Smart Wearables with Central Devices and Their Utilization in the Military

Bachelor's Thesis

Degree Programme in Computer Applications

Autumn 2025

Sara-Sofia Paananen

HAMK
Häme University
of Applied Sciences

Tiivistelmä

Koulutus	Tietojenkäsittelyn koulutus / Computer Applications
Tekijä	Sara-Sofia Paananen
Työn nimi	Äly- ja keskuslaitteen käyttö armeijassa
Ohjaaja	Mirlinda Kosova-Alija

Vuosi 2025

HAMK Tech on kokeillut e-urheilun suunniteltuja älyhihojen kaksikäyttöä yhdessä maanpuolustuskorkeakoulun kanssa. Nyt käsillä on e-urheiluun suunnitellun prototyypin jatkokehittäminen konseptiksi armeijalle. Tämä opinnäytetyö tarjoaa prototyypin käyttöliittymäsuunnittelusta ja esittelee älykkään puettavan laitteen prototyypin ensimmäisen iteraation.

Ensin teoriaosassa selitetään Suomen puolustusvoimien älylaitteisiin liittyvät käsitteet. Näitä ovat teoria älyvaatteiden teknologiasta, teknologiasta puolustusvoimissa, laiteturvallisuudesta ja prototyyppien käytöstä. Opinnäytetyössä käsitellään sitten uuden älyvaatteen kehitystä ja käyttöliittymäsuunnittelun prototyyppejä. Ensisijainen tutkimusmenetelmä oli kehitysprojekti. Tämä opinnäytetyö on enemmän teoreettinen kuin käytännöllinen.

Tässä opinnäytetyössä kehitetyt prototyypit eivät ole lopputuotteita, vaan tarkoitukseen rakennettuja konsepteja. Ne auttavat validoimaan kehitystä ja luomaan kehyksen HAMK Techin meneillään olevalle projektille. Prototyypin luomisen kautta tuotetun tiedon on tarkoitus ohjata lopputuotteiden tulevaa kehitystä. On suositeltavaa, että HAMK Tech ottaa huomioon turvallisuus- ja ympäristötekijät, joissa Suomen puolustusvoimat aikoo käyttää näitä laitteita.

Asiakkaan antama palaute korosti opinnäytetyön näkökohtia olennaisiksi sotilaskäyttöön tarvittavien puettavien teknologioiden suunnittelussa. Opinnäytetyössä esitetään kaikki vaatimukset ja projektin alkuvaiheessa tuotetut laiteprototyypit. Tulokset tukevat järjestelmien käyttöä sotilaskäytössä.

Avainsanat Smart wearables, Military, Peripheral device, Central device, Haptic feedback, Prototype
Sivut 41 sivua ja liitteitä 1 sivu

HAMK
Häme University
of Applied Sciences

Glossary

DP	Degree Programme in Computer Applications
Author	Sara-Sofia Paananen Year 2025
Subject	Smart Wearables with Central Devices and Their Utilization in the Military
Supervisors	Mirlinda Kosova-Alija

HAMK Tech has tested the dual use of smart sleeves designed for esports together with the National Defence University (NDU). The prototype designed for esports use is now being further developed into a concept for the military. This thesis provides a prototype of the user interface design and shows the first iteration of the smart wearable device prototype.

First, the concepts related to smart wearables in the military are explained in the theory. These include theory on smart wearables technology, technology in the defence force, device security, and prototyping. The thesis then proceeds to discuss the development of the new smart wearable device and the UI design prototypes. The primary research method that was used was the development methodology. This thesis is more theoretical than practical.

These prototypes developed in this thesis are not final products but are purpose-built concepts. They serve to validate development and establish a framework for the ongoing project at HAMK Tech. The knowledge generated through the prototype creation is intended to guide future development of the final products. It is recommended that HAMK Tech takes into consideration the security and environmental factors in which the military will utilize these devices.

Input from the client highlighted the thesis aspects to be essential for designing wearable technologies required for military purposes. The work of the thesis presents all requirements and device prototypes that have been produced during the beginning of the project. The results support the use of the systems for military use.

Keywords	Smart wearables, Military, Peripheral device, Central device, Haptic feedback, Prototype
Pages	41 pages and appendices 1 page

Glossary

Wearables	**Wearables** – Electronic devices that are designed to be worn on the body.
NDU	**National Defence University** – Military education and training for armed forces
Haptic Feedback	**Haptic Feedback** – Physical stimuli used in technology that simulate tactile experiences.
UI	**User Interface** – Communication between a person and a machine, allowing a user to control a device/software and receive feedback.
UX	**User Experience** – Overall experience of a person using a product.
Sensors	**Sensors** – A device that receives and responds to stimuli or a signal.
Peripheral Device	**Peripheral Device** – External device which preforms specific tasks and rely on central devices to operate.
Central Device	**Central Device** – Executes instructions of a user, for example a phone.
IoBT	**Internet of Battlefield Things** – Allows large scale connectivity between humans, networks, and interfaces.
OSI	**Open Systems Interconnection** – Framework that divides communication networks into abstract layers.
RUP	**Rational Unified Process** – In software development framework that is processed in phases.
ZTNA	**Zero Trust Network Access** – Security model which establishes trust with authentication and monitors access attempts.
OPSEC	**Operational Security** – Protects system integrity.
CPU	**Central Processing Unit** – Hardware component that converts data and allows devices to perform tasks.

Table of Contents

Figures

Tables

Appendices

1 Introduction

Technology as we know has been a big part of this past decade and has been integrated into everyday life, reshaping the way we work, communicate and manage our well-being. While smartphones help ease our connections globally, there are a lot of new technological revolutions underway, one includes the rise of smart wearables. These devices are designed to be worn on the body and to collect data that may provide insight into our social interactions, health and fitness. Smart wearables technology has very big potential for a variety of environments.

The introduction describes the author's interest in this thesis that explores smart wearables technology and its use for tactical communication within the military. This research is conducted with HAMK Tech, a research unit in the Häme University of Applied Sciences, which is developing wearable devices. Originally the wearables were only conceived for esports players but with time the scope expanded to the military and their communication needs in operations. The core usage for the device is to send haptic feedback to other personnel which potentially eliminates the need to communicate using hand signals or code words. The prototypes created in this thesis will demonstrate the core technical and functional requirements for a full-scale application. This will ensure that the final product is effective for real-world deployment.

Research questions that will be provided with a solution in this thesis:

- What are the minimum performance requirements for a haptic communication system to be considered operational in a defence context?
- What are the requirements for smart wearable textiles to support communication of patrols and groups in the defence sector?

2 Smart wearables

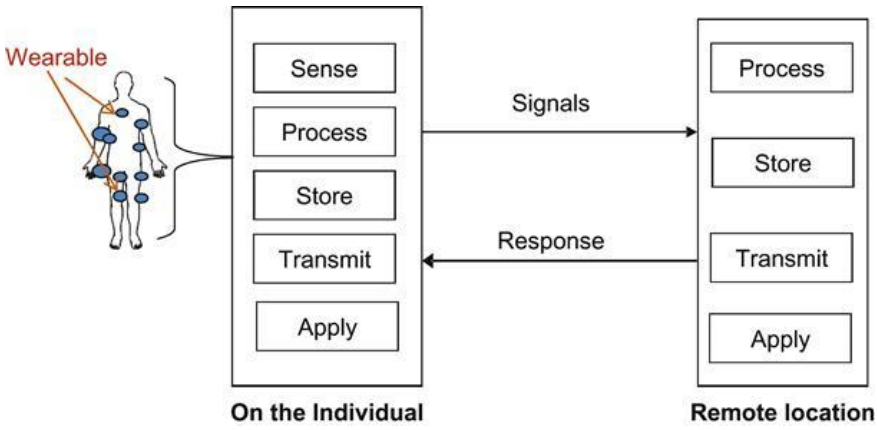
Wearables were briefly explained in the introduction but will be discussed more in depth in this chapter. To understand wearables in this thesis's context, it is necessary to know the technology itself. This chapter contains what wearable technology is, what attributes they have as well as taxonomy of wearables.

2.1 Wearable Technology

"Wearable" term nowadays has multiple meanings. It doesn't just refer to clothing; it can also refer to an accessory which is able to process personal information. The device can be a smart watch, a sensor on a helmet or even a smart garment used for running. Through these innovations, wearables can be personalized for specific usage and transform the standard of living. (Sazonov, E., 2014, chapter 1.1)

There are many tasks' wearables can perform, such as, sense, store, transmit, analyse and utilize. Each of these functions depend on what purpose the wearer is using the wearables devices for. (Sazonov, E., 2014, chapter 1.1) To better understand the way wearables work, Figure 1 shows what happens when the wearables are activated. For example, a wearable senses that a diver is in depths where they shouldn't be. The wearable then processes the data and an alert is issued. Simultaneously, the data can be transmitted to a remote location to be processed, for example the diving crew to know what is going on underwater. (Sazonov, E., 2014, chapter 1.1)

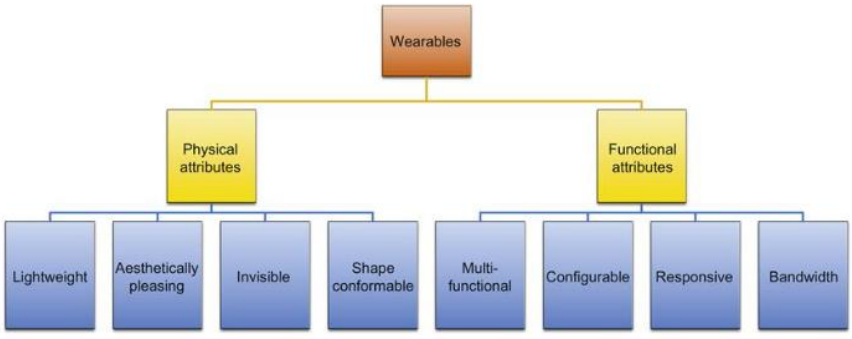
Figure 1. Workflow of how sensors can work with remote devices (Sazonov, E., 2014, chapter 1.1)



2.1.1 Wearable Attributes

All wearables must have the capability to sense (Sazonov, E., 2014, chapter 2). Wearable devices are equipped with at least one sensor, some of the sensors that may be seen in wearables can be proximity, force, motion, sound or contact sensors. (Becher, B., 2024) Both sensors and the wearable itself need to have functional and physical attributes to be able to be worn and utilized. Figure 2 shows a few attributes that each wearable should have.

