




MODERN MOBILITY  
HAZARD ANALYSIS DOCUMENT

Doc: DOC0005  
Rev: F

# HAZARD ANALYSIS DOCUMENT


**MECHATRONICS 4TB6  
GROUP 2**

NATHAN FUJIMOTO	1224348
PRAKHAR GARG	1204351
JOSH GILMOUR	1402325
AARON JASS	1218859
TYLER JASS	1218857
FAUZIA KHANUM	1209252
JACK LIU	1215056
GAGAN SINGH	1306242

	<p>MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

## Table of Contents

1 Introduction	5
2 Overview	6
2.1 Component Overview	6
2.2 Component Description	8
2.2.1 Navigation Module	8
2.2.2 Human Interface Module	8
2.2.3 Walker Interface Module	8
2.2.4 Drive Modules	8
2.3 System Variables	9
3 STPA	14
3.1 STPA - Navigation	15
3.1.1 Control Action Hazards	16
3.1.2 STPA Hazard Analysis	17
3.2 STPA - Manual Assist	20
3.2.1 Control Action Hazards	21
3.2.2 STPA Hazard Analysis	22
3.3 STPA - Battery Level	24
3.3.1 Control Action Hazards	25
3.3.2 STPA Hazard Analysis	25
4 Safety Considerations	27
4.1 Collision Hazard	27
4.2 Power Supply	27
4.3 Sensors	28
4.4 Electronic Part Failure	28
5 Conclusion	29


	<p>MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

## Table of Figures

Figure 1 - High Level Module Diagram	7
Figure 2 - STPA for Navigation Diagram	15
Figure 3 - STPA for Manual Assist	20
Figure 4 - STPA for Battery Level	24


## Table of Tables

Table 1 - System Variable Prefixes	9
Table 2 - Monitored Variables	9
Table 3 - Controlled Variables	11
Table 4 - Input Variables	11
Table 5 - Output Variables	13
Table 6 - STPA Hazard Analysis (Navigation)	17
Table 7 - STPA Hazard Analysis (Manual Assist)	22
Table 8 - STPA Hazard Analysis (Battery Level)	25

	<p style="text-align: center;">MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------


## Revision History

Rev	Author(s)	Description of Change	Peer Reviewed	Date
-	T.Jass	Original Document	A.Jass N.Fujimoto	04-Jan-2018
A	N.Fujimoto	Listing components	F. Khanum	04-Jan-2018
B	J.Gilmor F.Khanum A.Jass T.Jass	Began STPA Hazard Analysis Began List of Safety Consideration Adding Component descriptions	A.Jass T.Jass	05-Jan-2018
C	A.Jass T.Jass J.Liu	Developing component overview and component descriptions Added Introduction	N.Fujimoto J.Gilmour	06-Jan-2018
D	N.Fujimoto J.Gilmor	Added STPA diagrams Added STPA Hazards, Hazard Table	F. Khanum	08-Jan-2018
E	N.Fujimoto J.Gilmor F. Khanum	Completed initial draft of STPA Hazard Analysis Safety Considerations	T.Jass	09-Jan-2018
F	T.Jass N.Fujimoto	Added System variable tables and formatted document	A.Jass	11-Jan-2018

	<p>MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

## 1 Introduction

The purpose of this document is to outline the components, safety considerations, and hazards for the SmartWalker. The first part of this document will provide an overview of all the various hardware and software components, along with a brief description of each component. The second part will list the safety considerations for each component as well as detail how these safety considerations will be implemented. Finally, a comprehensive analysis will be conducted of potential hazards through a Systems-Theoretic Process Analysis (STPA) approach for each of our controlled processes. In this diagram, a list of potential hazards will be compiled by analyzing the potential interaction failures in the components, and in the environment, and steps to mitigate these failures will be discussed.

	<p>MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

## 2 Overview

### 2.1 Component Overview

The following diagram gives a high-level overview of the SmartWalker system from the inputs into the different modules to outputs per module. As seen below the system is made of four modules: the navigation module, the human interface module, the walker interface module, and the drive module. These modules will aid in finding and describing the different hazards present in the system.

