**Software Engineering Program**

**School of Science and Computer Engineering**

**University of Houston Clear Lake**

**SWEN 5532.01 Software Safety**

**Systems Theoretic Process Analysis (STPA) on Tragic Death from Technology**

**Group-3**

**Submitted by**

**Pujitha Muppireddi**

**Chandrakanth Koyyada**

**Ravindranath Reddy Thiyaagura**

**Table of Content**

* **Introduction……………………………………………………………………………4**
* **CAST Analysis………………………………………………………………………...4**
* **Accident**
* **Hazards**
* **Design For Safety……………………………………………………………………. 4**
* **Interlock**
* **Fault tolerance**
* **STPA Analysis Step – 0………………………………………………………………..5**
  + **System Description**
  + **Accident**
  + **Hazard**
  + **Linking Hazards and Accidents**
  + **Safety Constraints**
  + **System Goals**
  + **Design requirements**
  + **Control Structure**
* **STPA Analysis Step – 1………………………………………………………………10**
  + **Control Actions**
  + **Unsafe Control Actions Table**
  + **Corresponding Safety Constraints**
* **STPA Analysis Step – 2………………………………………………………………11**
  + **Control Structure with Process Model**
  + **Causal Factors Table**
* **Conclusion……………………………………………………………………………14**
* **References……………………………………………………………………………14**

# Introduction:

Mille John, an 85 year old lady living in a old age home (Webster) innovatively brought a Slammie Robot to help her whenever she is in trouble. On December 21, 2013 about 2.30 PM, Mille fell down due to pain in the chest and called the Slammie for help but it was helpless at that time due to failure of communication protocol and failed in contacting the front desk to convey the emergency information which leads to the Accident.

Based on the incident we did CAST (Casual Analysis System Theory) analysis followed by STPA (System Theoretic Process Analysis) analysis in order to find the reasons for the tragic death.

## CAST Analysis:

After the sequence of steps in CAST analysis we identified the following things as reasons for the incident.

* Accident(Loss)
* A-1: On December 21st 2013 Mille John, an 85 year old lady had died in a old age home (Webster) due to heart attack.
* Hazard
* H-1: Failure of communication protocol.
* H-2: Equipment Failure

# Design for Safety:

In order to maintain and use the Slammie efficiently, we identified the following safety principles through which we can overcome the failures that occurred in this scenario.

INTERLOCK:

* Interlock is used to enforce a sequence of actions or events
* Slammie Robot was designed by using Interlock in a way that it should make calls to emergency first and relatives next.

Fault Tolerance:

* Slammie Robot was designed with a failsafe protocol which will be useful when something went wrong
* If the primary system fails it will pass failure warnings and indicators so that the fault tolerance can get activated.

