SFWRENG 4G06 - Hazard Analysis

Group: NextStep (Group 10)

Justin Rosner, rosnej1
Daniel Noorduyn, noorduyd
Mengxi Lei, leim5
Alexander Samaha, samahaa
Tishko Araz, arazt

Department of Computing and Software
McMaster University
February 18, 2022

Contents

List of Tables

1 Revisions

Revision Number	**Date**	**Reason for Change**
Revision 0	December 1, 2021	N/A
Revision 1	February 18, 2022	Updating hazards to include assumptions that NextStep will be used indoors.

Table 1: Revision History

2 Introduction

2.1 Scope and Purpose

The purpose of this document is to identify the modules and subsystems of our NextStep system which are deemed hazardous and that can potentially cause damage to the users of our system. With such an analysis we can mitigate and possibly eliminate the risks that result from the hazards identified. Hazard analysis must be executed during the software development cycle, the requirement analysis, architectural design, and the actual creation of the modules and hardware wiring. This document will contain the hazard analysis of the NextStep subsystems and their inner workings. Hazards and risks will be identified from previous literature as well as experiments conducted that will give us a deeper insight of the how the system acts under certain conditions.

2.2 Background

Historically, blind and visually impaired people have turned to aids such as white canes, guide dogs, and tactile paving to help them navigate through the world. Although each of these have their own associated hazards, they are not similar enough in design to warrant mentioning in this document.

Instead, we wanted to take a look at a watch prototype designed by students at Wake Forest University (1) that makes use of a similar set of sensors like those that NextStep will be using. In this design there are two sonar sensors (one on the top of the wrist and one on the side of the wrist near the thumb). The user is able to sweep their arm around, detecting objects, and the device will buzz (provide haptic feedback) when there is an object close to where they are currently sweeping. Keeping in mind that this is not a product available for retail, so no existing hazard analysis was found. However, after looking at their implementation it is clear that there are some hazards involved that our group should keep in mind for NextStep. One such hazard is that their design only allows for two sensors of the same type, which also happen to be pointing in different directions. This does not leave much wiggle room for hardware failure. If one or both of the sensors stop working it would lead to a catastrophic failure wherein the device would be rendered useless.

Another device that operates on similar principles to NextStep is the commercially available Sunu Band (2). This device also uses sonar sensors on the user's wrist to detect objects and relay the information back to them using haptic feedback. The company Sunu performed a hazard analysis and were able to detect the following potential hazards:

- The sonar sensor becoming wet.
- Using the device in temperatures greater than 55 degrees Celsius.
- Detecting street curbs, drop-offs, stairways, uneven surfaces, slippery or wet surfaces, and moving vehicles.
- Interference from other ultrasonic devices (eg. Automatic room lighting, motion detectors, etc.)

2.3 Roadmap

The hazards identified in this analysis will be used to create additional safety requirements in the next revision of the functional requirements document. In addition to this, the uncovered hazards will affect the outcome of our design process as well, as for each hazard we will need to have a solution in the design that prevent or mitigate the hazard.

2.4 Definitions

Words	Definition
Risks	The probability that a system will enter a hazardous state or that an accident will occur due to the system.
Subsystem	A sub-component of the whole system that has its individual functionality independent or loosely dependant (uses 1-2 subsystems as a client) on other sub-components of the whole system.
Redundancy	The duplication of critical subsystems such that we can increase the reliability of the function of that subsystem.
Hazard	A combination of system and outside environment conditions that has the potential to endanger people or damage the environment.

Table 2: Definitions of words that come up frequently

2.5 Assumptions

The following items are critical assumptions that were made for the development of NextStep:

- The user understands the correct orientation of the device and how to properly wear it.
- The device will be used indoors and thus will not be exposed to water damage.
- The user will strictly use the device for walking-like movements (ie. The user will not jump or run with the device on) and will not move their head erratically.
- Nobody except the user will be interacting with the device. It is assumed nobody will sabotage the use of the device while a user is using NextStep.