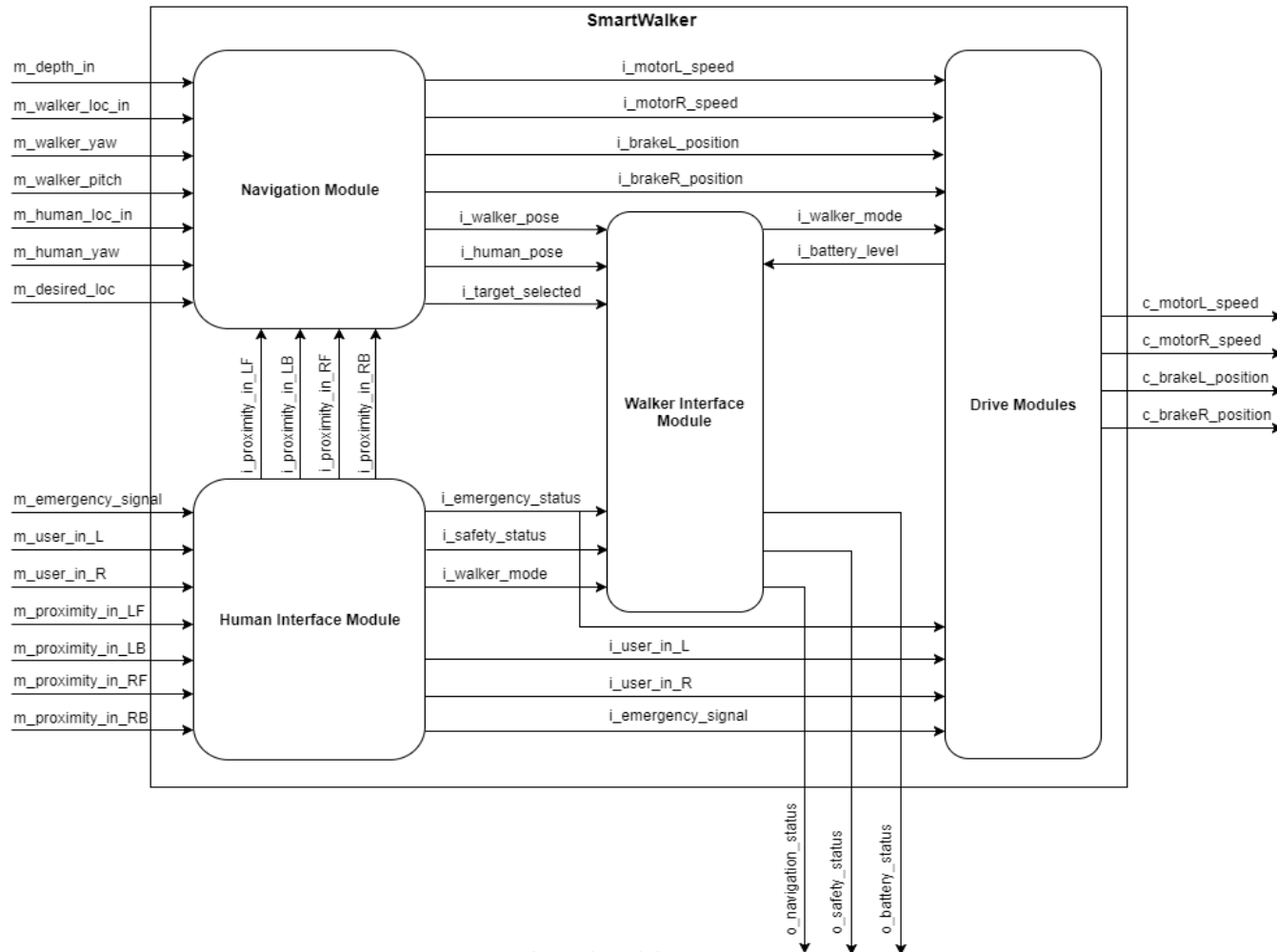



Figure 1 - High Level Module Diagram

	<p style="text-align: center;">MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

## 2.2 Component Description

A description of each component (or module) is given below.

### 2.2.1 Navigation Module

This module is the main navigation module which autonomously moves the SmartWalker between two locations within a room. This module directly takes in the main navigation depth image sensor data, mapping data and user target data, while receiving information from the human interface module about manual assistive needs and proximity to other objects. It passes motor and brake commands to the drive module and passes navigation variables to the walker interface module.

### 2.2.2 Human Interface Module

This module contains the human-machine interfaces that directly get inputs from the user while in manual use like handle information and the need for emergency braking. In addition, it is connected to proximity data which collects information on approaching objects to the human (and SmartWalker). The proximity information is passed on to the Navigation Module, safety data and emergency inputs are passed on to the Walker Interface Module, and finally the user handle inputs and emergency signal are connected to the Drive Module.

### 2.2.3 Walker Interface Module

The Walker Interface Module displays information of the walker's statuses to user while all modes. It takes in navigation information to output a navigation status to the user, as well as takes emergency status and safety status information to be displayed to the user's mobile device and walker screen depending on the mode of operation of the SmartWalker.

### 2.2.4 Drive Modules

This module takes in the motor/brake commands outputted by the Master Control Module and executes them by actuating the motors/brakes. It also receives the desired user speed (or braking request) and emergency request and executes them in real-time by again actuating the motors/brakes.



## 2.3 System Variables

The following are several tables specifying the system's different variables, a legend is included below providing the meaning of the prefixes:

**Table 1 - System Variable Prefixes**

Prefix	Meaning	Description
m	Monitored	Variables that store information from sensors about the physical environment.
c	Controlled	Variables that store information to be outputted to actuators.
i	Input	Purely software variable that is an input to a software module.
o	Output	Variable that is an output determined by a software module.

