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?

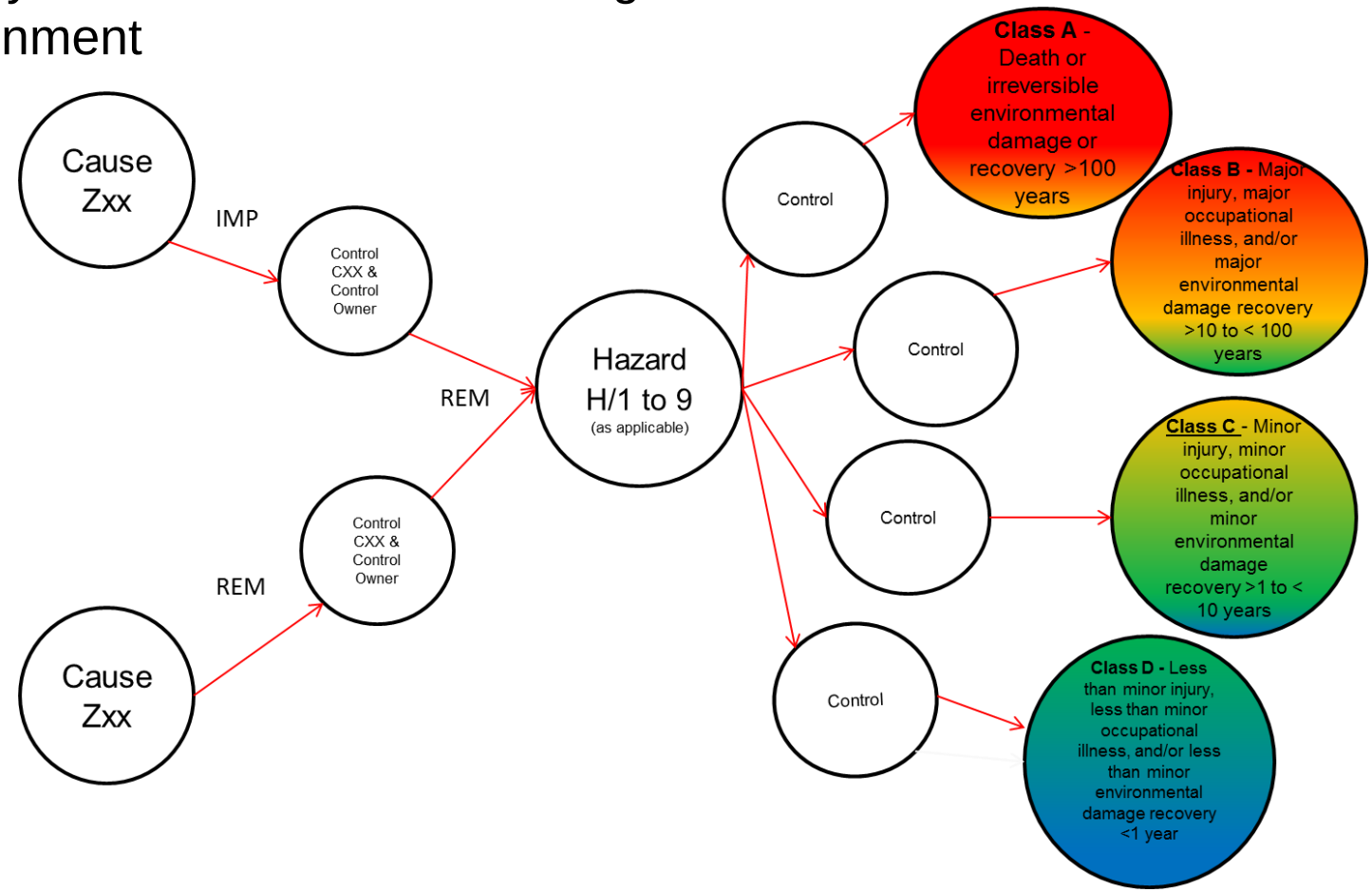
What does BAE Systems Saudi Arabia do?

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



BAE Systems Saudi Arabia Hazard Management - 2

All operational hazards will be part of those top level hazards

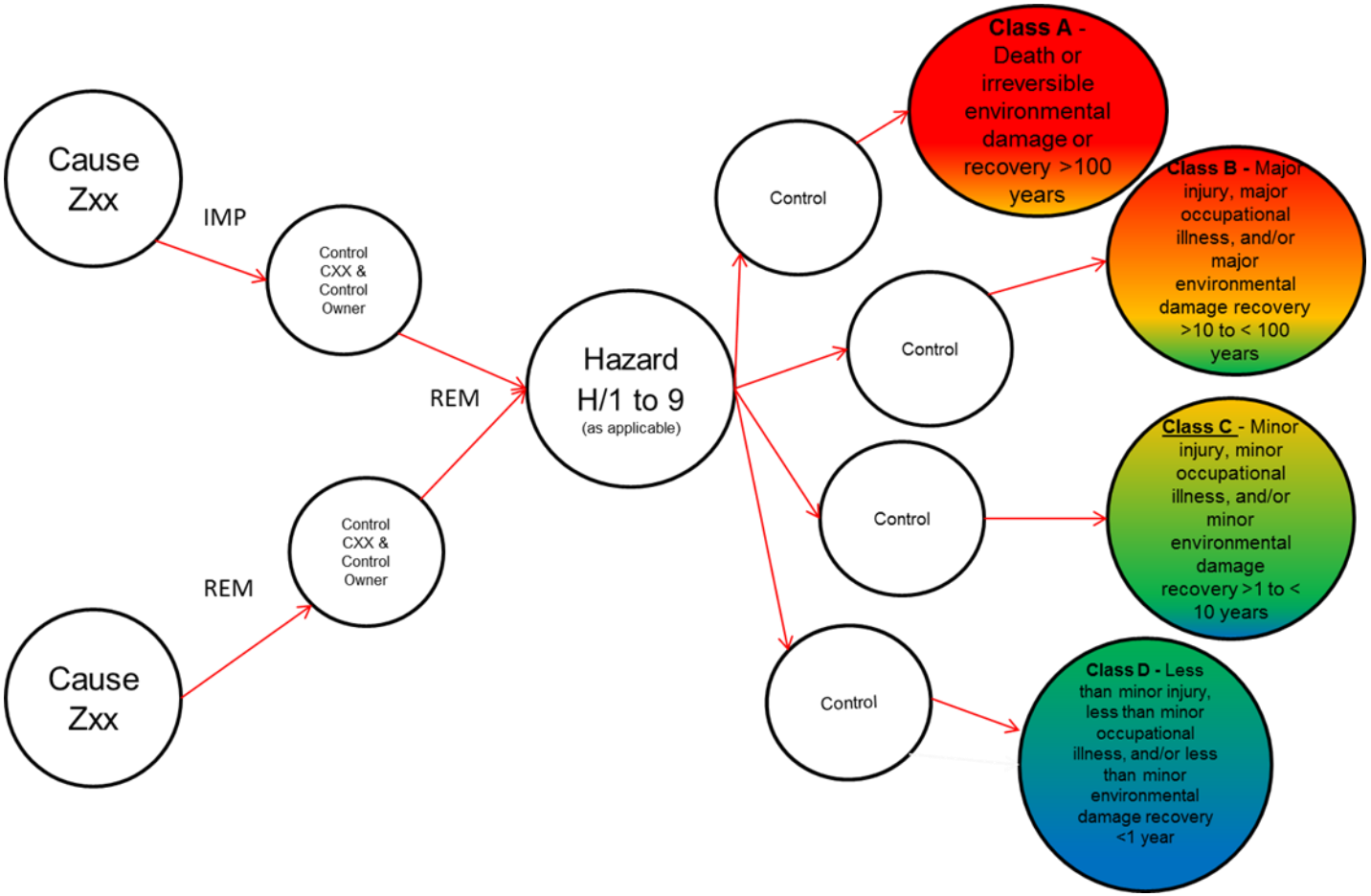
Hazard ID	Title
H1	Enterprise Safety, Governance & Assurance
H2	Inappropriate Application of Legislation, Regulation & Standards
H3	Unsuitable Condition/Standard of Components
H4	Integrity of Technical Data
H5	Configuration Control – Approved Data
H6	Configuration Control –Equipment
H7	Use of Approved Material, Components or Data
H8	Competence & Training
H9	Operational Working Environment

