**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 SLAMMIE ROBOT FAILURE**

**Group-1**

**Submitted by**

**Jaswanth Potini**

**Sandeep Kumar Reddy Eruvaram**

**Michael Findler**

**05/04/2016**

Table of Contents

1. [Introduction…..………………………………………………………………………3](#_Toc418434855)

2. [CAST Analysis.………………………………………………………………….…...3](#_Toc418434856)

2.1 [Accident………………………………………………………………..………..3](#_Toc418434857)

2.2 [Hazzard……………………………………………………………………..........3](#_Toc418434858)

3. Design for Safety………………………………………………………………….….4

4. STPA Analysis using XSTAMPP………………………………………………….....5

4.1 System Description………………………………………………………………5

4.2 Linking Accidents and Hazards…………………………………………………5

4.3 Safety Constraints………………………………………………………………6

4.4 Control Structure……………………………………………………………….6

4.5 Control Actions…………………………………………………………………7

4.6 Unsafe Control Actions Table…………………………………………………..7

4.7 Corresponding Safety Constraints………………………………………………7

4.8 Control Structure with Process Model………………………………………….8

4.9 Causal Factors……………………………………………………………….....9

5. Conclusion…………………………………………………………………….…….10

6. References…………………………………………………………………………..10

1. **Introduction:**

Ravi living in The Wolf Creek Apartments was suffering from heart disease. He was supervised by a doctor for past few years. He was also assisted by Chandu (a SLAMMIE Robot) which takes care of Ravi in his daily needs.

On December 31st, 2015, while Ravi was doing some work he suddenly felt pain in his chest and had a heart stroke. Ravi then sends an indication to chandu. Chandu tries to contact the doctor. Chandu could not make a call to the hospital due to bad internet service. Finally Ravi died with massive heart stroke.

1. **CAST Analysis:**
   1. **Accident:**

A1: Death of Ravi due to SLAMMIE Robot failure.

* 1. **Hazard:**

H1: The poor network connection.

H2: Fluctuations in the internet speed.

H3: Equipment failure.

H4: Congestion in the network.

1. **Design for Safety:**

**Monitoring:**

The Robot should be monitored or checked regularly to identify the defects. Monitoring is done to detect equipment malfunction. Detection of a hazardous event or condition is done by monitoring.

**How monitoring used in the system?**

Monitoring is done by having sample results of the other working system. It is to ensure that the system works fine and implement it to the system that they are designing. This does not work well in our system as the system failed to connect to the network.

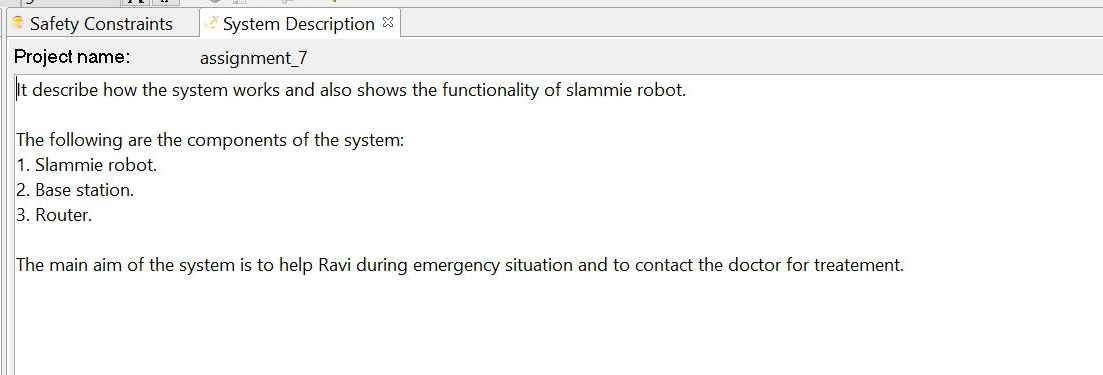
**Fault Tolerance:**

The Robot must be designed to tolerate faults so they have no or little negative impact.

