CRANFIELD UNIVERSITY

STEFANO TEDESCHI

A SYSTEMATIC DESIGN APPROACH TO IOT SECURITY FOR LEGACY PRODUCTION MACHINERY

SCHOOL OF AEROSPACE, TRANSPORT AND MANUFACTURING
Manufacturing Department

PhD
Academic Year: 2014 - 2020

Supervisor: Dr. Christos Emmanouilidis
Associate Supervisor: Prof. Konstantinos Salonitis
Prof. Jörn Mehnen
March 2020

CRANFIELD UNIVERSITY

SCHOOL OF AEROSPACE, TRANSPORT AND MANUFACTURING

PhD

Academic Year 2014 - 2020

STEFANO TEDESCHI

A SYSTEMATIC DESIGN APPROACH TO IOT SECURITY FOR LEGACY PRODUCTION MACHINERY

Supervisor: Dr. Christos Emmanouilidis
Associate Supervisors: Prof. Konstantinos Salonitis
Prof. Jörn Mehnen
March 2020

This thesis is submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

ABSTRACT

The Internet of Things (IoT) is an emerging topic of rapidly growing technical importance for the industry. The aim is to connect objects with unique identifiers and combine them with internet connectivity for data transfer. This advanced connectivity has significant potential in the workshop-level upgrade of existing legacy equipment to unlock new features and economic benefits especially for monitoring and control applications However, the introduction of the Industrial Internet of Things (IIoT) brings new additional security and integrity risks for the industrial environment in the form of network, communication, software and hardware security risks. This thesis addresses such fundamental new risks at their root by introducing a novel approach for IoT-enabled monitoring of legacy production machinery, which consist of five stages, incorporating security by design features. The first two phases of this novel approach aim to analyse current monitoring practices and security and vulnerability issues related to the application domain. The proposed approach applies three more stages which make the domain-relevant analysis to become application specific. These include a detailed model of the application context on legacy production machinery monitoring, together with its interfaces and functionality, implementing threat mitigations combined with a new modular IoT DAQ unit mechanism, validated by functional tests against Denial of Service (DoS) and clone attacks. Thus, to be effective, the design approach is further developed with application-specific functionality. This research demonstrates an instance of this innovative risk-averse design thinking through introducing an IoT device design which is applicable to a wide set of industrial scenarios. A practical showcase example of a specific implementation of the generic IoT design is given through a concrete industrial application that upgrades existing legacy machine tool equipment.

The reported work establishes a novel viewpoint for the understanding of IoT security risks and their consequent mitigation, opening a new space of risk-averse designs that can bring significant confidence in data, safety, and security of IoT-enabled industry.

Keywords:

Internet of Things (IoT); Industrial IoT devices; Cyber security; Threat models; Smart manufacturing; Industrial monitoring and control systems

ACKNOWLEDGEMENTS

I would like to express my gratitude to Dr. Christos Emmanouilidis, Prof. Konstantinos Salonitis, Prof. Jörn Mehnen and Prof. Rajkumar Roy my research supervisors. Their support, encouragement and advice provided me a constant source of motivation, insight and inspiration.

I am thankful to my sponsor the Kennametal for funding my research through and to Mitch Benko for supporting by expertise and knowledges useful at the scope of this research.

My greatest thanks to my parents Mr and Mrs Tedeschi, who I dedicate this Thesis. I also say thanks to my partner for supporting during this period and finally to all persons which I have met.

Above all, I give thanks to the God for making this come true.

LIST OF PUBBLICATIONS

1) Tedeschi S., Emmanouilidis C., Mehnen J., Roy R., (**2019**) A Design Approach to IoT Endpoint Security for Production Machinery Monitoring. Sensors, *19*(10), 2355; doi://doi.org/10.3390/s19102355
2) Tedeschi S., Rodrigues D.P., Emmanouilidis C., Erkoyuncu J.A., Roy R., Starr, A. (**2018**) A cost estimation approach for legacy systems in smart manufacturing implementation. Proceedings of the 6th International Conference on Through-life Engineering Services, *19*, , pp. 103- 110, doi: doi.org/10.1016/j.promfg.2018.01.015
3) Tedeschi S., Mehnen J., Tapoglou N., Roy R. (**2017**). Secure IoT Devices for the Maintenance of Machine Tools. Proceedings of the 5th International Conference on Through-life Engineering Services, *Procedia CIRP **,** 59,* pp. 150-155, doi:10.1016/j.procir.2016.10.002
4) Tedeschi S., Mehnen J., Roy R. (**2017**). IoT Security Hardware Framework for Remote Maintenance of Legacy Machine Tools. The Second International Conference on Internet of Things, Data and Cloud Computing (ICC’17), article No. 43, Cambridge, March 22-23, 2017, doi: 10.1145/3018896.3018938
5) Tedeschi S., Emmanouilidis C., Farnsworth M., Mehnen J., Roy R. (**2017**) New threats for old manufacturing problems: secure IoT-enable monitoring of legacy production machinery. APMS 2017 International Conference Advances in Production Management Systems, *513*, 2018, pp. 391-398, doi: //doi.org/10.1007/978-3-319-66923-6_46
6) Mehnen J., He H., Tedeschi S., Tapoglou N. (**2017**). Practical Security Aspects of the Internet of Things. Cyber security for Industry 4.0, pp.225-242, doi:10.1007/978-3-319-50660-9_9
7) Tedeschi S., Mehnen J., Tapoglou N., Roy R. (**2015**). Security Aspects in Cloud Based Condition Monitoring of Machine Tools. Proceedings of the 4th International Conference on Through-life Engineering Services, *Procedia CIRP 38* pp.47-52, doi:10.1016/j.procir.2015.07.046

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
API	Application Programming Interface
CBM	Condition-Based Maintenance
CM	Condition Monitoring
CNC	Computer Numerical Control
CPS	Cyber Physical Systems
CPPS	Cyber Physical Production Systems
CPU	Central Processing Unit
CoAP	Constrained Application Protocol
DAQ	Data Acquisition
DFD	Data Flow Diagram
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
FMEA	Failure Mode and Effects Analysis
HMI	Human Machine Interface
ICS	Industrial Control Systems
IR	InfraRed
IT	Information Technology
IoT	Internet of Things
MAC	Medium Access Control
MITM	Man-in-the-Middle
MS	Millisecond
LCCA	Log identity, Communication, Connection, Authentication
LPLA	Low Power Local Area
LPWA	Low Power Wide Area
OT	Operational Technology

OS	Operating System
OSCORE	Object Security for Constrained RESTful Environments
P2P	Peer-to-Peer
PAC	Programmable Automation Controller
PGP	Pretty Good Privacy
PLC	Programmable Logic Controller
PLM	Product Lifecycle Management
RF	Radio Frequency
RMS	Remote Monitoring System
SCADA	Supervisory Control and Data Acquisition
SCU	System Control Unit
SME	Small Medium Enterprise
SQL	Structured Query Language
WSN	Wireless Sensor Network
GDPR	General Data Protection Regulation
DNS	Domain Name System
PIN	Personal Identification Number

1 INTRODUCTION

Currently, the global machine tool industry is increasing the demand for continuous requests for customised products in various industrial sectors. As reported by Oxford Economics [1], the global machine tool market, driven by technological advances and the development of machine tools that offer unprecedented versatility and productivity, is expected to reach to over $99bn by 2022. Such a market growth will be facing the fact that manufacturing enterprises exert a strong hold on the economic growth of developed and developing nations alike. The reasons for such a demand of machine tools depends on significant benefits for the enterprise such as high process automation, high accuracy, excellent surface finish, and flexibility of operations connected with a low cost of the whole manufacturing process. However, to be competitive, manufacturing companies require that the machine tool can combine high-quality products in short time with an extremely low number of defects and operates as long as possible, avoiding prolonged shutdowns that would damage the company's profit [2].

Internet of Things (IoT) is a new technology which provides support in connecting machine equipment, devices and resources through different communication protocols [3]. This technology promotes the digitalisation revolution called Industry 4.0 [4], which combines consumer and advantages in an innovative reality in which processes, products, people and places are connected and data are acquired, traced, shared, combined, extracted and analysed for enabling better decision making. Smart Monitoring and Controls are some of the features which IoT may offer to the manufacturing sector for improving the value and quality of processes and products. With monitoring, objects act as sensors to produce information about themselves or their surroundings, while control allows remote control of objects. Also, this advanced connectivity, which includes data collection, data communication, and advanced analytics can support Enterprise Resource Planning (ERP) for maintenance resources operations [5]. While large companies are networked-based and more likely to deploy IoT network technology, Small-Medium Enterprises (SMEs) remain relatively reluctant to integrate such advanced connectivity and non-networked [6]. Therefore, the lack of resources and methodical approaches make it difficult to upgrade IT systems. Also, interconnecting machinery introduces security threats related to everything that interfaces with them. Solutions based on IoT connectivity can upgrade the data-generation and integration capabilities of a production system, but at the same time underlying potential security and privacy vulnerabilities and risks for the manufacturing process which make the enterprise more susceptible to attacks [7]. In addition, SMEs need to update their facilities and infrastructures to comply with standards and regulations and take advantage of IoT technology.

In this context, special attention is given to legacy machine tools which are not equipped with the latest connectivity technology and are usually not effective in terms of life-cycle duration and operational performance. Computer Numeric Control (CNC) machine tools remain constrained within the standardised CNC programming data exchanges further limited by a lack of versatile open Application Programming Interface (API), [8]. This makes it difficult to monitor systems easily, due to the lack of sensors and integrated devices capable of acquiring process data [9]. IoT technology may improve legacy production systems in order to achieve higher productivity and reduce machine breakdowns. This technology may support the integration of additional sensors required by the manufacturer or the customer for direct or indirect monitoring into a networked factory environment [10], for example for assessing the energy usage and machining parameters using power signals analysis [11], which allow optimising machine usage and maintenance actions. However, the implementation of new hardware and software at the workshop level (e.g. intelligent sensors, communication protocols, cloud computing, etc.), requires updating the corporate IT infrastructure [12].

IoT technology has started to be implemented into different industry sectors, while security and privacy challenges are increasingly highlighted as major sources of risks [13] [13] [14]. There are numerous reports of breaching basic security, for example through signal replaying or permitting the cloning of tags [15] [16].

Through these flaws, attackers are able to obtain access to services, facilities and critical data. Information can often be indirectly extracted from the hardware, software and network components, as some IoT systems may be susceptible to reverse engineering [17]. To prevent such an attacks, common defence techniques include cryptography [18], secure authentication protocols [19] improved resistance to cloning [20], and automatic malware detection [21]. Nevertheless, such countermeasures are not included by design in typical IoT devices.

Open CNC machines use communication capabilities over standard network protocols and provide APIs to access data by third-party applications [22] [23]. Numerical control machines are susceptible to attack against access to real-time machine data, modification of machining software or machine codes, tampering with production machinery, Denial of Service (DoS) attack, cloning devices and reverse engineering process.

While security management has received widespread attention in the field of information technology, functional security within production environment requires further attention. Various security approaches have been proposed but for a comprehensive handling of design for security, the application context is always of paramount importance. As a result, a typical handling of any design for security would start from the targeted system. Within such a viewpoint, a staged approach would start from application modelling, advance threat identification and analysis, and then progress to threat mitigation and validation [24] [25].

Despite substantial research in this field, it is still common to encounter a significant number of applications and research outputs targeting the introduction of IoT in manufacturing and addressing the upgrade of legacy production equipment, without due consideration for security management. This Thesis addresses this gap by establishing a novel viewpoint for the understanding of IoT endpoint security risks and their consequent mitigations for legacy production machinery. Also, it opens a new space of risk-averse designs that can improve trust in the integrity of data and processes in IoT-enabled industrial environments. Finally, it presents a design approach that includes five key phases.

This chapter consists of sections of which Section 1.1 aims at the background of the research and Section 1.2 focuses on the motivation of the research for the design a systematic approach for IoT-enabled remote monitoring for legacy production machine. In Section 1.3 the purpose and objectives of this research thesis are presented, and Section 1.4 is the contribution to knowledge, while Section 1.5 defines the research scope for this Thesis project. Finally, Section 1.6 provides a summary of the entire structure of the Thesis document.

1.1 Research Background

Manufacturing companies typically aim to deliver high quality products without the presence of defects and flaws.

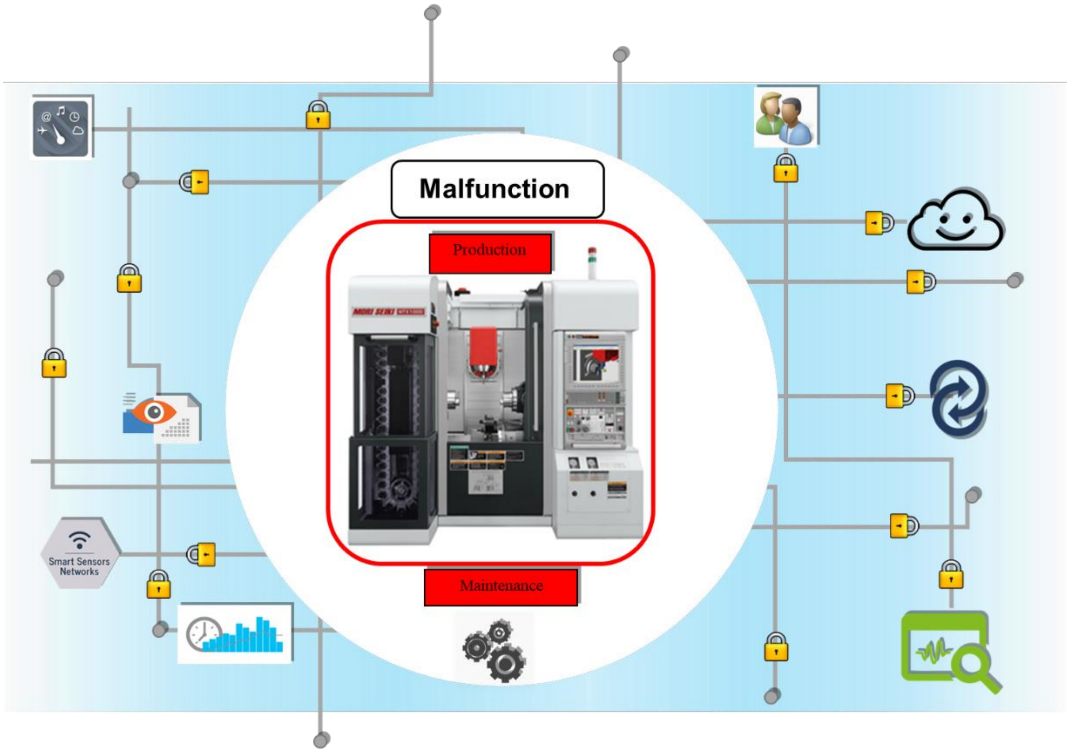


Figure 1: IoT integration with legacy production machinery

At the same time, it is important to make sure that production machines operate for a period of time without breakdowns and errors, which may contribute to compromising the product quality and competitiveness on the market, as well as a loss of money and time for the enterprise. Today, many manufacturing SMEs are equipped with legacy systems which are not effective in terms of life cycle and operational performance. These legacy systems, are natively lacking of external communication capabilities and often an API that could provide real-time machining data [11]. At the shop floor level, in the case of machine malfunctions, the manufacturer must shut down the machine for an appropriate period of time for the maintenance team to repair. This can sometimes mean a long delay before the machine returns to operational status. IoT may help to boost quality, identify problems before they occur and schedule the appropriate repair at the most efficient time (Figure 1). This in turn will also help to reduce raw material waste, improve equipment uptime and allow precise and more automatic production adjustments. All these opportunities contribute to a better control on the shop floor improving the efficiency of legacy systems and reducing the breakdown. Also, IoT data may support ERPs for improving data availability and communication throughout the enterprise and assist in making more informed decisions. Nevertheless, enterprises need to reconfigure the current Information Technology (IT) layer and include IoT, which will lead to better capabilities such as control, communication, and monitoring assets for industries.

At the same time, it creates new challenges and vulnerabilities, which has never been addressed before. Such new challenges are [26]:

- insecure web interfaces, that could lead to compromised devices along with compromised customers;
- insufficient authentication/authorisation, which can impact a business user accounts, and private data which may be modified, or deleted;
- insecure network services, which can generate an impact on devices which have been rendered useless from a network attack such as denial of service (DoS) attacks or allow the device to be used to facilitate attacks against other devices and networks;
- the privacy concern of personal data that is collected unnecessarily or is not protected properly;

- insecure cloud platform for managing data which could be modified and controlled;
- insufficient security configurability by anyone who has access to the device and the data could be stolen or modified;
- insecure software/firmware have effect on the business if data can be manipulated or modified and devices taken control of for the purpose of attacking other devices;
- poor physical security, where the data could be manipulated or modified, and the device under control for purposes other than what was originally intended.

These are some of the main challenges that appear as access points to network attacks. Therefore, vulnerabilities should be considered in the design phase of any IoT device for learning and developing security approaches ready to be implemented in the manufacturing sectors.