Figure 2. Physical and Functional attributes of a wearable (Sazonov, E., 2014, chapter 2)



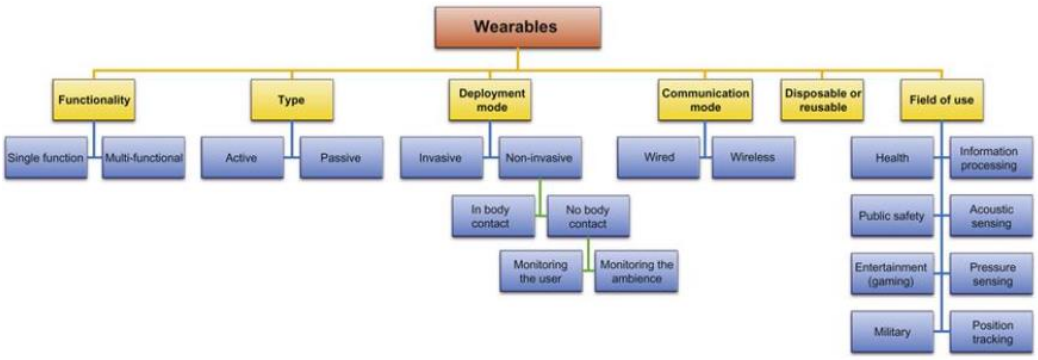
The wearable should be lightweight, and the form of the device should not hinder the movement of the user. A lot of the time the wearables are somewhere where they are visible. Wearers want it to be visually pleasing so that it can be worn even as a fashion statement. Most wearables become an extension of the user so when wearing wearable devices, they should feel comfortable. (Sazonov, E., 2014, chapter 2)

2.1.2 Taxonomy for Wearables

Wearables can be classified in many ways, as single or multi-functional, invasive or non-invasive. Invasive wearables are usually apart of the user and can be inserted through medical procedures. Non-invasive wearables don't require any incisions and can be worn on the user. For non-invasive wearables, they can either be in physical contact with the body or not. If there is no contact with the body, they can either be monitoring an individual or the surrounding environment. (Sazonov, E., 2014, chapter 2.1)

There are a lot of other classifications, such as a wearable being active of passive which can depend on whether the wearable needs power to operate. Another mode which wearables have is being wired or wireless. In wireless cases, the wires are built into the device itself, which allows the user the capability to communicate from a distance. The sensors in the devices can also be reusable or only one-time use. Lastly the wearables can be classified into different fields of application. (Sazonov, E., 2014, chapter 2.1) To better understand the flow of the taxonomy for wearables, Figure 3 shows each classification branch.

Figure 3. Taxonomy for wearables (Sazonov, E., 2014, chapter 2.1)



Taxonomy helps defining what wearables certain can do so that they can be selected according to the restrictions. It also helps the development and new wearables and their needed attributes for their intended usage.

3 Haptic Feedback

“Haptic feedback refers to the use of touch and vibrations to communicate sensations or feelings to a user, providing a more immersive experience” (Xu, T., n.d). Haptic technology has been sought to design ever since the 1990s. They wanted to create products which allow users to “feel” virtual objects whenever they receive tactile feedback. (Xu, T., n.d) This chapter talks about the different devices and how they work, what types of feedback they send, what benefits they offer and where haptics are used in the industry.

3.1 How haptic devices work

Haptic devices are utilized in many ways. They provide tactile feedback, which simulates digital environments using a sense of touch through motions, vibrations and forces. Haptic devices use sensors, motors and speakers as tools to be able to create haptic feedback. When a certain action is preformed, the programme on the device will output haptic feedback. The stimulus the user senses can be achieved by various technologies such as an exoskeleton, which are worn to support and assist movement, skin indentation devices or vibrotactile technology. (Xu, T., n.d)

Exoskeletons can be commonly found in the gaming industry and create stimuli by using active force feedback. To create these stimuli the devices, depend on electromechanical motors with which you target specific body parts which correspond with the experience in the game. (Xu, T., n.d)

Skin indentation can be spotted in various technology like haptic sleeves or other wearables. The mechanisms imitate the feeling of touching or moving an object when compressing skin. (Xu, T., n.d)

Lastly vibrotactile technology which is frequently used in virtual reality (VR) devices. Haptic devices that are equipped with this technology can create a shaking or rumbling sensation in addition to creating vibrational patterns. (Xu, T., n.d)

3.2 Feedback types

This division presents different types of feedback haptic devices can perform. Haptic feedback can be various forms, such as force and thermal feedback, but the most important category is tactile and haptic feedback in this thesis. (Fleury, M., 2020, chapter 2.2)

Tactile interfaces are in direct contact with the surface of the skin and stimulates it. With the sensation it provides it can be classified as tactile. The feedback can be a vibration, pressure, curvature, texture, friction, softness or hardness, temperature, and contact. Normally tactile devices should be small and lightweight. If the device is worn by a mobile user, the power it uses should be minimized. (Fleury, M., 2020, chapter 2.2.2)

Force feedback emulates realistic pressure and weight against the user and stimulates their ligaments, skin and muscles. It is applied deep enough that the users body parts can move involuntarily. Force feedback devices can either be biometric or non-biometric. Biometric force feedback haptics imitate human body parts like haptic gloves or exoskeletons. Non-biometric devices can for example be a wheel in a driving simulator. (Xu, T., n.d)

Thermal feedback haptics change the temperature on the skin, mimicking touching and object that is hot or cold. To create the thermal ques, actuators are applied to the skin which then transforms energy into heat and move to other parts of the body. So that the heat moves as quickly as tactile feedback, thermal feedback requires more power. (Xu, T., n.d)

Haptic feedback enhances user experience by providing benefits in immersion, accessibility, and accuracy. Its ability to create immersion makes digital interfaces feel realistic, like by a “click” of a touchscreen keyboard or game controller vibrating with a user’s actions in-game. Furthermore, haptics is a crucial part of accessibility, delivering information from touch to distinct vibration patterns. This is vital for users with visual or hearing impairments. Finally, haptic feedback devices improve user accuracy by providing tactile information of interactions, from reducing typos on touchscreens to improving precision in fields like robotic surgery training. (Xu, T., n.d)

4 Device Security and Connectivity

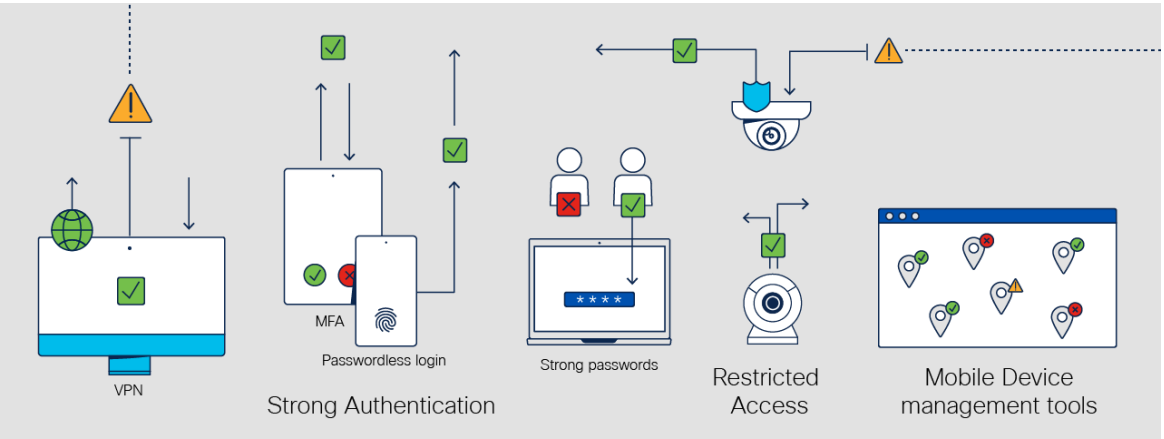
Security and connectivity of devices are crucial to have. This chapter discusses security that should be taken into consideration whenever creating systems as well as what Bluetooth low energy is and what benefits it provides.

4.1 Security

Being able to secure devices is crucial to safeguard data and be able to deny access to unauthorized users. Securing devices requires a multilayered approach where the zero trust network access (ZTNA) policy can be utilized to mitigate risks. (Cisco, n.d.) Security in the military is crucial since military devices are the foundation of defence operations. Devices used in military settings contain sensitive data, if compromised it can lead to mission failures and threaten national security. (Ace Computers, 2025)

“IoT device security helps prevent IoT devices from introducing threats to a network” (Cisco, n.d). Solutions can be deployed to grant visibility of all IoT devices on a user’s network. IoT means the Internet of Things which is a network of connected devices where different devices can communicate with each other and in remote servers. With the help of automated responses, it is faster for the user to react and detect abnormalities as well as reduce any risks of systems being compromised. (Cisco. N.d.) Figure 4 shows different methods that can be used to secure devices.

Figure 4. Different security methods (Cisco, n.d.)



To be able to control users access to any systems, data or networks, whitelisting and blacklisting are commonly used methods. Whitelisting lists systems, applications, users, email domains, IP addresses, or other institutions which have authorised access to a network, resource, or system. Blacklisting on the other hand defines what is prohibited from accessing information. (Zero Trust Blog, 2024)

For devices to meet standards required in the military, they are to be equipped with advances security features. Some of these include hardware-based encryption, that protects data in transit or at rest; and multi-factor authentication (MFA), which verify the user's identity using biometrics or PINs.

