DataPlex

FUNCTIONAL SPECIFICATIONS

Product: **Panic Grip**

DOCUMENT REVISION HISTORY

Document Revision/Date		Description of Change	Originator
1.0	25/01/2024	Initial draft of Panic Grip Functional Specs A dedicated section for Open Questions	Anurag Verma Shashank Mishra

Table of Contents

1 Abstract 4
2 PanicGrip – Smart Case 6
2.1 Form Factor. 6
2.2 Bluetooth Hardware 6
2.1 Other Components 6
3 Panic Grip - Smart Phone App 7
3.1 Operating System 7
3.2 Hardware Components 7
3.3 Authentication 7
3.4 Configuration 7
3.5 App functionality 8
4 PanicGrip – Security 8
4.1 Bluetooth Security 8
4.2 OS Security 8
4.3 User level Security 9
5 PanicGrip – Reliability 9
5.1 Bluetooth Reliability 9
5.2 High Availability 10
5.3 Signal Strength 10
5.4 Mobile Data / Internet 10
5.5 Fault Tolerance 10
5.6 Graceful termination of hardware activities 10
5.7 User Level 10
6 PanicGrip – Error Handling 11
6.1 Smart Case Bluetooth chip non-functional 11
6.2 Smart Case failed in sending the Bluetooth message to Smart Phone App. 11
6.3 Bluetooth Packets Collision 11
6.4 Bluetooth Packets Corruption 11
6.5 Weak Tower Signals / No Signal 11
6.6 Microphone non-functional 11
6.7 Camera non-functional 11

6.8 Flashlight non-functional 11
7 Open Questions 12
7.1 Questions on Smart Case 12
7.2 Questions on Configuration 12
7.3 Questions on App functionality 12
8 Appendix - A 13
9 Appendix - B 14

1 Abstract

The Panic Grip is a proposed product whose purpose is to provide a sense of security and safety to its users. It is designed as a personal safety device that can be used in emergency situations. The product

Functional specification of the proposed "Panic Grip" product is described in this document. The below Figure 1.1 is an embodiment of the PanicGrip Product. In the figure, two components are shown:

Smart Case: A mobile phone case/cover which will be equipped with Bluetooth microchip and other associated hardware and features. It allows a user to trigger an alert in case of an emergency by pressing a designated button. This will send an alert to the Smart Phone App which will then notify the designated emergency contacts with the user's location.

Smart Phone App: A Mobile phone application installed and running on a Smart Phone. Smart Phone also supposed to have basic features and functionalities such as Bluetooth, Camera, Audio/Video, Microphone, Speaker, Flashlight, GPS etc.

Smart case - Client	Smart Phone App - Server
(Device with a panic button)	(Panic Grip App)

Figure 1.1

The combination of Smart Case and PanicGrip App on a Smart Phone constitutes the Product named as PanicGrip.

Overall, the Panic Grip product is a useful tool for people who are concerned about their personal safety. It provides a sense of security and peace of mind knowing that help is just a button away. The combination of the Smart Case and Smart Phone App make it a reliable and efficient tool for emergency situations.

The Figure 1.1 also denotes that the Smart Case will act as a Client and App on Smart Phone as a Server. The communication between Smart Case and PanicGrip App will happen through Bluetooth protocol. The flow of the commands from the Client and the action taken by the Server is shown in the Figure 1.2