1.2 Research Motivation

A large number of sensors / devices in the workshop could generate a quantity of data that could easily be collected and analysed through IoT technology. Consequently, the increase in Internet use means that the hard borders of companies are disappearing and risks and vulnerabilities are growing [27]. In this context, cyber security has become a critical challenge for advanced manufacturing systems, which could be threatened by a wide range of cyberattacks from hacktivists. A major feature of an advanced manufacturing system is the capability of the supply to be connected to the manufacturing process at anytime and from anywhere. In this way, suppliers will have visibility and proactive supply to the production chain [28].

The IoT is where internet meets the physical world but generates security implications because the vulnerabilities move from the manipulating information to controlling the actuation. Consequently, the range of vulnerabilities expands drastically from known threats and devices of older control system to additional security threats of new devices, protocols, and workflow. As a result, companies move from closed system (e.g. SCADA) to IP-based Cyber Physical Systems [29]. Cyber security risks are linked to the traditional Industrial Control Systems (ICS) due to legacy equipment and not well equipped against modern networked environments [30]. This is because the components of a traditional ICS are communicated through specific protocols often without any security concern, which opens such control system to internetworked connectivity risks and vulnerabilities. Therefore, a key challenge aims to protect legitimate ICS from attacks when they are connected to the internet. Typically, cyber security threats are not acceptable and need to be "designed out" right at the initial IoT system setup stage.

This research offers the contributes to support and address some gaps by developing a security approach for a systematic security methodology applicable when introducing IoT for monitoring legacy production machinery in industrial environments. New security approaches and models are needed for addressing such vulnerabilities and threats.

1.3 Research aim & objectives

This research aims to develop a novel methodology to systematically design and integrate IoT data acquisition hardware and software unit with security provisions for remote monitoring of legacy production machinery.

The objectives for achieving the aim are:

1. Critically analyse current academic literature and industry practice to establish the research baseline and clarify research gaps.
2. Design a new approach for IoT-enabled monitoring of legacy production machinery with security provisions right from the design phase.
3. Apply the security design approach and demonstrate its feasibility through a prototype implementation of IoT-enabled data acquisition unit for production machinery monitoring.
4. Test and evaluate the approach on the pilot implementation to address selected key threats.

1.4 Research contributions

To address such needs this research has identified three main topics as a contribution to design a systematic approach for IoT-enabled monitoring of legacy production machines.

1. A new security design thinking approach for IoT-enabled legacy manufacturing machinery that includes five key stages.
2. A new authentication protocol that effectively implements the isolation principle applied at the IoT endpoint subsystem level with real-time functionality.
3. The proposed novel systematic approach can be applied to assess risks and vulnerabilities related for monitoring industrial production environments.

1.5 Research scope

In order to cover the purpose and objectives, the aim of this research is the study of a methodology for the efficient integration of IoT technology in the legacy production environment. Due to the existence of different implementation methodologies, the study would be limited to the security aspect for such implementation. Based on this, an identification of threats taxonomy and attack tree classification has considered. The success of this study was measured by testing and validation of an IoT device prototype for a legacy machine tool.

1.6 Thesis document structure

This section provides a description of the Thesis structure to give an overview of the entire thesis. The structure of the Thesis is designed to show the progression of the research from the research motivation, aims and objectives to the findings of the Thesis, the validations and conclusions. Chapter 1 introduces the research, its motivation that leads to the research aim and objectives. Chapter 2 provides a review of the literature in the domain area of the research topic. The review identifies gaps in the research study domain and the potential contributions to these areas. Chapter 3 provides a restatement of the research aim and objectives. The general research methodology adopted to achieve the research objectives are presented in this chapter. Chapter 4 discusses in detail the novelty design thinking approach proposed for this research. Chapter 5 presents the application model and data interface related such as a characterisation of the case study. It also presents the attack tree for the three main attack goals. Chapter 6 presents a novel modular IoT DAQ unit and the authentication protocols used for managing the IoT DAQ unit. Chapter 7 is offering the implementation of the modular IoT DAQ unit against DoS and cloning attacks. Chapter 8 concludes the research by providing a discussion of the research contributions, its limitations and finally future research directions.

2 LITERATURE REVIEW

Industry 4.0 is adding value for the manufacturing environments, bringing together Internet of Things (IoT), Machine-to-Machine (M2M) communication, Cyber Physical Systems (CPS), and contribute to supervisory and control operations for industrial monitoring systems. IoT technology has impact especially in terms of data capture and data sharing, by connecting machines, devices and resources. While it is very well suited for the new generation of CNC production machinery, the capability to improve the legacy production machinery has yet to be sufficiently addressed in the literature.

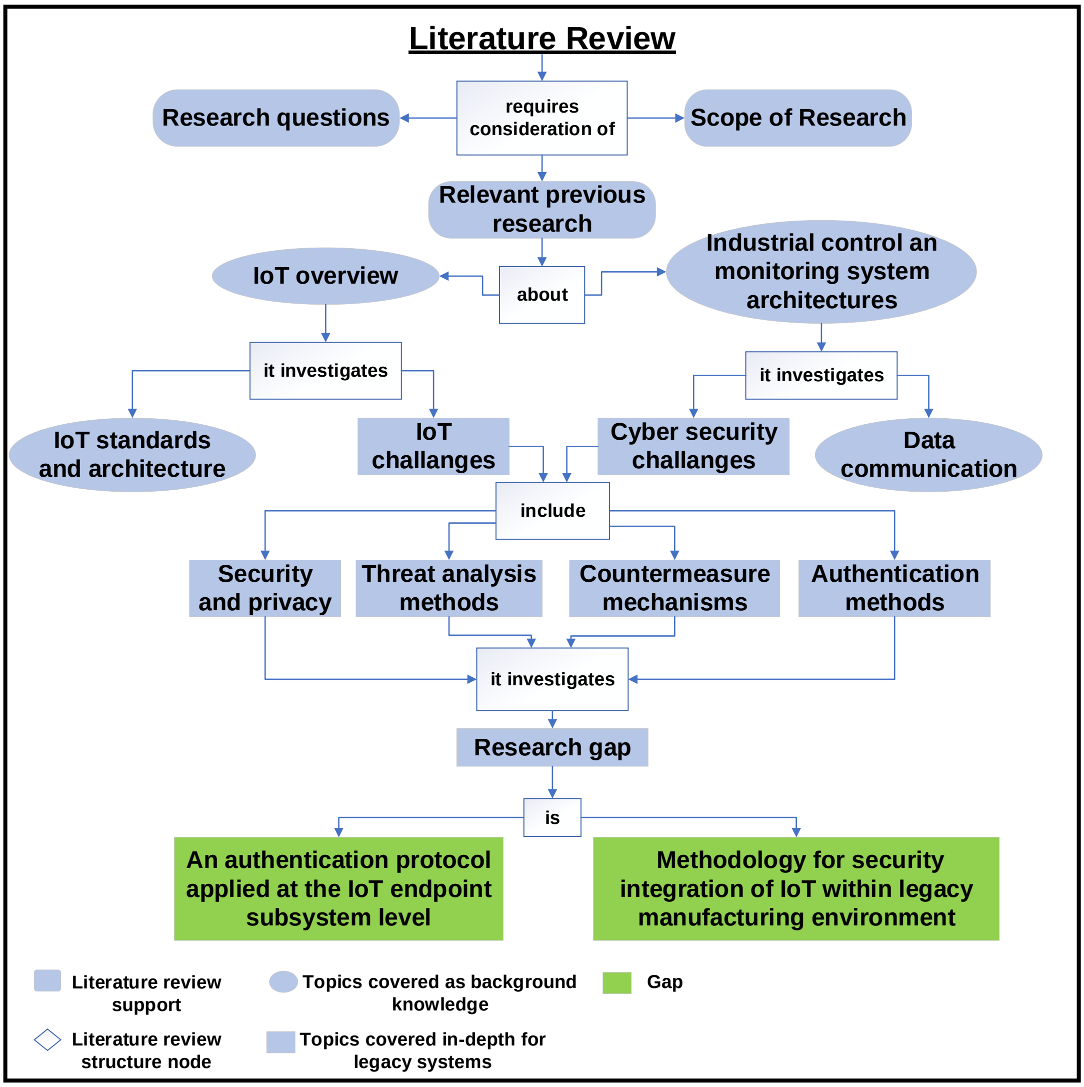

Literature Review
Research questions
requires consideration of
Scope of Research
Relevant previous research
IoT overview
about
Industrial control an monitoring system architectures
it investigates
it investigates
IoT standards and architecture
IoT challanges
Cyber security challanges
Data communication
include
Security and privacy
Threat analysis methods
Countermeasure mechanisms
Authentication methods
it investigates
Research gap
is
An authentication protocol applied at the IoT endpoint subsystem level
Methodology for security integration of IoT within legacy manufacturing environment
Literature review support
Topics covered as background knowledge
Gap
Literature review structure node
Topics covered in-depth for legacy systems

Figure 2: Literature review topics connection overview

Legacy production machines are often not well-equipped with modern communication technologies and consequently isolated due the lack of open APIs which makes it difficult to monitor and control the entire production process [11]. In addition, legacy production machines which are already equipped with a number of diagnostic services could be provided with supplementary sensors required by the end-user or the machine manufacturer for direct or indirect monitoring operations [9]. Although, IoT facilitates the implementation of new monitoring and control for legacy manufacturing industries, the security aspect related to approaches and mechanisms for the integration around legacy machines is not sufficiently covered in the literature. For this purpose, the chapter aim to identify which aspects have been covered in the literature that are dealing with the security integration of IoT technology within the manufacturing industry.

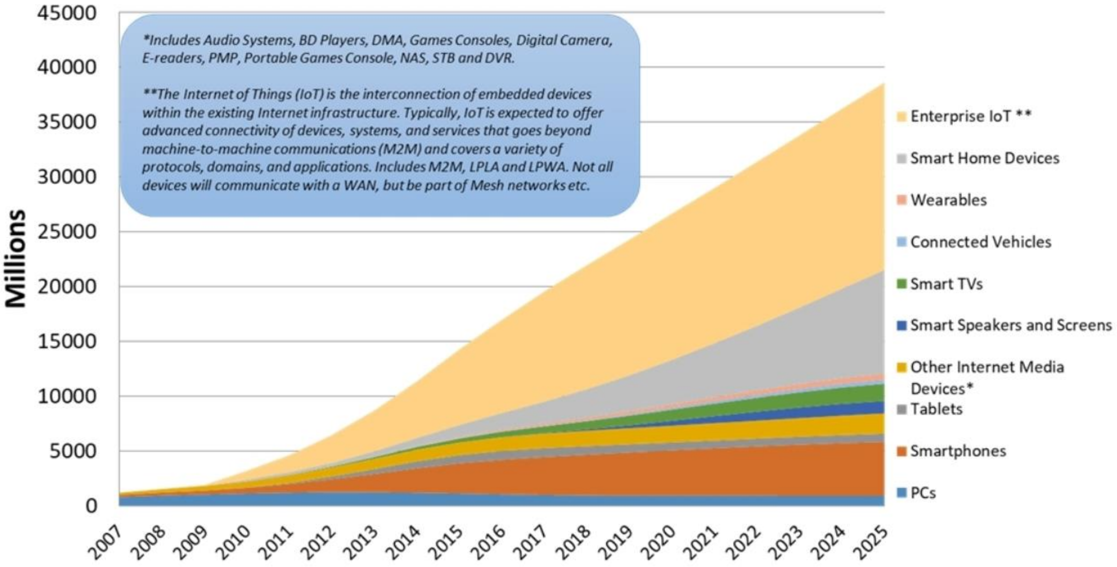
The methodology used for selecting the literature review is to capture the main keywords within the research aim, objectives and questions that were introduced in the previous chapter. The keywords were selected by designing a relevant tree, as shown in Figure 2. The first step was to identify the key thematic areas to start the search for keywords in literature such as IoT and industrial control and monitoring systems. These two key thematic areas have been further divided into relevant sub-areas. Some of these are for basic topics and to gather knowledge in the area, while others are for in-depth topics to form part of the core literature review. The relevant tree provided a useful method for structuring the literature search and ensured that all relevant parts of the literature had been thoroughly explored. Secondly, keywords such as, IoT security and privacy, threat analysis methods, countermeasure mechanisms and authentication mechanisms were searched using the digital library tool database (Scopus, Google Scholar, IEEEXplore, etc.), which identified a list of key authors, journals and research papers within the scope. The scope is to clearly define the risks and challenges of IoT-enabled for legacy production machines, particularly in the case of monitoring and control applications. This challenge for the purpose of this research concerns the security and authentication mechanisms to obtain access to IoT devices for monitoring operations. In addition, current architectures of industrial control and monitoring systems require further investigation of the application context as a way to identify possible attack endpoints. For this reason, an analysis of the current threat method identification methodologies is introduced. Industries connected-based require techniques for secure data protection and secure communication mechanisms, which may be achieved by threat analysis and methods. At the same time, therefore, this critical review is focussed on security incidents, risks and vulnerabilities for the manufacturing industry, and relative countermeasure mechanisms. An overview of the fundamentals and state-of-the-art is also provided to identify the baseline of the research and research gaps.

The structure of the chapter is divided into several sections covering, industrial control and monitoring systems, cyber security threats, and security approaches and techniques. In Section 2.1 an overview of the IoT technology, architecture and challenges with regards to security is presented. In Section 2.2 a critical review of security challenges is introduced for industries connected-based, while Section 2.3 is focused on security challenges for industrial monitoring and control operations. Section 2.4 covers the analysis of threats for the manufacturing industry, while Section 2.5 provides an overview of the common countermeasure mechanisms against attack entry-points. Section 2.6 compare threat modelling methodologies, while Section 2.7 introduces the gaps identified. Finally, Section 2.8 introduces a summary of the main points to conclude the chapter.

2.1 Internet of Things (IoT)

Internet of Things (IoT) is the biggest digital revolution introduced into the global network within the last few years, and refers to a system of interconnected computational devices (things), identifiable and able to transfer data over a network [31]. The concept of things can in practice be referred to any object capable of being identified, through the possession of an IP address, and capable of data transfer. For example, for supporting monitoring operations [32] [33], Machine-to-Machine interaction (M2M) between objects that have never had a computational capacity (electrical systems, production machines, refrigerators, clocks, washing machines, engines, etc.).

IoT has had an historical journey that starts from ArpaNet (1969) [34], which was the first computer network for military use in the Cold War, to the invention of the TCP/IP stack (1974) and the subsequent Domain Name System (DNS) (1989), passing through the invention of the World Wide Web (1989). The first time that the expression "Internet of Things (IoT)" was used was 1999, term coined by researcher Kevin Ashton, and it is precisely in these years that the set of concepts and ideas for IoT solutions were put together to prepare for the innovation that would upset the next decades of the computing world.



*Includes Audio Systems, BD Players, DMA, Games Consoles, Digital Camera, E-readers, PMP, Portable Games Console, NAS, STB and DVR.

**The Internet of Things (IoT) is the interconnection of embedded devices within the existing Internet infrastructure. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. Includes M2M, LPLA and LPWA. Not all devices will communicate with a WAN, but be part of Mesh networks etc.

Figure 3: Global Connected IoT Device Installed Base Forecast [35]

According to a recent forecast, the IoT market in the global world alone should reach 38.6 billion of installed devices by 2025, and over 50 billion by 2030 [35] [36]. Enterprise IoT is a promising sector for the implementation of IoT technology (Figure 3) [35].

Initially, the IoT was focused on optimising operational efficiency, automation and maintenance, instead today offers opportunities to improve productivity, create new businesses, reduce downtime, maximise the use of resources and the life cycle costs of resources for smart industry sectors.

This advanced connectivity aims to create endpoints on the network for interacting with people, machines and things, where industrial applications can handle the amount of information produced by devices for providing services to the customers.

The application scenarios for this technology are multiple [37] [38], but mainly focus on the manufacturing sectors. The main sectors benefiting from the IoT can be grouped into 4 macro topics: "Smart Cities", "Industrial IoT", "Smart Health" and "Smart Homes" which represent the best opportunities in terms of IoT investment [40], as shown in Figure 4.