4.2 Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE) is a variant of Bluetooth technology which is a common choice nowadays for wireless connection between devices that are in close proximity to each other. It's designed for devices that may need to run for long periods of time and consume less power than other devices. (Afaneh, M., 2023)

BLE is a good option for applications that require data transferring periodically. Bluetooth is in a constant state of connectivity unlike BLE which only operates when exchanging data. This helps devices extend their battery life and conserve energy. BLE is an excellent choice for IoT and IoBT applications. (Afaneh, M., 2023)

To be able to utilize the benefits of BLE better, it's crucial to understand the roles BLE devices play in communication process. This process requires the peripheral and central device roles; these are shown in Table 1. (Afaneh, M., 2023)

Table 1. What does peripheral and central mean (Afaneh, M., 2023)

BLE Roles	Definitions
Peripheral Devices	Provide data that are typically resource-constrained and low-power devices

Central Devices	“Client” devices that are less constrained and use more power

Central devices can be used to initiate connections, while peripheral devices are only able to advertise their presence to other devices in their vicinity. When these devices have been connected data can be retrieved and sent. The servers or data providers are the peripherals; the centrals are the client or consume data. These differences are crucial knowledge when designing and developing products that utilize BLE. (Afaneh, M., 2023)

5 Technology in the Military

Technologies like wearables have primarily been developed for use in daily civilian life but have been integrated into other sectors like the military. Technology in the military has been essential and leads to many new technological breakthroughs which can potentially change warfare. (Andås, H. E. 2020, p. 7) This chapter provides information about what Internet of Battle Things is, the different layers on the Internet of Battlefield Things, different challenges, solutions and future research developments, as well as what ruggedized devices are.

5.1 Internet of Battle Things

Because of new advancements in technology the Internet of Battlefield Things (IoBT) was created. “The concept of the IoBT was proposed by the U.S. Army Research Laboratory (ARL) to enable predictive analytics for intelligent command and control and battlefield services.” (Shi, H., et al., 2019, chapter 1) IoBT has become a practical reality, as soldiers are the ones who now depend on the equipment provided to communicate, plan and execute missions in large scales. (Shi, H., et al., 2019, chapter 1)

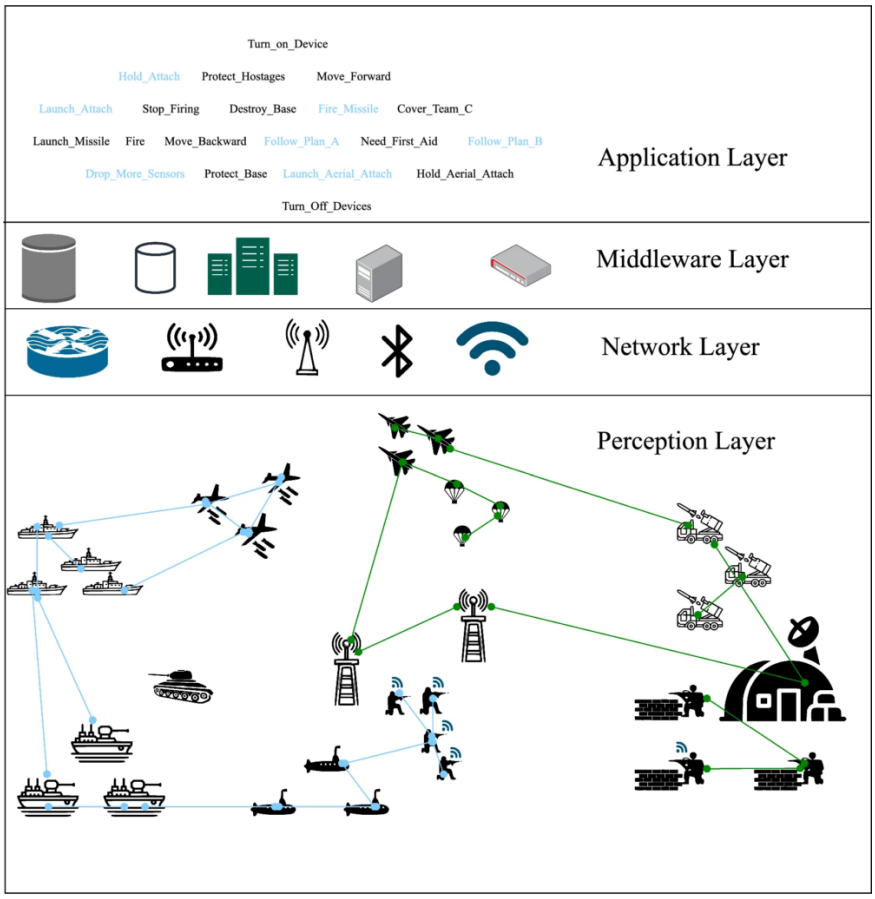
Even before the concept IoBT was initiated, researchers had begun the design of soldier equipment where there were multiple sensors. The research was primarily aimed to enhance situational control and resource competitiveness but additionally also led to increased security for soldiers in combat scenarios. (Shi, H., et al., 2019, chapter 2) There already are many existing wearable devices. Figure 5 shows some devices that soldiers use in the battlefield.

Figure 5. Wearables created for soldiers (Shi, H., et al., 2019)

Name	Research Unit	Type	Characteristic
LifeBEAM	LifeBEAM	Helmet	Uses an optical sensor to measure heart rate
CombatConnect	The Army's Program Executive Office	Wearable electronics system	Distributes data and power to and from devices via a smart hub integrated into the vest or plate carrier
Black Hornet 3	FLIR SYSTEM	Pocket-sized unmanned helicopter	An integrated camera that can be mounted on a squad member's combat vest as an elevated set of binoculars
Ground Warfare Acoustical Combat System	Gwacs Defense	A wearable tactical system	Identifies and locates hostile fire; detects and tracks Small UAVs
ExoAtlet	ExoAtlet	Lower body powered exoskeletons	Provides mobility assistance and decreases the metabolic cost of movement
SPaRK	SpringActive	Energy-scavenging exoskeletons	The collected energy can be turned into electricity to recharge a battery or directly power a device

"An IoBT network is a multi-domain ecosystem, encompassing land, air, sea, space, and cyberspace." (Astute, 2025) All of these ecosystems are intelligently interconnected. The data collected from sensors provide insight of actions soldiers take. Figure 6 describes the "network-centric warfare" concept which aligns with the principles of the Internet of Things (IoT). (Astute, 2025)

Figure 6. "Network-centric warfare" (Astute, 2025)



The architecture used in IoBT evolved from IoT but applies a five-layer model instead of the three or four-lay model that IoT typically has. The physical layer, similar to the Open Systems Interconnection (OSI) is the perception layer. The layer collects data through actuators, devices and sensors that interact with the physical world. (Astute, 2025)

The network layer transmits data that has been acquired from the perception layer to the application and processing layers. Due to the requirements in the battlefield, this layer often relies on different wireless communication tactics such as ad-hoc networks and satellites. (Astute, 2025)

The support layer is the middleware layer, often described as the processing layer. Here data gets pre-processed, filtered, aggregated and secured. Peripheral computing is an external device which connects to another device to extend its potential. In this stage peripheral computing is crucial, since it reduced bandwidth and latency requirements when processing happens closer to the data source. (Astute, 2025)

Lastly the application and business layers, where the application layer provides the soldier and commanders with the user interface and applications that they utilize. Data is visualised, analysed and drives decisions. (Astute, 2025) The business layer resides above the applications and focuses on monetisation, management and strategy systems of the IoBT. (Astute, 2025)

Utilizing technology to communicate in the battlefield comes with its own unique challenges that can determine the success or failure of missions. (Astute, 2025) Table 2 shows the different challenges that arise in the military communications.

Table 2. Communication challenges in IoBT (Astute, 2025)

Challenges	Description and Impact
Interoperability	IoBT systems are intrinsically diverse. Devices use various communication protocols which vary in data formats. They all must be able to seamlessly communicate.
Power and Energy Management	IoBT devices operate in off-grid and remote locations while also being battery-powered. To be able to operate its critical for the devices to minimize energy consumption.
Network Resilience	Networks are prone to physical damage, jamming and disruption. Devices must be capable to adapt, self-heal and uphold communication in degraded conditions.
Security	IoBT is vulnerable to attacks such as data manipulation, spoofing, denial-of-service and eavesdropping. To deter attacks systems should be encrypted, authenticated, and have intrusion

	detection systems in the constraints of IoBT recourses.
Cybersecurity	Preventing various cyber-attacks.
Data Management	Delivery and processing of data.

Table 3 lists different researched solutions that can address certain communication challenges.

Table 3. Research and Solutions (Astute, 2025)

Research	**Solutions**
Blockchain for Trust Management	Created systems for IoBT that are decentralised and tamper-proof. Only people authorised can access the network and data.
Attribute-Based Encryption (ABE)	Grants access control to data ensuring that specific devices can access and decrypt information.
AI/ML for Network Optimisation	To predict network failures, detect anomalies, and automate networks, machine learning algorithms are used to respond to changing conditions.
Edge Computing	The closer the processing is to the sensors helps with reducing bandwidth and latency requirements. In disconnected environments it’s possible to make real-time decisions.

Deception-Based Security	To mislead opponents, dummy IDs are used to protect the location of IoBT nodes
Cross-Layer Design	Utilize different network layers when communicating. This can lead to reducing energy savings.
Energy Harvesting	Portable devices have solar panels.
Software-Defined Networking (SDN) and Network Function Virtualisation (NFV)	Allow dynamic and flexible network management, which makes adapting to changings battlefield conditions easier.
5G and Beyond	IoBT must have high bandwidth and low latency of 5G to support applications.
Lightweight encryption	Overhead of security is reduced.

