A-STPA-Report

SLAMMIE ROBOT STPA1

Title	SLAMMIE ROBOT STPA1
Date and Time	08.09.2016, 11:30:22
Description	On April 1st, 2016 at the Lake Haven Independent Living Apartments (1051 Columbia Memorial Pkwy, Kemah, TX 77565), the UHCL SLAMMIE Robot had a communication failure; resulting in the death of Millie Kiesewetter (age 98). System Description : The system description will describe the detailed functionality the SLAMMIE robot and how it works. The system includes the following components: SLAMMIE robot -Immediately contacts Base station in any emergency situations -Communicates with Base station -Maps the surroundings daily Base Station -Charging station for SLAMMIE robot -calls immediately to front desk, as SLAMMIE reports External Sensors -Ping Location (Reports SLAMMIE) Internal Sensors -Detects sound -Maps surroundings Millie Kiesewetter -Contact Robot for help -move Robot during mopping

Accidents

No.	Title	Description	Related Hazards
1	Death of Millie Kiesewetter	On April 1st, 2016 at the Lake Haven Independent Living Apartments (1051 Columbia Memorial Pkwy, Kemah, TX 77565), the UHCL SLAMMIE Robot had a communication failure; resulting in the death of Millie Kiesewetter (age 98).	1, 2, 3

Hazards

No.	Title	Description	Related Accidents
1	Loss of communication with Base Station	Loss of communication with Base Station as the SLAMMIE got stuck in the bathroom. Both the bathroom and bedroom doors had been closed by Millie which blocked the signals	1
2	Communication signals got blocked	Communication signals got blocked as SLAMMIE got stuck inside the bathroom. There are some distractions as SLAMMIE was way inside the bathroom. Bathroom door was locked by MILLIE, so communication signals became weak.	1
3	Floor was slippery due to water from the flower vase	Millie hears a sound of an object breaking in the living room. She saw that it was the flower vase which has blown off the table due to the breeze coming from veranda [Millie kept the veranda door open since it was pleasant outside]. The water in the vase made a very slippery tile floor.	1

Safety Constraints

ID	Safety Constraint	Description
SC0.1	SLAMMIE shall not Loss Communication with Base Station	SLAMMIE shall not Loss Communication with Base Station. It should have communication with the base station all the time.
SC0	Communication signals shall not get blocked anytime	Communication signals shall not get blocked, the communication should be maintained between the SLAMMIE and the BASE STATION all the time.
SC0.3	Millie Kiesewetter should maintain distance from all hazardous objects	Floors should not be slippery, because moisture on the floor makes someone fall on the floor.

