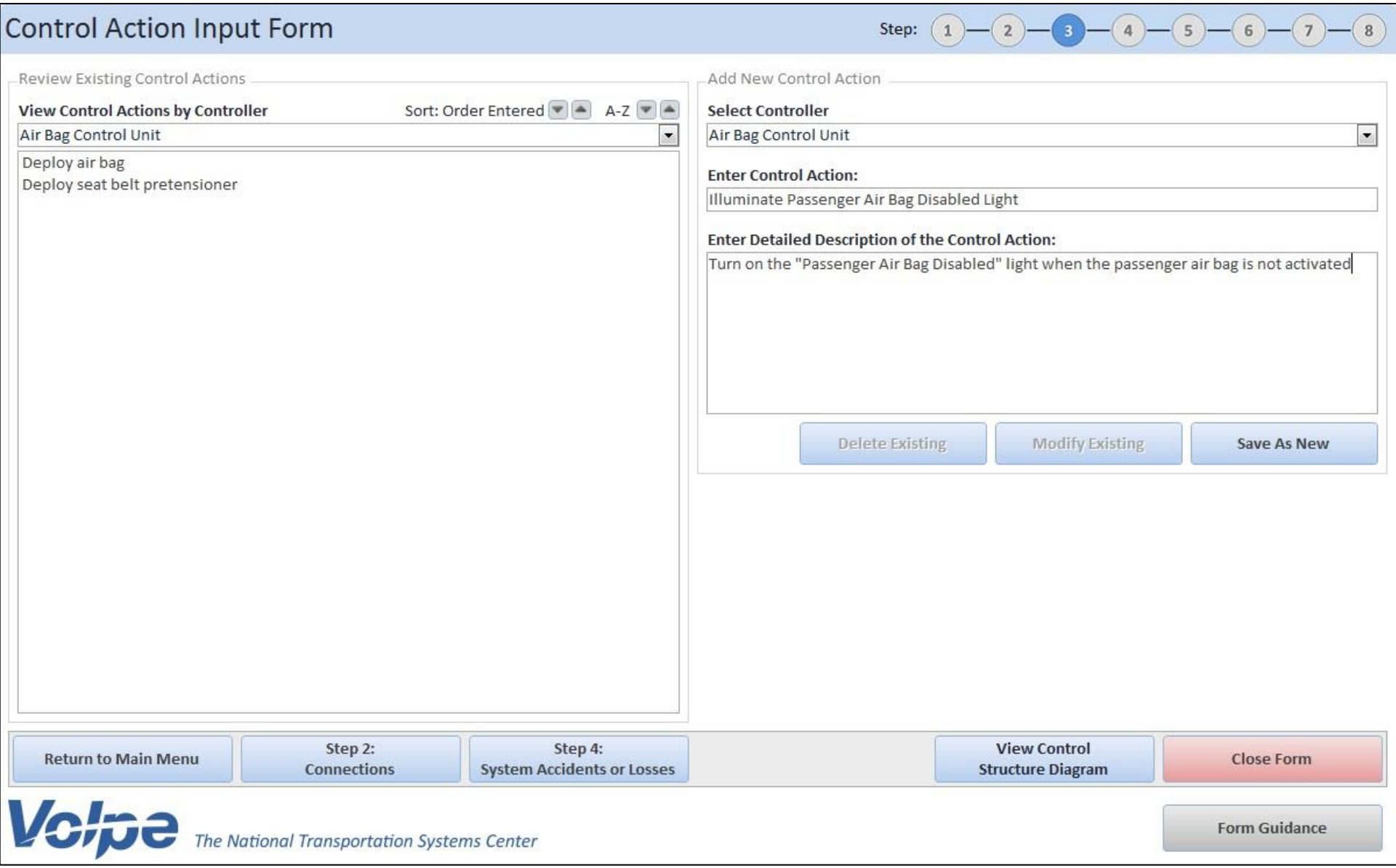

System Component Input Form
Step: 1 2 3 4 5 6 7 8
Review Existing System Components
Existing System Components
Sort: Order Entered A-Z
Air Bag Control Unit
Air Bag Module
Crash Sensor
Driver
Passenger Air Bag Indicator Light
Passenger Presence Sensing Module
Passenger Presence Sensor
Seat Belt Pretensioner
Seat Belt Tension Sensor
Seat Track Position Sensor
Vehicle (including Occupants)
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.
Delete Existing
Modify Existing
Save As New
Return to Main Menu
Previous Step
Step 2: Connections
View Control Structure Diagram
Close Form
Volpe
The National Transportation Systems Center
Form Guidance

