Hazard Analysis for SmartLock
4TB6 - Mechatronics Capstone

Team #5, Locked & Loaded
Abi Nevo, nevoa
Elsa Bassi, bassie
Steffi Ralph, ralphs1
Abdul Iqbal, iqbala18
Stephen De Jong, dejons1
Anthony Shenouda, shenoa2

March 4, 2023

Table 1: Revision History

Date	Developer(s)	Change
14-10-22	Elsa	Added FMEA
14-10-22	Abi	Added Critical Assumptions & Safety Reqs
14-10-22	Steffi	Intro, Scope & Purpose of Hazard Analysis & System Boundaries and Components
17-10-22	Abi	Revisions to Safety Requirements
19-10-22	Abi	Added probability and severity ratings to FMEA
19-11-22	Steffi	Updates for grammar, formatting and terminology
23-11-22	Steffi	Updates for consistency across documentation
03-03-23	Abi	Updating according to revised SRS

Contents

1 Introduction

This document aims to outline the hazards that may face the SmartLock. We are defining a hazard to be anything that puts the efficacy of the SmartLock at risk of failure or places the user in danger. Throughout this document, the potential hazards will be outlined, and through the use of hazard analysis techniques, we will aim to mitigate these risks.

2 Scope and Purpose of Hazard Analysis

This project's scope is to create a device that securely locks a bike, where the lock can be disengaged via a smartphone app and doesn't impede the rider's ability to use the bike, causing a safety issue. It is crucial to understand both, all the requirements of what the project is supposed to accomplish, but also all the risks that may accompany those requirements – this is the purpose of the hazard analysis. Furthermore, the analysis will aim to assess the system boundaries, critical assumptions and safety requirements to predict the potential hazards' effects in order to preemptively add precautions.

3 Definitions

Term	Definition
Hazard	An action that puts the efficacy of the SmartLock at risk of failure or places the user in danger
System Failure	System Failure is when the engagement of the lock malfunctions and the lock is no longer secure
Risk	A risk indicates a potential safety concern to the user
Error	An error indicates a problem with the software that relates to the engagement for the lock
Conflicts	A conflict indicates that an action is trying to be executed in the wrong state, ie. trying to engage the lock when the mechanism is open

4 System Boundaries and Components

The system can be broken into the following components and has the following boundaries:

4.1 Physical Components

Our physical components are the aspects that will be on the bike itself.

4.1.1 Locking Mechanism

The locking mechanism will be the component that ensures the security of the bike.

4.1.2 Opening/Closing Mechanism

The opening/closing mechanism is the component that will both attach the bike to an external frame and ensure that the wheels will stay connected to the bike when you leave it.

4.1.3 Sensors

The sensors will be used to indicate whether or not the lock is open/closed or engaged/disengaged.

4.1.4 Battery

The battery will be used to turn on the electromagnet which allows for the disengagement of the locking mechanism. It will also be used to power the Arduino (microcontroller) which will allow the smartphone app to communicate with the bike lock.

4.2 Software Components

The software components that we will be using are related to our smartphone app.

4.2.1 App

The app component itself will be used to communicate with the physical components, via the Arduino, to give the user information on the status of the lock and battery and to allow the user to disengage the lock.

4.2.2 Geotagging Location Services

The location service component will be used to communicate to the app where the bike was located upon engaging the lock, for the purpose of remembering where your bike was left.

4.3 Boundaries

4.3.1 Bike Size

The boundary that we need to work with on the physical components is the standard sizes of bikes so that the lock can be mounted properly.

4.3.2 Standard External Frames

The other physical boundary that we need to work within is the standard size/location of external frames which provides us with measurements for the open/closing mechanism that we must abide by.

4.3.3 Current Technology

The software boundary that we must remain within is the bounds of current technology; this is a very feasible and large boundary to work within as we do not plan to use any complex software.

5 Critical Assumptions

CA1: Assume operator is not tampering or purposefully damaging the product.

CA2: Assume weather is typical of Canada (i.e., no natural disasters).

CA3: Assume operator's smartphone (including all integrated technologies, like Geotagging) is functioning properly.

CA4: Assume Geotagging and Bluetooth signals are receivable and transmittable; operator is in a location that can be properly triangulated (i.e., operator is not underground, etc.).

CA5: Assume operator's bicycle has standard frame and dimensions, and functions properly.

CA6: Assume operator's smartphone has power/is charged.

6 Failure Modes and Effects Analysis

Likelihood and Severity are rated on a 1-10 scale, with 10 being the most probable/severe.