3 Component Overview

The overall design of NextStep can be broken down into the following components:

3.1 Data Collection

This component collects and filters data from an indoor setting using ultrasonic sensors and a Lidar. This information will then be communicated to the Sensor Fusion module. This component is key to the functionality of NextStep as without accurate data the Object Avoidance System will not be able to work properly.

3.2 Object Avoidance System

This component receives fused data from the Sensor Fusion component and then uses the Bubble Rebound algorithm to calculate a path through the obstacles for the user to follow.

3.3 User Guidance Mechanism

This component receives the necessary information from the Object Avoidance System and relays to the user via haptic feedback guidance on how to avoid running into obstacles. This is one of the key components of NextStep, as without a useful way of relaying information to the user, all of the data on where obstacles are is rendered useless.

3.4 User Inputs

Responsible for collecting information about the user to pass on to the Object Avoidance System.

3.5 Sensor Fusion

This component receives unfiltered data from the Data Collection Module and then proceeds to run a Kalman filter on it. The Kalman filter serves two purposes, to filter and then fuse the two data streams coming from the ultrasonic sensors and the Lidar. When this data is fused we can then send it to the Object Avoidance System to be used in the navigational algorithm.

3.6 System Diagnostics Module

This module will relay non-guidance information back to the user. This will include things such as battery level and any sensors that are malfunctioning.

4 Safety Considerations

4.1 Data Collection

4.1.1 Software Issues

- The component is unable to filter the data within the desired time.

4.1.2 Hardware Issues

- The component is unable to collect data due to sensor failure.
- The component is unable to acquire the data from sensor due to failure in wiring.
- The component is unable to filter the data due to processor failure.
- The component is unable to perform functionality due to improperly located sensors or sensor being blocked.

4.2 Object Avoidance System

4.2.1 Software Issues

- The system is unable to receive the data in desired time.
- The system is unable to process the data in desired time.

4.2.2 Hardware Issues

- The system is unable to perform functionality due to processor failure.

4.3 User Guidance Mechanism

4.3.1 Software Issues

- The component is unable to receive the data in desired time.
- The component is unable to process the data in desired time.

4.3.2 Hardware Issues

- The component is unable to calculate guidance information due to processor failure.
- The component is unable to output the guidance information to user due to hardware component failure.

4.4 User Inputs

4.4.1 Software Issues

- The ability to attack the system by injecting code.

4.4.2 Hardware Issues

- The component is unable to perform functionality due to hardware component failure.

4.5 Sensor Fusion

4.5.1 Software Issues

- The component is unable to receive the data in desired time.
- The component is unable to process the data in desired time.

4.5.2 Hardware Issues

- The component is unable to perform functionality due to processor failure.

4.6 System Diagnostic Module

4.6.1 Software Issues

- The component is unable to detect the hardware issue within the desired time.

4.6.2 Hardware Issues

- The system is unable to perform functionality due to processor failure.
- The system is unable to output the diagnostic result to user due to hardware failure.

5 Correlation Between Hazard Functions and Requirements

Hazard Function	Functional and Non-functional requirements
F1: Movement feedback to user	FR2
	FR3
	FR4
	FR5
	FR6
	PR5

Table 3: Correlation between hazard function 1 and requirements

Hazard Function	Functional and Non-functional requirements
F2: Object Detection and path creation	FR1
	FR3
	FR5
	FR6
	FR7
	FR9
	FR11
	FR12
	FR16
	FR18
	FR19
	PR1
	PR5
	PR7

Table 4: Correlation between hazard function 2 and requirements

Hazard Function	Functional and Non-functional requirements
F3: Movement Detection	FR1
	FR15
	FR17

Table 5: Correlation between hazard function 3 and requirements

Hazard Function	Functional and Non-functional requirements
F4: Sensor Calibration and user input	FR7
	FR8
	FR9
	FR13

Table 6: Correlation between hazard function 4 and requirements

Hazard Function	Functional and Non-functional requirements
F5: System process data in certain time	FR10 FR17

Table 7: Correlation between hazard function 5 and requirements

Hazard Function	Functional and Non-functional requirements
F6: System will have a reliable power subsystem and system diagnostics	FR4 FR13 PR6 PR11

Table 8: Correlation between hazard function 6 and requirements

6 FMEA Worksheet

6.1 Scope of Hazard Analysis and System Boundary

The following hazards are considered out of scope and will not be included in the hazard analysis.

