System Theoretic Process Analysis Application (STPA) in a Service Safety Environment

BAE Systems Hawk T-165
Aircrew Training Device Specifications

Nawaf Al-Malik
Senior Safety Engineer
Directorate of Safety
BAE Systems Saudi Arabia
Introduction

My main role?

What does BAE Systems Saudi Arabia do?

Our agenda will cover the following topics:
• BAE Systems Saudi Arabia Hazard Management
• How can STPA be applied to BAE Systems Saudi Arabia Hazard Management?
• STPA in practice
• Conclusion
• Question
BAE Systems Saudi Arabia Hazard Management - 1

- BAE Systems Saudi Arabia Management of hazards in a Service Safety Environment

---

Class A - Death or irreversible environmental damage or recovery >100 years

Class B - Major injury, major occupational illness, and/or major environmental damage recovery >10 to < 100 years

Class C - Minor injury, minor occupational illness, and/or minor environmental damage recovery >1 to < 10 years

Class D - Less than minor injury, less than minor occupational illness, and/or less than minor environmental damage recovery <1 year

---

Hazard H/1 to 9 (as applicable)

Cause Zxx

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Control

Con
# BAE Systems Saudi Arabia Hazard Management - 2

All operational hazards will be part of those top level hazards.

<table>
<thead>
<tr>
<th>Hazard ID</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>Enterprise Safety, Governance &amp; Assurance</td>
</tr>
<tr>
<td>H2</td>
<td>Inappropriate Application of Legislation, Regulation &amp; Standards</td>
</tr>
<tr>
<td>H3</td>
<td>Unsuitable Condition/Standard of Components</td>
</tr>
<tr>
<td>H4</td>
<td>Integrity of Technical Data</td>
</tr>
<tr>
<td>H5</td>
<td>Configuration Control – Approved Data</td>
</tr>
<tr>
<td>H6</td>
<td>Configuration Control – Equipment</td>
</tr>
<tr>
<td>H7</td>
<td>Use of Approved Material, Components or Data</td>
</tr>
<tr>
<td>H8</td>
<td>Competence &amp; Training</td>
</tr>
<tr>
<td>H9</td>
<td>Operational Working Environment</td>
</tr>
</tbody>
</table>
Using this typical Hazard Risk Matrix

<table>
<thead>
<tr>
<th>Probability</th>
<th>Catastrophic</th>
<th>Critical</th>
<th>Marginal</th>
<th>Negligible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>B</td>
</tr>
<tr>
<td>Probable</td>
<td>A</td>
<td>A</td>
<td>B</td>
<td>C</td>
</tr>
<tr>
<td>Occasional</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Remote</td>
<td>B</td>
<td>C</td>
<td>C</td>
<td>D</td>
</tr>
<tr>
<td>Improbable</td>
<td>C</td>
<td>C</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>Incredible</td>
<td>C</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>
STPA adopted in a Service Environment - 1

Hazard H/1 to 9 (as applicable)

Class A - Death or irreversible environmental damage or recovery >100 years
Class B - Major injury, major occupational illness, and/or major environmental damage recovery >10 to < 100 years
Class C - Minor injury, minor occupational illness, and/or minor environmental damage recovery >1 to < 10 years
Class D - Less than minor injury, less than minor occupational illness, and/or less than minor environmental damage recovery <1 year

Control

Cause Zxx

Control CXX & Control Owner

REM

Imp
STPA adopted in a Service Environment - 2
Applying STPA on a live project

STPA application on a Hawk T-165 Flight Simulator on a Main Operating Base in the Kingdom of Saudi Arabia
See next slide for a 3D view perspective of the Dome.
Process Sequence - 2