Significant progress has been made with researching solutions for communications in the IoBT environment. Nevertheless, there are several gaps in IoBT research that remain. Table 4 lists a few that are crucial to IoBT development of new technologies that will further enhance their devices full potential. (Astute, 2025)

Table 4. Future research for IoBT development (Astute, 2025)

Future Research	Developments
Integration of AI and Edge Computing	Edge devices can run lightweight AI models efficiently even when constrained.

Context-Aware Communication Protocols	In real-time protocols must be able to adapt to changing conditions.
Proactive Cybersecurity	Cyberattacks get countered by proactive defences.
Interdisciplinary Collaborations	IoBT solutions are made sure to be operational with the collaboration between engineers, military strategists.
Data Management	Data that is collected have relevant and efficient use.

5.2 Ruggedized Electronics

“In today’s high-stakes defence environment, ruggedized electronics play a vital role in ensuring the reliability, safety, and success of military missions” (Zayn, I., 2025). These gadgets are systems that are engineered to be able to survive extreme conditions. (Zayn, I., 2025)

Hardware systems are referred to as ruggedized, they are reinforced physically and electrically to be able to withstand the military battlefield environments. Some of the optimizations that enhance performance include, wide temperature ranges, high-shock, high-impact durability, and electromagnetic interference (EMI). These optimizations combine mechanical ruggedness, thermal protection, environmental sealing, and electrical shielding, which enhances the reliability of devices. (Zayn, I., 2025)

6 Methods and Tools

This chapter goes through the different methods and tools used to create the prototypes in this thesis. The prototyping includes theory about use cases, scenarios, user experience, and user interface. Methods explains the cycle of the creation of the thesis and the tools explain all the applications used to create use cases and prototypes.

6.1 Prototyping

Nearly all product, service and system development efforts are interwoven with prototyping. A prototype is a representation of a concept or final design, the creation of which can predetermine a significant portion of the resources used in development and ultimately impact the success of the final product. (Camburn, B., 2017, p. 1)

This chapter establishes the theoretical framework for prototype development, focusing on the core components of use cases, user experience (UX) and user interface (UI) design. This framework was applied in the practical section of this thesis (Chapter 7 & 8) to guide the creation of the wearable device and application prototypes.

6.1.1 Use Cases

“Use cases are used to describe the outwardly visible requirements of a system.” (Schneider, G., 2001, chapter 1) During the analysis phase of a project use cases are used to contribute to user guides and testing plans. Creating project schedules also benefit from use cases, since it can assist what each stage of the releases. (Schneider, G., 2001, chapter 1)

Use cases are used in various processes. One process which is commonly used is the Rational Unified Process (RUP). Table 5 shows the four primary phases of RUP. (Schneider, G., 2001, chapter 1)

Table 5. Primary phases of RUP (Schneider, G., 2001, chapter 1)

Phase	Process
Inception	Determines the projects scope and business cases are created.
Elaboration	Developing the base architecture, risk analysis, requirements analysis and creation of a plan for the next phase.
Construction	Iterations of analysis, design, implementation and testing.
Transition	Complete all phases, test, fine tune and create documentation. After completion start creating plan to deploy the product to the world.

The creation of use cases happens in the inception phase to assist the scope of the project. From there use cases become more detailed in the elaboration phase. Furthermore, when starting the design and development of a project, use cases are used then in the construction phase. Lastly, in the transition phase use cases are utilized to create training and user guides. (Schneider, G., 2001, chapter 1)

6.1.2 Scenarios

Scenarios are categorised as a set of tasks that a set of users preform or want to perform. It describes a future technology that will aid the users in their task. “A scenario blends a carefully researched description of some set of real ongoing activities with an imaginative futuristic look at how technology could support those activities better.” (Nardi, B. A., 1992, p. 13)

A scenario’s purpose is to visualise a task done by a human which could be supported by technology. When making decisions on designs it’s useful to use scenarios as a reference

point. They provide guidelines on certain ways technology should perform. (Nardi, B. A., 1992, p. 13)

Descriptions of scenarios should depict the whole activity, so recourse, social settings and goals of users. Having scenarios written will provide more context and help with solving the problem without having to only rely on imagination. (Nardi, B. A., 1992, p. 13)

6.1.3 User Experience (UX) Design

UX design has become widely recognized and in every industry a mission-critical consideration. UX is critical to be able to create quality designs as well as help with costs of building projects. “Too often, the people who design and construct buildings and parks don’t worry about whether they will work properly or what will they cost to run. Once the project is complete, they can move on to the next job. But the public has to live with badly build, poorly designed buildings and spaces; taxpayers often have to foot the bill for putting them right again.” (Hartson, R., Pyla, P. S., 2018, chapter 1.3.2)

To be able to create an acceptable user experience you need to factor in, usability, usefulness, emotional impact, and meaningfulness. (Hartson, R., Pyla, P. S., 2018, chapter 1.4) Table 6 lists the user experience components and states why they are crucial in creating projects.

Table 6. UX Components (Hartson, R., Pyla, P. S., 2018, chapter 1.4)

Components	**Usefulness**
Usability	A foundational component that makes elements seen on screen reveal if they are clickable or not. Other components won’t give the feeling of a good interface without good usability.
Usefulness	Utility of all components. The product must have a backend software which can produce the power and functionalities.

Emotional Impact	User satisfaction when using or playing something. It can be joy, fun, exploration, happiness, sense of identity or even the “wow” factor in UX design.
Meaningfulness	How the product can have a meaningful effect on the user.

6.1.4 User Interface (UI) Design

Just like user experience, user interfaces play a critical role in creating a quality design of a product. The user should be capable to perform tasks with ease and engage interaction between the user and a system. “Good” and “bad” are mostly used to describe things that are eye catching, for example, colours or pictures. These are usually aesthetics of UI but using positive and negative terms also apply to the usability of an interface. (Stone, D., et al., 2005, p. 6)

Usability is defined by two key aspects. Firstly, to the users the system has been designed and developed for should recognize it to be useful for themselves. Secondly, looking at usability at a wider angle can extend the scope for the design instead of looking at only immediate environments. (Stone, D., et al., 2005, p. 6) Usability focuses on the efficiency of an application and the satisfaction of users. (Stone, D., et al., 2005, p. 7)

User interface and user experience both have laws that they fulfil to create a product that a user will be pleased with. Two laws that both experiences follow are Hick’s and Jakob’s laws. (Gmitter, N., 2025)

Hick’s law expresses that the time taken making decisions corresponds to how complex and numerous choices available. Utilizing this law when creating UI design, can assist decision making which reduces the number of choices and reduces cognitive load. (Gmitter, N., 2025)

Jackob’s law highlights the importance of preference when using websites and applications. The users prefer to use systems which work identically to others they’ve used

before. By following design patters and conventions that have been established, designers require less learning and are able to create more instinctive interfaces. (Gmitter, N., 2025)

User-centred design (UCD) examines the key aspects and laws of user interfaces. This ensures that when creating a UCD the user is involved throughout the design and development. (Stone, D., et al., 2005, p. 15) “User-centred design not only focuses on understanding the users of a computer system under development but also requires and understanding of the tasks users will perform with the system and of the environment” (Stone, D., et al., 2005, p. 15). A systems usability can be optimized by utilizing the UCD approach. (Stone, D., et al., 2005, p. 15)

6.2 Methodology

This thesis follows a development methodology which cycles through phases: requirements and design. This methodology was used throughout the duration of the thesis, compiling up-to-date requirements in collaboration with HAMK Tech and the National Defence University (NDU).

Development methodology aims to match the environment that the products operate in. The methodology goes into four phases: early requirements, late requirements, architectural design and detailed design. In the early requirements stage an understanding of the underlying problem is addressed. Later requirements are where the system qualities and functionalities are described. The architectural designing phase is where the architecture of the system is defined through control, subsystems, data which is interconnected and other dependencies. Lastly the detailed design phase defines the architectural portion in more detail. (Castro, J., 2001)

6.3 Tools

The practical work of the thesis was done in Figma, a graphics tool that’s used by many designers and developers to create UI software designs. Figma was used to create a UI prototype to help visualize the applications requirements and how they work together to create a working application.

Unified Modeling Language (UML) was developed to be able to provide notations and graphical language to help describe object-oriented models. UML helps with

understanding, developing, and communicating different views. Alongside use cases there are other types of diagrams that use UML such as class, object, communication, sequence, state machine, and activity diagrams. (Gomaa, H., 2011) Use case creation in this thesis was done in Draw.io. Draw.io is a tool used to create various diagrams. The use cases visually represent how smart wearable devices work together in different scenarios as well as create a diagram to help understand how the target group operates.

The textile prototype was created with the help of two other colleagues working alongside the client. A postdoctoral researcher and a student writing their bachelor's thesis about the design of smart wearables textile. The prototype helps provide an understanding of the way this smart wearable device is designed to function with the application. The prototype is created in paint, which is an application for creating, manipulating, and editing images and drawings.

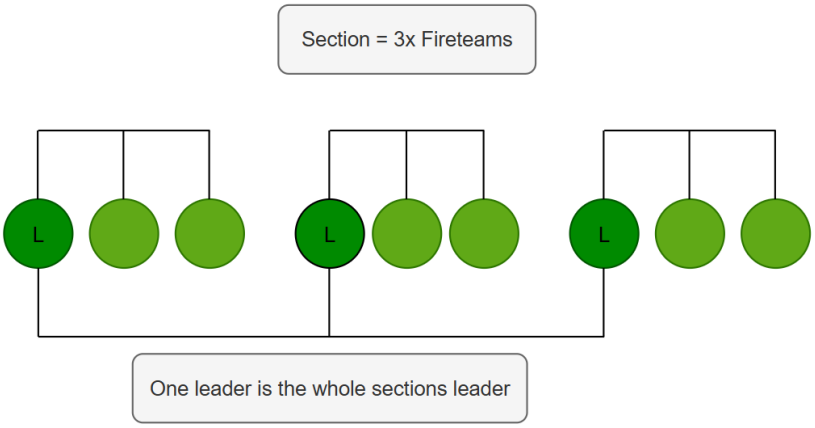
To ensure a traceable workflow, the project timetable was upheld in a task system in google calendar. Simultaneously, with the client and other companions, documents were created to document the requirements, ideas and designs to ensure that the project knowledge was recorded and easily accessible for everyone.

