**Report on STPA ANALYSIS OF IROBOT (SLAM ROBOT)**

GROUP 2: Arpita Dasgupta, Sravya Konduru, Venkatesh Tummalapalli

**Table of Content**

1. **Introduction…………………………………………………………………..3**
2. **Accident Description…………………………………………………………3**
3. **CAST Analysis………………………………………………………………..3**
4. **STPA Analysis……………………………………………………………......4**
5. **STPA Analysis Step – 0……………………………………………………...4**
   1. **System Description…………………………………………………...5**
   2. **Accidents……………………………………………………………...5**
   3. **Hazards…………………………………………………………….....5**
   4. **Linking Hazards and Accidents…………………………………….6**
   5. **Safety Constraints…………………………………………………...6**
   6. **System Goals…………………………………………………………6**
   7. **Design requirements………………………………………………...7**
   8. **Control Structure……………………………………………………7**
6. **STPA Analysis Step – 1……………………………………………………..7**
   1. **Control actions………………………………………………………8**
   2. **Unsafe Control Actions Table……………………………………...8**
   3. **Corresponding Safety Constraints………………………………...9**
7. **STPA Analysis Step – 2…………………………………………………….9**
   1. **Control Structure with Process model……………………………10**
   2. **Casual Factors Table………………………………………………11**
8. **Summary…………………………………………………………………....11**
9. **References…………………………………………………………………..11**
10. **INTRODUCTION**

The accident leading to death of Macy, a 64-year-old lady, is analyzed using System Theoretic Process Analysis (STPA) from the XSTAMPP software.

1. **ACCIDENT DESCRIPTION**

Macy, a 64-year-old woman had an iRobot to supervise her. One fine day, her apartment was flooded with water because the shower faucet was broken. Macy tried to mop the floor. Macy changed the base station of iRobot. While mopping the floor, she suddenly fell down and shouted for help. The sensors sensed the message and sent the message to iRobot to take corresponding action. But iRobot was unable to move. The reason was Macy changed the position of base station and iRobot could not map its location, Macy’s location as well due to the water on the floor. IRobot took lot of time to remap the location and found Macy shouting for help. IRobot took stream of images of Macy and sent them to Jack (Macy’s son). Jack tried to contact iRobot to call nearby Emergency services. As iRobot took lot of time to remap, capturing images which consumed lot of charge and lead the system to shut down. Jack informed the urgency of help to the emergency services. Macy was admitted into the hospital. After two days, Macy died.

1. **CAST Analysis**:

CAST process involves six steps:

1. Identify the accident
2. Identify the hazards
3. Identify the safety constraints
4. Identify the proximal events
5. Draw the control structure
6. Analyze each component
7. **STPA Analysis:**

STPA (System theoretic Process Analysis):

Systems Theoretic Process Analysis is a new hazard analysis technique. This allows find more types of accident scenarios

Steps involved in STPA analysis:

Step – 0 Construct the control structure CAST analysis)

Step – 1 Identify unsafe control actions(UCAs)

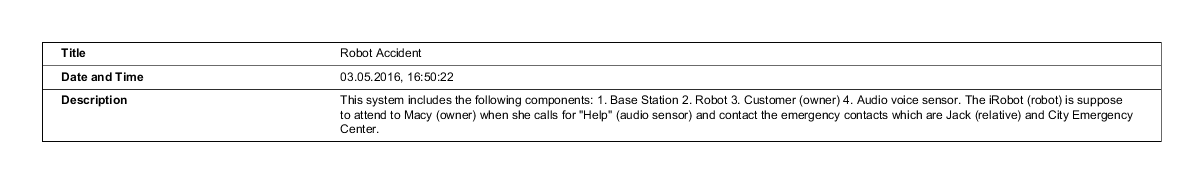
Step – 2 Causal Analysis

The system includes the following components:

1. Base station
2. Robot
3. Customer (owner)
4. Audio voice sensor

The iRobot (robot) is supposed to attend to Macy (owner) when she calls “Help” (audio sensor) and contact the emergency contacts which are Jack (relative) and City Emergency Center in this case.

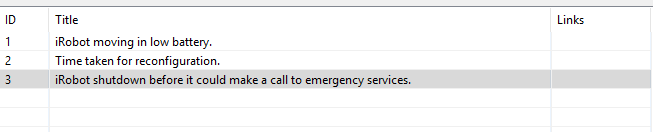
To analyze the accident both CAST analysis and STPA analysis were carried out using XSTAMP tool.