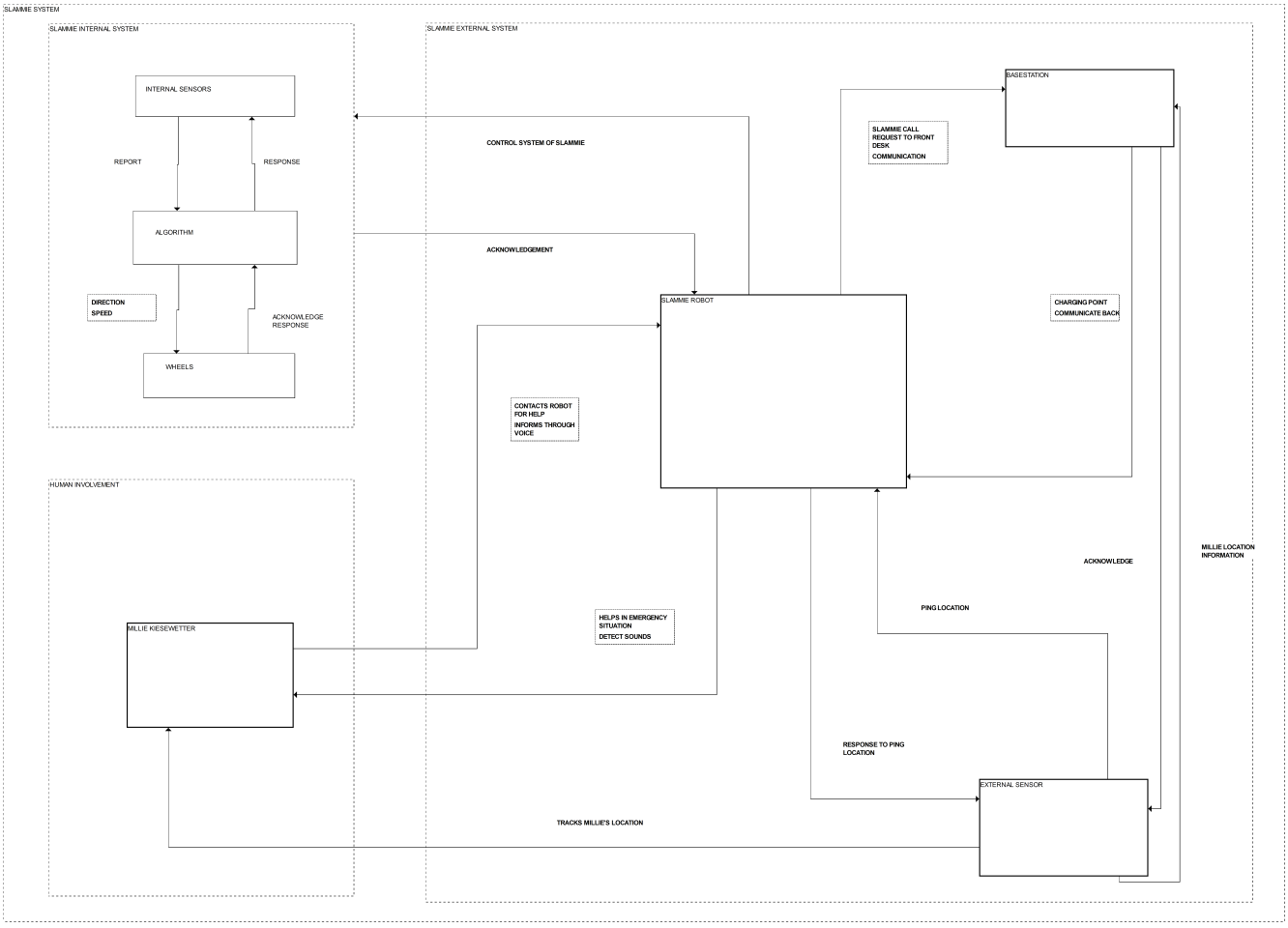
System Goals

No.	System Goal	Description
1	SLAMMIE ROBOT should work efficiently by choosing alternatives whenever primary system fails	There should be alternatives in order to prevent accidents. SLAMMIE ROBOT should find alternatives whenever primary system fails
2	Protect Millie kiesewetter all points of time	The goal of Slammie robot and its system is to protect Millie kiesewetter from emergency situations
3	Communication should be maintained	Communication should be maintained between Slammie robot and base station all points of time

Design Requirements

No.	Design Requirement	Description
1	The Slammie Robot shall work accordigly to the situations whenever needed	The main Design requirement for the Slammie is it should work efficiently and act accordingly to the emergency situations to help the Millie.
2	Slammie Robot requires to protect customer by alerting in all emergency conditions.	Slammie Robot requires to protect customer by alerting in all emergency conditions.