After CAST we done STPA with different levels as follows

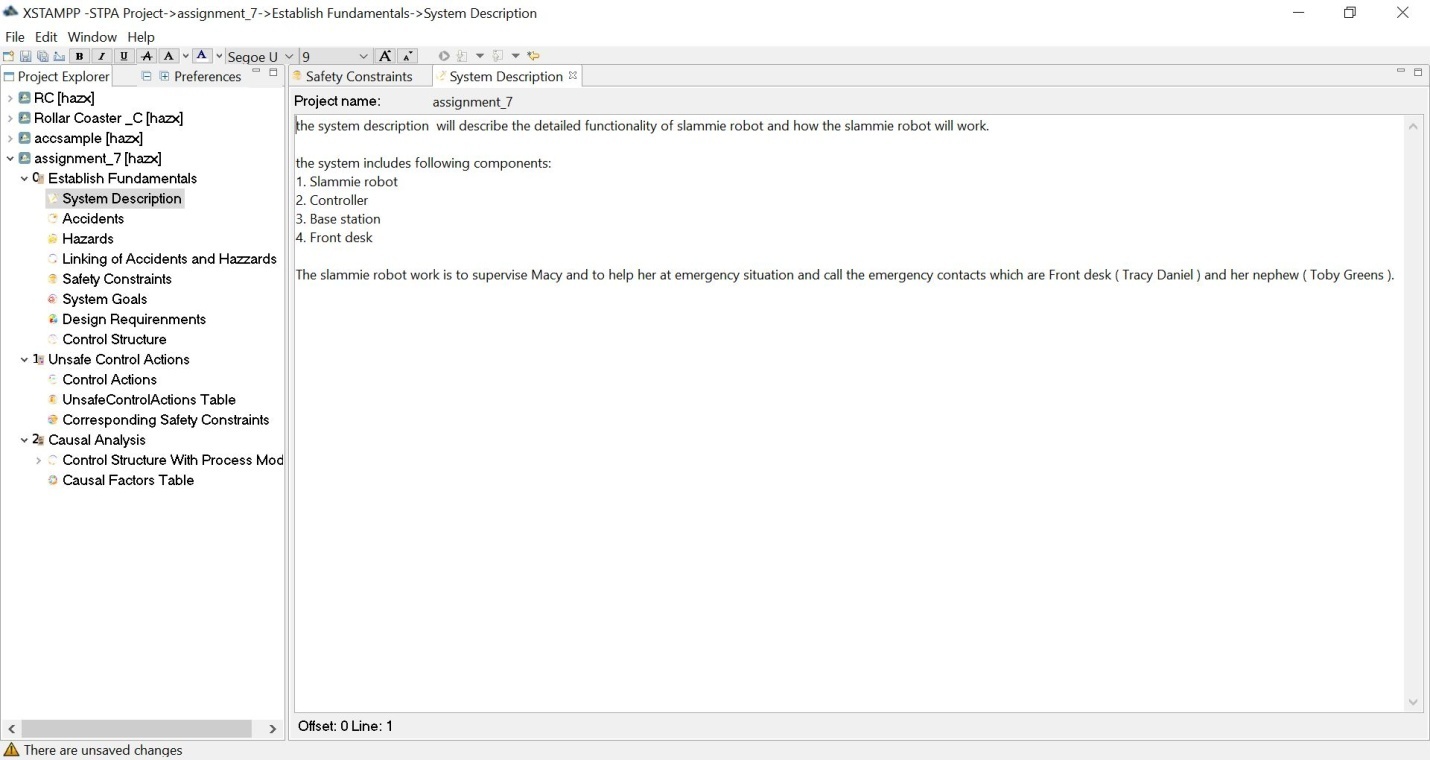
# System Theoretic Process Analysis (LEVEL 0):

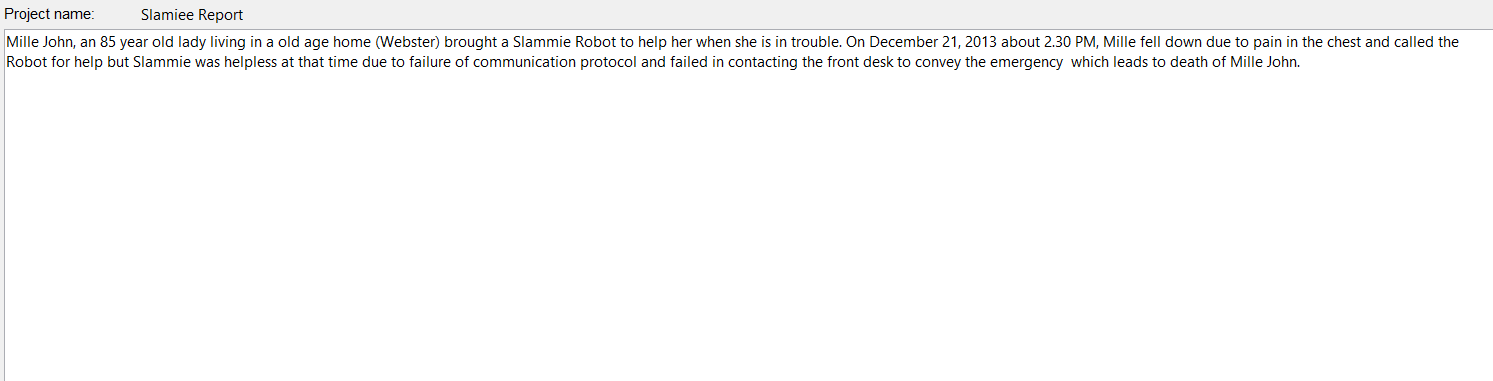
System Description: The system description will describe the detailed functionality of the Slammie robot and how the Slammie robot will work.