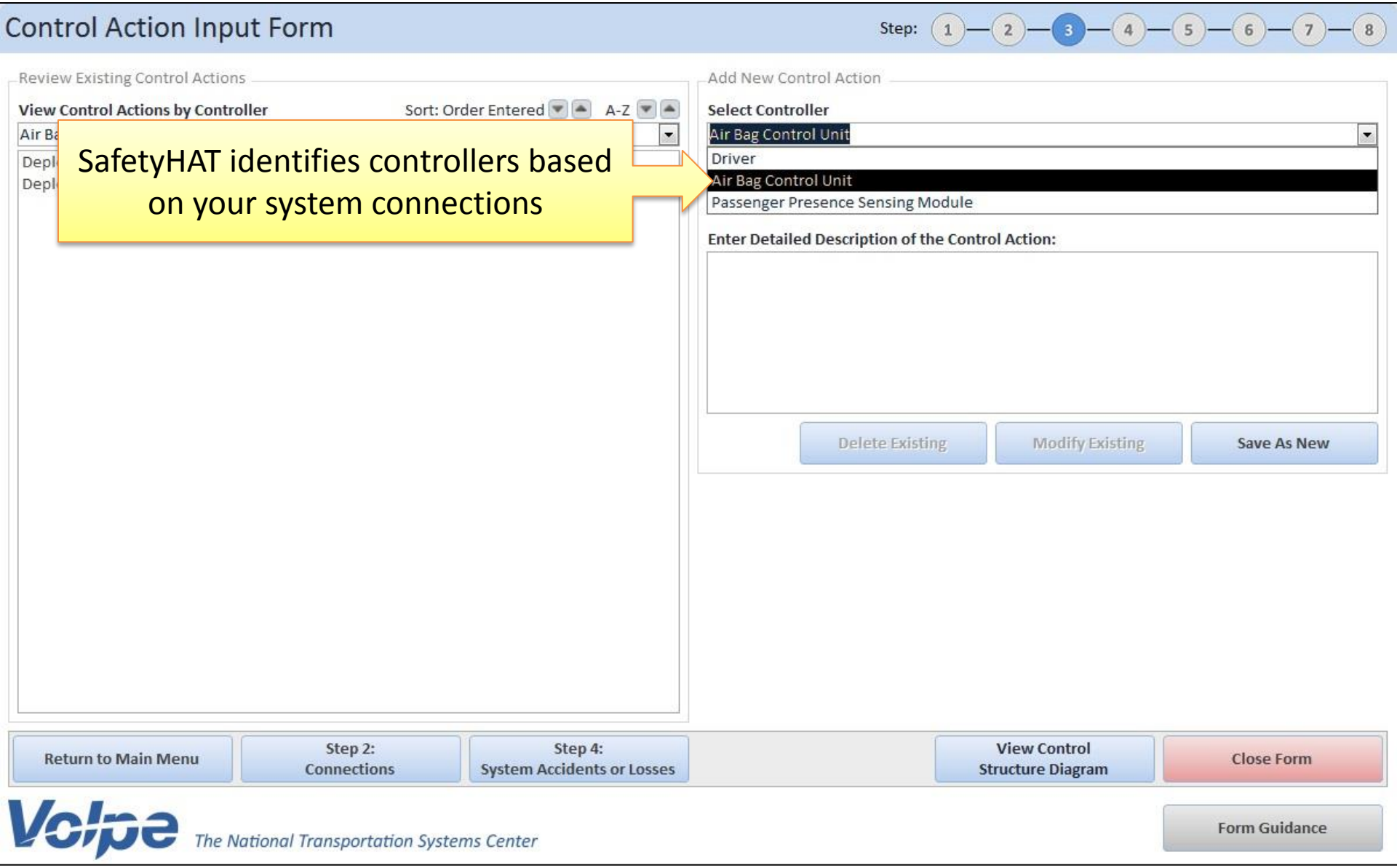

System Component Input Form
Step: 1 2 3 4 5 6 7 8
Review Existing System Components
Existing System Components
Sort: Order Entered A-Z
Air Bag Control Unit
Air Bag Module
Crash Sensor
Driver
Passenger Air Bag Indicator Light
Passenger Presence Sensing Module
Passenger Presence Sensor
Seat Belt Pretensioner
Seat Belt Tension Sensor
Seat Track Position Sensor
Vehicle (including Occupants)
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.
Delete Existing
Modify Existing
Save As New
The navigation bar allows you to move easily between data entry forms
Return to Main Menu
Previous Step
Step 2: Connections
View Control Structure Diagram
Close Form
Volpe
The National Transportation Systems Center
Form Guidance