Table 2: Failure Modes and Effects Analysis

Design Function	Failure Mode	Failure Effects	Failure Causes	Detection	Recommended Actions	Design Controls	Safety Req.	Likelihood	Severity
The intended user engages and disengages the locking mechanism	Male and female locking ends are not secured together; the structural integrity of the lock is compromised	Bike not secured (vulnerable to theft or loss) by the intended user, an unintended user (thief) or independent lock failure	1. Faulty electromagnetic coil 2. Battery supply disrupted by faulty wire 3. The battery can no longer supply voltage 4. Misshapen mechanical locking component 5. Water, cold temperature or dirt damage 6. Improper use	Perform inspection of locking mechanism internals by opening it up with simple tools. Signs of deformation and/or breaking due to torsional shear stress may be visible	Replace: - faulty electromagnetic coil - faulty wires - faulty battery - misshapen mechanical locking component	Mechanism to manually disengage provided	SR1, FR9	3	10
Attaches bike to an external frame or bike rack	a) Lock does not fit around external frame b) Lock is broken along its body and cannot move as intended	Bike cannot be secured to an external frame (vulnerable to theft or loss)	The lock is: - too short - too rigid or not flexible enough to fit - broken: a piece of lock has become stuck, loose or fallen off - too wide to fit through an external frame - used improperly	1. Attempt to fit the lock to an external frame 2. Perform inspection of physical lock to detect any components compromising structural integrity or any signs of deformation or breaking due to bending stress	1. Find a different external frame that fits the lock 2. Repair lock with spare pieces, tightening loose pieces or lubricating moving parts	Lock will be designed with high flexibility	SR2	a) 4 b) 2	a)8 b)10
Transmits and receives signal to engage/ disengage locking mechanism from the app to the lock	Locking mechanism fails to engage or disengage; lock remains in an undesired state	1. If fails to engage, bike not secured (vulnerable to theft or loss) 2. If fails to disengage, the bike cannot be detached from the external frame	1. App malfunction; unable to prepare or receive signal 2. Wireless connection from SmartLock to smartphone disrupted by external force 3. Communication protocol error 4. Battery supply disrupted by faulty wire 5. The battery can no longer supply voltage to the transmitting/receiving unit	Locking mechanism is stuck in an undesired state after multiple attempts to engage or disengage	1. Reboot app 2. Replace any faulty wires 3. Replace faulty battery 4. Manually move smartphone and SmartLock such that they are in closer proximity to each other	Long-lasting battery installed	NFR13, NFR14	3	10
Transmits, receives & displays status information (engaged/ disengaged, battery percentage) from the lock to the app	Status information not shown on the app or is inaccurate	Accurate information not known; battery may be low or require replacement and/or bike may not be secured (vulnerable to theft or loss)	1. Internal app malfunction or high latency 2. Status information not transmitted or received (see 'Transmits and receives engagement /disengagement signal from the App' above) 3. Smartphone malfunction or battery depletion 4. Faulty status sensors	1. The app appears to be malfunctioning (not loading, the screen is frozen or information appears to be inaccurate or lagging) 2. Status information is inaccurate upon inspection of the actual status of lock internals	1. Reboot Smartphone 2. Reboot App 3. Replace faulty status sensors 4. Charge smartphone	Ability to manually check status information	SR1	3	7
Withstands water from rainfall	Water appears to have permeated the SmartLock	1. Electronics damaged 2. Locking mechanism damaged 3. Mechanical components rusted	1. Ineffective waterproofing (permeable sealing) of locking mechanism, electronics and mechanical components 2. Improper use (in inclement weather more severe than average rainfall)	Perform inspection of locking mechanism, electronics and mechanical components. Corrosion, damaged components or water observed.	Replace water-damaged components	1. The system is well sealed against the environment. 2. Aside from housing, the lock system is composed of materials which resist corrosion	SR3, NFR6, NFR7	8	8
'Geotags' location of bike and displays on app	Location information not shown on the app or is inaccurate	Accurate location information not known; the user may not be able to locate bike	1. Smartphone geotag software malfunction (inaccurate location recorded) 2. Internal app malfunction 3. Smartphone battery depletion 4. Location geocached somewhere with poor satellite triangulation capabilities or poor cellphone service 5. Data sharing issue with smartphone geotag software	1. The app appears to be malfunctioning (not loading, the screen is frozen or lagging or information appears to be inaccurate). 2. Geocached location is inaccurate when compared to the actual location 3. Smartphone indicates battery or data sharing issue	1. Reboot GPS software app 2. Reboot smartphone 3. Reboot App 4. Charge smartphone 5. Move to a location with better service and satellite triangulation capabilities	None	mitigation is covered by critical assumptions	7	6
Contains and carries all physical lock components on the bike when not in use	Some or all physical lock components cannot safely be mounted on the bike due to the absence of proper storage that accommodates all components	1. Components placed in inappropriate storage locations such that they dangle off the bike or asymmetrically weigh down the bike 2. Components aren't mounted to the bike	1. Physical lock component storage system lacks space for all components 2. Broken or malfunctioning physical lock component storage system 3. Physical lock components too large to be mounted safely on the bike	Physical lock components cannot be stored safely on the bike	Repair and/or expand faulty storage system	Initial check to ensure mounting system and corresponding components function as intended	FR10	2	5

7 Safety and Security Requirements

7.1 New Requirements - October 2022

The following requirements must be added to the SRS document in the Non-Functional Requirements Category:

SR1: Internal parts of locking mechanism shall be accessible and replaceable (see NFR12 in SRS).

SR2: Product shall be adaptable and be able to fit a wide variety of external frames/bike racks (see NFR14 in SRS).

7.2 Existing Requirements

The following requirements have already been included in the SRS document, and are restated here for convenience:

FR6: Lock must only be engaged/disengaged by the intended user(s).
FR7: The lock can be mounted to the bike's frame.
NFR11: Battery must last for greater than 1 month and/or 60 rides before needing to be replaced or charged.

8 Roadmap

The safety requirements that will be implemented in the scope of Mechatronics Capstone 4TB6 are SR1 and SR2. They are vital to the functionality, safety and security of the SmartLock and are reasonably achievable given the constraints of the course, project and Team.

Other requirements were identified as being important for a high-quality project, but the team has decided it is not feasible to implement them within the time frame or resources of the project, and are therefore out of our scope. These requirements are:

SR3: Product shall be made from anti-corrosive materials.

SR4: The lock must be waterproofed to withstand normal rainfall.

SR5: The lock must be waterproofed to withstand normal splashing while riding.