STPA Automation Tool
Outline

- Automating Analysis
  - Define Purpose of the Analysis
    - Identify Losses
    - Identify System-Level Requirements
      - Identify Functions
      - Clear Unused Functional Hazards
      - Identify Unsafe Conditions
    - Identify System Constraints
  - Create Hazard Summary
    - Fill In Hazard Summary
    - Losses Traceability
    - System Constraints Traceability
- Model the Control Structure
  - draw.io Integration
- Identify Unsafe Control Actions
  - Create Unsafe Control Action Table
    - Pulls data from draw.io Control Structure Model
  - Identify Unsafe Control Actions
  - Create Controller Constraint Table
  - Unsafe Control Actions Traceability
- Identify Loss Scenarios
  - Template
- Questions?
- Tool Link
Automating Analysis
Soap Box - The Dangers of Automating Analysis

Automating Analyses can be incredibly useful
- Decrease time it takes to complete
- Reduce errors by standardizing wording
- Repeatability of analysis

However, it can also be very dangerous to automate analyses
- Over-reliance on the tool
- Reduced thinking about the problem

The goal of any analysis automation effort should be to reduce the effort to produce the analysis without affecting the quality of the analysis. This means that analysis automation tools should only automate tasks that do not require engineering effort.
Define Purpose of the Analysis
Define Purpose of the Analysis

The STPA Handbook identifies 4 steps that comprise the definition of the purpose of the STPA

1. Identify Losses
2. Identify system-level hazards
3. Identify system-level constraints
4. Refine hazards
Identify Losses

The STPA Handbook, Chapter 2, identifies a set of example losses. The first function in the tool asks the user to identify which of these example losses apply to their system, then prompts the user for additional losses that they want to consider.

<table>
<thead>
<tr>
<th>Loss ID</th>
<th>Loss Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>L-1</td>
<td>Loss of life or injury to people</td>
</tr>
<tr>
<td>L-2</td>
<td>Loss of or damage to vehicle</td>
</tr>
<tr>
<td>L-3</td>
<td>Loss of or damage to objects outside the vehicle</td>
</tr>
<tr>
<td>L-4</td>
<td>Loss of mission (failure to complete mission)</td>
</tr>
<tr>
<td>L-5</td>
<td>Loss of customer satisfaction</td>
</tr>
</tbody>
</table>
Identify System-Level Hazards

The STPA Handbook identifies one method of defining hazards in the form of `<System> <Unsafe Condition>`

  E.g., `<Aircraft> <violate minimum separation standards in flight>`

ISO-26262 uses a `<Keyword> <Function>` approach for identifying hazards

  E.g., `<Loss of> <Braking>`

The STPA Automation Tool supports both methods. For the Function approach, the Identify Functions function prompts the user for their functions, prompts the user with a list of default keywords, and asks the user if they want to add keywords. It then populates a list of hazards in the `<Keyword> <Function>` format.

Next, the user selects which of the default functional hazards actually apply to their system and runs the Clear Unused Functional Hazards function which deletes the unused functional hazards and generates Hazard ID numbers.
Identify System-Level Hazards

Add a Function?
Enter additional Function and press Yes, or press No

Add Keywords?
Default Keywords are Loss of, Too Much, Not Enough, Early, Late, Reverse, Unintentional, Stuck, Erratic.

Add a Keywords?
Enter additional Keywords and press Yes, or press No
## Identify System-Level Hazards

<table>
<thead>
<tr>
<th>Hazard ID</th>
<th>Functions</th>
<th>Hazards</th>
<th>Hazard Description</th>
<th>Hazard Applies to Function?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Braking</td>
<td>Loss of Braking</td>
<td>Braking</td>
<td>Early Braking</td>
<td>☑️</td>
</tr>
<tr>
<td>Braking</td>
<td>Too Much Braking</td>
<td>Not Enough Braking</td>
<td>Reverse Braking</td>
<td>☐️</td>
</tr>
<tr>
<td>Braking</td>
<td>Late Braking</td>
<td>Unintentional Braking</td>
<td>Erratic Braking</td>
<td>☑️</td>
</tr>
<tr>
<td>Braking</td>
<td>Stuck Braking</td>
<td></td>
<td>Loss of Steering</td>
<td>☑️</td>
</tr>
<tr>
<td>Steering</td>
<td>Loss of Steering</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hazard ID</th>
<th>Functions</th>
<th>Hazards</th>
<th>Hazard Description</th>
<th>Hazard Applies to Function?</th>
</tr>
</thead>
<tbody>
<tr>
<td>[FH-1.1]</td>
<td>Braking</td>
<td>Loss of Braking</td>
<td></td>
<td>☑️</td>
</tr>
<tr>
<td>[FH-1.2]</td>
<td>Braking</td>
<td>Unintentional Braking</td>
<td></td>
<td>☑️</td>
</tr>
<tr>
<td>[FH-2.1]</td>
<td>Steering</td>
<td>Loss of Steering</td>
<td></td>
<td>☑️</td>
</tr>
<tr>
<td>[FH-3.1]</td>
<td>Acceleration</td>
<td>Loss of Acceleration</td>
<td></td>
<td>☑️</td>
</tr>
</tbody>
</table>
Identify System-Level Hazards