BAE Systems Saudi Arabia Hazard Management - 3

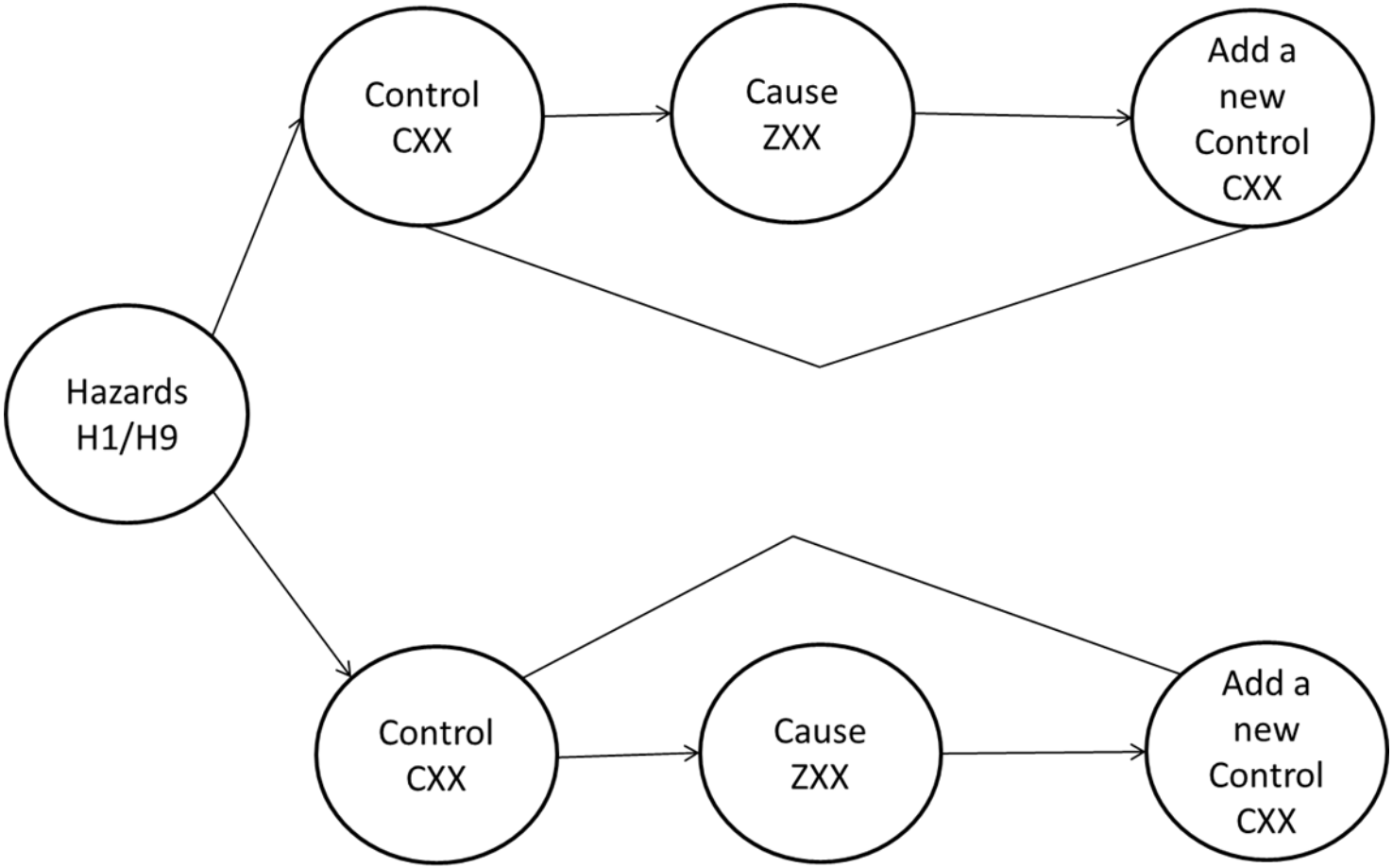
Using this typical Hazard
Risk Matrix

	Severity			
Probability	**Catastrophic**	**Critical**	**Marginal**	**Negligible**
Frequent	**A**	**A**	**A**	**B**
Probable	**A**	**A**	**B**	**C**
Occasional	**A**	**B**	**C**	**C**
Remote	**B**	**C**	**C**	**D**
Improbable	**C**	**C**	**D**	**D**
Incredible	**C**	**D**	**D**	**D**

