Using STPA trend analysis to determine key system drivers

Katherine Belvin
Product Review Engineer
March 27, 2017
Introduction

• Aircraft production is complex and can be hazardous

• Hazardous energy managed via Lockout-Tagout (LOTO)
  • Group Coordinator
  • Primary Authorized Employee
  • Authorized Employee

• Why do LOTO-related incidents and injuries occur?

• STPA method applied to LOTO

• Goal: Implement the most effective solutions
STPA for Hazardous Energy Control

Manager / Team Lead

Group Coordinator

Next Shift/Stall GC

Hazardous Energy Focal

Primary Authorized Employee

Next Shift/Stall Primary Authorized Employee

Authorized Employee

Next Shift/Stall Authorized Employee

Logbook

Qualified Person

Lockout devices & tags

Aircraft circuit, system, or component

Affected Employee

Copyright © 2017 Boeing. All rights reserved per conditions on title page.
Hazardous Energy Focal

Group Coordinator

Primary Authorized Employee

Authorized Employee

Lockout devices & tags

Aircraft circuit, system, or component

Logbook

Affected Employee

STPA for Hazardous Energy Control
STPA Example

Controller & Control Action

- Primary Authorized Employee
- Aircraft circuit, system, or component
- Perform Tryout

Unsafe Control Actions

Performing Tryout is Made Unsafe By:
- Performing Tryout on the wrong component
- Performing Tryout procedure incorrectly
- Performing the wrong Tryout procedure
- Not performing Tryout
- Performing Tryout too late
- Performing Tryout too soon (before energy is released)

Causal Scenarios

Wrong Tryout Procedure Used Because:
- Employee doesn’t know it’s the wrong procedure
- Employee could not find the right procedure
- Employee was rushed and did not want to find the right procedure
- Higher authority employee suggested the procedure
- Etc....
STPA Limitations

- Analysis results in too much data for easy comprehension
- Controllers: 13
- Control actions: 48
- Unsafe control actions: 200
- Causal scenarios that could result in incidents or injury: 958

Challenges

- How to put all of this data into context of the “bigger picture”?  
- How to translate that knowledge into business decisions?
Applying Trend Grouping

Three categories of system drivers:

- Mental models
- Inadequate information or resources
- Process deficiency

Which of these causes the greatest systemic impact?
How are they related?
How to prioritize and estimate improvement?
## Category Drivers by Group

<table>
<thead>
<tr>
<th>Mental Models</th>
<th>Resources / Information</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reacting to time pressure</td>
<td>Required people cannot be located</td>
<td>Inadequate training / experience</td>
</tr>
<tr>
<td>Believed to be inconsequential</td>
<td>Production complexity</td>
<td>Unclear role assignments</td>
</tr>
<tr>
<td>Belief that another employee did / will perform task</td>
<td>Unavailable information</td>
<td>Unclear requirements</td>
</tr>
<tr>
<td>Attention was diverted</td>
<td>Required resources cannot be located</td>
<td>Process unenforced</td>
</tr>
<tr>
<td>Situational misperception</td>
<td>Device failure</td>
<td>Unclear authority</td>
</tr>
</tbody>
</table>

Copyright © 2017 Boeing. All rights reserved per conditions on title page.
Trend Grouping Example

• Controller: Primary Authorized Employee (PAE)
  • **Unsafe Control Action**: Performs incorrect Tryout procedure because...
  • **Causal Scenario**: ... PAE was given an incorrect procedure, does not know where to find procedures and believes that taking the time to find a correct one would result in unacceptable production delay.

• Trend Grouping: Assigning Key Drivers
  • **Causal Action**: Incorrect Tryout
  • **Mental Model**: Reacting to Time Pressure
  • **Resource / Information Deficiency**: Required resources cannot be located
  • (no process driver)
Results
Actions Breakdown

Quantity Causal Actions: 958
Top Processes by Action

Quantity Process: 295

- Data Entry
- Configuration / Deconflicting
- Logbook Process
- Task / Role Assignment
- Check In / Access Error
- Incorrect HECP

Legend:
- Inexperience / Training
- Unclear Requirements
- Unclear Role Assignments

Copyright © 2017 Boeing. All rights reserved per conditions on title page.
TOP DRIVER CORRELATIONS

- Unclear Role Assignments (27%)
- Incorrect HECP (7%)
- Time Pressure (26%)
- Configuration / Deconflicting (13%)
- Inexperience / Training (37%)
- Production Complexity (28%)
- Task / Role Assignment (10%)
- Check In / Access (8%)
- Unclear Requirements (24%)
- Unclear Role Assignments (27%)
- Someone Else Did It (12%)
- LOTO Removal (<1%)
- Did Not Communicate (6%)
- Forgot (15%)
- Configuration / Deconflicting (13%)
- Data Entry (17%)
- Unavailable Information (34%)
- Inexperience / Training (37%)
- Time Pressure (26%)
- Unavailable People (23%)
- Logbook Process (12%)

Actions
- Mental Model
- Process

Resources & Information

Quantity common scenarios
- 8 – 11
- 12 – 15
- 17 - 21

Copyright © 2017 Boeing. All rights reserved per conditions on title page.
How STPA Results Translate to Business Priorities

Main Message: Focus on Areas with Greatest Systemic Impact

Highest Priority Actions

- Focus on Reduction in Data Entry
  - Correlated with over half each of Mental Model and Resource & Information drivers
- Improve Accessibility to Information
  - Strong relationship with Configuration / Deconflicting errors
- Simplify Administrative Tasks
  - A third of causal actions are correlated with Time Pressure driver

Lowest Priority Actions

- Revamp LOTO process: Smallest group of assigned drivers
- Heavier emphasis on “compliance”
Summary

• STPA provides detailed insight to incident and injury causality mechanisms
• Large quantities of data are generated
• Cut through complexity with trend grouping
• Enables prioritization of improvements based on estimated impact