The System includes the following components:

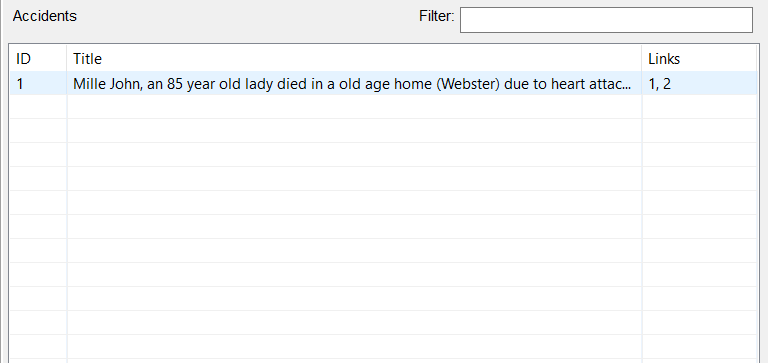
1. Slammie robot
2. Controller
3. Base Station
4. Front Desk

The Slammie robot work is to supervise Macy and to help her at emergency situation and call the emergency contacts which are front desk (Tracy Daniel) and her nephew (Toby Greens).

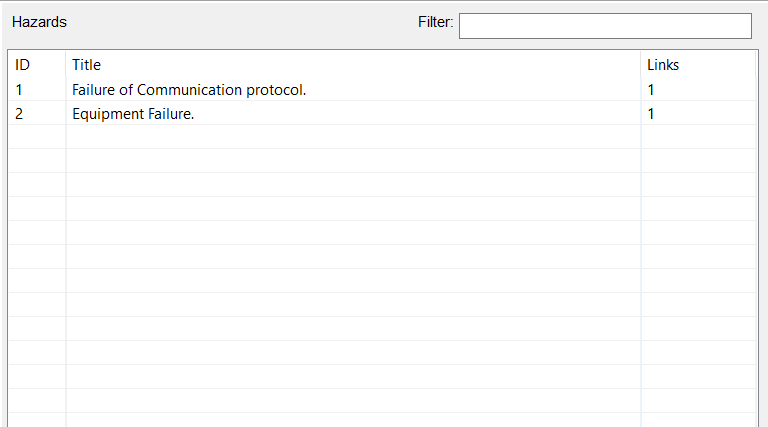




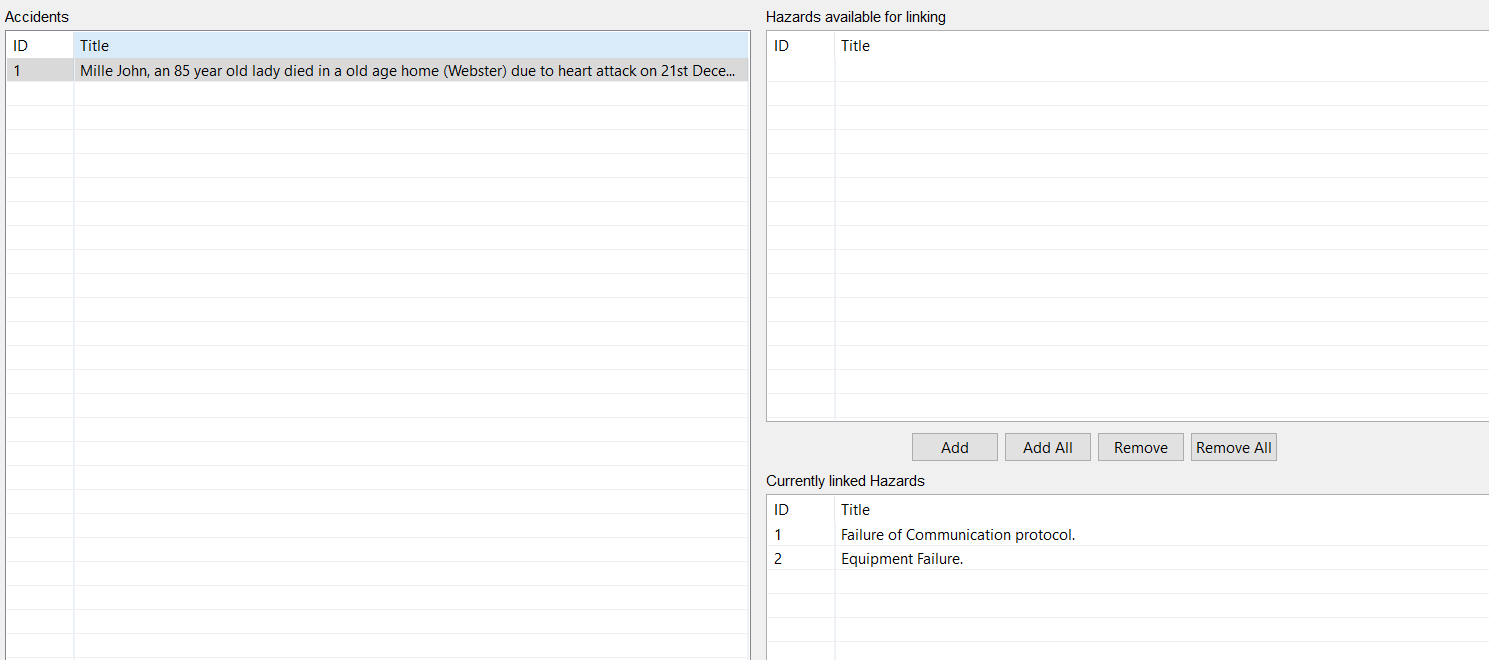
Accidents: Accident will tell about the incident which was happened and leads to death.



