Integrating State Machine Analysis with STPA

Asim Abdulkhaleq, Ph.D. Student
Institute of Software Technology
University of Stuttgart, Germany

Joint work with:
Prof. Dr. Stefan Wagner

STAMP Workshop 2013
Cambridge, MIT, USA
28. March 2013
Problem Statement:

- There is no systematic way to let the safety analyst know how to evaluate each control action. Moreover, STPA does not represent system states, which have an effect on the safety of control action.

Research Objectives:

- Fill this gap and find ways for including and better analysing the dynamic behaviour of systems during STPA hazard analysis.
- We plan to investigate various modeling and analysis techniques.
Proposed Methodology

- Use STPA to identify the potential for inadequate scenarios.
- Use Finite State Machine (FSM) to model the dynamic behaviour of the system.
- Assess each control action with FSM based on all the possible system states.

Assess each control action based on system states.

Consider the system states and its effect on the control actions.

Proposed methodology aims to:

- Use STPA to identify the potential for inadequate scenarios.
- Use Finite State Machine (FSM) to model the dynamic behaviour of the system.
- Assess each control action with FSM based on all the possible system states.
Anti-Lock Braking System is a safety system on motor vehicles which prevents the wheels from locking while braking.

The ABS Architecture:

![ABS Architecture Diagram](http://www.pakwheels.com)
Unsafe Control Actions (UCAs)

Unsafe Control Action: Brake event applied but not received by ABS

Legend:
- Components in control Structure
- Commands or data flow

Diagram:
- Human Operator
  - Brake Pedal Command
  - ABS Warnings
- Controller
  - Rotational Speed of Wheels
- Other Inputs:
  - Deceleration Rate
  - Wheel Speed Sensors
- Sensors
  - Wheel Speed
- Actuator
  - Hydraulic Control Unit (HCU)
  - Pressure control
  - Valves
- Controlled Process
  - Vehicle
  - Friction
- Valves

Components in control Structure Commands or data flow

Unsafe Control Action: Brake event applied but not received by ABS
Unsafe Control Actions (UCAs)

Examples of potentially inadequate control actions of ABS system:

<table>
<thead>
<tr>
<th>Control Actions</th>
<th>Action required but not provided</th>
<th>Unsafe action provided</th>
<th>Incorrect Timing/Order</th>
<th>Stopped too soon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brake Pedal Command</td>
<td>Brake event applied but not received by ABS [H.1]</td>
<td>Brake event is too short</td>
<td>Brake event provided too late</td>
<td>Brake event stopped too soon</td>
</tr>
</tbody>
</table>

I must evaluate each row to determine whether it is a hazardous state, but how?

You can assess them based on timing information, but what about other factors such as the states of the system?
FSM Construction

In ABS example:

- ECU controller has four operating modes: Inactive, handleLock, applyBrakePedal and reducePressure.
- Valve component has three modes: open, block and release.
- HCU actutor has three modes: Inactive, stopPump and openPump.

How to evaluate the control action whether it leads to hazard or not by considering all potential combinations of relevant states?

FSM can be used to determine the system states that affect the safety of the control action.
FSM Construction of Controller (ECU)

Construct FSM for each controller and combine the relevant states for evaluating control actions.

Where: $S_0$ = inactive (brake not pressed),
$S_1$= handlelock,
$S_2$= applyBreakPedal,
$S_3$= pressureReduction,
$S_4$= MonitorDeceleration
and $WL$= WheelLocked.
The control action table for the brake pedal command based on the potential combination of system states.

<table>
<thead>
<tr>
<th>Control Actions</th>
<th>Wheel Status</th>
<th>Wheel Speed</th>
<th>Valve Status</th>
<th>Hazardous?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brake Pedal Command</td>
<td>Locked</td>
<td>slow</td>
<td>open</td>
<td>Yes</td>
</tr>
<tr>
<td>Brake Pedal Command</td>
<td>Locked</td>
<td>fast</td>
<td>open</td>
<td>Yes</td>
</tr>
<tr>
<td>Brake Pedal Command</td>
<td>Locked</td>
<td>slow</td>
<td>close</td>
<td>No</td>
</tr>
</tbody>
</table>

E.g. Unsafe Control Action:
If we consider *the brake pedal command* that can be a hazardous control action, it consists of the values of the following process model state variables:

- The brake pedal is pressed.
- Valve is open.
- Wheel is locked.
- The wheel speed exceeded a preset maximum level.

E.g. Refine Safety Constraints: When brake pedal is pressed, the status of wheel lock should be false, the status of valve should be closed and the wheel speed should not exceed a preset maximum level.
The End…

Thank You!

Safety analysis for complex system

- Human-oriented
- Components-oriented
- Software Interaction
- Environment-oriented