LAB University of Applied Sciences

ELECTRONIC THEFT PREVENTION

LAB-UNIVERSITY OF APPLIED SCIENCES
Engineer (AMK)
Information and Communications Technology
Spring 2020
Lassi Lääperi

Abstract

Author(s) Lääperi, Lassi	Type of publication Bachelor's thesis	Published Spring 2020
	Number of pages 39	

Title of publication

Electronic theft prevention

Name of Degree

Information and Communications Technology

Abstract

Kemppi OY is the leading manufacturer of welding equipment in Finland and one of the largest in its field in Europe. Kemppi's Minarc product family contains multiple different devices and their modern revisions under the additional title EVO. Minarc devices are designed to be portable and usable on the go. The lightest Minarc machine weighs only 4Kg with the bulkiest variant weighing less than 10Kg. Despite being small and only TIG/MMA capable, Minarc devices are not necessarily cheap. The price for the cheapest machine of the Minarc family revolves around 500e with the priciest devices being close to 2000e.

The convenience of the modern world is a double-edged sword. What is convenient for the user is also convenient for the thief, especially when it comes to portability.

The thesis takes a brief look into small item theft prevention methods and modern electronic ways to prevent theft. The case was to create a device for Kemppi Oy's Minarc welder that addresses the issue of equipment theft. The goal of the device was to incorporate new and existing IoT technologies to enable potential conversion of dumb machines into IoT ones through an additional connectivity module or a software update depending on the capabilities of existing devices. The IoT's inherent connectivity to the internet can be used to detect, prevent and potentially deter theft. The device created in this thesis ended up using Bluetooth for its short range and LoRa for long range communication. A Raspberry Pi computer was used as the core of the device. The device was tested at Kemppi's factory in Lahti to determine its range and usability in real world applications.

Keywords

Bluetooth, LoRa, IoT, Theft, GPS

Tiivistelmä

Tekijä(t) Lääperi, Lassi	Julkaisun laji Opinnäytetyö, AMK	Valmistumisaika Kevät 2020
	Sivumäärä 39	

Työn nimi

Elektroninen varkaudenesto

Tutkinto

Insinööri (AMK)

Tiivistelmä

Opinnäytetyön toimeksiantaja on Kemppi Oy. Kemppi on Suomen suurin hitsauslaitevalmistaja ja yksi alansa suurimmista Euroopassa. Kempin Minarc-tuoteperhe sisältää monia laitteita, joista uusimmat versiot ovat lisänimen EVO alla. Koneperheen kevyin laite painaa ainoastaan 4 kg ja painavin alle 10 kg. Halvimmillaan Minarc-perheen koneen jälleenmyyntihinta on 500 euron luokkaa ja kalleimman laitteen hinta hipoo 2000 euron rajaa. Minarc-laitteet on suunniteltu kannettavaksi ja käytettäväksi liikkuvilla työmailla. Liikuteltavat laitteet ovat varkaille hyvä kohde. Työn taustalla on jälleenmyyjien ja asiakkaiden kohtaamat ongelmat varkauksien kanssa.

Työssä tutkittiin lyhyesti pienlaitteiden varkaudenestotapoja ja moderneja elektronisia vaihtoehtoja. Työn tavoitteena oli kehittää Kempin Minarc-hitsauslaitteeseen varkaudenestolaite, jolla varkauksia voidaan ehkäistä tai vähentää.

Opinnäytetyön tuloksena syntyneessä laitteessa käytetään jo olemassa olevia ja uusia IoT-tekniikoita, jotka voivat mahdollistaa normaalin työkoneen muuttamisen IoT-laitteeksi joko lisämoduulin tai ohjelmistopäivityksen kautta. IoT-laitteille olennaista yhteyttä internetiin voidaan käyttää varkauksien havainnointiin ja estoon. Luodussa laitteessa päädyttiin käyttämään Bluetooth-radiota lyhyen matkan ja LoRa-radiota pitkän matkan kommunikointiin. Ytimenä laitteessa toimii Raspberry Pi-tietokone.

Laitetta testattiin Kempin tehtaalla sen käytännöllisyyden ja kommunikointietäisyyksien selvittämiseksi. Testeissä saavutettiin yli 100 metrin Bluetooth-kommunikointietäisyys. Testitulosten perusteella voitiin päätellä laitteen soveltuvan käyttöön kentällä, kun etäisyydet eivät ole suuria.

Asiasanat

Bluetooth, LoRa, IoT, Theft, GPS

CONTENTS

Terms

ABP = Activation By Personalization

ADR = Adaptive Data Rate

AOA = Angle of Arrival

AOD = Angle of departure

AP = Access Point

BLE = Bluetooth Low Energy

DRM = Digital Rights Management

ERA = European Rental Association

FSK = Frequency Key Shifting

GPS = Global Positioning System

ISM = Industrial, Scientific and Medical

IoT = Internet Of Things

LoRa = Long Range Radio

LOS = Line Of Sight

NFC = Near Field Communication

NMEA = National Marine Electronics Association

OTAA = Over The Air Activation

RFID = Radio Frequency Identification

RSSI = Received Signal Strength Indicator

SoC = System On a Chip

SPI = Serial Port Interface

TER = The Equipment Register

UART = Universal Asyncronous Receive Transmit

UUID = Universally Uni0que Identifier

VAHTI = Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä

1 INTRODUCTION

Since the dawn of time theft has been a problem in human societies. Although through the centuries law enforcement and advances in asset protection have managed to thwart the theft problem, a modern society provides modern problems such as the reduction in size and increase in the value of everyday items. Old methods such as locks and chains are losing their effectiveness to protect modern devices due to portability and small size becoming the norm even for industrial machines such as welders.

Kemppi OY is the leading manufacturer of welding equipment in Finland and one of the largest in its field in Europe. In 2019 Kemppi celebrated its 70th birthday. Their headquarters and electronics factory are based in Lahti with the electronics factory being the largest in Finland. Due to their size and popularity of their devices, Kemppi has received concerns about equipment theft from its resellers. The case for this thesis is to create a device to address this issue. The case device could be incorporated into products such as Kemppi’s small Minarc welder. Although Kemppi devices are used in this thesis the case device is designed to be universal and not manufacturer-specific. The case device will use one or more of the technologies already in use in the industry or a more modern version of those, for example Bluetooth 5.

The purpose of this thesis is to examine theft and methods to prevent it, and to prototype a new modern solution to the age–old problem of theft. This thesis briefly looks into how much equipment is lost because of theft. The thesis will also cover some common theft prevention methods in use, including physical ones. Some potential near-future or less known theft prevention technologies are also covered briefly.

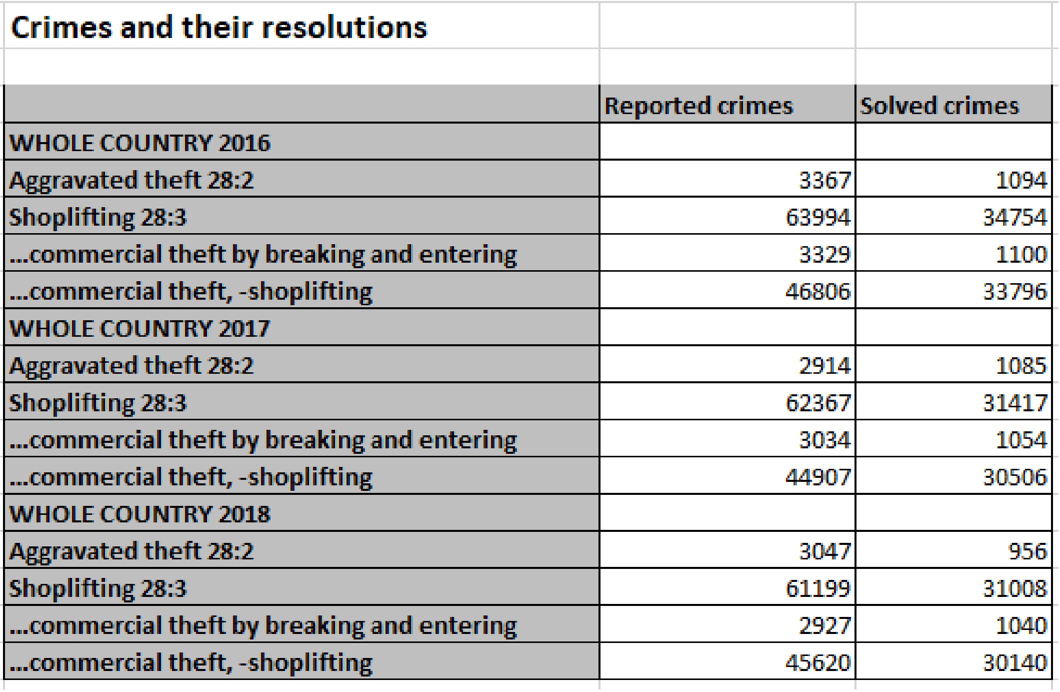
2 THEFT

When talking about theft and electronic theft prevention, this thesis focuses on retail and industrial theft. The methods used by these fields are quite similar and both suffer from various losses caused by theft. The lack of comprehensive sources can be explained by the sensitivity of the topic. High theft rates can leave a negative Image about the company.

Since Kemppi is a Finnish company, a more Finnish-based view is taken assessing theft. Foreign sources are used to reinforce the idea that theft and the need for new prevention devices is global.

One reliable source, Tilastokeskus, the Finnish national statistics centre, lists generalised crime statistics for January–September 2019. According to Tilastokeskus statistics, during January–September 2019 there were 158 200 reported property thefts and 92 700 cases of theft where shoplifting accounted for 34 400 cases (~37%) (Suomen virallinen tilasto (SVT) 2019). While the statistics broadly categorize thefts, they can still be used to assess the necessity of theft prevention solutions.

Table 1. Theft statistics 2016–2018 (Tilastokeskus 2019)



Crimes and their resolutions

	Reported crimes	Solved crimes
WHOLE COUNTRY 2016		
Aggravated theft 28:2	3367	1094
Shoplifting 28:3	63994	34754
...commercial theft by breaking and entering	3329	1100
...commercial theft, -shoplifting	46806	33796
WHOLE COUNTRY 2017		
Aggravated theft 28:2	2914	1085
Shoplifting 28:3	62367	31417
...commercial theft by breaking and entering	3034	1054
...commercial theft, -shoplifting	44907	30506
WHOLE COUNTRY 2018		
Aggravated theft 28:2	3047	956
Shoplifting 28:3	61199	31008
...commercial theft by breaking and entering	2927	1040
...commercial theft, -shoplifting	45620	30140

Table 1 above is taken from the Tilastokeskus statistic database and shows the number of reported thefts from 2016 to 2018 and how many of them were solved. The fact implying a need for theft prevention solutions is the percentage of solved thefts. Out of around 3000 aggravated thefts only about 33% were solved. Statistics by Tilastokeskus do not tell what type of thefts these were but it can be hypothesised that even if part of this unsolved 66% of thefts was industrial small equipment, the loss of production and financial losses caused from production downtime could be significant. Especially in the case of some of the thefts being localised.

An important thing to note when looking at the statistics is that the value of the stolen item is one of the defining factors in whether the crime is considered theft or petty theft. The value, or what is considered a small value, is not defined in the law, which leaves the monetary limit for the local courts and prosecutors to decide (Näpistys 1990/769, 3 §).

Some sources claim that this monetary value limit can be up to 500 euros (Antto 2015, 40.; Minilex 2019). When taking into consideration the value limit of 500 euros between petty theft and theft, and the fact that small equipment such as welding machines can cost much less than 500 euros, theft of these often somewhat portable devices can seem quick and profitable. Theft prevention devices can act as a deterrent in these cases of opportunistic thefts. According to the Finnish law, the act of removing or circumventing theft prevention elevates the crime from mere petty theft to theft. Thus, even a bad theft prevention device can serve a deterrent purpose.

In terms of perpetrators and value of stolen goods, according to a survey conducted in the USA by JACK L. HAYES INTERNATIONAL, INC, 279,000 shoplifters were caught in 2018 from which 28,145 (~10%) were employees of the companies. The report also states that the value of items recovered from caught shoplifters averaged around 400$ USD. The report also states an interesting finding: while with an average shoplifter, not an employee, the case value was around 301$ USD, the average value for an employee caught stealing was more than three times the amount (around 1300$ USD). The value of stolen goods recovered totaled around 241,000$ USD, but the survey estimates that the recovered amount only counts as low as 7.8% from total losses to theft. This percentage can also be much lower, since the calculation in the survey gives a large 30% margin for losses caused by inventory mismanagement. (JACK L. HAYES INTERNATION INC 2019, 1–9.)

The survey also presents an interesting finding that could be related to digitalization and automatization of stores. Figures from 2017 and 2018 show a decrease in shoplifter apprehensions, but also show an increase in value per case. Respondents in the survey estimated this could be caused by less retail staff on the shop floor, causing an increase in opportunistic thieves. The decreasing amount of staff on the shop floor could be attributed to the increase in popularity of electronic displays and shop assistants, causing now unnecessary staff to be laid off or transferred to other duties. (JACK L. HAYES INTERNATION INC 2019, 3.)

Based on this one report alone employees made up 10% of shoplifters, with the shoplifting amounts counting 33% from the total value of recovered goods. Even though employee theft is much rarer than theft by outsiders, the financial damage caused by internal theft is much higher.

To put these percentages into perspective, a CNBC article from 2015 states that a survey by National Trade Federation (NRF) and University of Florida found inventory losses from criminal activity to be around 44 billion USD (Reuters 2015). Though the number also includes “administrative errors”, it can be speculated that some of these errors might have had malicious motives behind them. Another figure that helps with scale is a claim made by Antto Terras in his book that states annual retail losses from theft being around 500 million euros (Antto 2015, 19).

National Equipment Register (NER), an organization that tracks thefts and stolen equipment in the United States, estimated the value of stolen equipment to be around 300 million USD in 2016 (National Equipment Register 2016, 27). ERA estimates this number to be over 500 million euros in the rental industry alone (European Rental Association 2019, 1). These numbers are significantly lower than what NRF found, but this is due to ERA being a European source and NER focusing specifically on small worksite equipment, rather than retail industry as a whole.