STPA adopted in a Service Environment - 1

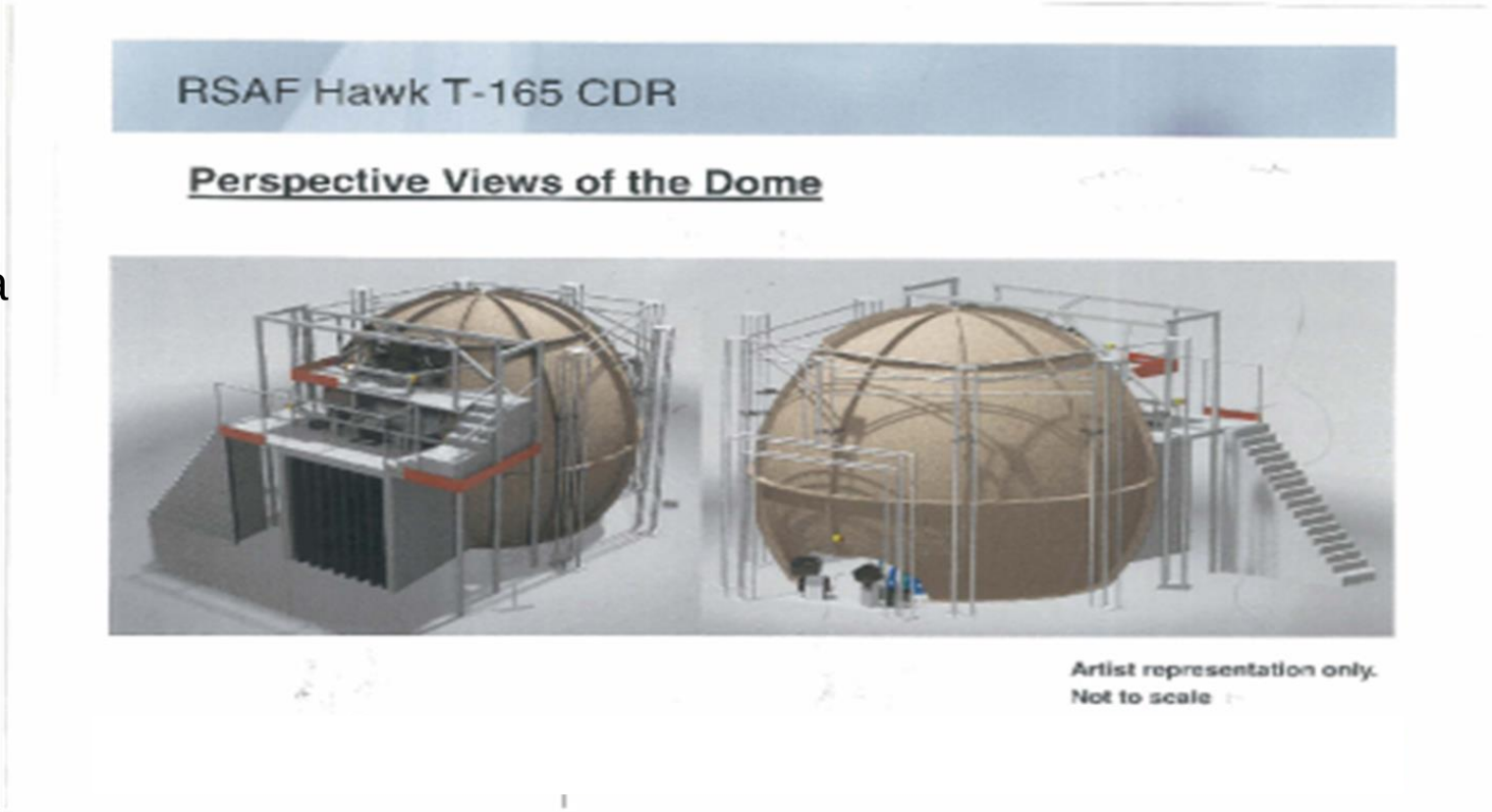


STPA adopted in a Service Environment - 2

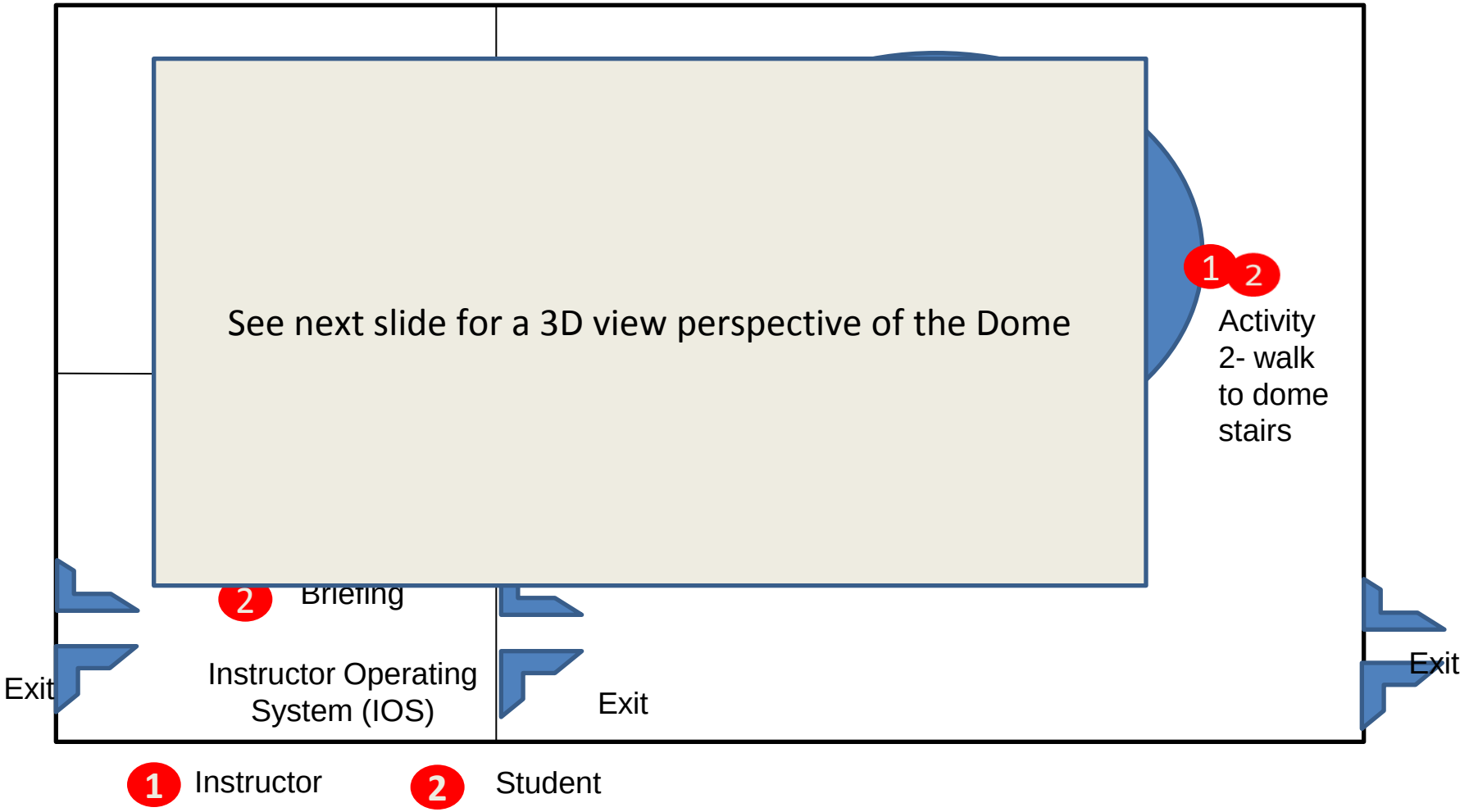