**Table 2 - Monitored Variables**

Variable	Description	Units	Range
<i>m_battery_lvl</i>	Power level of battery.	Battery Sustain of Charge (%)	[0, 100]
<i>m_battery_rel</i>	Reliability of the battery.	Battery Health (%)	[0, 100]
<i>m_proximity_in_LF</i>	Proximity to any objects in the environment (front-left side).	Distance (cm)	[0, 500]
<i>m_proximity_in_RF</i>	Proximity to objects in the environment (front-right side).	Distance (cm)	[0, 500]
<i>m_proximity_in_LB</i>	Proximity to any objects in the environment (back-left side).	Distance (cm)	[0, 500]
<i>m_proximity_in_RB</i>	Proximity to objects in the environment (back-right side).	Distance (cm)	[0, 500]
<i>m_depth_in</i>	Depth of the upcoming ground	Distance (cm)	[-100, 0]

	with respect to the bottom of the walker.		
<i>m_walker_yaw</i>	Orientation of the walker (yaw) with respect to the walker's z-axis.	Angle (deg)	[-180, 180]
<i>m_walker_pitch</i>	Orientation of the walker (pitch) with respect to the walker's y-axis.	Angle (deg)	[-45, 45]
<i>m_walker_loc_out</i>	Global location of the walker.	[Longitude (deg), Latitude (deg)]	[-180, 180; -90,90]
<i>m_walker_loc_in</i>	Location of the walker inside the patient room, with respect to a preset coordinate system.	[x,y] on room map	[0, 100; 0, 100]
<i>m_human_loc_in</i>	Location of the human based on their phone, with respect to a preset coordinate system.	[x, y] on room map	[0, 100; 0, 100]
<i>m_human_yaw</i>	Orientation of the human (yaw) with respect to the human's z-axis.	Angle (deg)	[-45, 45]
<i>m_desired_loc</i>	User selected desired location for the walker in autonomous mode	Enum (states)	GoDocking, GoHuman
<i>m_dock_aligned</i>	Walker is physically aligned with the docking station	Boolean	0, 1
<i>m_user_in_L</i>	Desired forward assisted movement for the user, for the left motor.	Custom	[-100,100]
<i>m_user_in_R</i>	Desired forward assisted	Custom	[-100,100]


	movement for the user, for the left motor.		
<i>m_emergency_signal</i>	Signal for monitoring an emergency situation.	Boolean	0, 1

**Table 3 - Controlled Variables**


Variable	Description	Units	Range
<i>c_motorL_speed</i>	Left motor speed.	Angular velocity (deg/s)	[0, 50]
<i>c_motorR_speed</i>	Right motor speed.	Angular velocity (deg/s)	[0, 50]
<i>c_brakeL_position</i>	Left brake position.	Brake Position (%)	[0, 100]
<i>c_brakeR_position</i>	Right brake position.	Brake Position (%)	[0, 100]
<i>c_charge_walker</i>	Charge the walker.	Boolean	0, 1
<i>c_dock_connected</i>	Walker physically connected to the docking station.	Boolean	0, 1

**Table 4 - Input Variables**

Variable	Description	Data Type	Range
<i>i_motorL_speed</i>	Left wheel motor forward speed command.	32 bit float	[0, 2]
<i>i_motorR_speed</i>	Right wheel motor forward speed command.	32 bit float	[0, 2]

	<p style="text-align: center;">MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------


<i>i_brakeL_position</i>	Left brake motor position command.	32 bit float	[0, 1]
<i>i_brakeR_position</i>	Right brake motor position command.	32 bit float	[0, 1]
<i>i_walker_pose</i>	Walker's position and orientation within room map.	32 bit float array (x, y, z, $\theta$ )	[0, 100; 0, 100; 0, 100; -180, 180]
<i>i_human_pose</i>	User's position and orientation within room map.	32 bit float array (x, y, z, $\theta$ )	[0, 100; 0, 100; 0, 100; -180, 180]
<i>i_target_selected</i>	User's desired navigation target for walker.	Enum	USER, DOCK
<i>i_proximity_in_LF</i>	Proximity to objects (left-front side).	32 bit float	[0, 500]
<i>i_proximity_in_LB</i>	Proximity to objects (left-back side).	32 bit float	[0, 500]
<i>i_proximity_in_RB</i>	Proximity to objects (right-front side).	32 bit float	[0, 500]
<i>i_proximity_in_RF</i>	Proximity to objects (right-front side).	32 bit float	[0, 500]
<i>i_emergency_status</i>	Walker's status of immediate emergencies.	Enum	NON_EMER, EMER
<i>i_safety_status</i>	Walker's status of unsafe scenarios approaching.	Enum	SAFE, UNSAFE
<i>i_walker_mode</i>	The mode of operation.	Enum	INIT, MAN, AUTO
<i>i_user_input_R</i>	Requested forward assisted movement for the user, for the left motor.	16 bit uint	[0, 1024]

	<p>MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

<i>i_user_input_L</i>	Requested forward assisted movement for the user, for the right motor.	16 bit uint	0, 1024]
<i>i_emergency_signal</i>	Signal indicating an emergency situation.	Boolean	0, 1

**Table 5 - Output Variables**

Variable	Description	Data Type	Range
<i>o_navigation_status</i>	Current state of the Walker's navigation process	Enum	IDLE, INIT, TRAN, FINE
<i>o_safety_status</i>	Current state of the overall system's safety	Enum	UNSAFE, SAFE

	<p>MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

### 3 STPA

In order to properly identify a comprehensive list of hazards for the SmartWalker project, a STPA Hazard Analysis was completed of the main controlled processes of the walker. For each of the main controlled processes, a NRC diagram was created for each to outline the appropriate control actions. Next general hazards were outlined for each and then finally hazards were organized by the four STPA categories.