**How fault tolerance used in the system?**

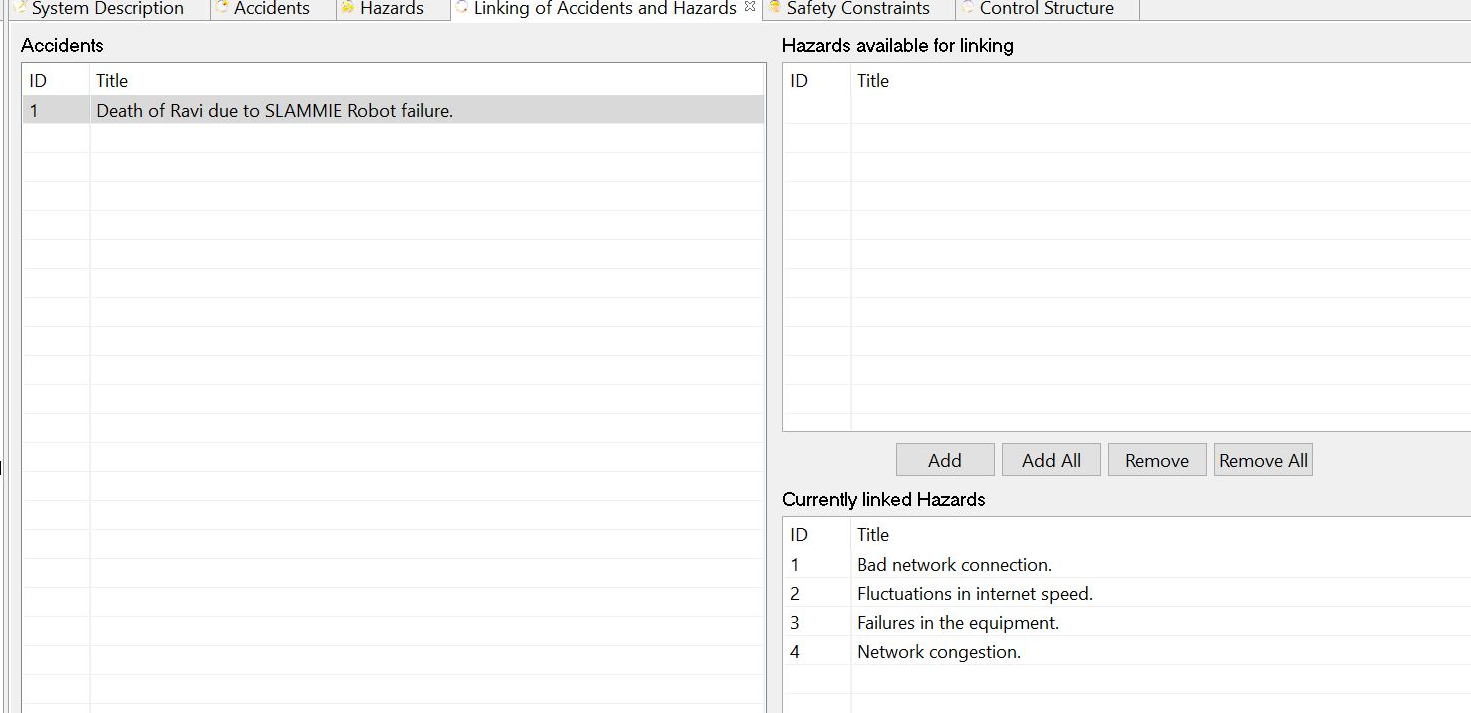
The Robot is designed in such a way that, during poor network connection it should switch to an alternative network connection if provided. This design feature has not worked in our system as there is no alternative connection in the house.

1. **STPA Analysis using XSTAMPP:**
   1. **System Description:**

****

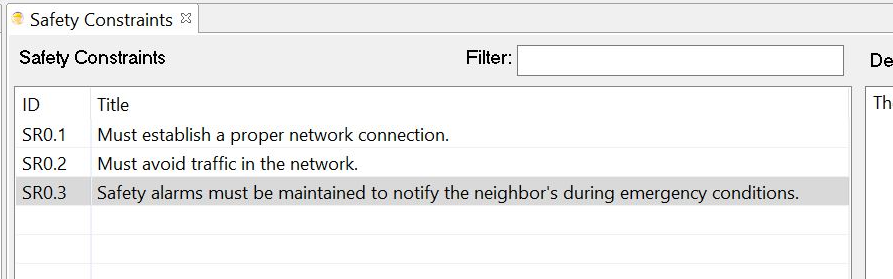
* 1. **Linking Accidents and Hazards:**

Link all the hazards that are the causes for an accident.