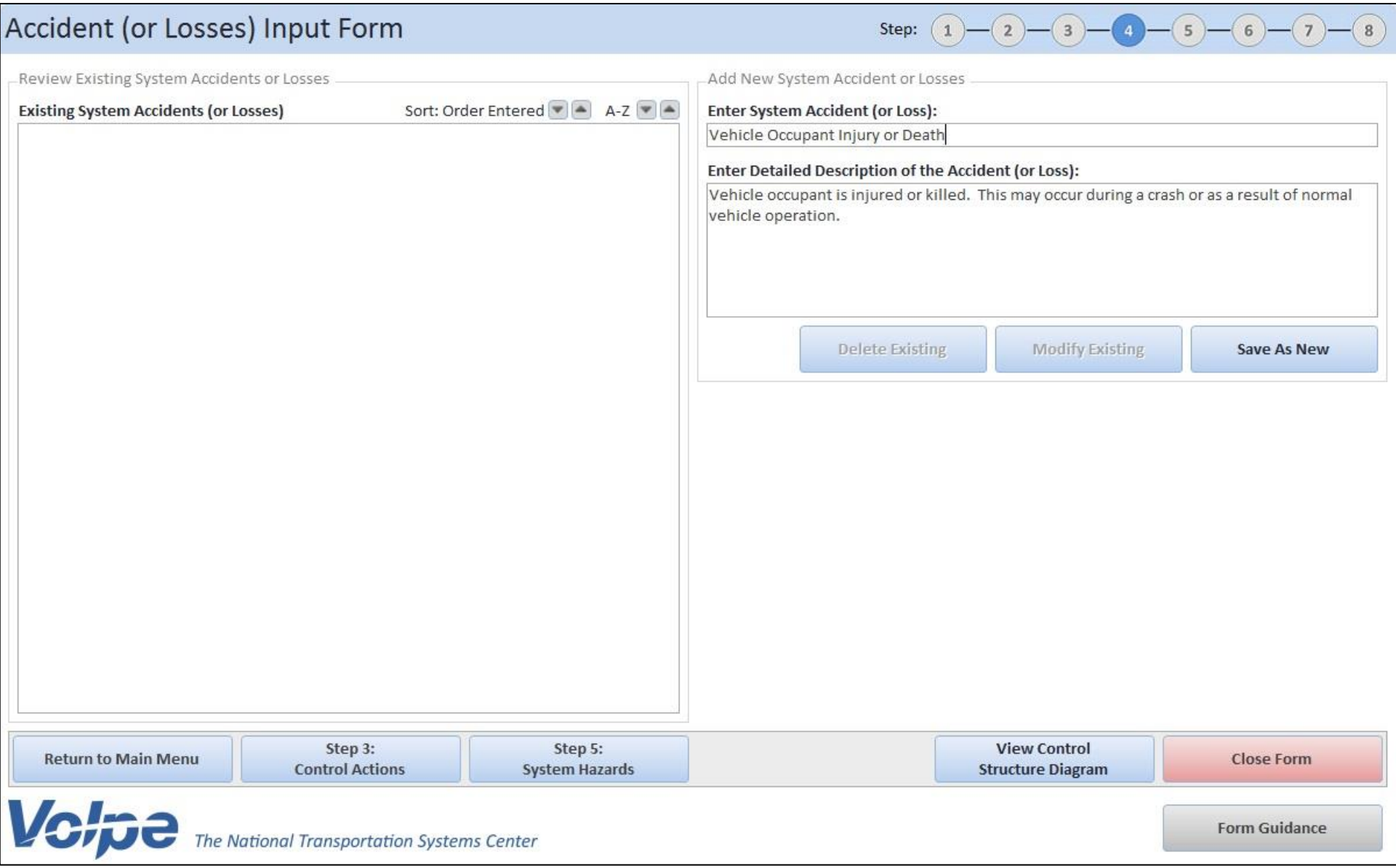

System Component Input Form
Step: 1 2 3 4 5 6 7 8
Review Existing System Components
Existing System Components
Sort: Order Entered A-Z
Air Bag Control Unit
Air Bag Module
Crash Sensor
Driver
Passenger Air Bag Indicator Light
Passenger Presence Sensing Module
Passenger Presence Sensor
Seat Belt Pretensioner
Seat Belt Tension Sensor
Seat Track Position Sensor
Vehicle (including Occupants)
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.
Delete Existing
Modify Existing
Save As New
Review entered data …
…and add, modify, or delete data
Return to Main Menu
Previous Step
Step 2: Connections
View Control Structure Diagram
Close Form
Volpe
The National Transportation Systems Center
Form Guidance