Following the HAMK guidelines on the responsible use of AI, this thesis acknowledges the use of AI-assisted tools that can support research. During the process of the thesis, without copying content directly, DeepSeek was used to help understand how to create a logical flow for chapters.

7 Practical: Device Requirements

This chapter is the start of the practical part of the thesis. The objective of this thesis prototype is to create a base UI design for the military to utilize with smart wearables. Previously stated in the introduction, the smart wearables devices core utilization is to be able to communicate with other teams using haptic feedback. This then eliminates the use of other communication methods. For the prototype designs to become reality, requirements need to be set.

Figure 7. Target group



The smart wearables are intended to be used by land-based forces in the military, as shown in Figure 7. There are three teams in one section, which consists of three leaders and six soldiers. One of the team's leaders is the whole section's commander. Table 7 shows the requirements to be able to communicate between each fireteam in both the device and interface prototypes.

Table 7. Communication requirements of fireteam members

Member	Requirement
Section Leader	Can communicate with their team and other team leaders
Fireteam Leaders	Can communicate with their own team and other leaders
Soldiers	Is only able to communicate with their own team

There is a hierarchy system in the defence force. Higher commanding officers can communicate with other higher-ranked officers while soldiers can communicate with non-commissioned officers. When taking the hierarchy system into consideration, we now know how each commander, leader and soldier can communicate within the section. The

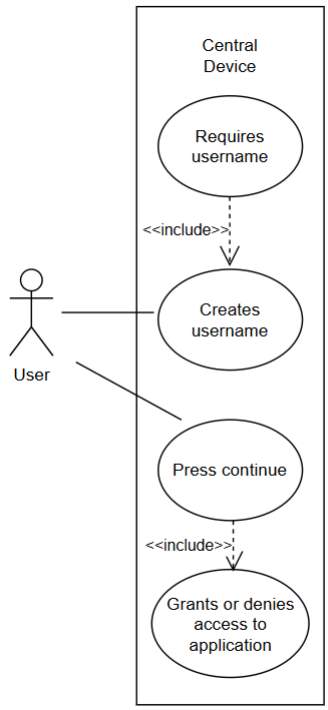
sections commander holds the most power, since they're able to communicate with other leaders and get information from other patrols or command centers.

7.1 Central Device Handling

Central devices have their own requirements to be able to function. Before the peripheral connection, the user is required to set a username to be able to be recognised by other members of the fireteam. To get a better visualization of how the central devices work use cases have been created to show the interactions between the user and devices in this chapter as well as chapter 7.2.

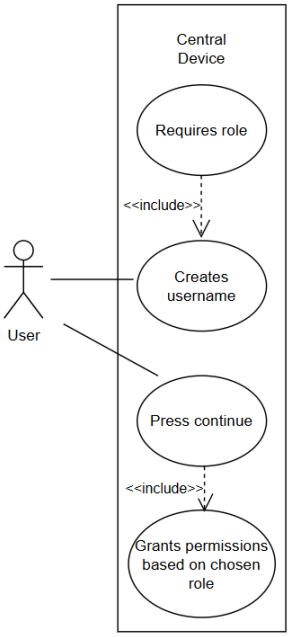
Figure 8 shows the creation of the username. The system requires the user to give input a name and will either grant the user access to the application or show an error based on the input given. If the username is the same as other members, it will ask for a different input. The include arrows in each of the figures represents the dependency between each requirement. Include is always a mandatory relationship between each use case while exclude would be for optional dependencies.

Figure 8. Username requirements



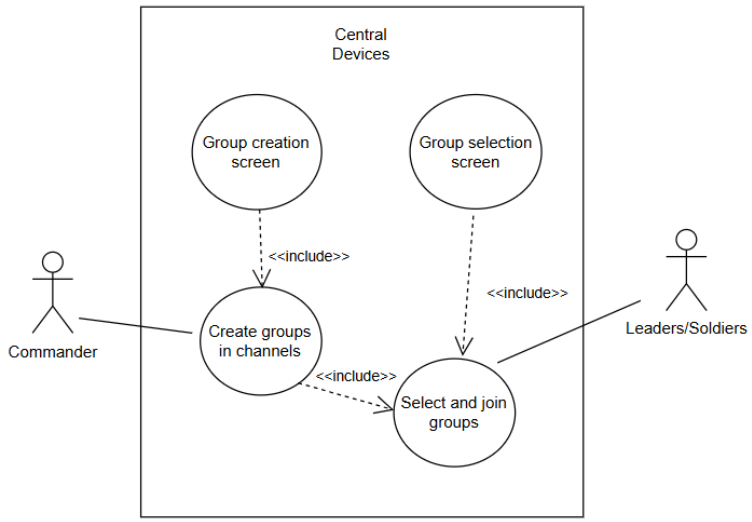
Central devices require to have grouping abilities so that fireteams can be formed in the sections. To achieve this, there is role selection, then group creation or joining of groups. To be able to move to creating and joining groups each user is required to select a role as shown in Figure 9.

Figure 9. Role requirement



As stated in the in the device requirements chapter, there are three roles, commander, leader and soldier. Permissions are given based on the role you choose. Once the role has been selected it will show the user a role specific interface. In this interface the user sees the group creation or selection. When the roles are taken into consideration, only certain users can create groups and join while other users are only capable of joining groups.

Figure 10. Group creation



The commanders are the only ones that can create groups while leaders are given access to join two groups and have access to both the channel where they communicate to other leaders and their own fireteam. Soldiers will only be given access to one group for their fireteam. This is shown in Figure 10. Once all members have joined their required groups, they're able to communicate between each member of their team.

In the battlefield devices may go through extreme scenarios that may cause the device to not function. If the device were to malfunction or get severely damaged, the central device could have the capability to still work on its own. Communication through the central device can be a possibility but there are still other communication methods that military users may use such as a radio, verbal or hand signals to quickly relay information in these circumstances.

7.2 Peripheral Device Utilization

Peripheral refers to the smart wearables device which is worn by the user. These devices can only be utilized once a central device has initialized the connection. Before the device is initialized, it stands by waiting for a connection to form.

Figure 11. Connecting devices

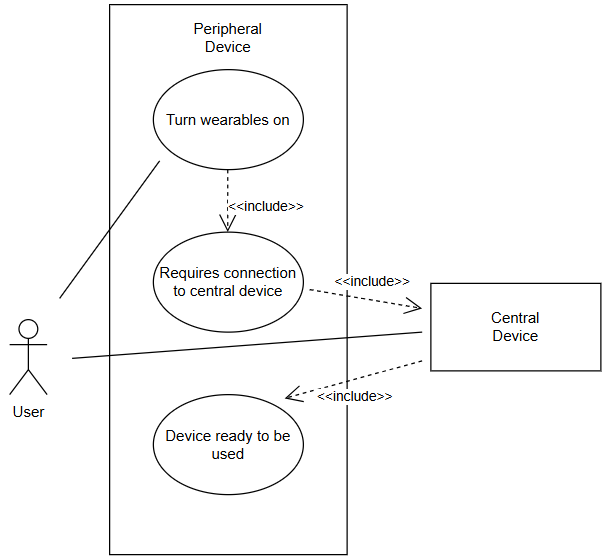
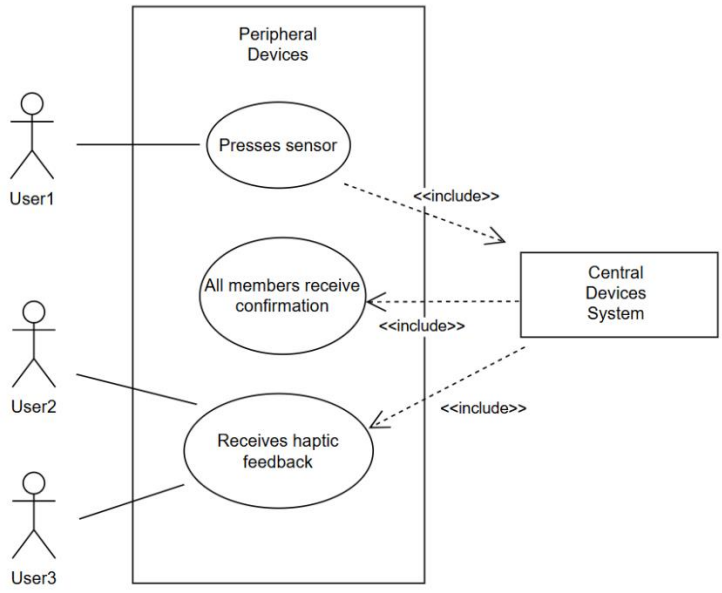


Figure 11 shows the user turning the peripheral device on. Once the device is on, the user connects to their peripheral device using the central device. The application creates a connection to the network before the smart wearable is ready to be utilized.

Without anyone connected to the same network or group, the smart wearables will not work the way intended. Figure 12 shows how the peripheral device depends on the central device to be able to function. This is the main utilization of both devices in the battlefield.