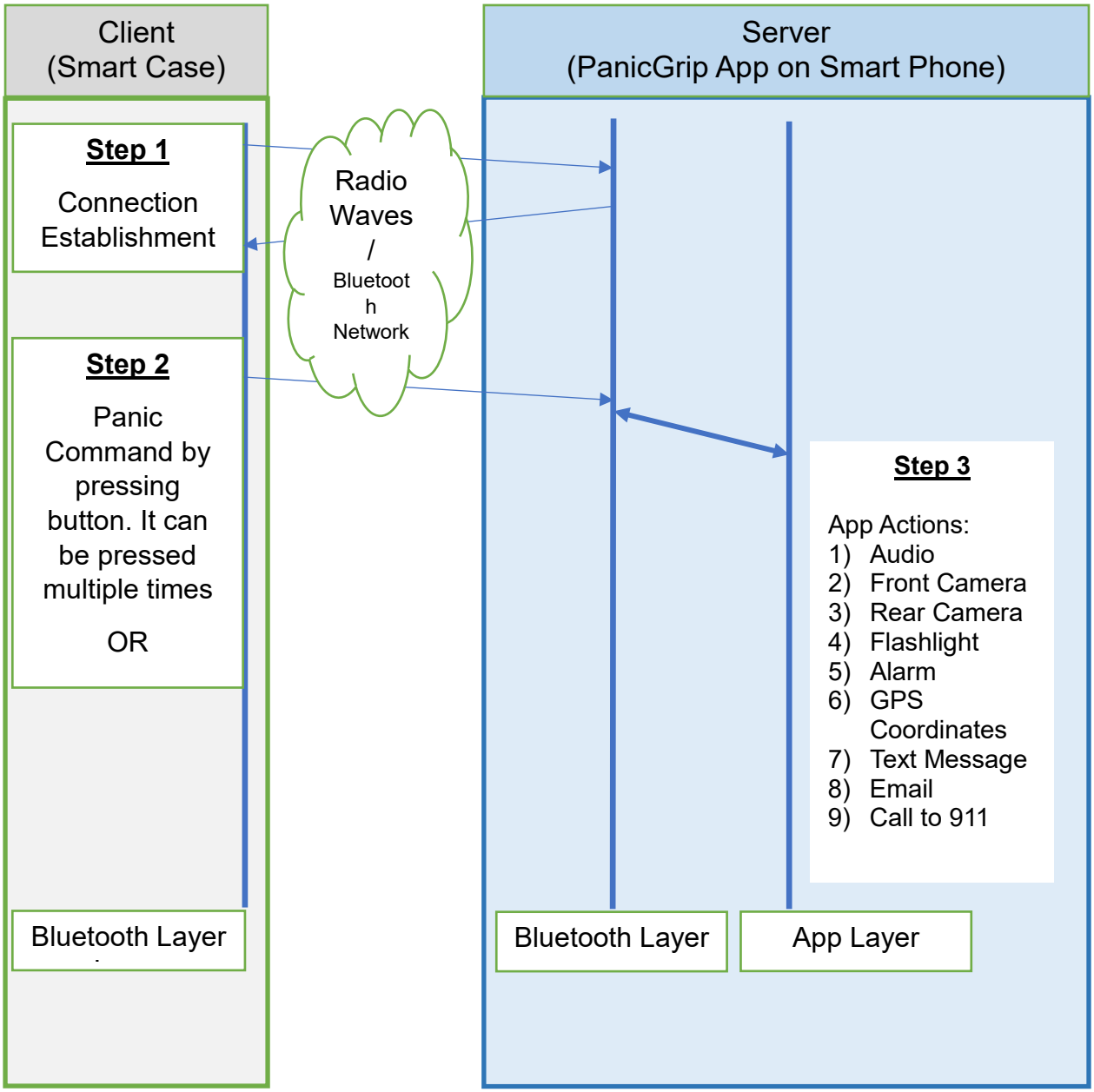

Figure 1.2

In the subsequent sections we are going to cover top level details of Smart Case and PanicGrip App.

2 PanicGrip – Smart Case

Smart Case will be have following hardware details and attributes

2.1 Form Factor.

1) All latest Android Smart Phones (subject to how far we can support backward)
2) All latest iOS Smart Phones (subject to how far we can support backward)

2.2 Bluetooth Hardware

We will be considering following list (but not limited to) of attributes/features/specifications of Bluetooth hardware present in the Smart Case.

Attributes, Specifications and Features of Bluetooth	
Standard	IEEE 802.15.1
Frequency Range	2.402 to 2.48 GHz.
Version	5.4 (Min 4.0)
Class / Type	1) Bluetooth Low Energy (BLE) 2) Bluetooth Classic
Profile	1) Emergency Profile 2) Generic Profile
Distance	Not more than 10 feet.
Power Consumption	Not more than 2.5 Milliwatts
Connection Types	1) Peer to Peer 2) Broadcast

More details about Bluetooth are available in Appendix section.