Control Structure Diagram



Control Actions

No.	Control Action	Description
1	SPEED	Speed and wheel controls are managed by the slammie algorithm
2	DIRECTION	Slammie robot have directions which is managed by the algorithm
3	PING LOCATION	Ping location is nothing but indicating a particular place to the Slammie robot
4	RESPONSE TO PING LOCATION	Slammie reply to the external sensor about the location
5	COMMUNICATE BACK	Communicating from base station to slammie robot
6	CHARGING POINT	Base station is used as the charging point for Slammie robot
7	COMMUNICATION	Slammie Robot has a communication network with the base station
8	SLAMMIE CALL REQUEST TO FRONT DESK	In emergency situation, slammie robot makes a call request in order for the base station to call the front desk
9	INFORMS THROUGH VOICE	Millie needs to moves the robot in order to mopp the surroundings
10	CONTACTS ROBOT FOR HELP	Millie contacts robot in any emergency conditions
11	DETECT SOUNDS	Slammie robot has an internal sensors which detects sound of millie
12	HELPS IN EMERGENCY SITUATION	Slammie robot detects sound of millie and helps by reporting it to the emergency services
13	CONTROL SYSTEM OF SLAMMIE	Its consists of algorithm which helps slammie to work accordingly
14	TRACKS MILLIE'S LOCATION	External sensors tracks millie and pings location to slammie robot in emergency
15	ACKNOWLEDGEMENT	Accepting and responding to slammie robot
16	ACKNOWLEDGE	Accepting and responding to external sensors
17	MILLIE LOCATION INFORMATION	External sensor pings location of millie to base station as well

Unsafe Control Actions

Control Action	Not providing causes hazard	Providing causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long
SPEED				

Control Action	Not providing causes hazard	Providing causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long
	UCA1.1 SLAMMIE tried to move but got stuck onto the towel which made it unable to move [H-1]	UCA1.2 SLAMMIE provided information that it was moving instead of not [H-1]	UCA1.3 SLAMMIE started speeding the wheels faster as it was not moving forward [H-1]	UCA1.4 SLAMMIE stopped working too soon as the battary got drained due to speeding [H-1]
DIRECTION	UCA1.5 Robot tried to find direction to the base station but lost communication with base station [H-2]	UCA1.6 SLAMMIE provided false information that it was moving towards base station [H-2]	UCA1.7 SlAMMIE robot had wrong timing entering into the bathroom [H-2]	UCA1.8 Robot stopped working too soon as it got direction less [H-2]
PING LOCATION	UCA1.9 SLAMMIE got multiple pings at a time, and got muddled [H-1,H-2]	UCA1.10 Sensor provided false information and pings wrong location [H-1,H-2]	UCA1.11 Instead of examine the location, SLAMMIE started mapping the apartment [H-1,H-2]	UCA1.12 SLAMMIE took too long in reacting to the sensors location alert [H-1,H-2]
RESPONSE TO PING LOCATION	UCA1.13 SLAMMIE Inspects only one location among multiple alerts. [H-1]	UCA1.14 Sensor provided false information saying false alarm [H-1]	UCA1.15 Instead of examine the location, SLAMMIE started mapping the apartment [H-1]	UCA1.16 SLAMMIE took too long in reacting to the sensors location alert [H-1]
COMMUNICATE BACK				UCA1.20 Base station stopped too soon in communicating with Slammie [H-1]

Control Action	Not providing causes hazard	Providing causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long
	UCA1.17 Base Station tried to communicate with Slammie but the signals got blocked [H-2]	UCA1.18 Base station provided false information that it had communicated with Slammie [H-2]	UCA1.19 Instead of calling to the Front desk, Base station had communicated back with Slammie [H-1]	
CHARGING POINT	UCA1.21 Slammie tried to charge itself through base station, but the power was down [H-1,H-2]	UCA1.22 Slammie provided false information that the charging was maximum [H-1,H-2]	UCA1.23 Instead of charging, Slammie made a false order to map the surroundings [H-1,H-2]	UCA1.24 Slammie took too long time in charging itself [H-1,H-2]
COMMUNICATION	UCA1.25 Slammie tried to communicate with Base station about the emergency but the signals got blocked [H-1]	UCA1.26 Slammie provided false statement that there is no accident occurred [H-1]	UCA1.28 Slammie provided false information about battery status instead of providing emergency call request first [H-1]	UCA1.27 Slammie took too long time to communicate with the Base station [H-1]
SLAMMIE CALL REQUEST TO FRONT DESK	UCA1.29 Slammie called the front desk, but it got directed to voice mail [H-2]	UCA1.30 Front desk provided the false information that there is no call received [H-2]	UCA1.31 Front desk person was on another emergency service [H-2]	UCA1.32 Slammie took long time to communicate with the Front desk [H-2]
INFORMS THROUGH VOICE				

