

SANDIA REPORT

SAND2020-1230995

Printed November 2020

SYS800 Master's Project Final Report General Diagrams & Templates

Working Copies for Final Report

Dulce Barrera

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Project Charter Template

SAND2020-1230995

Problem/Opportunity Statement:

Currently the black box system is in the design and development phase. As the system design undergoes qualification & transitions to the production phase it will be key to evaluate, determine and integrate accident based criteria and capabilities into the design

Design Objectives:

- The system will include....
- The system shall be able to....
- If project parameters allow, new capabilities should be incorporated into parts of design

Project Objectives:

- Identify system(s) that will be used to develop the design & will contain the design details
- Link communication channels and increase knowledge sharing between designers and accident response team
- Conduct work per the existing processes, designs, & procedures. Develop and implement additional tools as needed (Optimal solution & continuous improvement focus)

Scope Information:

- Scope includes the design capabilities, procedures, and processes that meet the needs of our customers
- This Project facilitates design and requirements to meet both short-term and long-term customer business objectives

Scope Boundaries: requirement changes are outside of the scope of this study. Enhancements to the design capabilities that help fulfill those requirements are within scope

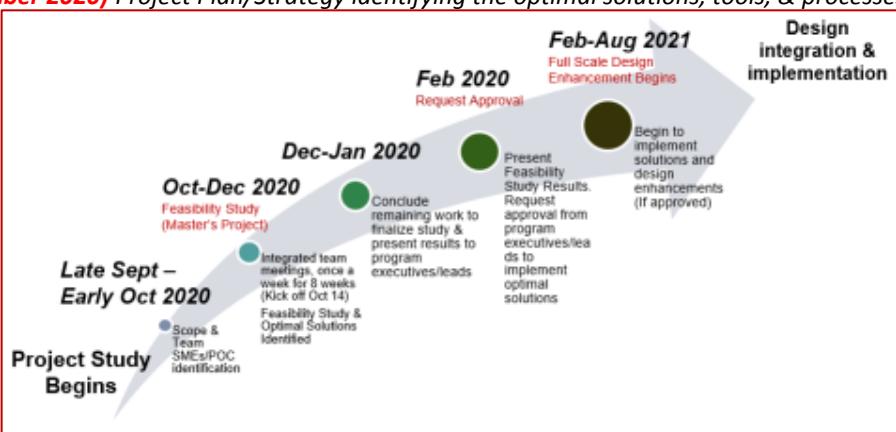
Project Constraints:

- Resources (people), project schedule, limited funding
- Security constraints: Broad spectrum of portioning of information in various classification categories

Deliverables:

- Documents: Feasibility Study & Project Plan
- Identification of integrated mission, organizational objectives, goals, milestones, & systems engineering elements

Schedule Summary: *(Sept 2020-November 2020) Project Plan/Strategy identifying the optimal solutions, tools, & processes (April 2021-Aug 2021) Definition of Design, design development and integration*



Dates:

Sept 2020-November 2020 (Master's Project)

- 9/22/2020: Identify Stakeholders & pinpoint scope & needs
- 9/28/2020: Prework for feasibility study begins
- 10/14/2020: Official project & feasibility study 'kick off'
- 10/31/2020: First Draft of Master's paper submitted
- 11/30/2020: Final Master's Project Report submitted
- 2/1/2021: Request approval from Project Executives
- 2/15/2021: Design Begins (if approved)

Champion: Manager

Sponsors: Lead

Team Lead: Dulce Barrera

Team Members:

- Design Subsystem Lead 1
- Design Team member 1 (SME)
- Design Subsystem Lead 2
- Accident Response Team Lead 1
- Accident Response Team Member 2
- Accident Response Team Member 3
- Design Team accident Response Lead & Point of Contact (POC)
- Systems Engineering Lead
- Systems Engineering Team member
- Quality engineer

Strategic/Business Objective Tie:

- Align accident response and design team mission, organizational objectives, goals, milestones, performance
- **Drivers:**
- **Key Terms:**

Scoping**Step 1**

- Conduct a Market Survey & Interviews
- Identify Objectives & Generate the Problem Statement

**System
Operations
Mapping****Step 2**

- Understand OPS/CONOPS & identify criteria of importance (people vs system)

**Generate
Ideas****Step 3**

- Generate Possible Ideas/Methods (Swim Lane diagram, SME input (Technical, processes, and information management solutions))

**Identify &
Evaluate
Alternatives****Step 4**

- Evaluate Alternatives (Dot Value analysis, PICK Chart/Weighed Decision)

**Leadership
Decision****Step 5**

- Identify leading alternative based on analysis & define supporting feasibility attributes (Cost, Schedule, Implementation Details including assembly model & milestones)

Step 6

- Inform Project Executives/Leads. Present Recommended path/solutions

Accident Response Team

Interview 2:
Accident Response Team interviewed
Number of interviewee(s): 3

Design Team

Interview 1:
Team member tasked with action from Design Review interviewed
Number of interviewee(s): 1

