

# SANDIA REPORT

SAND2020-1230995

Printed November 2020

# SYS800 Master's Project Final Report General Diagrams & Templates

Working Copies for Final Report

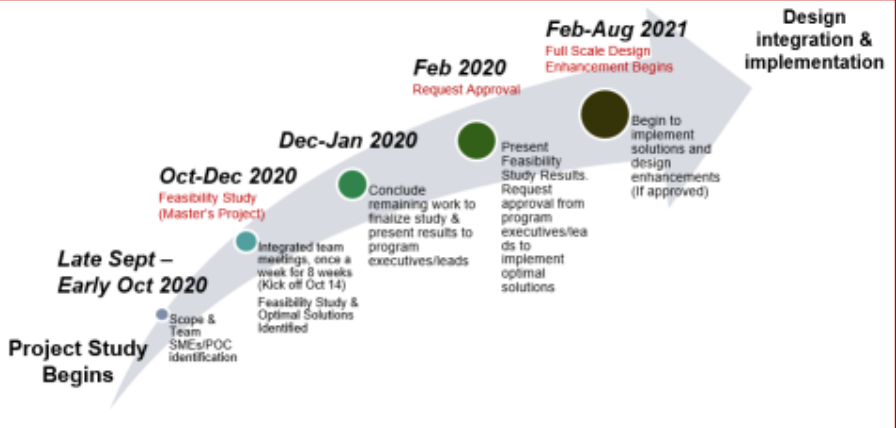
Dulce Barrera

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

<p><b>Problem/Opportunity Statement:</b></p> <p>Currently the black box system is in the design and development phase. As the system design undergoes qualification &amp; transitions to the production phase it will be key to evaluate, determine and integrate accident based criteria and capabilities into the design</p>	<p><b>Dates:</b></p> <p>Sept 2020-November 2020 (Master’s Project)</p> <ul style="list-style-type: none"><li>9/22/2020: Identify Stakeholders &amp; pinpoint scope &amp; needs</li><li>9/28/2020: Pework for feasibility study begins</li><li>10/14/2020: Official project &amp; feasibility study ‘kick off’</li><li>10/31/2020: First Draft of Master’s paper submitted</li><li>11/30/2020: Final Master’s Project Report submitted</li><li>2/1/2021: Request approval from Project Executives</li><li>2/15/2021: Design Begins (if approved)</li></ul>
<p><b>Design Objectives:</b></p> <ul style="list-style-type: none"><li>The system will include....</li><li>The system shall be able to....</li><li>If project parameters allow, new capabilities should be incorporated into parts of design</li></ul>	<p><b>Champion:</b> Manager</p> <p><b>Sponsors:</b> Lead</p> <p><b>Team Lead:</b> Dulce Barrera</p>
<p><b>Project Objectives:</b></p> <ul style="list-style-type: none"><li>Identify system(s) that will be used to develop the design &amp; will contain the design details</li><li>Link communication channels and increase knowledge sharing between designers and accident response team</li><li>Conduct work per the existing processes, designs, &amp; procedures. Develop and implement additional tools as needed (Optimal solution &amp; continuous improvement focus)</li></ul>	<p><b>Team Members:</b></p> <ul style="list-style-type: none"><li>Design Subsystem Lead 1</li><li>Design Team member 1 (SME)</li><li>Design Subsystem Lead 2</li><li>Accident Response Team Lead 1</li><li>Accident Response Team Member 2</li><li>Accident Response Team Member 3</li><li>Design Team accident Response Lead &amp; Point of Contact (POC)</li><li>Systems Engineering Lead</li><li>Systems Engineering Team member</li><li>Quality engineer</li></ul>
<p><b>Scope Information:</b></p> <ul style="list-style-type: none"><li>Scope includes the design capabilities, procedures, and processes that meet the needs of our customers</li><li>This Project facilitates design and requirements to meet both short-term and long-term customer business objectives</li></ul> <p><b>Scope Boundaries:</b> requirement changes are outside of the scope of this study. Enhancements to the design capabilities that help fulfill those requirements are within scope</p>	
<p><b>Project Constraints:</b></p> <ul style="list-style-type: none"><li>Resources (people), project schedule, limited funding</li><li>Security constraints: Broad spectrum of portioning of information in various classification categories</li></ul>	
<p><b>Deliverables:</b></p> <ul style="list-style-type: none"><li>Documents: Feasibility Study &amp; Project Plan</li><li>Identification of integrated mission, organizational objectives, goals, milestones, &amp; systems engineering elements</li></ul> <p><b>Schedule Summary:</b> <i>(Sept 2020-November 2020) Project Plan/Strategy identifying the optimal solutions, tools, &amp; processes (April 2021-Aug 2021) Definition of Design, design development and integration</i></p>	
	<p><b>Strategic/Business Objective Tie:</b></p> <ul style="list-style-type: none"><li>Align accident response and design team mission, organizational objectives, goals, milestones, performance</li><li><i>Drivers:</i></li><li><i>Key Terms:</i></li></ul>