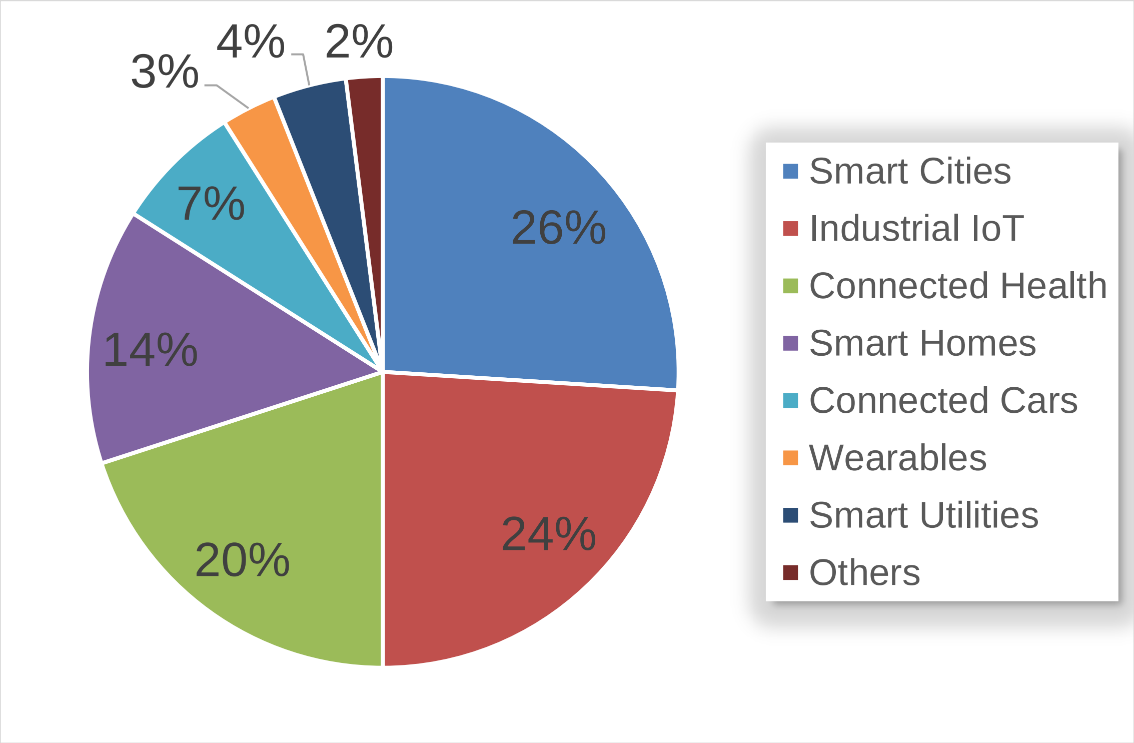


Figure 4: Global IoT market by relative size of IoT spending [39]

IoT is linking the physical and the digital world, including collecting, analysing and evaluating data and information for business decision support. Such a technology requires to be studied at the architecture level for a better understanding of interaction and integration capabilities with the different industrial environments monitoring systems.

In the past, data came mainly from data-centre servers located largely in the centre of the network, to users on the edge of the network. In today's internet, data is mainly produced at the edge of the network by IoT devices, smart/autonomous vehicles, wearable devices, sensors and the like, then processed on the data centre server. This data will be of enormous volume, but also of significant value. The IoT traffic to cloud-computing servers will grow 12-fold from 2018 to 2022 [40]. More than 40% of the IoT market will be services that will be offloading data from IoT devices to the cloud for enhanced processing [41] to which includes security and non-security related operations. The sheer volume of the market shows the opportunity, as well as the importance of ensuring secure uninterrupted operations.

Privacy and security of IoT data is therefore, becoming extremely important. The current Internet infrastructure is not ready to host large volumes of data from the edge. Therefore, it makes it difficult for the current model to send everything back to the cloud for processing because it simply cannot cope with the wave of data coming from the edge. Reports have shown that by 2026, there will be over 50 billion IoT devices connected to the internet [42]. As these numbers continues to grow, it becomes imperative to identify flaws and vulnerabilities targeting IoT devices. Improperly secured IoT devices are routinely compromised by threat actors abusing them to conduct malicious activity, such as Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks. By building a threat intelligence IoT solution able to detect and monitor these threats is essential to minimise the damage caused by cyber-criminals.

2.1.1 IoT Standards and Architectures

With the rapidly growing number of initiatives aimed at facilitating interoperability, simplifying development and enabling implementation for industries, the need for a reference architecture becomes clear. Therefore, a variety of reference architectures are evolving in close collaboration between industry and research. The state-of-art offers different reference architectures proposed in scientific papers, standards and white papers published by main vendors. In details a few survey papers [43] [44] proposed a definition of IoT enabled system and the main research issues. An IoT-enabled system that outlines interoperability with the main security challenges related to the different IoT areas: architecture, communication, data processing, data management, security and privacy is presented [45]. Although solutions have been proposed they do not cover all the various areas of the IoT. Nevertheless, the architecture comprises high computational power, high bandwidth system, and the interaction of low power devices between a local network and a personal network.

The reference model introduced in the recommendation [46] consists of four levels in which management and security skills are associated between each level. This recommendation distinguishes between generic security that is independent of the application context and specific security that is application-related but without specifying security methods and mechanisms. Similarity, [47] which includes four layers and offer a detailed mapping of services and functionalities which should be offered by an IoT service platform. This general IoT reference architecture model introduced, places security as an important indication of performance. This can be achieved through the assessment of confidentiality, integrity, authenticity and confirmation of exchanged information between IoT devices. However, this reference architecture does not introduce methods or approaches to identify and implement security. The Industrial Internet Consortium (IIC) introduces the Industrial Internet Reference Architecture (IIRA) [48] and the Industrial Internet Security Framework (IISF) [49] which has a strong industry focus, enables IIoT system architects to design their own systems based on a common framework and concepts but is lacking in security assessment. The Reference Architectural Model Industry 4.0 (RAMI) [50], introduces the general properties of IoT systems as stimulating aspects for Industry 4.0, in particular for the production sector. An architecture and model which catch the functional and information perspectives and a detailed analysis of system requirements in presented [51]. At the same time IEEE Standards Association (SA) is working on a standard to design reference architectures across multiple domains. This standard provides a conceptual basis of things in the IoT and elaborates the stakeholder concerns as a collection of architecture viewpoints which provides the body of the framework description [52]. Finally, IoT vendors propose reference architectures in order to guide for setting up an IoT hardware and software applications relying upon components they produce [53] [54] [55] [56]. In addition, the current increase in network infrastructure in various industrial sectors has highlighted the need to store threats and vulnerabilities from the design stage of IoT devices. The European Network and Information Security Agency (ENISA), which has experience in the field of information security, have stressed the need to record threats [57]. Much effort needs to be focused on those areas that can significantly reduce exposure to cyber-attacks.

With the IoT reference architectures, enterprises are guided during the implementation of IoT technology and able to cover the communication gap between different business layers, for example between management layer infrastructure and the shop floor layer infrastructure and promote a unique infrastructure for sharing data and information together.

However, with this great technological evolution, numerous challenges are faced, especially with regards to security and privacy [58].

2.1.2 IoT technology challenges

The integration of IoT technology for manufacturing sectors lack the security approaches that recommends methods for the development of new systems, which are increasingly safe, efficient and adaptive [59].

The data produced by devices need to be collected, saved, processed and sent through systems that can ensure efficiency, low power consumption, reasonable costs, privacy, and security. Such systems should be configured to avoid overloading which may not support the amount of information.

While methods for devices authentication and identification have been developed [60] [61] [62], there are still studies in progress for user authentication and identification methods.

In order to create an intelligent system, especially for monitoring and control operations, the systems should extract data and produce self-configuration capabilities to provide protocols, languages and formats used by devices for transmitting the information.

2.2 Industrial Cyber security challenges

The application and integration of IoT technology to the Manufacturing sectors represent the “Industrial Internet of Things (IIoT)”. With the IIoT implementation, manufacturing companies may be able to quickly operate in monitoring, controlling and maintaining operations, reducing time and costs. All these activities can be managed remotely anywhere but at the same time, this means that anyone who is able to infiltrate one of the computing nodes within the production network infrastructure is able to attack critical security systems [63]. Such a risk is even more serious if the attack can be performed remotely through the various interfaces to the machine communication with the outside world such as mobile devices, and smartphones [64] [65].

Manufacturing companies have been subject to numerous cyber-attacks, targeting access to sensitive information or falling victim to ransomware operations aimed at blocking access to the computer [66] [67] [68]. This kind of attacks requires physical access to the device for gaining control of it or in some case remote access after gained the authentication credentials of it.

The management of IoT devices includes both software and hardware updates which are essential for the operation and security of IoT devices. In fact, the software and hardware updates not only allows new functions to be released but also allows security problems, such as cloning or Denial of Service (DoS) attacks to be addressed [69] [70]. Therefore, it is essential these updates take place in a safe and timely manner. In order to ensure the integration of IoT communication technology into the manufacturing sector, vulnerabilities and risks must be identified. These categories of vulnerabilities and risks help to create good practices and standards [71]:

- Exponential growth and new vulnerabilities:

The exponentially increasing connection of devices [72], represents a step towards to digitalisation, but at the same time, it contributes to an increase of vulnerabilities. Specifically, from having to protect individual computers (or mobile devices), to having to protect different sensors each with main own level of internal security or more commonly without any security levels. It should also be considered that by connecting many devices in the network, the access points where an opponent could exploit any type of attack increases (classic and not) with the intention of gaining access to this network for a certain period of time.

- Safety and Security:

Devices are implemented with minimal software to meet the application requirements, without security measures (software and devices released quickly). In the past, releasing one or more updates was crucial to protecting associated enterprise servers, while, today through IoT devices it is impossible to carry out updates or patches. These devices lack security support due to low computational capacity, which makes it difficult to design small devices with a light security protocol.

With IoT technology, security has an impact on the safety of the industrial environment. In the event of an attack, the system can fail in economic risk and expand into risks of danger to humans.

- Code heterogeneity and vulnerability:

Many IoT devices designed today do not provide security mechanisms at the communication level, due to the lack of security standards that require continuous updates, especially if, different devices must communicate within the same application environment. Even if the devices, architecture and interactions were completely predictable and secure, it is essential that the code itself that runs on the device is secure. Also, it is not trivial to consider the heterogeneity between platforms and the levels of programmability of the devices. Even with the most secure IoT architecture in the world, if a single endpoint collapses the entire architecture can be compromised. For example, in the case of cloud security solutions, it is normal to rely on the solutions that vendors offer, even if there is the need to evaluate and outline requirements of a company regards managing personal data and sensitive data.

- Business data protection and user behaviour:

Privacy is a key topic that needs to be addressed in the field of security, in the sense that the data is safe and secure, and the company treats the data confidentially. Most of the outstanding issues are regulated in the General Data Protection Regulation (GDPR) [73] which entered into force in May 2018, and thus moving towards a homogeneous and transparent regulation for the consumer. The first line of defence for any IoT users is to use best-practice like changing a device's default passwords, using updates, security-configurable devices, not connecting many devices to a single endpoint.

During the past few years many countries, despite an attitude that has always not been really focussed on cyber security, have begun to outline and invest in real action plans on information security [74], for example, the protection of information and data of citizens, institutions, and much more [75] [76]. Security issues are becoming a point of fundamental discussions and needs to be addressed at all levels of each sector. Therefore, implementing a generic solution for the communication of IoT security devices is difficult as well as a generic architecture, due to its heterogeneous nature and adaptive application nature.

In the field of Information Technology (IT), security means "information security", i.e. "The degree of resistance of the information to (or protection of the information from) harm" [77]. The basic requirements that guarantee information security are called CIA triad [78]:

- Confidentiality: Confidentiality is essential to ensure privacy and the ability to protect data from all individuals who are not authorised to see it. Confidentiality can be breached in the event of tampering with the device containing sensitive data, by an attacker who enters the system and in general by any situation in which data loss or theft occurs. In this case, the most used methods to ensure confidentiality are encryption, the combination of username and password, Personal Identification Number (PIN) codes and identity checks based on biometrics (fingerprints, voice recognition).

- Integrity: Integrity means the ability to prevent unauthorised or unwanted changes to the data. It means that the data must be protected against unauthorised changes or deletions, but also against unauthorised access to the system causing unwanted changes. Therefore, in order to maintain integrity, it is necessary to prevent unauthorised changes to our data, as well as allow the ability to reverse the authorised changes. Modern operating systems are an excellent example of a mechanism that allows the control of the various levels of integrity. To prevent unauthorised changes, these systems implement various levels of permissions to discover unauthorised users. In addition, these systems allow users to restore or eliminate unwanted changes in the event of an error.
- Availability: Availability refers to the opportunity to access data when we need it. A loss of availability can be related to a wide variety of errors or malfunctions within a system, which do not allow users access. These issues are often associated with operating system failures, errors, network attacks, blackouts. When these failures are caused by attacks outside the system, they are commonly referred to as Denial of Service (DoS) attacks, as they interrupt the normal accessibility of a service. Local or remote backup systems, hardware and archive redundancy, firewalls and routers configured to neutralise DoS attacks, uninterruptible power supplies, physical access control, and performance monitoring are just some of the mechanisms for maintaining availability.

A security solution must be part of a real corporate action plan, which concerns not only the sharing of information between multiple departments of a company, but also relates to deciding which levels of trade-off are chosen for different aspects of a product (performance/security, heterogeneity standardisation, security/maintenance). It is a fact that needs to be addressed strategically right at the design stage of any IoT hardware and software solution.

2.3 Industrial monitoring and control systems

The emergence of Industry 4.0 is leading to the deployment of IIoT environment, where legacy production machinery and conventional Industrial Control Systems (ICS) within industrial settings is converging with IoT networking. Moreover, the synergy of IoT deployments with data-driven analytics supported by machine learning (ML), has shown promise in improving condition monitoring, predictive planning and flexible asset management, thus maximising productivity, but at the same time increasing the risk of cyber-attacks [79][80][81].

CPS and IoT open up a wide range of security risks relevant to both the design time and runtime approach [82]. In many cases, unsafe and insecure system operations resulted in a real loss of service and a loss of control of the industrial environment [83] [84] [85] [86]. Additionally, companies often run old versions of desktop operating systems, making it difficult to update the system against network vulnerabilities. Therefore, it is important to understand the objectives of security attacks within the application environment.

In contrast with IT systems, ICSs are Operational Technology (OT) systems [87], which act to offer reliable real-time operations with the necessary execution performance and real-time production security. It is also evidenced that the increased complexity and integration with IoT technology gives rise to several cyber security challenges.

While the IoT is relevant to cyber security including risks to interact with the physical world, the introduction of systematic approaches for automated threat detection would allow prioritising security resources and improve decision making. A classification of attacks and countermeasures on security and privacy for IoT devices is presented [88]. Such a classification is divided into 4 categories:

- the physical attack when the attacker is in a close distance to the device,

- the network attack involves manipulating the IoT networking system,
- the software attack includes vulnerabilities inside the IoT applications, and
- the encryption attack consists of breaking the system encryption.

IoT architectures include a large number of legacy equipment like actuators, sensors, machines connected to a set of specialised ICS devices based on Internet Protocol (IP). Legacy as well as modern production machinery, which are originally systems design without security provisions do not have enough security support for reasons that range from the high manufacturing cost to the inability of remotely patching legacy systems. At the same time, IP-based protocols are also prone to a large range of protocol-specific as well as network-oriented attacks. Therefore, there is an undoubted cyber security risk landscape encompassing the implementation of different communication protocols for IoT deployment.

New types of malware (e.g., Mirai [89] and many of its variants) as well as a range of cyber physical attacks (e.g. cloning attack, network jamming or CPU-level micro-architectural attacks) are proven to defeat current mitigation solutions.

In many industrial sectors, time to market, cost pressure and performance have been prioritised over cyber security [90] and the isolation was the only security for many legacy machines. Currently, the circumstances have changed, and the vulnerabilities of these systems have increased. For example, Stuxnet [91], was infiltrated to an Iranian nuclear plant through an USB drive connected to one of the computer terminals, which was connected to the PLCs of the plant. A provider of corporate security solutions revealed from an industrial report that in 82% of cases an internal attack could have penetrated the industrial system from the corporate network [92] due to poor information protection. The Symantec shows that IoT attacks on honeypot computers have almost doubled in less than a year [93]. Therefore, companies need to control the network and protect it from these deliberate and targeted attacks on IIoT systems [94].

2.3.1 Industrial Control System (ICS) functionality

ICS includes many configurations of control systems such as DCS, SCADA, PLC, IACS, which play an important role in the manufacturing sector and require the implementation of adequate security mechanisms [95].A typical ICS system involves many subsystems such as loop of control systems [96], the monitoring and maintenance tools of remote stations and the interfaces of the machines connected around specific protocols on a multi-level network. The sensors measure physical quantities and return electrical quantities. Then the data is sent to the controller for processing procedures through algorithms which establish points to generate and manipulate variables to control actuators such as valves, motors and switches. The whole system uses these components to process controls which are implemented based on the inputs from the controller. Due to the critical aspect of networking and communication features, many of the ICSs have been developed and installed without concern to the recent security issues, which target them as a vulnerable system.