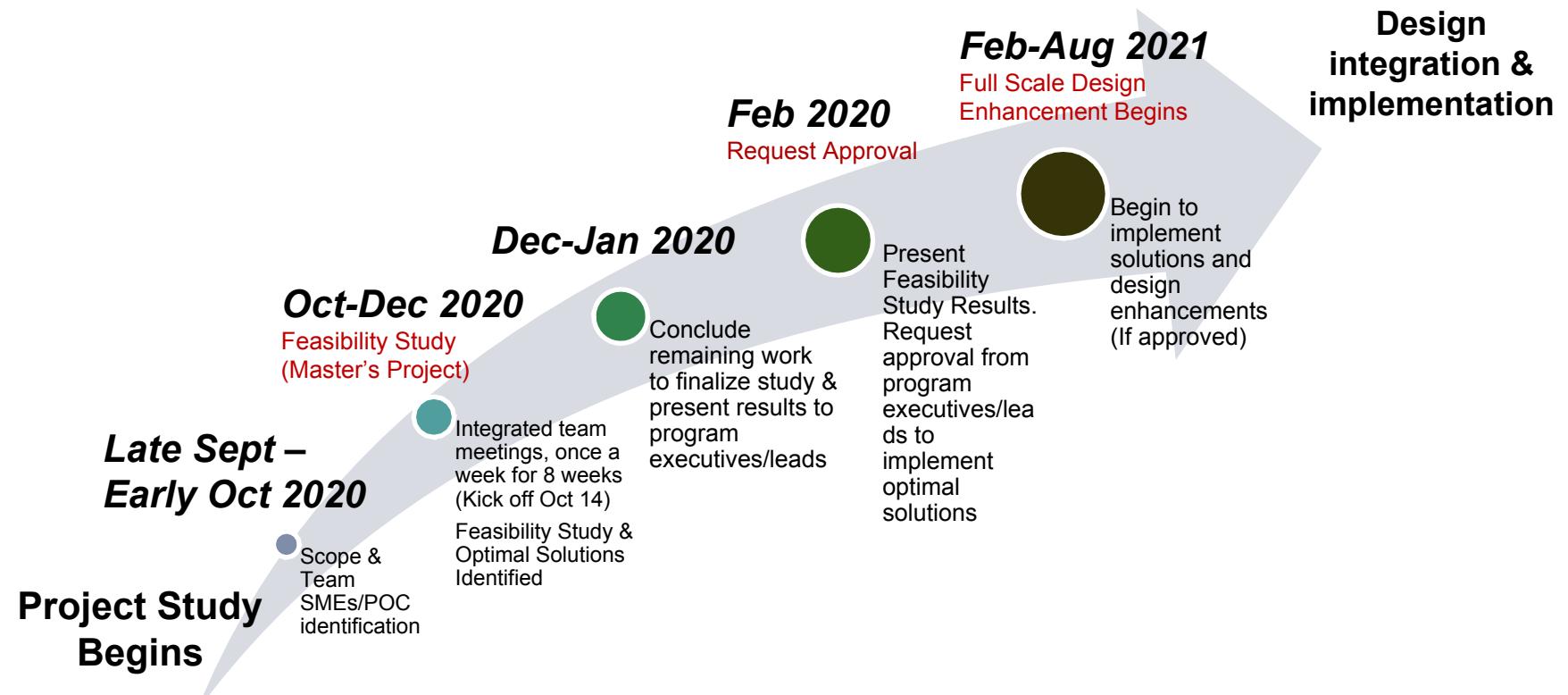
Interview 3:
Design Team Accident Response Lead/POC interviewed
Number of interviewee(s): 1

Interview 4:
Subsystem Leads interviewed
Number of interviewee(s): 2

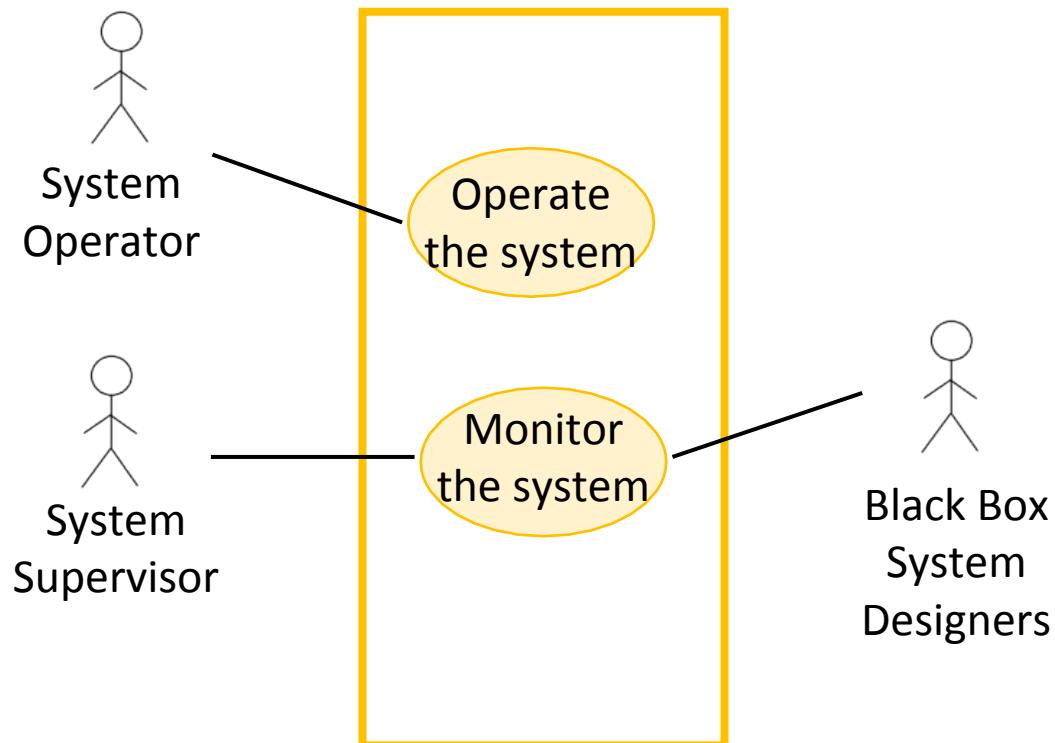
Interview 5:
Systems Engineers Interviewed
Number of interviewee(s): 2