Hazards: Hazards will tell the reasons for the accident happened.

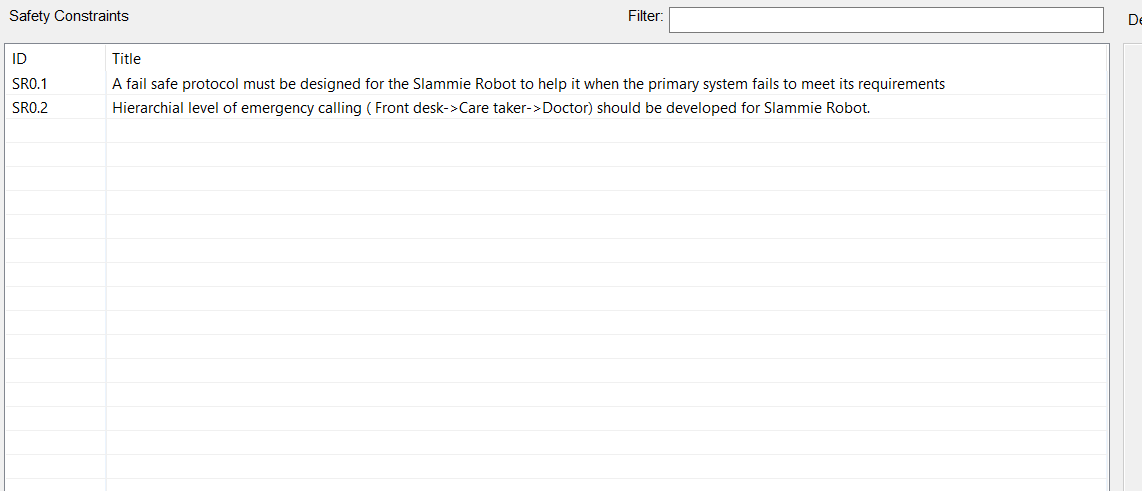


Linking of accidents and hazards: We link the Accidents and Hazards by using this Xstamp analysis.

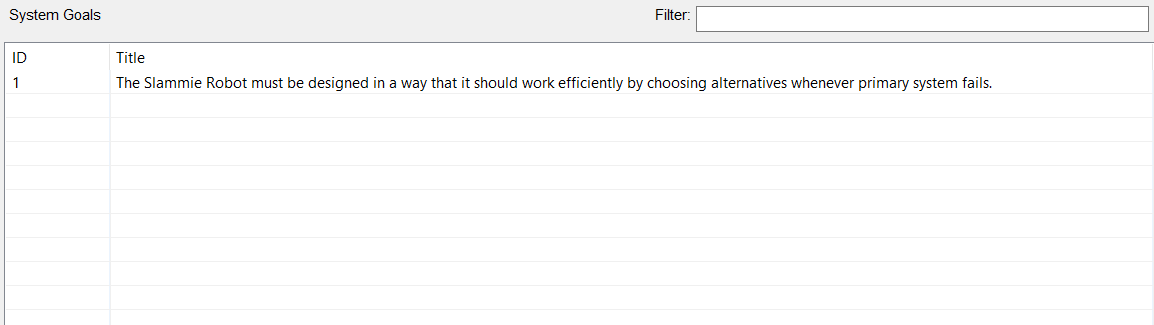


Safety Constraints:

To maintain the safety in the Slammie we need to design it by considering the following constraints

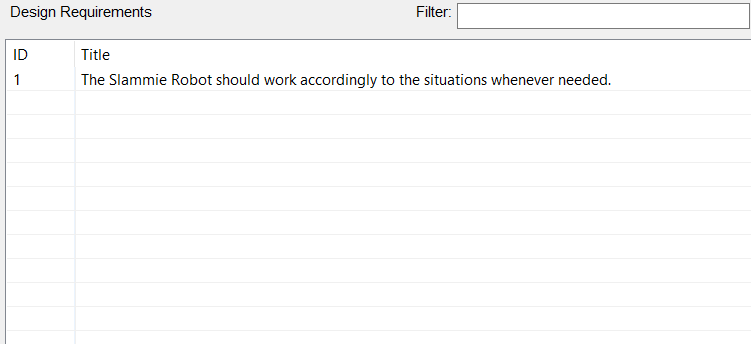


System Goals: System Goal will tell the main achievement of the Slammie robot.



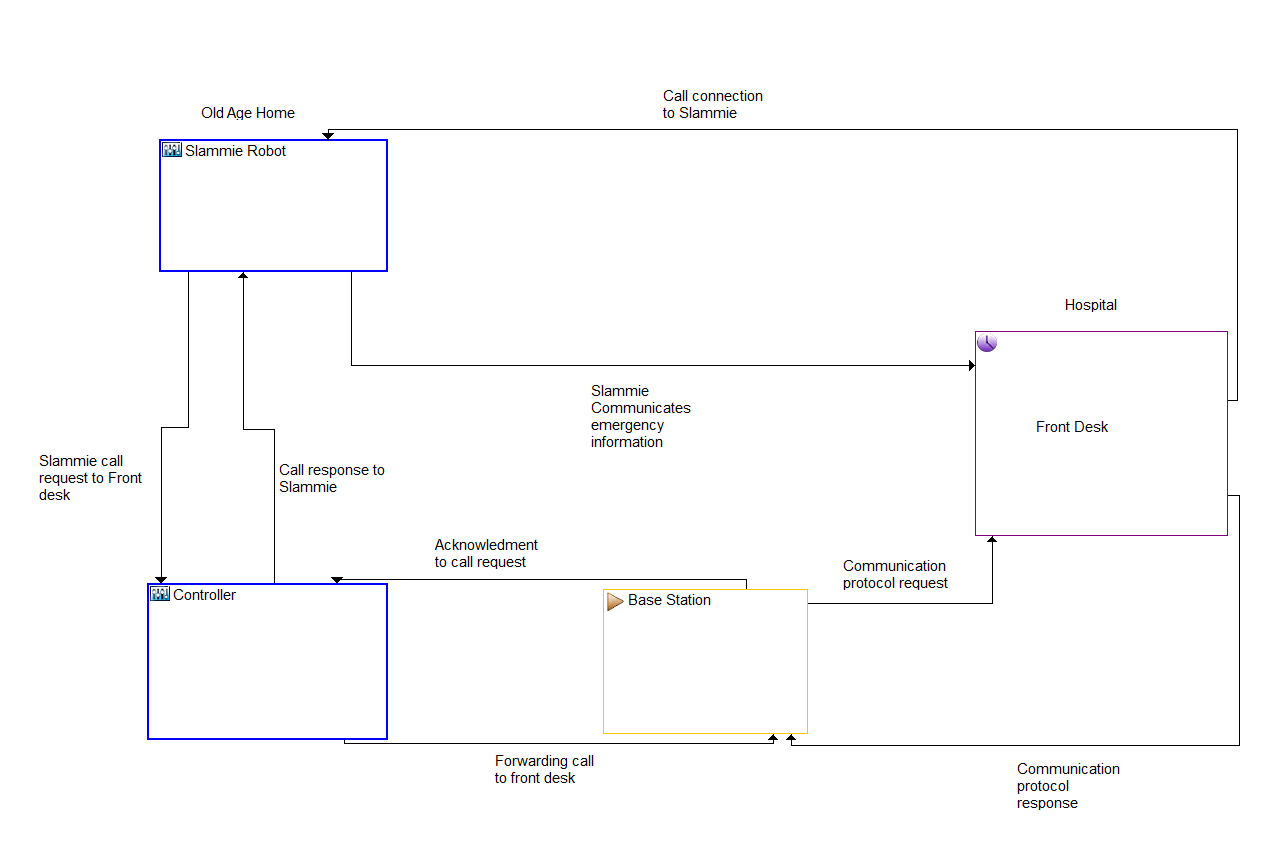
Design Requirements:

The main Design requirement for the Slammie is it should work efficiently and act accordingly to the emergency situations to help the people.