**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)

**Step 5**

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

**Leadership  
Decision****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

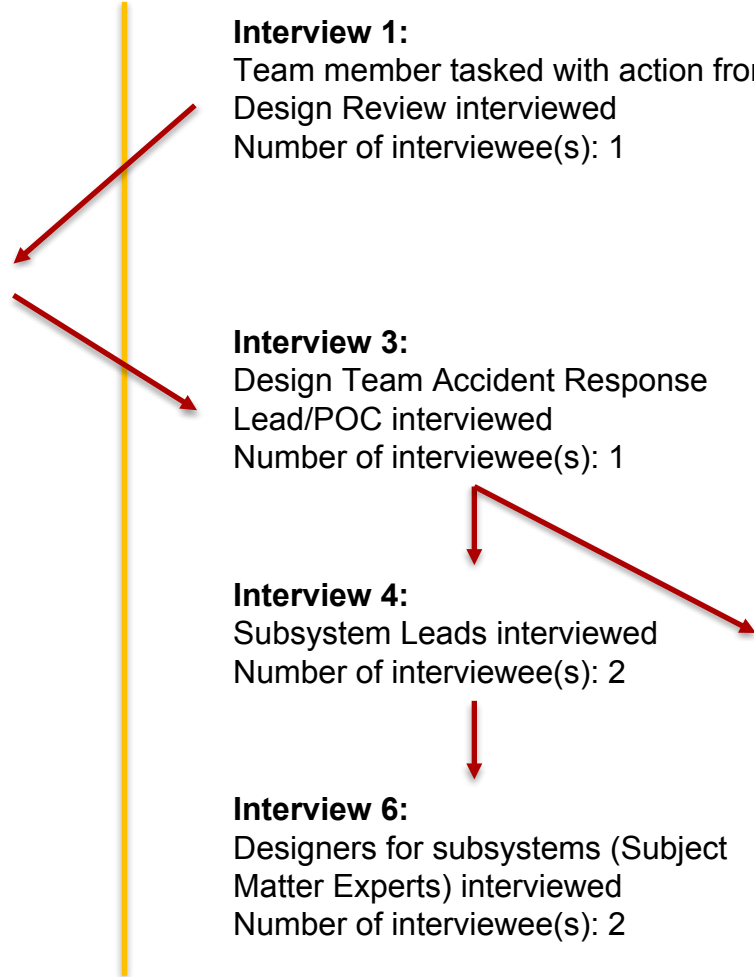
**Interview 1:**  
Team member tasked with action from  
Design Review interviewed  
Number of interviewee(s): 1

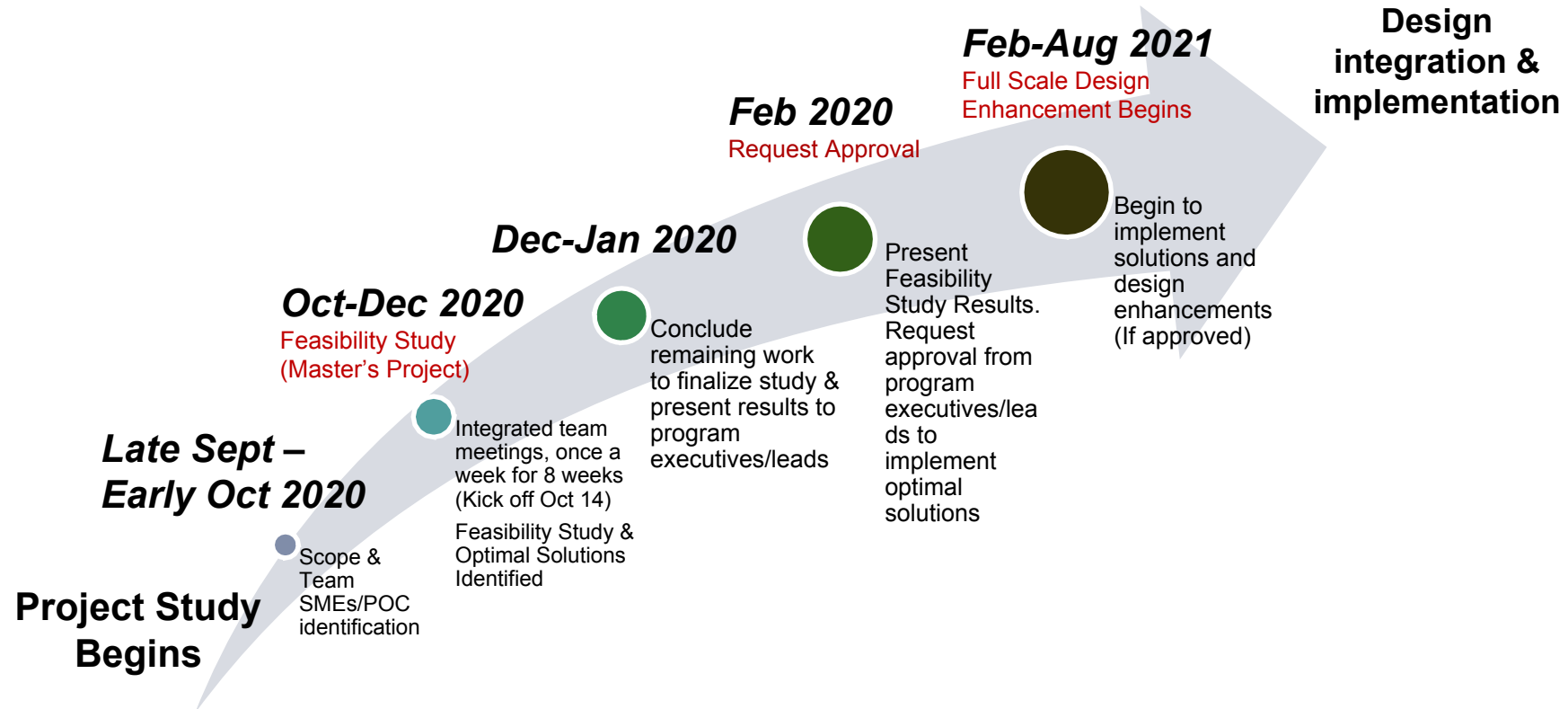
**Interview 3:**  
Design Team Accident Response  
Lead/POC interviewed  
Number of interviewee(s): 1