New solutions, especially for theft recovery, are needed as numbers by ERA paint a dark picture of recovery efficiency. According to ERA, the rate of recovered stolen equipment is between 5–20% (European Rental Association 2019, 1).

Losses are not only limited to the value of stolen equipment. If thefts occur on worksites and no equipment is available to replace stolen ones, a situation where work cannot continue becomes possible. Losses from production downtime can be much greater than the value of stolen equipment.

Numbers may vary, depending on the union the workers belong to, along with other factors, but just by looking at students'/trainees' wages, which Finnish Central Organization For Motor Trades and Repairs union lists as starting from 9.35–9.50e/h, the cost of one missed workday (7.5h) becomes 71.25e (Autoalan Keskusliitto RY; Teollisuusliitto RY 2017, 29). These costs can quickly accumulate, depending on the availability of backup equipment.

Largest costs can occur if project timetables start to fail due to lost production time. These costs can be in hundreds of millions depending on the scale of the project. For example, the Areva–Siemens company, which is building the Olkiluoto 3 nuclear reactor, is expected to pay 400 million euros as late fees for failing to finish the project on time. The 400me sum does not include potential penalties, which could add a few million euros more. (Rosendahl 2019.)

Damages caused by theft and the resulting delays are not necessarily only monetary. Depending on the size of the industry and customer base, the damages to the company's reputation can result in losing customers.

3 THEFT PREVENTION

Crime relies on opportunity and low risk and depends on rational decision making. The goal of theft prevention is to affect these variables to lower the incentive for criminal activity, with principles revolving around prevent, respond and solve. (Speights, Downs & Raz 2018, 31.)

Theft and the methods of dealing with it can be divided into two groups, theft prevention and theft recovery. While theft prevention focuses on preventing the theft from taking place (e.g. chaining a pc monitor to a wall), and theft recovery focuses on recovering the stolen device (for example through GPS tracking), hardly any of them address the motive of the theft. While money itself is hard to render unusable in case of a theft, devices and small equipment could potentially be “bricked” in case of theft. “Bricking” is a slang term in computer science and electronics used to mean a broken electronic device that lacks any functionality or usability (Techopedia 2020). Bricking in this case means disabling the device, rendering it inoperable. If the device were to be “bricked” in case of theft, this would mean there is no motive to steal, since the stolen item loses its value upon being stolen.

3.1 Physical Security

A variety of different technologies are currently in use in theft prevention applications. The most common and the simplest of these to implement is physical security. Physical security can come in many forms, depending on the location that needs securing, and is usually the cheapest option when it comes to theft prevention.

ERA (European Rental Association) notes that one of the most basic practices for physical security is providing safe containers to worksites. In addition to providing secure containers to worksites, ERA suggests chaining equipment together. This is intended to make potential theft as time and physically consuming as possible. Though anti–theft chains, as shown in Image 1, can be broken with proper equipment, this causes an additional burden for the would–be thief. (European Rental Association 2019, 2.)

Image 1. Antitheft Cable (John Morris Group 2020)

TER (The Equipment Register) in its manual titled *Loss Prevention and Security Techniques for Equipment Owners & Hirers* published in 2017, states that site security is vital for asset protection, but also notes that implementing it can be difficult if the work site is mobile (e.g. small repairs/construction sites), or very large (e.g. farms/some dockyards). Some examples of site security are:

- Warning signs
- Fencing/Barriers
- Lighting
- Locks

The TER manual names locks as usually the weakest link in site security. Locks can be picked or forced relatively easily if the manufacturing quality of the lock is shoddy, and combination locks come with the risk of an employee sharing the code. (The Equipment Register 2017, 8–9.)

In addition to TER and ERA recommendations there are more official publications about site/equipment security. As an example, one of these official publications is the Finnish VAHTI (Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä). VAHTI publications primarily focus on information security on governmental level, but since they need to pass through much scrutiny, some of their recommendations can be implemented partly or in a lesser extent to provide effective security measures. VAHTI documents can also provide the same insights as TER and ERA, but with more authority. VAHTI documents for example suggest fencing or limiting access to worksites, if this is impossible the sites borders could be marked with warning signs (VALTIOVARAINMINISTERIÖ 2013, 23–24,27).

This official recommendation for site security brings up the same point TER and ERA have made about site security. Although unlike NER and ERA, VAHTI documents dive deeper into the issues, and bring up circumstances when implementing a security feature is not practical.

Although physical security seems like the obvious choice when taking in the factors of cost, effectiveness and ease of implementation, it is important to remember, that like in every other problem there is no silver bullet for theft prevention. Any one solution, be it physical or electronic, is not enough to stop or prevent theft entirely. Theft prevention devices are not designed to prevent all theft, but act more in a dual role, prevention for amateurs and deterrent for the professionals. The most effective security is a combination of different methods, with each designed to combat different risk factor.

3.2 RFID

RFID is visible in everyday life from smartcards to factory inventory management. RFID in theft prevention is arguably mostly visible in retail stores and libraries. For example, a large number of library books contain RFID barcode labels, which are deactivated when the book is checked out.

Image 2. RFID library tag (RFIDHY 2020)

If the tag(s) in Image 2 isn’t deactivated, the tag is detected by RFID detectors, shown on Image 3, located usually near entrances or exits and causes an alarm to trigger.

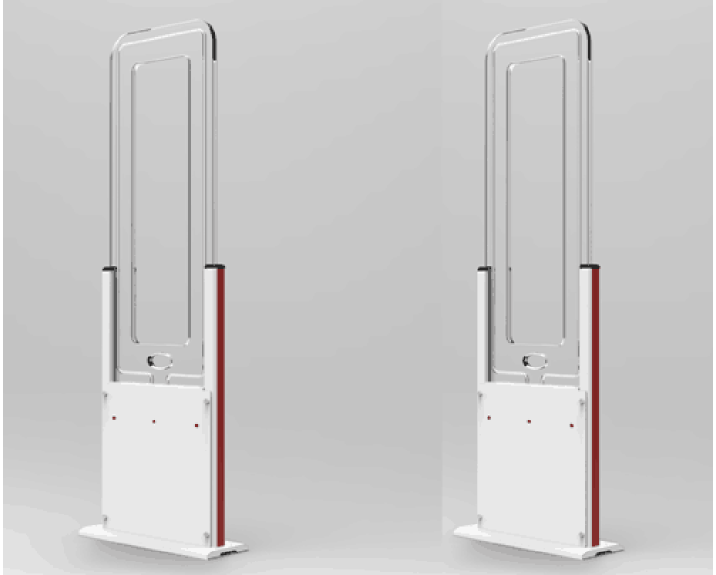


Image 3. RFID gate (Alibaba 2020)

3.2.1 Basics

RFID (Radio Frequency–Identification) has been the staple of the tracking industry for decades. In its most basic form, RFID tag or label consists of an LC tank circuit, which is usually made of a coil and a capacitor. Modern and secure tags use specialized RFID IC's that enable security and digital data transfer. As the name suggests, RFID works by utilizing radio waves. When the reader sends out a radio signal, the coil on the receiver tag energizes inducing a current and filling up the capacitator. Once the signal changes, the current induced by the receiver coil changes too, causing oscillation between the coil and the capacitator. This oscillation produces current changes in the coil, which in term produce a varying magnetic field which when tuned correctly can send a radio signal that the sender can intercept.

Since RFID technology is popular with billions of new tags attached to products every year, some have raised concerns about the environmental effects of plastic and non–degradable tags. In an article published in RFID journal in 2014 John Rogers, a professor of materials science at the University of Illinois, states that they have managed to create an RFID tag out of biodegradable materials, but are still working on making the chip also biodegradable (Roberti 2014). This problem of making the RFID chip itself biodegradable seems to have been solved in 2019. On 5th of June 2019 StoraEnso proclaimed in a blog post about the end of plastic RFID tags and presented their own ECO™ RFID tag technology (Voipio 2019). Though the blog post touts these new tags as biodegradable, ecological and economical alternative to regular RFID tags, the blog post or ECO™ technology brochures do not mention anything about the biodegradability of the RFID IC itself.

3.2.2 Types

RFID tag types can be divided into three groups; active battery powered tags, battery assisted passive tags and plain passive tags.

RFID tag types can be ranked by their transmission power and range:

1. Active tags
2. Battery assisted tags
3. Passive tags

Although RFID is usually used in close proximity situations, using radio technology as its base allows the potential range to vary up to multiple kilometers, if some manufacturers are to be believed (SkyRFID 2020).

As with other RF based technologies, effective range of RFID is typically limited by three factors; environment, tag type and local laws. Environment with large amounts of radio interference or obstacles such as walls, door and natural obstacles (e.g. trees, hills) might limit or make the technology unusable, depending on the use case. From these three tag types, passive tags impose the greatest limitations, since passive RFID tags get their energy from the signal created by the reader. This, combined with local laws that might limit the reader transmission power and potential obstacles in the operating environment, can limit the effective range of passive tags down to few meters (GS1 2020, 2–20).

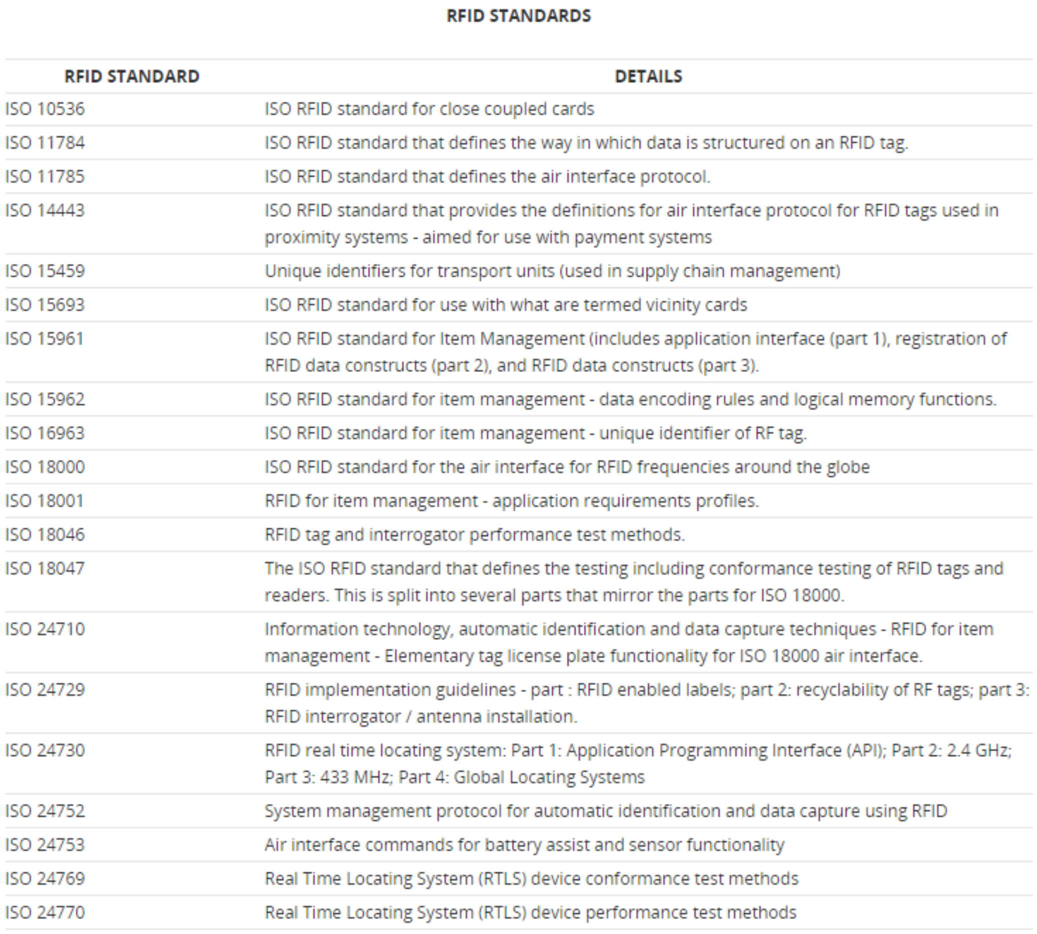
3.2.3 Weakness

Primary weakness of RFID tags is the coil, which is essential for RFID to work. Cheaper RFID tags aren’t tampering proof, since the additional cost outweighs the benefits. The easiest way to disable RFID tag is to puncture the tag, causing the coil to short circuit and cause the tag to become inoperable. This is the case especially with passive RFID tags, since they rely on the coil for power. Effectiveness of passive tags is also limited by them being easily interfered with. Reflective materials can be used to encapsulate the RFID tag, thus preventing the radio signals from ever reaching back the transmitter. This method of interference is especially popular in shoplifting and retail store thefts, and is seen in form of “booster bags” (Womack 2018).

3.2.4 Standards

RFID technology has many differing standards as seen from table 2 taken from Electronics–Notes website (Electronics Notes 2020). In addition to this large number of different standards, RFID also operates on multiple different frequencies, all of which have their own standards. This spread in operating frequencies and standards is problematic, since a product using RFID technology might not be compatible with tags and readers that operate only on some specific standard.