Activity 6 – Go to stairs

Activity 4 – Go inside Dome

Activity 5 – Straps

Activity 3 – Climb the stairs
Process Sequence -3

See next slide for a 3D view perspective of the Dome
Process Sequence - 4

Activity 11 - climb the stairs

Activity 12 - Go to inside dome

Activity 13 - Strap off

Activity 14 - Go to stairs
Process Sequence - 5

Activity 15 - Go down using stairs
Activity 16 – Get out using exit door

1 Instructor 2 student
## System Interfaces

<table>
<thead>
<tr>
<th>System Interfaces (From/To)</th>
<th>Instructor Operating System</th>
<th>Stairs start point</th>
<th>Stairs end point</th>
<th>Inside Dome</th>
<th>Strap</th>
<th>Communication Channels/tools</th>
<th>Safe Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instructor Operating System</td>
<td>NA</td>
<td>Activity 2/10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Activity 9</td>
<td>0</td>
</tr>
<tr>
<td>Stairs start point</td>
<td>Activity 8</td>
<td>NA</td>
<td>Activity 3/11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Activity 16</td>
</tr>
<tr>
<td>Stairs end point</td>
<td>0</td>
<td>Activity 7/15</td>
<td>NA</td>
<td>Activity 4/12</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Inside Dome</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>NA</td>
<td>Activity 5/13</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Strap</td>
<td>0</td>
<td>0</td>
<td>Activity 6/14</td>
<td>0</td>
<td>NA</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Communication Channels/tools</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>NA</td>
<td>0</td>
</tr>
<tr>
<td>Safe Zone</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>NA</td>
<td>0</td>
</tr>
</tbody>
</table>

Approved for Public Release
Process Model
### Analysis

<table>
<thead>
<tr>
<th>From Activity</th>
<th>Activity</th>
<th>To Activity No</th>
<th>Associated hazard</th>
<th>Control</th>
<th>Activity Behavior Categories</th>
<th>Causes</th>
<th>Pre HRI</th>
<th>Class Risk</th>
<th>Post HRI</th>
<th>Class Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOS Movement</td>
<td>Start point 2</td>
<td>2</td>
<td>NA</td>
<td>NA</td>
<td>Provided</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>IOS Movement</td>
<td>Start point 2</td>
<td>2</td>
<td>Not provided</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>IOS Movement</td>
<td>Start point 2</td>
<td>2</td>
<td>Provided Too soon</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>IOS Movement</td>
<td>Start point 2</td>
<td>2</td>
<td>Provided Too late</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>IOS Movement</td>
<td>Start point 2</td>
<td>2</td>
<td>stopped Too soon</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Start point Movement</td>
<td>End point 3</td>
<td>H1/ H2/ H9</td>
<td>C1 - Risk Assessments</td>
<td>Provided</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Start point Movement</td>
<td>End point 3</td>
<td>H1/ H2/ H9</td>
<td>C1 - Risk Assessments</td>
<td>Not provided</td>
<td>Lack of proper working environment</td>
<td>Frequent/ Catastrophic</td>
<td>A</td>
<td>Improbable / Catastrophic</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Start point Movement</td>
<td>End point 3</td>
<td>H1/ H2/ H9</td>
<td>C1 - Risk Assessments</td>
<td>Provided Too soon</td>
<td>Improper holistic view assessment</td>
<td>Improbable/ Catastrophic</td>
<td>C</td>
<td>Incredible/Catastrophic</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Start point Movement</td>
<td>End point 3</td>
<td>H1/ H2/ H9</td>
<td>C1 - Risk Assessments</td>
<td>Provided Too late</td>
<td>Lack of proper configuration</td>
<td>Improbable/ Marginal</td>
<td>D</td>
<td>Incredible/ Marginal</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>Start point Movement</td>
<td>End point 3</td>
<td>H1/ H2/ H9</td>
<td>C1 - Risk Assessments</td>
<td>stopped Too soon</td>
<td>Lack of proper working environment</td>
<td>Probable/ Catastrophic</td>
<td>A</td>
<td>Improbable / Catastrophic</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>End point Movement</td>
<td>Inside Dome 4</td>
<td>H1/ H2/ H9</td>
<td>See C1</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Inside Dome Movement</td>
<td>Strap 5</td>
<td>H1/ H2/ H7/ H8</td>
<td>C2 - Proper Strapping Training along with post and pre checks</td>
<td>Provided</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Inside Dome Movement</td>
<td>Strap 5</td>
<td>H1/ H2/ H7/ H8</td>
<td>Student falling while operation</td>
<td>Not provided</td>
<td>Frequent/ Catastrophic</td>
<td>A</td>
<td>Improbable/ Catastrophic</td>
<td>C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Analysis – Example