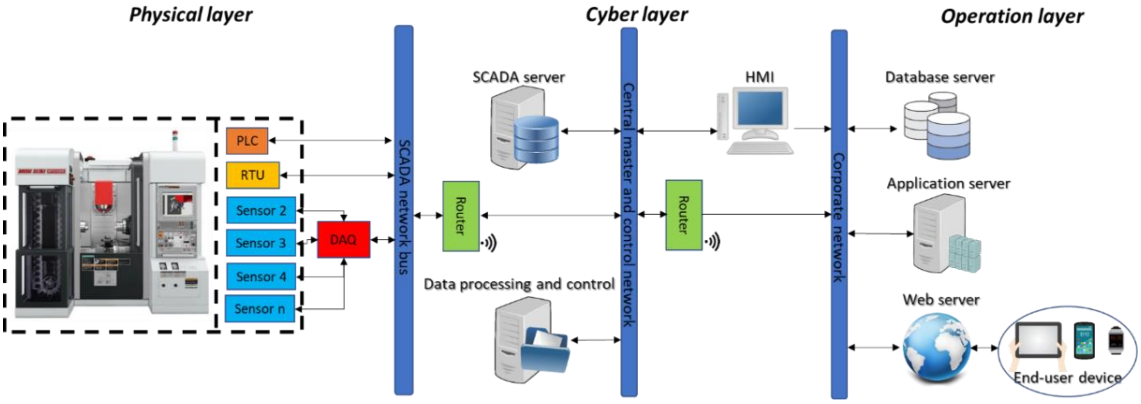


Figure 5: An example of SCADA model based on industrial control system integrated with the corporate network

Figure 5 shows an example of modern ICS which consists of supervisory controls and data acquisition. Inside the physical layer, the control network involves Programmable Logic Control (PLC) and Remote Terminal Unit (RTU). The system collects information from sensors attached to the physical system. Based on that information, the local controllers (PLC/RTU) engage the actuators to perform specific operations on the physical system. In the cyber layer, the server monitors and controls the remote device supervises the field device and provides a distributed decision over a range of different situations [97] [98]. In the operation layer the data is recorded and stored into the database server for further applications and it is accessible from the web server.

2.3.2 Industrial Control System (ICS) security

IoT technology integration for faster, automated data extraction and intelligent decision making exposes ICS to multiple security threats [99] [100] [101]. Currently, industrial control systems have changed and protocols such as Modbus, TCP/IP, offer gateway onto ICS to enable remote monitoring of distributive resources on and existing network infrastructures.

An ICS system is based on industrial network which operates via different protocols including: EtherNet/IP, Distributed Network Protocols version 3 (DNP3) and are interconnected with systems like, PLCs, RTU, Master Terminal Unit (MTU), Human Machine Interface (HMI), sensor and actuators. In detail, the RTU is used for monitoring, storing and controlling the state of physical devices locally. MTU is able to monitor and control different RTUs via communication links. In detail, the MTU reads the status parameters of physical devices in remote locations and reads the control parameters of the RTUs. The HMI allows operators to modify the parameters of RTUs and to control MTU parameters as operators are able to view the status of physical devices.

In modern industrial control systems, network data is derived from machine applications. In this case, the current corporate network for modern ICS is exposed to access password vulnerabilities, which could be an access point for an attacker. In order to obtain the password and consequently access the critical data of the distribution networks, devices and actuators, an attacker can use different password cracking techniques [102] [103]. Therefore, the lack of knowledge in the field of control software and Operating Systems (OS) security, generates limited opportunities for updating software control capabilities [104] [105]. Industrial IoT systems are forced to work on much older versions of OSs or no longer supported versions of the operating system, security patches and service packs [101]. In addition, IoT devices have less computational processing capacity, which is a limit for the communication of industrial control systems. Doing so, the protocols result in a more vulnerable position to malicious attacks. In detail, once MTUs or RTUs that use different types of network traffic and application behaviours are infected with malicious software, traditional IT security tools may not recognise malicious attacks, hence a new framework for malware detection is needed [104] [106]. Therefore, the design and development of secure IoT architectures and attack detection systems for ICS is a crucial topic for industries that requires further research and new solutions.

2.4 Threats analysis for industrial monitoring and control systems

Security incidents have raised security concerns in ICS. Companies have been subject to cyberattacks, aiming to acquire access to sensitive information [107] [67] by manipulating access to computers [108] [109]."Stuxnet" [110] was intended to infect the PLC and SCADA computer that controls the uranium enrichment process of Iran's nuclear plants, by being capable to change the frequency drives, affecting centrifuge normal operational conditions [111]. Stuxnet was not the only threat to Iran's energy infrastructure but was followed by other malware such as Duqu, Flame, Shamoon, Gauss, Duqu 2.0, Shamoon 2.0 and Stonedrill [112]. Therefore, to avoid unexpected changes, a quality control system (QC) is often needed for industry. This system must be strong and flexible in covering several changes with a scheme of security methods for preventing, detecting and recovering attacks [113] to better understand the relationships between threats in phase, planning, production and industrial control system [114]. ENISA introduced a report to better understand attack practices and the evolution of malware. This report analyses the panorama of cutting edge cyber threats based on interactions with experts on the topic of Cyber Threat Intelligence (CTI) [57].

Table 1: ENISA overview and comparison of the current threat landscape 2018 vs 2017 [57]

Top Threats 2017	Assessed trend 2017	Top Threats 2018	Assessed trend 2018	Change in ranking
Malware	Stable	Malware	Stable	Same
Web based attacks	Increasing	Web based attacks	Increasing	Same
Web Application Attack	Increasing	Web Application Attack	Stable	Same
Phishing	Increasing	Phishing	Increasing	Same
Spam	Increasing	Denial of Service	Increasing	Going Down
Denial of Service	Increasing	Spam	Stable	Going Up
Ransomware	Increasing	Botnets	Increasing	Going Up
Botnets	Increasing	Data Breaches	Increasing	Going Up
Insider threat	Stable	Insider threat	Declining	Same
Physical manipulation/damage/theft/loss	Stable	Physical manipulation/damage/theft/loss	Stable	Same
Data breaches	Increasing	Information Leakage	Increasing	Going Up
Identity Theft	Increasing	Identity Theft	Increasing	Same
Information Leakage	Increasing	Crypto jacking	Increasing	NEW
Exploit Kits	Declining	Ransomware	Declining	Going Down
Cyber Espionage	Increasing	Cyber Espionage	Declining	Same

Table 1 introduces the main cyber-criminal attacks ranked in 2018 showing the continuing demand for contextualising and actionable information about cyber threats. Therefore, to understand the current trend, a comparison is made against 2017, where only one new threat has been introduced called "information leakage" which see the system reveal some information to unauthorised parties.

Therefore, contextualising security scenarios and providing a classification of threat types is important for defining security approaches and countermeasures. For example, physical accessibility to the target IoT device is a vulnerability which exposes the data, to several networking and software attacks exploiting vulnerabilities inside IoT applications as well as the encryption attacks, which involves breaking the system encryption making this the possibility of a threat [115] [116]. In other cases, allowing signal reproduction or tag cloning [15] [16] may allow attackers to access critical data, services and facilities.

New risks are emerging with the connectivity of Industry 4.0, which involves an analysis of the security problems and vulnerabilities related to the implementation of the IoT in a production environment. In order to define the best countermeasure mechanisms, any vulnerability that creates an impact on the integrity of the system should be quantified previously. Thus, methods and approaches are required in order to identify risks and vulnerabilities during the design phase for any production IoT enabled integration. Consequently, relevant mitigation strategies must be defined.

2.5 Countermeasure mechanisms

Different scenarios are integrating IoT technology which requires innovative solutions mainly focussed on the security. Most of these integrations remain a "niche" with solutions only focus at the edge of the network as a single endpoint, rather than paying attention to the whole network. An IoT product in network terms cannot be considered independent and separate from the rest of the world from a security point of view, as it interacts with the existing network, with all endpoints, clouds, and both physical and virtual IT systems. Individual IoT security strategies only end up adding elements and reducing vision, especially in the supervisory and control systems for industry [117]. Some modern solutions use devices with updated firmware to ensure system integrity but potentially vulnerable to hacking [118].

By focusing on IoT endpoints, device security can be supported by authentication mechanisms. The Object Security for Constrained RESTful Environments

(OSCORE) is a lightweight communication security protocol that provides application-level end-to-end security for IoT settings. It is designed to protect as much information as possible while still allowing for Constrained Application Protocol (CoAP) proxy operations. At the same time, a corresponding lightweight authentication key exchange protocol is missing [119]. There are some specific solutions used in the past, such as IAM (Identity and Access Management (CSA, 2015)). In order to address the distributed nature of wireless discovery in IoT, the approach Software-Defined Networking (SDN) proposed an approach to network management based on identity authentication scheme in order to improve network performance and monitoring it more like cloud computing [120]. In order to establish communication, the PAuthKey authentication protocol is introduced, mainly focused on obtaining the encryption credentials [121]. Another key point is to ensure the confidentiality of sensitive data, with IoT encryption solutions that use standard encryption algorithms and Public Key Infrastructure (PKI) for network security. This encryption solution includes digital certificates trusted by the device browser but has often violated this reliability. The problem is that not all digital certificate issuers always apply their security policies carefully and consistently [122].

In addition to traditional security properties, IoT technology requires analysis tools (data collection, aggregation, monitoring and normalization to provide reports) for detecting IoT threats (which may generate instability of the IoT network). Initially, the security requirements must be identified during the design phase and adapt traditional security systems (with updated firmware), with structurally very limited resources and fully integrated into the network. In this context, it is necessary to contextualise which critical scenarios of an IoT monitoring product could be different from others already in terms of prototype and software design. The developers of the IoT monitoring device software must involve analysts and security users, who are required to define step-off trade-offs, considerations and what security aspects to guarantee, evaluate and verify, carefully analysing every factor that could compromise a decision. The goal is to support the design phase to ensure that IoT hardware and software are built following security requirements. In this context, the effort to be adopted will be to seek a software design methodology that guarantees incremental and iterative development, but which also includes security properties during the design phase, and which is open to maintainability and extensibility. Agile's working methodology [123] (with reference to Scrum and XP techniques such as Test-Driven Development (TDD), helps to respond to the unpredictability of software construction and evolves through collaboration between teams. It is therefore important to contextualise security vulnerability scenarios and provide an analysis of the types of security threats. OWASP (Open web application security project) [124], aims to improve the computer security of applications, that introduces the most common risks and attack scenarios within a web application and to collect and explain the most common errors. In recent years, with the consolidation of IoT, OWASP has also defined the most common vulnerabilities of architecture for this technology creating a specific OWASP IoT project [125] and defining the most common vulnerabilities within the IoT architecture [126]. As far as IoT architecture is concerned, it is possible to associate different attacks on the different architectural levels of IoT (application, network and level of perception), which in many cases exploit the vulnerabilities shared between the different levels. Security management has received very broad attention in the field of information security, while IoT security remains a challenge due to the need to cover the entire technology, from the physical to the application layer for extended network systems.

2.6 Threat modelling methods

Security organisations and experts are recognising the importance of choosing the right threat modelling methodology for an organisation’s specific challenges. In order to have complete design management for security, various approaches have been proposed. For such approaches, the application context is always of paramount importance. Although each approach to threat modelling provides identification of threats from a theoretical perspective, it varies in terms of quality and consistency received for resources invested from a practical perspective.

Table 2: Key points of Threat-Modelling Methods

Methodology/approach for threat identification	**Key points**
STRIDE [24] [127]	The goal is to obtain an application with Confidentiality, Integrity and Availability (CIA) security properties, together with Authorisation, Authentication and Non-repudiation. It is in line with the Microsoft Trustworthy Computing directive of January 2002 [128], which ensures that Microsoft's software developers think about security during the design phase. It is a developer-focused and influences the software industry.
The Process for Attack Simulation and Threat Analysis (PASTA) [25]	The goal is to use technical requirements to align business objectives considering business impact analysis and compliance requirements. The threat modelling methodology consists of an attacker-focused perspective and potential threats with risk and impact analyses. It is primarily used for organisations wishing to align threat modelling with strategic objectives through business impact analysis. Such alignment can sometimes be a weak point depending on the organisation, which can take many additional hours of training and education. It is an attacker focused.
LINDUUN [24]	It is a privacy threat methodology which supports analysts to identify confidentiality requirements. It can be used as a framework to identify privacy threats in addition to STRIDE. However, it does not explicitly provide risk analysis support.
ATTACK TREE [129]	It is the oldest approach for modelling threats against computer systems. It is in fact a qualitative approach that allows security analysts to develop the necessary documentation to make the right choices. However, attention must be paid to the limitations of the attack trees that must be understood before using it.
Common Vulnerability Scoring System (CVVS) [130]	The goal is to define vulnerability and produce a numerical severity score for each common vulnerability and exposure. It is composed of three

	metric groups (Basic, Temporal and Environmental), where it is possible to recover the score. CVSS is often used in conjunction with other threat modelling approaches. However, it does not explain how to assess the risks of system components such as resources, groups of resources, products and ignores both the sources of attack and the attack paths for calculating the risk.
Quantitative Threat Modelling Method (QTMM) [131]	It consists of attack trees and STRIDE method applied in synergy. Aims to solve some problems with threat modelling for cyber physical systems that have had complex interdependencies between their components. It requires a better understanding of how to quantify security and privacy risks.
TRIKE [132]	It consists of a risk-based approach and a risk modelling process. The approach is a model of requirements, which ensures that the level of risk assigned to each activity is acceptable to the various stakeholders. This approach requires that a person know the whole system to conduct an attack surface analysis that makes scaling difficult on larger systems.
Visual, Agile, and Simple Threat (VAST MODELLING) [133]	Contributes directly to risk management. It is explicitly designed to be scalable and integrates seamlessly into an Agile environment and provides achievable, accurate and consistent results for developers, security teams. It is an enterprise-focused practical approach that recognises the security problems of development and infrastructure teams. Two types of models are required: operational threat models and application threat models.
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [134]	It is a practice focused methodology for assessing organisational (non-technical) risks that may result from violated data resources. This model offers a solid view of resources and organisational risks, but documentation can become voluminous. In addition, as technology systems add users, applications and functionality, a manual process can quickly become unmanageable.

Table 2 summarises the main threat modelling methods available in the industrial security literature, highlighting the key points for each of these methods. Each threat model provides the means to identify threats. However, on a practical level, threat modelling methodologies vary in terms of consistency, quality and value received for the resources invested. Although threat methodologies may be able to identify potential threats, the type of threats identified will vary significantly. Therefore, the challenge is to choose a threat modelling methodology based on the desired results. In addition, these methodologies do not offer higher-level guidelines, which sufficiently address the risks introduced at the IoT endpoint level. They also do not consider the context of the real-time application and integration with SCADA, IACS, ICS, DCS and PLC. The Industrial Internet of Things (IIoT) has focused on the integration of IoT technology and industrial equipment. Most of the threat methods trying to identify risks and vulnerabilities between IoT and the current supervisory and control systems for the industry which aims to identify and build defence mechanisms, sometimes without being efficiently implementation especially in the case of legacy industrial machines integration. Despite substantial research in the field, there is still a significant number of applications and research outputs targeting the introduction of IoT in manufacturing and in particular addressing the upgrade of legacy production equipment, without due consideration for security management.

2.7 Knowledge gap

IoT is an advanced communication technology with identifiable interconnected devices on the network, capable of supporting and updating legacy production machinery especially, to support the control and monitoring operations during the production processes. This integration creates new risks and vulnerabilities which requires the implementation of new models and approaches to identify risks and vulnerabilities. This security must be considered from the initial design stage of any IoT supervision and control devices taking into account in advance the origin of any attack. Several reference architectures and models provide high level guidance regarding architecture considerations for securing IoT without paying attention to the practical aspects at the shop floor level especially, for integrating monitoring and control IoT devices. In addition, the lack of threat taxonomy makes it difficult to identify the countermeasure mechanisms. Device security may be supported by authentication mechanisms against software issues, but hardware countermeasure mechanisms are still missing. Therefore, the major gap identified is that an approach that practically address security and integrity risks when incorporating IoT within legacy production environment is missing. This approach should easily identify the risks and vulnerabilities of legacy production machinery for the systematic integration of IoT technology and to monitor any changes related to the development of security solutions. Also, the integration of IoT within an industrial environment is managed by authentication mechanisms often heavy in terms of processing capabilities which focus only on the software aspects of the IoT application. Itis important to define a lightweight authentication protocol with real-time functionality, which increases the complexity required by any attack approach to compromise the IoT device and monitoring via hardware and software functionality.

2.8 Chapter Summary

Some modern solutions use devices that guarantee a form of integrity through the firmware update but at the same time can cause vulnerabilities. Another key property of security is identity and user-centred and software-based access protection, but still lacking hardware authentication mechanisms.

Classic security properties are combined with new IoT connectivity for data collection, aggregation, monitoring and normalisation and to provide reports for threat detection. It is natural to think that these approaches to security are indispensable to be considered as a starting point for the design of security and, at the same time, they collide with the intrinsic limits of the connected devices at the network. Terminal nodes structurally have very few resources in terms of computational capacity, which means that it would not be practical to implement cryptographic mechanisms on these devices which would overload the calculation. Furthermore, in order to isolate the device from possible attacks, it would be a good idea to segment the network. If on the one hand, it is necessary to have full visibility of the network interaction between all the actors of an IT architecture, on the other it is necessary to design the system in order to isolate the sections at risk and limit the damage, in order to maintain them at a manageable level.

Once the security requirements have been identified during the design phase of an IoT solution, it is necessary to adapt traditional security systems to the reality in which the devices are rigid (with firmware difficult to modify) and fully integrated into the network. In order to discover vulnerabilities and risks for IoT integration in manufacturing companies, it is important to precisely contextualise the operational and implementation scenario for an IoT product right from the design phase. In the past, security has always been studied in relation to the abstraction level indicated as network security level, security transport level and security applications. Today different approaches are proposed that overcome the limitation, supporting the innovation of IoT technology which is represented by the proposal of a real architectural stack on several levels. Therefore, approaches that consider best practices and guidelines to formulate a new domain-specific approach are required, helping to bridge the gap between the introduction of IoT connectivity at the shop floor and shielding system and operational integrity.