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

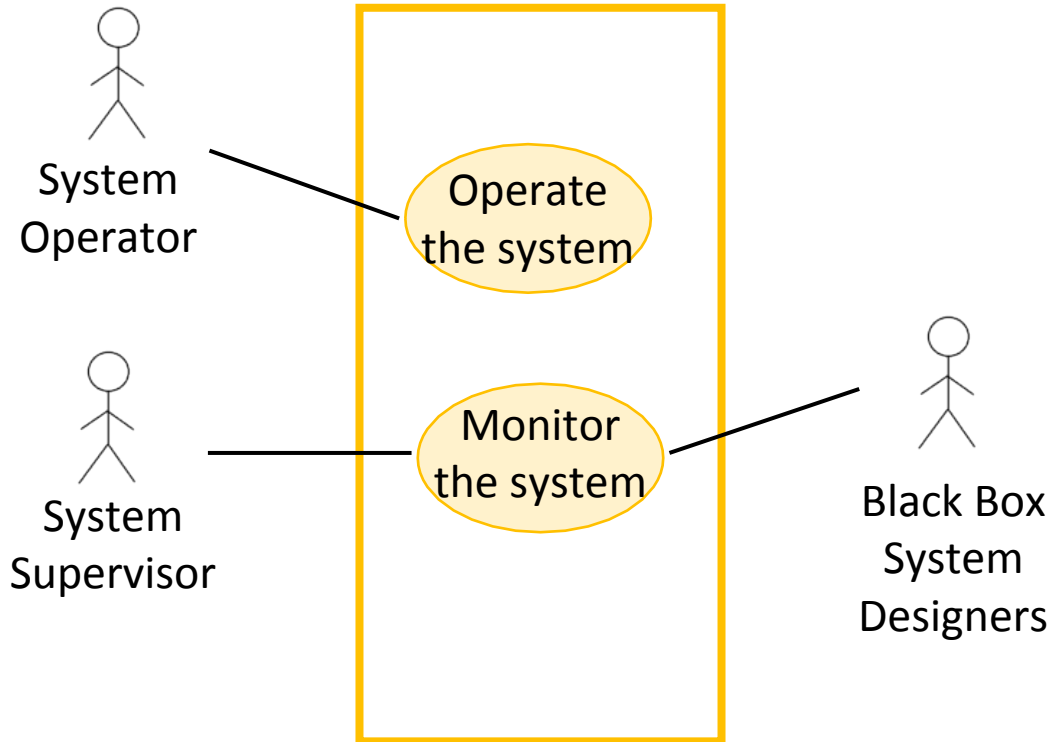
**Interview 6:**  
Designers for subsystems (Subject  
Matter Experts) interviewed  
Number of interviewee(s): 2