<table>
<thead>
<tr>
<th>From</th>
<th>Activity</th>
<th>To</th>
<th>Activity No</th>
<th>Associated hazard</th>
<th>Control</th>
<th>Activity Behavior Categories</th>
<th>Causes</th>
<th>Pre HRI</th>
<th>Class Risk</th>
<th>Post HRI</th>
<th>Class Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start point</td>
<td>Movement</td>
<td>End point</td>
<td>3</td>
<td>H1/ H2/ H9</td>
<td>C1 - Risk Assessments</td>
<td>Not provided</td>
<td>Lack of proper working environment</td>
<td>Frequent/ Catastrophic</td>
<td>A</td>
<td>Improbable / Catastrophic</td>
<td>C</td>
</tr>
</tbody>
</table>

Microsoft Excel Worksheet
Analysis - Summary

- Systems Examined: 75
- Safety risks Identified: 64
- Safety Control issues Identified: 51
<table>
<thead>
<tr>
<th>From Activity</th>
<th>To Activity</th>
<th>Activity No</th>
<th>Associated hazard</th>
<th>Control</th>
<th>Activity Behavior Categories</th>
<th>Causes</th>
<th>Pre HRI Class Risk</th>
<th>Post HRI Class Risk</th>
<th>Management Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start point Movement</td>
<td>End point 3 H2/ H2/ H9</td>
<td>C1 - Risk Assessments</td>
<td>Not provided</td>
<td>Lack of proper working environment</td>
<td>Frequent/ Catastrophic</td>
<td>A</td>
<td>Improbable / Catastrophic</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Start point Movement</td>
<td>End point 3 H2/ H2/ H9</td>
<td>C1 - Risk Assessments</td>
<td>Provided Too soon</td>
<td>Improper holistic view assessment</td>
<td>Improbable/ Catastrophic</td>
<td>C</td>
<td>Incredible/ Catastrophic</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Start point Movement</td>
<td>End point 3 H2/ H2/ H9</td>
<td>C1 - Risk Assessments</td>
<td>Provided Too late</td>
<td>Lack of proper configuration</td>
<td>Improbable/ Marginal</td>
<td>D</td>
<td>Incredible/ Marginal</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>Start point Movement</td>
<td>End point 3 H2/ H2/ H9</td>
<td>C1 - Risk Assessments</td>
<td>stopped Too soon</td>
<td>Lack of proper working environment</td>
<td>Probable/ Catastrophic</td>
<td>A</td>
<td>Improbable / Catastrophic</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Inside Dome Movement and Strapping</td>
<td>Strap 5 H2/ H2/ H7/ H8</td>
<td>C2 - Proper Strapping Training along with post and pre checks</td>
<td>Not provided</td>
<td>Student falling while operation</td>
<td>Frequent / Catastrophic</td>
<td>A</td>
<td>Improbable/ Catastrophic</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Inside Dome Movement and Strapping</td>
<td>Strap 5 H2/ H2/ H7/ H8</td>
<td>C2 - Proper Strapping Training along with post and pre checks</td>
<td>Provided Too soon</td>
<td>Student falling while operation</td>
<td>Remote/ Catastrophic</td>
<td>B</td>
<td>Improbable/ Catastrophic</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Inside Dome Movement and Strapping</td>
<td>Strap 5 H2/ H2/ H7/ H8</td>
<td>C2 - Proper Strapping Training along with post and pre checks</td>
<td>Provided Too late</td>
<td>Student falling while operation</td>
<td>Remote/ Catastrophic</td>
<td>B</td>
<td>Improbable/ Catastrophic</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Inside Dome Movement and Strapping</td>
<td>Strap 5 H2/ H2/ H7/ H8</td>
<td>C2 - Proper Strapping Training along with post and pre checks</td>
<td>stopped Too soon</td>
<td>Student falling while operation</td>