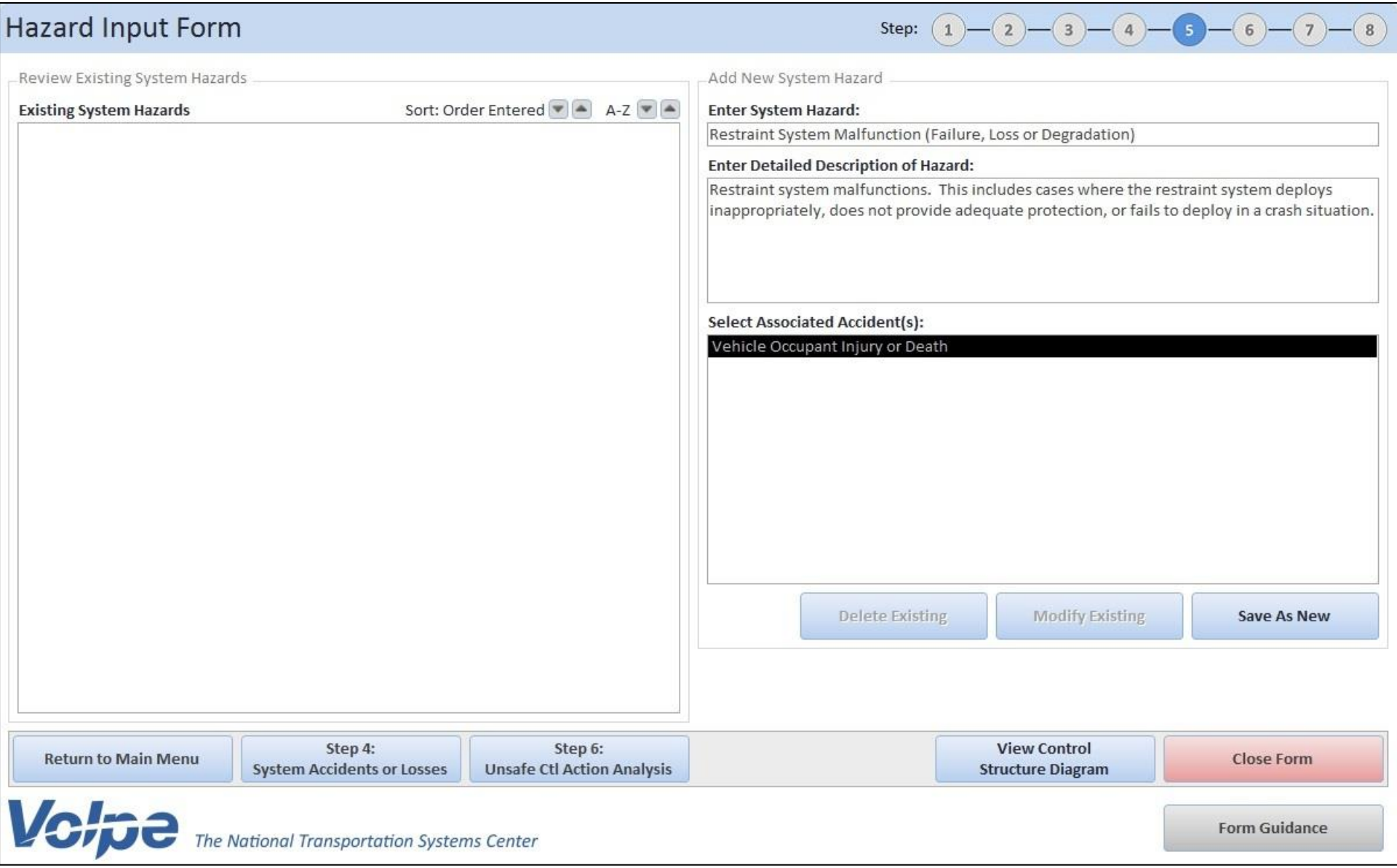

System Connections Input Form
Step: 1 2 3 4 5 6 7 8
Review Existing System Connections
Existing System Connections
Sort: Order Entered
A-Z From Type A-Z To Type
Air Bag Control Unit Controller Passenger Air Bag Indicator Ligh Actuator
Air Bag Control Unit Controller Air Bag Module Actuator
Air Bag Control Unit Controller Seat Belt Pretensioner Actuator
Air Bag Module Actuator Vehicle (including Occupants) Controlled Process
Crash Sensor Sensor Air Bag Control Unit Controller
Passenger Air Bag Indicator Ligh Sensor Driver Controller
Passenger Presence Sensing Mo Controller Air Bag Control Unit Actuator
Passenger Presence Sensing Mo Controller Air Bag Control Unit Actuator
Passenger Presence Sensor Sensor Passenger Presence Sensing Mo Controller
Seat Belt Pretensioner Actuator Vehicle (including Occupants) Controlled Process
Seat Belt Tension Sensor Sensor Passenger Presence Sensing Mo Controller
Seat Track Position Sensor Sensor Air Bag Control Unit Controller
Vehicle (including Occupants) Controlled Process Seat Track Position Sensor Sensor
Vehicle (including Occupants) Controlled Process Seat Belt Tension Sensor Sensor
Vehicle (including Occupants) Controlled Process Crash Sensor Sensor
Vehicle (including Occupants) Controlled Process Passenger Presence Sensor Sensor
Add New System Connection
Connection Originating Component
Name:
Type:
Connection Terminating Component
Name:
Type:
Enter a Connection Description:
Delete Existing
Modify Existing
Save As New
Return to Main Menu
Step 1: Component
Step 3: Control Action
View Control Structure Diagram
Close Form
Volpe The National Transportation Systems Center
Form Guidance