### 3.1 STPA - Navigation

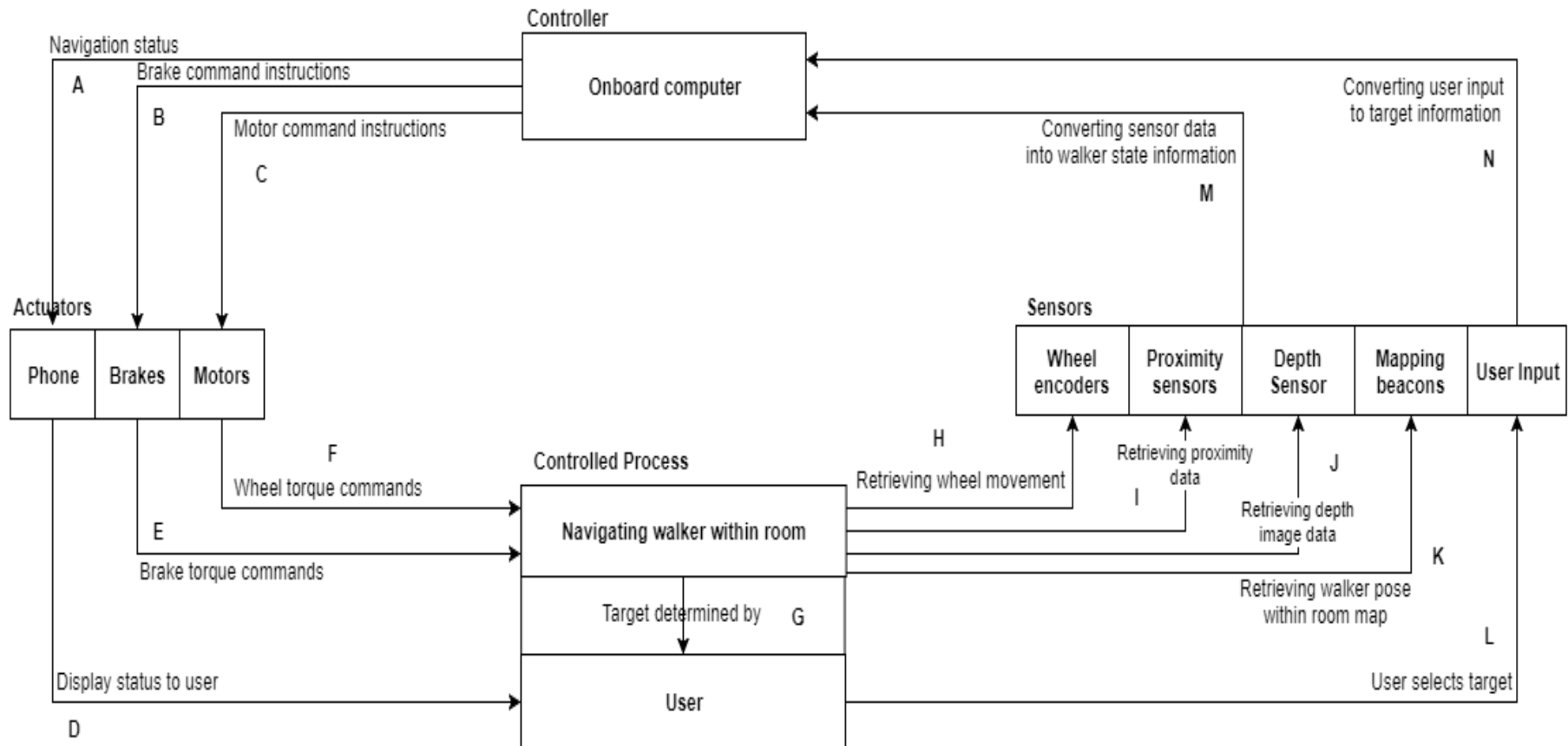



Figure 2 - STPA for Navigation Diagram

	<p style="text-align: center;">MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

### 3.1.1 Control Action Hazards

#### Navigation Status Hazards (A):

- Incorrect status sent
- Incorrect status signal timing

#### Brake Command Instructions Hazards (B):

- Incorrect command sent
- Incorrect command instruction timing

#### Motor Command Instructions Hazards (C):

- Incorrect command sent
- Incorrect command instruction timing

#### Display Status to User Hazards (D):

- Operational delays
- Same as A

#### Brake Torque Commands Hazards (E):

- Operational delays
- Same as B

#### Wheel Torque Commands Hazards (F):

- Operational delays
- Same as F

#### Target Received Hazards (G)

- Invalid user target selection received
- Valid but incorrect user target selection received
- Incorrect user target selection timing


#### Retrieving Wheel Movement Hazards (H):

- Invalid wheel movement data received
- Valid but incorrect wheel movement data received
- Incorrect wheel movement data retrieval timing

#### Retrieving Proximity Data Hazards (I):

- Invalid proximity data received
- Valid but incorrect proximity data received
- Incorrect proximity data retrieval timing



	<p style="text-align: center;">MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

**Retrieving Depth Image Data Hazards (J):**

- Invalid depth image data received
- Valid but incorrect depth image data received
- Incorrect depth image data retrieval timing

**Retrieving Walker Pose within Room Map (K):**

- Invalid walker pose within room map received
- Valid but incorrect walker pose within room map received
- Incorrect walker pose within room map retrieval timing