Control Structure:

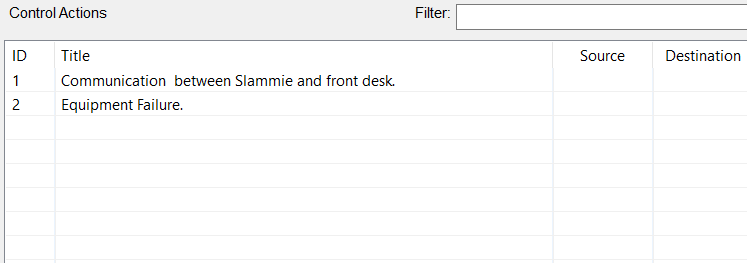
We designed the following control structure and it will explain the main activities of each and every component of the system.



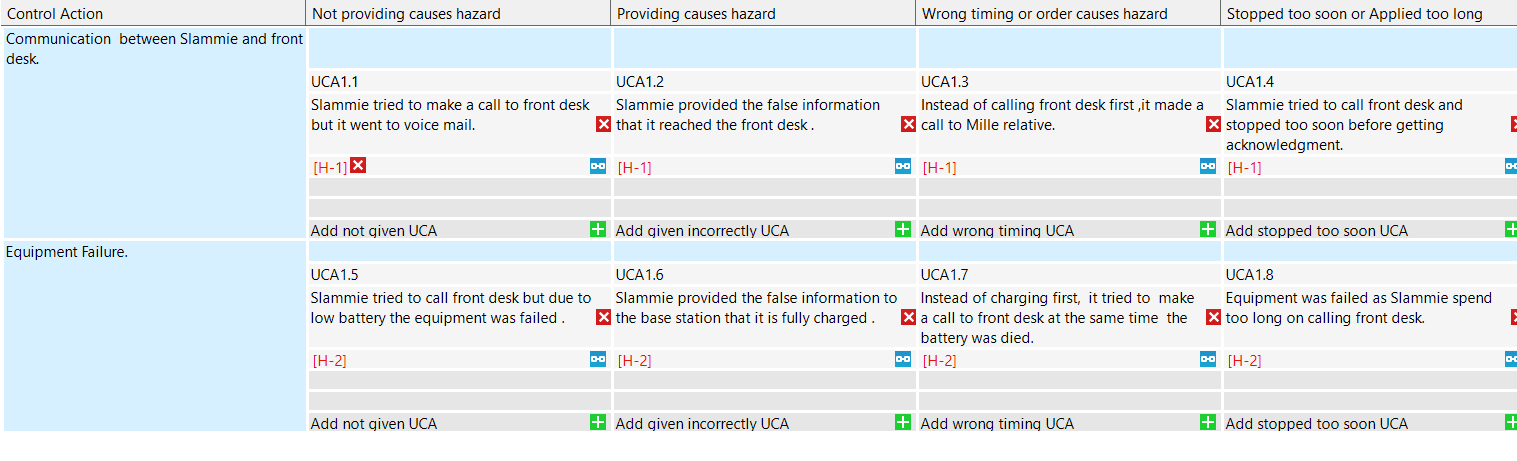
## 

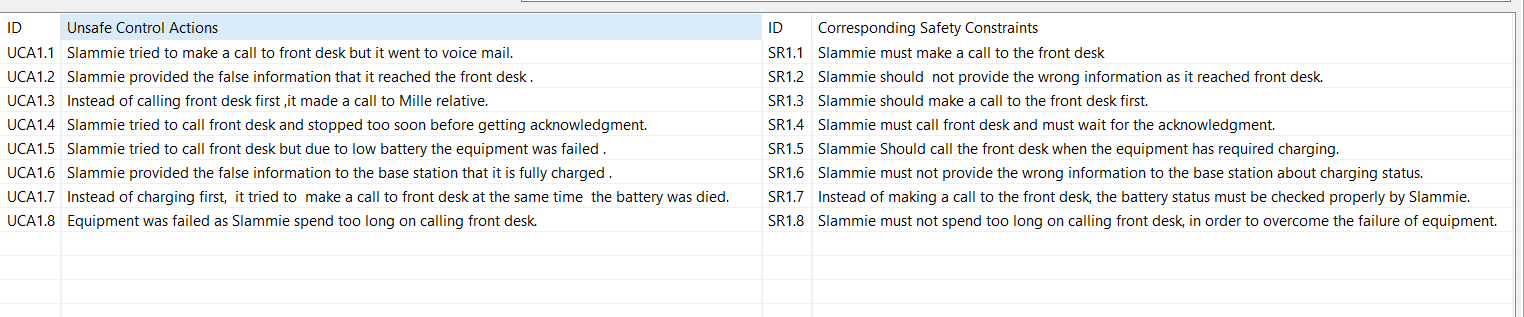
## System Theoretic Process Analysis(Level 1):