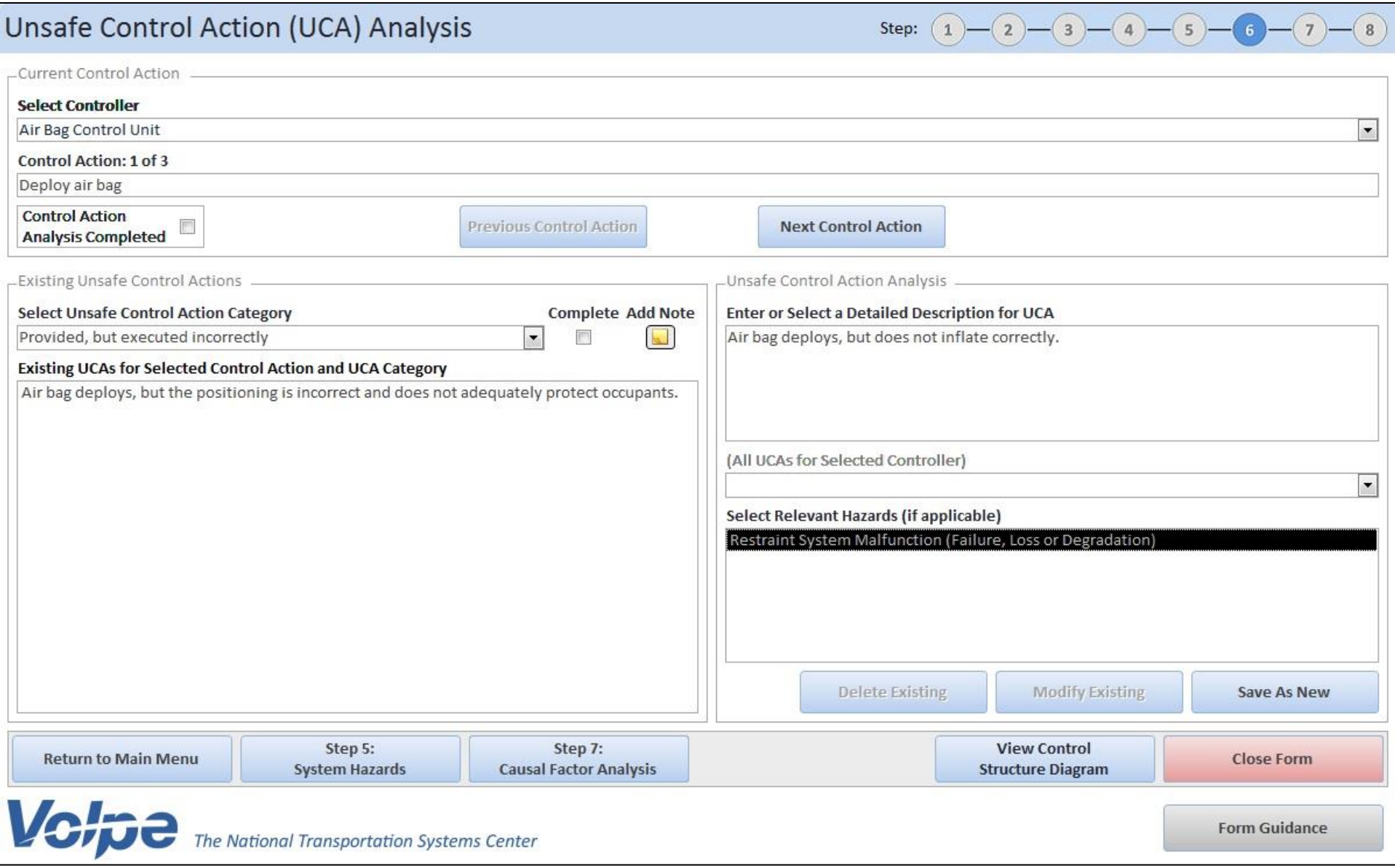

System Connections Input Form
Step: 1 2 3 4 5 6 7 8
Review Existing System Connections
Existing System Connections
Sort: Order Entered
A-Z From
Type
A-Z To
Type
Air Bag Control Unit Controller Passenger Air Bag Indicator Ligh Actuator
Air Bag Control Unit Controller Air Bag Module Actuator
Air Bag Control Unit
Air Bag Module
Crash Sensor
Passenger Air Bag Indicato
Passenger Presence Sensir
Passenger Presence Sensir
Passenger Presence Sensor Sensor Passenger Presence Sensing Mo Controller
Seat Belt Pretensioner Actuator Vehicle (including Occupants) Controlled Process
Seat Belt Tension Sensor Sensor Passenger Presence Sensing Mo Controller
Seat Track Position Sensor Sensor Air Bag Control Unit Controller
Vehicle (including Occupants) Controlled Process Seat Track Position Sensor Sensor
Vehicle (including Occupants) Controlled Process Seat Belt Tension Sensor Sensor
Vehicle (including Occupants) Controlled Process Crash Sensor Sensor
Vehicle (including Occupants) Controlled Process Passenger Presence Sensor Sensor
SafetyHAT uses information about your system to simplify data entry
Add New System Connection
Connection Originating Component
Name:
Type:
Connect
Name:
Enter a
Air Bag Control Unit
Air Bag Module
Crash Sensor
Driver
Passenger Air Bag Button
Passenger Air Bag Indicator Light
Passenger Presence Sensing Module
Passenger Presence Sensor
Seat Belt Pretensioner
Seat Belt Tension Sensor
Seat Track Position Sensor
Vehicle (including Occupants)
Delete Existing
Modify Existing
Save As New
Return to Main Menu
Step 1: Component
Step 3: Control Action
View Control Structure Diagram
Close Form
Volpe
The National Transportation Systems Center
Form Guidance

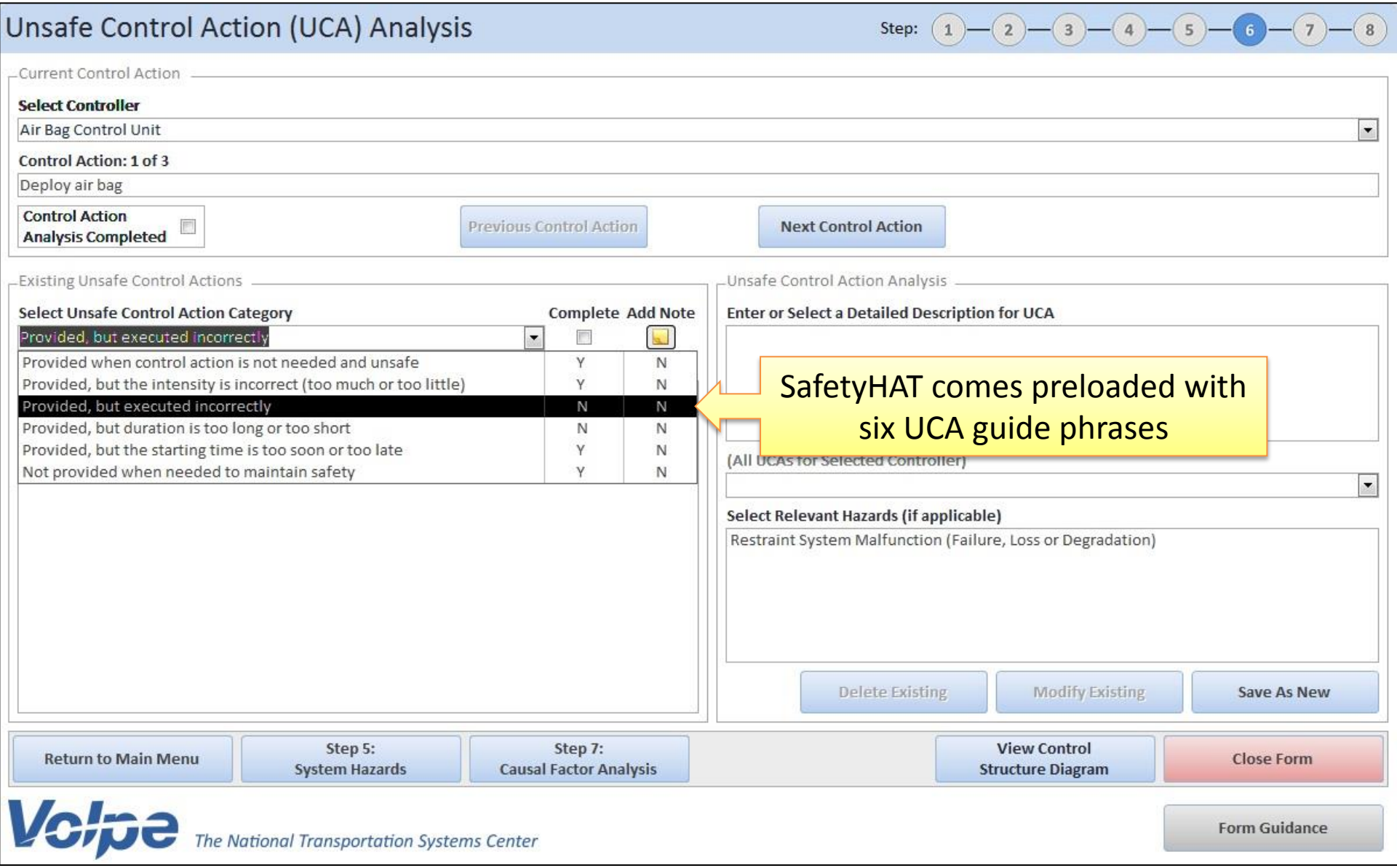

Control Action Input Form
Step: 1 2 3 4 5 6 7 8
Review Existing Control Actions
View Control Actions by Controller
Sort: Order Entered A-Z
Air Bag Control Unit
Deploy air bag
Deploy seat belt pretensioner
Add New Control Action
Select Controller
Air Bag Control Unit
Enter Control Action:
Illuminate Passenger Air Bag Disabled Light
Enter Detailed Description of the Control Action:
Turn on the "Passenger Air Bag Disabled" light when the passenger air bag is not activated
Delete Existing
Modify Existing
Save As New
Return to Main Menu
Step 2: Connections
Step 4: System Accidents or Losses
View Control Structure Diagram
Close Form
Volpe
The National Transportation Systems Center
Form Guidance


