Systems Theoretic Process Analysis (STPA)
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios

(Leveson, 2012)
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios

(Leveson, 2012)
STPA
(System-Theoretic Process Analysis)

• Identify accidents and hazards
• Draw the control structure

**Step 1: Identify unsafe control actions**

• Step 2: Identify causal factors and create scenarios

(Leveson, 2012)
ITP Exercise

a new in-trail procedure for trans-oceanic flights
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios

(Leveson, 2012)
Example System: Aviation

System-level Accident (Loss): ?

Image removed due to copyright restrictions.
Example System: Aviation

System-level Accident (Loss): Two aircraft collide
System-level Accident (Loss): Two aircraft collide
System-level Hazard: ?
Hazard

• Definition: A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss).

• Something we can **control**

• Examples:

<table>
<thead>
<tr>
<th>Accident</th>
<th>Hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Satellite becomes lost or unrecoverable</td>
<td>Satellite maneuvers out of orbit</td>
</tr>
<tr>
<td>People die from exposure to toxic chemicals</td>
<td>Toxic chemicals are released into the atmosphere</td>
</tr>
<tr>
<td>People die from radiation sickness</td>
<td>Nuclear power plant releases radioactive materials</td>
</tr>
<tr>
<td>People die from food poisoning</td>
<td>Food products containing pathogens are sold</td>
</tr>
</tbody>
</table>
System-level Accident (Loss): Two aircraft collide
System-level Hazard: Two aircraft violate minimum separation
Aviation Examples

• System-level Accident (loss)
  – Two aircraft collide
  – Aircraft crashes into terrain / ocean

• System-level Hazards
  – Two aircraft violate minimum separation
  – Aircraft enters unsafe atmospheric region
  – Aircraft enters uncontrolled state
  – Aircraft enters unsafe attitude
  – Aircraft enters prohibited area
Aviation Examples

• System-level Accident (loss)
  – A-1: Two aircraft collide
  – A-2: Aircraft crashes into terrain / ocean

• System-level Hazards
  – H-1: Two aircraft violate minimum separation
  – H-2: Aircraft enters unsafe atmospheric region
  – H-3: Aircraft enters uncontrolled state
  – H-4: Aircraft enters unsafe attitude
  – H-5: Aircraft enters prohibited area
STPA
(System-Theoretic Process Analysis)

• Identify accidents and hazards
• Draw the control structure
• Step 1: Identify unsafe control actions
• Step 2: Identify causal factors and create scenarios

(Leveson, 2012)
STPA application:
NextGen In-Trail Procedure (ITP)

Current State

- Pilots will have separation information
- Pilots decide when to request a passing maneuver
- Air Traffic Control approves/denies request

Proposed Change
STPA Analysis

• High-level (simple) Control Structure
  – Main components and controllers?
STPA Analysis

• High-level (simple) Control Structure
  – Who controls who?
STPA Analysis

• High-level (simple) Control Structure
  – What commands are sent?
• High-level (simple) Control Structure

STPA Analysis
STPA Analysis

• More complex control structure
Example High-level control structure

- Congress
  - Directives, funding
  - Reports
- FAA
  - Regulations, procedures
  - Reports
- ATC
  - Instructions
  - Acknowledgement, requests
- Pilots
  - Execute maneuvers
  - Aircraft status, position, etc
- Aircraft
STPA
(System-Theoretic Process Analysis)

• Identify accidents and hazards
• Draw the control structure
• Step 1: Identify unsafe control actions
• Step 2: Identify causal factors and create scenarios

(Leveson, 2012)
Identify Unsafe Control Actions

<table>
<thead>
<tr>
<th>Flight Crew Action (Role)</th>
<th>Not providing causes hazard</th>
<th>Providing Causes hazard</th>
<th>Incorrect Timing/Order</th>
<th>Stopped Too Soon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute Passing Maneuver</td>
<td>Pilots perform ITP when ITP criteria are not met or request has been refused [H-1]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Structure of a Hazardous Control Action

Four parts of a hazardous control action

– Source Controller: 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: conditions for the hazard to occur
  • (system or environmental state in which command is provided)

Example: “Pilots provide ITP maneuver when ITP criteria not met”
## Defining Safety Constraints

<table>
<thead>
<tr>
<th>Unsafe Control Action</th>
<th>Safety Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pilot performs ITP when ITP criteria are not met or request has been refused</td>
<td>Pilot must not perform ITP when criteria are not met or request has been refused</td>
</tr>
<tr>
<td>Pilot starts maneuver late after having re-verified ITP criteria</td>
<td>Pilot must start maneuver within X minutes of re-verifying ITP criteria</td>
</tr>
<tr>
<td>Etc.</td>
<td>Etc.</td>
</tr>
</tbody>
</table>
STPA
(System-Theoretic Process Analysis)

• Identify accidents and hazards
• Draw the control structure
• Step 1: Identify unsafe control actions
• Step 2: Identify causal factors and create scenarios

(Leveson, 2012)
STPA Step 2: Causal scenarios

UCA: Pilot executes maneuver when criteria are not met [H-1]

For information about citing these materials or our Terms of Use, visit: https://ocw.mit.edu/terms.