Interview 6:
Designers for subsystems (Subject Matter Experts) interviewed
Number of interviewee(s): 2

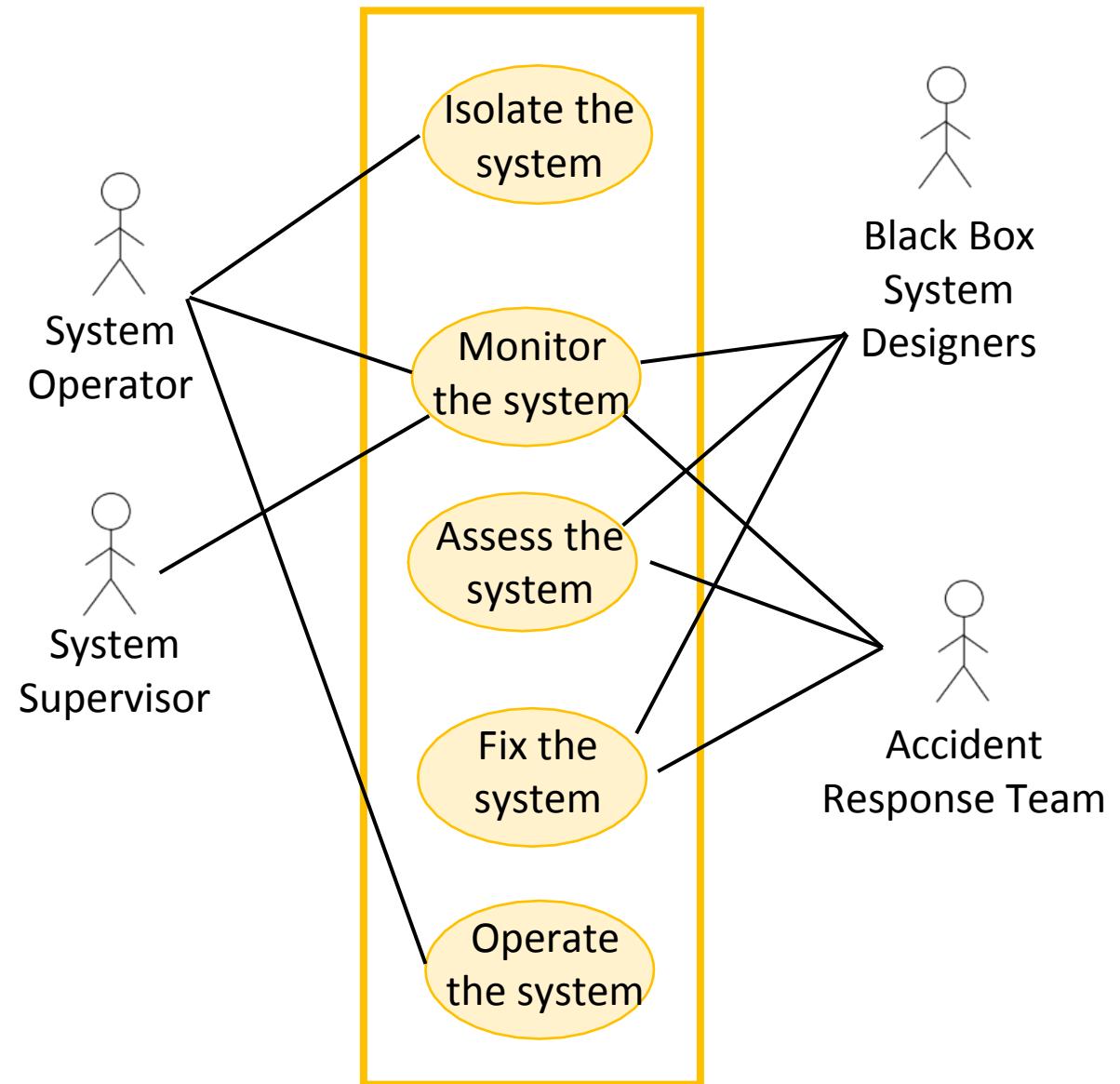


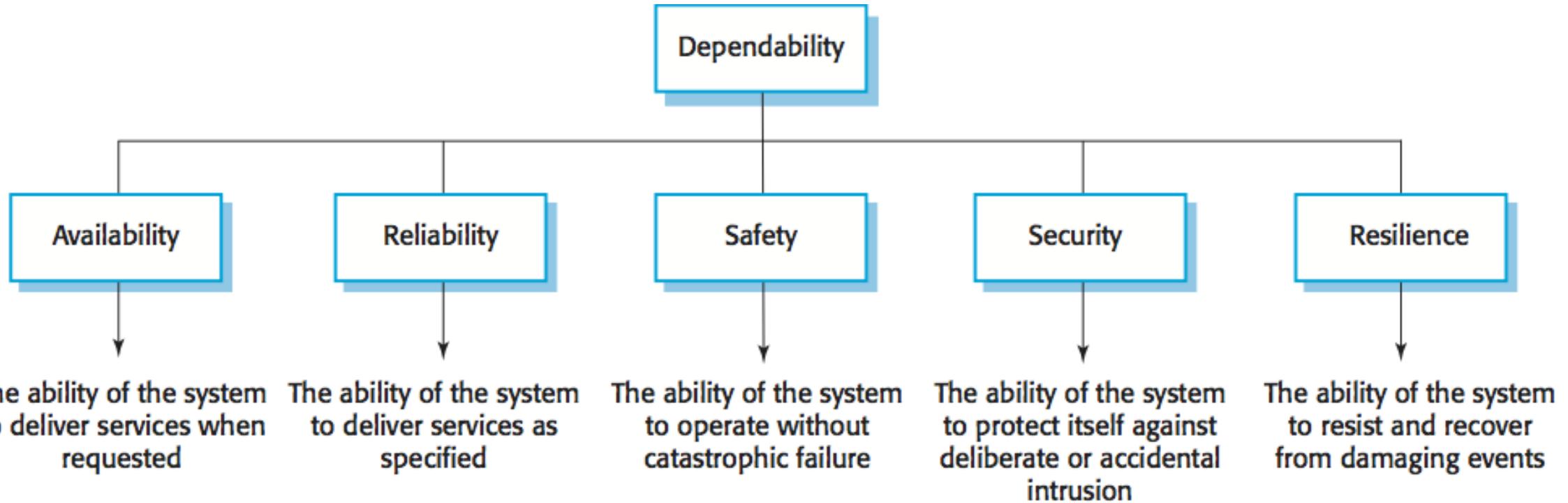


Routine Operations



Accident Response Operations

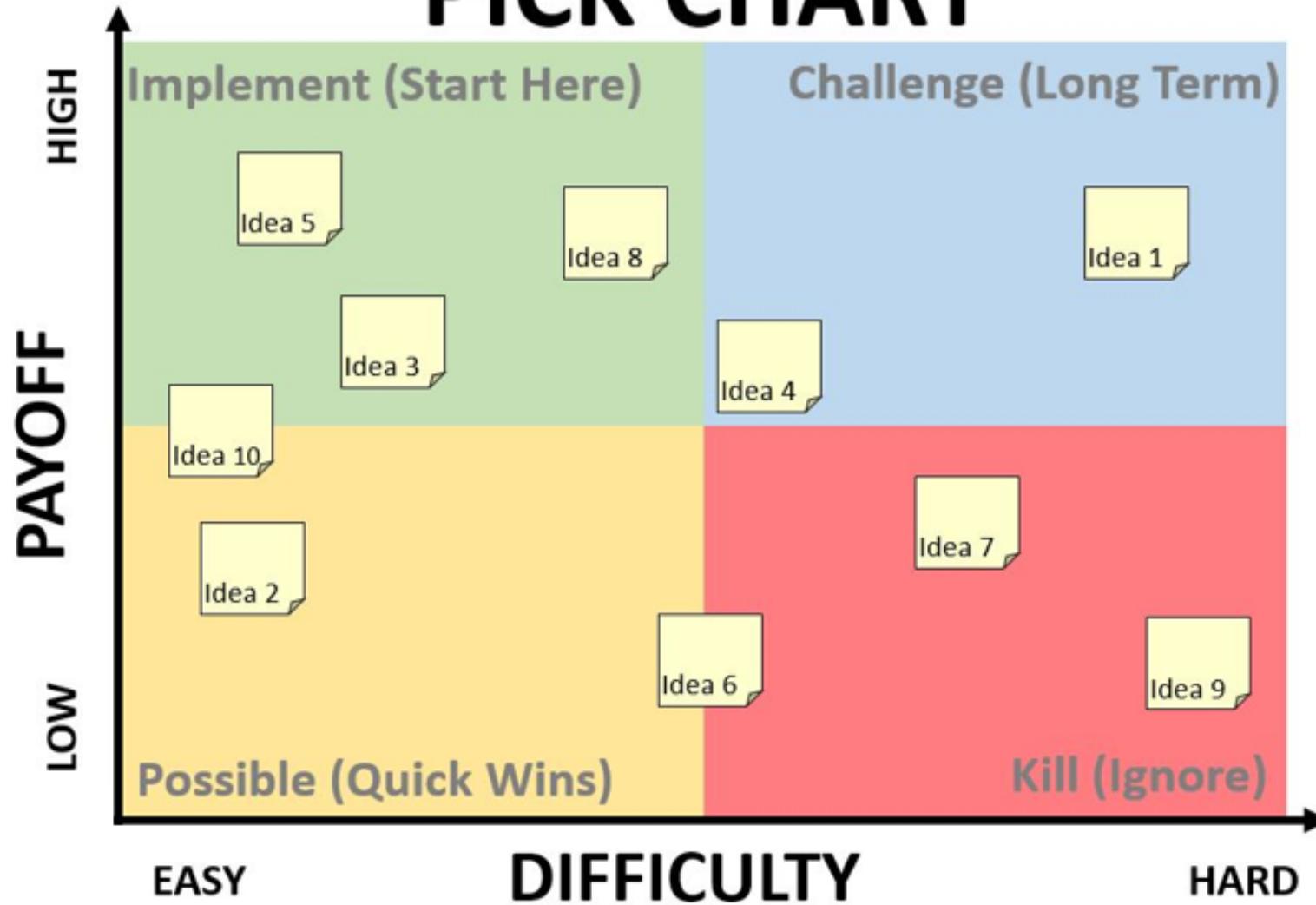




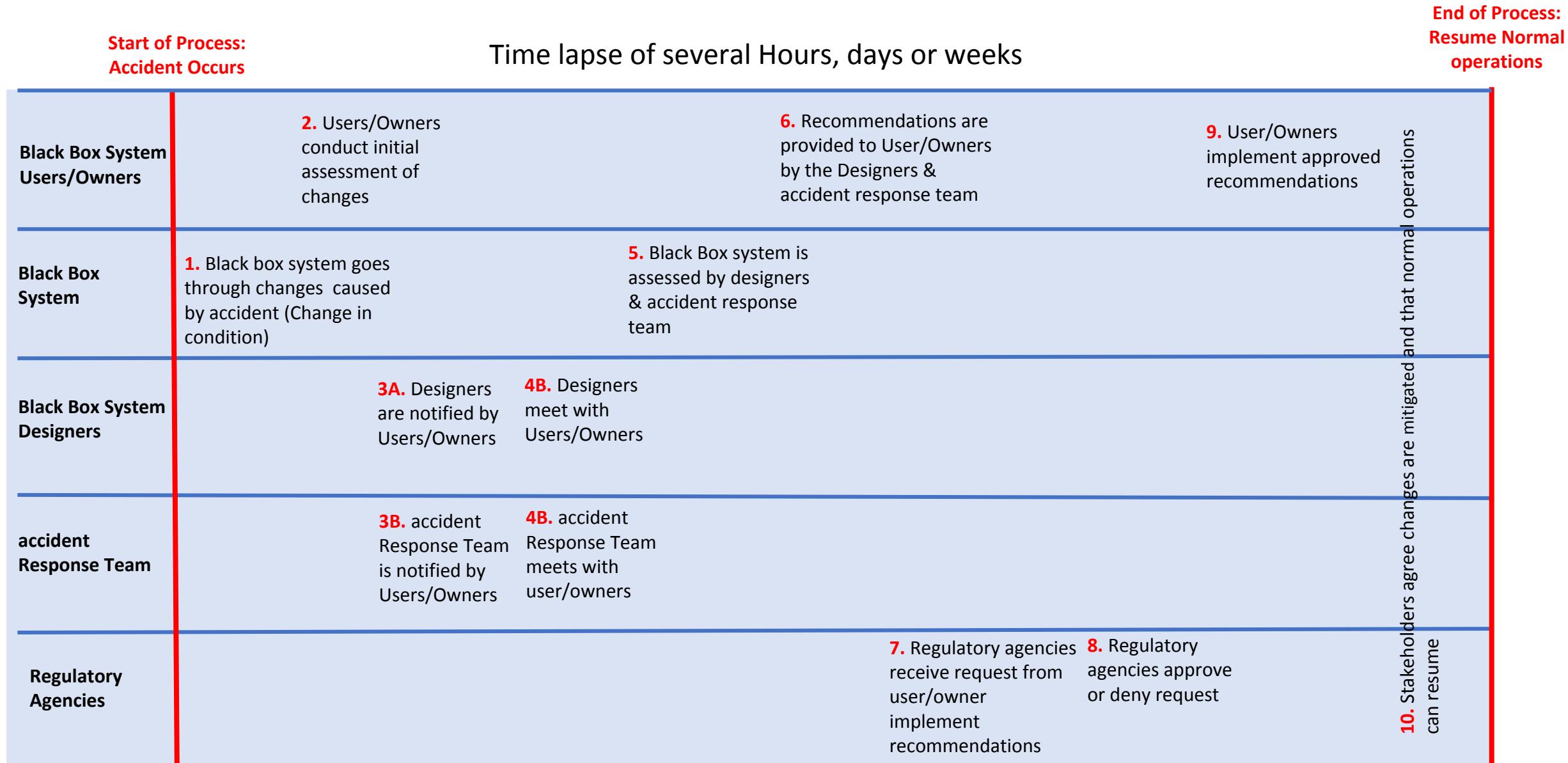
Accident Response Operations

Role (Stakeholder)	Responsibility	Accountability	Authority
Accident Response Team	Responsible for safety assessment	Accountable for safety logistics & monitoring information & procedures	Designate system as 'Safe'