Table 2. RFID Standards (Electronics Notes 2020)



RFID STANDARDS

RFID STANDARD	DETAILS
ISO 10536	ISO RFID standard for close coupled cards
ISO 11784	ISO RFID standard that defines the way in which data is structured on an RFID tag.
ISO 11785	ISO RFID standard that defines the air interface protocol.
ISO 14443	ISO RFID standard that provides the definitions for air interface protocol for RFID tags used in proximity systems - aimed for use with payment systems
ISO 15459	Unique identifiers for transport units (used in supply chain management)
ISO 15693	ISO RFID standard for use with what are termed vicinity cards
ISO 15961	ISO RFID standard for Item Management (includes application interface (part 1), registration of RFID data constructs (part 2), and RFID data constructs (part 3).
ISO 15962	ISO RFID standard for item management - data encoding rules and logical memory functions.
ISO 16963	ISO RFID standard for item management - unique identifier of RF tag.
ISO 18000	ISO RFID standard for the air interface for RFID frequencies around the globe
ISO 18001	RFID for item management - application requirements profiles.
ISO 18046	RFID tag and interrogator performance test methods.
ISO 18047	The ISO RFID standard that defines the testing including conformance testing of RFID tags and readers. This is split into several parts that mirror the parts for ISO 18000.
ISO 24710	Information technology, automatic identification and data capture techniques - RFID for item management - Elementary tag license plate functionality for ISO 18000 air interface.
ISO 24729	RFID implementation guidelines - part : RFID enabled labels; part 2: recyclability of RF tags; part 3: RFID interrogator / antenna installation.
ISO 24730	RFID real time locating system: Part 1: Application Programming Interface (API); Part 2: 2.4 GHz; Part 3: 433 MHz; Part 4: Global Locating Systems
ISO 24752	System management protocol for automatic identification and data capture using RFID
ISO 24753	Air interface commands for battery assist and sensor functionality
ISO 24769	Real Time Locating System (RTLS) device conformance test methods
ISO 24770	Real Time Locating System (RTLS) device performance test methods

3.3 Bluetooth

An example of the use of Bluetooth in theft prevention, can be a common Bluetooth key locator tag like the in Image 4. These tags simply alert the user if they move too far away from the tag. Although the main use of these devices seems to be as ordinary as preventing locking yourself out of the house, the fact that the distance and presence of the tag is monitored, makes the same concept easily applicable to theft prevention. When reliable and constant asset tracking is achieved, anomalies can be monitored thus providing *theft detection*.

Image 4. Bluetooth tracker tag (Powerstick 2020)

3.3.1 Basics

Bluetooth is a semi short range peer–to–peer and broadcast capable data transmission technology, that operates on the 2.4GHz ISM (Industrial, Scientific and Medical) band along with other data transfer technologies, such as Wi–Fi. Since its conception, Bluetooth has been used quite extensively in mobile devices and accessories, but has also seen an increase in use in IoT applications. This is due to its LE (Low Energy) version that is designed towards IoT, and other applications that require a lower power consumption than classic. Bluetooth's specifications and further development is handled by Bluetooth SIG.

3.3.2 Classic and Low Energy

When talking about Bluetooth, an important distinction between Bluetooth Classic, and Bluetooth LE, has to be made clear. Although Bluetooth has existed since 1999, what we now know as Bluetooth LE was developed by Nokia in mid 2000s and was called Wibree. After that it was incorporated into Bluetooth 4.0 and introduced to the public in 2010. Upon its release it was not under the name LE, but was called Bluetooth Smart. Since the initial name caused confusion in developers and users alike, it was later named LE, and all older tech is grouped under umbrella term Bluetooth Classic. Although the name was changed to Low Energy that is arguably less confusing, some sources, guides and older literature on the internet still use the term Bluetooth Smart and do not make a sufficient distinction between the new and the old term, making research and development sources sometimes hard to comprehend. (Get Connected Blog 2019) Difference of classic and LE stacks can be seen from figure 2.

Probably one lesser known fact is, that classic Bluetooth devices cannot communicate directly with Bluetooth LE devices (Torvmark 2014, 2.). This is not immediately apparent to a consumer or a user, who primarily use Bluetooth through devices such as smart phones. This is due to most smart phones containing a dual Bluetooth radio, which enables apparently seamless operation between Classic and LE.

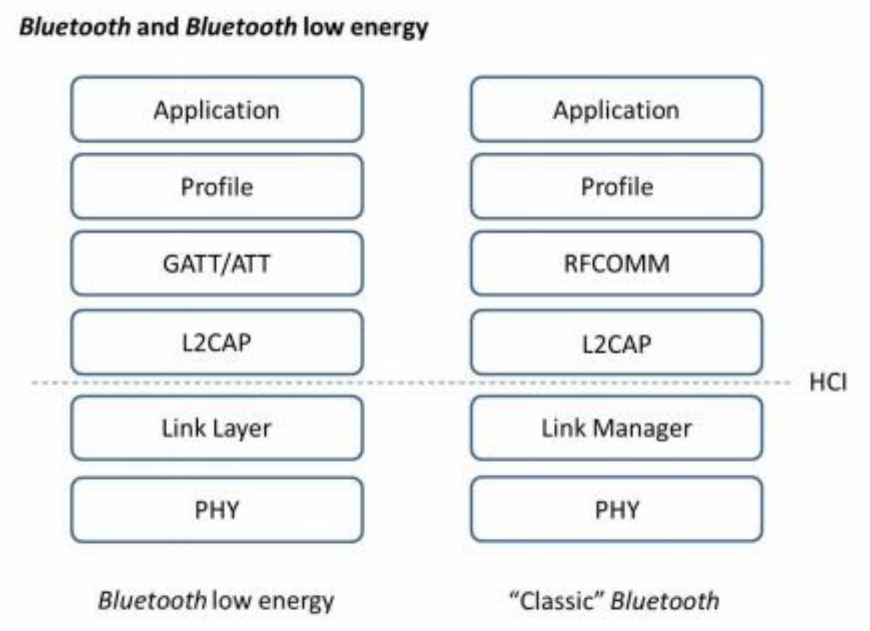


Figure 1. Bluetooth Classic and LE stack (Torvmark 2014, 4.)

3.3.3 Profiles

Bluetooth implements its data exchange in form of Bluetooth profiles. Profiles encapsulate all Bluetooth protocol layers, typically from PHY to L2CAP in them, and help to provide interoperability between different Bluetooth devices with differing versions. This interoperability is achieved if both devices follow the rules specification of a specific profile. According to Bluetooth documentation, even data formats can be defined by the profile. (Bluetooth SIG 2019, 267–269.)

Although, this depends on the way the Bluetooth profile is implemented and accessed. For example, using Laird's BL654 and AT commands data format is hexadecimal, string or integer (Laird 2018b, 8.)

GAP (Generic Access Profile) is a base profile that is implemented by all Bluetooth devices. What this profile defines, differs depending on if the Bluetooth device is LE capable, or an older BR/EDR type. (Bluetooth SIG 2019, 268.)

3.3.4 Locatability

Since Bluetooth has similar characteristics as Wi–Fi, it is capable of many of the same functionalities used with Wi–Fi, such as location and distance approximations.

The distance approximation is usually done by using RSSI (Received Signal Strength Indicator), value of the connection, and location/direction can be estimated by combining RSSI value with Bluetooth 5.1's new AOD and AOA estimation capabilities. AOD and AOA are acronyms of Angle Of Arrival and Angle Of Departure. What these mean in terms of Bluetooth is that a Bluetooth 5.1 capable device with multiple antennas is able to estimate the direction from which a packet was either received or sent to. (Bluetooth SIG 2019, 281–284.)

According to Bluetooth 5.1 feature overview document, AOA and AOD are not the only improvement coming to Bluetooth location mechanics. The feature document also mentions a roadmap, and promises to provide IPS (Indoor Positioning System) and RTLS (Real–Time Location System) capabilities in the future, but this roadmap was not found on Bluetooth.com. (Woolley 2019, 4–5.)

3.3.5 Interference negation

Since many wireless technologies operate on the 2.4GHz ISM band due to its usage not requiring a license, interference can occur between devices receiving or transmitting on the same frequency at the same time. Without means to negate radio interference, appliances such as smart fridges, tv's and Wi–Fi access points could disrupt or prevent the usage of Bluetooth devices, such as headsets.

How different technologies deal with negating interference differs, but some methods remain the same. One of the common methods to deal with interference relates to spread spectrum and frequency hopping. A spread spectrum basically means the spectrum of frequencies a radio transmission is spread to.

Simple example of this would be that when sending 10 bytes of data, rather than using one frequency to send all the 10 bytes, the bytes are spread across 10 channels. Then, when one byte is transferred on channel 1, the channel is then changed before sending the next byte, effectively spreading the transmission on a spectrum, while engaging in frequency hopping when changing channels.

By using frequency hopping like described in an example, data retransmission times can be reduced; if interference occurs it is unlikely it affects all the frequencies used, thus enabling at least some of the data to get through. Depending on the application this might be enough. Some applications could compensate for the missing data without making the application unusable. Video data, for example, could suffer from lost frames and stutter and still be usable.

Frequency hopping in itself just describes the idea of spreading the transmission on different frequencies to avoid interference, but how it is implemented differs between technologies. One implementation of frequency hopping method in Bluetooth is called Adaptive Frequency Hopping (AFH). In AFH channels used in transmitting data are constantly monitored for interference, and if interference is detected, channels list is changed according to detected interference. (Bluetooth SIG 2019, 274–275.)

How many hops are made, depends on the mode and type of Bluetooth used. For example, classic Bluetooth using BR (Basic Rate) modulation does hops on over 79 channels and discovery on 32, whilst Bluetooth LE hops only on 37 channels and uses discovery on 3 channels (Torvmark 2014, 3.). Minimum amount of channel allowed by Bluetooth specification for AFH is 20 (Bluetooth SIG 2019, 274).

More or less hops are not always better. In a case of 79 channels, chances of interruption and radio interference is lower than on 37 hops, but since LE does discovery on only three channels, as opposed to 32, the connection time is quicker. Smaller connection time is also beneficial in terms of LE since the radio can be turned off faster, thus providing greater energy savings.

Modulation in data transfer using radios describes how data is encoded into the carrier wave. What modulation types are available differs, depending on the type of Bluetooth in use (LE or Classic). Bluetooth's basic rate (1Mbit/s) uses Gaussian frequency shift keying as its modulation method, and this has been present in Bluetooth since version 1. In order to achieve higher data transfer rates EDR (Enhanced Data Rate) was introduced in Bluetooth version 2. This modulation uses two different types of phase shift keying methods to achieve transmission speeds of up to 3Mbps of raw data. (Electronics Notes 2019)

3.4 GPS

3.4.1 Operation

GPS (Global Positioning System) is a wide area location technology that uses specialized satellites to obtain its global coordinates. The GPS system was initially developed for military use but has since transitioned into civilian implementations as well. GPS network is operated and maintained by the U.S government. Today the GPS network consists of over 30 satellites that transmit their positions and time at certain intervals, and these signals can then be picked up by GPS receivers. The location of the receiver is determined by the time it took for it to receive the signal and is based on the doppler effect. (NASA 2019)

Popularity of GPS is high in theft recovery devices, since it's one of the few technologies capable of providing tracking ability globally. Most common use for GPS anti–theft trackers seems to be vehicles, but GPS location is also popular in tracking items that have a build in GPS receiver, although it is not their primary purpose, such as mobile phones.

Image 5. ORBCOMM GPS Tracker (ORBCOMM 2017)

Though GPS seems like the "go to" solution for tracking, there are limitations in its use. Highly populated and dense urban areas can make GPS unusable, since they might not be able to provide sufficiently accurate data. Even though devices such as ORBCOMM XT–4760 shown in Image 5 are capable of ~2.5m accuracy, in an urban small area this can cover multiple apartments (ORBCOMM 2017, 2). Additionally, walls, structures and radio interference from other electronic devices can hamper the operation.

GPS is also vulnerable to purposely inflicted interference, that can cause the GPS to lose signal completely and become inoperable. Depending on the device in which GPS is used, this purposeful interference can be as easy to cause as submerging the device in water or placing it in a tinfoil covered bag (such as booster bags).

Another pitfall of GPS is that it requires another connection to make the GPS data available. This can be in form of Wi–Fi connection, or more commonly used GPRS connection that is made with a SIM card. If no internet or GSM network connection is available, it can be hard to make anything useful out of GPS data since it cannot be transferred out from the device. The requirement for an additional radio for data transfer has drawbacks that directly affect the usability of GPS, if SIM card and mobile network is used then there are usually recurring charges, but this depends on the mobile network operator. In a case where SIM and mobile network connectivity is replaced by for example Wi–Fi then different problems arise.

Additional radio also provides more technically inclined thieves another attack surface. If the operation of GPS module cannot be blocked, then maybe the additional radio's operation can be interfered with, thus rendering the whole device ineffective.

In conclusion, while GPS does its job well and provides sufficiently accurate data, it is not in itself suitable for real time–tracking, or theft prevention devices.

3.4.2 Messages and message format

GPS message types may vary between each manufacturers' implementation, but there are also common protocols. One of these is the NMEA (National Marine Electronics Association) standard, which according to gpsworld.com is supported by every GPS manufacturer (Gakstatter 2015). Different versions of the NMEA message standard exist, with the latest version being NMEA 2000. Earlier versions such as NMEA 0183 are still commonly used, and according to article on GitLab commercial GPS receivers have not adopted the 2000 standard. (Eric 2019.)

NMEA will only be covered briefly and through secondary sources due to extensive commercialization of the standard. The NMEA protocol specification could not be viewed directly, since it is copyrighted with a starting price tag of 1000$. (NMEA 2018.)

NMEA messages differ slightly depending on the version. NMEA 0183 for example defines over 20 different message types. These messages may contain data about the GPS location or information about the satellites currently available. NMEA sentences are transmitted through an asynchronous serial connection. The serial connection parameters are defined in the NMEA specification, including the baud rate, that despite being defined as 4800bps, can differ depending on the GPS module manufacturer. (Eric 2019.)

Format for NMEA 0183 message is simple and easy to understand. Each message starts with a "$" character followed by two letter "talker ID" which is usually "GP" and is followed by a three letter "type code". After the initial sentence tag comes the actual message data that is separated by commas. (Eric 2019.)

3.5 ZigBee

While ZigBee has similar capabilities to Bluetooth and Wi–Fi, it was not chosen as a comparable technology since currently no Kemppi product utilizes ZigBee. This would inevitably mean a raise in production costs if existing hardware cannot be used.

There are products that encompass many popular radios into one neat IC such as nRF52840 from Nordic Semiconductor which includes both Bluetooth and ZigBee capabilities (Nordic Semiconductor 2020). Since ZigBee is not already in use in Kemppi's products this module was not considered since BL654 already provides similar functionality and is a successor to a chip already used in Kemppi's radio cards.