Applying STPA on a live project

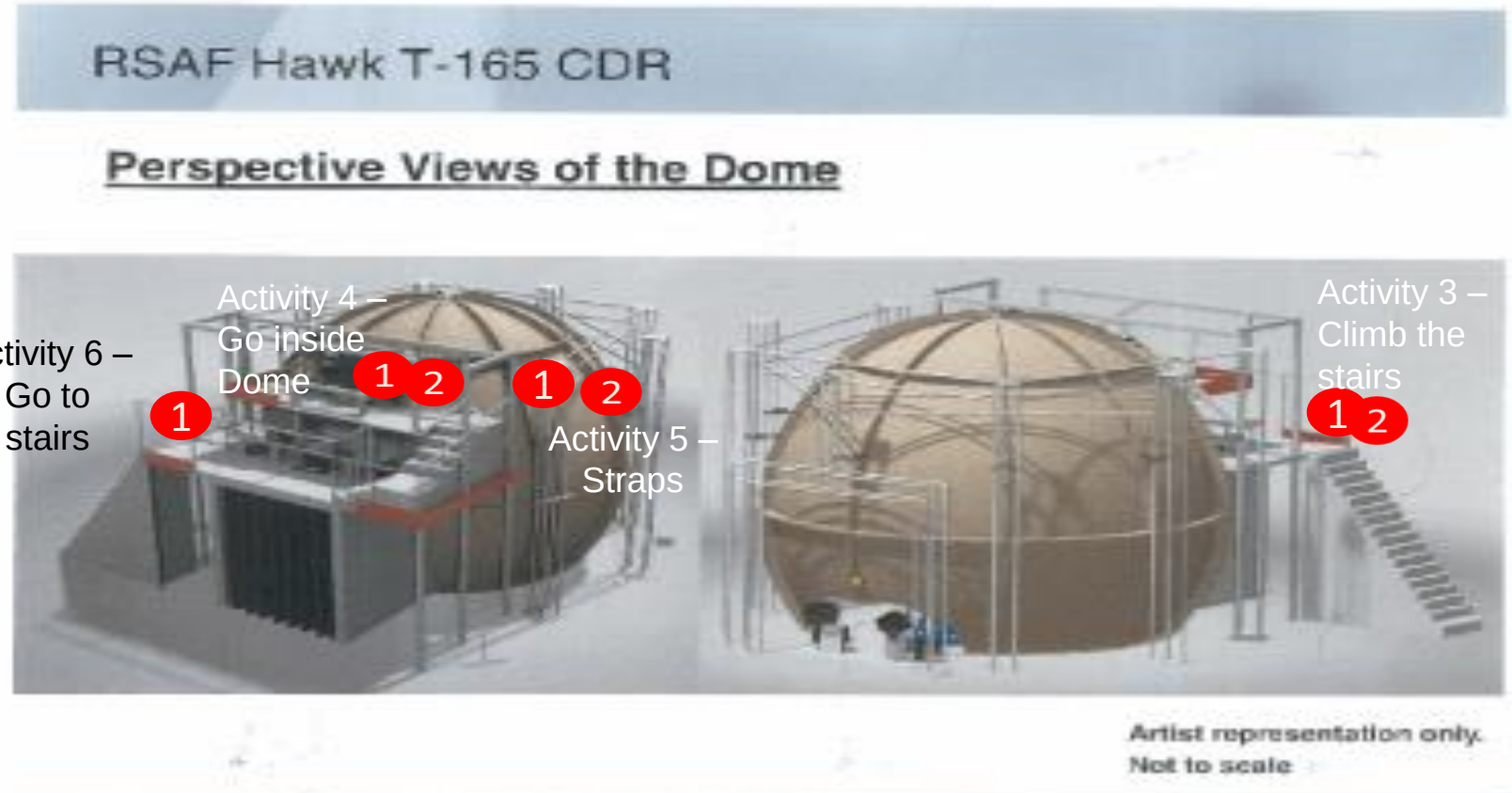
STPA application on a Hawk T-165 Flight Simulator on a Main Operating Base in the Kingdom of Saudi Arabia