1. **STPA Analysis Step – 0: (CAST Analysis)**   
   **5.1 SYSTEM DESCRIPTION**

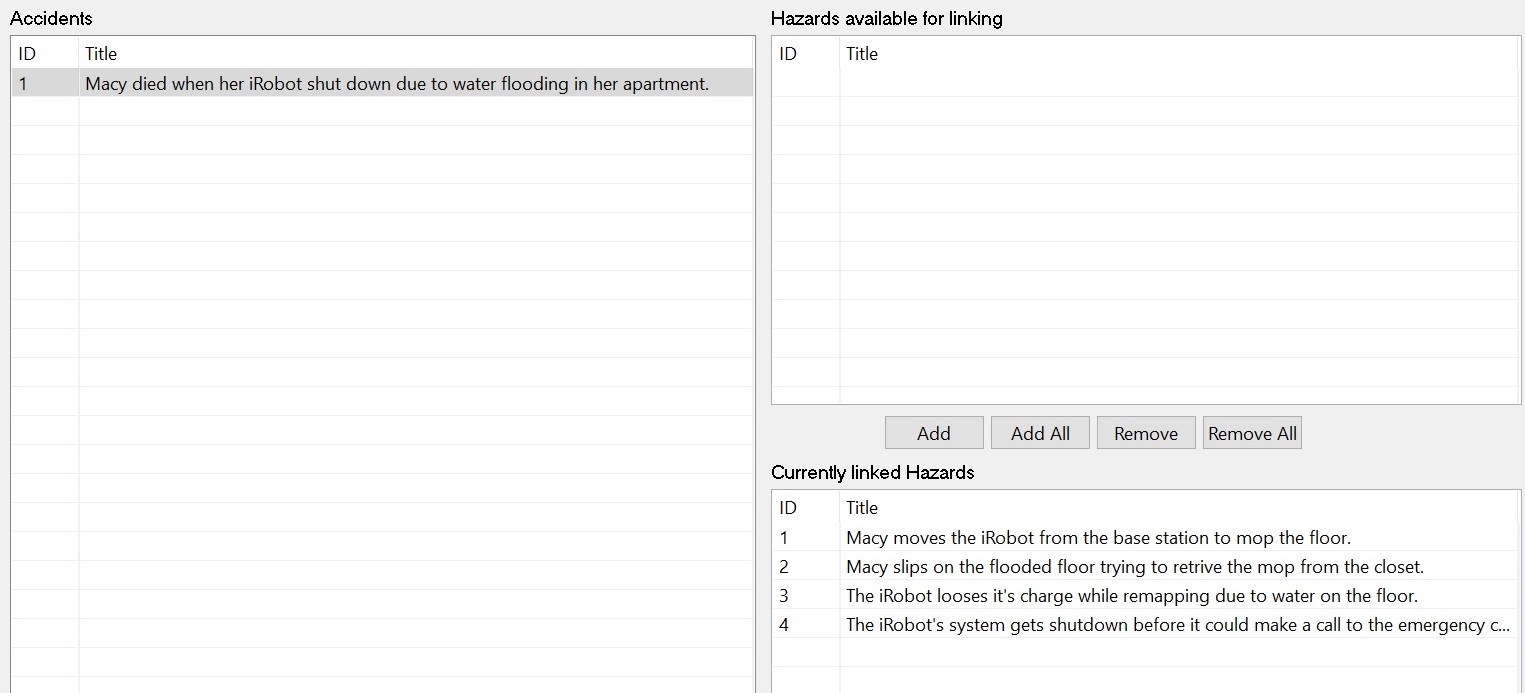
**5.2 ACCIDENT**

A 64 old woman Macy died when her iRobot shut down due to water flooding in her apartment.