Black Box system designer	Responsible for functional assessment	Accountable for black box system logistics & monitoring information & procedures	Designates system as 'Available/Functional' or 'Not Available or Non-functional'
Black Box System Users	Responsible for operating system and isolation of system	Accountable for status/state system until response team arrives.	Designate the system with 'Confirmed Isolation'
Regulatory Agency	Responsible for coordinating with all teams	Accountable for ownership of the system	Authorizes use of logistics & monitoring plans
All	Responsible to communicating & integrating with other teams	Accountable for effective planning and support within their area of expertise	Designate the system as 'Resilient, return to operations' or 'Non-resilient, maintain isolated' upon conclusion of response

PICK CHART



System Level Mapping



Note: When using a number and letter it means events are taking place in parallel.

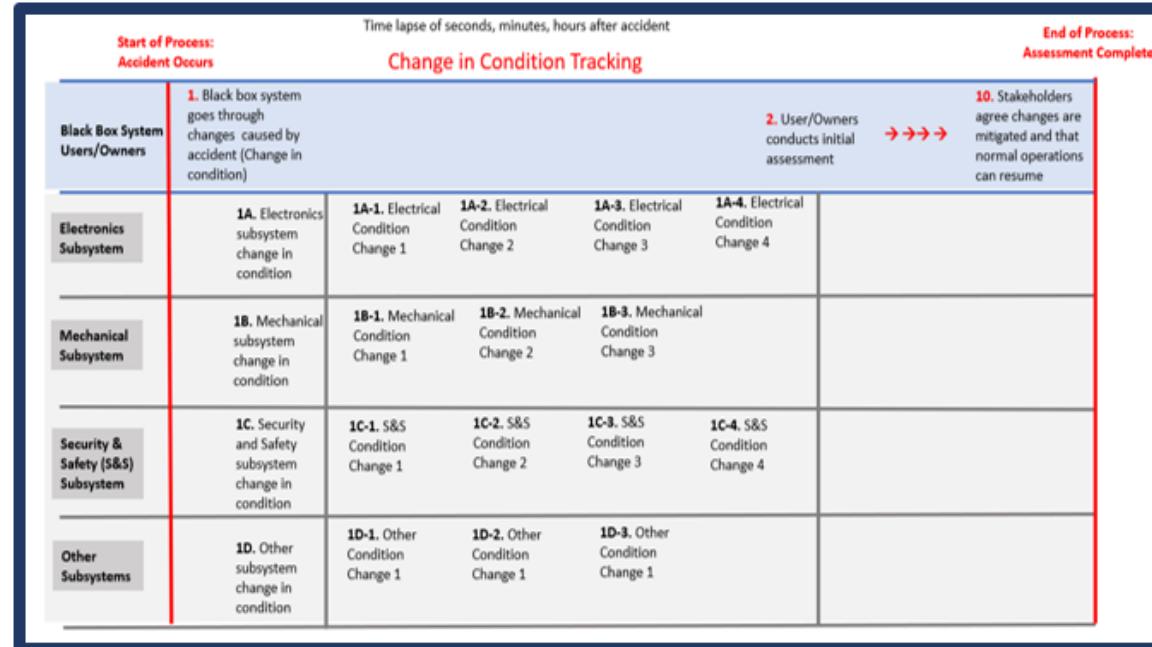
Subsystem Level Mapping (Between Steps 1&2)