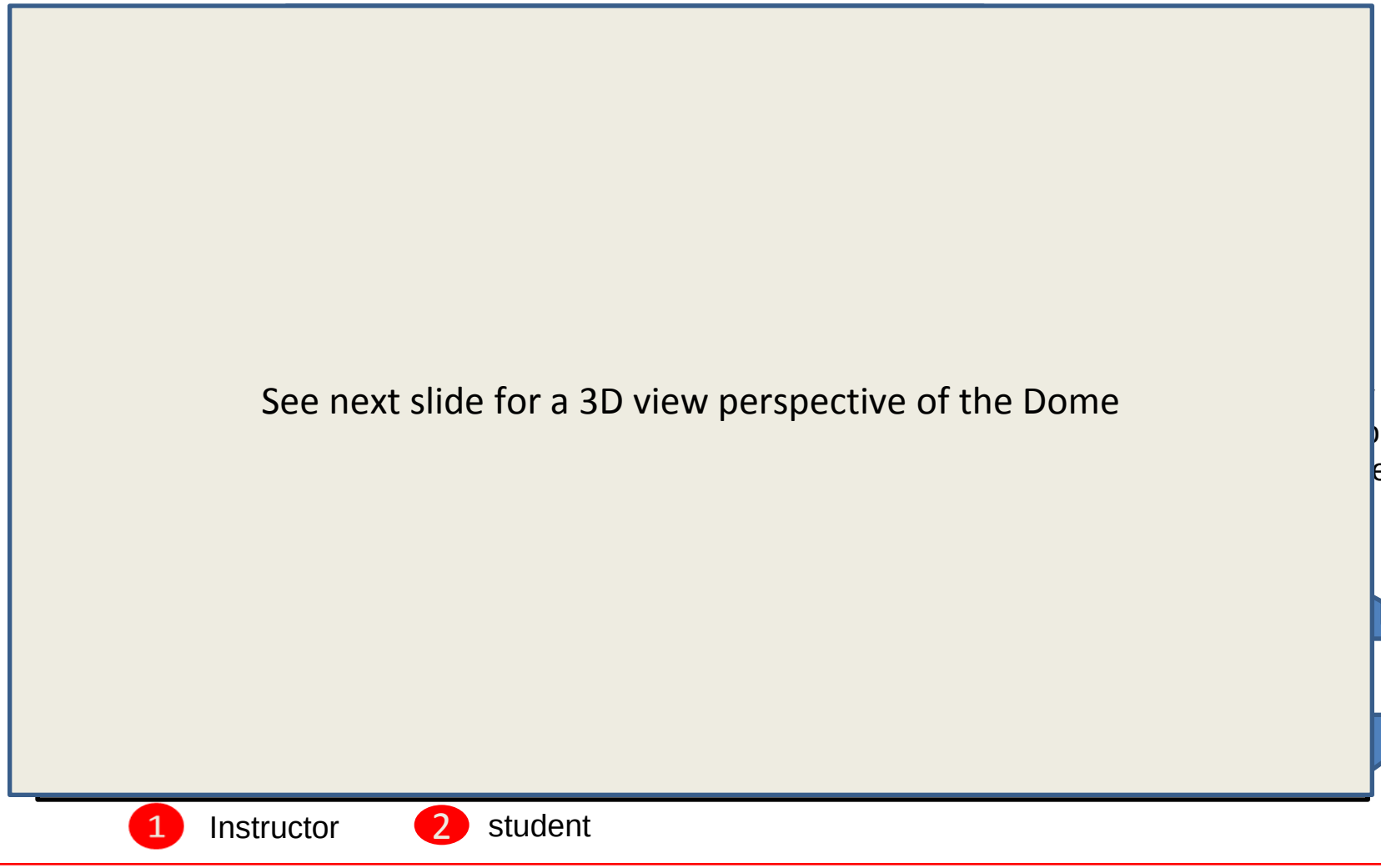
Process Sequence -1



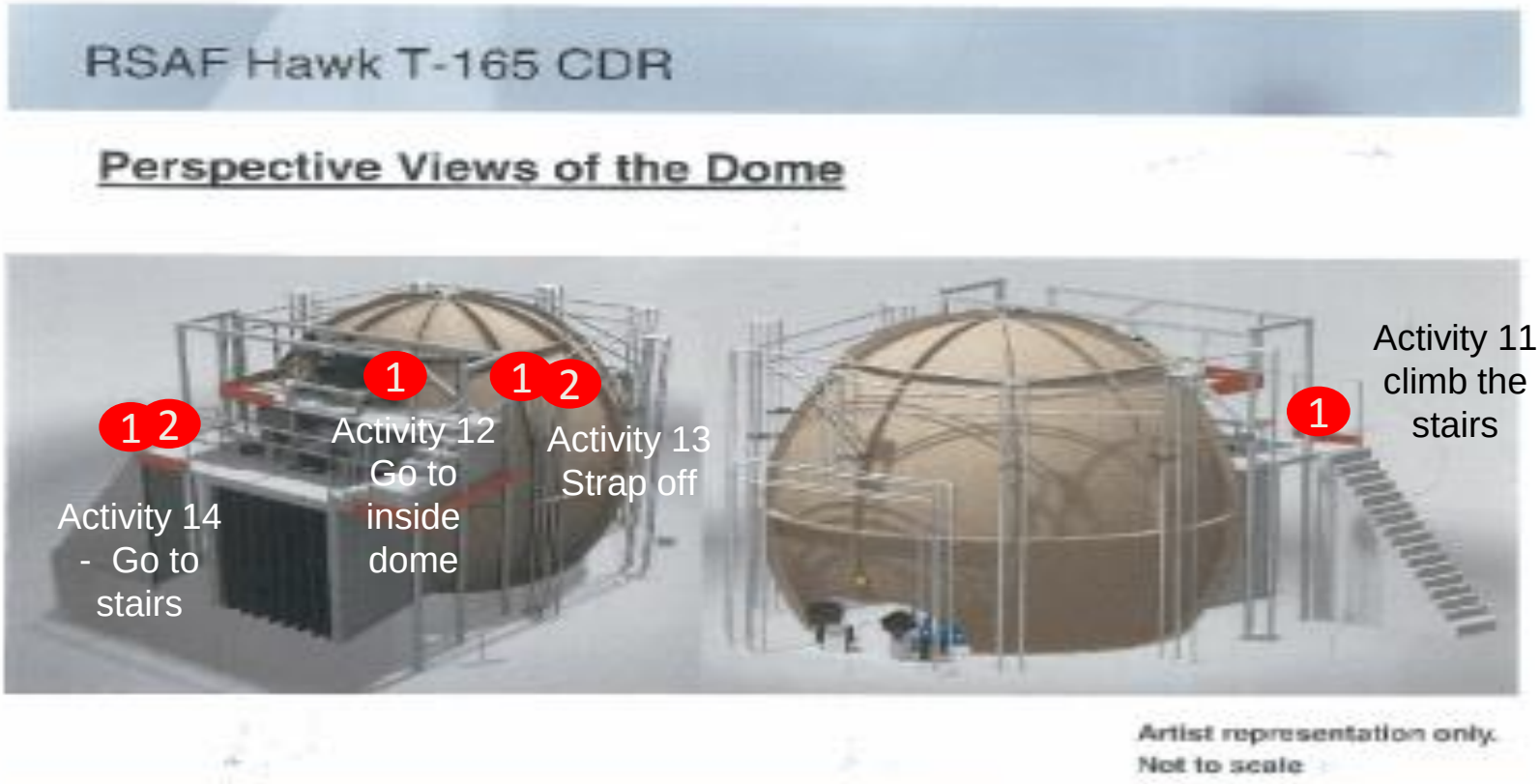
Process Sequence - 2



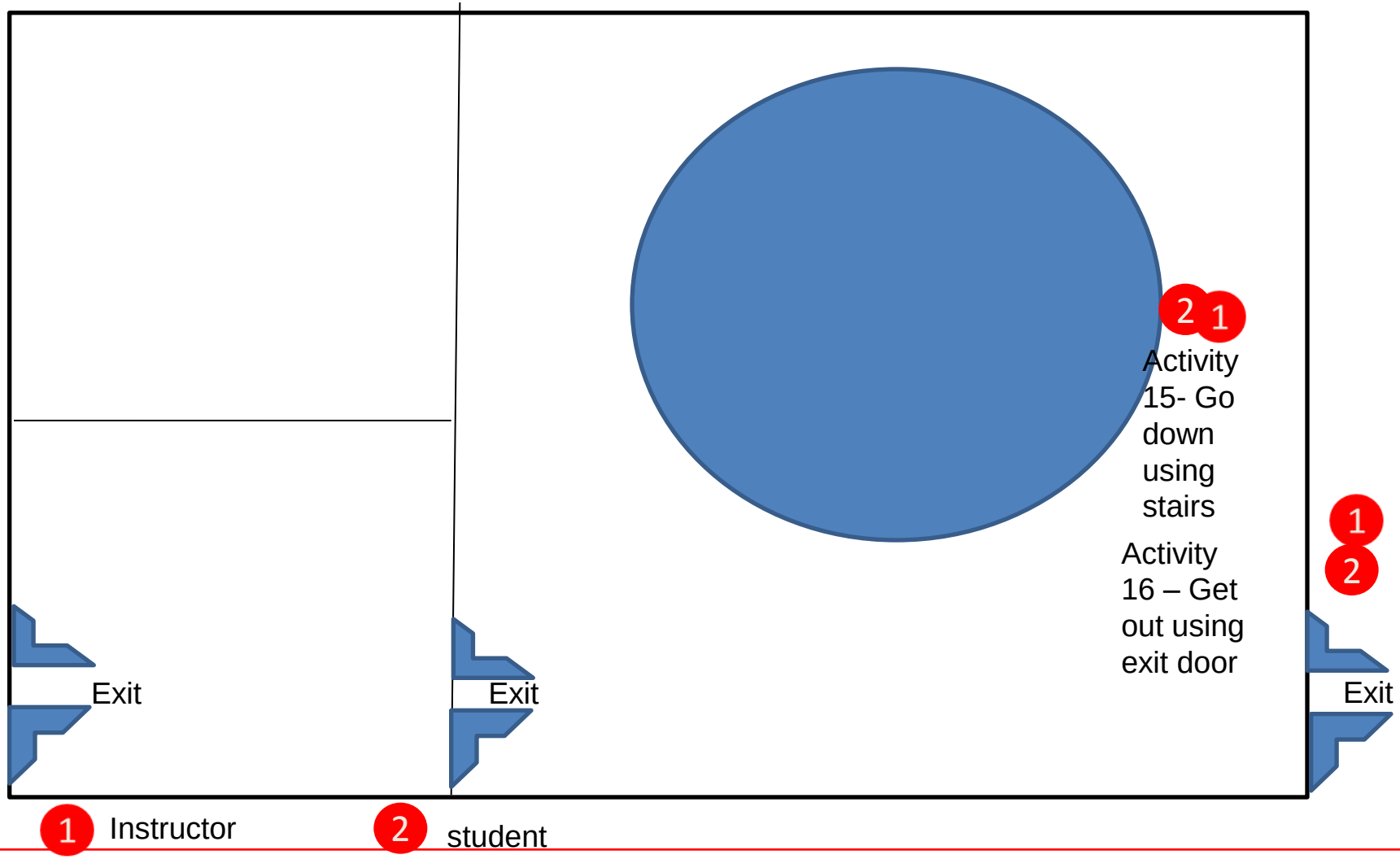
Process Sequence -3



Process Sequence - 4



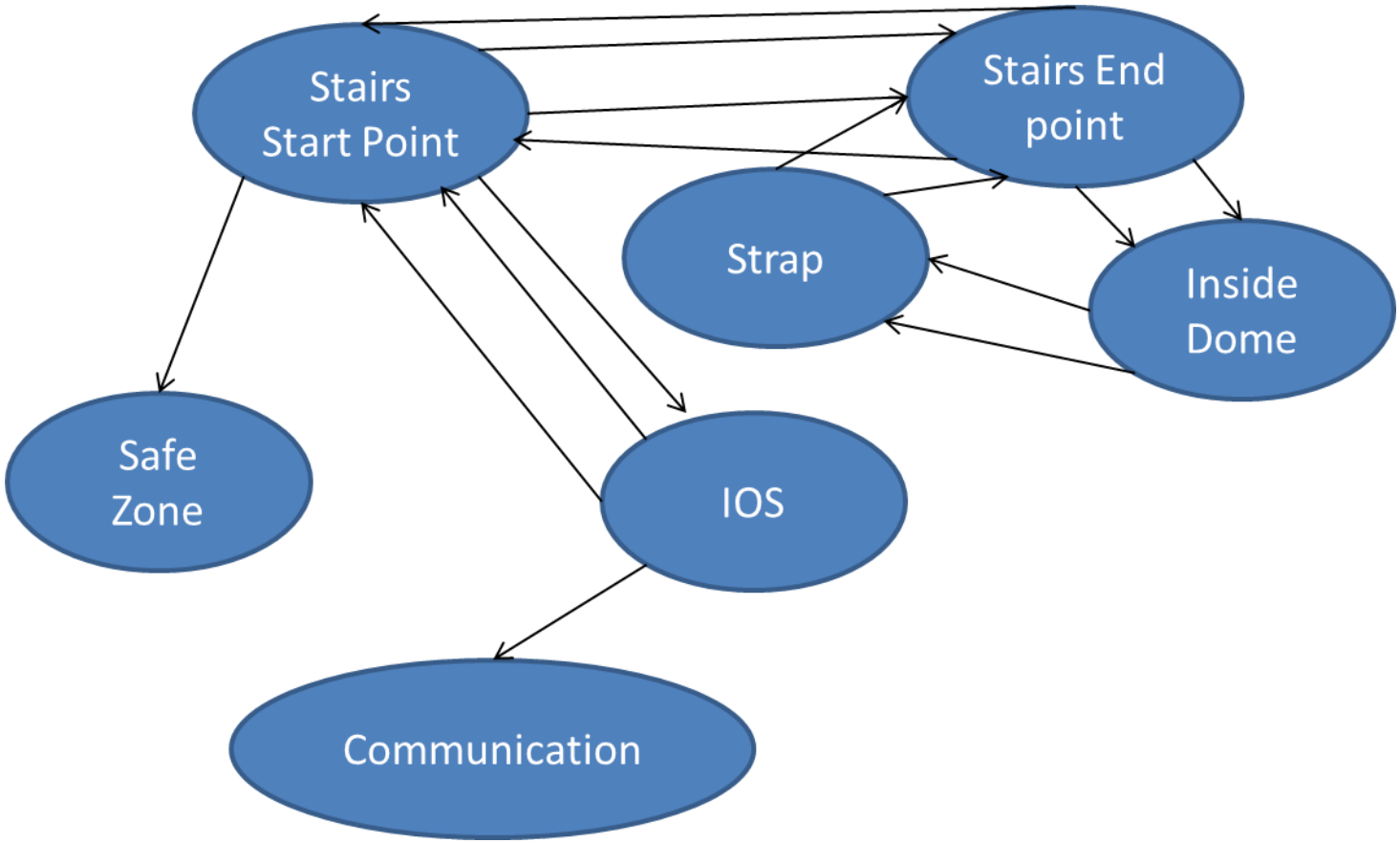
