Using STPA and CAST to Design for Serviceability and Diagnostics

Hannah Slominski


Advisor: Nancy Leveson
“Why does it say paper jam, when there is no paper jam!?!?”
-- Samir Nagheenanajjar (Actor: Ajay Naidu), Office Space 1998
Motivation

Increased challenges meeting customer needs for equipment serviceability and support

• Increased product complexity
• Fast rate of technology change
• Technician shortages
• Increasing cost of machine unavailability
Motivation

Finally a method that accounts for emerging behavior and manages system complexity!

Curious about STPA applications beyond safety

- Security (Young & Leveson, 2013)
- Producibility (Ball, 2015)
- Quality (Goerges, 2013)
- Testing (Montes, 2016)
Purpose

Can STPA and CAST be used to improve product serviceability?

- Can it generate hardware and software serviceability requirements?
- Can it generate recommendations for the product development?
- Are any analysis modifications are required?

Can safety-STPA control structure be reused for serviceability?
Approach

CAST Case Study

• Existing diagnostic issue
• Analyzed full hierarchical control structure

STPA Case Study

• Future system early in conceptual phase, software-intensive
• Safety analysis, then serviceability analysis
Case Study 1: CAST Results

3 Physical Process Recommendations
6 Physical Process Control Recommendations

9 Product Support Recommendations
7 Product Design Recommendations
5 Product Test Recommendations
10 Management Recommendations
4 Key Systemic Factors

Key Insight –
Addressing the physical process and control is the tip of the iceberg
Case Study 2: STPA Results

Analyzing just two UCA’s generated:

16 Software, hardware and technical information requirements
10 Development process recommendations

Key Takeaway – STPA successfully generated serviceability requirements for a complex system in the conceptual design phase
## Terminology

<table>
<thead>
<tr>
<th>STAMP Term</th>
<th>STAMP Definition</th>
<th>Proposed Service STAMP Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss</td>
<td>A loss involves something of value to stakeholders. Losses may include any loss that is unacceptable to the stakeholders. (Leveson, 2011)</td>
<td>Loss</td>
</tr>
<tr>
<td>Accident</td>
<td>An accident is an unplanned and undesired loss event. (Leveson, 2011)</td>
<td>Loss Event</td>
</tr>
<tr>
<td>Hazard</td>
<td>A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss. (Leveson &amp; Thomas, 2018)</td>
<td>Hazard</td>
</tr>
<tr>
<td>Unsafe Control Action</td>
<td>An Unsafe Control Action (UCA) is a control action that, in a particular context and worst-case environment, will lead to a hazard. (Leveson &amp; Thomas, 2018)</td>
<td>Unserviceable Control Action</td>
</tr>
</tbody>
</table>
Losses

Unplanned downtime due to inadequate serviceability (L-1)
Financial losses incurred through warranty costs (L-2)
Customer dissatisfied (L-3)

Key Takeaway – Leverage broad definition of a loss

*A loss involves something of value to stakeholders. Losses may include any loss that is unacceptable to the stakeholders.* (Leveson, 2011)

Massachusetts Institute of Technology
Hazard Examples

Operator takes the wrong action to mitigate the problem or ignores a service alarm  (L-1, L-3)

Service technician does the wrong repair  (L-1, L-2, L-3)

Machine falsely indicates a problem  (L-1, L-2, L-3)

Repair & troubleshooting time exceeds <X> minutes  (L-1, L-2, L-3)
Key Takeaway – Service tasks are the controls
**Table 3: Service Responsibilities - Physical Process Control System (PCU)**

<table>
<thead>
<tr>
<th>General Responsibilities</th>
<th>Specific</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor conditions</td>
<td></td>
</tr>
<tr>
<td>Detect and decide when problems exist that require service action</td>
<td>X</td>
</tr>
<tr>
<td>Protect the machine from damage when problems are detected</td>
<td>X</td>
</tr>
<tr>
<td>Isolate problems and determine the repair required</td>
<td>X</td>
</tr>
<tr>
<td>Alarm the operator and technician to problems and communicate control action needed</td>
<td>X</td>
</tr>
<tr>
<td>Provide automatic troubleshooting aids: display relevant values, provide diagnostic tests and calibrations</td>
<td>X</td>
</tr>
<tr>
<td>Detect and decide when problems are fixed</td>
<td></td>
</tr>
</tbody>
</table>

**Table 4: Service Responsibilities – Operator (OP)**

<table>
<thead>
<tr>
<th>General Responsibilities</th>
<th>Specific</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operate the equipment in a way that does not lead to machine damage</td>
<td></td>
</tr>
<tr>
<td>Monitor equipment condition and alarms</td>
<td></td>
</tr>
<tr>
<td>Maintain the equipment: Applicable to loss event listed below</td>
<td></td>
</tr>
<tr>
<td>Check and maintain hydraulic oil level</td>
<td>X</td>
</tr>
<tr>
<td>Change oil filter (when restricted or per regular interval?)</td>
<td></td>
</tr>
<tr>
<td>Respond to problems that occur</td>
<td></td>
</tr>
<tr>
<td>Follow DTC and operator manual instructions</td>
<td>X</td>
</tr>
<tr>
<td>Request service support</td>
<td></td>
</tr>
<tr>
<td>Communicate observed symptoms to service technician</td>
<td></td>
</tr>
</tbody>
</table>

**Key Takeaway** – Generated reusable general responsibilities and specific to the loss event. Reused in STPA case study
### Table 12: Service Responsibilities - Operator (OP)

<table>
<thead>
<tr>
<th>ID</th>
<th>Responsibilities</th>
<th>Feedback Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>OP.R.1</td>
<td>Operate the equipment in a way that does not lead to machine damage or machine</td>
<td>TI DTC alarms, other system DTC alarms, TI disabled status, machine operating</td>
</tr>
<tr>
<td></td>
<td>unavailability</td>
<td>conditions, visual monitoring</td>
</tr>
<tr>
<td>OP.R.1.1</td>
<td>Manually control the function because TI is disabled</td>
<td>TI disabled status (if not observable without an indicator, machine must provide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>active feedback), visual monitoring</td>
</tr>
<tr>
<td>OP.R.2</td>
<td>Maintain the equipment</td>
<td>Maintenance required indicator</td>
</tr>
<tr>
<td>OP.R.2.1</td>
<td>Clean TI sensors</td>
<td>Sensor dirty status (if not observable from the operator seat), visual inspection</td>
</tr>
</tbody>
</table>

**Key Takeaway** – Some design requirements become apparent even before generating UCAs.
UCA Examples

**PCU Control Action:** Provide “replace component” code

- **UCA:** Physical process control unit (PCU) provides “replace component” code when component does not need replacement (H-1, H-2)

**Technician Control Action:** Replace component

- **UCA:** Service technician replaces component when it does not need replacement (H-2, H-6)
Conclusions

Successfully demonstrated STAMP applied to serviceability
- Same STPA and CAST steps
- Leverage broad definition of a loss
- Incremental process guides a service-friendly design

Generated hardware, software, and service instructions requirements simultaneously
Safety and Serviceability Alignment

STAMP elements:

– Reuse higher levels of control structure
– Different lower levels of control structure
– Different hazards and UCAs

Design considerations:

– Operator’s responsibility to monitor alarms
Other Insights

Reliability ≠ Safety

Reliability ≠ Machine Availability
Other Insights

Use service information to drive desired human behavior vs. identify a “root cause”
Better options:

1. Provide information that drives desired operator behavior (example: restart)

2. Don’t have an active alarm
References