Control Action	Not providing causes hazard	Providing causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long
	UCA1.33 Customer moves the robot while mopping, but forgets to reconnect to the base station [H-3]	UCA1.34 Millie moves robot while mopping, but forgets to reconnect to the base station [H-3]	UCA1.35 Customer disconnects the robot for mopping and the accident happens [H-3]	UCA1.36 Customer disconnects the robot and applied too long time for mopping [H-3]
CONTACTS ROBOT FOR HELP	UCA1.37 Customer tries to contact robot during emergency situations, but the robot doesn't respond [H-2]	UCA1.38 Robot provides false information that it rescued the customer [H-1]	UCA1.39 Customer tries to contact robot for help but it started mapping the surroundings [H-2]	UCA1.40 robot stopped working too soon as the communication was poor [H-2]
DETECT SOUNDS	UCA1.41 Slammie robot fails to detect sound in emergency situation [H-2]	UCA1.42 Robot provided false information that sound has been detected [H-2]	UCA1.43 Robot detected other alternative sound instead of customer [H-2]	UCA1.44 Robot stopped working too soon instead of detecting sounds [H-2]
HELPS IN EMERGENCY SITUATION	UCA1.45 Slammie robot tries to help customer but couldn't because of loss of communication [H-1]	UCA1.46 Base station was not responding to the situations [H-1]	UCA1.47 loss of communication during the emergency situation [H-1]	UCA1.48 due to loss of communication the robot response to the emergency team got stopped [H-1]
CONTROL SYSTEM OF SLAMMIE			UCA1.51 Slammie entered the bathroom was a wrong timing [H-1,H-2]	

Control Action	Not providing causes hazard	Providing causes hazard	Wrong timing or order causes hazard	Stopped too soon or applied too long
	UCA1.49 Slammie robot tries to help customer but there was an error in the process according to the algorithm [H-1,H-2,H-3]	UCA1.50 Slammie robot while searching the customer, entered into the bathroom while floor was wet and lost communication as well [H-1,H-2,H-3]		UCA1.52 Slammie stopped working too as soon as it lost it's communication [H-1,H-2]
TRACKS MILLIE'S LOCATION	UCA1.54 External sensor pings millie location, but slammie had no sight of millie in that area [H-2]	UCA1.53 External sensor provided false information about the accident [H-2]	UCA1.55 Slammie lost its communication with the base station while sensors reported the accident [H-2]	UCA1.56 external sensor stopped working too soon during the accident [H-2]
ACKNOWLEDGEM	[Not Hazardous]			
ACKNOWLEDGE				
MILLIE LOCATION INFORMATION				

Corresponding Safety Constraints

ID	Unsafe Control Actions	ID	Corresponding Safety Constraints
UCA1.1	SLAMMIE tried to move but got stuck onto the towel which made it unable to move	SC1.1	SLAMMIE shall alart when got stuck onto anything which makes it unable to move
UCA1.2	SLAMMIE provided information that it was moving instead of not	SC1.2	SLAMMIE shall provided information that it was moving instead of not
UCA1.3	SLAMMIE started speeding the wheels faster as it was not moving forward	SC1.3	SLAMMIE shall report speeding the wheels and not able to move foward