Time lapse of seconds, minutes, hours after accident

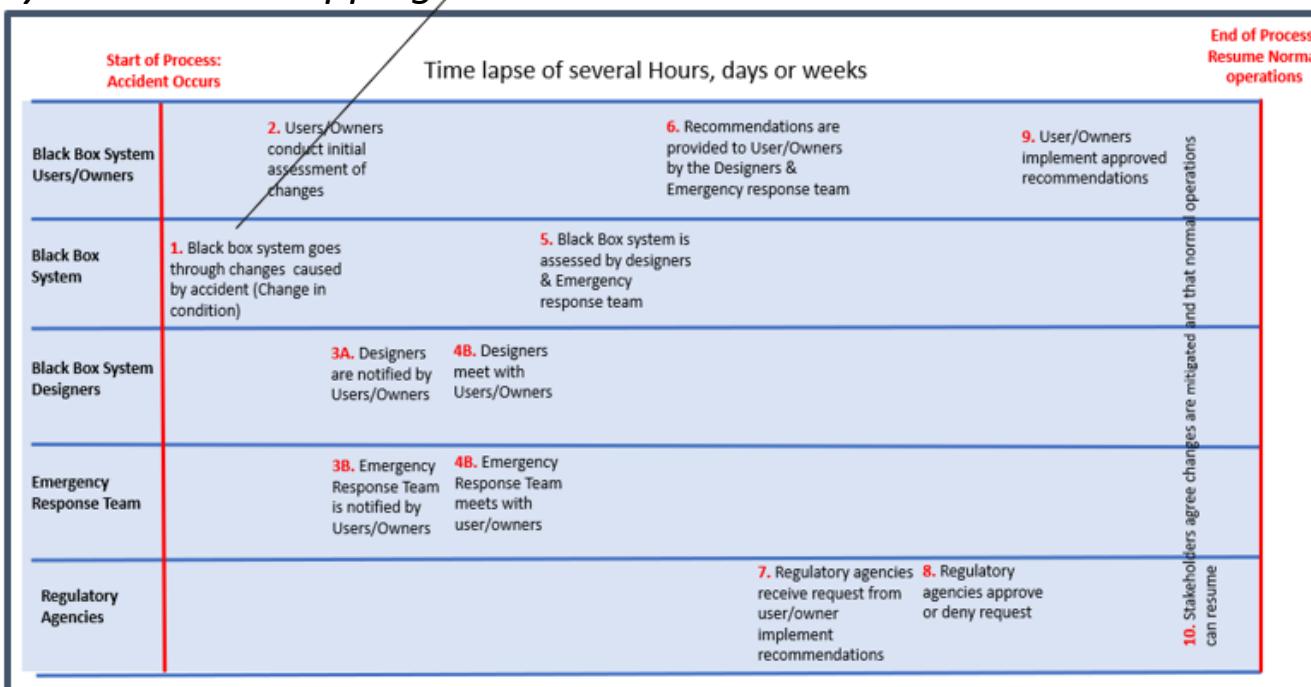
Change in Condition Tracking

							Start of Process: Accident Occurs			End of Process: Assessment Complete		
							→ → →					
										10. Stakeholders agree changes are mitigated and that normal operations can resume		
Black Box System Users/Owners		1. Black box system goes through changes caused by accident (Change in condition)					2. User/Owners conducts initial assessment		→ → →			
Electronics Subsystem		1A. Electronics subsystem change in condition	1A-1. Electrical Condition Change 1	1A-2. Electrical Condition Change 2	1A-3. Electrical Condition Change 3	1A-4. Electrical Condition Change 4						
Mechanical Subsystem		1B. Mechanical subsystem change in condition	1B-1. Mechanical Condition Change 1	1B-2. Mechanical Condition Change 2	1B-3. Mechanical Condition Change 3							
Security & Safety (S&S) Subsystem		1C. Security and Safety subsystem change in condition	1C-1. S&S Condition Change 1	1C-2. S&S Condition Change 2	1C-3. S&S Condition Change 3	1C-4. S&S Condition Change 4						
Other Subsystems		1D. Other subsystem change in condition	1D-1. Other Condition Change 1	1D-2. Other Condition Change 1	1D-3. Other Condition Change 1							

Subsystem Level Mapping (Between Steps 1&2)



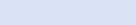
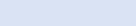
System Level Mapping