Control Action Input Form
Step: 1 2 3 4 5 6 7 8
Review Existing Control Actions
View Control Actions by Controller
Sort: Order Entered A-Z
Air Ba
Depl
Depl
SafetyHAT identifies controllers based on your system connections
Add New Control Action
Select Controller
Air Bag Control Unit
Driver
Air Bag Control Unit
Passenger Presence Sensing Module
Enter Detailed Description of the Control Action:
Delete Existing
Modify Existing
Save As New
Return to Main Menu
Step 2: Connections
Step 4: System Accidents or Losses
View Control Structure Diagram
Close Form
Volpe
The National Transportation Systems Center
Form Guidance


Accident (or Losses) Input Form
Step: 1 2 3 4 5 6 7 8
Review Existing System Accidents or Losses
Existing System Accidents (or Losses)
Sort: Order Entered A-Z
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.
Delete Existing
Modify Existing
Save As New
Return to Main Menu
Step 3: Control Actions
Step 5: System Hazards
View Control Structure Diagram
Close Form
Volpe
The National Transportation Systems Center
Form Guidance


Hazard Input Form
Step: 1 2 3 4 5 6 7 8
Review Existing System Hazards
Existing System Hazards
Sort: Order Entered A-Z
Add New System Hazard
Enter System Hazard:
Restraint System Malfunction (Failure, Loss or Degradation)
Enter Detailed Description of Hazard:
Restraint 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
Delete Existing
Modify Existing
Save As New
Return to Main Menu
Step 4: System Accidents or Losses
Step 6: Unsafe Ctl Action Analysis
View Control Structure Diagram
Close Form
Volpe
The National Transportation Systems Center
Form Guidance


Unsafe Control Action (UCA) Analysis
Step: 1 2 3 4 5 6 7 8
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
Complete
Add Note
Provided, but executed incorrectly
Existing UCAs 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)
Restraint 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


Unsafe Control Action (UCA) Analysis
Step: 1 2 3 4 5 6 7 8
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
Complete
Add Note
Provided, but executed incorrectly
Provided when control action is not needed and unsafe Y N
Provided, but the intensity is incorrect (too much or too little) Y N
Provided, but executed incorrectly N N
Provided, but duration is too long or too short N N
Provided, but the starting time is too soon or too late Y N
Not provided when needed to maintain safety Y N
Unsafe Control Action Analysis
Enter or Select a Detailed Description for UCA
SafetyHAT comes preloaded with six UCA guide phrases
(All UCAs for Selected Controller)
Select Relevant Hazards (if applicable)
Restraint 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

Causal Factor Analysis

Step: 1 — 2 — 3 — 4 — 5 — 6 — 7 — 8

Unsafe Control Action Details

Controller 1 of 2

Air Bag Control Unit

Associated Hazards:

Restraint System Malfunction (Failure, Loss or Degradation)

Description 7 of 8

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

Control Action Analysis Completed ☐

Previous Controller | Previous Record | Next Record | Next Controller

Add Note

Existing Causal Factor Analyses

Sort: Order Entered ▼▲ Component Name A-Z ▼▲

Existing Causal Factors for Selected Unsafe Control Action

Causal Factor	Component Name or Connection From	Connection To
Hazardous interaction with other components	Air Bag Control Unit	
Hazardous interaction with other components	Air Bag Control Unit	
Controller hardware faulty, change over time	Air Bag Control Unit	
Controller hardware faulty, change over time	Air Bag Control Unit	
Software error (inadequate control algorithm,	Air Bag Control Unit	
Sensor inadequate operation, change over tim	Crash Sensor	
Sensor to controller signal inadequate, missing	Crash Sensor	Air Bag Control Unit

Causal Factor Analysis

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.