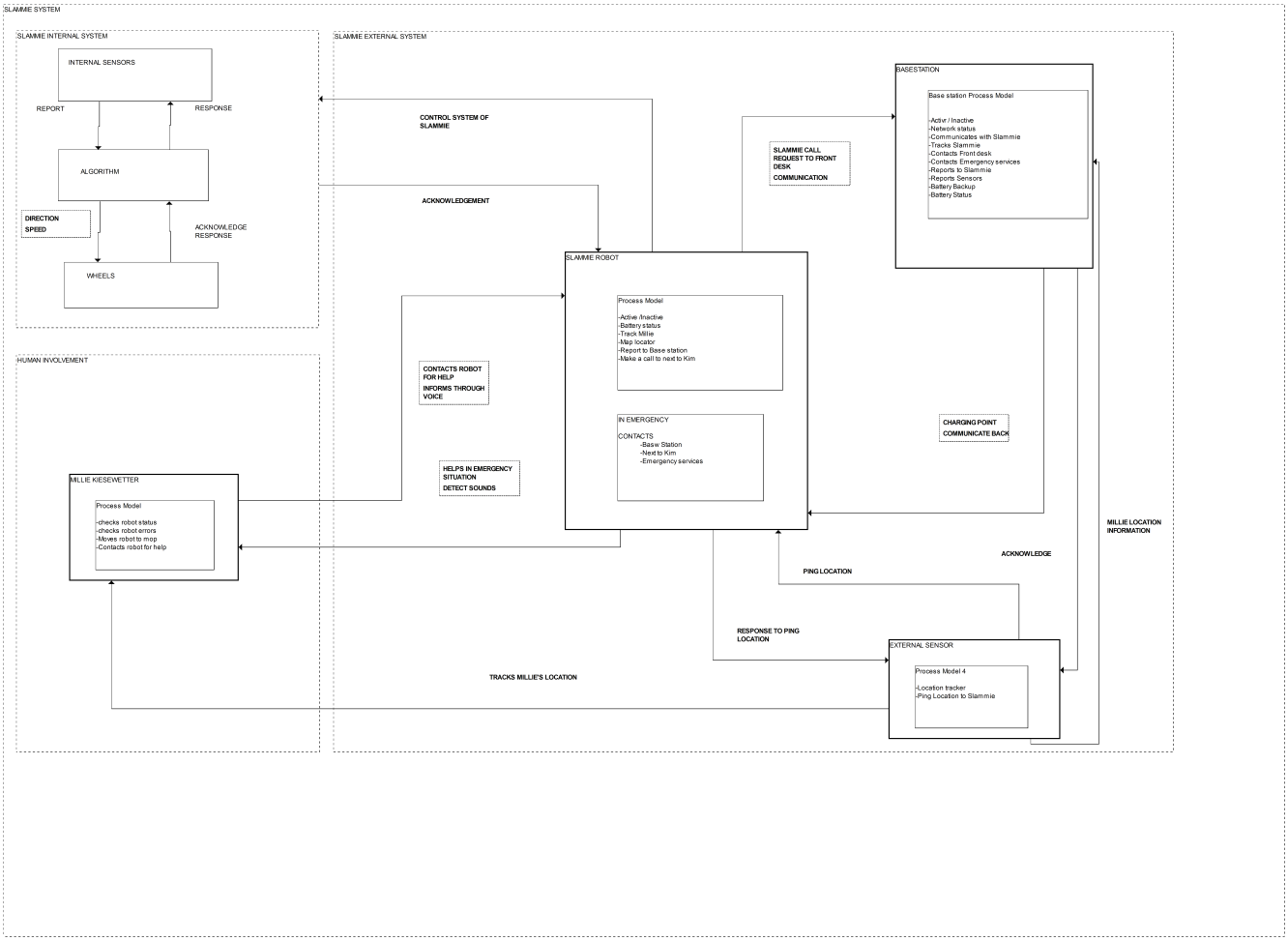
ID	Unsafe Control Actions	ID	Corresponding Safety Constraints
UCA1.4	SLAMMIE stopped working too soon as the battary got drained due to speeding	SC1.4	SLAMMIE shall not stop working while speeding
UCA1.5	Robot tried to find direction to the base station but lost communication with base station	SC1.5	Robot tried to find direction to the base station but lost communication with base station
UCA1.6	SLAMMIE provided false information that it was moving towards base station	SC1.6	SLAMMIE shall not provided false information that it was moving towards base station
UCA1.7	SlAMMIE robot had wrong timing entering into the bathroom	SC1.7	Slammie shall not enter the bathroom
UCA1.8	Robot stopped working too soon as it got direction less	SC1.8	Robot shall work in all situations
UCA1.9	SLAMMIE got multiple pings at a time, and got muddled	SC1.9	Slammie robot shall not muddle in any situation
UCA1.10	Sensor provided false information and pings wrong location	SC1.10	Sensor shall not provide false information
UCA1.11	Instead of examine the location, SLAMMIE started mapping the apartment	SC1.11	Slammie shall need to examine the location and map later
UCA1.12	SLAMMIE took too long in reacting to the sensors location alert	SC1.12	Slammie shall not take longer time in reacting
UCA1.13	SLAMMIE Inspects only one location among multiple alerts.	SC1.13	slammie should inspects multiple location as well
UCA1.14	Sensor provided false information saying false alarm	SC1.14	Sensors shall not provide false alarm
UCA1.15	Instead of examine the location, SLAMMIE started mapping the apartment	SC1.15	Slammie shall need to examine the location first
UCA1.16	SLAMMIE took too long in reacting to the sensors location alert	SC1.16	Slammie shall not take too long time in reacting to the situations
UCA1.17	Base Station tried to communicate with Slammie but the signals got blocked	SC1.17	Signals shall not be blocked
UCA1.18	Base station provided false information that it had communicated with Slammie	SC1.18	Base station shall not provide false information that it had communicated with slammie
UCA1.19	Instead of calling to the Front desk, Base station had communicated back with Slammie	SC1.19	Base station shall contact front desk first during emergency
UCA1.20	Base station stopped too soon in communicating with Slammie	SC1.20	Base station shall not stop communicating with slammie

