Extending and Automating STPA for Requirements Generation and Analysis

John Thomas
4/18/2012
Traditional Safety Engineering

Create Design

Hazard Analysis (FTA, FMEA, HAZOP, etc)

- Find chains of failure events that lead to accidents

Resolution

- Add redundancy, protective functions, “patches”

(Vincoli, 1993); (Bahr, 1997); (FAA SSH, 2000); (AF SSH, 2000)
Traditional Hazard Analysis Methods

- Failure Modes Effects and Criticality Analysis (1949)
  - Reliability technique; start with component failures, find effects
- Fault Tree Analysis (1961)
  - Top-down approach; start with hazard, find failure combinations
- Hazards and Operability Analysis (1960s)
  - Apply guidewords to components, find consequences
- Event Tree Analysis (1975)
  - Start with initiating event, trace forward in time

- Require fairly detailed design
- Not much help creating safety requirements from the start
- Especially complex software requirements

(Hammer, 1972); (Lawley, 1974); (Vesely et al., 1981); (Rasmussen, 1975); (Rasmussen, 1990); (Garrett, 2002); (Lisagor, 2006)
STPA (System-Theoretic Process Analysis)

- Built on STAMP model
- Start from hazards
- Identify hazardous control actions and safety constraints
- Identify scenarios that lead to violation of safety constraints

(STAMP Model)

(STPA Hazard Analysis)

Applied without systematic procedures for these parts

(Leveson, 2011)
STPA Control Flaws

Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)

Controller

Process Model (inconsistent, incomplete, or incorrect)

Controller

Control input or external information wrong or missing

Actuator

Inappropriate, ineffective, or missing control action

Inadequate operation

Delayed operation

Controller

Controller

Sensor

Inadequate operation

Feedback

Inadequate or missing feedback

Feedback Delays

Incorrect or no information provided

Measurement inaccuracies

Feedback delays

Controller

Controlled Process

Component failures

Changes over time

Controller

Unidentified or out-of-range disturbance

Process output contributes to system hazard

Need to create requirements specification without control flaws
Formal (model-based) requirements specification language

Example: SpecTRM-RL Model of TCAS II Collision Avoidance Logic

Formal mathematical representation:

Other-Traffic =
(Alt-Reporting == Lost) ∧ ¬Bearing-Valid V (Alt-Reporting == Lost) ∧ ¬Range-Valid V
(Alt-Reporting == Lost) ∧ Bearing-Valid ∧ Range-Valid ∧ ¬Proximate-Traffic-Condition ∧ ¬Potential-Threat-Condition V (Other-Aircraft == On-Ground)

(Leveson, 2000), (Zimmerman, 2002)
Structure of a Hazardous Control Action

Example: “Operator provides open train door command when train is moving”
Structure of a Hazardous Control Action

Example: “Operator provides open train door command when train is moving”

Four parts of a hazardous control action

– Source: the controller that can provide the control action
– Type: whether the control action was provided or not provided
– Control Action: the controller’s command that was provided / missing
– Context: the system or environmental state in which command is provided

Process Model

<table>
<thead>
<tr>
<th>Train motion</th>
<th>Stopped Moving</th>
</tr>
</thead>
<tbody>
<tr>
<td>Train location</td>
<td>At platform Not Aligned</td>
</tr>
</tbody>
</table>
Identifying Hazardous Control Actions

• Type 1: Providing control action causes hazard
  – 1a) Define potential contexts (combinations of process model values)
  – 1b) Determine whether the control action is hazardous in each context
  – 1c) Determine whether control action can still be hazardous if too early/too late

• Type 2: Not providing control action causes hazard
  – Same as above, but for an absence of the selected control action
Example: Train door controller

System Hazards

H-1: Doors close on a person in the doorway

H-2: Doors open when the train is moving or not at platform

H-3: Passengers/staff are unable to exit during an emergency
Example: Control loop

Door Controller

Process model
- Door obstruction
  - Person in doorway
  - Person not in doorway
  - Unknown
- Door position
  - Fully open
  - Fully closed
  - Partially open
  - Unknown
- Train position
  - Aligned with platform
  - Not aligned with platform
  - Unknown
- Train motion
  - Stopped
  - Train is moving
  - Unknown
- Emergency
  - No emergency
  - Evacuation required
  - Unknown

Commands:
- Open door
- Stop opening door
- Close door
- Stop closing door

Other Inputs
- Train motion
- Train position
- Emergency Indicator

Feedback
- Door position
- Door obstruction

Door Actuator

Door Sensors

Physical Door
Process

- Identify hazards
- Create control structure
- Create process model

Identify Unsafe Control Actions
- For each control action, consider:
  - 1) Providing causes hazard
  - 2) Not providing causes hazard

- Identify Causes of Unsafe Control Actions
1) Control action is provided

- Control action: *Door Open* command
- 1a) Define potential contexts (combinations of process model variables)