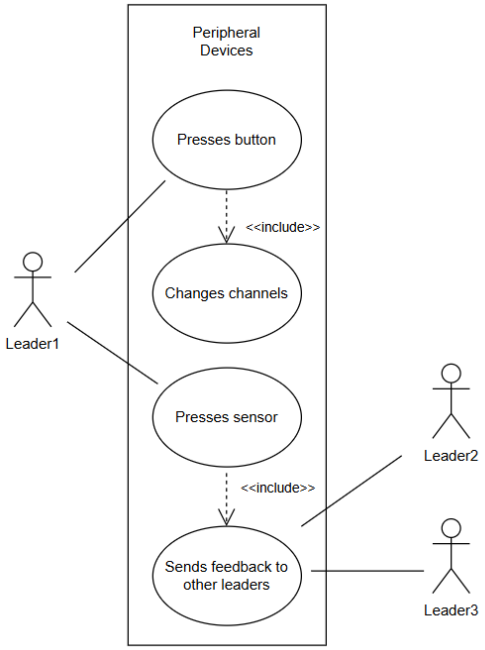
Figure 12. Haptic feedback



A user from a fireteam taps the peripheral devices sensor, which then relays that information to the application, through the network, and then to other users who then receive haptic feedback. The user who sends haptic feedback will receive confirmation that the haptic feedback has been sent and delivered to everyone else. The other members will get haptic feedback and confirmation that they have received feedback. If the confirmation hasn't been sent, then the users will know that the devices may have been compromised or damaged. During the communication process, edge computing reduces latency and bandwidth making sending and receiving haptic feedback immediate.

There are certain scenarios where leaders have acquired information which needs to be relayed to all leaders in their section. This can be done with changing channels on the peripheral as seen in Figure 13.

Figure 13. Changing channels



One of the leaders can press a button on their smart wearables device which allows them to rotate between channels. Once channels are changed, the leader that changed channels can relay information to other leaders. For other leaders to communicate back they also require changing the channel that they're in. Changing channels can also be done through the central device, though this option is feasible, it shouldn't be used as the main way to move though channels.

8 Device Prototypes

With all the requirements stated, the prototypes for the peripheral and central device have successfully been created to suit the needs of the National Defence University (NDU). During this thesis the development of these devices is still ongoing and at the first stages of building prototypes. These prototypes are subject to change in the future once this project can start building the first test devices. This chapter showcases the smart wearables and the UI design prototypes.

8.1 Peripheral Device Prototype

In an earlier sleeve Spiritus Ludi wearables design, the electronics were in places where they weren't sufficient for defence force use. In the testing's that were done in the field tests at the Military Defence University (MDU) the smart wearables sleeve was capable of functioning in extreme scenarios but needs to be refined so that the materials and electronics are more durable and roles and groups can be accessed with both peripheral and central devices.

To be able to add these functionalities another prototype for the smart wearables' devices was created with the help of a post-doctoral researcher and a student creating their bachelor's thesis on the textiles of the smart wearables.

Figure 14. Smart wearables device prototype

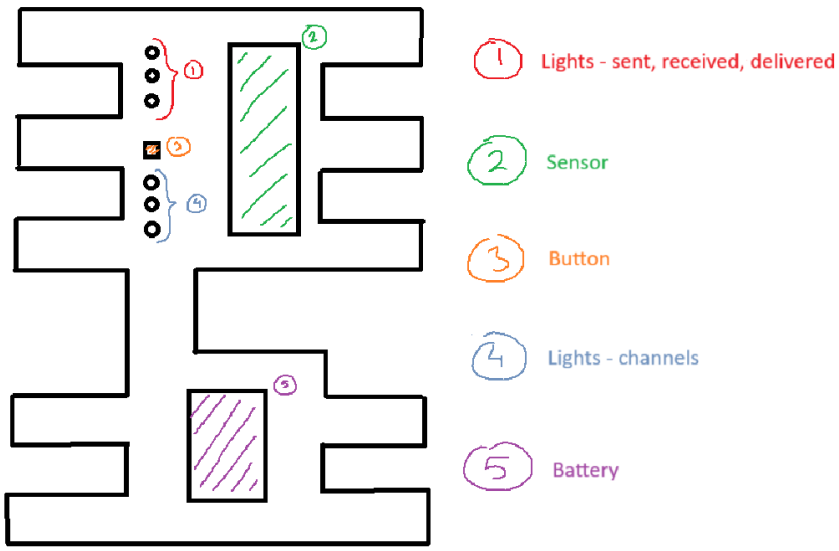


Figure 14 shows the first device prototype that was created. It wraps around the right forearm with straps and is worn on top of military jackets. When the user wears the devices, the sensor, will be on the outside of the forearm and the other buttons and lights on the inside of the forearm. On the top part of the sleeve on the upper arm is where the battery and central processing unit (CPU) will be located which can be charged when necessary. The CPU is what allows the peripheral device to carry out its required tasks and control the flow of the data.

All these components are linked to each other with wires to be able to function properly. The first three buttons are where the lights will be shown to the user when they either send a message, receive a message and get confirmation that their message has been received by all other users. The big green area in Figure 14 is the sensor which the users tap to send haptic feedback. The orange square is the switch which is used to change between channels. There are two channels, one where the user can communicate between their team they joined, and the second one is to change to a channel where the leaders can communicate.

For this first iteration of the prototype the button that switches on the device and lights indicating when it’s turned on have not been implemented. The motor that sends haptic feedback will also be implemented later in the project when the best placement is found, which is usually in direct contact with the skin. All these electronics should be able to withstand the harsh environments.

8.2 Central Devices UI Design Prototype

The UI design prototype is meant for HAMK Tech to be able to test the functionality of the smart wearables sleeve. Once tested and considered to be up to standards with the requirements, only then will the smart wearables device be given to the military for further utilization. The military will use their own devices and network connections which cannot be accessed by unauthorized users.

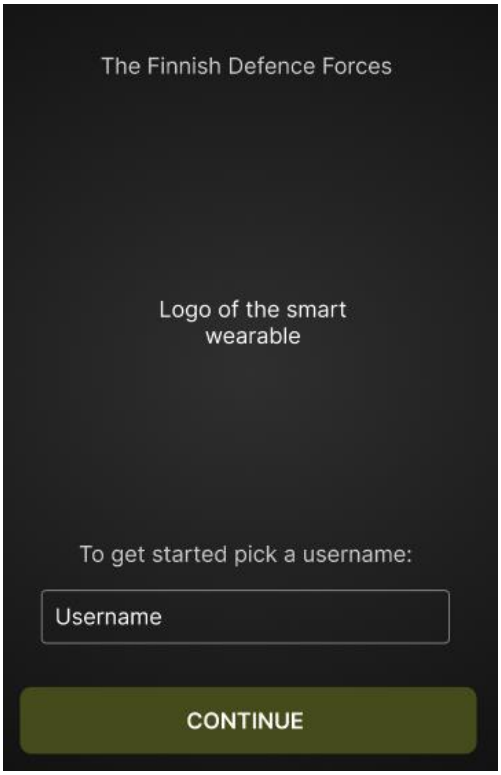
The UI design takes inspiration from an existing prototype that is used in another smart wearable product being designed in HAMK Tech. This UI redesign implements the core usage of the application which the military can take into consideration when creating the necessary functions that suit their devices.

The redesign was guided by the core UX/UI principles tailored for defence use. The results interface prioritizes simplicity which can reduce time in learning the application. For optimal use in low-light environments, the design utilizes a non-reflective, low-contrast color scheme, avoiding bright or distracting colors.

8.2.1 All members

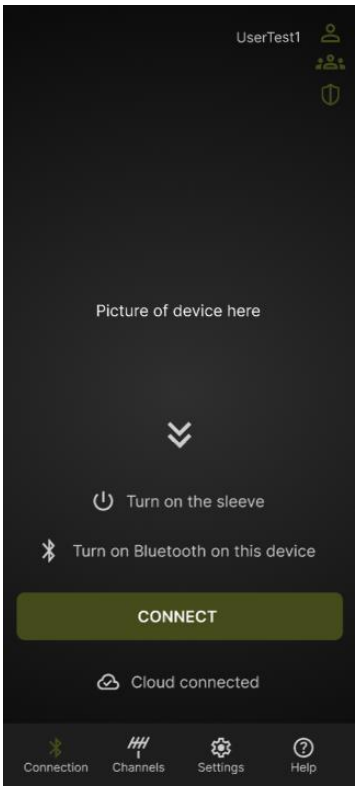
When preparing defenses, all members of the section in the patrol sectors must be able to access the application and connect the smart wearables. With the help of Figure 15, Figure 16, Figure 17, and Figure 18, the setup of the application was created.

Figure 15. Start screen



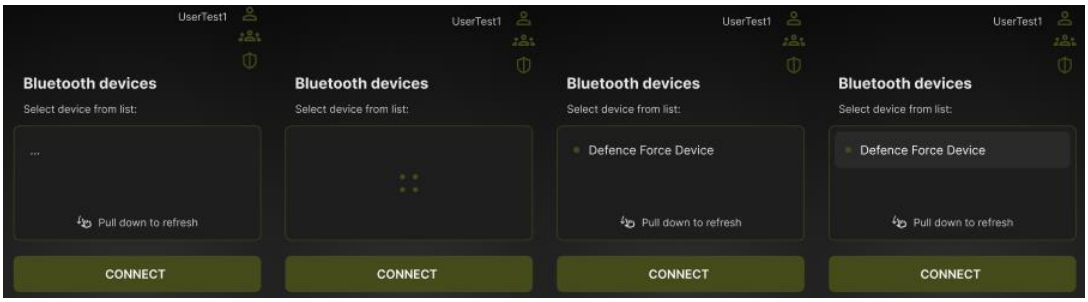
The starting screen Figure 15 requires the members' username to be typed into the input to be able to proceed. If no username is created, then an error will pop up to tell the user to type something. Another error will also occur if the username is the same as other members. To make the process secure a two-factor-authentication can be implemented so that the application is more secure.