****

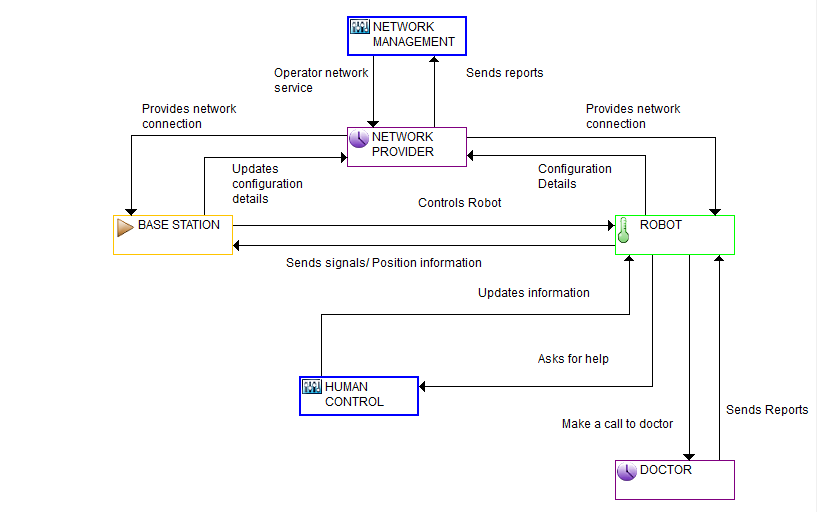
* 1. **Safety Constraints:**

Safety constraints are provided to ensure the safety of the system.

****

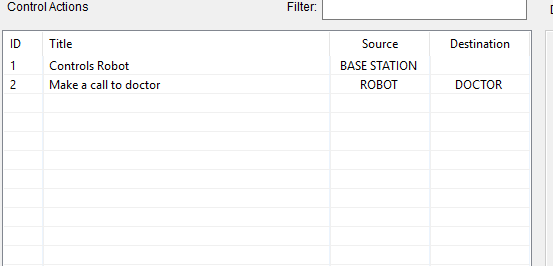
* 1. **Control Structure:**

It describes the system work model and the connectivity of all the components in the system.

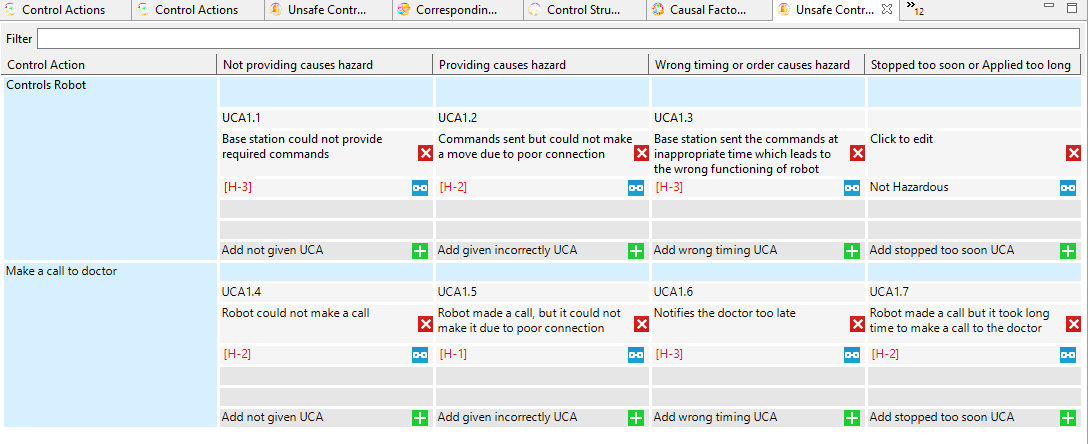
****

* 1. **Control Actions:**

Control actions perform some operation based on some input from the system.