The Smart Case can/will have other components to complement the Bluetooth chip and its functionality.

2.1 Other Components

a. Microphone
b. Button
c. Charging Port

3 Panic Grip - Smart Phone App

This section will focus on the different aspects of App.

3.1 Operating System

a. Android OS
b. iOS

Currently we are targeting the latest versions of Android and iOS. We'll come to this point for backward compatibility.

3.2 Hardware Components

PanicGrip App will need access to the following list of hardware components after a successful installation and first-time invocation.

1) Microphone
2) Camera
    a. To take pictures
    b. To record videos
3) Location / GPS
    a. Current location aka coordinates
4) Flashlight
5) Disk

3.3 Authentication

The authentication process will depend on the Bluetooth handshaking and authentication process. A successful authentication means Smart Case and Smart Phone App will be paired initially and connected for later message exchanges.

3.4 Configuration

PanicGrip will allow users to configure following things

1. Contact Numbers
2. Email Address
3. Time for audio recording
4. Time for video recording
5. Alarm Duration
6. [..]

All the configurable data will be stored in a text file on the disk of the Smartphone. The exact no. of contact numbers and email addresses will be decided at the time of designing the App.

3.5 App functionality

Primary Feature

PanicGrip App will be configured as per the details mentioned in Configuration section

PanicGrip App will be in passive mode listening for messages from Bluetooth stack. As soon as the “PANIC” messages arrives, APP will activate Flashlight and Alarm and start capturing following data in parallel:

1) Audio recording of 10 seconds from microphone
2) Video recording of 10 seconds from Front camera
3) Video recording of 10 seconds from Rear camera
4) GPR Coordinates (Latitude and Longitude)

Once the data is captured, it will compress the data and send it to the configured recipients over email along with a preconfigured text message.

In addition to sending email and text message, the App will also invoke Emergency Phone Number (911).

Secondary Feature

App will also present a virtual “Panic Button” on its screen for those users who have been already using the phone i.e. they have time to open the App. In that scenario, User can press this virtual panic button and the product will achieve the same result as it mentioned in **Primary Feature**.

4 PanicGrip – Security

PanicGrip security will depend upon following components:

4.1 Bluetooth Security

The Bluetooth security model includes five distinct security features: pairing, bonding, device authentication, encryption and message integrity.

- Pairing: the process for creating one or more shared secret keys
- Bonding: the act of storing the keys created during pairing for use in subsequent connections in order to form a trusted device pair
- Device authentication: verification that the two devices have the same keys
- Encryption: message confidentiality
- Message integrity: protects against message forgeries

4.2 OS Security

a. Android Security
b. iOS Security

4.3 User level Security

User is supposed to take care of the Smart Case and Mobile phone.

5 PanicGrip – Reliability

PanicGrip security reliability will depend upon following components or levels:

1) Bluetooth Reliability
2) High Availability
3) Signal Strength
4) Mobile Data / Internet
5) Fault Tolerance
6) Graceful termination of hardware activities.
7) User Level

Let's dive deep into each entry.

5.1 Bluetooth Reliability

Reliability of packets in Bluetooth will be provided through following means.

The Cyclic Redundancy Check (CRC)

All Bluetooth packets contain a Cyclic Redundancy Check (CRC) field which appears at or near to the end of the packet. CRCs are a commonly used mechanism for detecting cases where transmitted data has been unintentionally changed due to issues like collisions.

When a new packet is formulated by the link layer, a CRC value is calculated by applying the CRC algorithm to the other bits in the packet. The resultant 24-bit value is then added to the packet. On receiving a packet, the link layer in the receiving device recalculates the CRC and compares the result with the CRC value included in the received packet. If the two values are not the same, it is concluded that one or more bits in the transmitted packet have been changed and the packet is discarded. It should be noted that the CRC is not a security mechanism since a packet could be deliberately altered and the CRC easily recalculated.