3.6 Emerging technologies

3.6.1 DRM

Digital Rights Management (DRM) is a technology usually found in desktop/gaming console software products rather than embedded systems. This can be seen from figure 3 which prominently features Epic Games and Microsoft Store logos.

As popularity of IoT devices rises software is ever more increasingly present and integral part in previously dumb devices such as coffee makers and fridges. Software protections can be used to protect not only from digital but also physical theft. After all, if the device relies on software that stops working in case of theft what's the motive to commit theft?

Circumventing DRM systems is nothing new and games with the latest DRM software usually last only few months before the protection is broken. In a case of embedded software, which often lacks the IO of its counterparts, this kind of DRM circumvention can be much harder and maybe not worth the effort.

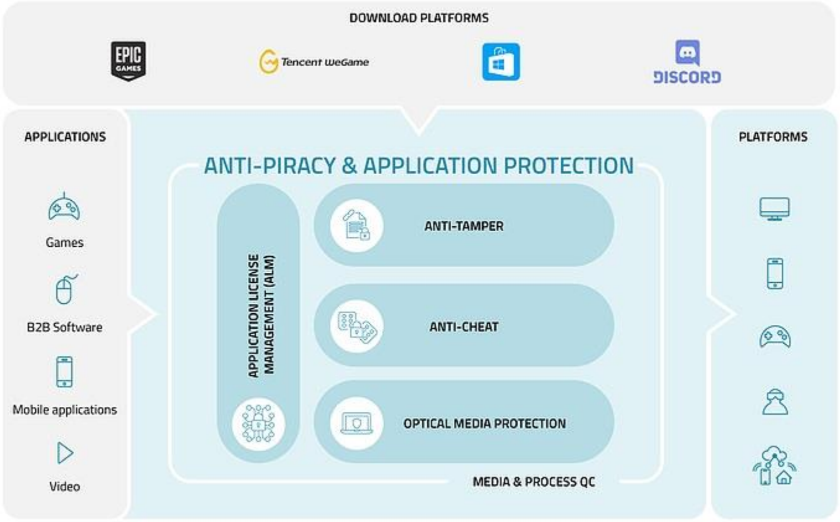


Figure 2. Denuvo DRM (Irderto 2020)

One way DRM works is to use some sort of external connection to call home, usually to verify a license. If the call is unsuccessful the DRM protection activates and prevents usage or the device or software. (Irdeto 2020.)

DRM methods have their downsides too. One of the leading DRM providers Denuvo has often been criticised by end users for performance issues caused by the software as well as its always online requirement (Hoffman 2018; Krasnai 2019). This could hamper or prevent embedded device functionality if the DRM requires too much computing power. In the future DRM could rise to more prominence in manufacturing environments, due to IoT becoming more popular and industry 4.0 on the horizon. Industry of the future will heavily rely on software and interconnected devices. Each of these devices could contain copyright protected programs and DRM technology would be a natural choice to prevent misuse or intellectual property theft in addition to physical theft.

3.6.2 LORA

LoRa Alliance is a non–profit organization founded in 2015 that is responsible for LoRa standardization and promotion. Currently the alliance has over 500 members including big well–known companies such as Amazon, Cisco and ARM. (LoRa Alliance® 2020.)

LoRa has great potential to be utilized in theft prevention since it has long range and free and unlicensed network. It has been used in smart sensor devices such as RamiSmart (Ramirent 2019). In addition to this large companies such as Alibaba and Semtech have announced a LoRa based GPS free tracker designed for theft prevention (Bloomberg 2019).

LoRa (Long Range Radio) is a relatively new technology that provides low power, low bandwidth and long-range radio communications designed specifically for use in IoT applications such as smart meters, sensors etc (LoRa Alliance 2015, 5). Since the usage of LoRa network is potentially free and range of even a single device can be multiple kilometres, peer to peer communications could be established with extremely low costs.

While LoRa is about the OSI layer 1 (physical layer) communication LoRaWAN builds upon this radio technology and adds features such as encryption and identification that can be used to secure and identify different LoRaWAN devices. (LoRa Alliance 2015, 7.)

LoRaWAN architecture usually consists of four parts:

- End Nodes
- Gateways
- Network Server
- Application Server

Network topology in LoRaWAN is typically star of stars where gateways are in the center and end devices are the tips of the star. End devices operate on a single hop LoRa or FSK to communicate with one or many gateways that are connected to an IP network. End nodes in LoRa architecture are the actual IoT devices for example a temperature sensor. Gateways work as concentrators, they gather LoRa messages from all end nodes in their range and pass the messages to the application server through an internet connection. (LoRa Alliance 2018, 1, 7, 12.) Visual representation of LoRa architecture is shown in figure 4.

Network server is responsible for managing the network. This is to transfer processing from gateways and nodes to central server thus reducing power consumption of end devices. (LoRa Alliance 2015, 8.)

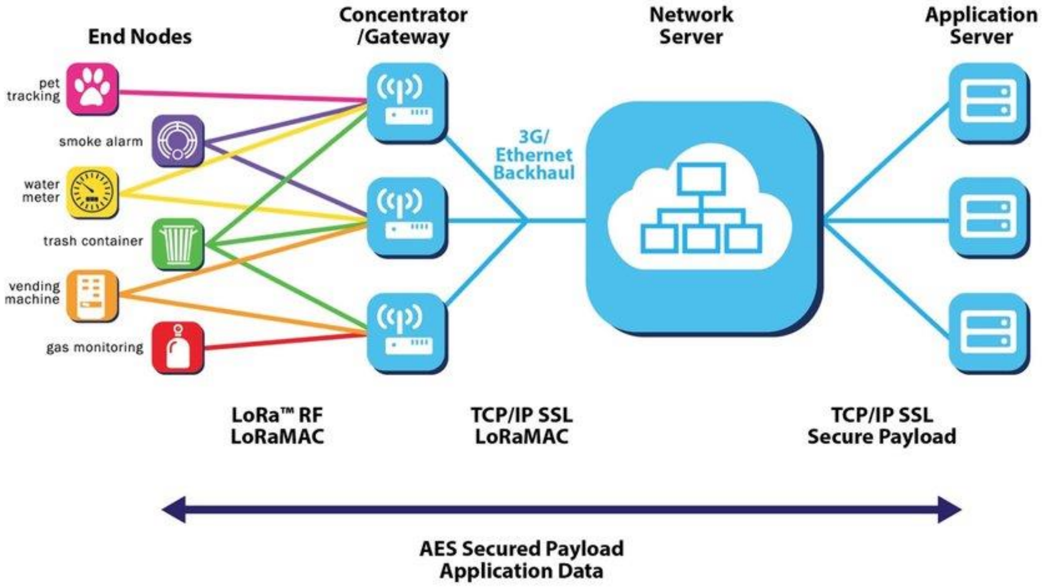


Figure 3. LoRa Architecture (LoRa Alliance 2018)

LoRaWAN regional parameters document specifies frequency ranges for different geographical regions. European area has a designated operation frequency of 863-870Mhz and 433-434Mhz with at least three default channels implemented by every end device. In LoRaWAN these European frequency areas have a common name of EU868 and EU433. (LoRa Alliance 2019, 23, 39.)

Connection times in Lora seem long but this seemingly long connection time is explained by the Lora regional parameters document which states that join request accept delay times are by default 5–6s. Although according to the document these default settings can be changed, the application server may reject parameters that differ from the default. (LoRa Alliance 2019, 21.)

The network can manage the data rates of individual end nodes. This is called Adaptive Data Rate (ADR) and is used to maximize network capacity and end node battery life. It is also possible to use fixed data rate. Number of channels and their data rates vary by region basis but in Europe for example there are 8 multi data rate channels and additional two fixed rate channels with highest speed only available with FSK (Frequency Key Shifting) modulation. (LoRa Alliance 2015, 9–10.)

LoRa specification defines two ways to join a LoRa network, an ABP (Activation-By-Personalization) and OTAA (Over-The-Air-Activation). ABP differs from OTAA in a way that it connects directly to the network with parameters device address (DevAddr), network session key (NwkSKey) and application session key (AppSKey) rather than with End–device identifier (DevEUI), application identifier (AppEUI) and Application key (AppKey) used in OTAA. With ABP secret keys like network session key are hardcoded on the device whilst OTAA uses its parameters to negotiate the secret key exchange from the application server. (LoRa Alliance 2018, 33–37.)

4 THEFT PREVENTION PROTOTYPE

In a meeting with the R&D manager of Kemppi, several variations of the theft prevention prototype were discussed. Some of them can be seen in Image 6. The development method was also briefly discussed, with iterative prototyping being chosen as the method.

For the prototype theft prevention device three different ideas were conceived. Since devices dealing with theft are usually divided to theft prevention devices (that try to prevent theft) and theft recovery devices (that enable the recovery of stolen goods), it was decided that each concept idea should target one of these device roles. In addition to these two device types, a third one was hypothesized.

This third device role can be called “theft nullification” or “usability limiter”, the idea being that if there is no monetary or functional benefit from stolen property then what is the point to steal it in the first place, other than to cause malice? The “theft nullification” device intends to do this by temporarily “bricking” the device in the event of theft. While this term is often used to describe devices that have broken due to misuse or software corruption, in this case the “bricking” is intentional and can be undone, making it function more like a software lock. This can also be thought of as usability/software geofencing. However this idea is not applicable in all potential target devices. Electronic screwdrivers for example are still “dumb” machines with limited processing power and no ICs except for motor control and support circuitry. Since the theft nullification device intends to achieve its “bricking” effect by using software, this might not be feasible with these kinds of devices. The fully mechanical nature of some small equipment makes using this sort of approach impossible to implement.

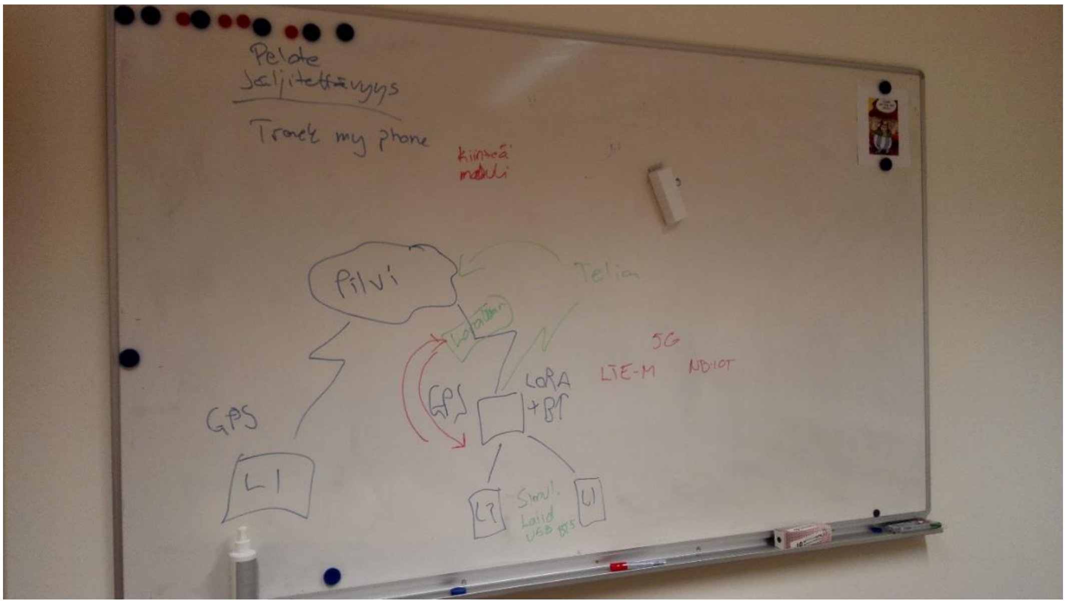


Image 6. Prototyping during meeting

The theft prevention method that was found to be the most interesting and was ultimately chosen as the method was the “nullification” method which bricks the target device in the case of theft. It was chosen due to it being a more uncommon approach to a common problem. While theft prevention devices can be described as active protection and theft recovery devices as reactive, the theft nullification device is a mix of both.

The idea in the prototype was to use small, cheap and embeddable chips as “tags” that can be tracked. These tags can be thought to be similar to a common RFID tag. RFID tags were briefly considered but due to the multitude of standards and the need for data transfer they were ultimately not chosen since Bluetooth outperforms RFID and some Kemppi machines already contain Bluetooth radios. The tags report their existence to a listener later referred to as the “Access Point”, with data used to identify the tag and its location. The access point reads and records this data and passes a message back to the tag that determines whether the device is allowed to operate. If the message received from the access point indicates that the tag should not operate, the tag then bricks the device it is connected to until it is unbricked by the access point or through some other method. Records collected by the access point are sent through the LoRa network to a server which can monitor the tags and detect inconsistencies. These inconsistencies are use case specific and out of the scope of this thesis but in essence these inconsistencies should provide a timely detection of theft if the company using the tags has proper inventory management procedures in place. The tags are not designed to handle messy and inconsistent placement of tag devices and access points.

4.1 Target device

The prototype is designed to be compatible with Kemppi Oy’s Minarc Evo portable welder shown in Image 7. Since the prototype device idea is designed and tested with Kemppi products in mind, it is inevitably somewhat compatible with other Kemppi products that internally work similar to Minarc Evo devices. Though the prototype is geared towards one specific product, the idea should be compatible with a range of different types of small equipment and not limited to Kemppi Oy’s devices.

Image 7. Kemppi Minarc (Kemppi 2020)

Depending on the size, power consumption and other characteristics of the prototype, which can vary depending on parts used and if casing is made or needed, the prototype could be used with devices such as electronic screw drivers, toolboxes, lawn mowers etc. The goal of the prototype is not to be an all–in–one universal small equipment theft prevention device, but if the prototype idea works in one application, then it could be refined further to fit other applications and environments.