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Train Motion</th>
<th>Emergency</th>
<th>Train Position</th>
<th>Door Obstruction</th>
<th>Door Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door open command</td>
<td>Stopped</td>
<td>No</td>
<td>Aligned with platform</td>
<td>Not obstructed</td>
<td>Closed</td>
</tr>
<tr>
<td>Door open command</td>
<td>Stopped</td>
<td>No</td>
<td>Aligned with platform</td>
<td>Not obstructed</td>
<td>Open</td>
</tr>
<tr>
<td>Door open command</td>
<td>Stopped</td>
<td>Yes</td>
<td>Aligned with platform</td>
<td>Obstructed</td>
<td>Closed</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
1) Control action is provided

Control action: *Door Open* command
- 1a) Define potential contexts (combinations of process model variables)
- 1b) Determine whether the control action is hazardous in each context

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Train Motion</th>
<th>Emergency</th>
<th>Train Position</th>
<th>Door Obst. / Position</th>
<th>Hazardous?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door open command</td>
<td>Moving</td>
<td>No</td>
<td>(doesn’t matter)</td>
<td>(doesn’t matter)</td>
<td>Yes</td>
</tr>
<tr>
<td>Door open command</td>
<td>Moving</td>
<td>Yes</td>
<td>(doesn’t matter)</td>
<td>(doesn’t matter)</td>
<td>Yes*</td>
</tr>
<tr>
<td>Door open command</td>
<td>Stopped</td>
<td>Yes</td>
<td>(doesn’t matter)</td>
<td>(doesn’t matter)</td>
<td>No</td>
</tr>
<tr>
<td>Door open command</td>
<td>Stopped</td>
<td>No</td>
<td>Not at platform</td>
<td>(doesn’t matter)</td>
<td>Yes</td>
</tr>
<tr>
<td>Door open command</td>
<td>Stopped</td>
<td>No</td>
<td>At platform</td>
<td>(doesn’t matter)</td>
<td>No</td>
</tr>
</tbody>
</table>

*Design decision: In this situation, evacuate passengers to other cars. Meanwhile, stop the train and then open doors.*
1) Control action is provided

Control action: *Door Open* command

- 1a) Define potential contexts (combinations of process model variables)
- 1b) Determine whether the control action is hazardous in each context
- 1c) Determine whether control action can still be hazardous if too early/too late

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Train Motion</th>
<th>Emergency</th>
<th>Train Position</th>
<th>Door Obst. / Position</th>
<th>Hazardous?</th>
<th>Hazardous if provided too early?</th>
<th>Hazardous if provided too late?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door open command</td>
<td>Moving</td>
<td>No</td>
<td>(doesn’t matter)</td>
<td>(doesn’t matter)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Door open command</td>
<td>Moving</td>
<td>Yes</td>
<td>(doesn’t matter)</td>
<td>(doesn’t matter)</td>
<td>Yes*</td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
<tr>
<td>Door open command</td>
<td>Stopped</td>
<td>Yes</td>
<td>(doesn’t matter)</td>
<td>(doesn’t matter)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Door open command</td>
<td>Stopped</td>
<td>No</td>
<td>Not at platform</td>
<td>(doesn’t matter)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Door open command</td>
<td>Stopped</td>
<td>No</td>
<td>At platform</td>
<td>(doesn’t matter)</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
2) Control action is not provided

Control action: *Door Open* command

- 2a) Identify process model variables
- 2b) Determine whether the absence of control action is hazardous in each context

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Train Motion</th>
<th>Emergency</th>
<th>Train Position</th>
<th>Door Obst. / Pos.</th>
<th>Hazardous?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door open command not provided</td>
<td>Stopped</td>
<td>Yes</td>
<td>(doesn’t matter)</td>
<td>(doesn’t matter)</td>
<td>Yes</td>
</tr>
<tr>
<td>Door open command not provided</td>
<td>Stopped</td>
<td>(doesn’t matter)</td>
<td>(doesn’t matter)</td>
<td>Closing on obstruction</td>
<td>Yes</td>
</tr>
<tr>
<td>Door open command not provided</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

(all others)
## Resulting List of Hazardous Control Actions

<table>
<thead>
<tr>
<th>Hazardous Control Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door open command provided while train is moving and there is no emergency</td>
</tr>
<tr>
<td>Door open command provided too late while train is stopped and emergency exists</td>
</tr>
<tr>
<td>Door open command provided while train is stopped, no emergency, and not at platform</td>
</tr>
<tr>
<td>Door open command provided while train is moving and emergency exists</td>
</tr>
<tr>
<td>Door open command <strong>not</strong> provided while train is stopped and emergency exists</td>
</tr>
<tr>
<td>Door open command <strong>not</strong> provided while doors are closing on someone</td>
</tr>
</tbody>
</table>

Much of this can be automated to assist the safety engineer!
Generating safety requirements

Hazardous Control Actions

Formal (model-based) requirements specification

<table>
<thead>
<tr>
<th>Condition</th>
<th>State</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alt-Reporting in-state Lost</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>Bearing-Valid</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>Range-Valid</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>Proximate-Traffic-Condition</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>Potential-Threat-Condition</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>Other-Aircraft in-state On-Ground</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>
Generating safety requirements