Control Actions: The control actions will tell what type of actions to be performed by the system.



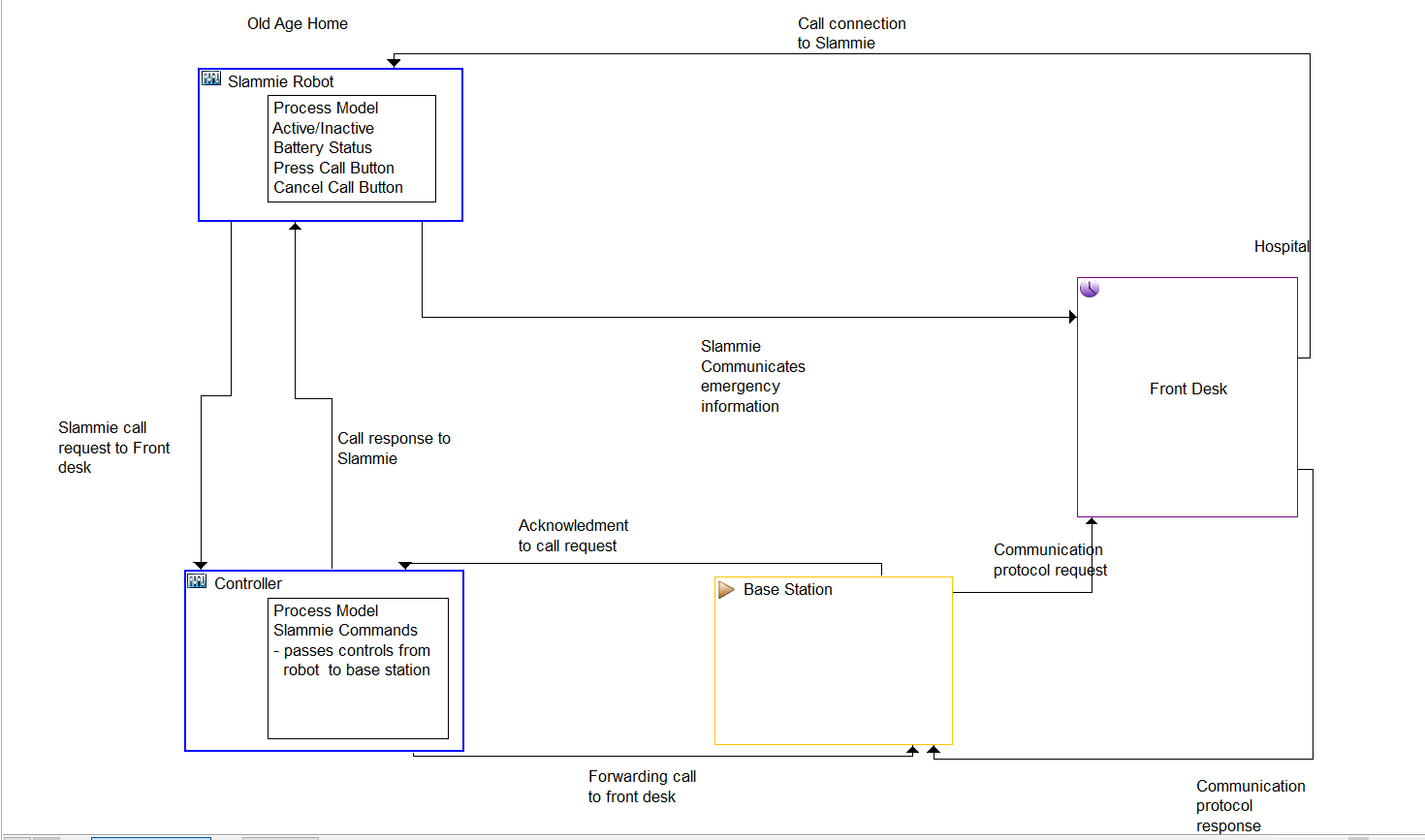
Unsafe Control Actions Table: This table tells about the detail description of how the control actions performed by the system which causes hazard.