Process Sequence - 5



System Interfaces

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

Process Model



Analysis

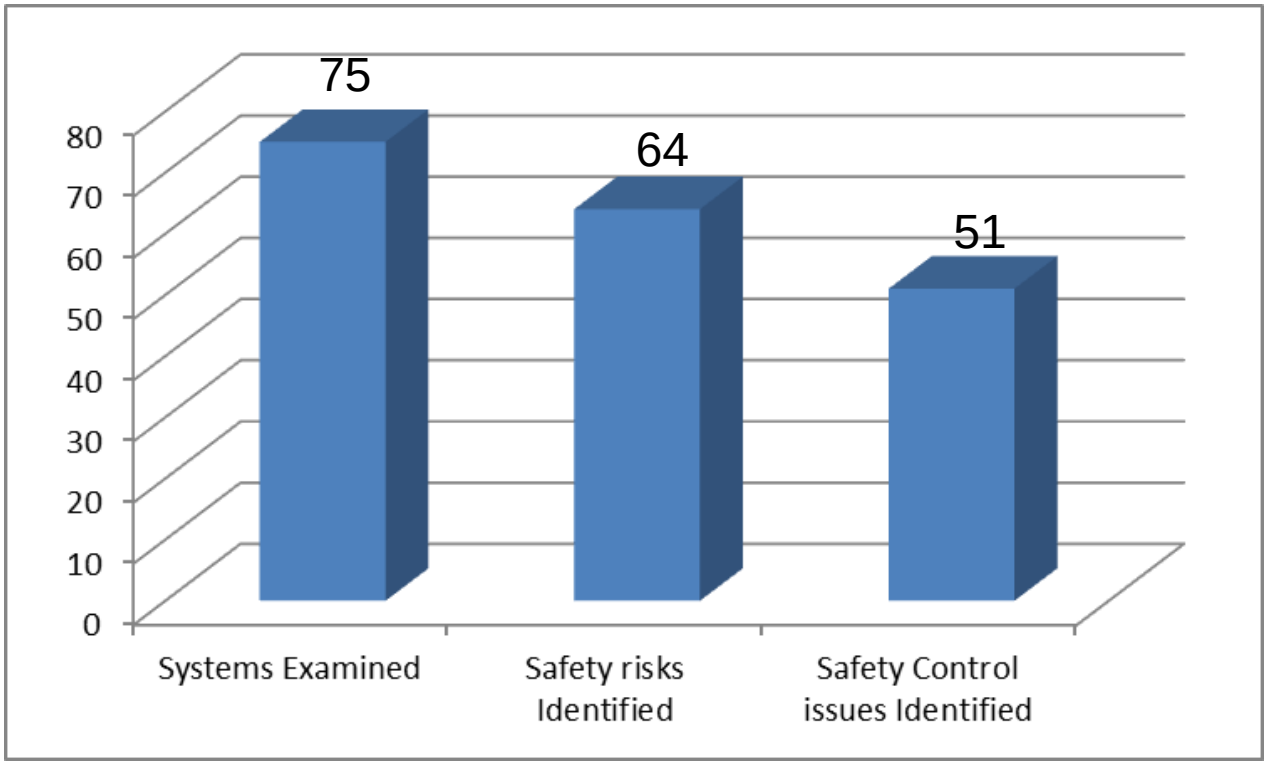
From	Activity	To	Activity No	Assoociated hazard	Control	Activity Behavior Categories	Causes	Pre HRI	Class Risk	Post HRI	Class Risk
IOS	Movement	Start point	2	NA	NA	Provided	NA	NA	NA	NA	NA
IOS	Movement	Start point	2			Not provided	NA	NA	NA	NA	NA
IOS	Movement	Start point	2			Provided Too soon	NA	NA	NA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