**User Selects Target (L):**

- Same as G

**Converting Sensor Data into Walker State Information (M):**

- Operational Delays
- Same as G, H, I, J, L

**Converting User Input to Target Information Hazards (N):**

- Operational Delays
- Same as G

### 3.1.2 STPA Hazard Analysis

**Table 6 - STPA Hazard Analysis (Navigation)**

Control Action	Category 1 (A control action required for safety is not provided or not followed)	Category 2 (An unsafe control action is provided that leads to a hazard)	Category 3 (A potentially safe control action is provided too early, too late, or out of sequence)	Category 4 (A safe control action is stopped too soon)
<b>Sending Navigation Status (A, D)</b>	System does not send navigation status when needed for the user (A1).	System sends that the walker has arrived when walker has yet to arrive (and vice-versa) (A2).	System sends walker has arrived too early or too late to the user (A3).	N/A.
<b>Sending Brake Command Instructions (B, E)</b>	Brake commands are not sent when requested or with	System sends an inappropriate brake command	Brake command is sent too early or too late which	Brake command is stopped too early before walker can

	an incorrect message format (B1).	for current navigation needs (B2).	forces navigation position out of sync (B3).	be fully actuated (B4).
<b>Sending Motor Command Instructions (C)</b>	Motor commands are not sent when requested or with an incorrect message format (C1).	System sends an inappropriate motor command for current navigation needs (C2).	Motor command is sent too early or too late which forces navigation position out of sync (C3).	Motor command is stopped too early before walker can be fully actuated (C4).
<b>Brake Torque Commands (E)</b>	Brake commands are not provided (E1).	Incorrect braking torque applied to wheels. Brakes are abruptly applied at too high a speed (E2).	Brakes react to commands too early or too late (E3).	Brakes stop braking when they should not (E4).
<b>Wheel Torque Commands (F)</b>	Torque command for wheels is not provided (F1).	Incorrect torque is applied to wheels. Too high of a torque is produced by the motors (F2).	Motors react to commands too early or too late (F3).	Motors stop applying torque when they should not (F4).
<b>User Selects Target Location (G, L)</b>	User does not select a target location when needed (G1).	User selects an inappropriate target location (G2).	User selects a target location out of sequence (G3).	N/A.
<b>Retrieving Wheel Movement Data (H)</b>	Sensor does not read a wheel's movement data (H1).	Sensor reads incorrect wheel movement data based on current walker state (H2).	Sensor reads wheel movement data too early or too late (H3).	Sensor data acquisition of wheel movement data stopped too soon (H4).
<b>Retrieving Proximity Data (I)</b>	Proximity sensor does not read data (I1).	Proximity sensor reads incorrect data based on current walker state (I2).	Proximity sensor reads data too early or too late (I3).	Sensor data acquisition proximity data stopped too soon (I4).
<b>Retrieving Depth</b>	Depth image	Depth image	Depth image	Sensor data



MODERN MOBILITY  
HAZARD ANALYSIS DOCUMENT

Doc: DOC0005  
Rev: F

<b>Image Data (J)</b>	sensor does not read data (J1).	sensor reads incorrect data based on current walker state (J2).	sensor reads data too early or too late (J3).	acquisition of depth image data stopped too soon (J4).
<b>Retrieving Walker Pose within Room Map (K)</b>	Sensor does not read walker's pose within room map (K1).	Sensor reads incorrect walker pose within room map based on current walker position (K2).	Sensor reads walker pose within room map data too early or too late resulting in out of sequence acquisition (K3).	Sensor data acquisition of walker pose within room map stopped too soon (H4).
<b>Converting Sensor Data into Walker State Information (M)</b>	System does not convert sensor data into walker state or converts to an incorrect format (M1).	System incorrectly converts sensor data into an incorrect walker state (M2).	System converts sensor data into walker state information too early or too late (M3).	System conversion of sensor data into walker state information is stopped abruptly (M4).
<b>Converting User Input to Target Information (N)</b>	System does not convert selected user target or converts to an incorrect format (N1).	System incorrectly converts selected user target into an incorrect location (N2).	System converts user selected target into target location too early or too late (N3).	System conversion of user selected target into target location is stopped abruptly (N4).