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

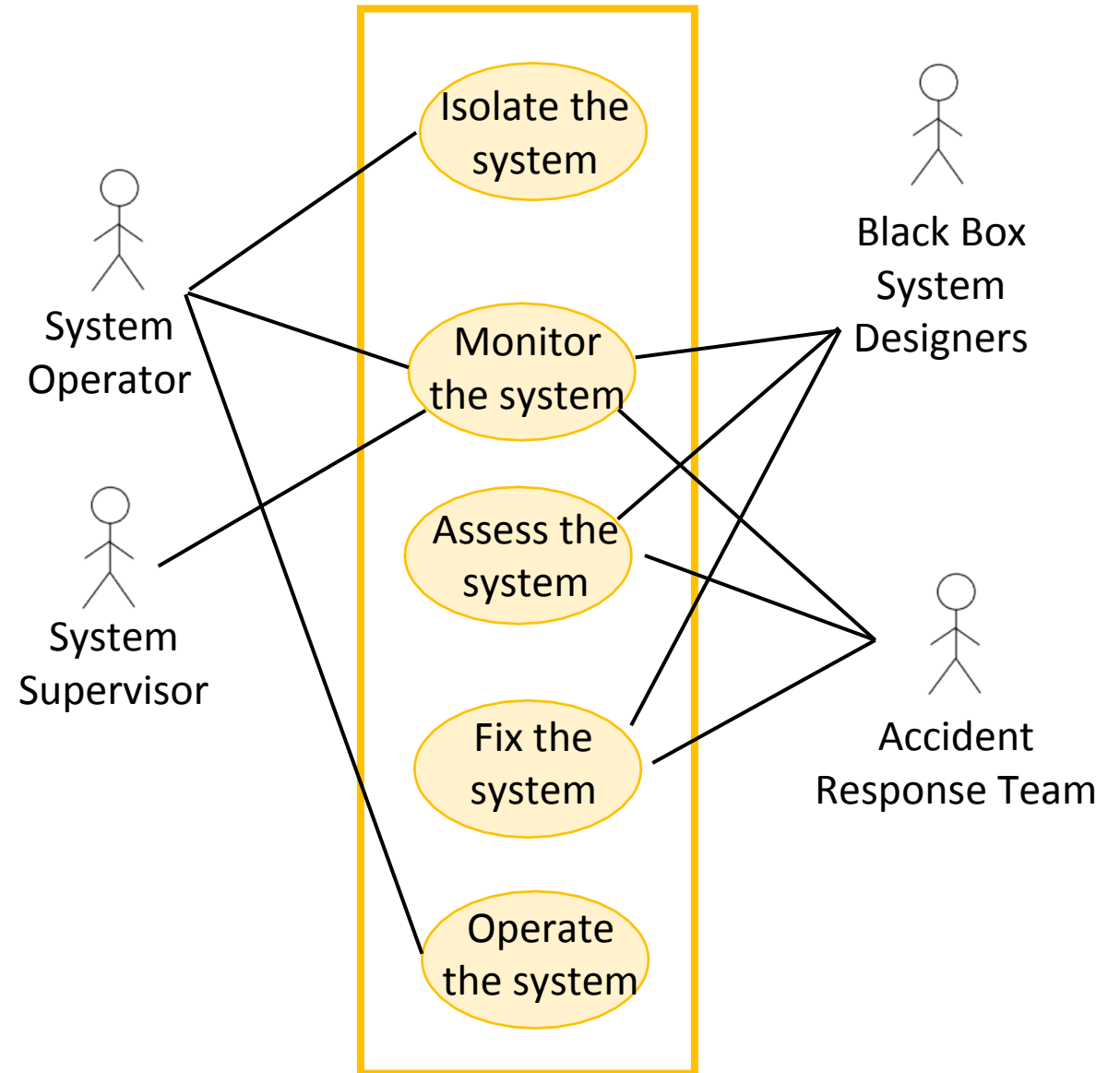


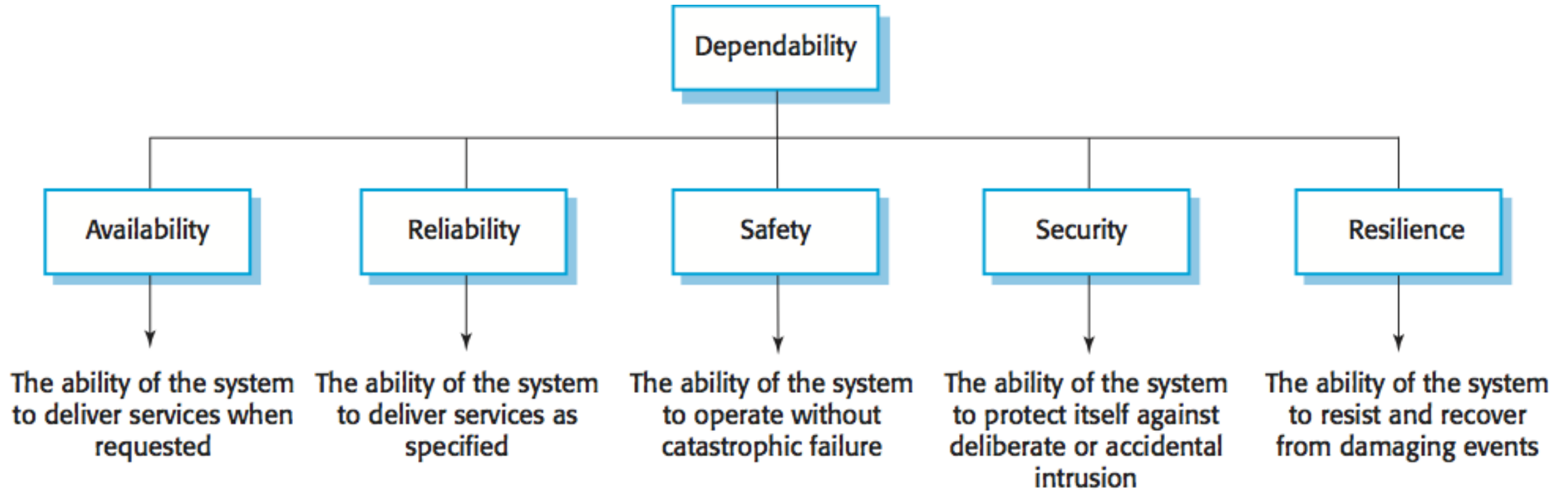


## Routine Operations



## Accident Response Operations



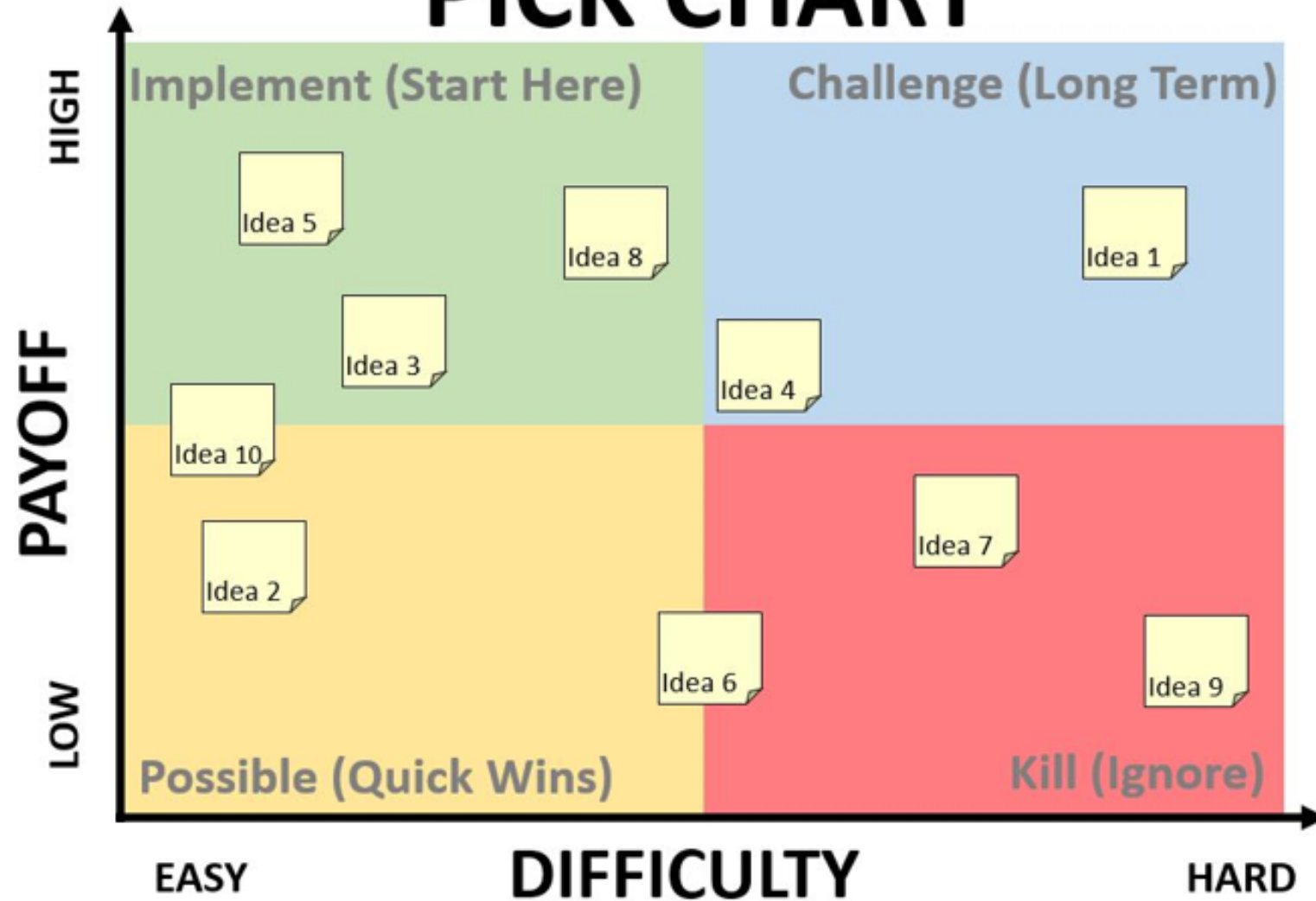


# Accident Response Operations

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

End of Process:  
Resume Normal  
operations

Start of Process:  
Accident Occurs

Time lapse of several Hours, days or weeks