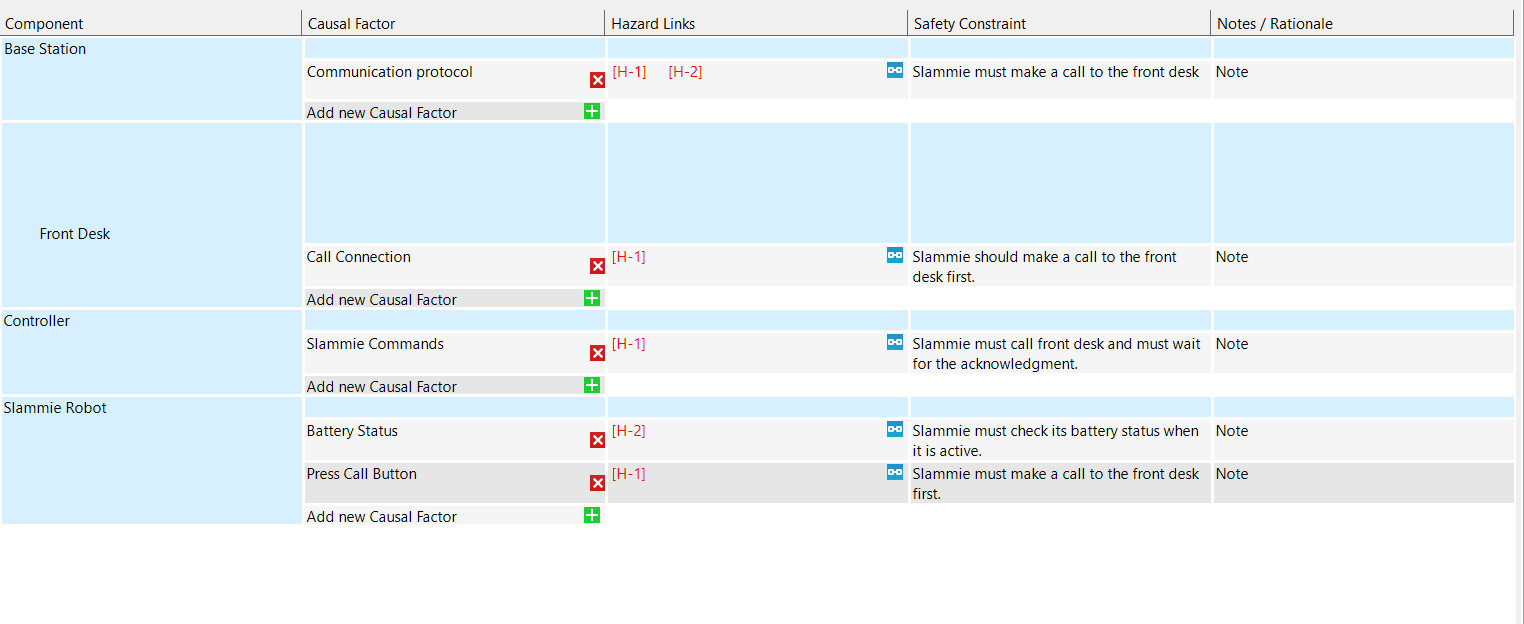
Corresponding Safety Constraints: The Corresponding Safety Constraints are to be included in the system performance so that hazard or accident will not happen. 

## System Theoretic Process Analysis (Level 2):

Control Structure with process model: The system includes the control structure with the process model as that it will tell the operations that are performed.



Causal Factors Table: This table tells about the operations performed by each and every component in the system and it will also describe their corresponding Hazards and Safety constraints.



# Conclusion:

Finally, we can conclude that the Slammie must be designed with the new control structure and fail safe protocols in order to avoid the local network issues which leads to the loss of lives.

# References:

* <https://mitpress.mit.edu/sites/default/files/titles/free_download/9780262016629_Engineering_a_Safer_World.pdf>