4.2 Electronic Parts

Out of all the variants, a prototype that uses Bluetooth as the communication method between the tag and AP and LoRa between AP and the backend (internet) was chosen. These technologies were chosen because they offer good capabilities in terms of short- and long-range communications and there are no monthly expenses like with GSM-based solutions.

The electronic parts, especially the BL654 and Raspberry Pi, were chosen because of familiarity with these devices and because some Kemppi products already use these electronic modules. Using the same base electronics can provide better compatibility and hardware interchangeability.

4.2.1 CPU – Raspberry Pi 3 and MKR1300

Raspberry Pi is a popular single board computer that comes in a variety of forms. Most people are familiar with Raspberry Pi's versions 1,2,3,4 and their variants A,B,+ models that are the size of a credit card and feature IO commonly found in modern PC's such as HDMI and 3.5mm audio jack. Less well–known versions of Raspberry Pi are the zero, zero w and compute module variants, which are geared towards a more specific use case, as opposed to the general use nature of other Raspberry Pi versions.

Common to all Raspberry's is the SoC (System on a chip) on the board which is part of the BCM2XXX family (Raspberry Pi 2020). The specific SoC version differs depending on the Raspberry Pi's model. Capabilities in terms of raw processing power differ a lot between Raspberry Pi models based on what processor the BCM chip contains. This difference can be demonstrated by comparing the Raspberry Pi 3B+ and zero. While the 3B+ model features a quad–core ARM Cortex A53, the zero only has 700Mhz ARM1176JZF–S.

Although Raspberry Pi is marketed and widely viewed as a hobbyist and prototype board, it has also found use in many professional business applications such as Kemppi's digital connectivity module shown in Image 8.

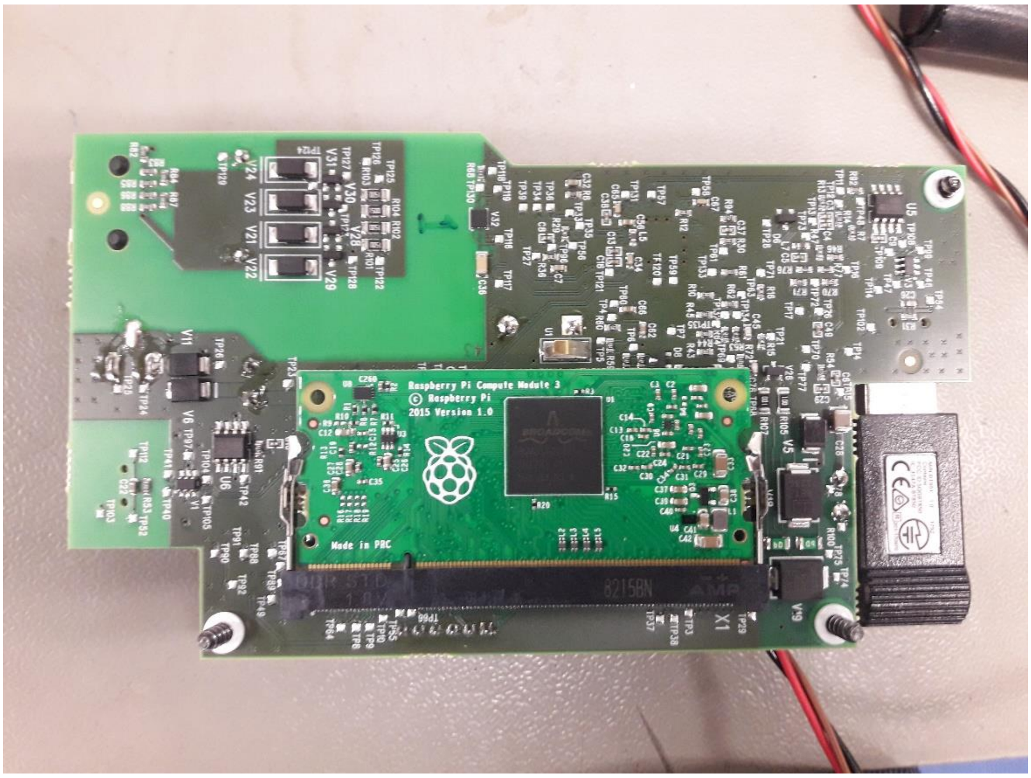


Image 8. Raspberry Pi compute module and BL652 in Kemppi DCM

MKR1300 is a development board produced by a widely known hobbyist/enthusiast company Arduino. Arduino MKR1300 is on the same base PCB layout as the MKR Zero, uses the same 32bit SAMD21 Cortex–M0 ARM microprocessor and provides similar features and IO but is accompanied with a Murata CMWX1ZZABZ Lo–Ra module. The board has a micro UFL connector for an antenna that is used by the LoRa module. A compatible antenna is not included with the MKR1300 but the technical specifications on the Arduino store page state that the antenna power is 2db (Arduino 2020). It is unclear what this refers to since the Murata module's documentation does not mention any integrated antennas (Murata Investment Co 2016, 4).

When configuring MKR1300, a guide on the Arduino project hub was followed which detailed the first configuration and TheThingsNetwork integration. (FabLab_CastelfrancoVeneto 2019)

4.2.2 Bluetooth – BL654

BL654 is a Bluetooth module based on Nordic nRF52840 manufactured by Laird. BL654 is not just a Bluetooth module but is also capable of NFC communications, depending on the module variant. BL654 comes with many programming options in terms of language, even being able to be programmed by using Laird's own super set of BASIC language called SmartBASIC. Using SmartBASIC and programmable GPIO pins, BL654 can be used in standalone applications such as a Bluetooth remote.

As an alternative to using SmartBASIC, the BL654 module can be controlled by another microprocessor using a serial interface and AT commands. AT commands, also known as the Hayes command set, is a set of ASCII commands following a specific pattern originally designed to be used with modems. Though using SmartBASIC provides more in–depth usage of BL654's capabilities, almost all of this can be achieved by simple AT commands without the need to program the module itself. To enable the use of AT commands, BL654 must be flashed with the ATinterface program provided by Laird (Laird 2020a). The AT parser program by Laird is written with SmartBasic and modification of the software is encouraged.

The module contains an S register. Similarly to old modems, the BL654's S register contains various values that are used to control settings. For example S register number 302 defines the UART interface's baud rate. (Laird 2018b, 29.)

The S register can also be used as a non–volatile storage. The BL654's documentation states that S register slots 117–137 can store integer values from –128 to +127. Slots 213–219 are also free to be used and can store larger integer values. These slots can hold values from –32768 up to +32767. (Laird 2018b, 28–29.) This non–volatile storage can be used to store data over boot without the need for external memory modules. Although there are only a few slots and their size range from int8 to int16, they could be used to hold data such as startup flags, settings values and potentially even a MAC address or GPS coordinates.

4.2.3 GPS – Ublox NEO6M

The NEO-6 GPS module is a stand–alone GPS receiver produced by ublox. The module features a small form factor of 16x12.2.x2.4mm and a high performing positioning engine capable of TTFF (Time-To-First-Fix) of under 1 second on hot start. NEO–6 series modules are capable of great accuracy: according to the datasheet, GPS position accuracy can be as high as 2.5m with velocity accuracy of 0.1m/s and heading error less than 1 degree. All NEO–6 receivers support a passive or an active antenna. The recommended minimum gain of an antenna is 15db. This lower limit is based on the signal loss in the RF cable. (U-Blox 2011, 5, 10.)

Power consumption of NEO–6 modules is minimal. The maximum current draw of the module is as low as 67mA with a voltage of 3.6v. This figure can be reduced down to a mere 11mA when operating in power saving mode. (U-Blox 2011, 15.)

The NEO–6 module has multiple interfacing options one of which is UART. The messages outputted through this interface can be in NMEA or UBX format. NMEA is the standard GPS message format whilst UBX is a ublox proprietary format. The output message format and UART baud rate can be changed on the NEO–6 by changing the state of the start–up configuration pins. By default, the module goes into mode where the output format is NMEA and the UART baud rate is 9600. While the message type and baud rate is defined by two pins, a third one can be used to set the power mode. Default power setting is set to “maximum performance”. (U-Blox 2011, 22.)

4.3 Client

4.3.1 Electronics

The theft prevention tag or device, referred to from now on as client, consists of Raspberry Pi 3 model b version 1.2 and a Laird BL654 Bluetooth USB module. The client device is depicted in Image 9.

Image 9. Client device

4.3.2 Operation

In the client, Raspberry is used solely for running a program that communicates through the USB connection with the BL654 module and passes AT commands to it. AT commands, also known as the Hayes command set, are historically modem configuration commands that always start with the letters “AT”, which stand for attention. Though AT commands date back to the 1980’s, they are still widely used with different telecommunications devices such as Lairds BL654. The client’s communication with the BL654 was done with the AT parser program provided by Laird because it is open source and because the program provides all the required functionality. Using the AT parser program also leaves room for module interchangeability since the new module would only need to conform to the same AT message format and naming.

Although Raspberry Pi 3 contains a Bluetooth chip, it is not used in this prototype for two primary reasons. It is not Bluetooth 5 capable and is not modular.

In order to maximize compatibility with Kemppi’s devices, some of which already use Bluetooth for various purposes, a similar chip was selected. At least some of Kemppi’s devices utilize a BL652 module as their Bluetooth interface and with BL654 being successor to BL652 and having the same form factor, using only BL654’s capabilities could provide backwards compatibility to older devices as well as enable newer devices to use the prototype’s theft prevention functionality with only a software update. By potentially providing theft prevention features by a software update, it is plausible to make it an optional addon product that does not affect the manufacturing costs of low–end devices.

In terms of Bluetooth, the client acts in a central role while the access point acts as the peripheral. This sort of relation was chosen because in Bluetooth peripherals act as advertisers and only central devices can initiate a connection. While a system where the access point acts as a central and client devices as peripherals would work and would provide the ability to read multiple devices at the same time, it is impractical to do so. This is due to the fact that the clients are IoT devices and might not have a constant power source, and therefore minimizing the power consumption of clients is a priority. The access point, on the other hand, does not need to worry about power consumption, so it makes sense to concentrate power hungry operations (such as sending advert packets) to it. In addition to the central–peripheral schema, Bluetooth devices can also operate on an observer–broadcaster schema. Whilst this works on certain applications such as displays listening to adverts for sensor data, it is not practical to use this schema between the clients and access points since the advert packets are not encrypted and to detect theft, clients need to announce their presence to the access point at certain intervals, which would require creating a connection to the access point.

4.3.3 Software

The software of the client tag is written in JavaScript and run on the NodeJS environment. NodeJS is an event–based JavaScript running environment that internally uses the same JavaScript engine as Google Chrome.

The operation of the client’s software can be described as a finite state machine. Each step of the process is a state that expects a certain input and reacts accordingly. For example, state 2 in the client handles scanning nearby BLE devices and does so until one of two conditions is fulfilled. Either the scan loop times out, or it finds an advert belonging to the target device. Depending on which condition is fulfilled, the state transitions either a step back or moves forward. Not all states of the client software are capable of returning a step. Most states react to unexpected input by resetting the whole process. The client has seven different states, which are numbered from 1 to 7. Once the last state is reached, the state resets back to 1.

The operation and states of the client can be explained as a list of steps that go as following:

1. This is the wait state. The client waits/sleeps for a predefined number of seconds and then calls a function to start the reporting procedure.
2. Scan state. The client scans for adverts until the scan times out or the target device’s advert is found.
3. Connection state. The client acting as a central device initiates a connection with the target access point.
4. Service Query. The client queries services and searches the returned UUIDs for matches to target service and characteristics.
5. Write state. The client writes its ID and GPS area coordinates to the peripheral device and enables notifications.
6. Notification state. In this state the client waits until the access point has determined if the received coordinates match the device’s allowed area. After the determination, the access point replies to the client using a notification that contains a Boolean value that represent whether the client is in an allowed area.
7. Disconnect and react state. In the final state the client parses the notification message it received and determines if it enables/disables the attached device’s functionality, after which it disconnects from the access point and restarts the sleep loop.

4.3.4 Placement

When talking about the placement options of the client tag, it should be noted that the Raspberry Pi used in the tag is bulky and intended only as a placeholder. Since the intended replacement of the Raspberry Pi is the machine the tag is attached to, the size of the tag can be thought to be the same as the Bluetooth module’s size. In essence, the Raspberry only hosts a program that mimics an actual device.

The BL654 module used in this case comes in many forms, each with a differing size. Though the size could be smaller, the following section on placement is written with the size of the USB variant in mind. The connection method of the tag to the target device may vary. A UART connection is assumed and plug-and-play type of functionality is not considered.