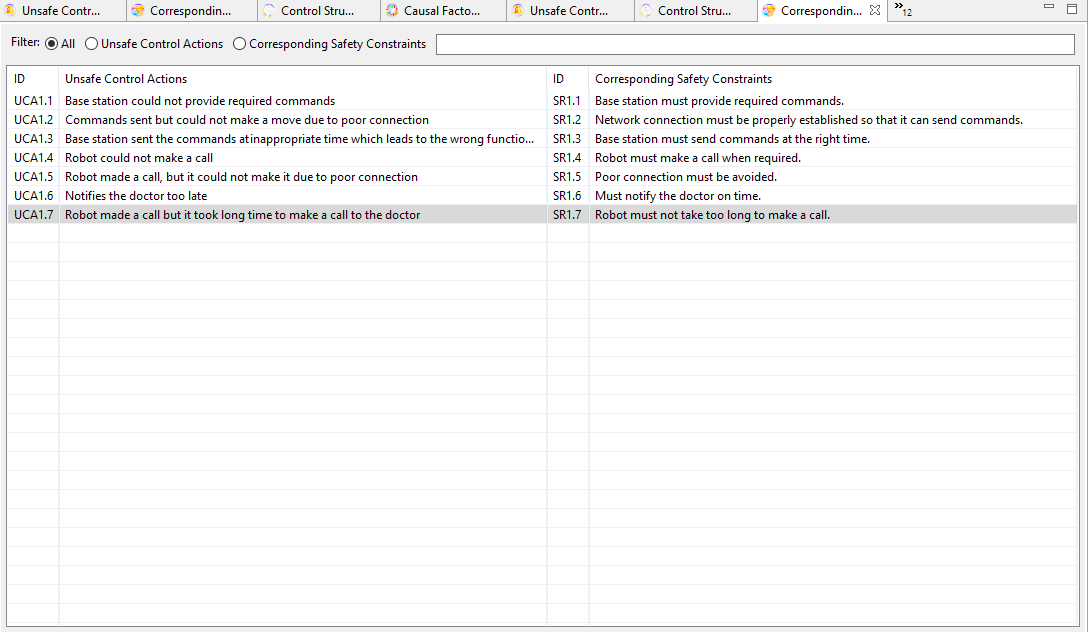
****

* 1. **Unsafe Control Actions Table:**

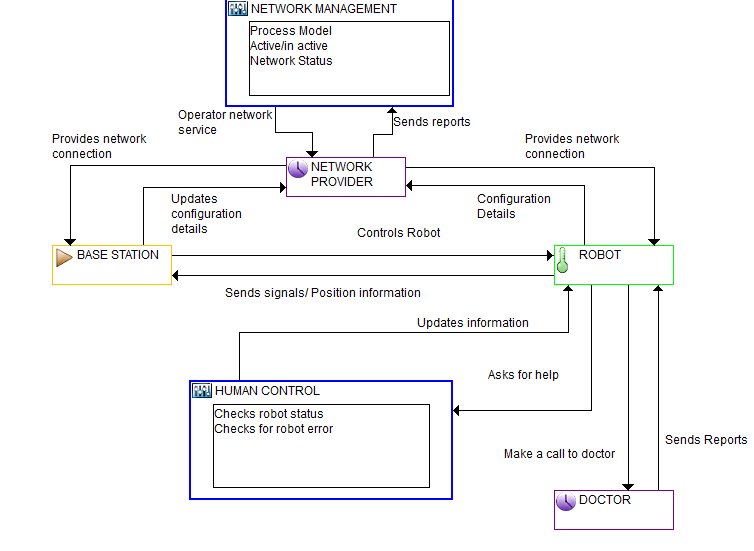
****

* 1. **Corresponding Safety Constraints:**

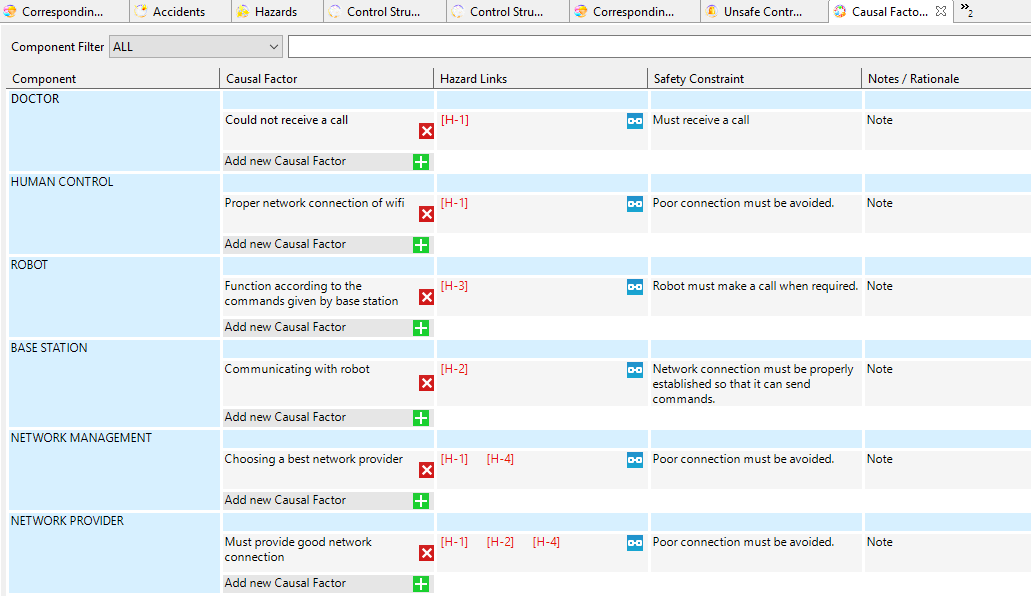
For all the unsafe control actions, the safety constraints are identified to provide the safety to the system.

****

* 1. **Control Structure with Process Model:**

****

* 1. **Causal Factors:**



1. **Conclusion:**

The accident occurred due to the poor network connection. Safety must be taken into account during design phase.

1. **References:**
2. [**https://mitpress.mit.edu/sites/default/files/titles/free\_download/9780262016629\_Engineering\_a\_Safer\_World.pdf**](https://mitpress.mit.edu/sites/default/files/titles/free_download/9780262016629_Engineering_a_Safer_World.pdf)