### 3.2 STPA - Manual Assist

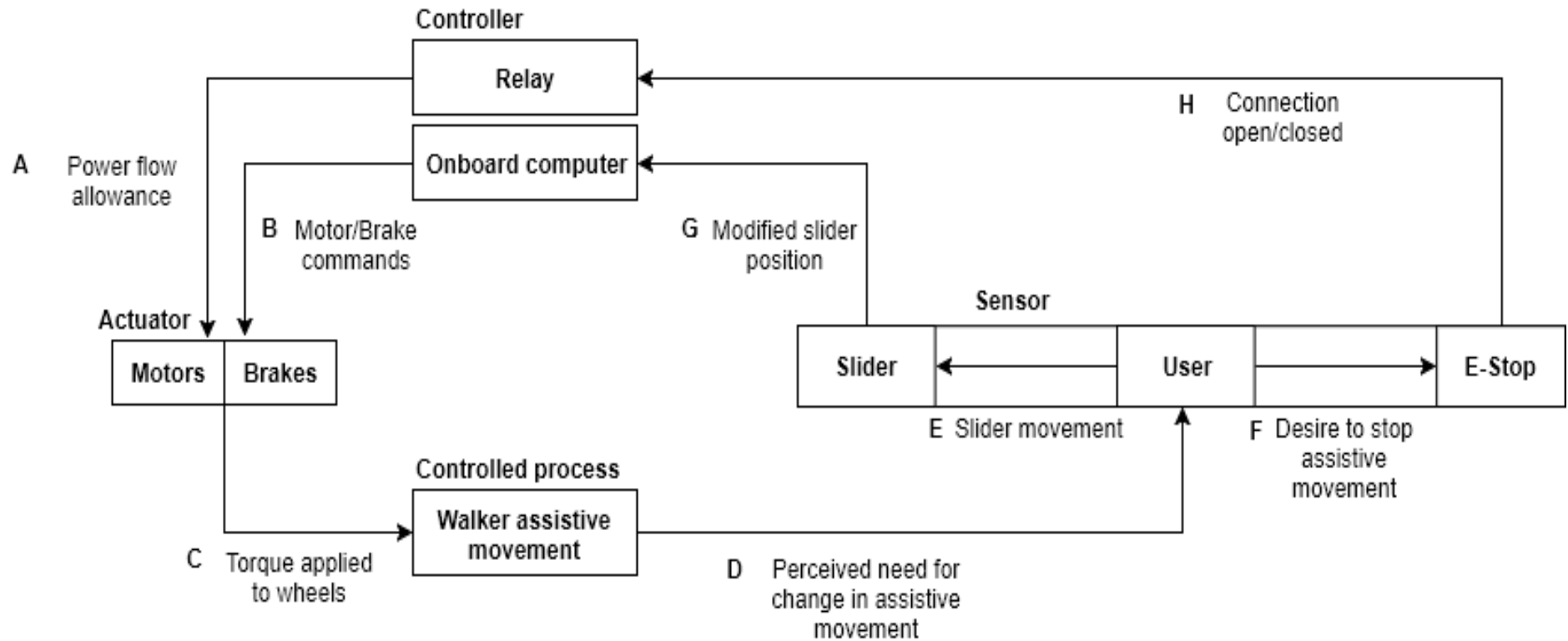



Figure 3 - STPA for Manual Assist

	<p style="text-align: center;">MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

### 3.2.1 Control Action Hazards

#### Power Flow Allowance Hazards (A):

- Incorrect allowance
- Timing of change in signal

#### Motor/Brake Commands Hazards (B):

- Invalid commands sent
- Incorrect commands sent
- Incorrect command instruction timing
- Command exceeds capabilities of actuator

#### Torque Applied to Wheels Hazards (C):

- Incorrect torque applied
- Operational delays

#### Perceived Need for Change in Assistive Movement Hazards (D):

- Incorrect change perceived
- Delay in perception of change

#### Slider Movement Hazards (E):

- Component failure or wear
- Delay in movement

#### Desire to Stop Assistive Movement Hazards (F):


- Timing of action incorrect
- E-Stop pressed accidentally
- Component failure

#### Modified Slider Position Hazards (G):

- Incorrect status signal timing
- Incorrect status value sent
- Invalid status value sent

#### Connection Open/Closed Hazards (H):

- Incorrect status signal timing
- Incorrect status sent

	<p style="text-align: center;">MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

### 3.2.2 STPA Hazard Analysis

**Table 7 - STPA Hazard Analysis (Manual Assist)**

Control Action	Category 1 (A control action required for safety is not provided or not followed)	Category 2 (An unsafe control action is provided that leads to a hazard)	Category 3 (A potentially safe control action is provided too early, too late, or out of sequence)	Category 4 (A safe control action is stopped too soon)
<b>Power flow allowance (A)</b>	Power flow allowance does not change when relay receives 'signal' from E-stop to cut power (A1).	N/A.	Allowance changes too late after E-stop press (A3).	The relay allows power flow to the system even when the E-stop button is pressed (A4).
<b>Motor/Brake commands (B)</b>	Motor and brake commands not followed. Motor and brake commands that cannot be actuated are sent. Commands are not sent at all (B1).	Commands that include the motors and brakes actuating at the same time are sent. Motor torque commands that are too high are sent (B2).	The motor/brake commands are sent out too late. Motor and brake commands are mixed up (B3).	Command to brake is stopped abruptly. Command for motor actuation is stopped abruptly (B4).
<b>Torque applied to wheels (C)</b>	Incorrect torque applied by motor. Brakes not correctly applying torque to wheels. (C1)	Brakes not applying correct amount of torque to wheels. Too high a torque is produced by the motors. Brakes are abruptly applied at too high a speed (C2)	Motors or brakes react to commands too late. Motors and brakes actuate at same time due to incorrect commands (C3)	Brakes stop braking when they should not. Motors stop applying torque when they should not (C4)
<b>Perceived need</b>	No change	An incorrect	Perception of	N/A.

for change in assistive movement (D)	provided by user (D1).	change is perceived by user (D2).	change is delayed by user (D3).	
<b>Slider movement (E)</b>	Slider not moved in relation to desired change in assistive movement (E1).	Slider moved incorrectly in relation to desired change in assistive movement. Slider moved too quickly (E2).	Slider movement is delayed in relation to perception of change in assistive movement (C3).	Slider movement stopped or modified before change in movement is implemented (C4).
<b>Desire to stop assistive movement (F)</b>	E-Stop does not register press from user due to mechanical failure (F1).	E-Stop pressed accidentally by user (F2).	E-Stop is pressed too late by user (F3).	E-Stop releases when it should not (F4).
<b>Modified slider position (G)</b>	Position is not transmitted sent at all (G1).	Position transmitted is incorrect. Position transmitted is invalid (G2).	Position is sent too late (G3).	N/A.
<b>Connection open/closed (H)</b>	The state of the connection is not correctly set by the E-Stop (H1).	N/A.	The connection is not closed or opened fast enough (H3).	The connection is opened abruptly when it should be closed, or vice versa (H4).