Figure 16. Connection to devices



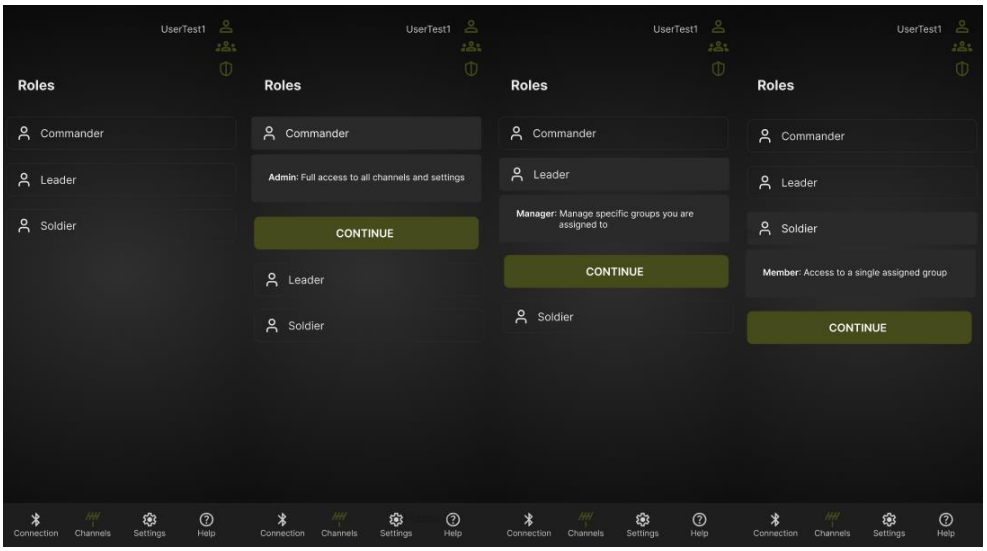
After creating the username, the sections members can connect the peripheral device to the central device. The connection screen, Figure 16, will be visible to the user before connecting to any device.

Figure 17. Selecting device



When wanting to connect the peripheral device, the users will get a screen showing the available devices. If none appears the box can be pulled down to refresh the connection until devices appear, shown in Figure 17. Once the user's own device becomes visible it can be selected to move forward to role selection in Figure 18.

Figure 18. Role selection interface

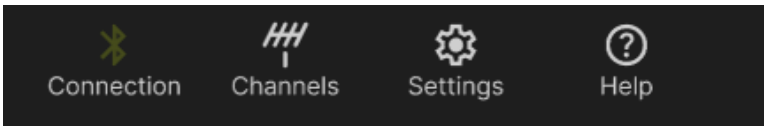


Roles can be selected by clicking on them. A dropdown will appear to give more information about the role itself and its permissions. After selection the permissions will be saved, and the system will modify the UI to the roles. To avoid the users from clicking the wrong role, the system can check the users ID through the network before allowing them to proceed. The users may also have their own devices which other military members can't access, if this is the case, the system can check their device ID and the permissions it holds.

Figure 19. User, group, and role

At the top right of each device there are three icons, as shown in Figure 19. These icons are used to identify the devices user; the group they're in and the role that they have selected.

Figure 20. Footer

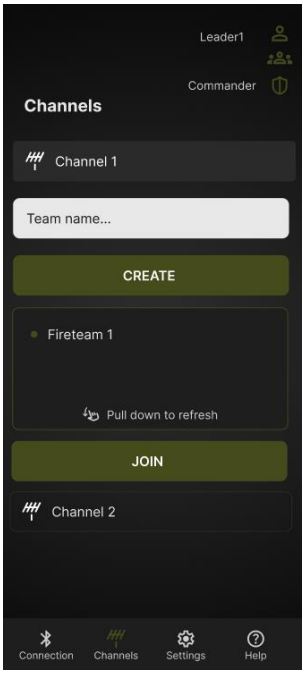


At the bottom of the screen a footer is shown with all the necessities for the application, Figure 20. The connection for connecting the peripheral, channels for joining groups, settings to be able to change your username; and help where there are instructions for the use of the wearables and the connection. When clicking on one of the icons it will change colors indicating that the user has switched to another screen.

8.2.2 Commanders

Instead of just choosing to create only groups it's more feasible to create channels for them. This helps with the development of the application as well as helps maintain the interface. It can also help with the connection overhead having to only deal with two persistent and stable connections.

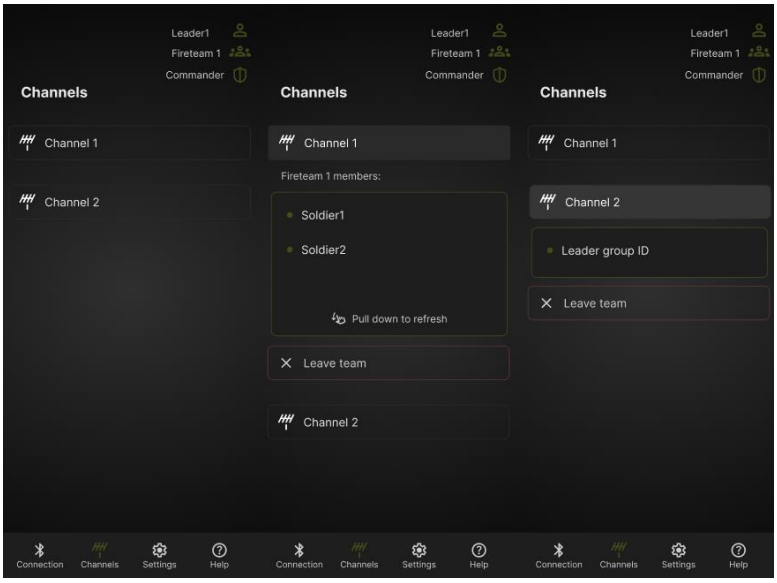
Figure 21. Group creation



When selecting the commander role, it will unlock the rights to create teams in channels. The channels are automatically created, since there only needs to be groups for each

fireteam and a channel for the leaders to communicate. The commander will create teams into each channel as shown in Figure 21. When clicking on a channel a dropdown will appear. Here the names for each team will be created and displayed to everyone else in the fireteam.

Figure 22. Commander and leader channels

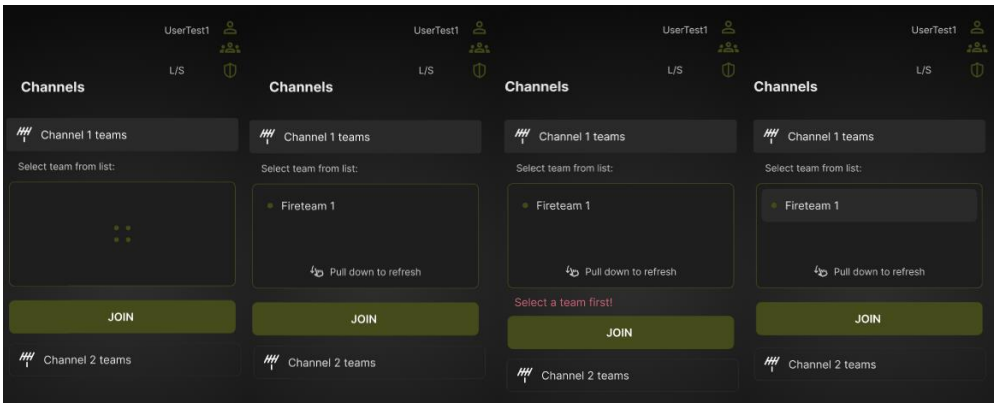


Once the commander has joined their fireteam group will the left screen in Figure 22 be shown. Here other team members and channels are listed. If required, the user can leave the team. When pressing the Channel 2 dropdown, the commander then automatically changes to the channel. When in Channel 2, the leaders of other fireteam members will receive haptic feedback when another leader sends messages in that channel.

8.2.3 Leaders and Soldiers

Leaders and soldiers have different permissions than that of the commander. They can’t create channels but can join them. These screens are shown in Figure 23.

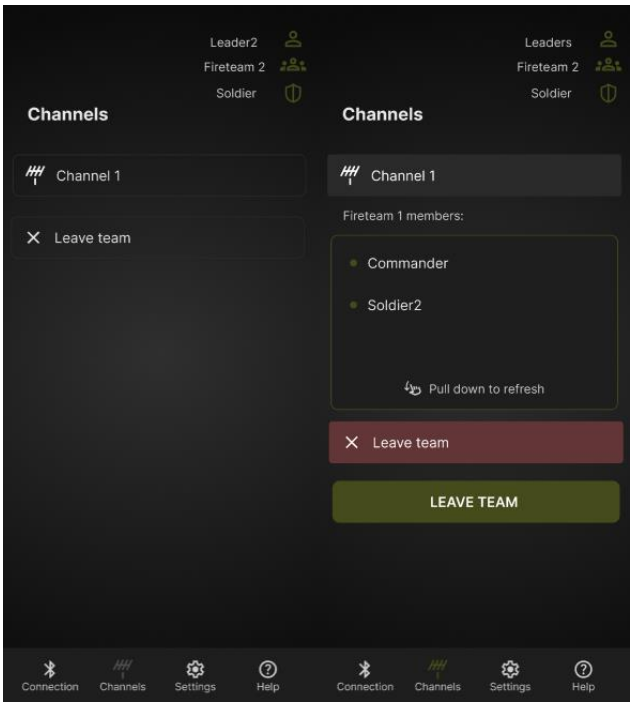
Figure 23. Joining channels and groups



Once the members click the team's icon at the bottom of the screen the channels will appear. Channels will appear where leaders are able to join one group per channel, but soldiers can only choose Channel 1. Just like in Figure 17 when selecting peripheral devices, the groups that have been created by the commander will show up in the dropdown menu.

To be able to move onto the screen where the channels and team members are shown, the user must choose a group to join.