ID	Unsafe Control Actions	ID	Corresponding Safety Constraints
UCA1.21	Slammie tried to charge itself through base station, but the power was down	SC1.21	Power shall not get down anytime
UCA1.22	Slammie provided false information that the charging was maximum	SC1.22	Slammie shall not provide false information that the charging was maximum
UCA1.23	Instead of charging, Slammie made a false order to map the surroundings	SC1.23	Slammie shall charge first instead of mapping
UCA1.24	Slammie took too long time in charging itself	SC1.24	Slammie shall not take too long time in charging
UCA1.25	Slammie tried to communicate with Base station about the emergency but the signals got blocked	SC1.25	Signals shall not be blocked
UCA1.26	Slammie provided false statement that there is no accident occurred	SC1.26	Slammie shall not provide false statement about any accidents or any emergency situations
UCA1.27	Slammie took too long time to communicate with the Base station	SC1.27	Slammie shall not take too long time to communicate with base station
UCA1.28	Slammie provided false information about battery status instead of providing emergency call request first	SC1.28	Slammie shall not provide false information about the battery status
UCA1.29	Slammie called the front desk, but it got directed to voice mail	SC1.29	Call from Slammie shall not get directed to voice mail
UCA1.30	Front desk provided the false information that there is no call received	SC1.30	Front desk shall not provide any false information about call receiving
UCA1.31	Front desk person was on another emergency service	SC1.31	Front desk shall have alternative lines
UCA1.32	Slammie took long time to communicate with the Front desk	SC1.32	Slammie shall not take long time to communicate with the front desk
UCA1.33	Customer moves the robot while mopping, but forgets to reconnect to the base station	SC1.33	Customer shall mot forgets to reccoonect to the base station back
UCA1.34	Millie moves robot while mopping, but forgets to reconnect to the base station	SC1.34	Millie shall mot forget to reconnect to the base station
UCA1.35	Customer disconnects the robot for mopping and the accident happens	SC1.35	Customer shall not disconnect the robot with the base station
UCA1.36	Customer disconnects the robot and applied too long time for mopping	SC1.36	Customer shall not disconnect the robot with the base station in any situations
UCA1.37	Customer tries to contact robot during emergency situations, but the robot doesn't respond	SC1.37	Robot shall respond in all the situations