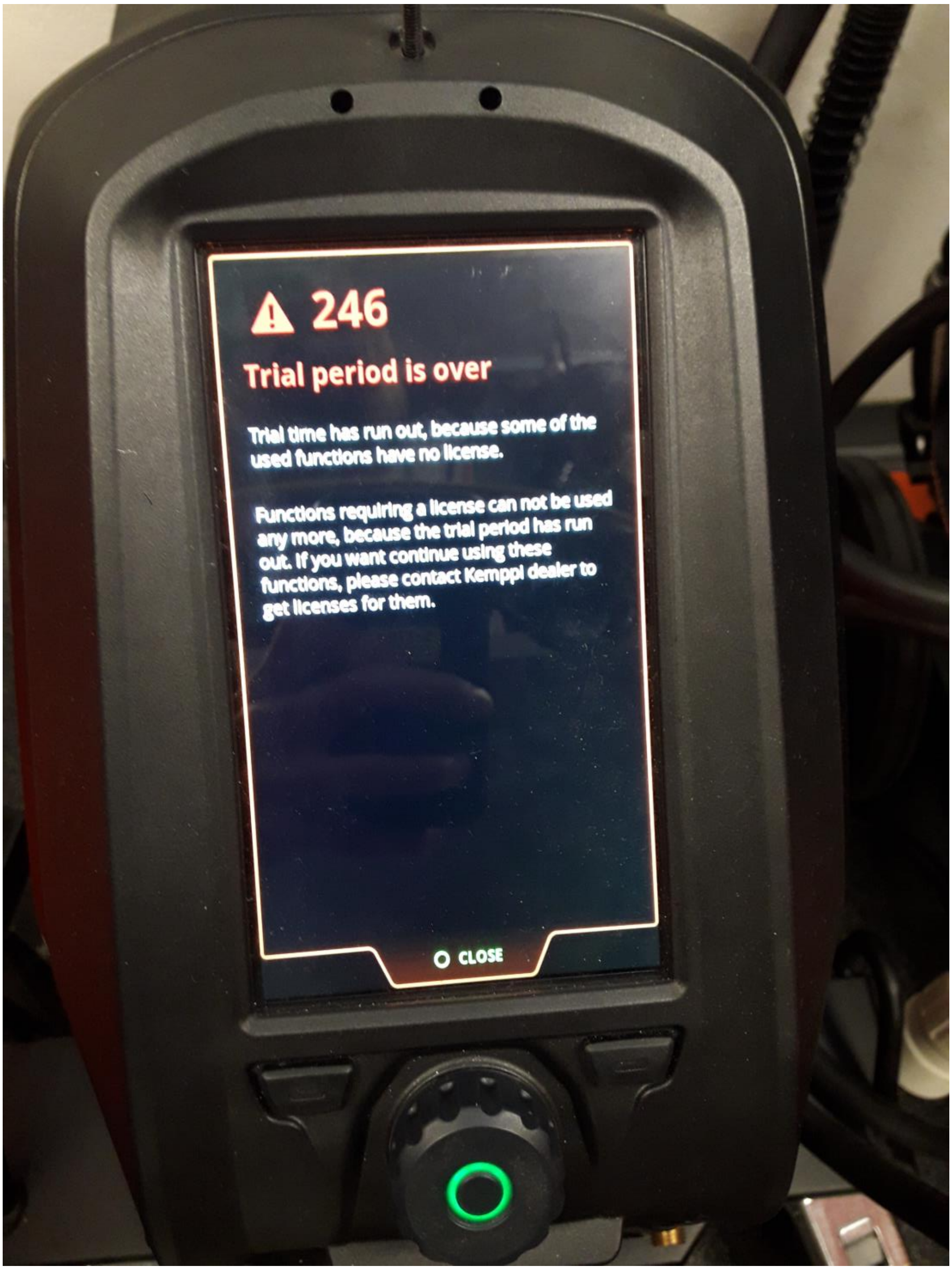
The relatively small size of the Bluetooth module enables it to be potentially attached to a variety of devices. In the case of Minarc, the device could be attached to the back of the control panel. Some Kemppi welding machines already include a Bluetooth module slot behind the control panel. In machines like these the theft protection functionality could be implemented through a software update without any hardware changes, or at most through a software update and the replacement or insertion of a compatible Bluetooth module. Depending on the IO and processing power capabilities of the target device, the tag could be integrated or attached to as small devices as multimeters, battery chargers, electronic screwdrivers and other small equipment.

Since the functionality of the tag relies solely on a Bluetooth connection, and the Bluetooth dongle used in the prototype is a USB variant, the tag could be used in machines that have a free USB connector. Kemppi's machines from 2017 onwards have had a USB connector used mainly for the MobileMaintenance app and software updates but most of the time the connector is free. Instead of reprogramming the radio card, the dongle could be a "plug-and-play" implementation using the mostly free USB port.

4.3.5 Bricking

During the meeting with Kemppi's R&D manager, it was also decided that the actual theft prevention method that affects the functionality of the device being protected would only be hypothesized but not actually implemented.

The way some Kemppi devices could be disabled would be to write to device's internal parameter table it contains bits that affect the machine's operation. One of these is a "weldingNotAllowed" bit, which directly affects the machine's primary use, welding. Locking this bit's state to 1 would disable (brick) the device causing it to become totally unusable. Other values and files could also be modified if the bricking effect needs to be limited. One file that is present on the welder's file system is the welding license file. Removing or writing 0 values to some or all fields in this file would have the effect of removing some or all welding features from the machine. This would effectively achieve the same result as setting the "weldingNotAllowed" bit to 1 but with more control over the features. A potential result of bricking or license removal is shown in Image 10.



⚠ 246

Trial period is over

Trial time has run out, because some of the used functions have no license.

Functions requiring a license can not be used any more, because the trial period has run out. If you want continue using these functions, please contact Kemppi dealer to get licenses for them.

Image 10. Kemppi MasterTIG device with expired license

Although protections like these could be reversed by accessing the device’s CAN bus and reverting the bits or license value, this would require the would-be attacker to possess some technical reverse engineering skills or Kemppi insider information. It is unlikely people engaging in thefts or in organized crime have the skills or patience required to reverse engineer a whole file system that has a proprietary file format called Kemppi bit file (.kbf).

4.4 Access Point

4.4.1 Working principle

The AP (Access Point) works as a gateway to the internet and a bridge between Bluetooth “tag” devices and LoRaWAN network. AP collects reports from nearby devices and keeps a record of them, then at specific intervals these records are forwarded to the LoRa radio and sent to Lora server. AP is also responsible for determining if coordinates supplied by the tag devices are valid and handles distributing new coordinates on request. Access point and its components can be seen in Image 11.

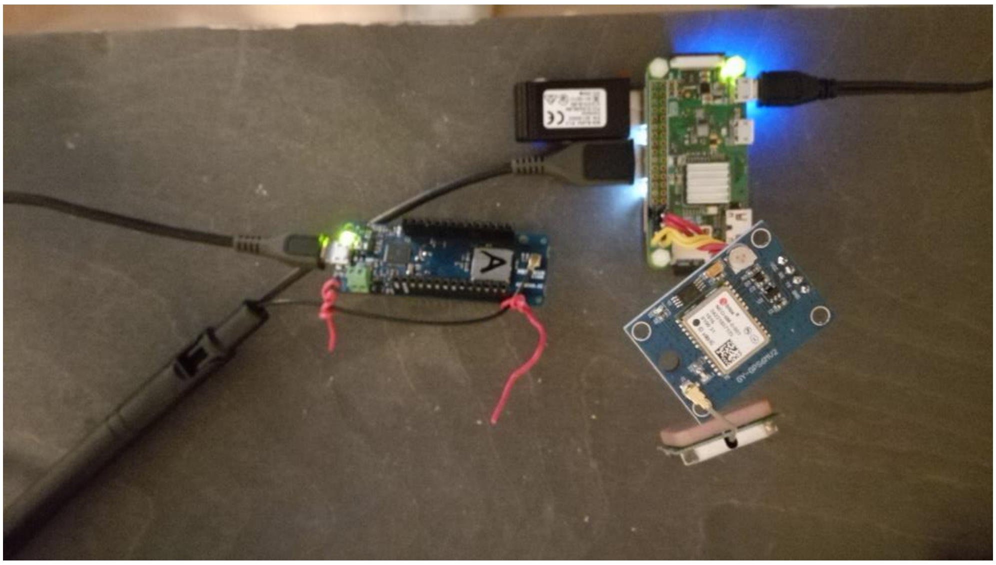


Image 11. Access Point

4.4.2 Electronics

AP consists of 4 different electronic components

- Raspberry Pi 3
- BL654 Bluetooth USB dongle
- NEO6M GPS uart module
- MKR1300

Out of these four Raspberry Pi is the core of the AP device. It manages the communication between the Bluetooth and LoRa radios and checks the clients coordinates during Bluetooth message by comparing them with data received from NEO6M. Raspberry Pi is running the latest version of Raspbian Buster OS which is based on Linux distro called Debian Buster.

BL654 is connected to one of Raspberry’s USB ports. Depending on the operating system running on the Raspberry the USB port of BL654 might be shown as “COMXX” or

“/ttyUSBX” with the X symbol representing a port number. In the case of the AP which is running Linux BL654 is usually mapped to “/ttyUSB0” since it is expected to be the first USB device.

NEO6M is responsible for supplying GPS coordinates to Raspberry which are subsequently forwarded to tags if they ask for new GPS coordinates. The GPS module is connected to Raspberry’s GPIO pins 14 and 15 which are mapped to a “/ttySXX” port with “S” symbol meaning Serial and “X” the port number. The actual port name might not be in form of “/ttySXX” depending on the serial configuration.

MKR1300 is also connected to Raspberry through a USB port. Since MKR1300 lacks support for Software Serial library and its only hardware serial is used to communicate with the Murata LoRa radio, USB was chosen. MKR1300 is responsible for listening its USB serial port for Bluetooth records to be send to LoRa network. MKR1300 is a single purpose device that only engages in limited communication (half–duplex) with the Raspberry and could be replaced with a LoRa radio module directly.

4.4.3 Software

Software of the access point is divided into different components called services. Each service is responsible for one specific task in accordance with the separation of concerns principle. A separate main service instantiates these services and manages the communication between them. Each service consists of a JavaScript class. Software architecture of the AP can be described as service–orientated or component based.

Services running on the access point are:

1. RecorderService

2. LoggerService

3. BluetoothService

4. UpdaterService

5. GpsService

One instance of each service is created by the main process running on the access point. Recorder service is responsible for keeping records of each Bluetooth transaction, these records are at some point transferred to UpdaterService. UpdaterService is responsible for handling communication between the Raspberry Pi and MKR1300. LoggerService is used to create logs that can be used to debug bugs and anomalies in operation. BluetoothService can be considered the main part of the access point. It handles the communication and parses the AT messages send to and from the BL654 dongle. BluetoothService also contains an instance of RecorderService that is used to save received messages. GpsService is responsible for communication with the GPS module through a UART connection on Raspberry’s GPIO pins 13 and 14. These GPS coordinates are used by the BluetoothService to verify tag locations and are assigned to tags when they request new coordinates. Since the accesspoint manages multiple IO ports (2 USB, 1 Serial) use of worker threads was considered but according to NodeJS documentation, threading is unnecessary for IO related operations (Node.js 2020).

After start up the main service initializes all previously listed services except RecorderService. RecorderService is an internal part of BluetoothService and it is initialised at the same time as BluetoothService.

First service to start is the GpsService. Since the gps module can take up to 30 seconds to get a satellite connection all the other services are started after this (ublox 2020, 6).

Once the services are started a createService() function of BluetoothService is called. This function is only called once every startup and is used to initialize the BL654's Bluetooth radio and to populate its GATT table with a custom Bluetooth service.

After successful initialization of all services the access point waits for incoming Bluetooth messages. When the access point receives an incoming connection the Bluetooth service starts a kick timer. This kick timer is used to throw out clients that take too long to send their data. The kick timer is started when the service receives a AT message beginning with the word "connect" and is cleared when the service receives a message with "discon" word. Once a client tag has connected to the access point it enables notifications to be received from the access point then writes its ID and current GPS boundary to characteristics on the BL654 Bluetooth service. After each client write the access point parses the incoming data and calls RecorderServices addRecord() method which is used to build and populate string arrays that are used to store the communication data. When the access point receives the GPS boundary data it compares the coordinates with its current location and uses a Bluetooth notification to inform the client if it is in its allowed area. If the GPS coordinates received from the client are "0A0A" then the access point sends back its own coordinates. "0A0A" message is used to symbolise "request new coordinates" message.

At certain intervals the number of records in RecorderService is checked and if the number is larger than 0 the records are retrieved from the recorder and passed to UpdaterService. UpdaterService is split to two different devices. The JavaScript side on Raspberry Pi is responsible for keeping the serial communication with MKR1300 open and for writing records to it when update is called.

The code running on MKR1300 is made using C/C++ and Arduino IDE/VisualCode. The C/C++ code listens the serial port and waits for messages starting with a "RECORDS" tag. Once this message is received the tag is removed and the record data is minimized by removing other than crucial characters. The parsed message is then added to MKR's message array. Length of the message array is polled between certain intervals and if the array contains messages the MKR tries to send them to a LoRa network. If the message sending fails, then the message is not removed from the array.

4.5 Receiver

Receiver in this case is the LoRa network server. This server is hosted by TheThingsNetwork and is only used to verify that a message from client tag successfully reached the internet through the AP.

The gateway and LoRa concentrator used in this case was RHF0M301 by RisingHF. The RHF0M301 is attached to a Raspberry Pi and software by RisingHF is used to transmit/pipe LoRa messages received by the radio to the network server. In a real–world application this gateway could/should be replaced with more powerful variant depending on the use case.

4.6 Power

Current consumption of each module can be retrieved from their datasheets. Absolute maximum current draw values for the components are:

- GPS module: 67mA (U-Blox 2011, 15)
- RPI Zero W: 100–150mA (Raspberry Pi Foundation 2020)
- RPI 3B+: 500mA (Raspberry Pi Foundation 2020)
- BL654: 14.8mA (Laird 2018a, 20)
- MKR1300: ~3–6mA

No documents about the MKR1300 make any mention of its current consumption. The SAMD21 documentation seems to imply a maximum of ~3–6mA current consumption (Microchip Technology Inc 2018, 988-991). This is used as an estimate for MKR1300's power consumption although the real number is likely much higher.

From the individual component current draw values potential maximum values for the tag and access point can be calculated. Since the tag device consists of only Raspberry Pi 3B+ and the BL654 the tag should consume around 514.8mA. The access point consist of GPS, Bluetooth and LoRa module in addition to a Raspberry Pi zero W and based on the datasheet info of each component the device should draw around 231.8+MKRmA. Although the access point has more separate electronic components the large difference in power consumption can be explained by the difference in Raspberry Pi's. According to Raspberry Pi's documentation the Pi 3B+ model consumes over 3 times more power than the Zero (Raspberry Pi Foundation 2020).

4.7 Cost factor

Based on prices listed on Mouser, a large multinational electronics supplier, the price of the tag would be around ~55.07e and the access point would cost around ~82.36e. Cost of the tag could be as low as 0e in terms of electronics if the device already contains a Bluetooth radio and the theft prevention functionality is added through software update.