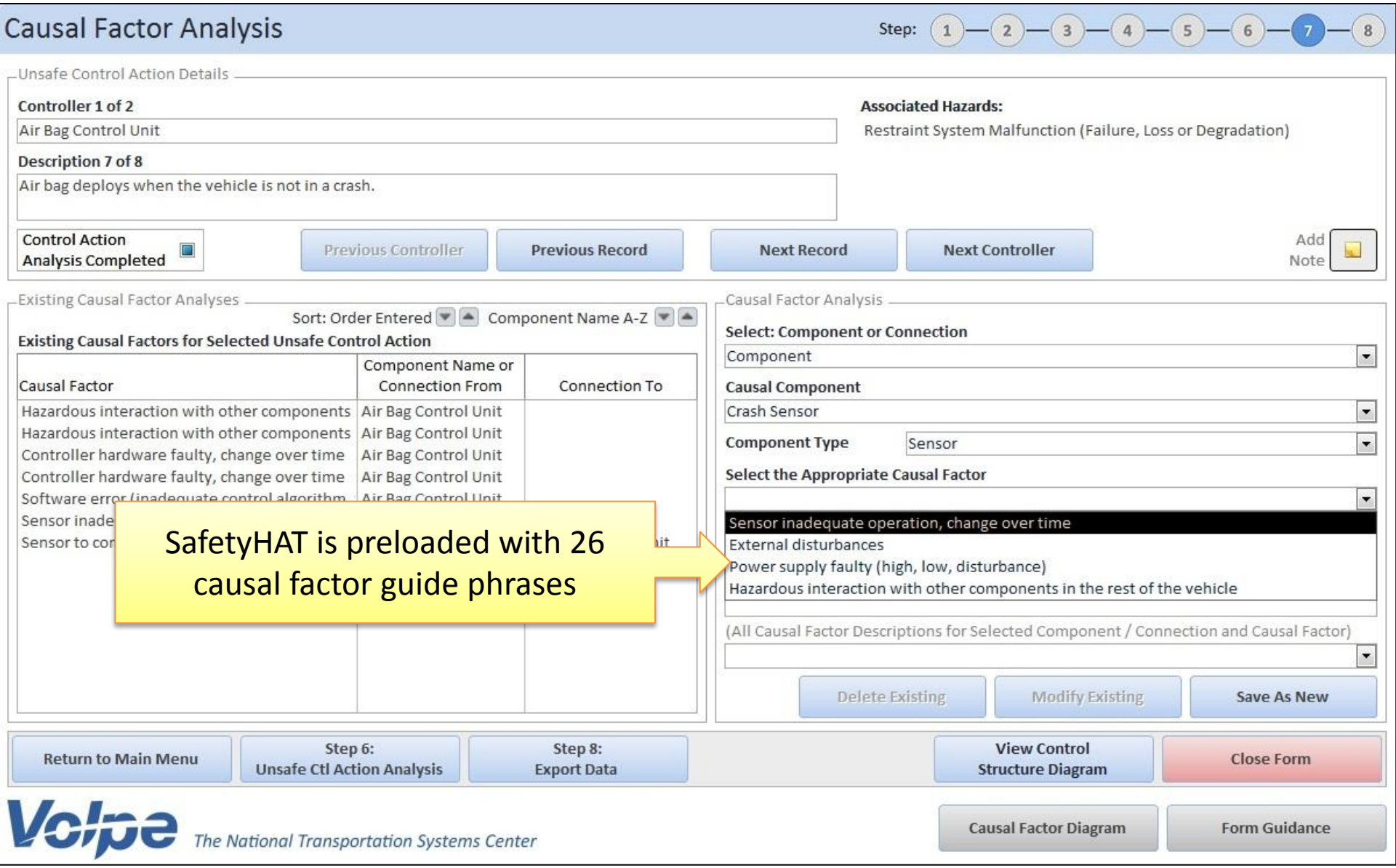
(All Causal Factor Descriptions for Selected Component / Connection and Causal Factor)

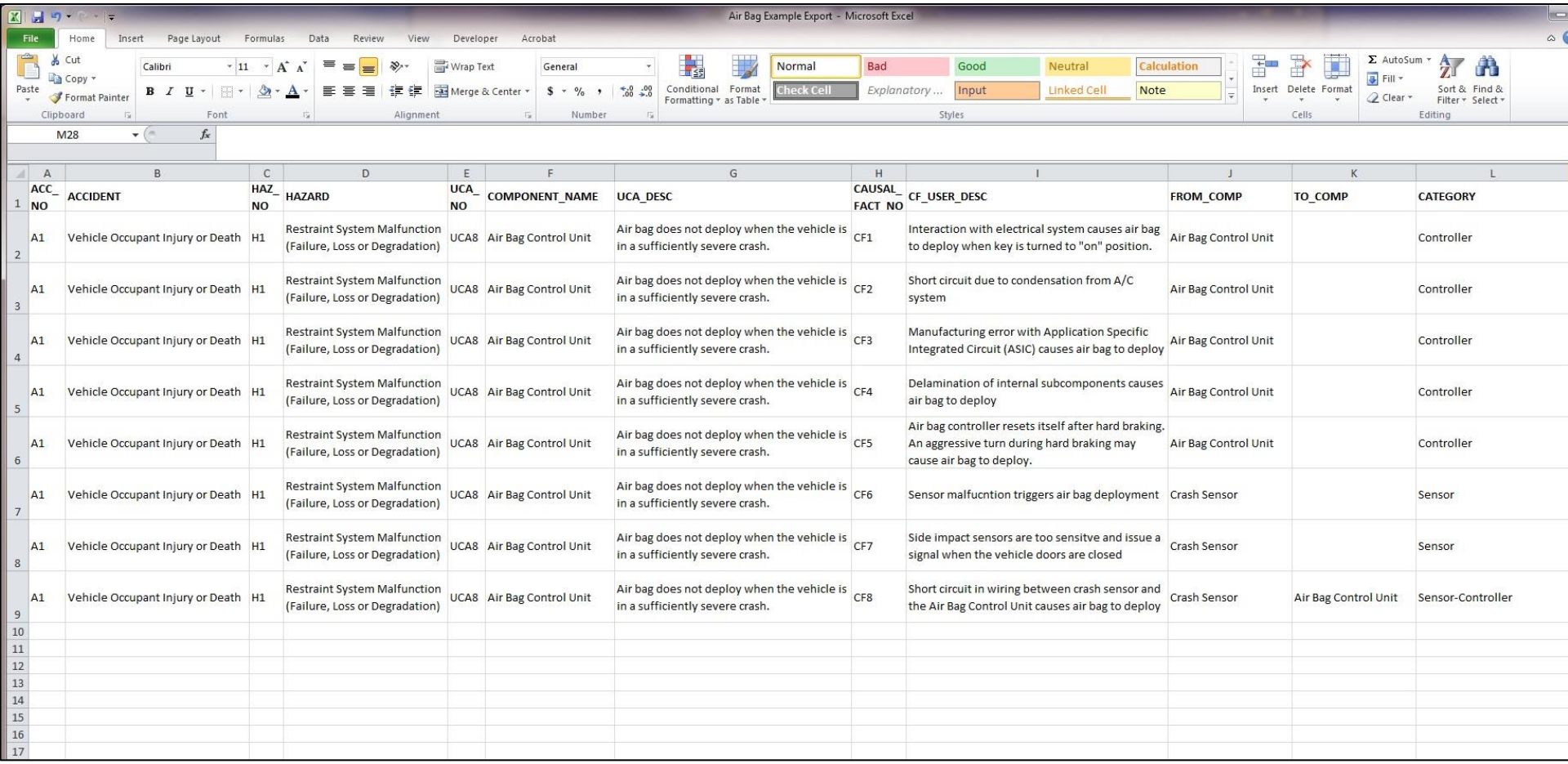
Delete Existing | Modify Existing | Save As New