For the Unsafe Condition approach, the Identify Unsafe Conditions function prompts the user for the name of the system, then prompts the user for all of the unsafe conditions for that system. Then it asks the user if there are additional systems and repeats the process for all systems.
Identify System Constraints

The Identify System Constraints function prompts the user for the preventative measure for \(<\text{Keyword}>\) \(<\text{Function}>\) hazards, prompts the user to invert the condition for \(<\text{System}>\) \(<\text{Unsafe Condition}>\) hazards, and prompts the user for any additional system constraints.

After the prompts, the function populates the system constraints table.
Identify System Constraints

Preventative Measures
Enter Preventative Measure for Loss of Braking:

Yes No

Inverted Conditions
Enter System and Inverted Condition for hazard:
Vehicle stops in unsafe location (e.g., in an intersection)
Example Entry: Vehicle must satisfy minimum separation standards at all times.

Yes No

Additional Constraints?
Do you have additional constraints?

Yes No

Add a Constraint?
Enter additional Constraint and press Yes, or press No

Yes No

System Constraint ID | System Constraint
--- | ---
[SC-1] If Loss of Braking occurs then loss of braking must be detected and mitigated
[SC-2] If Unintentional Braking occurs then unintentional braking must be detected and mitigated
[SC-3] If Loss of Steering occurs then loss of steering must be detected and mitigated
[SC-4] If Loss of Acceleration occurs then loss of acceleration must be detected and mitigated
[SC-6] Test Constraint
Create Hazard Summary

There are three functions to create the hazard summary. The first function populates the hazards from the Functional Hazards and System Hazards tabs into the Hazard Summary tab. The other two functions help the user populate the Losses Traceability and System Constraint Traceability for all of the hazards.

<table>
<thead>
<tr>
<th>ID</th>
<th>Hazard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[FH-1.1]</td>
<td>Loss of Braking</td>
<td></td>
</tr>
<tr>
<td>[FH-1.2]</td>
<td>Unintentional Braking</td>
<td></td>
</tr>
<tr>
<td>[FH-2.1]</td>
<td>Loss of Steering</td>
<td></td>
</tr>
<tr>
<td>[FH-3.1]</td>
<td>Loss of Acceleration</td>
<td></td>
</tr>
<tr>
<td>[SH-1]</td>
<td>Vehicle stops in unsafe location (e.g., in an intersection)</td>
<td></td>
</tr>
</tbody>
</table>
Create Hazard Summary

Losses Traceability

Lossses

For each Hazard, select all applicable Losses

[FH-1.1] Loss of Braking

☐ [L-1] Loss of life or injury to people
☐ [L-2] Loss of or damage to vehicle

Losses Traceability

[FH-1.2] Unintentional Braking

☐ [L-1] Loss of life or injury to people
☐ [L-2] Loss of or damage to vehicle
☐ [L-3] Loss of or damage to objects outside the vehicle
☑ [L-4] Loss of mission (failure to complete mission)
☑ [L-5] Loss of customer satisfaction
Create Hazard Summary

System Constraints Traceability

**System Constraints**

For each Hazard, select all applicable System Constraints

[FH-1.1] Loss of Braking

- [SC-1] If Loss of Braking occurs then loss of braking must be detected and mitigated
- [SC-2] If Unintentional Braking occurs then unintentional braking must be detected and mitigated
- [SC-3] If Loss of Steering occurs then loss of steering must be detected and mitigated
- [SC-4] If Loss of Acceleration occurs then loss of acceleration must be detected and mitigated
- [SC-5] Vehicle must not stop in unsafe location.
- [SC-6] Test Constraint
## Create Hazard Summary

<table>
<thead>
<tr>
<th>ID</th>
<th>Hazard</th>
<th>Description</th>
<th>Losses Traceability</th>
<th>System Constraints Traceability</th>
</tr>
</thead>
<tbody>
<tr>
<td>[FH-1.1]</td>
<td>Loss of Braking</td>
<td></td>
<td>[L-2] Loss of or damage to vehicle&lt;br&gt;[L-6] Loss of customer satisfaction&lt;br&gt;[L-1] Loss of life or injury to people&lt;br&gt;[L-4] Loss of mission (failure to complete mission)</td>
<td>[SC-1] If Loss of Braking occurs then loss of braking must be detected and mitigated&lt;br&gt;[SC-6] Test Constraint</td>
</tr>
<tr>
<td>[FH-1.2]</td>
<td>Unintentional Braking</td>
<td></td>
<td>[L-5] Loss of customer satisfaction&lt;br&gt;[L-3] Loss of or damage to objects outside the vehicle</td>
<td>[SC-2] If Unintentional Braking occurs then unintentional braking must be detected and mitigated</td>
</tr>
<tr>
<td>[FH-2.1]</td>
<td>Loss of Steering</td>
<td></td>
<td>[L-4] Loss of mission (failure to complete mission)&lt;br&gt;[L-5] Loss of customer satisfaction</td>
<td>[SC-3] If Loss of Steering occurs then loss of steering must be detected and mitigated</td>
</tr>
<tr>
<td>[SH-1]</td>
<td>Vehicle stops in unsafe location (e.g. in an intersection)</td>
<td></td>
<td>[L-2] Loss of or damage to vehicle&lt;br&gt;[L-1] Loss of life or injury to people&lt;br&gt;[L-3] Loss of or damage to objects outside the vehicle&lt;br&gt;[L-5] Loss of customer satisfaction</td>
<td>[SC-5] Vehicle must not stop in unsafe location&lt;br&gt;[SC-6] Test Constraint</td>
</tr>
</tbody>
</table>
Model the Control Structure
Model the Control Structure