NEO6M:	21,15e (Mouser Electronics 2020)
BL654:	8,60–15,29e (Mouser Electronics 2020)
RPI Zero:	15,21e (Mouser Electronics 2020)
RPI 3B+:	39,78e (Mouser Electronics 2020)
MKR1300:	37,32e (Mouser Electronics 2020)

Priciest components of the system undoubtedly are the MKR1300 module and Raspberry 3B+. When considering the real world costs the Raspberry 3B+ could be omitted entirely bringing down the costs of already potentially “free” tag. MKR1300's cost is almost equal to Raspberry but similarly to Raspberry the costs of the LoRa module could be brought down ~3–7e per module if different component such as Semtech SX1261IMLTRT is used (Mouser Electronics 2020).

4.8 Tests

Testing was not done on individual software components (Unit Tests) but their functionality was tested during integration and system tests. It can be presumed that if the whole system works as expected so do the individual components of the system.

Access point range tests were made by setting up the tag and the access point with some common settings that affect range. On BL654’s settings list, Tx/Rx power and modulation parameters seemed most integral to range. On AP and tag, Tx/Rx power was set to max (8dbm) and modulation’s value was switched between tests on each device.

When the AP and tag were both configured with modulation of 2MPHY and Tx/Rx power of 0dbm, a line of sight (LOS) range of about 120 to 150 meters was achieved. Another test was done with modulation set to 125KPHY and Tx/Rx power of +8dbm, which achieved a LOS range of 150m with ease. Range was not tested further since the testing area ran out of room. (Factory floor is 150m long). Both tests were done in the Kemppi assembly factory.

Since the previous tests were done in LOS, some tests were also done with obstacles in the way to get a better picture about the real–world performance. A range of about 50–60m was achieved when the line of sight was blocked by walls and storage shelfs.

Access points advertising range was also tested using an app by Nordic Semiconductor called nRF Connect. Using the app, the access point was connectable up to a range of ~100m. However, these results might be misleading since although the access point is capable of Bluetooth 5, the phone(s) used were only capable of Bluetooth 4.2.

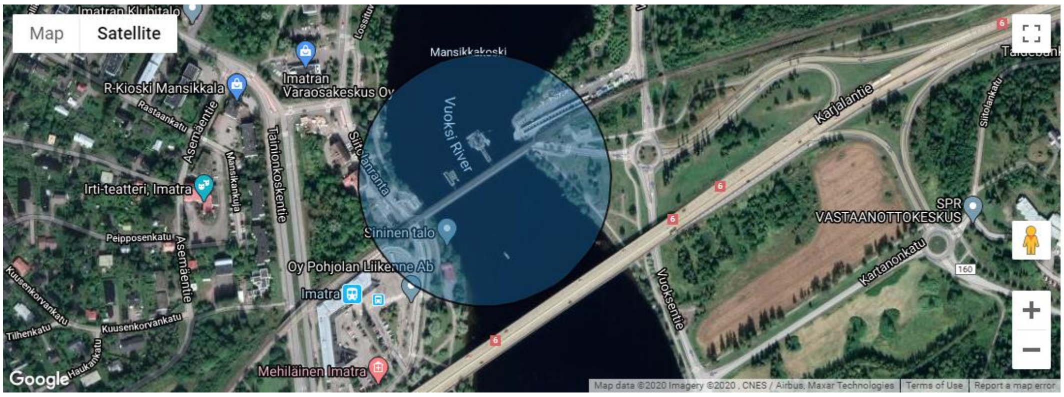


Image 4 – Railway construction site at Imatra (Google Maps, 2020)

As seen from the test results Bluetooth’s range is far from the +1Km that was achieved by Laird (Laird 2019, 10). Regardless of this, the range of 150m is sufficient for the device to operate in real-world use. For example, the railway bridge construction site at Imatra in Image 4 has a length of about 180 meters. This construction site could be potentially covered with just two access point devices. Since a lot of construction sites like the one at Imatra are outdoors, the LOS range can be used to evaluate the potential coverage of access point devices in these situations.

An unforeseen problem was discovered during testing. It was first assumed that if a smart phone is able to get GPS coordinates, in one situation then the NEO6M would be able to do the same. Testing at Kemppi’s cellar proved this assumption wrong. While smart phones were able to get GPS coordinates the NEO6M was unable to receive GPRMC or

GPGGA messages. This might be due to the fact that smart phones are able to utilize their internet connection for better GPS performance. Another reason for this problem could be the fact that the access point filters out any message from NEO6M that is not identified with GPRMC or GPGGA.

During testing, some problems with the MKR1300 were encountered. Problems with the MKR1300 were mainly caused by inconsistent and lacking documentation on LoRa libraries. Some function parameters were not mentioned in the documentation, which caused some confusion.

4.9 Improvements

4.9.1 Remote Configuration

The prototype done in this thesis did not contain any method to set and change the client tag's software configuration other than the initial GPS boundary setup. In order for the prototype to be commercialized and to be used on a larger scale, a system that enables remote and easy access to the client needs to be implemented.

Since the prototype uses BL654 as its Bluetooth module, it is logical to try to take full benefit of all the module's features, one of which is NFC (Near Field Communication). According to the Pew Research Centre, around +60% of the first world's population own a smart phone (Jacob, Caldwell & Hanyu 2018). The number has steadily been increasing and it is estimated that by 2023, 7.33 billion phones will be in use (Statista 2019). In light of these facts it is not unreasonable to assume that NFC could be a natural improvement to the prototype without adding any additional complexity to the end user. Though most users have their personal smart phones or devices provided by their employer, not every smart phone is NFC capable. This could cause problems especially with larger corporations that would potentially need to update their large number of existing smart phones.

Remote configuration could be done through some other method than NFC. Client devices could use a Bluetooth service that would enable remote configuration with only software changes, and an additional button or a GPIO pin event could be used to signal the Bluetooth module to switch to configuration mode. Depending on the actual implementation of the tag, the "main" device could provide the interface and functionality to change the module's settings. For example, if the tag was to be implemented in one of Kemppi's devices with an LCD screen, as seen in Image 10, the configuration interface could be shown as an additional menu on the welder's settings page.

The main purpose of the tag is to prevent theft and hamper attempts at it and thus it is important to keep security in mind when deciding what and how to implement remote configurability. Although Bluetooth has security features such as pin code when pairing, it is hard to control the reach of the wireless signal, therefore giving a potential attacker the opportunity to stay out of sight and remain undetected. Every security and authentication solution has its problems but in Bluetooth these problems seem severe. According to an old research paper done at Tel Aviv University, a 4-digit Bluetooth pin was cracked in less than half a second with an old Pentium III processor (Yaniv & Avishai, 2005). Though the paper is quite outdated since it precedes Bluetooth LE, it raises a good point that is quite relevant today. The paper refers to Bluetooth as short–range technology with a "nominal range of about 10m" and claims the short range is "perceived as a security feature" but this is not true today, especially with Bluetooth LE. If this 10m range is compared with the max range of Bluetooth LE of over 1000m, then the security effect of the short range is effectively void. Regardless of the method ultimately chosen, the security effects need to be taken into a account or else the effectiveness of the whole system is at risk.

4.9.2 Two–Factor authentication

The previously mentioned remote configuration feature could be extended to serve other purposes, some of which could potentially solve the problem of security on the transport (Bluetooth/NFC) layer. Since smart phones are increasingly common and available in work areas, a two–factor authentication system could be implemented with relative ease.

Two-factor authentication can be described as a double log in a system. The first factor in the authentication procedure is a normal password, and the second factor usually a personal secret question, or something physical such as a smart phone with an authenticator app. This type of authentication is already in use in many commonly used gaming apps such as Valve’s Steam and Blizzards Battle.net. Although these features are optional, they have been in use for years, showing that they have a use. A more serious example of two factor authentication is Osuuspankki’s OP–mobiili app. The banking app requires the user to register a mobile device that is then used to receive SMS messages containing keys to the bank’s physical dictionary-like key–code notebook. After the initial setup, the mobile banking app can be used with a meagre 4–digit code. Although the inner workings of the OP–mobiili banking app are unknown, solely the fact that a bank is willing to use mobile verification and a 4–digit code as a means of verification shows that the system can be made secure and easy to use.

A two-factor authentication system could be integrated to any of the multiple mobile apps Kemppi already has in the Google play store. Depending on the app, the features of the authentication and configuration options could differ. Kemppi’s Mobile Maintenance app for example is geared towards technicians and retailers and this app could contain the ability to configure/reconfigure multiple devices at once. This could help equipment rental companies in keeping inventory and quickly reconfiguring returning devices. The WeldEye app on the other hand, is focused towards the end user’s needs. Since the app is already used to configure the machine, additional verification and theft prevention features could potentially be easily tagged on.

The authentication part comes now when the tag, device and smart phone are all connected. Through this bridge the Bluetooth module could ask for license key verification from some secure server, double check its assigned settings and potentially report any anomalies directly back to the internet. This could happen in a case where the module has not managed to connect to AP for verification but then someone connects to the device with a compatible app.

Verifying keys or “calling home” could also provide flexibility in the anti–theft methods used. If unlocking the device (re–enabling functionality) only requires a tap on an app that is already used during work, then the locking window could be reduced significantly without hampering its usability.

4.9.3 Miniaturization

At its current state the prototype is unnecessarily large and clunky. Both the client tag and the access point device could be fitted into a more compact and portable space. Miniaturization in case of the tag would be especially beneficial since its purpose is to be used with small equipment that is often portable.

4.9.4 Access point

The access point consists of three parts, a BL654 Bluetooth module, Raspberry Pi and an MKR1300. While each part serves a specific purpose and the current design could be called modular, the functionality of these three devices could be compressed into only one. Currently the BL654 runs an AT command interface program by Laird written with SmartBasic to handle Bluetooth, MKR1300 uses C/C++ code to communicate with LoRa network, and Raspberry Pi uses JavaScript running in NodeJS to control and pass messages between BL654 and MKR1300. On a larger scale this separation into three devices with three distinct programming languages is detrimental. The end result would be a fractured code base with each part requiring a specific set of skills to maintain and improve. A solution for this problem would be to integrate these devices to a single module or at least to use a unified language like C or C++. This unification could be achieved by using BL654 as a replacement for the Raspberry Pi’s functionality. Since SmartBasic language provides support for common IO and the chip in BL654 contains the same ports (Serial) used by the Raspberry Pi, the BL654 module could be used to handle Raspberry Pi’s current functionality. If in addition to removing the Raspberry Pi, MKR1300 would be replaced with for example the Murata or other LoRa chip, then the BL654 would be able to manage the whole system without the need to split the devices or the code base into parts.

4.9.5 Tag

The tag consists of two devices, Raspberry Pi and BL654 module. Unlike with the access point, Raspberry Pi in the tag device is a placeholder for the actual device that is monitored. With the access point most of the miniaturization comes from combining electronics but with the client tag the possibilities of miniaturization depend on the use case. In devices such as the Minarc welder, computing power is readily available since the device already does much more complex computing than just parsing AT messages and therefore in this use case moving the AT parsing to BL654 would not provide much of an improvement. On the other hand, in a case like an electronic screwdriver or a mobile generator this kind of excess processing power is not available. Thus in a use case like this it would be beneficial to incorporate the Raspberry Pi’s functionality into the BL654 module itself and by doing this the tag could turn into an actual easy-to-place tag depending on the power supply solution.

5 CONCLUSION

In conclusion, the prototype can be considered a success. Although there are inefficiencies in both Bluetooth and LoRa communication, these are problems that can be solved by fine tuning in possible future variations.

The client tag and the device it is connected to can communicate with an access point to exchange data such as GPS coordinates. The tag and the access point are able to communicate, which can help in theft detection and asset recovery.

The mere fact that the tag is able to turn small equipment into IoT devices helps to address the issue of employee theft since they have the knowledge of the system's existence but not how it operates, thus even a prototype device can create a psychological deterrent. Small theft and organized crime are harder to stop but since the tag can potentially brick the device it is attached to, these thieves might not want to waste time stealing something with little to no resale value. In addition, since the access point can potentially detect thefts when they happen, the costs of production downtime can be reduced.

References

Alibaba, 2020. *RFID hf gate reader contactless wireless Gate reader HF RFID gate attendance RFID school attendance.* [Accessed 30 3 2020]. Available at: https://www.alibaba.com/product–detail/RFID–hf–gate–reader–contactless–wireless_60529448561.html

Antto, T. 2015. Stockmann yard – myymäläetsivän muistelmat. Helsinki: Like Kustannus Oy.