- Formal requirements can be derived using
  - Discrete mathematical structure for hazardous control actions
  - Predicate calculus underlying formal requirements
- Automatically generate formal requirements given these relationships!
Hazardous control actions: mathematical representation

Example: “Operator provides open train door command when train is moving”

Hazardous control action as 4-tuple \((S, T, CA, C)\) where:

- \(S \in \text{Controllers [from control structure]}\)
- \(T \in \{\text{Provided, Not Provided}\}\)
- \(CA \in \text{ControlActions}(S)\)
- \(C = \{V, S\} \mid (V \in \text{PMV}) \land (S \in \text{PMS}) \land S \text{ child } V\)
Hazardous control actions -> formal requirements specifications

1. Describing hazardous, functional, and required behavior
   - \( \text{HP}(h \in H, \text{ca} \in \text{CA}, c \in C) \)
     - True iff providing command \( \text{ca} \) in context \( c \) will cause hazard \( h \)
   - \( \text{HNP}(h \in H, \text{ca} \in \text{CA}, c \in C) \)
     - True iff not providing command \( \text{ca} \) in context \( c \) will cause hazard \( h \)
   - \( \text{FP}(f \in F, \text{ca} \in \text{CA}, c \in C) \)
     - True iff providing command \( \text{ca} \) in context \( c \) is necessary to achieve function \( f \)
   - \( \text{R}((\text{ca} \in \text{CA}, c \in C) \)
     - True iff command \( \text{CA} \) is required to be provided in context \( c \)

2. Consistency checks
   - \( \forall h_1 \in H, h_2 \in H \rightarrow \nexists \text{ca} \in \text{CA}, c \in C : \text{HP}(h_1, \text{ca}, c) \land \text{HNP}(h_2, \text{ca}, c) \)
     - For every potential context, it must be possible to avoid hazardous control actions/inactions. In other words, if it is hazardous to provide \( \text{CA} \) then it should be non-hazardous to not provide \( \text{CA} \)
   - \( \forall h \in H, f \in F \rightarrow \nexists \text{ca} \in \text{CA}, c \in C : \text{HP}(h, \text{ca}, c) \land \text{FP}(f, \text{ca}, c) \)
     - For every potential context, if it is necessary to provide a command to fulfill a function then it must not be hazardous to provide the command in that context

3. Requirements generation (SpecTRM-RL tables)
   - Compute \( \text{R}((\text{ca} \in \text{CA}, c \in C) \) to satisfy the following:
     - \( \forall h, \text{ca}, c : h \in H \land \text{ca} \in \text{CA} \land c \in C \rightarrow [\text{HP}(h, \text{ca}, c) \rightarrow \neg \text{R}(\text{ca}, c)] \)
     - \( \forall h, \text{ca}, c : h \in H \land \text{ca} \in \text{CA} \land c \in C \rightarrow [\text{R}(\text{ca}, c) \rightarrow \text{HNP}(h, \text{ca}, c)] \)
     - \( \forall f, \text{ca}, c : f \in F \land \text{ca} \in \text{CA} \land c \in C \rightarrow [\text{FP}(f, \text{ca}, c) \rightarrow \text{R}(\text{ca}, c)] \)
Generating safety requirements

- Example: Generated black-box model for door controller

<table>
<thead>
<tr>
<th>Provide 'Open Doors' command</th>
<th>Behavior required for function</th>
<th>Behavior required for safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door State</td>
<td>Doors not closing on person</td>
<td>T</td>
</tr>
<tr>
<td></td>
<td>Doors closing on person</td>
<td></td>
</tr>
<tr>
<td>Train Position</td>
<td>Aligned with platform</td>
<td>T</td>
</tr>
<tr>
<td></td>
<td>Not aligned with platform</td>
<td></td>
</tr>
<tr>
<td>Train Motion</td>
<td>Stopped</td>
<td>T</td>
</tr>
<tr>
<td></td>
<td>Train is moving</td>
<td></td>
</tr>
<tr>
<td>Emergency</td>
<td>No emergency</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Emergency exists</td>
<td>T</td>
</tr>
</tbody>
</table>

Open Doors =
(Train Position in-state Aligned) \land (Train Motion in-state Stopped) \lor (Train Motion in-state Stopped) \land (Emergency in-state exists) \lor (Door State in-state closing on person) \land (Train Motion in-state Stopped)
Detecting conflicts

• Can automatically check consistency using info in context tables

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Train Motion</th>
<th>Emergency</th>
<th>Hazardous?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door open command</td>
<td>Moving</td>
<td>Yes</td>
<td>Yes*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Train Motion</th>
<th>Emergency</th>
<th>Hazardous?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door open command not provided</td>
<td>Moving</td>
<td>Yes</td>
<td>Yes*</td>
</tr>
</tbody>
</table>
Summary

• Systematic process for performing STPA
• Method to help automate STPA
• Drives the creation of requirements and definition of control algorithms from the STPA analysis
• Automatically generating formal safety requirements
• Analyze not only safety aspects, but also functional goals
• Consistency checks to detect safety vs. functional conflicts
Thank you!

Questions?