ID	Unsafe Control Actions	ID	Corresponding Safety Constraints
UCA1.38	Robot provides false information that it rescued the customer	SC1.38	Robot shall not provide any false information
UCA1.39	Customer tries to contact robot for help but it started mapping the surroundings	SC1.39	Robot shall stop mapping in any emergency situations
UCA1.40	robot stopped working too soon as the communication was poor	SC1.40	Robot shall not stop working
UCA1.41	Slammie robot fails to detect sound in emergency situation	SC1.41	Slammie robot shall not fail in detecting sounds
UCA1.42	Robot provided false information that sound has been detected	SC1.42	Robot shall not provide any false information
UCA1.43	Robot detected other alternative sound instead of customer	SC1.43	Robot shall need to inspect all locations
UCA1.44	Robot stopped working too soon instead of detecting sounds	SC1.44	Robot shall not stop working too soon
UCA1.45	Slammie robot tries to help customer but couldn't because of loss of communication	SC1.45	Slammie robot shall not lose communication
UCA1.46	Base station was not responding to the situations	SC1.46	Base station shall respond to the any situations
UCA1.47	loss of communication during the emergency situation	SC1.47	There should be no communication loss all the time
UCA1.48	due to loss of communication the robot response to the emergency team got stopped	SC1.48	Robot response to the emergency situation shall not get stopped
UCA1.49	Slammie robot tries to help customer but there was an error in the process according to the algorithm	SC1.49	There shall not be any type of errors in the algorithm
UCA1.50	Slammie robot while searching the customer, entered into the bathroom while floor was wet and lost communication as well	SC1.50	Robot shall not enter any wet flooring area and shall not lose communication
UCA1.51	Slammie entered the bathroom was a wrong timing	SC1.51	Slammie shall not enter the bathroom
UCA1.52	Slammie stopped working too as soon as it lost it's communication	SC1.52	Slammie shall not lose communication
UCA1.53	External sensor provided false information about the accident	SC1.53	External sensor shall not provide any false information about the accident
UCA1.54	External sensor pings millie location, but slammie had no sight of millie in that area	SC1.54	External sensor shall ping wrong locations

ID	Unsafe Control Actions	ID	Corresponding Safety Constraints
UCA1.55	Slammie lost its communication with the base station while sensors reported the accident	SC1.55	Slammie shall not lose its communication with the base station
UCA1.56	external sensor stopped working too soon during the accident	SC1.56	external senors shall not stop working

Control Structure Diagram with Process Model



Causal Factors

Component	Causal Factor	Hazard Links	Safety Constraint	Notes
SLAMMIE SYSTEM	—	—	—	—
Dashed Box 1	—	—	—	—
SLAMMIE EXTERNAL SYSTEM	—	—	—	—
HUMAN INVOLVEMENT	—	—	—	—
SLAMMIE INTERNAL SYSTEM	—	—	—	—
MILLIE LOCATION INFORMATION	—	—	—	—
ACKNOWLEDGE	—	—	—	—
ACKNOWLEDGEMENT	—	—	—	—
BASESTATION	Communication protocol	H-1,H-2	Base station shall not provide false information that it had communicated with slammie	In order to prevent accident, Base station shall not provide false information to slammie
TRACKS MILLIE'S LOCATION	—	—	—	—
ALGORITHM	A process set of rules and regulations	H-1,H-2,H-3	There shall not be any type of errors in the algorithm	Errors in the algorithm will leads to robotic failures which may to accidents
CONTROL SYSTEM OF SLAMMIE	—	—	—	—
?	—	—	—	—
?	—	—	—	—

Component	Causal Factor	Hazard Links	Safety Constraint	Notes
?	—	—	—	—
?	—	—	—	—
RESPONSE TO PING LOCATION	—	—	—	—
PING LOCATION	—	—	—	—
?	—	—	—	—
EXTERNAL SENSOR	Location Indicator	H-1	Sensors shall not provide false alarm	External and internal sensors should work consistently
SLAMMIE ROBOT	Battery status	H-1,H-2	Slammie robot shall not muddle in any situation	Slammie robot shall not muddle in any situation
MILLIE KIESEWETTER	Customer Involved	H-3	Millie shall not forget to reconnect to the base station	Millie should be connected with the base station all the time
WHEELS	Speed and direction	H-3	Slammie shall not enter the bathroom	Slammie shall not enter the bathroom which has moist surroundings
INTERNAL SENSORS	Sound Detection	H-1,H-2	SLAMMIE shall not provided false information that it was moving towards base station	SLAMMIE shall not provided any false information to the base station