Arduino, 2020. *ARDUINO MKR WAN 1300 (LORA CONNECTIVITY).* [Accessed 8 1 2020]. Available at: https://store.arduino.cc/arduino–mkr–wan–1300–lora–connectivity–1414

AUTOALAN KESKUSLIITO RY; TEOLLISUUSLIITTO RY, 2017. *AUTOALAN KAUPAN JA KORJAAMOTOIMINNAN TYÖEHTOSOPIMUS 2017–2020.* [Accessed 15 3 2020]. Available at: http://www.akl.fi/files/5097/AKL–TL_uusi_tes_2017_–_2020.pdf

Bloomberg, 2019. *Semtech and Alibaba Cloud Prevent Asset Loss and Theft with LoRa®–based Tracker.* [Accessed 31 3 2020]. Available at: https://www.bloomberg.com/press–releases/2019–09–18/semtech–and–alibaba–cloud–prevent–asset–loss–and–theft–with–lora–based–tracker

Bluetooth SIG, 2019. [Accessed 12 3 2020]. Available at: https://vtsociety.org/wp–content/uploads/2019/07/Core_v5.1.pdf

Electronics Notes, 2019. *Bluetooth radio interface, modulation, & channels.* [Accessed 3 12 2019]. Available at: https://www.electronics–notes.com/articles/connectivity/bluetooth/radio–interface–modulation–channels.php

Electronics Notes, 2020. *RFID Standards: ISO, IEC, EPCglobal.* [Accessed 2 2 2020]. Available at: https://www.electronics–notes.com/articles/connectivity/rfid–radio–frequency–identification/standards–iec–iso–epcglobal.php

Eric, S. R., 2019. *gitlab.* [Accessed 12 2 2020]. Available at: https://gpsd.gitlab.io/gpsd/NMEA.html

European Rental Association, 2019. [Accessed 21 2 2020]. Available at: https://erarental.org/en/download_file/PublicationDownload/19/era–guide–for–theft–prevention

FabLab_CastelfrancoVeneto, 2019. *MKR WAN 1310 Meets The Things Network!.* [Accessed 28 2 2020]. Available at: https://create.arduino.cc/projecthub/146376/mkr–wan–1310–meets–the–things–network–fff013#toc–first–registration–of–your–mkr–wan–1300–or–mkr–wan–1310–on–ttn–2

Gakstatter, E., 2015. *What Exactly Is GPS NMEA Data?.* [Accessed 30 2 2020]. Available at: https://www.gpsworld.com/what–exactly–is–gps–nmea–data/

Get Connected Blog, 2019. *The Difference Between Classic Bluetooth and Bluetooth Low Energy.* [Accessed 9 12 2019]. Available at: https://blog.nordicsemi.com/getconnected/the–difference–between–classic–bluetooth–and–bluetooth–low–energy

Google Maps, 2020. *Mansikkakosken ratasilta, Imatra.* [Accessed 30 3 2020]. Available at: https://www.google.fi/maps/place/Mansikkakosken+ratasilta/@61.1971771,28.7775461,454m/data=!3m2!1e3!4b1!4m5!3m4!1s0x4690a63e9528f5c9:0xa3b28cd711650533!8m2!3d61.1971745!4d28.7797349

GS1, 2020. *RFID at UFH Regulations.* [Accessed 14 3 2020]. Available at: https://www.gs1.org/docs/epc/uhf_regulations.pdf

Hoffman, C., 2018. *What Is Denuvo, and Why Do Gamers Hate It?.* [Accessed 15 3 2020]. Available at: https://www.howtogeek.com/400126/what–is–denuvo–and–why–do–gamers–hate–it/

Irdeto, 2020. *Denuvo.* [Accessed 15 3 2020]. Available at: https://www.irdeto.com/denuvo

JACK L. HAYES INTERNATION INC, 2019. [Accessed 6 2 2020]. Available at: http://hayesinternational.com/wp–content/uploads/2012/01/31st–Annual–Retail–Theft–Survey–2019–With–Thoughts–Behind–Numbers.pdf

JACOB, P., CALDWELL, B. & HANYU, C. 2018. *Social Media Use Continues to Rise in Developing Countries but Plateaus Across Developed Ones.* [Accessed 10 3 2020]. Available at: https://www.pewresearch.org/global/2018/06/19/social–media–use–continues–to–rise–in–developing–countries–but–plateaus–across–developed–ones/#table

John Morris Group, 2020. *Adam Equipment 8030 Kensington Style Security Combination Lock and Cable.* [Accessed 30 3 2020]. Available at: https://www.johnmorrisgroup.com/AU/Product/51022/Adam–Equipment–8030–Kensington–Style–Security–Combination–Lock–and–Cable

Kemppi, 2020. *Minarc Evo.* [[Accessed 1 4 2020]. Available at: https://www.kemppi.com/fi–FI/tuotteet/family/minarc–evo/

Krasnai, T., 2019. *'Borderlands 3' Set to Launch with Denuvo DRM Software.* [Accessed 15 3 2020]. Available at: https://www.exclusivelygames.com/borderlands–3–set–to–launch–with–denuvo–drm–software/

Laird, 2018a. *BL654 Datasheet.* [Accessed 31 1 2020]. Available at: https://assets.lairdtech.com/home/brandworld/files/BL654%20Datasheet%20v1_1.pdf

Laird, 2018b. *BL65x AT Interface Application User Guide.* [Accessed 1 3 2020]. Available at: https://connectivity–staging.s3.us–east–2.amazonaws.com/s3fs–public/2018–10/BL65x%20AT%20Interface%20Application%20User%20Guide.pdf

Laird, 2019. *Laird Range Testing.* [Accessed 12 2 2020]. Available at: https://connectivity–staging.s3.us–east–2.amazonaws.com/2019–09/CS–AN–RangeTesting–BL654_v1_1_0.pdf

LAIRD, 2020. *BL654–Applications.* [Accessed 2 2 2020]. Available at: https://github.com/LairdCP/BL654–Applications

LoRa Alliance®, 2020. *About LoRa Alliance®.* [Accessed 11 2 2020]. Available at: https://lora–alliance.org/about–lora–alliance

LoRa Alliance, 2015. *What is LoraWAN.* [Accessed 11 2 2020]. Available at: https://lora–alliance.org/sites/default/files/2018–04/what–is–lorawan.pdf

LoRa Alliance, 2018. *LoRaWAN 1.0.3 Specification.* [Accessed 14 2 2020]. Available at: https://lora–alliance.org/sites/default/files/2018–07/lorawan1.0.3.pdf

LoRa Alliance, 2019. *LoRaWAN Regional Parameters.* [Accessed 14 2 2020]. Available at: https://lora–alliance.org/sites/default/files/2020–01/rp_2–1.0.0_final_release.pdf

Microchip Technology Inc., 2018. [Accessed 15 3 2020]. Available at: https://content.arduino.cc/assets/mkr–microchip_samd21_family_full_datasheet–ds40001882d.pdf

Minilex, 2019. *Rikoslaki ja näpistys.* [Accessed 3 12 2019]. Available at: https://www.minilex.fi/a/rikoslaki–ja–n%C3%A4pistys

Mouser Electronics, 2020. [Accessed 14 2 2020]. Available at: https://www.mouser.fi/ProductDetail/Seeed–Studio/102110357?qs=sGAEpiMZZMsG1k5vdNM%2FcwvtHz54rjh9bl2OmNsTQNk%3D

Mouser Electronics, 2020. [Accessed 14 2 2020]. Available at: https://www.mouser.fi/ProductDetail/Raspberry–Pi/RPI3–MODBP–BULK?qs=sGAEpiMZZMve4%2FbfQkoj%252BFahespDt2PCtZmaxsahQ%252Bo%3D

Mouser Electronics, 2020. [Accessed 14 2 2020]. Available at: https://www.mouser.fi/ProductDetail/Arduino/ABX00017?qs=sGAEpiMZZMsau3FfU1KdGGH7zBD1JGe0qxSMiDxGRFmXQZuuc6pd2Q%3D%3D

Mouser Electronics, 2020. [Accessed 14 2 2020]. Available at: https://www.mouser.fi/ProductDetail/Semtech/SX1261IMLTRT?qs=sGAEpiMZZMve4%2FbfQkoj%252BMto6zrE2IyZvKOxHASRdBY%3D

Mouser Electronics, 2020. *Mouser.* [Accessed 14 2 2020]. Available at: https://www.mouser.fi/Search/Refine?Keyword=laird+bl654&Ns=Pricing|0

Mouser Electronics, 2020. *Seeed Studio 113020003.* [Accessed 14 2 2020]. Available at: https://www.mouser.fi/ProductDetail/Seeed–Studio/113020003?qs=sGAEpiMZZMtH%2FBOfAD3t9TlN2a7Hkji4jlsWahiEwIyX8rAr%2FS1nyQ%3D%3D

Murata Investment Co, 2016. *Sub–G Module Data Sheet.* [Accessed 8 1 2020]. Available at: https://wireless.murata.com/datasheet?/RFM/data/type_abz.pdf

NASA, 2019. *What is GPS?.* [Accessed 6 11 2019]. Available at: https://www.nasa.gov/directorates/heo/scan/communications/policy/what_is_gps

National Equipment Register, 2016. *Equipment Theft Report.* [Accessed 11 2 2020]. Available at: http://www.ner.net/wp–content/uploads/2017/10/Annual–Theft–Report–2016.pdf

NMEA, 2018. *NMEA 0183 Standard.* [Accessed 5 1 2020]. Available at: https://www.nmea.org/content/STANDARDS/NMEA_0183_Standard

Node.js, 2020. *Node.js v12.16.1 Documentation.* [Accessed 31 3 2020]. Available at: https://nodejs.org/dist/latest–v12.x/docs/api/worker_threads.html

Nordic Semiconductor, 2020. *nRF52840 Dongle.* [Accessed 8 2 2020]. Available at: https://www.nordicsemi.com/Software–and–tools/Development–Kits/nRF52840–Dongle

Oikeusministeriö, 1990. *Rikoslaki.* [Accessed 3 12 2019]. Available at: https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

ORBCOMM, 2017. *XT 4760 – Datasheet.* [Accessed 21 2 2020]. Available at: https://www.orbcomm.com/PDF/datasheet/xt–4760.pdf

Powerstick, 2020. *Beagle 1.0.* [Accessed 30 3 2020]. Available at: http://powerstick.com/main/beagle/

Ramirent, 2019. *RamiSmart–portaali tuo älyä rakennusaikaiseen olosuhteiden hallintaan.* [Accessed 15 3 2020]. Available at: https://www.ramirent.fi/blogi/ramismart–portaali–tuo–alya–rakennusaikaiseen–olosuhteiden–hallintaan

Raspberry Pi Foundation, 2020. *FAQ.* [Accessed 31 1 2020]. Available at: https://www.raspberrypi.org/documentation/faqs/#pi–power

Raspberry Pi, 2020. [Accessed 31 1 2020].
Available at: https://www.raspberrypi.org/documentation/hardware/raspberrypi/

Reuters, 2015. *Shoplifting, other fraud cost US retailers $44 billion in 2014: Survey.* [Accessed 30 1 2020]. Available at: https://www.cnbc.com/2015/06/24/shoplifting–other–fraud–cost–us–retailers–44–billion–in–2014–survey.html

RFIDHY, 2020. *HF RFID Library Tag.* [Accessed 30 3 2020]. Available at: https://www.rfidhy.com/rfid–products/hf–rfid–library–tag/

Roberti, M., 2014. *Green RFID Tags.* [Accessed 15 10 2019]. Available at: https://www.rfidjournal.com/articles/view?11715

Rosendahl, J., 2019. *Olkiluoto 3:n uusi viive voi maksaa Arevalle.* [Accessed 15 3 2020]. Available at: https://www.kauppalehti.fi/uutiset/olkiluoto–3n–uusi–viive–voi–maksaa–arevalle/a55ea144–7c8c–4a5b–b605–d6e75efa9cba

SkyRFID, 2020. *RFID Range.* [Accessed 2 2 2020]. Available at: https://skyrfid.com/RFID_Range.php

Speights, D., Downs, D. & Raz, A., 2018. Essentials of modelling and analytics Retail Risk Management and Asset Protection. In: *Essentials of modelling and analytics Retail Risk Management and Asset Protection.* New York: Routledge, p. 31.

Statista, 2019. *Forecast number of mobile users worldwide from 2019 to 2023.* [Accessed 10 3 2020]. Available at:

https://www.statista.com/statistics/218984/number–of–global–mobile–users–since–2010/

Suomen virallinen tilasto (SVT), 2019. *Rikos– ja pakkokeinotilasto.* [Accessed 29 11 2019]. Available at: https://www.stat.fi/til/rpk/2019/03/rpk_2019_03_2019–10–17_tie_001_fi.html

Techopedia, 2020. *Bricking.* [Accessed 3 1 2020]. Available at: https://www.techopedia.com/definition/24221/bricking

The Equipment Register, 2017. *Loss Prevention and Security Techniques for Equipment Owners & Hirers.* [Accessed 11 2 2020]. Available at: https://www.ter–europe.org/wp–content/uploads/2017/04/TER–Loss–Prevention–Security–Techniques–Mar–17.pdf

Tilastokeskus, 2019. *Rikos– ja pakkokeinotilasto.* [Accessed 30 3 2020]. Available at: http://pxnet2.stat.fi/PXWeb/pxweb/fi/StatFin/StatFin__oik__rpk__tiet/statfin_rpk_pxt_11ce.px/table/tableViewLayout1/?loadedQueryId=335f44a5–8173–49b3–ae57–49ac6c30a6a2&timeType=from&timeValue=2016

Torvmark, K., 2014. *Three flavors of Bluetooth: Which one to choose?.* [Accessed 9 12 2019]. Available at: http://www.ti.com/lit/wp/swry007/swry007.pdf

U–Blox, 2011. *NEO–6 u–blox 6 GPS Modules.* [Accessed 12 2 2020]. Available at: https://www.u–blox.com/sites/default/files/products/documents/NEO–6_DataSheet_%28GPS.G6–HW–09005%29.pdf

ublox, 2020. *NEO–6 u–blox 6 GPS Modules Datasheet.* [Accessed 12 2 2020]. Available at: https://www.u–blox.com/sites/default/files/products/documents/NEO–6_DataSheet_%28GPS.G6–HW–09005%29.pdf

VALTIOVARAINMINISTERIÖ, 2013. *VAHTI 2/2013 Toimitilojen tietoturvaohje.* [Accessed 6 11 2019]. Available at: https://www.vahtiohje.fi/web/guest/vahti–2/2013

Voipio, V., 2019. *Plastic RFID Tags Could Soon Be History.* [Accessed 15 10 2019]. Available at: https://www.storaenso.com/en/inspiration–centre/renewable–future–blog/2019/6/plastic–rfid–tags–could–soon–be–history

Womack, S., 2018. *Are Retailers Selling Shoplifting Tools?.* [Accessed 14 3 2020]. Available at: https://losspreventionmedia.com/are–retailers–selling–shoplifting–tools/

Woolley, M., 2019. *Bluetooth Core Specification v5.1 Feature Overview.* [Accessed 8 12 2019]. Available at: https://3pl46c46ctx02p7rzdsvsg21–wpengine.netdna–ssl.com/wp–content/uploads/2019/03/1901_Feature_Overview_Brief_FINAL.pdf

Yaniv, S. & Avishai, W., 2005. *Cracking the Bluetooth PIN.* [Accessed 10 3 2020]. Available at: http://www.eng.tau.ac.il/~yash/shaked–wool–mobisys05/

ATTACHMENTS