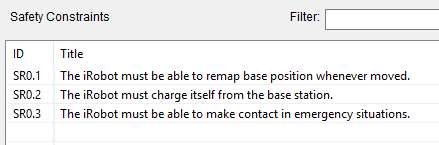
**5.3 HAZARDS**

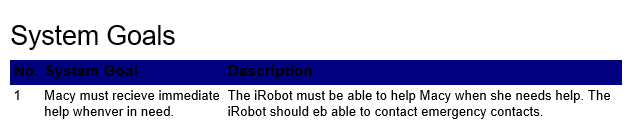


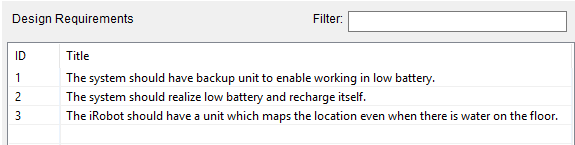
* 1. **Linking Hazards and actions**

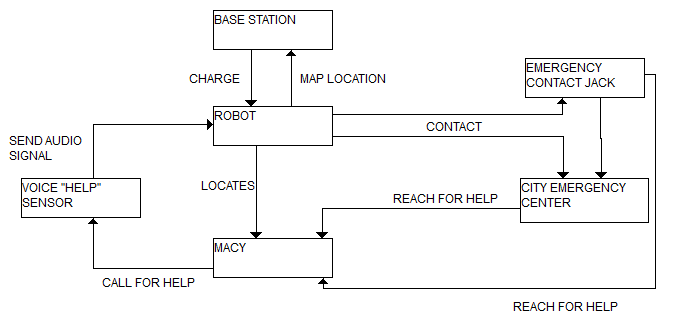


**5.5 SAFETY CONSTRAINTS**



**5.6 SYSTEM GOALS**

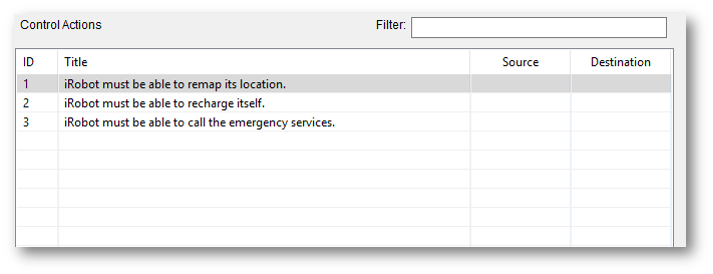
**5.7 DESIGN REQUIREMENTS**

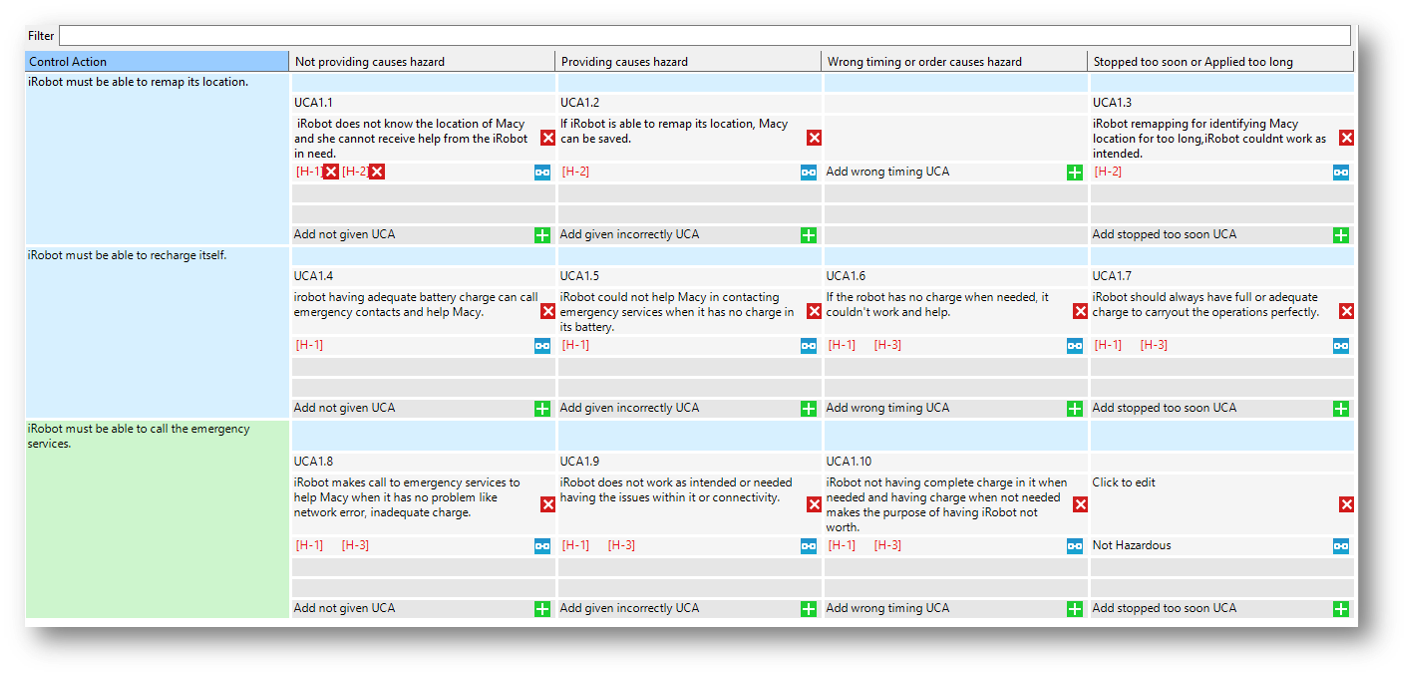
**5.8 CONTROL STRUCTURE**

1. **STPA Analysis Step – 1**:

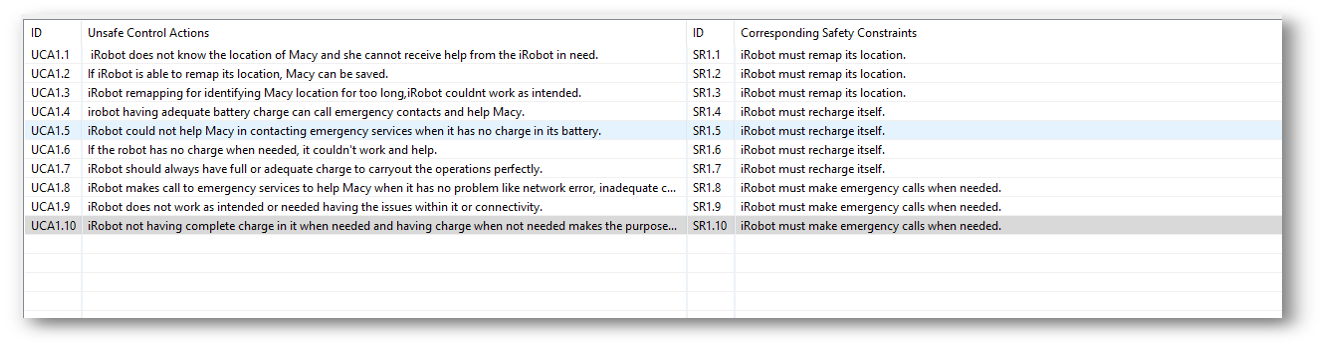
In this step, Unsafe control actions are determined and corresponding safety constraints are linked with it.

**6.1 Control Actions:**

**6.2 Unsafe Control Actions Table:**



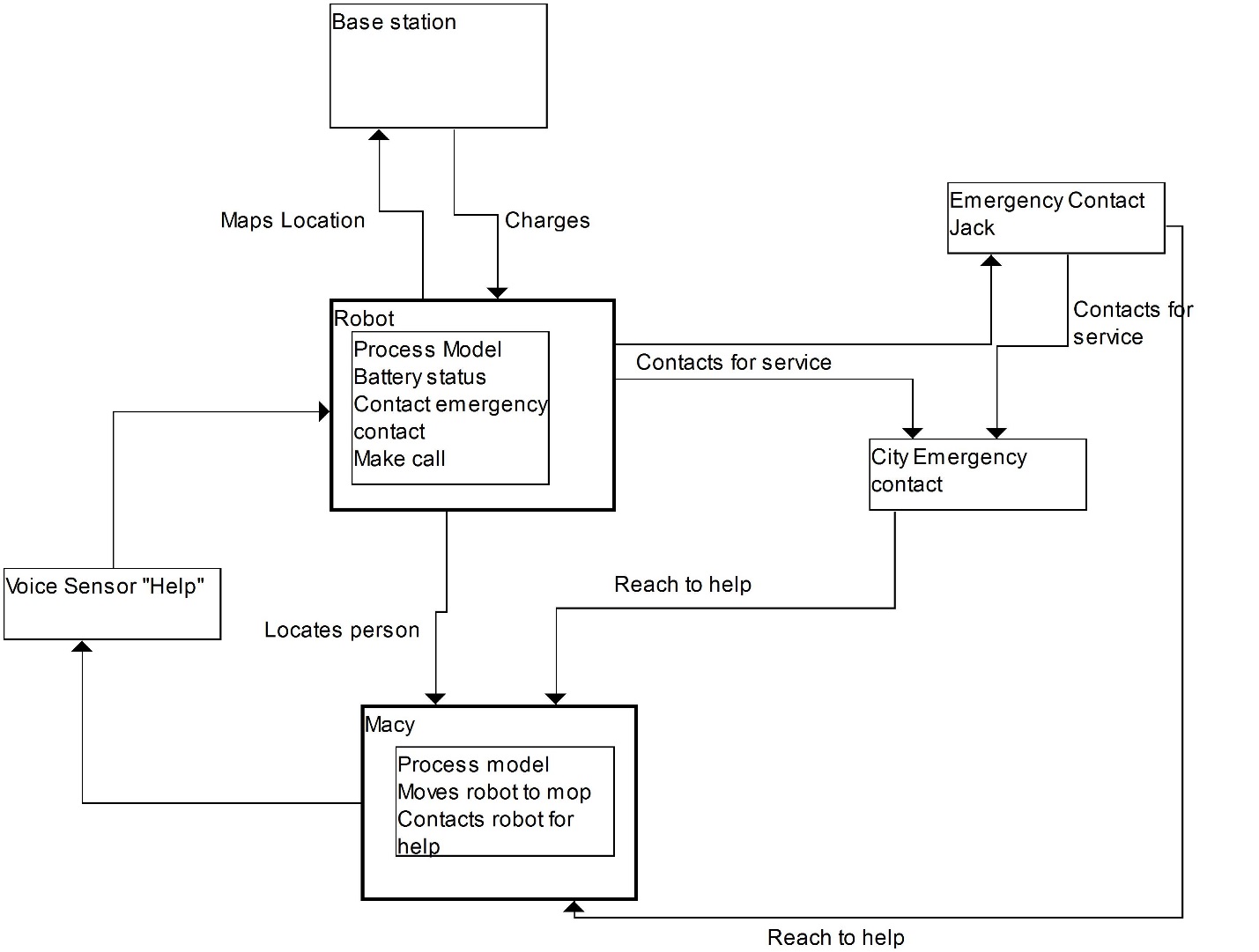
**6.3 Corresponding Safety Constraints:**