3 RESEARCH METHODOLOGY

The review of the relevant literature presented in the second chapter showed that the lack of systematic approaches related to the integration of IoT technology in the manufacturing industry was mainly limited to monitoring and maintenance operations without paying attention to security aspects. Other than that, most studies involve the implementation of encryption and authentication mechanisms against software problems, but hardware countermeasure mechanisms are still missing. Such hardware threats should be taken into consideration when designing an embedded IoT device. The identified gaps based on the literature review led to the development of goals, objectives, scope and adopted the methodology of this research. This chapter presents the research methodology and approach that are used to achieve the research aims and objectives. The research design and methodology is introduced in Section 3.1. In Section 3.2 data collection methodology in research are discussed. Section 3.3 is the adopted methodology, and in Section 3.4 the summary of the main points for this chapter is presented.

3.1 Research Design and Methodology

The term research has received different definitions based on the context of application. An overview of methodologies and techniques used for scientific research is introduced [135]. Shuttleworth defines research as the broadest sense is any collection of information, data and facts in order to advance knowledge. These definitions assume that research is a systematic data collection and analysis activity involving a series of processes [136]. Creswell provides the sequential steps below to make research a systematic process of collecting and analysing data in order to increase understanding of a problem [137]:

- Identifying a Research Problem
- Reviewing the Literature
- Specifying a Purpose and Research Questions or Hypotheses
- Collecting Quantitative Data

- Analysing and Interpreting Quantitative Data
- Collecting Qualitative Data
- Analysing and Interpreting Qualitative Data
- Reporting and Evaluating Research

In order to extend decisions from broad assumptions to detailed data collection and analysis methods, it is necessary to select a research methodology [137].

3.1.1 Research Design Based on Application

From the point of view of its application, research can be classified into two broad categories. Pure research consists of developing and testing of hypothesis and theories which usually do not have practical application at the present time [138]. The applied research focuses on solving practical problems by using existing procedures and methods such as the body of knowledge in that research domain to solve a specific issue [139]. It is always better to initially identify the research application, then if possible, an appropriate strategy for data collection and analysis techniques. The research being undertaken in this Thesis is an applied research, as it seeks to solve an industry problem.

3.1.2 Research Design Based on Different Approaches

Several terminologies are present in the literature to refer to the research approach, for example, “strategy or methodology” [140] [141]. In regards to research design there are two distinct approaches, qualitative and quantitative [142]. Often a research tend to be more qualitative than quantitative and vice versa [137]. As a result of this a mixed method approach has been introduce which refer to as the combination of qualitative and quantitative approaches [137]. In detail, qualitative research aims to explore and understanding the meaning ascribed to a human or social problem by individuals or a group. Quantitative approach is used for examining the relationships between variables using numerical format for testing objective theories [137]. These variables are measurable so that the data can be analysed statistically. The mixed method approach is a research approach which combines qualitative and quantitative approaches, with underlying some philosophical assumptions. In case that a combination of qualitative and quantitative approaches is possible, as within certain limits all types of research are suitable for both approaches [143]. This research will make use of both qualitative and quantitative approaches for this study. As a result, the mixed method approach allow the presentation of qualitative data using quantitative method of analysis enabling researchers to carry out well managed and well documented research [141].

3.1.3 Research Inquiry Strategy

The research inquire strategy which can be classified into three classes based on objectives such as descriptive, explanatory, and exploratory [144]. A descriptive research require is an intense previous knowledge of the background issue under study [140] describing the “what”, “why”, “where”, “when” and “how” research questions seek the description of a phenomenon in a systematic pattern. An explanatory research attempts to answer the question why and identify relationship between aspects of a phenomenon [140]. In case the objective is in areas where little is known or for generating new hypothesis and ideas for future researches the exploratory research is undertaken [140]. Such a research approach suggests the adaptability of exploratory research to many research strategies such as survey, experiment, and case study [144].

3.1.4 Research Strategies for Data Collection

Robson [140] argues that a good research strategy should have good compatibility between the purpose of the research, the theory, the research questions and the sampling strategy. The research strategy should focus on answering research questions. The data collection method should provide answers to the research questions. Robson [140] presented traditional research strategies for collecting research data in both quantitative and qualitative research. These research strategies include experiments, case study, grounded theory, survey and ethnography study [137] [140].

3.2 Data Collection Methodology

There are numerous methods in the literature for collecting data in a format such as a survey, interviews, literature review, observations and experiments which, depending on the type of approach to research, the design of qualitative, quantitative or mixed research [137] [140].

3.2.1 Review of Literature

According to Creswell [137] the review of literature helps to determine if a research topic is worth studying. At the same time provides insights for the researcher to limit the scope to a needed area of inquiry. Also, a literature review fills the gaps of the research via the knowledge gained during the previous studies and provides the basis for establishing the relevance of a study and the comparison of the study results with previous findings. Finally, the literature review provides knowledge of what is already know, what methods have been used, and possible limitation of existing knowledge about a problem domain.

3.2.2 Interviews

The interview is very useful for gathering specific information, which maybe only some people know, or to gather very thorough knowledge [140]. The interviews unlike the use of questionnaires where data can be recorded and analyse via different methods, involve verbal interactions [145] and its permit for more elaborate data collection method compared to other methods of data collection. Despite the advantages the interview structure seems to collect the major consideration. Based on the structure that a researcher can use there are three types of interviewing techniques [140]:

- structured, uses a rigid procedure for the interview questions which in some cases allows little or no opportunity for modifications[145] [140]. Such an interview consists in addressing standardised and structured questions to all candidates, mitigating the possibility that the interviewer deviates from the established scheme. The result, therefore, is that of caging both the selector and the candidate within an interview grid. This is a type of interview widely used because, it is possible to predetermine judgments via score scales and checklists;

- semi-structured is a compromise between a structured interview and an unstructured interview. The interviewer identifies the areas to be explored but leaves the interviewee free to proceed according to the order and method he prefers [140]. It provides more flexibility than the structured interview;
- unstructured is characterised by poor planning of the objectives they want to achieve and by a low control exercised by the interviewer on the interaction. The respondent is left ample room for the interview self-management, although the selector may reserve some questions or ask for some clarifications Though this technique the interview may have difficult in the analysis of the result and may lose control of the interview [140].

3.2.3 Experiments

Experiments is a different way for data collection methodology, which allow the researcher to study cause and effect relationships between independent and dependent variables. The aims is to test the impact of an intervention on an outcomes, controlling for all other factors which might influence the outcomes [137].

3.3 General Research Methodology Adopted

The adopted research design is based on the research aim, objectives and intend to cover the research scope of this study. The present study is an applied research methodology that uses existing information, methodologies and techniques already present in the body of knowledge to solve an industry need. This research is exploratory as it seeks new insights into strategies to develop a novel endpoint methodology for systematically integrate and design robust secure IoT data acquisition hardware and software for monitoring legacy production machinery remotely. The study seeks a mixture of the qualitative and quantitative research design approach. The type of data to be collected and analysed is an important factor in the employed research design approach. During the study, both qualitative and quantitative data must be sought, hence the combined approach. The gathering of information about the research domain with respect to the case study selection to reflect current practice is presented and is carried out through use of questionnaires semi-structured and unstructured interviews and observations. The transcript of the questionnaire adopted is presented in Appendix A.

The focus of this research is to propose an end point security by design real-time approach for IoT-enabled monitoring of legacy production machinery that can be used for initial integration of IoT technology within the legacy manufacturing environments. Hence, the selection of the case study data collection methodology which requires the development of detailed, intensive knowledge about a case, which in this study is the security of an IoT data acquisition system. Literature review, experiments, computer simulations, interviews, and document analysis will be employed as strategies for elucidating the required knowledge to achieve the scope of this research. Although case studies are traditionally more suited for qualitative research, the implementation of experiments in case studies is becoming a current approach. A case study can be used as an experimental investigation and can include a combination of quantitative or qualitative evidence [144]. The requirements of this survey are the motivation of the research design approach and the data collection methodologies.

This research investigates the dependency of security IoT devices for monitoring application on the legacy production machines. In this research, a novel end point security risk-averse design thinking approach is presented through development of an innovative IoT device security implementation, following the isolation principle of modularity, included a new lightweight authentication protocol. Such a security design thinking approach is implemented using two case studies:

- Denial of Service (DoS) attack;
- Cloning attack.

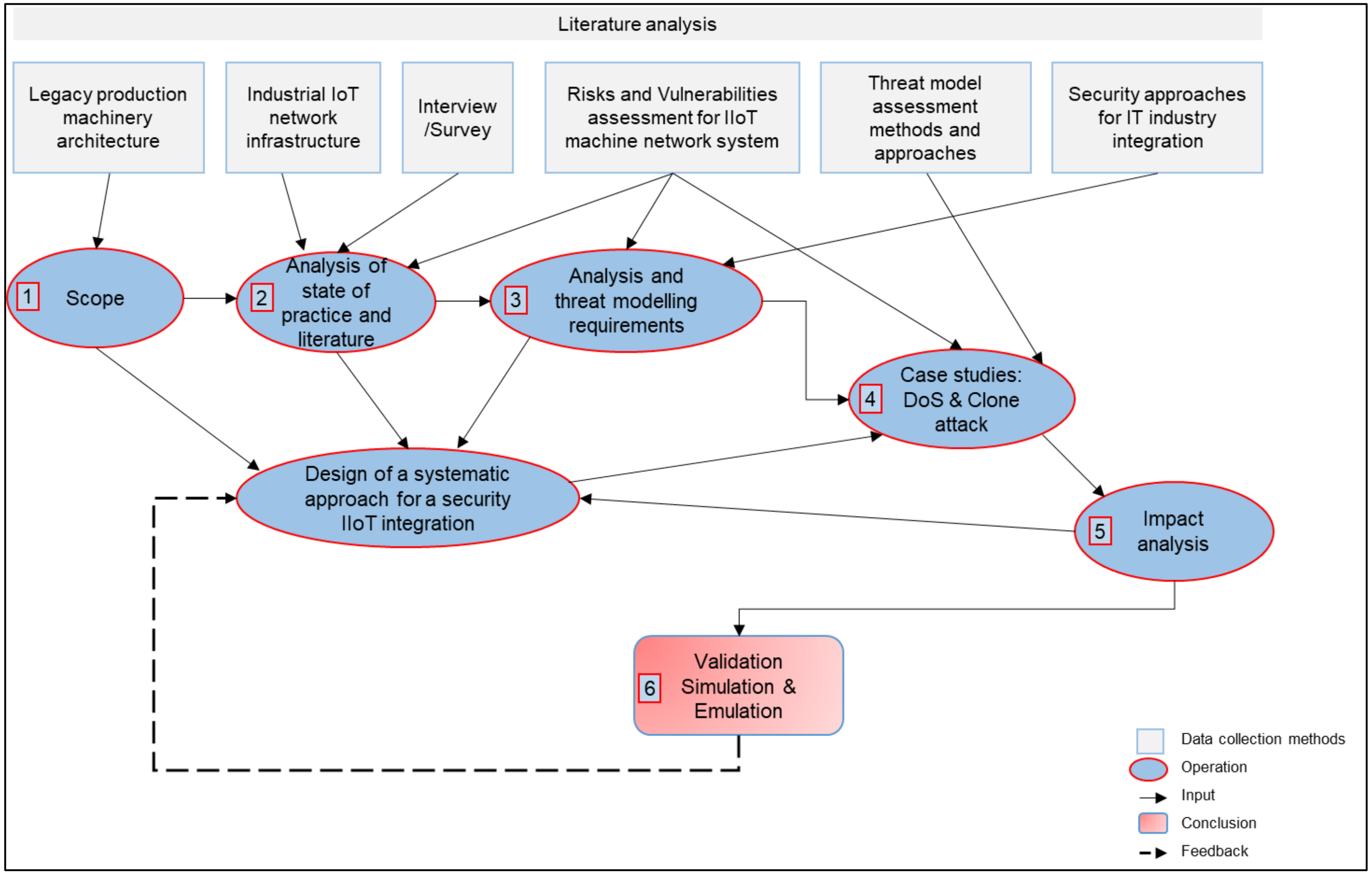

Literature analysis
Legacy production machinery architecture
Industrial IoT network infrastructure
Interview /Survey
Risks and Vulnerabilities assessment for IIoT machine network system
Threat model assessment methods and approaches
Security approaches for IT industry integration
1 Scope
2 Analysis of state of practice and literature
3 Analysis and threat modelling requirements
4 Case studies: DoS & Clone attack
Design of a systematic approach for a security IIoT integration
5 Impact analysis
6 Validation Simulation & Emulation
Data collection methods
Operation
Input
Conclusion
Feedback

Figure 6: Overview of the adopted research methodology

The rationale for selecting DoS and Clone attack is based on the findings of a case study selection process carried out in the review of the literature. This research is applied research done in collaboration between academia and industry which try to suggest a novel security approach when IoT technology is implemented inside the manufacturing industry for the remote monitoring application. Figure 6 presents the research methodology adopted to achieve the aim of this thesis. The first 2 phases collect knowledge from the literature to cover the scope, identify the context of the application and the associated risks and vulnerabilities. The result of the first 2 phases is to design a systematic approach for IIoT security integration. Phase 3 analyses attack threats and identify the requirement for designing threat models. Phase 4 assesses the literature for the threat model risks, vulnerabilities and methods to identify attack scenarios. Phase 5 is the impact analysis for the selected countermeasure mechanisms. Finally, the validation phase consists of simulation and emulation activities that returns feedback for further improvements of the current systematic approach identified.

Data collection

The knowledge for this research has been captured using three main sources:

- published journal papers, conference papers and technical reports,
- interview and survey with expert and industrial observation, and
- simulations and emulations.

A review of the literature was carried out to identify security challenges, risks and countermeasure mechanisms of existing monitoring architecture for legacy production machinery, IoT security risks and vulnerabilities, as well as the common threat methodologies and approaches for addressing some of these security risks. The literature survey provided a comprehensive understanding of existing research, methods for the integration of security IoT technology within the industry, their strengths and limitations, and as well as the knowledge gap in the study of design a security approach for designing IoT embedded devices for the manufacturing industry. The industry visit and interview of experts were carried out to understand how the research fits into an industrial context. The interviews and industry observation helped to identify the current IT industry level and security level used into the manufacturing industry.

A questionnaire survey was created for this research to gather knowledge which was not available from books and literature to understand the actual application context and aspects of the functional impact of potential compromise in the monitoring infrastructure and tools and this is presented in Appendix A. Both industries and research organisations were involved in this survey. The salient information was used to guide the purpose and direction of this research project. The survey shows, the sensor data being collected in a machine database before being processed by the maintenance software within the manufacturing companies. The machine is equipped with encryption mechanisms and passwords for authentication. Furthermore, in order to monitor the deterioration of the spindle unit, in particular for the motor bearings, it is necessary to design an intelligent system that monitors vibrations, temperature and noise.

3.3.1 Research Parameters

This research studies the influence of secure design features on the architecture for the iteration of IoT technology into a manufacturing environment. Due to the different implementation of an IoT architecture, the research is focussed on the monitoring aspect for industrial production machinery. In carrying out this study certain parameters have been identified to be of interest. Such parameters include the dependent from the inability to communicate with the Cloud, the System Control Unit (SCU), the User Devices, inability to upgrade the firmware, inability to use the Human Machine Interface (HMI), inability to collect correct data from the sensors, to protect sensor data, and to send data correctly.

3.3.2 Research Instruments and Materials

The research deploys a novel modular IoT DAQ unit and utilises the use of tests to achieve its aim and objectives. Two types of tests methods were employed in this research. The type of experiments used were hardware experiments and computer simulation and emulation experiments. Hardware experiments to characterise the physical operation of the authentication protocol for the modular IoT DAQ unit were carried out. This was done to deploy a novel authentication protocol which cascades the complexity of compromising its own security, allowing access to for authorised users and provide data validation for further use in the computer simulations and emulations. The computer simulation and emulation experiments were used to replicate the behaviour of a system starting from a conceptual model and prove the feasibility of such modular IoT DAQ unit against two case study (DoS attack and clone attack). Finally, validation and discussion to describe the analysis of findings.

3.4 Chapter Summary

This chapter presents the aim, objective and scope of the research. It also presents the methodology used in attaining the aim and objectives of the research. A literature review of research methods and approaches is undertaken with an aim of selecting the most appropriate methodology. A mixed study research approach was adopted, integrating both qualitative and quantitative research methods. Due to the plethora of security threat methods and IoT monitoring applications for the manufacturing industry, a case study approach is selected. Based on the nature of the study the variables and experimental methods to be used are highlighted, and finally, a validation procedure is presented to validate the effectiveness of the systematic design thinking approach to design security IoT monitoring devices for the legacy production machines. In the next chapter details of the methodology and procedures followed in eliciting expert knowledge and observation for such a systematic design thinking approach are presented.