Analysis – Example

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

Microsoft Excel Worksheet

Analysis - Summary



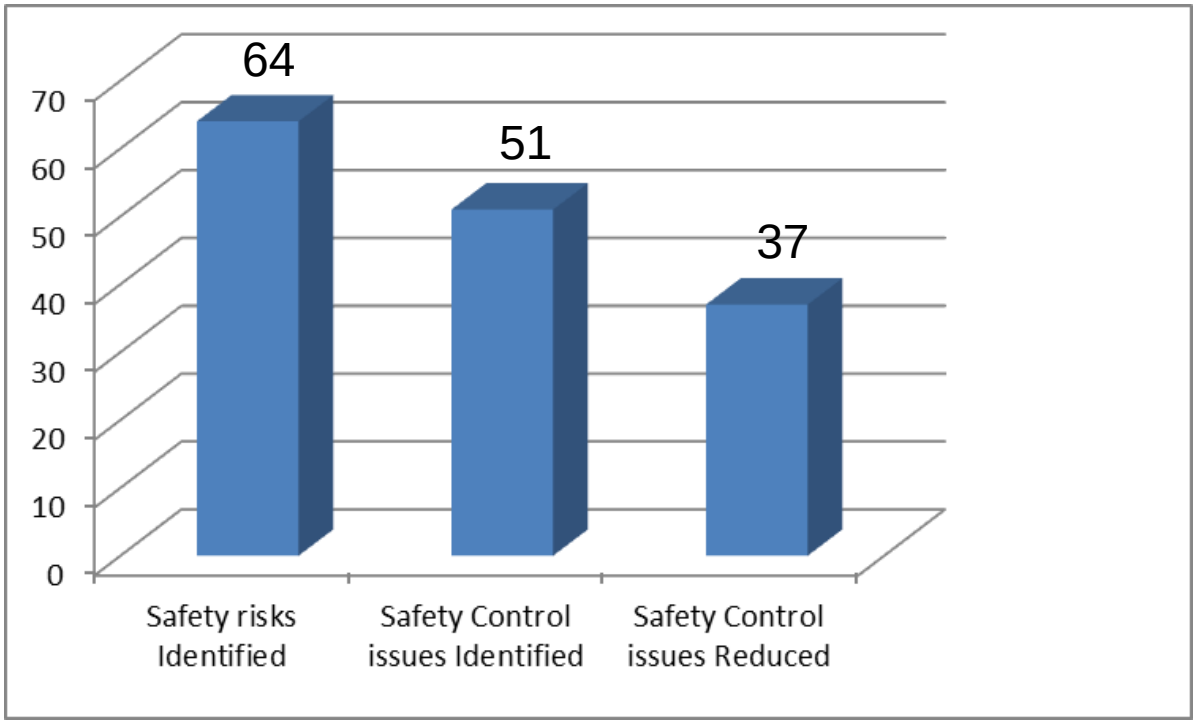
BAE SYSTEMS
INSPIRED WORK
السعودية

Filtered Analysis

From	Activity	To	Activity No	Assoociated hazard	Control	Activity Behavior Categories	Causes	Pre HRI	Class Risk	Post HRI	Class Risk
Start point	Movement	End point	3	H1/ H2/ H9	C1 - Risk Assessments	Not provided	Lack of proper working environemnt	Frequent/ Catastrophic	A	Improbable / Catastrophic	C
Start point	Movement	End point	3	H1/ H2/ H9	C1 - Risk Assessments	Provided Too soon	Improper holistic view assessment	Improbable/ Catastrophic	C	Incredible/Catastrophihc	C
Start point	Movement	End point	3	H1/ H2/ H9	C1 - Risk Assessments	Provided Too late	Lack of proper configuration	Improbable/ Marginal	D	Incredible/ Marginal	D
Start point	Movement	End point	3	H1/ H2/ H9	C1 - Risk Assessments	stopped Too soon	Lack of proper working environemnt	Probable/ Catastrophic	A	Improbable / Catastrophic	C
Inside Dome	Movement and Strapping	Strap	5	H1/ H2/ H7/ H8	C2 - Proper Strapping Training along with post and pre checks	Not provided	Student falling while operation	Frequent / Catastrophic	A	Improbable/ Catastrophic	C
Inside Dome	Movement and Strapping	Strap	5	H1/ H2/ H7/ H8	C2 - Proper Strapping Training along with post and pre checks	Provided Too soon	Student falling while operation	Remote/ Catastrophic	B	Improbable/ Catastrophic	C
Inside Dome	Movement and Strapping	Strap	5	H1/ H2/ H7/ H8	C2 - Proper Strapping Training along with post and pre checks	Provided Too late	Student falling while operation	Remote/ Catastrophic	B	Improbable/ Catastrophic	C
Inside Dome	Movement and Strapping	Strap	5	H1/ H2/ H7/ H8	C2 - Proper Strapping Training along with post and pre checks	stopped Too soon	Student falling while operation	Frequent / Catastrophic	A	Improbable/ Catastrophic	C
IOS	Movement and establish communication	Communication	9	H3/H7/H9	C3 - Calibration and regular checks and assurance to adherance to instruction manuals	Not provided	Lack of proper communication toolsets functionality	Probable/ Marginal	B	Incredible/ Marginal	D
IOS	Movement and establish communication	Communication	9	H3/H7/H9	C3 - Calibration and regular checks and assurance to adherance to instruction manuals	Provided Too soon	Lack of proper communication toolsets functionality	Remote/ Marginal	C	Improbable/ Marginal	D
IOS	Movement and establish communication	Communication	9	H3/H7/H9	C3 - Calibration and regular checks and assurance to adherance to instruction manuals	Provided Too late	Lack of proper communication toolsets functionality	Remote/ Marginal	C	Improbable/ Marginal	D
IOS	Movement and establish communication	Communication	9	H3/H7/H9	C3 - Calibration and regular checks and assurance to adherance to instruction manuals	stopped Too soon	Lack of proper communication toolsets functionality	Probable/ Marginal	B	Incredible/ Marginal	D
IOS	Movement	Start point	10	H1/H2/H3/H9	C4 - Emergency Response Planning	Not provided	Not aware of fire event	Frequent/ Catastrophic	A	Improbable/ Catastrophic	C
IOS	Movement	Start point	10	H1/H2/H3/H9	C4 - Emergency Response Planning	Provided Too late	Not able to exit to Assembly Point	Frequent/ Catastrophic	A	Improbable/ Catastrophic	C
IOS	Movement	Start point	10	H1/H2/H3/H9	C4 - Emergency Response Planning	stopped Too soon	Not able to exit to Assembly Point	Occassonal/Catastrophic	A	Improbable/Catastrophihc	C

Microsoft Excel Worksheet

Filtered Analysis - Summary



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