Change in Condition Tracking

Time lapse of seconds, minutes, hours after accident

Change in Condition Tracking

Start of Process: Accident Occurs							End of Process: Assessment Complete
Black Box System Users/Owners	1. Black box system goes through changes caused by accident (Change in condition)			2. User/Owners conducts initial assessment		  	10. Stakeholders agree changes are mitigated and that normal operations can resume
Electronics Subsystem	1A. Electronics subsystem change in condition	1A-1. Electrical Condition Change 1	1A-2. Electrical Condition Change 2	1A-3. Electrical Condition Change 3	1A-4. Electrical Condition Change 4		
		<i>Status indicator or monitoring capability</i>	<i>Status indicator or monitoring capability</i>	<i>Status indicator or monitoring capability</i>	<i>Status indicator or monitoring capability</i>		
Mechanical Subsystem	1B. Mechanical subsystem change in condition	1B-1. Mechanical Condition Change 1	1B-2. Mechanical Condition Change 2	1B-3. Mechanical Condition Change 3			
		<i>Status indicator or monitoring capability</i>	<i>Status indicator or monitoring capability</i>	<i>Status indicator or monitoring capability</i>			
Security & Safety (S&S) Subsystem	1C. Security and Safety subsystem change in condition	1C-1. S&S Condition Change 1	1C-2. S&S Condition Change 2	1C-3. S&S Condition Change 3	1C-4. S&S Condition Change 4		
		<i>Status indicator or monitoring capability</i>	<i>Status indicator or monitoring capability</i>	<i>Status indicator or monitoring capability</i>	<i>Status indicator or monitoring capability</i>		
Other Subsystems	1D. Other subsystem change in condition	1D-1. Other Condition Change 1	1D-2. Other Condition Change 1	1D-3. Other Condition Change 1			
		<i>Status indicator or monitoring capability</i>	<i>Status indicator or monitoring capability</i>	<i>Status indicator or monitoring capability</i>			

Legend



Existing Capability

Improve Existing Capability

New Capability

SAND2020-1230995

Dot Value Analysis

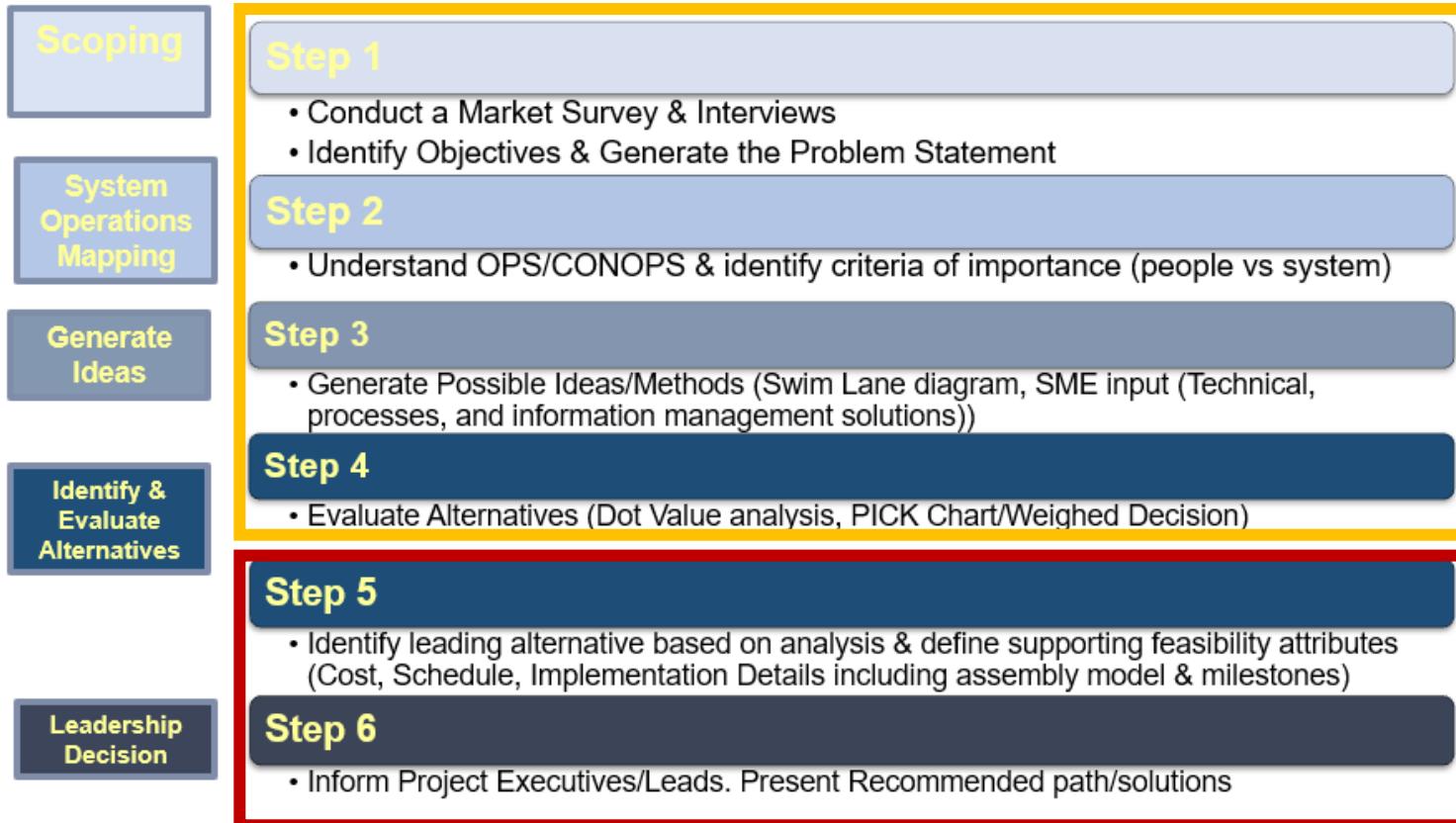
Start of Process:
Accident Occurs

Time lapse of seconds, minutes, hours after accident
Change in Condition Tracking