4 DESIGN THINKING METHODOLOGY FOR IoT SECURITY IN AN INDUSTRIAL ENVIRONMENT

The integration of IoT technology in real-time monitoring of production machinery is an important application objective that offers significant opportunities to transform production in the context of the digital industry, creating new security risks. The design of IoT security architectures is, therefore, one of the fundamental challenges of Industry 4.0. Monitoring of production machinery is a key application goal when introducing IoT into such environments. The security of IoT devices makes a fundamental contribution to any IoT security approach in industrial environments that must take into account the relevant recommendations and standards [146].

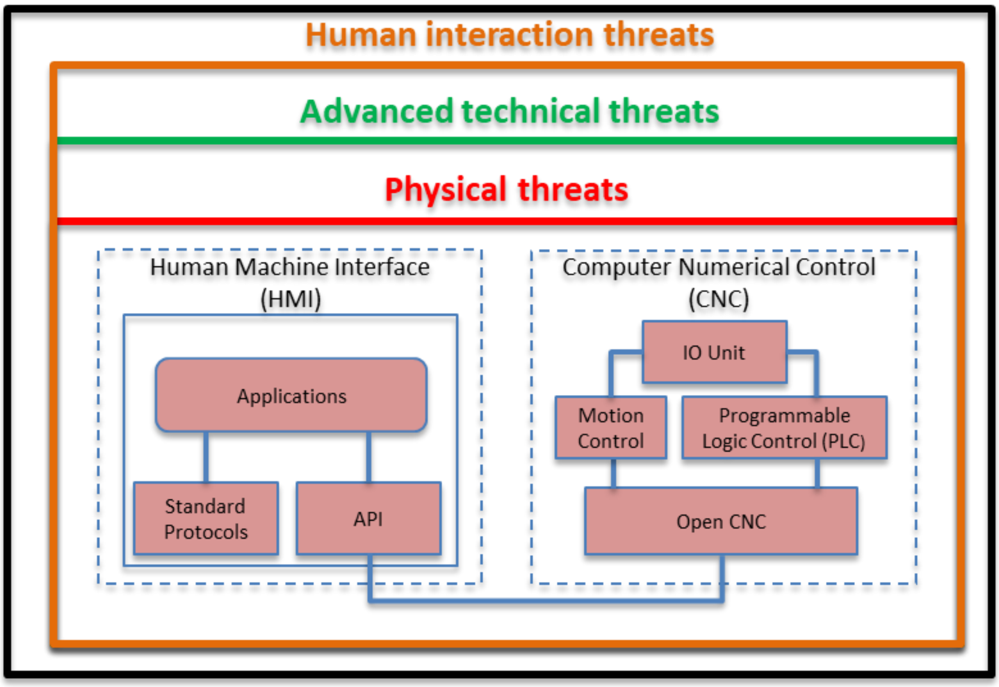

Human interaction threats
Advanced technical threats
Physical threats
Human Machine Interface (HMI)
Applications
Standard Protocols
API
Computer Numerical Control (CNC)
IO Unit
Motion Control
Programmable Logic Control (PLC)
Open CNC

Figure 7: Abstract view of threats for legacy production machinery monitoring. API: application programming interfaces

An abstract view of the nature of threats related to legacy manufacturing machinery is shown in Figure 6, which shows that open numerical control machines use communication capabilities over standard network protocols and provide APIs to access data from third-party applications. Such a CNC machine could be susceptible to attacks against access to real-time machine data, tampering with production machinery, modification of the machine software or machine code for machining operations, cloning devices, as well as the introduction of Denial of attacks Service (DoS) or reverse engineering processes. The attack can be classified into three groups, namely physical threats at the low-layer, various intermediate technical threats, and human interaction threats at the top-layer. Physical threats can have a tangible direct impact which involves physical tampering, such as physical damage to machinery, infrastructure or damage to personnel. Advanced technical threats can cause software and data tampering and refer to technology-enabled access to the network layer. Threats of human interaction are relevant to human interaction with technical systems. This chapter introduce a comprehensive and systematic design thinking approach for IoT device security, which includes five key stages:

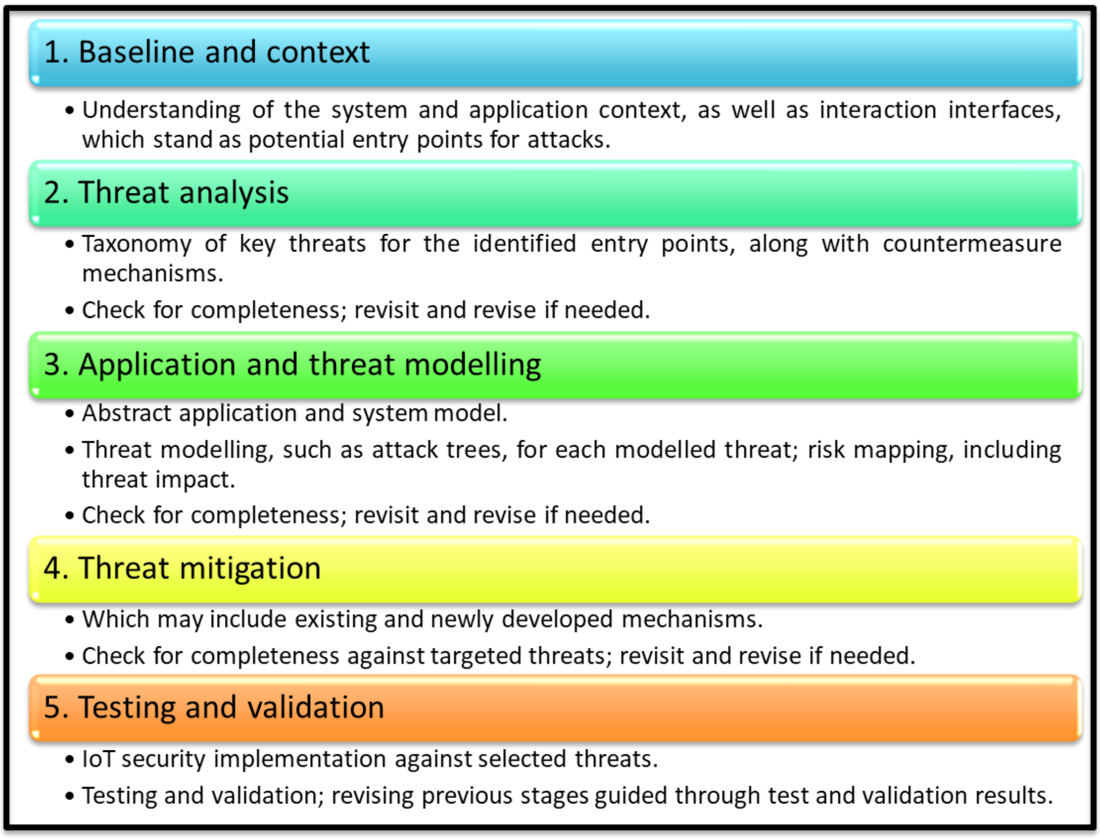
1. Baseline and Context.
2. Threat analysis.
3. Application and threat modelling.
4. Threat mitigation.
5. Testing and validation.

Such a structured approach is defined through an evaluation of possible attack entry points in current industrial control and monitoring systems.

“Baseline and Context” and “Threat analysis” phases are described in detail in this chapter. “Application and threat modelling”, “Threat mitigation” and “Testing and validation” requires not only specific application domains but also threat analysis is required which will be described in more detail during the next chapters. This conceptual level contribution may benefit from additional methods and tools like Model-Based System Engineering (MBSE) and security meta-models which may be relevant to move from a more abstract concept model to a more specific and practical application case [147].

4.1 Monitoring system security for legacy industrial production machinery

The present research proposes a comprehensive and systematic design thinking approach for IoT device security, which includes five key stages (Figure 8), defined through an evaluation of possible attack entry points in current industrial control and monitoring systems.



1. Baseline and context

- Understanding of the system and application context, as well as interaction interfaces, which stand as potential entry points for attacks.

2. Threat analysis

- Taxonomy of key threats for the identified entry points, along with countermeasure mechanisms.
- Check for completeness; revisit and revise if needed.

3. Application and threat modelling

- Abstract application and system model.
- Threat modelling, such as attack trees, for each modelled threat; risk mapping, including threat impact.
- Check for completeness; revisit and revise if needed.

4. Threat mitigation

- Which may include existing and newly developed mechanisms.
- Check for completeness against targeted threats; revisit and revise if needed.

5. Testing and validation

- IoT security implementation against selected threats.
- Testing and validation; revising previous stages guided through test and validation results.

Figure 8: Design thinking approach for IoT embedded device security

Feedback from each phase reveals a need to reconsider analysis, modelling, design, and implementation choices for all earlier phases.

- **Baseline and context**. The first stage involves an analysis of current practices in production environments and outlines guidelines for introducing security by design on IoT devices with a special emphasis on hardware-related security aspects. This serves as a key design perspective in developing a solution for manufacturing environments. An understanding of the application context is necessary in order to apply the proposed concepts to a specific application target. This is shown in the case of IoT-enabled legacy production machinery monitoring by abstracting a typical monitoring architecture and identifying interfaces as entry points for attacks.

- **Threat analysis**. The second phase includes an analysis of the main security vulnerabilities associated with the implementation of IoT in the production environment. Such vulnerabilities are classified under categories of physical, human interaction and advanced technical threat. In addition, possible mitigation mechanisms are proposed and the impact risk assessment is quantified into three categories (high, medium and low) performing in line with the recommendations [148].
- **Application and threat modelling**. The third phase focuses on the specific targeted application, producing a more detailed abstract model of the targeted system, along with its interfaces and functionality. The reason is to define the attack target, which is to gain access to the network, system communication, and data acquisition unit. It involves systematic threat modelling via attack trees for each key threats. The threat model needs to be checked for completeness, accuracy and coverage of security threats. A more detailed model is produced of the targeted system, along with its interfaces and functionality. Modelling tools include data flow diagrams (DFD) [149] to understand the permeation of data trust between components, and systematic threat modelling via attack trees [150], which need to be checked for coverage of security threats.
- **Threat mitigation**. The fourth phase moves on from the design and modelling stages to the implementation of security threats-mitigation mechanisms. In the present work the implementation is through an innovative IoT device security implementation, based on modularity and a new lightweight and flexible authentication protocol. This is integrated in a prototype IoT device for monitoring (modular IoT Data Acquisition – IoT DAQ unit).

- **Testing and validation**. The final phase includes the testing and validation of the developed implementation against selected threats. Results from this phase can be used for improving the effectiveness of all previous stages. The test phase might include functional testing and simulation testing, while validation may be performed in a test or a controlled operational environment. To demonstrate the application of our design thinking approach, two cases were considered – Denial of Service (DoS) test and clone attacks test. These functional tests considered aims to deliver a monitoring system which works without any interruption.

4.2 Design thinking for IoT security in an industrial environment

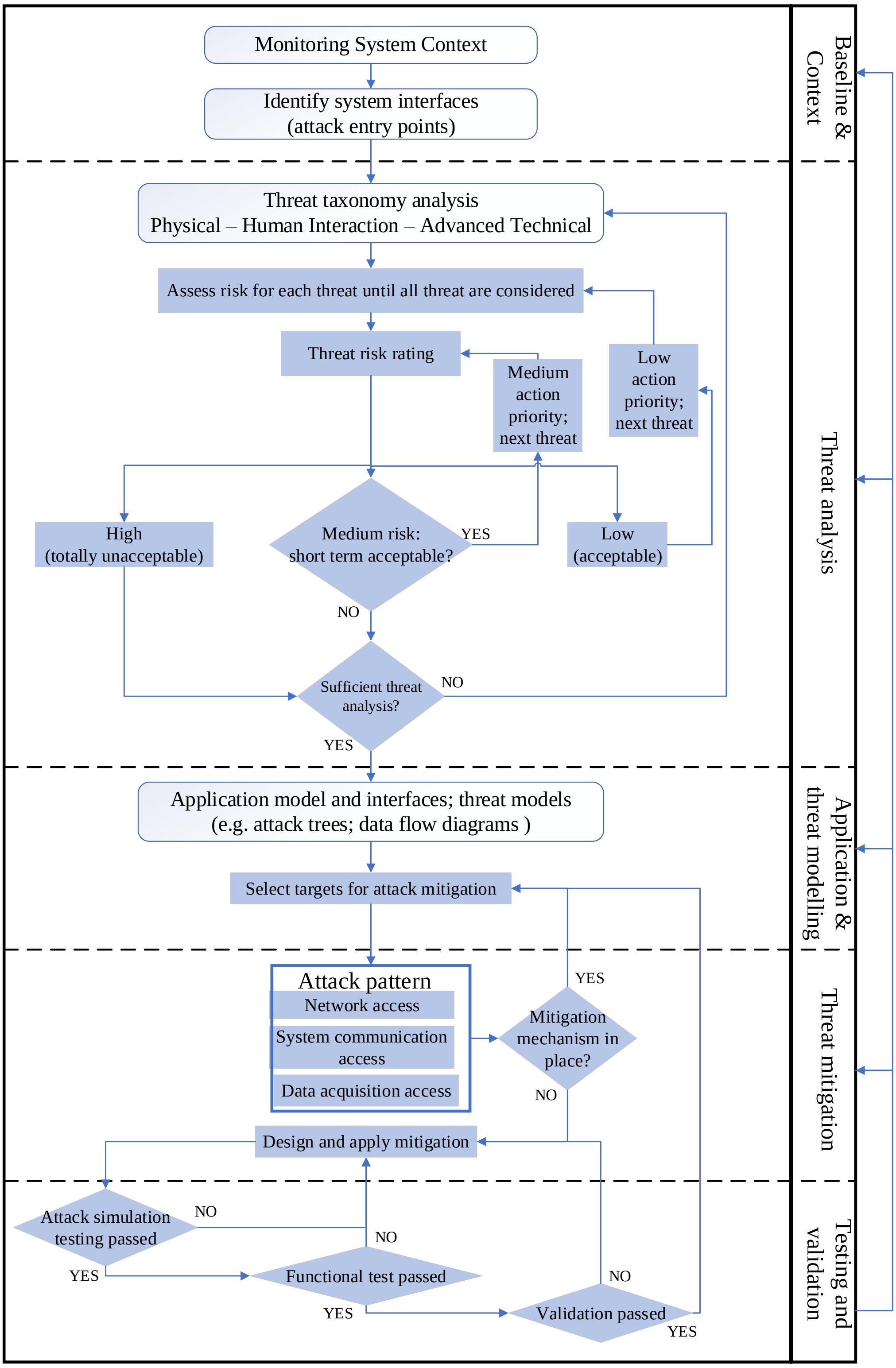

Monitoring System Context
Identify system interfaces (attack entry points)
Threat taxonomy analysis
Physical – Human Interaction – Advanced Technical
Assess risk for each threat until all threat are considered
Threat risk rating
Medium action priority; next threat
Low action priority; next threat
High (totally unacceptable)
Medium risk: short term acceptable?
YES
Low (acceptable)
NO
Sufficient threat analysis?
NO
YES
Application model and interfaces; threat models (e.g. attack trees; data flow diagrams)
Select targets for attack mitigation
Attack pattern
Network access
System communication access
Data acquisition access
YES
Mitigation mechanism in place?
NO
Design and apply mitigation
Attack simulation testing passed
NO
YES
NO
Functional test passed
YES
NO
Validation passed
YES
Baseline & Context
Threat analysis
Application & threat modelling
Threat mitigation
Testing and validation

Figure 9: Design thinking approach for security IoT devices in the production environment

The proposed systematic approach flowchart is presented in Figure 9 which reads from top to bottom applied to a real-time monitoring application related to production environments. The first stage (Baseline and Context) is useful to define the current technology of the monitoring system. It is important to define which kind of IoT integration (hardware or software) is required for the current control and monitoring system, while the attention is focused on the security aspect for defining attack entry points inside the system, which an attacker can gain access. This serves as a key design perspective in developing a solution for manufacturing environments. An understanding of the application context is necessary in order to apply the proposed concepts to a specific application target. This is shown in the case of IoT-enabled legacy production machinery monitoring by abstracting a typical monitoring architecture and identifying interfaces as entry points for attacks.

The second stage (Threat analysis) identifies the interfaces which pose security risks, involves an analysis of key security issues and vulnerabilities related to the implementation of IoT technology inside a production environment, classifying them under broader categories of physical, human interaction, and advanced technical threats. A taxonomy of threats falling under these categories is then produced, including potential mitigation mechanisms. If the threat is not included inside one of these three categories, the model moves back to the initial stage.

After identifying the categories of threats, the third phase (modelling of applications and threats) produces a more detailed model of the targeted system, which includes interfaces and functionalities involving a systematic threat modelling via attack trees, which need to be checked for coverage of security threats. This phase consists of re-design the current system integrated to IoT connectivity, then looking for the attack targets, which are Network access, System communication access, DAQ unit access. These attack trees help our approach to design mitigation mechanisms.

The fourth phase moves on from the design and modelling stages to the implementation one. In the present work the implementation involves the development of an innovative IoT device security implementation, based on modularity and a new lightweight and flexible authentication protocol, integrated in a prototype IoT device for Data Acquisition (DAQ) unit. The final phase includes the testing and validation of the developed implementation against selected threats. Results from this phase can be fed back to improve the effectiveness of all previous phases.