The Message Integrity Code (MIC)

Bluetooth LE packets may be encrypted. All encrypted packets include a field called the Message Integrity Check (MIC). The MIC is in fact a message authentication code but since the acronym MAC has other uses in the field of communications, in the Bluetooth specification, MIC is used. The MIC is not a reliability feature per se. It is a security feature whose purpose is to enable the detection of attempts to deliberately tamper with the contents of a packet. But since part of our informal definition of reliability is that the data transmitted should be the data received and we acknowledge that changes may be unintentional or deliberate, we include it here for completeness.

Communication of data over Bluetooth® technology makes use of more than one radio channel. Using multiple radio channels makes Bluetooth communication highly reliable in busy radio environments, where collisions and interference are likely to occur

5.2 High Availability

A single Bluetooth chip on a Smart Case will be a single point of failure (SPOF). If the chip becomes non-functional due to any reason, the PanicGrip App on the Smart Phone will not be able to send any information to the recipients.

In order to handle the SPOF scenario and achieve High Availability, Smart Case can have another Bluetooth chip in the PCB. It essentially means that, there will be two Bluetooth chips and both will be in either Active-Active mode or Active-Passive mode.

Here both the chips will be paired in advance with the Smart Phone Panic Grip App and Panic Button will activate both the Bluetooth chips to send “PANIC” messages to Panic Grip App. The precondition here is that, we need to check Bluetooth specs whether this configuration is allowed.

5.3 Signal Strength

Mobile phone signal strength will play a major role in sending text messages, calling 911 and providing internet / Mobile data.

5.4 Mobile Data / Internet

Mobile data / Internet should be up and running all the time. It will be used to send emails to the recipients.

5.5 Fault Tolerance

App is supposed to be functional all the times irrespective of failure in any or all hardware components it accessed. If all of the hardware components failed then

5.6 Graceful termination of hardware activities

PanicGrip App will depend upon the hardware as described in Hardware Components section. If any or all of the hardware components are already being utilized by other Apps then a graceful termination will be required in order to achieve the desired functionality of PanicGrip App and also the Mobile Phone is into consistent state.

5.7 User Level

User is not supposed to force stop the App by any means. User should periodically check if the APP is running. This level is one of the weakest links in achieving reliability.

6 PanicGrip – Error Handling

Errors in PanicGrip product can happen at multiple places. Following are some of the error scenarios.

1. Smart Case Bluetooth chip non-functional
2. Smart Case failed in sending the Bluetooth message to Smart Phone App.
3. Bluetooth packets dropped due to collision
4. Bluetooth packet corrupted
5. Weak Tower Signals / No Signal
6. Microphone non-functional
7. Camera non-functional
8. Flashlight non-functional
9. No Internet.

Let's dive deep into above error scenarios.

6.1 Smart Case Bluetooth chip non-functional

App will periodically check the above errors and notify or alert the User

6.2 Smart Case failed in sending the Bluetooth message to Smart Phone App.

This error can be avoided by providing the High Availability of Bluetooth devices in Smart Case.

6.3 Bluetooth Packets Collision

6.4 Bluetooth Packets Corruption

The above errors will be handled at Bluetooth layer with the help of CRC and MIC

6.5 Weak Tower Signals / No Signal

App will keep on retrying for sending the Panic Data until the Mobile Phone battery becomes low (hits 10 percent threshold)

6.6 Microphone non-functional

6.7 Camera non-functional

6.8 Flashlight non-functional

In the event of any hardware failure, the PanicGrip App on the Smart Phone will be able to capture as much data as it can from the available list of functional hardware components.

7 Open Questions

7.1 Questions on Smart Case

Q1) what will be the programming interface for Bluetooth chip. Will there be any API or APIs?

Q2) Will the microphone be a part of Smart Case for taking voice command. If yes, then will the microphone be always in listening mode to take voice command?

Q3) Class of the Bluetooth chip i.e. BR/EDR or LE or any other.

Q4) How the Bluetooth device will be charged?

7.2 Questions on Configuration

The answers are just for reference purpose.

Q1: What will happen if a user deletes the App's configuration data from Settings?

Ans: App will keep default values wherever required.

Q2: Will the configuration file a user readable text file. What if someone changes/tamper that file?