- User inputs the wrong dimension for their height but it is still within a reasonable value. NextStep would not be able to tell if the user is maliciously giving bad information.
- User incorrectly dons the device (example: pointing the wrong way). NextStep would not be able to tell if the device is on the user incorrectly.
- Detecting objects moving faster than a walking pace.
- Because the device will be used strictly inside, water damage won't be considered. The device will be calibrated for the optimal interior temperature setting (18-24°C) so any environmental temperature causing inconsistencies and therefore hazards won't be considered.

Table 9: Failure Mode and Effect Analysis worksheet

Component	Failure Mode	Causal Failures	Effects	Probability of Occurrence (out of 10, 0 being least, 10 being most)	Severity Ranking (out of 10, 0 being least severe, 10 being most severe)	Detection Ranking (out of 10,0 being least difficult, 10 being most difficult)	RPN (out of 1000, higher the number, more priority given)	Ref
F1	User hits a stationary object.	a. Sensor misses detecting something; b. Sensor is broken; c. Object location incorrectly calculated; d. Incorrect way to avoid object produced;	User hits an object.	3	10	2	60	**H1-1**
	User hits a slow moving object.	a. Sensor misses detecting something; b. Sensor is broken; c. Object location incorrectly calculated; d. Incorrect way to avoid object produced; e. System processed data too slowly;	User hits an object.	4	10	2	80	**H1-2**
F2	Object location incorrectly calculated.	a. Object moving too fast; b. Cancellation errors; c. Wrong data passed from sensors; d. Data filtering errors;	User hits an object.	3.5	8	5	140	**H2-1**
	Incorrect way to avoid object produced.	a. Dynamic object moving too fast; b. Wrong user dimensions given; c. Data processing too slow;	a. User hits the object; b. User is directed into another object;	4	8	5	160	**H2-2**
F3	Sensor misses detecting something.	a. Sensor malfunction; b. Sensor blocked; c. Object is too small; d. Object components don't reflect sonic waves; e. Interference from other sonic waves; f. Lidar laser light reflected off object;	User hits an object.	3	8	9	216	**H3-1**
	Sensor detects a phantom object.	a. Sensor positioned incorrectly; b. Something is blocking the sensor;	User avoids an object that isn't there.	2	3	8	48	**H3-2**
F4	Sensor is broken.	a. Fall damage; b. Sensor shorted; c. Wear and tear;	User hits an object.	2	10	2	40	**H4-1**
	Wrong user dimensions given.	a. User inputted incorrect dimensions; b. User inputted dimensions in wrong units;	a. User hits an object; b. User avoids an object unnecessarily;	3	2	10	60	**H4-2**
F5	Object detection feedback is too slow.	a. System processed data too slowly; b. Object is moving too fast; c. User is moving too fast;	User hits an object.	3	8	2	48	**H5-1**
F6	Device shuts down unexpectedly.	a. Battery is empty; b. Battery is malfunctioning; c. Power module is malfunctioning;	User can no longer use the device as intended.	2	7	1	14	**H6-1**

7 References

(1) L. Stinson, “A buzzing sonar watch that helps blind people navigate,” Wired, 20-Nov-2014. [Online]. Available: https://www.wired.com/2014/11/buzzing-sonar-watch-helps-blind-people-navigate/. [Accessed: 30-Nov-2021].

(2) Sunu, Sunu Band. [Online]. Available: https://www.sunu.com/. [Accessed: 30-Nov-2021].