The STPA Automation Tool integrates with draw.io for modeling the Control Structure. Create the Control Structure Model using rectangles for items in the system (e.g., controllers, controlled processes, etc.) and directional connectors for control actions, feedback, and data. Label all rectangles and directional connectors.

Once the Control Structure is modeled, export as an image (PNG, JPEG, SVG) to pull into the STPA Automation Tool. Then export as XML and save to Google Drive to be able to automatically create the Unsafe Control Actions Table from the Control Structure Model.
Identify Unsafe Control Actions
Identify Unsafe Control Actions

The STPA Automation Tool can automatically extract the information from the draw.io Control Structure Model. Select the Create Unsafe Control Actions function, and enter the URL where the XML file was saved in Google Drive.

The tool reads the XML file and extracts the directional connectors and the source and destination rectangles to create the table.

Select the Arrow Type for each directional connector from the drop down menu:
- Control Action
- Feedback
- Data/Other
Identify Unsafe Control Actions

The Identify Unsafe Control Actions function guides the user through the set of potential Unsafe Control Actions, and if the Unsafe Control Action applies to their system, asks the user to enter the context that makes it an unsafe control action.

![Image of the Identify Unsafe Control Actions function](image_url)
Identify Unsafe Control Actions

The Create Control Constraints function guides the user through developing the Control Constraints for each Unsafe Control Action. It prompts the user for limits of how much or time when appropriate for the Unsafe Control Action.
Identify Unsafe Control Actions

The Unsafe Control Actions Traceability function guides the user through tracing the Unsafe Control Actions to the Hazards.

For each Unsafe Control Action, select all applicable Hazards

[UCA-1] Safety Steward does not provide Press E-Stop to E-Stop when a collision is imminent

[UCA-2] Safety Steward provides Press E-Stop to E-Stop when there is no imminent collision
- [FH-1.1] Loss of Braking
- [FH-1.2] Unintentional Braking
- [FH-2.1] Loss of Steering
- [FH-3.1] Loss of Acceleration
- [SH-1] Vehicle stops in unsafe location (e.g. in an intersection)

[UCA-3] Safety Steward provides Press E-Stop to E-Stop when the vehicle is parked
# Identify Unsafe Control Actions

<table>
<thead>
<tr>
<th>Unsafe Control Action</th>
<th>Hazard Traceability</th>
<th>Controller Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>[UCA-1] Safety Steward does not provide Press E-Stop to E-Stop when a collision is imminent</td>
<td>[FH-1.1] Loss of Braking</td>
<td>[CC-1] Safety Steward must provide Press E-Stop to E-Stop when a collision is imminent</td>
</tr>
<tr>
<td>[UCA-2] Safety Steward provides Press E-Stop to E-Stop when there is no imminent collision</td>
<td>[FH-3.1] Loss of Acceleration</td>
<td>[CC-2] Safety Steward must not provide Press E-Stop to E-Stop when there is no imminent collision</td>
</tr>
<tr>
<td>[UCA-3] Safety Steward provides Press E-Stop to E-Stop when the vehicle is parked</td>
<td>[SH-1] Vehicle stops in unsafe location (e.g. in an intersection)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[FH-2.1] Loss of Steering</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[FH-1.2] Unintentional Braking</td>
<td></td>
</tr>
<tr>
<td>[UCA-4] Safety Steward provides Press E-Stop too early to E-Stop when AV still has time to mitigate the</td>
<td>[FH-3.1] Loss of Acceleration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[FH-2.1] Loss of Steering</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[FH-1.2] Unintentional Braking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[SH-1] Vehicle stops in unsafe location (e.g. in an intersection)</td>
<td></td>
</tr>
</tbody>
</table>
Identify Loss Scenarios
Identify Loss Scenarios

This is the most important part of the analysis. Since it requires in-depth engineering analysis, no automation is provided. However, a template is provided as part of the Controller Constraints tab where the analysis can be performed.
Questions?
Tool Link

https://docs.google.com/spreadsheets/d/1RR04D2UPmyZAtwojIzfKY6jHOefAmNMFTsNcd0-hk7c/copy