Black Box System Users/Owners	2. Users/Owners conduct initial assessment of changes		6. Recommendations are provided to User/Owners by the Designers & accident response team		9. User/Owners implement approved recommendations	10. Stakeholders agree changes are mitigated and that normal operations can resume
Black Box System	1. Black box system goes through changes caused by accident (Change in condition)		5. Black Box system is assessed by designers & accident response team			
Black Box System Designers	3A. Designers are notified by Users/Owners		4B. Designers meet with Users/Owners			
accident Response Team	3B. accident Response Team is notified by Users/Owners		4B. accident Response Team meets with user/owners			
Regulatory Agencies			7. Regulatory agencies receive request from user/owner implement recommendations		8. Regulatory agencies approve or deny request	

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

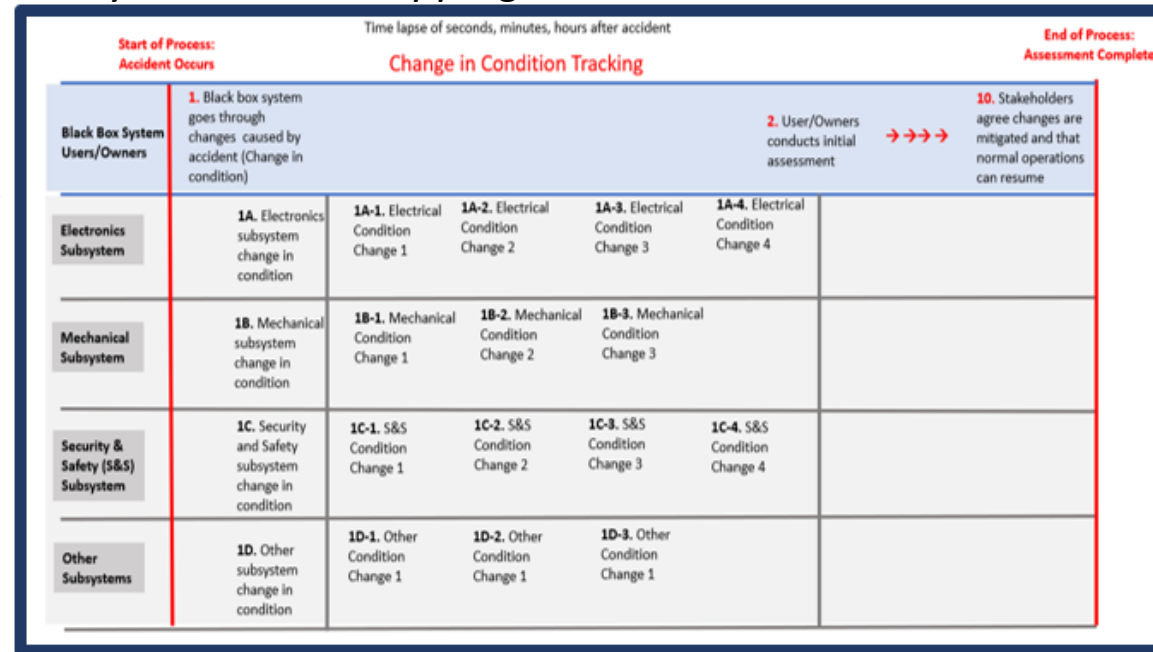
**Start of Process:**  
**Accident Occurs**