### 3.3 STPA - Battery Level

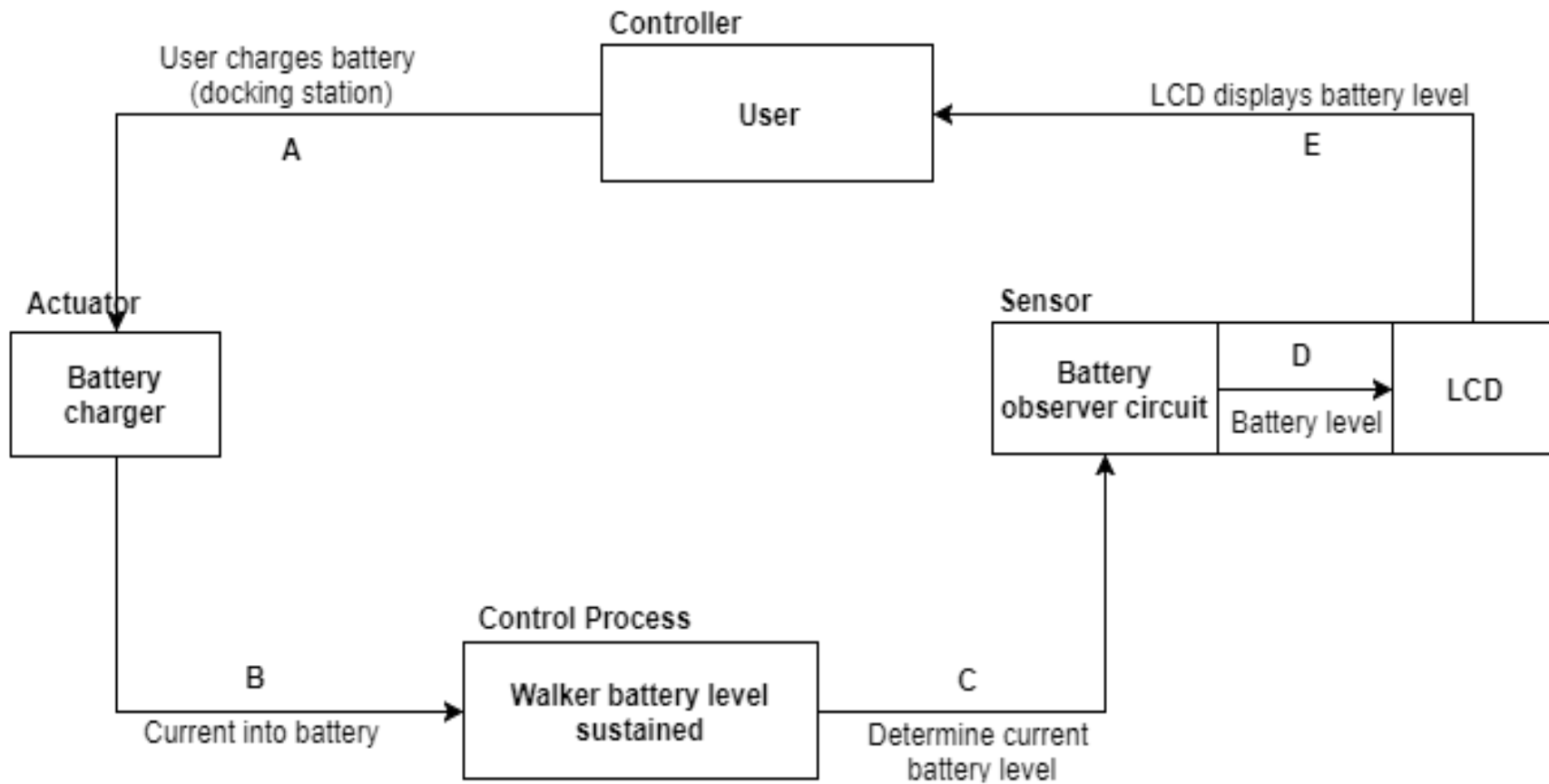


Figure 4 - STPA for Battery Level



### 3.3.1 Control Action Hazards

#### User Charges Battery Hazards (A):

- Incorrect connection to docking station

#### Current into Battery Hazards (B)

- Incorrect current value to battery
- Incorrect battery current supply timing

#### Determine Current Battery Level Hazards (C):

- Invalid determination of current battery level
- Valid, but incorrect determination of current battery level
- Incorrect determination of current battery level timing