End of Process:
Assessment Complete

Black Box System Users/Owners	1. Black box system goes through changes caused by accident (Change in condition)				2. User/Owners conducts initial assessment	10. Stakeholders agree changes are mitigated and that normal operations can resume
					→ → →	
Electronics Subsystem	1A. Electronics subsystem change in condition	1A-1. Electrical Condition Change 1 E Status indicator or monitoring capability	1A-2. Electrical Condition Change 2 N Status indicator or monitoring capability	1A-3. Electrical Condition Change 3 N Status indicator or monitoring capability	1A-4. Electrical Condition Change 4 I Status indicator or monitoring capability	
Mechanical Subsystem	1B. Mechanical subsystem change in condition	1B-1. Mechanical Condition Change 1 I Status indicator or monitoring capability	1B-2. Mechanical Condition Change 2 N Status indicator or monitoring capability	1B-3. Mechanical Condition Change 3 E Status indicator or monitoring capability		
Security & Safety (S&S) Subsystem	1C. Security and Safety subsystem change in condition	1C-1. S&S Condition Change 1 E Status indicator or monitoring capability	1C-2. S&S Condition Change 2 I Status indicator or monitoring capability	1C-3. S&S Condition Change 3 E Status indicator or monitoring capability	1C-4. S&S Condition Change 4 N Status indicator or monitoring capability	
Other Subsystems	1D. Other subsystem change in condition	1D-1. Other Condition Change 1 N Status indicator or monitoring capability	1D-2. Other Condition Change 1 E Status indicator or monitoring capability	1D-3. Other Condition Change 1 I Status indicator or monitoring capability		

Work Status



Evaluated
during 8 week
study

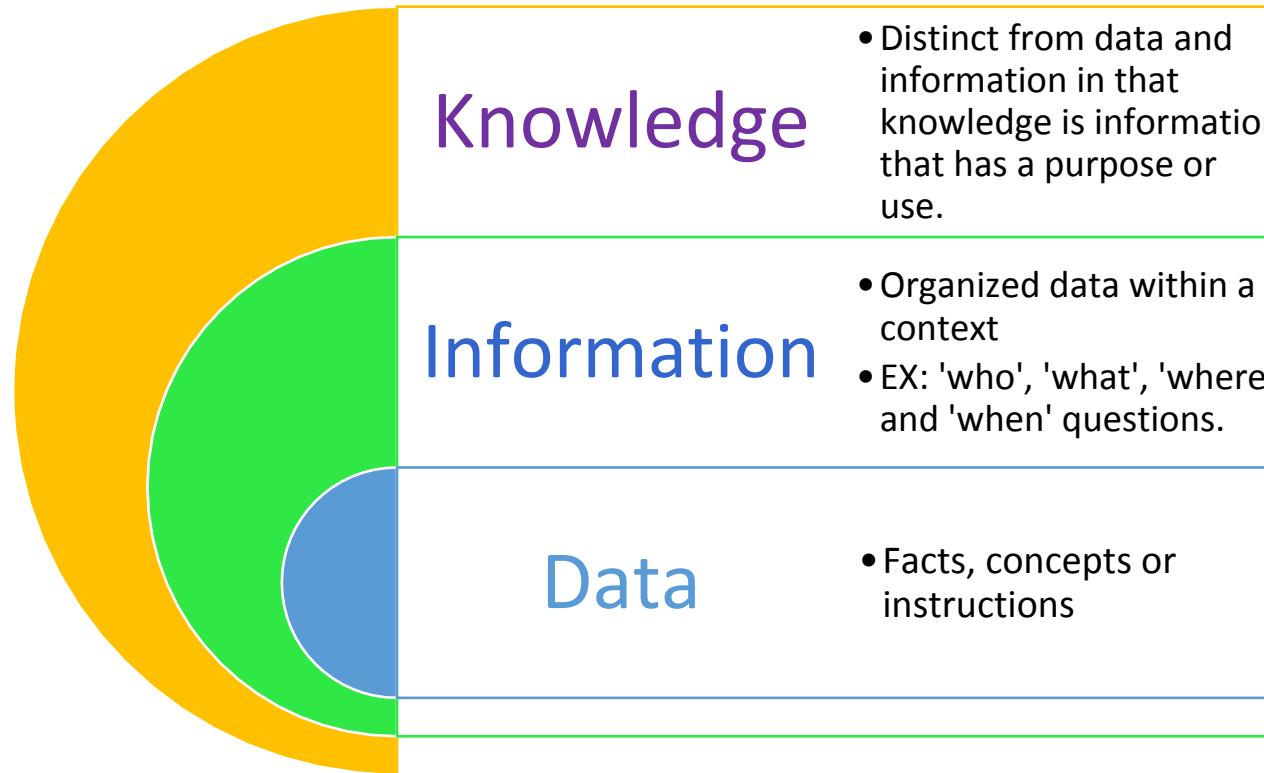
(Focus on technical &
operational feasibility)

Future Work

(Focus on schedule &
cost feasibility)

What is Knowledge?

“Gaining knowledge may be defined as the process of acquiring, understanding and interpreting information.”



The Three Types of knowledge

IAEA-TECDOC-1510 divides knowledge into three distinct categories: explicit, implicit and tacit

Explicit

- Is contained in documents, drawings, calculations, designs, databases, procedures, and manuals

Implicit

- Knowledge rendered through conversations, meetings, interviews, etc. Is difficult to reveal, but recordable

Tacit

- Is 'what we know, but don't know we know'. It involves behavior, culture and practices.