4.3 Baseline and Context

The proposed design thinking approach is applied to real-time condition monitoring (CM) application in an industrial environment. CM refers to the acquisition and processing of data which indicates the status of a machine over time [146]. It enables the identification of recommended maintenance strategies based on the actual condition of the monitored assets, rather than at pre-determined intervals. This allows a Condition – Based Maintenance (CBM) strategy to be implemented [151].

An appropriate CM approach consistent with a CBM strategy involves equipment audits, cost benefits analysis, monitoring method selection, reliability and critical audits, data acquisition and analysis, determination of appropriate maintenance actions, and review processes. A typical condition monitoring system for machine tools comprises of sensors, a data acquisition (DAQ) unit or microprocessor, a host computer, and adequate software [152] [153] that may also be compactly available as a data logging device. Signals acquired via the DAQ unit are transmitted and processed by dedicated software, which enables the machine health to be determined. More advanced condition monitoring may also involve prognostics, and maintenance action determination [153]. Web services allow multiple users to view data on the same network or over the internet. In wireless sensing, sensor data can be transmitted to a DAQ unit, which in turn may be radio frequency-enabled, enabling further transmission for remote data hosting and processing. Remote monitoring systems (RMS), which employ network communication between monitored machinery and back end systems or involve retrofitting monitored assets with a communication device [153].

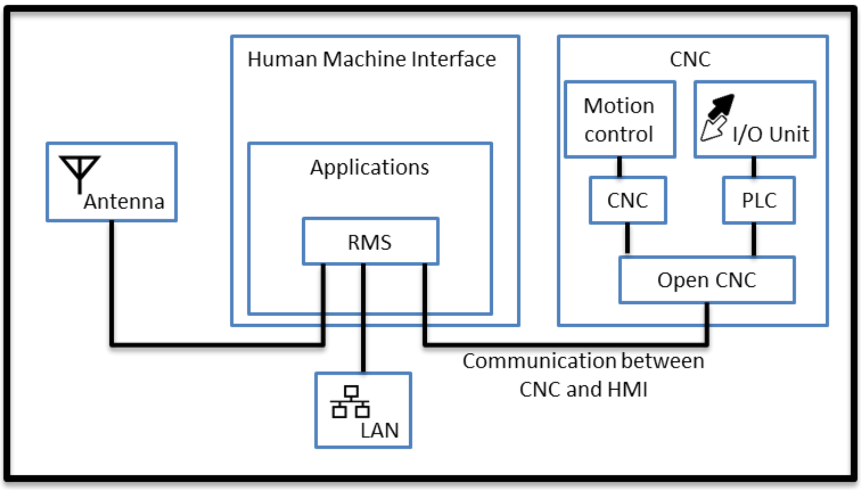


Figure 10: Example of remote monitoring system [153]

Figure 10 shows an abstract example of such a system, where monitored parameters relevant to the machine operating status are transmitted to the remote server of the manufacturer. Alert messages can be set to be generated and sent when some abnormality is detected, which may even be related to non-functional issues, for example in cases that a data buffer reaches a specified level, or that certain time has elapsed since the last transmission. Prime developments contribute to the concept of closed loop product lifecycle management (PLM) via connected products for upgrading the value proposition of product usage in operating environments [154]. However, the integration of IoT technologies in such products creates additional vulnerabilities for the hardware, software and networks of such environments, and this applies to IoT-enabled production machinery too. For this reason, the integration of IoT in manufacturing and specially on legacy machinery, requires a re-thinking of the design IoT approach to security [155].

IoT technology creates data streams that update the value proposition of using the product in operating environments [154]. This connectivity applies to production machines and generates additional vulnerabilities. Therefore, integration of IoT on legacy production machines requires a re-think of their security design [155].

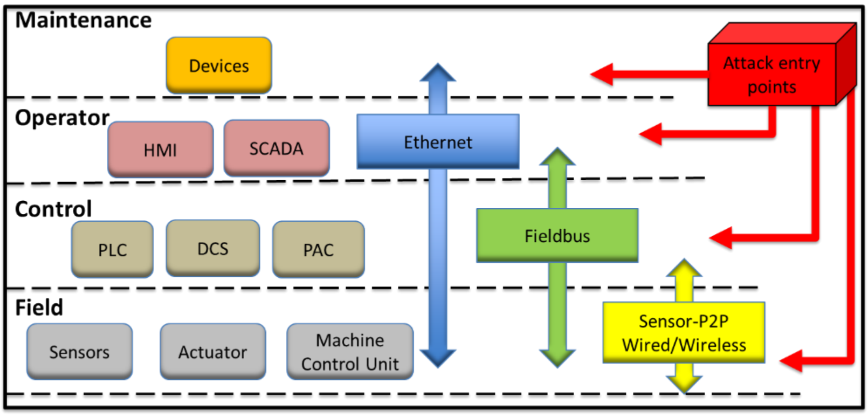


Figure 11: Legacy machine tool monitoring system attack entry points

Figure 11 offers an abstract view of a machinery monitoring system, highlighting potential entry points for security attacks, assuming three standard communication protocol families, namely wired or wireless peer-to-peer (P2P), fieldbus and Ethernet, as part of stage one of the design thinking approach. The involved networking allows the exchange of data through Programmable Logic Controllers (PLC), Distributed Control Systems (DCS), Programmable Automation Controllers (PAC)s, and Human – Machine Interfaces (HMI)s on appropriate devices for monitoring, maintenance planning, and action execution.

4.4 Threat Analysis

This section provides an overview of threat analysis for industrial environments and monitoring systems. This mapping can be looked at from the viewpoint of the ISA-95 reference architecture, as adapted and mapped in five layers by the European Union Agency for Network and Information Security (ENISA) for the security of intelligent production [156]. In detail, the field level of Figure 11 corresponds to Level 1, the control level to Level 2, the operator level to Level 3, and the upper level refers to the application context. The upper level (Level 4) in this case refers to interfaces exposed to devices accessing maintenance management and planning software and services. Unless the permeation of trust in such an architecture is duly considered, IoT-enabled industrial monitoring systems create increased security risks.

This second stage includes recommendation on information security management system such as the ISO27000 family of standards (ISMS, ISO/IEC 27001 [157]), where the threat identification, as part of security risk assessment (ISO27005) [158], is central to devising a security approach. Security risk assessments in organisations can be carried out via a sequence of actions, including identification of threat sources and characteristics. System vulnerabilities can consider as attack events which depending on the results, may cause adverse impacts, reason because vulnerabilities should need to be quantifying and converted into risk mapping [148]. However, such recommendations are not specific enough to cover legacy monitoring architectures for production machinery. Approaches relevant to cloud computing information security risk management [159], would be highly relevant to the domain studied here, but would still need be considered in the light of specific application domain characteristics.

Lessons learned from other domains, such as finance, wherein cyber-attacks were already the prime source of bankrupt, highlight the need to provide guidance to identify, assess and evaluate potential risks in order to prevent future domain-specific breaches [160]. Nevertheless, despite the growing body of work on IoT security, threat identification cannot be completed without application domain considerations. In this research, legacy production machinery and their monitoring systems are the application domain of interest.

The first step towards designing a security approach tailored to a specific type of systems is to understand the nature of potential threats that such a system would be open to.

In this regard, ENISA has produced a threat taxonomy for Industry 4.0 [156], which classifies threats into (a) nefarious activity or abuse; (b) eavesdropping, interception, or hacking; (c) physical attack; (d) unintentional or accidental; (e) failures or malfunctions; (f) outages; (g) legal; and (h) disaster.

After defining the application domain, the research proposes three categories of threats: human interaction threats (HIT), advanced technical threats (ATT) and physical threats (PT). A differentiating factor between human-machine operating interactions and the rest is the actual nature of the operation: specifically, all automatic operations are excluded from human-machine interactions while semi-automatic and manual operations that require human intervention are included within human interactions. Software and network systems entry points are difficult to enumerate and are subject to change while, hardware entry points are fewer and moderately well determined. The hardware attacker's goals can target information leakage [161], tampering [162], denial of service (DoS) [163], and cloning [70]. For each threat type a threat analysis is required for identifying activities which may generate relevant vulnerability to be exploited. Threats exploiting vulnerabilities may cause direct adverse impact in system functionality or cause indirect harm on data integrity and network function. The potential harm that each one of these threats may cause when exploiting system vulnerabilities is assessed by rating the impact in categories such as those recommended in the National Institute of Standard and Technology (NIST) [148] (Table 3). For specific application needs, risk levels can be adapted to produce finer risk granularity if needed. The likelihood of the identified risks is further assessed (Table 4) and the final risk impact is quantified as the product of risk impact and likelihood (Table 5). IoT-enabled production assets create enhanced production data flows and therefore, DFD is a fitting model to study security vulnerabilities of key system entities. DFDs employ symbols for key processes and entities:

- External Entities (EE), considered as end point of a system.
- Processes (P), such as system or unit functionality.
- Data Flows (DF), i.e. ways to transfer data.
- Data Storage (DS), such as database or files for recorded information.

Table 3: Impact rating

High (H)	The threat is unacceptable. Immediate measures for reducing the risk to data or system integrity should be taken.

Medium (M)	The risk may be acceptable over the short term. Countermeasures to reduce the risk should be implemented.
Low (L)	The risks are acceptable. Measures to further reduce risk or mitigate hazards should be implemented in conjunction with other security and countermeasures, for example upgrades to reduce data integrity risks.

Table 4: Risks likelihood (Chance rating)

High (H)	The threat-source is both highly motivated and sufficiently capable and the countermeasures to prevent exploiting the vulnerabilities are ineffective.
Moderate (M)	The source of the threat is motivated and capable, however some countermeasures in the short time could hinder the success of exploiting the vulnerability.
Low (L)	The threat-source lacks motivation and capability, and the countermeasures are enough to prevent the hazard.

Table 5: Score rating (SR) = Impact rating x Chance rating

Impact → →				
Chance → →		Low (L)	Moderate (M)	High (H)
	High (H)	(H) Chance (L) Impact	(H) Chance (M) Impact	(H) Chance (H) Impact
	Moderate (M)	(M) Chance (L) Impact	(M) Chance (M) Impact	(M) Chance (H) Impact
	Low (L)	(L) Chance (L) Impact	(L) Chance (M) Impact	(L) Chance (H) Impact

The score rating matrix (Table 5) allows consideration of how to respond to the identified risks and definition of any countermeasures especially for those that are most likely to occur. Those risks evaluated as a high chance (Table 4) along with a high impact (Table 3) should be addressed as killer risks. These risks are very likely to occur and will have a significant impact at the workflow level and ultimately costs. As result is a structured way of prioritising security risks and therefore potential recommended actions and investments to address them. This analysis is a necessary step to establish a sound baseline for designing an approach to increasing the level for monitoring system security, when upgrading legacy equipment with IoT devices, as introduced in the next section.

4.4.1 New threat classification scheme for IoT-enabled production environments

When designing a security approach tailored to a specific type of systems, the challenge is to understand the nature of potential threats that such a system would be open. Table 6 shows an overview of the most common causes of data compromise in industrial applications based on literature analysis but can be revised to serve specific interests/concerns depending on the domain of the application. These threats are entry points for an attacker which can interface with the attack target. Therefore, such an analysis makes easier to design and develop a systematic approach to security. In the present work, it is used to establish a sound baseline for designing an approach to increase the level of monitoring system security, when upgrading legacy equipment with IoT technology, as introduced in the next section. The table provides a threat classification scheme along with threat taxonomy and risk impact quantification and applicable DFD modelling entities. Risks with a high chance and impact that could occur should be considered a priority in the design of mitigation mechanisms. The risk quantification in the tables is indicative and the actual risks in a specific implementation are likely to vary. Such a table can be filled in with proper impact quantifications only after giving an application context and that in its current form is generic and preliminary and that it needs to be revisited in a given application context which is specified into the next chapter.

Table 6: Threat classification

IoT-Enabled Production Environments: Threats Taxonomy										
Activity	Threat types			EXTERNAL ENTITY (EE)	DATA FLOW (DF)	DATA STORE (DS)	PROCESS (P)	Impact Rating	Chance Rating	Score Rating
	HIT	ATT	PT							
Negligence	X						X	M	M	M

Social Engineering	X			X			X	H	L	M
Errors & omissions	X						X	H	L	M
Physical Intrusions	X		X		X	X	X	H	L	M
User Misuse	X			X			X	H	L	M
Unauthorised remote accesses	X						X	H	L	M
External hardware	X						X	H	L	M
Physical destruction	X		X				X	H	L	M
Command injection		X			X		X	M	L	L
Denial of Service (DoS)		X			X	X	X	H	M	H
Signal replaying		X			X	X	X	M	L	L
Cloning		X			X	X	X	H	M	H
Remote switch off		X			X		X	H	L	M
Signal blocking or jamming		X			X		X	H	L	M
Reverse engineering		X	X		X	X	X	H	L	M
Side-channel		X	X		X	X	X	H	L	H
Wireless zapping		X			X		X	M	L	L
Software	X	X			X	X	X	H	L	M
Electromagnetic interference			X				X	M	L	L
Cable cuts			X	X			X	H	L	M
Power fluctuation			X				X	M	M	M
Voltage spikes			X				X	H	L	M
Installation errors			X				X	M	L	L
Tampering			X		X	X	X	H	L	M
Takeover of an authorised session			X		X	X	X	H	L	M
Internal attacks			X		X		X	M	L	L

4.5 Application and threat modelling

Threat modelling is a structured approach that identifies potential security threats, assessing their risk and providing the necessary countermeasures. It can be defined as the systematic review of application features and architecture from security point of view. The modelling of the threats involves the identification of the assets in a structured process, identifying the potential threats and then categorising them and determining the appropriate mitigation strategies. The process provides a structured approach to identify and classify threats based on the system software and hardware components, flows of data and on the boundaries of trust (borders within which there are security criteria). Unlike penetration testing or fuzzing, threat modelling can be performed during the system design phase making it independent of code development.

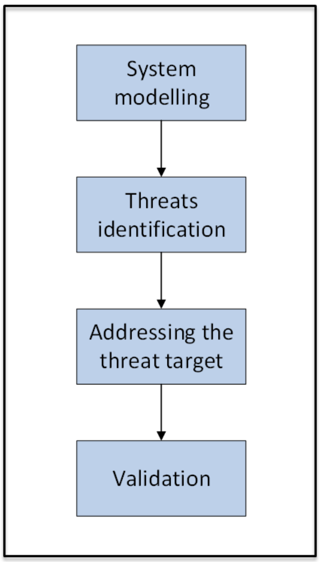


Figure 12: Application and threat modelling framework

Introduced in the software development life cycle, threat modelling can help ensure security already in the design phase of an application, reducing costs and the necessary subsequent security corrections in the project. Even existing systems can benefit from this process. Unknown or unresolved security problems can be identified in the system and a risk classification can be applied to identified vulnerabilities. The process can also be adapted to development practices such as Agile [164]. Identifying the threats and deciding how to proceed makes the requirements clear and allow to target efforts to security properties. Security requirements may also need to take into account additional threats whose resolution may be too complex and expensive. The threat modelling process is identified as a set of steps that achieve sub objectives rather than a single activity (Figure 11). It consists of 4 steps: system modelling where it is require to create an abstract model of the current system; threat identification phase, which aim to define the threats nature and background; addressing the threat target which aim to define what is the target of such a threat and the current countermeasure practice; and finally the validation of the threat mitigation mechanisms.

Data flow diagrams (DFD) are used in many threats modelling processes to provide a consistent and compact way to model the data flows present in an application through the use of six distinct forms that represent: the process, the multiple processes, the external entity, the data archive, the data flow, the data storage and the privileged perimeter (trust boundary).

4.6 Threat mitigation

The Information and Communication Technology (ICT) infrastructure cannot be considered 100% secure; even if there are measures and lines of action that any manufacturing company and organisation can reasonably adopt to significantly reduce the risk of a possible computer intrusion. Through a detailed and comprehensive analysis of local attacks and threats, enterprises should be able to recognise attack target, background and implementing mitigation mechanisms. Hence, government organisations are keen to provide guidelines for protecting the system enterprise from cyber-attacks [165]. Usually, to prevent common attacks, typical mitigation mechanisms need to be adopted like cryptography techniques, secure authentication protocols, a physical system for improving resistance to tampering, malware detection systems. For example, this research introduces and implement a novel authentication protocol consists of 5 phases named:

- Phase 0: Start.
- Phase 1: Log identity authentication.

- Phase 2: encrypted Communication.
- Phase 3: secure Connection.
- Phase 4: Authentication.

The motivation is to increase security complexity, requiring agreement on two parameters for each phase. In addition, each stage uses AES encryption, which is a limitation for IoT devices due to low computational capabilities and contributes to additional security. The mitigation mechanisms following the novel authentication protocol will be described in more detail in Chapter 6.

4.7 Testing and validation

Testing and validation are the control activities comparing the result phase of the development process along with the product requirements, generally in compliance with the initial requirements. Results from this phase can be feedback to improve the effectiveness of all previous phases. To demonstrate the application of the approach, two cases were considered – Denial of Service (DoS) test and clone attacks test. The functional aim of the test it to deliver uninterrupted monitoring service.