Ans: For security purpose we can think of encrypting this file. Tampering thing needs to be discussed but normally it is the duty of the smart phone owner/user to secure the data present in his mobile phone. Alternatively, we can think of storing the file in Cloud Storage of the User.

7.3 Questions on App functionality

There could be a possibility that, while processing "PANIC" message some of the hardware components might be busy in some operations such as:

1. A phone call is already going on.
2. A video player is active i.e. playing a video.
3. A Camera app is already active.
4. Location is active due to Google Maps App.
5. Bluetooth device on the Smart Phone is already connected to other Bluetooth devices such as Car Music system, Bluetooth headset

PanicGrip App will need to stop these activities.

Q1: How will the Panic Grip App stop the ongoing activities on the dependent hardware?

8 Appendix - A

Bluetooth General Description

Bluetooth wireless technology is a short-range communications system intended to replace the cable(s) connecting portable and/or fixed electronic devices. The key features of Bluetooth wireless technology are robustness, low power consumption, and low cost. Many features of the specification are optional, allowing product differentiation. There are two forms of Bluetooth wireless technology systems: Basic Rate (BR) and Low Energy (LE). Both systems include device discovery, connection establishment and connection mechanisms. The Basic Rate system includes an optional Enhanced Data Rate (EDR) extension. The Basic Rate system offers synchronous and asynchronous connections with data rates of 721.2 kb/ s for Basic Rate and 2.1 Mb/s for Enhanced Data Rate. The LE system includes features designed to enable products that require lower current consumption, lower complexity and lower cost than BR/EDR. The LE system is also designed for use cases and applications with lower data rates and has lower duty cycles. The LE system includes an optional 2 Mb/s physical layer data rate and also offers isochronous data transfer in a connection-oriented and connectionless mechanism that uses the isochronous transports

Bluetooth Transmitter / Receiver Synchronisation

The type of radio used in Bluetooth® devices is called a half-duplex radio. This means that two devices can communicate with each other in each direction, but not simultaneously. First one radio transmits while the other radio receives, and then the other radio transmits while the first radio receives. A radio of this type can be in one of three states at any one point in time; either transmitting on a given radio channel, listening to a particular channel or idle.

If a receiver device is not listening when another in-range device transmits some data or it is not listening on the channel that the transmitter is using then the transmitted data will not be received.

Coexistence and Collocation

Different radio technologies may use the same part of the radio spectrum. Bluetooth® technology and Wi-Fi[1] both use the Industrial, Scientific and Medical (ISM) 2.4GHz band, for example. When two or more radio technologies share a part of the radio spectrum, we have what is known as a *coexistence* issue. One technology may interfere with the other if suitable mitigation steps are not taken. When two or more radio technologies are supported by the same device, they are said to be collocated. *Collocated* radios may interfere with each other without measures being taken to minimise or eliminate this issue.

Spread Spectrum

Bluetooth® technology uses the 2.4GHz ISM radio band. 2.4 GHz ISM does not define a single frequency, but rather it defines a range of frequencies, in this case starting at 2400 MHz and ending at 2483.5 MHz when used with Bluetooth LE, this frequency range is divided into 40 channels, each 2 MHz wide. Bluetooth BR/EDR divides it into 80 channels of 1 MHz width.

Each channel is numbered, starting at channel zero. Channel zero has a centre frequency of 2402 MHz, leaving a gap of 1 MHz between the lowest frequency delimiting channel zero and the start of the ISM 2.4 GHz band. Channel 39 has a centre frequency of 2480 MHz, which leaves a gap of 2.5 MHz to the end of the ISM 2.4 GHz band

Single Points of Failure

Communication systems are just that. *Systems*. Systems by definition, consist of multiple inter-related components and in some cases, a component may be key to the overall, reliable operation of the system. Failure of that one key component can therefore cause the whole system to fail. A component with this property is known as a *single point of failure*.

.

9 Appendix – B

List of documents which laid the foundation of this Functional Spec.

1. Panic Grip Patent Casing
2. Program Flowchart Page 2 Casing
3. Technical Drawings

Note: Appendix B files are added as PDF attachment. Use Adobe PDF reader to view.