#### Battery Level Sent to LCD Hazards (D):

- Operational delays
- Same as C

#### LCD Displays Battery Level Hazards (E):


- Operational delays
- Same as C

### 3.3.2 STPA Hazard Analysis

**Table 8 - STPA Hazard Analysis (Battery Level)**

Control Action	Category 1 (A control action required for safety is not provided or not followed)	Category 2 (An unsafe control action is provided that leads to a hazard)	Category 3 (A potentially safe control action is provided too early, too late, or out of sequence)	Category 4 (A safe control action is stopped too soon)
<b>User Moving the Walker to Charge the Battery (A)</b>	User does not put walker back to docking station to charge the battery (A1).	User puts the walker to an incorrect location to charge the battery (A2).	User puts walker to docking station to charge battery too late (A3).	User putting walker to docking station to charge battery stopped abruptly (A4).
<b>Determining the Current Needed to Charge the</b>	Battery charger does not send current to charge	Battery charger sends too little or too much current	Battery charge sends current to charge battery too	Battery charger stops charging battery abruptly

<b>Battery (B)</b>	the battery (B1).	to charge the battery (B2).	early or too late (B3).	(B4).
<b>Determining the Current Battery Level on the Walker (C, D)</b>	System does not determine current battery level (C1).	System determines the incorrect value for current battery level (C2).	System determines current battery level too late (C3).	System determination of current battery level is stopped too soon (C4).
<b>Current Battery Level Shown to User on LCD (E)</b>	LCD is not provided with a battery level, or provided incorrectly (E1).	Current battery level provided to LCD is incorrect (too high or too low) (E2).	Current battery level is provided and shown on LCD too late (E3).	Current battery level stops from being displayed on the LCD (E4).

	<p style="text-align: center;">MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

## 4 Safety Considerations

The safety of the user is one of the most important aspects of the SmartWalker, therefore, it is important that any component that could harm the user directly be considered. Certain functions are very dependent on the hardware working correctly without obstruction. The system must be able to analyze and either adapt properly or defuse the situation, pertaining to the system, from escalating catastrophically. The following is a list of some of the high-risk hazards and ways to mitigate the risk of them occurring. These solutions will not necessarily be implemented, however, feasible solutions for these hazards will be implemented to ensure a safe system.

### 4.1 Collision Hazard

#### Issue

The risk of the SmartWalker colliding with an object or person can range from high to catastrophic, during autonomous mode. The SmartWalker is intended to work in a hospital environment where there is a lot of sensitive and expensive equipment and injured/ill patients. Compared to other autonomous systems, such as a Roomba, a simple bump into the wall or furniture would not lead to high to catastrophic consequences. It is vital that the SmartWalker avoid collision as much as possible.

#### Solution

The solution would be to minimize if not eliminate the risk of this hazard occurring. Several small steps in product development process need to be taken into consideration


### 4.2 Power Supply

#### Issues

1. Not enough power for the system
2. Not charging correctly

#### Solutions

1. Several steps can be taken to mitigate the issue of not having enough power. Display the battery level to the user so they are aware of their current state, warn the user when the battery level reaches a certain point, and then power down safely (gracefully) when the battery reaches a critical level. Unlock the brakes when there is no power so that the walker can be moved to a safe location.
2. The best solution would be for the walker to run a self-diagnosis when it senses the walker docked and plugged in to charge, the battery level less than 100%, and the battery not being charged. After the diagnosis, the walker would send a message to the user of the issue based on results. An alternate solution would be for the walker to send a warning to either the users phone or the HMI that the battery is not charging. The user can then investigate further if there is an issue or not.

	<p style="text-align: center;">MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

### 4.3 Sensors

#### Issues

1. Sensor is blocked and is unable to properly take readings
2. Sensor is blocked and taking incorrect readings
3. Sensor is damaged and is unable to properly take readings
4. Sensor is damaged and taking incorrect readings

#### Solutions

1. Display warning to user on HMI. User to remove blockage.
2. If the user notices that the walker is not working properly, they can use the emergency stop button.
3. Display warning to user on HMI. User to have sensor repaired or replaced.
4. If the user notices that the walker is not working properly, they can use the emergency stop button.

### 4.4 Electronic Part Failure


Electronic parts in this case is any part used in the electrical subsystem of the SmartWalker that is not the power supply or a sensor.

#### Issues

1. Loss of Control
2. Exposed or broken wires

#### Solutions

1. Make an emergency stop available to the user. The stop option will be applied by the user when there is an emergency involving the SmartWalker and it needs to be immediately be stopped (apply brakes/stop motors, send message to user of emergency button being applied, cease all functions and restart upon emergency stop being disabled).
2. Construct the SmartWalker to hide/cover all wiring and electronics. Leave an access panel for troubleshooting issues. Since the environment of the walker is within a hospital the cover does not need to be weatherproof.

	<p>MODERN MOBILITY HAZARD ANALYSIS DOCUMENT</p>	<p>Doc: DOC0005 Rev: F</p>
--	---	--------------------------------

## 5 Conclusion

An important part of product development is completing a hazard analysis to ensure that the system is safe for use. Using the STPA process we have noted several hazards both major and minor that are present in the system. While we cannot eliminate all the hazards we can reduce the risk of these hazards from occurring. Each hazard is referenced against the System Requirements document of the SmartWalker so that the project is accommodative and adherent to the possible hazards per component. Any changes in requirements will be followed by updated system and component diagrams to adhere in order to adhere to said changes.