## Change in Condition Tracking

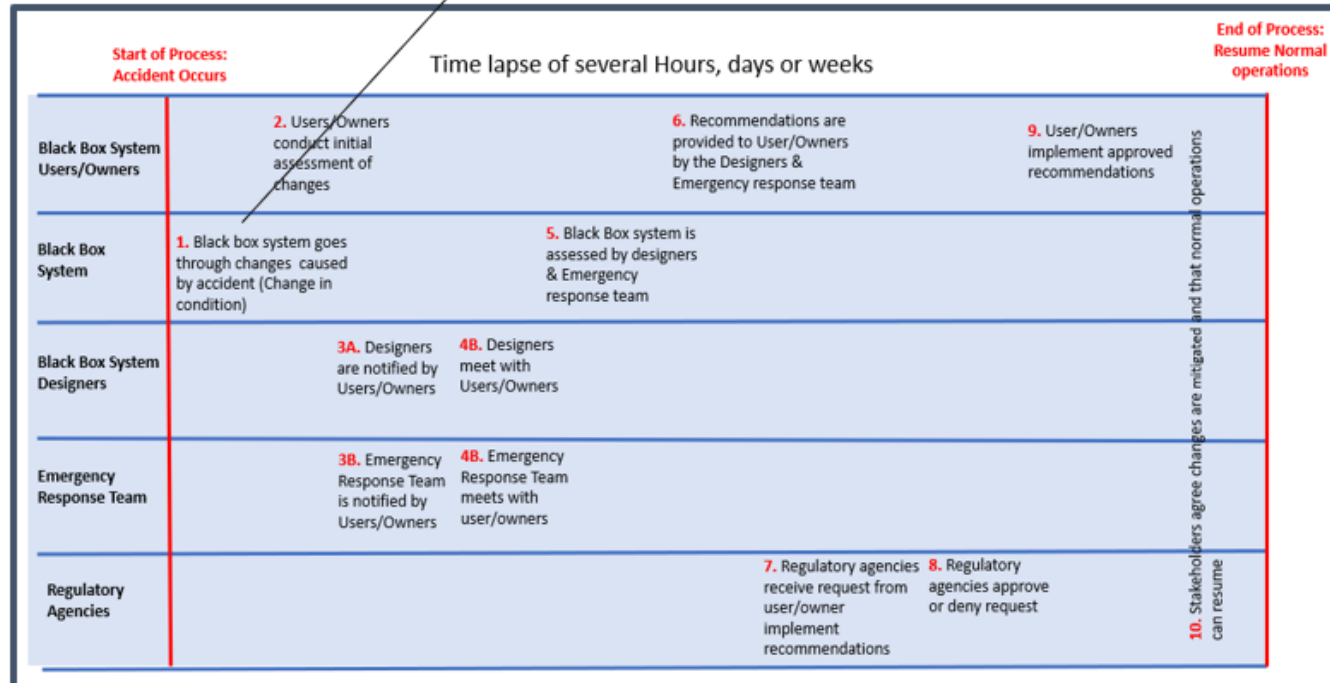
**End of Process:**  
**Assessment Complete**