****

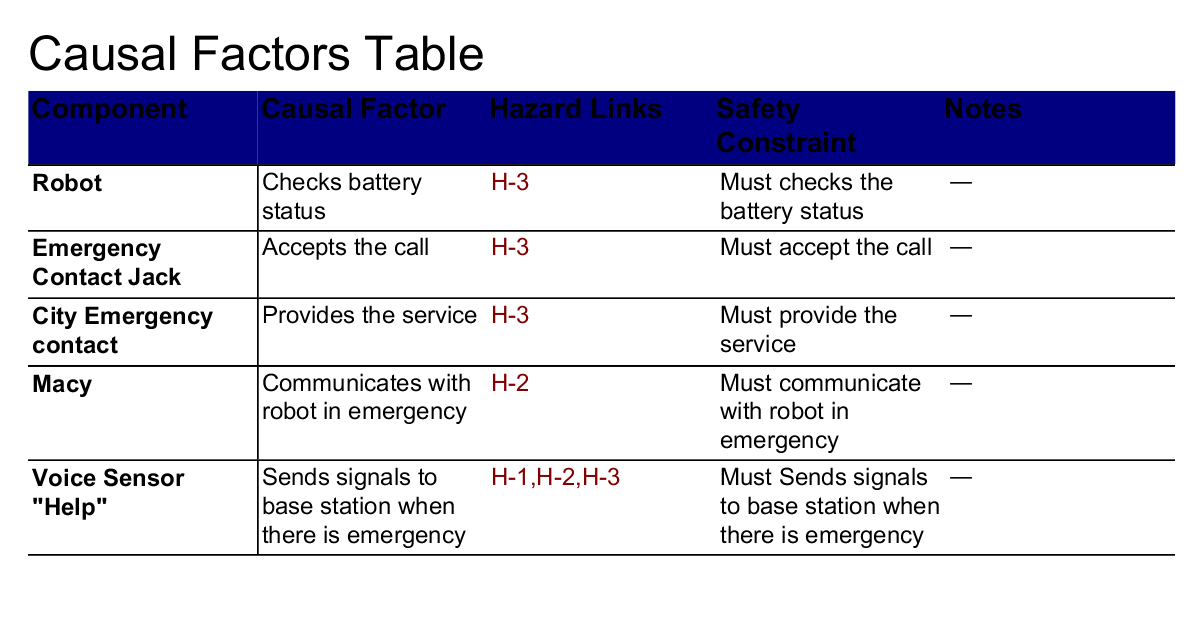
1. **STPA Analysis Step – 2:**

In this step, process model is included in the control structure. A casual factors table is also mapped in this step.

**7.1 Control Structure with Process model**:



**Casual Factors Table:**

****

1. **Summary:**

The STPA analysis provides information about each and every control actions that could lead to accident and corresponding safety constraints.

1. **References:**

1.https://mitpress.mit.edu/sites/default/files/titles/free\_download/9780262016629\_Engineering\_a\_Safer\_World.pdf

2. https://blog.udemy.com/xampp-tutorial/