Return to Main Menu | Step 6: Unsafe Ctl Action Analysis | Step 8: Export Data | View Control Structure Diagram | Close Form

Volpe The National Transportation Systems Center

Causal Factor Diagram | Form Guidance


Causal Factor Analysis
Step: 1 2 3 4 5 6 7 8
Unsafe Control Action Details
Controller 1 of 2
Air Bag Control Unit
Associated Hazards:
Restraint System Malfunction (Failure, Loss or Degradation)
Description 7 of 8
Air bag deploys when the vehicle is not in a crash.
Control Action Analysis Completed
Previous Controller
Previous Record
Next Record
Next Controller
Add Note
Existing Causal Factor Analyses
Sort: Order Entered
Component Name A-Z
Existing Causal Factors for Selected Unsafe Control Action
Causal Factor
Component Name or Connection From
Connection To
Hazardous interaction with other components
Air Bag Control Unit
Hazardous interaction with other components
Air Bag Control Unit
Controller hardware faulty, change over time
Air Bag Control Unit
Controller hardware faulty, change over time
Air Bag Control Unit
Causal Factor Analysis
Select: Component or Connection
Component
Causal Component
Crash Sensor
Component Type
Sensor
Select the Appropriate Causal Factor
Sensor inadequate operation, change over time
External disturbances
Power supply faulty (high, low, disturbance)
Hazardous interaction with other components in the rest of the vehicle
(All Causal Factor Descriptions for Selected Component / Connection and Causal Factor)
Delete Existing
Modify Existing
Save As New
SafetyHAT is preloaded with 26 causal factor guide phrases
Return to Main Menu
Step 6: Unsafe Ctl Action Analysis
Step 8: Export Data
View Control Structure Diagram
Close Form
Volpe
The National Transportation Systems Center
Causal Factor Diagram
Form Guidance



ACC_NO	ACCIDENT	HAZ_NO	HAZARD	UCA_NO	COMPONENT_NAME	UCA_DESC	CAUSAL_FACT_NO	CF_USER_DESC	FROM_COMP	TO_COMP	CATEGORY
A1	Vehicle Occupant Injury or Death	H1	Restraint System Malfunction (Failure, Loss or Degradation)	UCA8	Air Bag Control Unit	Air bag does not deploy when the vehicle is in a sufficiently severe crash.	CF1	Interaction with electrical system causes air bag to deploy when key is turned to "on" position.	Air Bag Control Unit		Controller
A1	Vehicle Occupant Injury or Death	H1	Restraint System Malfunction (Failure, Loss or Degradation)	UCA8	Air Bag Control Unit	Air bag does not deploy when the vehicle is in a sufficiently severe crash.	CF2	Short circuit due to condensation from A/C system	Air Bag Control Unit		Controller
A1	Vehicle Occupant Injury or Death	H1	Restraint System Malfunction (Failure, Loss or Degradation)	UCA8	Air Bag Control Unit	Air bag does not deploy when the vehicle is in a sufficiently severe crash.	CF3	Manufacturing error with Application Specific Integrated Circuit (ASIC) causes air bag to deploy	Air Bag Control Unit		Controller
A1	Vehicle Occupant Injury or Death	H1	Restraint System Malfunction (Failure, Loss or Degradation)	UCA8	Air Bag Control Unit	Air bag does not deploy when the vehicle is in a sufficiently severe crash.	CF4	Delamination of internal subcomponents causes air bag to deploy	Air Bag Control Unit		Controller
A1	Vehicle Occupant Injury or Death	H1	Restraint System Malfunction (Failure, Loss or Degradation)	UCA8	Air Bag Control Unit	Air bag does not deploy when the vehicle is in a sufficiently severe crash.	CF5	Air bag controller resets itself after hard braking. An aggressive turn during hard braking may cause air bag to deploy.	Air Bag Control Unit		Controller
A1	Vehicle Occupant Injury or Death	H1	Restraint System Malfunction (Failure, Loss or Degradation)	UCA8	Air Bag Control Unit	Air bag does not deploy when the vehicle is in a sufficiently severe crash.	CF6	Sensor malfucntion triggers air bag deployment	Crash Sensor		Sensor
A1	Vehicle Occupant Injury or Death	H1	Restraint System Malfunction (Failure, Loss or Degradation)	UCA8	Air Bag Control Unit	Air bag does not deploy when the vehicle is in a sufficiently severe crash.	CF7	Side impact sensors are too sensitve and issue a signal when the vehicle doors are closed	Crash Sensor		Sensor
A1	Vehicle Occupant Injury or Death	H1	Restraint System Malfunction (Failure, Loss or Degradation)	UCA8	Air Bag Control Unit	Air bag does not deploy when the vehicle is in a sufficiently severe crash.	CF8	Short circuit in wiring between crash sensor and the Air Bag Control Unit causes air bag to deploy	Crash Sensor	Air Bag Control Unit	Sensor-Controller

- 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

- 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

- SafetyHAT User Guide is available from: http://www.volpe.dot.gov/SafetyHAT

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