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




**Start of Process:**  
**Accident Occurs**

## Change in Condition Tracking

**End of Process:**  
**Assessment Complete**

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

Legend















-  Existing Capability
-  Improve Existing Capability
-  New Capability

Dot Value Analysis

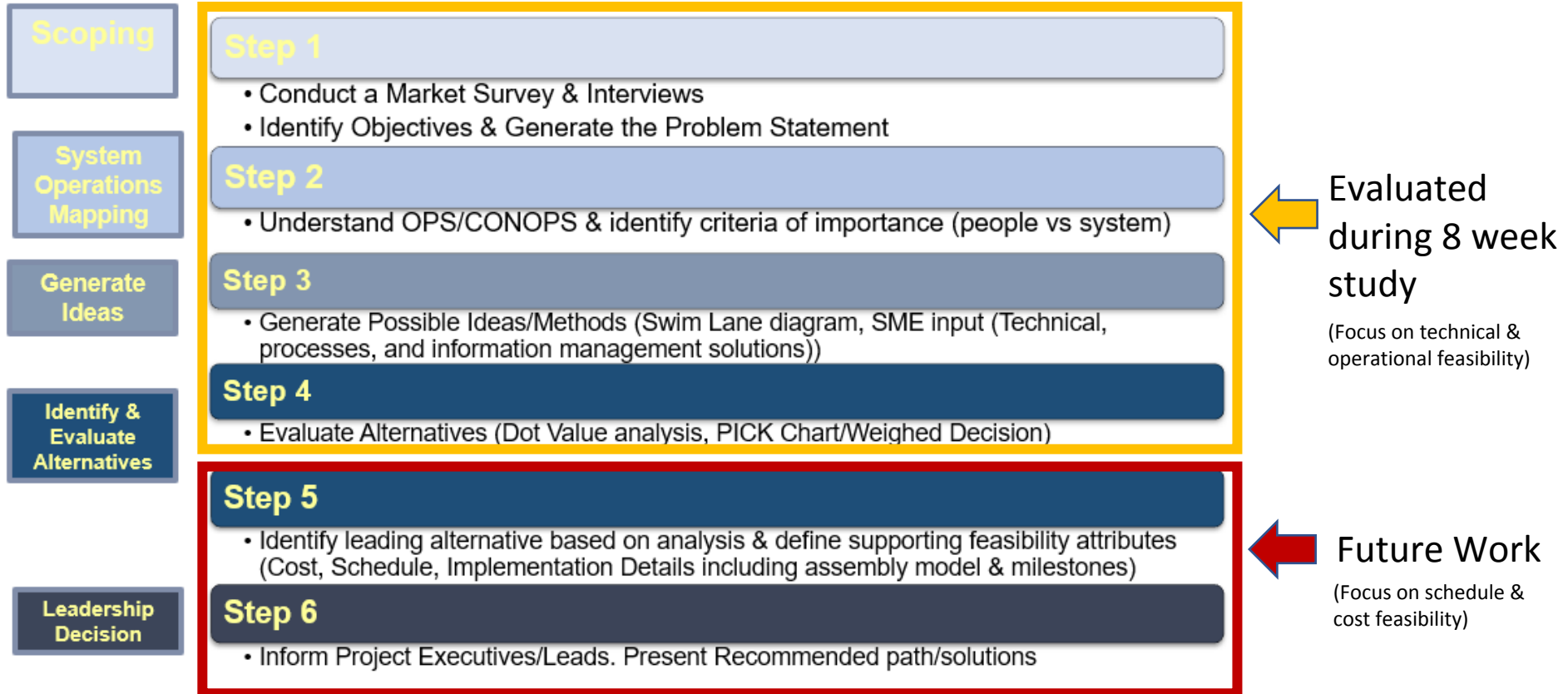
Start of Process:  
Accident Occurs

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

End of Process:  
Assessment Complete

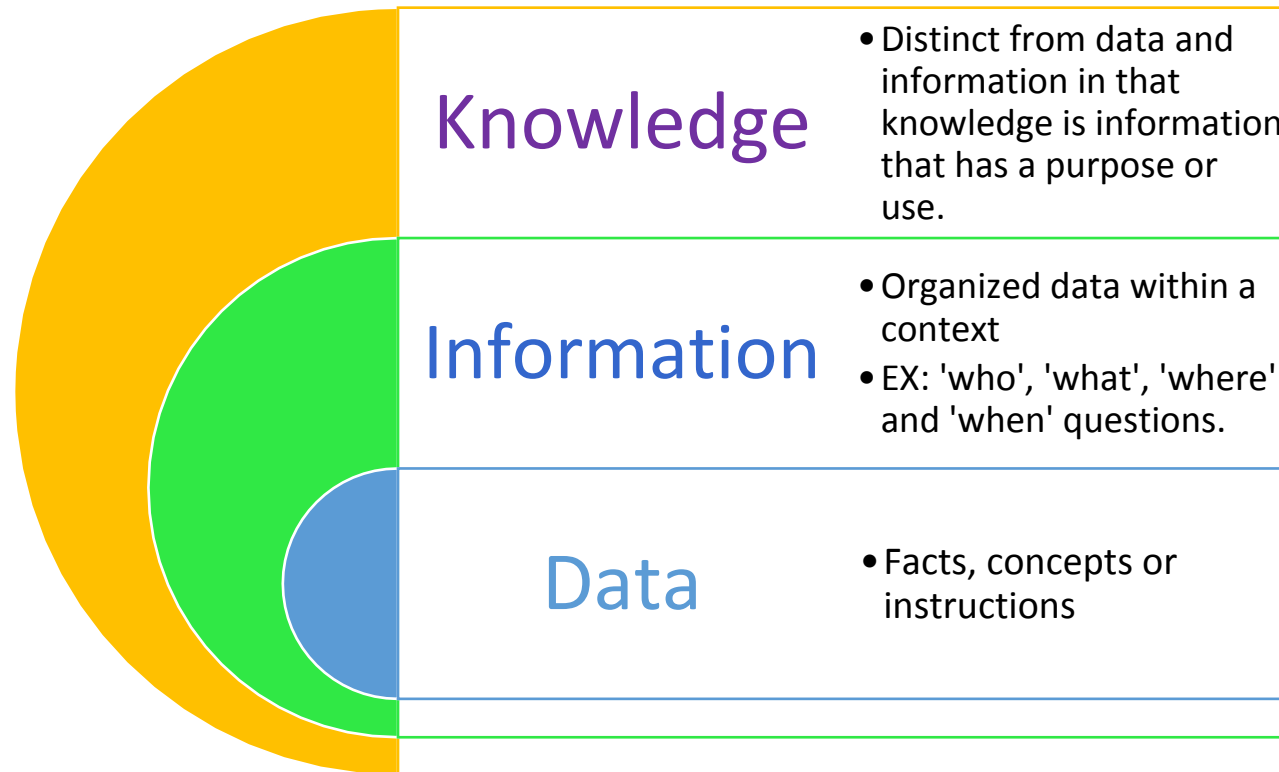
Black Box System Users/Owners		1. Black box system goes through changes caused by accident (Change in condition)				2. User/Owners conducts initial assessment	→ → → →	10. Stakeholders agree changes are mitigated and that normal operations can resume
Electronics Subsystem	1A. Electronics subsystem change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

# Work Status



# 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.