<td>Frequent / Catastrophic</td>
<td>A</td>
<td>Improbable/ Catastrophic</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>IOS Movement and establish communication</td>
<td>Communication 9 H3/H7/H9</td>
<td>C3 - Calibration and regular checks and assurance to adherence to instruction manuals</td>
<td>Not provided</td>
<td>Lack of proper communication toolsets functionality</td>
<td>Probable/ Marginal</td>
<td>B</td>
<td>Incredible/ Marginal</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>IOS Movement and establish communication</td>
<td>Communication 9 H3/H7/H9</td>
<td>C3 - Calibration and regular checks and assurance to adherence to instruction manuals</td>
<td>Provided Too soon</td>
<td>Lack of proper communication toolsets functionality</td>
<td>Remote/ Marginal</td>
<td>C</td>
<td>Incredible/ Marginal</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>IOS Movement and establish communication</td>
<td>Communication 9 H3/H7/H9</td>
<td>C3 - Calibration and regular checks and assurance to adherence to instruction manuals</td>
<td>Provided Too late</td>
<td>Lack of proper communication toolsets functionality</td>
<td>Remote/ Marginal</td>
<td>C</td>
<td>Incredible/ Marginal</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>IOS Movement and establish communication</td>
<td>Communication 9 H3/H7/H9</td>
<td>C3 - Calibration and regular checks and assurance to adherence to instruction manuals</td>
<td>stopped Too soon</td>
<td>Lack of proper communication toolsets functionality</td>
<td>Probable/ Marginal</td>
<td>B</td>
<td>Incredible/ Marginal</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>IOS Movement Start point</td>
<td>Start point 10 H2/H2/H3/H9</td>
<td>C4 - Emergency Response Planning</td>
<td>Not provided</td>
<td>Not aware of fire event</td>
<td>Frequent/ Catastrophic</td>
<td>A</td>
<td>Improbable/ Catastrophic</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>IOS Movement Start point</td>
<td>Start point 10 H2/H2/H3/H9</td>
<td>C4 - Emergency Response Planning</td>
<td>Provided Too late</td>
<td>Not able to exit to Assembly Point</td>
<td>Frequent/ Catastrophic</td>
<td>A</td>
<td>Improbable/ Catastrophic</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>IOS Movement Start point</td>
<td>Start point 10 H2/H2/H3/H9</td>
<td>C4 - Emergency Response Planning</td>
<td>stopped Too soon</td>
<td>Not able to exit to Assembly Point</td>
<td>Occasional/ Catastrophic</td>
<td>A</td>
<td>Improbable/ Catastrophic</td>
<td>C</td>
<td></td>
</tr>
</tbody>
</table>
Filtered Analysis - Summary

- Safety risks Identified: 64
- Safety Control issues Identified: 51
- Safety Control issues Reduced: 37
Conclusion

Through doing this exercise with a very small scaled project, my comments are as listed below.

1. Takes long time to do.
2. Needs an Engineering Systems Thinking Approach
3. I would recommend it to be in conjunction with another Hazard Identification tool. Not in isolate.
4. It should be implemented at the initiation design phase.
5. It identifies secondary safety risks – control behaviors.
6. Can be understood by non-safety experts.
7. Doesn’t require extensive training.

It is to be noted that BAE Systems Saudi Arabia Safety Training is assessing the usage and adoption of STPA perceiving recommendations provided.
Questions

- Thank you
- Any Questions