Figure 24. Soldiers' channels



The screens in Figure 24 are what soldiers see. Just like everyone else in the section soldiers and leaders can leave the team if necessary. When clicking to leave the team it will show another button to confirm that the user wants to leave. This ensures that the user can’t accidentally leave.

The two key differences between the commanders, leaders and soldiers’ screens are the number of channels they can access. Soldiers only have channel 1 available to them while leaders have both channels 1 & 2 shown in Figure 22.

8.3 Ethics and Sustainability

This thesis acknowledges the ethical and sustainability of wearable technology. User privacy, data security and environmental impacts are issues that have been considered during the creation of the peripheral and central device prototypes.

Ethically the smart wearables device doesn’t collect nor store any sensitive or medical information from the users. The wearables devices were created to send haptic feedback as a communication method to relay information quickly without having to use other communication methods.

In the ongoing smart wearables project, sustainability has been implemented. The iterations of the smart wearables prototype create devices that reduce environmental impact by being easily reparable and recyclable. The peripheral devices electronics will also be able to withstand the different extreme environments that they will be utilized in. The central device user interface prototype uses BLE that allows the application to use less power and run for longer periods of time which in return reduces energy consumption making the devices last longer. The central devices can also be ruggedized so that they’re able to last longer in extreme environmental conditions and won’t need to be replaced as often.

9 Results

Having presented the key results, the following discussion evaluates their significance in relation to the research questions and future implementation. The thesis outcome validates a concept of the prototypes, which includes a UI design prototype and an iteration of the peripheral device. The results address the research questions by demonstrating the feasibility of the prototype concepts for the use in the defence context.

The application is required to have username creation, role selection, groups to join, and the ability to connect to the peripheral device. These have all been implemented into the UI design which will be then implemented into the application itself. With these core functionalities designed, the haptic communication system is considered operational in the defence context.

The first iteration of the wearables prototype design displays the placement of devices electronics and how the device functions on the user. These electronics are required in the wearables to be able to support communication between patrols and groups in the defence sector. If any of the electronics are not implemented, the wearables device cannot be utilized effectively.

Reflecting on the process, the thesis timeline demanded a focused scope that led to achieving a viable and documented UI design concept. This ensures the project can continue to move forward after transferring the knowledge over to HAMK. Therefore, these prototypes establish the foundation of the first milestone, providing a purpose-built version with which functional physical devices can be developed.

In the future the security of the interface should be considered during the creation of the application. Operational security (OPSEC) is crucial to have since these devices will be given to the military where sensitive data can compromise system integrity. The device's interface can be secured by taking necessary precautions as stated about device security in chapter 4, where unauthorized users aren't able to access the interface. For example, adding an additional password for each user's device and implementing a role permissions check, where the system can check the user's role before giving them access to the correct interface. The client should also take into account how the leaders will be able to differentiate between their fireteam communication and the communication between the leaders when receiving haptic feedback.

This thesis topic is still at the first stages of development. This information obtained in the thesis will be given to HAMK Tech to further develop the peripheral and central device prototypes. Once the devices have been created, tested and considered to be up to standard, the devices will then be given to the National Defence University (NDU) for further testing and implementation into the military.

The client's feedback was positive: "The thesis reviews essential aspects of designing wearable technologies with mediated touch for military use. In the empirical part of the work the requirements are presented and device prototype concepting including UI design. The work conducted in the thesis supports the general conceiting of the smart sleeve system for military use in HAMK Tech." (Meeting with HAMK Tech client, 2025)

10 Summary

This thesis shows a development approach, using the two prototypes created as primary means to answer the research questions and implement the requirements that were given by the client. Identifying the requirements and implementing them into a working system and observing how they'll work in a real-world context, the prototypes serve as a purpose-built version from the other wearables prototype created for esports use.

Before this thesis, I've worked on the Spiritus Ludi smart wearables sleeve which HAMK Tech created to be utilized in the esports community. I have a good understanding of how wearables work but I learned more about the military and their requirements needed for these first iterations of the prototypes to be considered operational in the defence context. I also learned more about the security concerns that may occur in these types of devices and how they should be handled when creating the systems for the interface prototype.

In the future HAMK Tech will be moving forward with these prototypes and creating functional devices. Once these devices have been created, tested in different environments, and have implemented all the required functionalities, they will then be given to the National Defence University (NDU) for further research and testing. The long-term objective of this project is to deploy the devices for military purposes.

References

Ace Computers. (2025, July 14). *Secure Computers for Military Operations: Safeguarding Data, Devices, and Defences*. Ace Computers. https://acecomputers.com/secure-computers-for-military-data-protection/

Afaneh, M. (2023, June 7). *Mastering BLE: A Guide to Peripherals and Centrals*. Novel Bits. https://novelbits.io/ble-peripherals-centrals-guide/

Andås, H. E. (2020). *Emerging technology trends for defence and security*. FFI. https://www.ffi.no/en/publications-archive/emerging-technology-trends-for-defence-and-security

Astute. (2025). The Internet of Battle Things (IoBT): *Communication Challenges and Emerging Solutions*. Astute. https://www.astutegroup.com/news/defence/the-internet-of-battle-things-iobt-communication-challenges-and-emerging-solutions/

Becher, B. (2024, October 24). *18 Types of Sensors to Know.* Built In. https://builtin.com/articles/types-of-sensors

Camburn, B., Viswanathan, V., Linsey, J., Anderson, D., Jensen, D, Crawford, R., Otto, K., Wood, K. (2017, August 03). *Design prototyping methods: state of the art in strategies, techniques, and guidelines*. Cambridge University Press. https://www.cambridge.org/core/journals/design-science/article/design-prototyping-methods-state-of-the-art-in-strategies-techniques-and-guidelines/560B306A5E799AEE54D30E0D2C1B7063

Castro, J., Kolp, M., Mylopoulos, J. (2001) *A Requirements-Driven Development Methodology*. Springer Nature Link. https://doi.org/10.1007/3-540-45341-5_8

Cisco. (n.d.) *What Is Device Security?*. Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-device-security.html

Fleury, M., Lioi, G., Barillot, C., Lécuyer, A. (2020). *A Survey on the Use of Haptic Feedback for Brain-Computer Interfaces and Neurofeedback*. Front. Neurosci. https://doi.org/10.3389/fnins.2020.00528

Gmitter, N. (2025). *Laws of UI*. UI Laws. https://www.uilaws.com/

Gomaa, H. (2011). *Software Modeling and Design: UML, Use Cases, Patterns, and Software Architectures*. Google Books. https://books.google.fi/books?hl=en&lr=&id=TqZi-hAX17YC&oi=fnd&pg=PR7&dq=UML+use+cases&ots=4XWeAc2vNL&sig=PI6eD1ZrRg0Jj7a3txmOIFlzoUE&redir_esc=y#v=onepage&q=UML%20use%20cases&f=false

Hartson, R., Pyla, P. S. (2019). *The UX Book: Agile UX Design for a Quality User*. Google Books. https://books.google.fi/books?hl=en&lr=&id=RHIGCwAAQBAJ&oi=fnd&pg=PP1&dq=UX&ots=EOIfJsmZsN&sig=rYgLd02qSL8nz_0T1-DAVS2Pqog&redir_esc=y#v=onepage&q=UX&f=false

McElroy, K. (2016). *Prototyping for Designers*. O'Reilly. https://learning.oreilly.com/library/view/prototyping-for-designers/9781491954072/

Nardi, B. A. (1992). *The use of scenarios in design. Association for Computing Machinery*. https://doi.org/10.1145/142167.142171

Sazonov, E., (2014). *Wearable Sensors*. O'Reilly. https://learning.oreilly.com/library/view/wearable-sensors/9780124186620/xhtml/chp001.xhtml

Schneider, G., Winters, J. P., (2001). *Applying Use Cases: A Practical Guide*. Google Books. https://books.google.fi/books?hl=en&lr=&id=mOCZ1xjqQyMC&oi=fnd&pg=PT18&dq=use+cases&ots=44wNM7Appi&sig=Wm6ryqZ2_D2QEBam0sBYiib4R4s&redir_esc=y#v=onepage&q&f=false

Shi, H., Zhao, H., Liu, Y., Gao, W., & Dou, S. C. (2019). *Systematic Analysis of a Military Wearable Device Based on a Multi-Level Fusion Framework: Research Directions.* MDPI. https://doi.org/10.3390/s19122651

Stone, D., Jarret, C., Woodroffe, M., Minocha, S., (2005). *User Interface Design and Evaluation*. Google Books. https://books.google.fi/books?hl=en&lr=&id=VvSoyqPBPbMC&oi=fnd&pg=PR21&dq=UI+design&ots=d9OVQ-rPUe&sig=1iZWh9Suwz2ZODzjhcdoImOUn8U&redir_esc=y#v=onepage&q=UI%20design&f=false

Xu, T. (n.d) *What Is Haptic Feedback?* Retrieved 26 October 2025 from https://builtin.com/hardware/haptic-technology

Zero Trust Blog. (2024, February 9). *Whitelisting vs Blacklisting: What's the Difference?*. Zero Trust Blog. https://instasafe.com/blog/whitelisting-vs-blacklisting-whats-the-difference/

Appendix 1: Data management plan

The reasearch data in this thesis will be conducted with HAMK Tech’s data that is public. No personal data was collected during this research.

Data collected for this thesis will be processed and stored on the author’s own computer which is password protected. Backups of the data will be saved in separate folders away from the other files being analysed. The thesis author and thesis supervisor will have access to handle the data collected.

This data is owned by the client from HAMK as part of development for HAMK Techs research field. Any information that is not publicly available will not be showcased in the thesis.

After the thesis is completed, the anonymized data will be transferred to the ownership of HAMK for possible further research and development. An agreement regarding the rights to use the data in the future will be written with the thesis author and commissioner connection and then attached to the thesis.