Chapter 7 details two attack scenarios in the context of analysing the selected application case for demonstrating the application of the new approach. In particular, the implementation and testing of mitigation mechanisms against denial of service (DoS) [166] and clone attacks [70]. Therefore, the design of an innovative security implementation of an IoT endpoint device, which is managed by a new authentication protocol is consistent with the isolation principle and integrated into a prototype IoT DAQ unit device as presented in more detail in Chapter 6.

4.8 Chapter summary

This chapter introduces an original comprehensive and systematic design approach for IoT device security adopted in attaining the aim and objectives of the research. Such a structured approach is defined through an evaluation of possible attack entry points in current industrial control and monitoring systems.

A taxonomy of threats has been introduced along with threat analysis approach to identify activities which may generate relevant vulnerabilities which may cause a direct adverse impact on system functionality or cause indirect harm on data integrity and network function. The threats classification makes it easier to design and develop a more systematic approach, for increasing the level of system security, when upgrading legacy equipment with IoT devices which will be introduced in the next chapter A systematic classification of typical potential threats within the digital production environment has been introduced, as well as a risk-based approach for assessing the impact of exploiting system vulnerabilities. The approach is applied in next chapter which outlines an abstract application model for connected legacy production machinery.

5 APPLICATION MODEL AND DATA INTERFACES

Having introduced the new systematic design thinking approach for IoT security, the aim of this chapter is to apply it on pilot implementation. The focus is on machine tool monitoring, as a representative example of legacy production machinery. This section comprises the following steps:

- Definition of an abstract application model of machine tool monitoring, identifying interfaces (links) between components, which could also be potential targets for a security attack.
- Develop a threat model for the studied system, adopting an attack tree modelling approach.
- Produce an implementation instance of the proposed approach employing rapid prototyping IoT device components for machine tool monitoring.

5.1 Application model

The application instance studied is that of monitoring machine tools. The application model considers the key components of a machine tool monitoring system and data exchange interfaces (connections), prior to the implementation of the proposed IoT security approach, as illustrated in Figure 12. Following a representation similar to [167], Figure 12 shows the concept of a production environment equipped with IoT technology. The local architecture consists of the workplace environment with communication technologies and IoT-enabled DAQ unit, which includes three modules. The control unit module is in charge of processing and analysis operations and receives real-time data from the sensor module that is physically attached to the machine. The collected data may then be passed to external or visual user interfaces. Finally, data are transmitted to either the cloud-based system, the System Control Unit (SCU) or both via the communication module. While the local architecture enables data transfer from the machine tool to the user/external interfaces, the remote architecture stores, manages, analyses, and visualises data on a dashboard to aid future actions. Such a remote architecture involves communication technology enables data transfer to the cloud-based system for processing and analysing data and defining actions to the user devices in retrofit. Inside the cloud, the data is processed, recorded and analysed for defining performance actions which needs to be implemented to the machine tool for maintaining high quality of the products and avoiding machine breakdown.

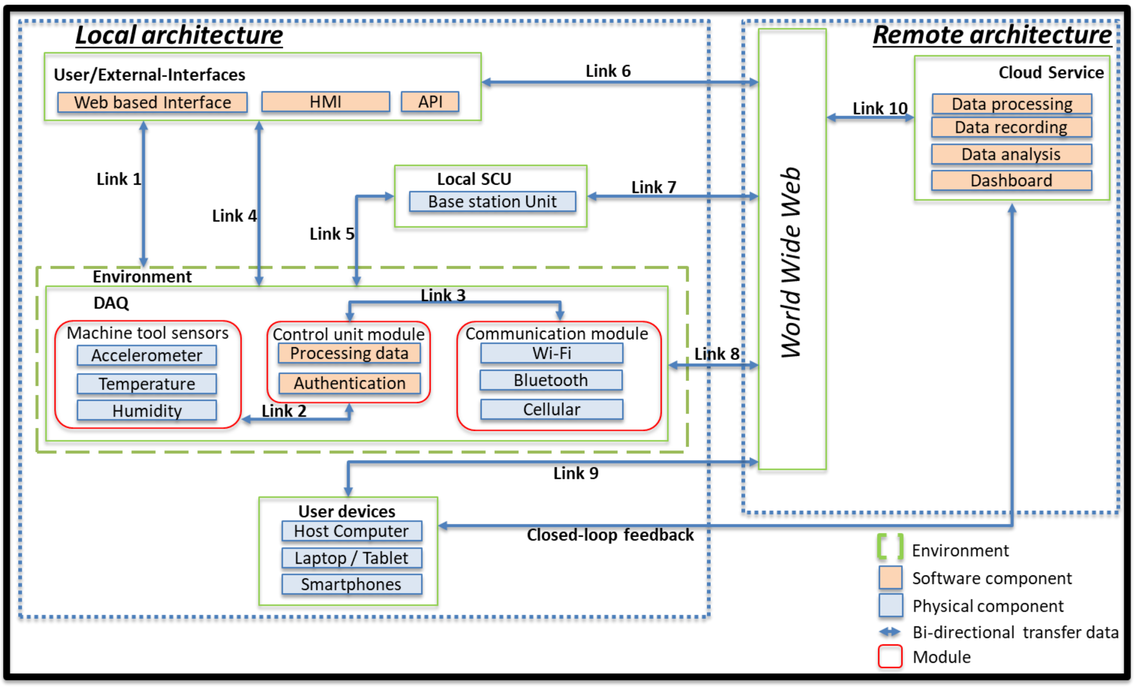


Figure 13: Application model of the connected legacy production machinery

Such functionality which resides inside the local architecture is offered through the cloud to end-user devices. The data flows across the links are:

- Link 1: The manufacturing environment includes machine tool, the DAQ unit modules with access to configuration web-service to deliver configuration and management services.
- Link 2: Machine data acquired from the sensor module are transmitted to the control unit module.
- Link 3: Authentication mechanism are processed into the control unit module for transmitting data to the communication module.
- Link 4: The DAQ unit provides a user-interface to visualise and manage the acquisition of data in real-time and processing authentication mechanism which enabled monitoring service operations.

- Link 5: The DAQ unit and the SCU exchange data between the sensor module and the local architecture.
- Link 6: User/External interfaces offer data visualisation and support or trigger proper actions.
- Link 7: Cloud access is employed from the SCU to offer machine data management to users.
- Link 8: Internet communication is established between the DAQ unit and the cloud system.
- Link 9: User devices are communicating with the cloud or server through the internet, exchanging information relevant monitoring information.
- Link 10: Data management and visualisation services are made available to the user.

These mapped links could be considered as possible attack entry points for the pilot implementation production environment scenario. Consequently, link 1 is considered a physical attack entry point, which may compromise the integrity of hardware equipment's like devices, sensors, and data. Specifically, the web-based interface connection is an attack entry point for software threats (e.g., trojans and viruses), as well as DoS and remote access control attacks. In order to gain access to the interfaces, physical access to the machine and, device is required. This may expose the users to side-channel, reverse engineering, or cloning attacks, as well as electronic malfunctions due to voltage spike, electromagnetic interference and power fluctuation. Therefore, links 2 and 3 are physical attack entry points for tampering and physical intrusion operations, where cloning, side-channel and reverse engineering techniques could compromise the system. Links 4 and 5 offers opportunity to, software attacks, command injection, unauthorised remote access, DoS and cloning attack entry points. Links 6, 7, 8 and 9 are network attack entry points which may cause breakdown or system process malfunction to the network via ATTs such as DoS, command injections, reverse and social engineering attacks. Finally, link 10 represents an entry point for error and omission, unauthorised remote access, social engineering, command injection, DoS, and software attacks. HITs are relevant to all interfaces and components and may cause data loss, process malfunctions, and network breakdown.

5.1.1 Data Flow Diagram for the application model

Having available an abstract application model along with a map of its real-time data exchanges, facilitates the modelling of threats for the specific application and data interfaces. It is used to map the data transfer between the subsystems introduced into the abstract application model and classified such as input /output, and data storage elements. Such classification allows better identification of attack entry points and a better understand the impact related to these attacks.

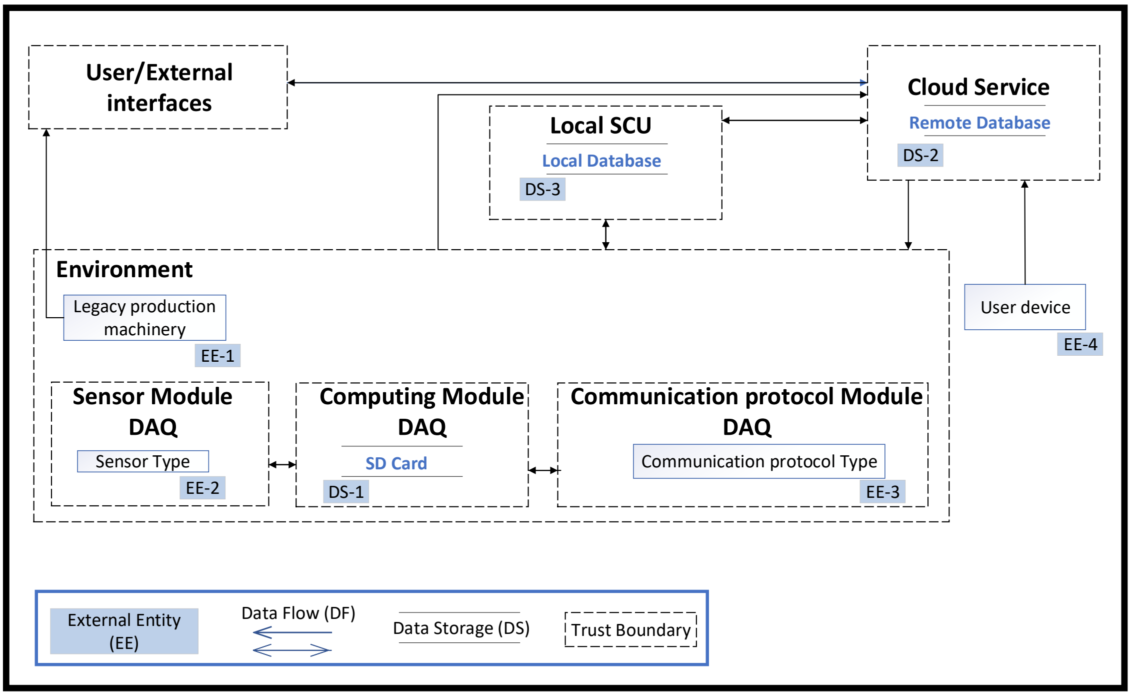


Figure 14: Data Flow Diagram (DFD) of the connected legacy production machinery

Figure 13 shows a simplified DFD concept for IoT-enabled monitoring in a manufacturing environment. The trust boundaries of subsystems are denoted with dotted line rectangles; external subsystems are represented by solid line rectangles; arrows indicate data flows; interfaces with external entities and storage are marked with a solid coloured rectangle. A security approach aims to protect the trust boundaries and data flows, which can be targeted by threats, so as to result in enhanced permeation of trust between components and subsystems. The modelling of these threat goals is the subject of the next section.

5.2 Threat Goals Modelling

Understanding the trust boundaries between subsystems making it easier to understand potential attack targets. In order to devise mitigation mechanisms, it is of interest to understand the specific goals of an attacker when they are pursuing attack targets. Attack tree modelling is a common structured approach to illustrate the main potential goals of an attacker [129]. The top node of an attack tree is the key attack target. Lower level goals and individual malicious activities, which may contribute to reaching that goal, are located below the main node. Steps between the lower nodes and the top node depict intermediate states or attacker sub-goals. In this section threat goals are analysed by means of attack tree modelling for the machinery monitoring application. The main goals in this example are:

- gaining access to the network,
- gaining access to the communication for the supervisory and control architecture [168]
- and modifying the DAQ unit system [169].

The attack trees are defined in the higher-level threat modelling (e.g. by means of tables such as Table 5 and Table 6) and provide insight into how an attacker may succeed in reaching the attack goals. Each of the above three attack goals are modelled by means of attack trees next.

5.2.1 Network access

In order to gain access to the network wherein the monitoring system operates, an attacker can use malicious actions to compromise, delay or gain access to data devices or server systems connected with the network.

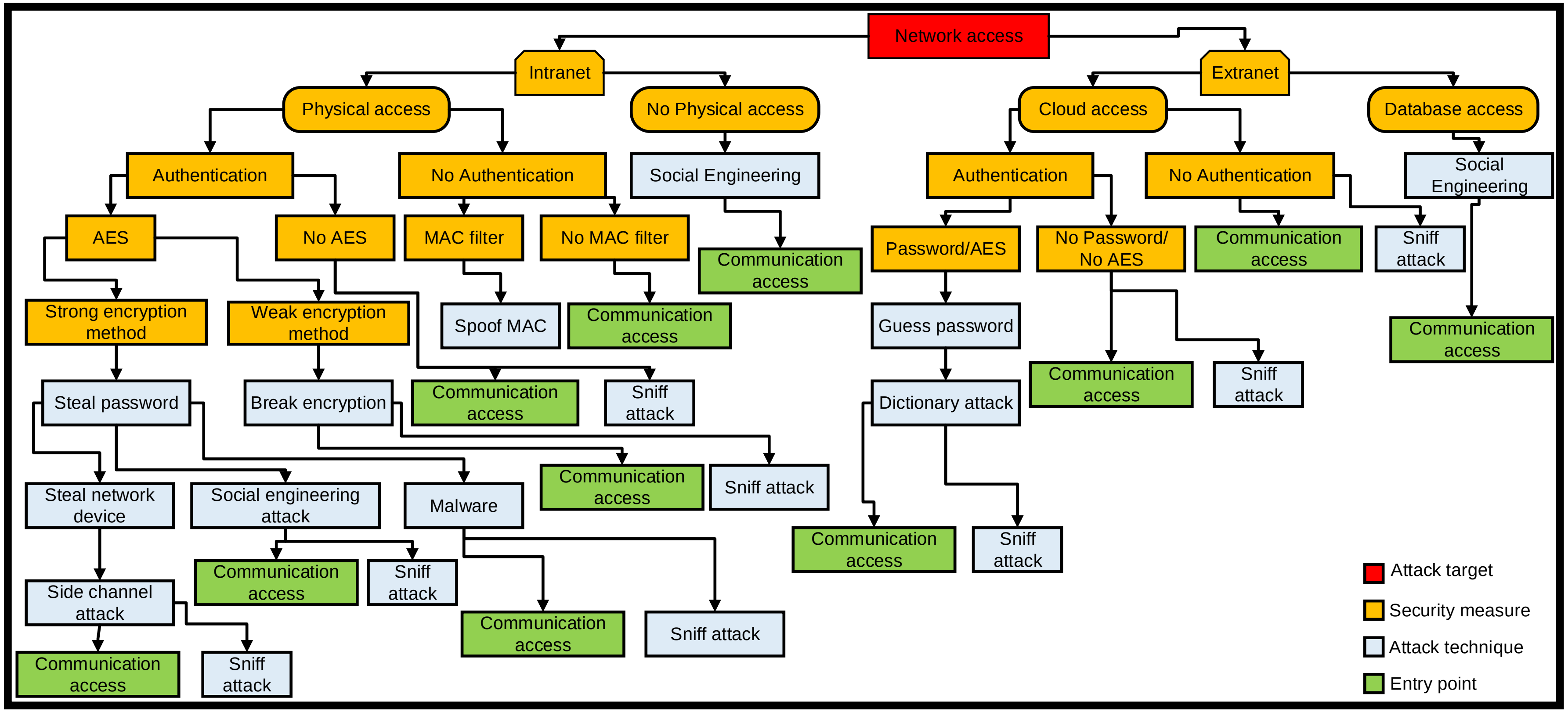


Figure 15: Network attack access tree

Figure 14 shows the attack tree that models the network access threat goals. Usually, companies may have public and private networks, which are subject to access rights and are exposed to staff, customers, suppliers or partners. Within the intranet there may be parts of the architecture which can be modified by access to the hardware for upgrading firmware, updating software and replacing components. However, other entities do not require physical access to the architecture and are modified remotely, changing the method used by the attacker to gain access. Upon gaining physical access to the hardware of the architecture, the attacker can then gain further access to the network through devices, cables or plugs, radio interference or wireless and wired networking means. If an attacker does not have physical access, network access can be achieved via other means, such as the social engineering method [170]. The current typical protection practice is to employ an encryption method and have a Media Access Control (MAC) filter as a security measure. In this case, the spoofing attack technique [171] can be used to gain access to the network. If a strong encryption method is employed (such as Pretty Good Privacy (PGP) [172] or Advanced Encryption Standard (AES)), the attacker can obtain the encryption password through a social engineering method, installing some malware for reading the encryption password, or by breaking into specific network devices via a side channel method. If the system devices are equipped with a weak encryption method, it may be easily broken with cryptography attacks. On the extranet side, the system can be equipped with password authentication. An attacker can guess the password using the dictionary method [173] to bypass the firewall and gain access to the local network.

5.2.2 System communication access

Remote access applications allow ubiquitous supervision and control through networked devices, whilst HMI allow enable control via a front machine panel. An attack may seek to gain access to the communication system to compromise supervisory systems and modify machine parameters.

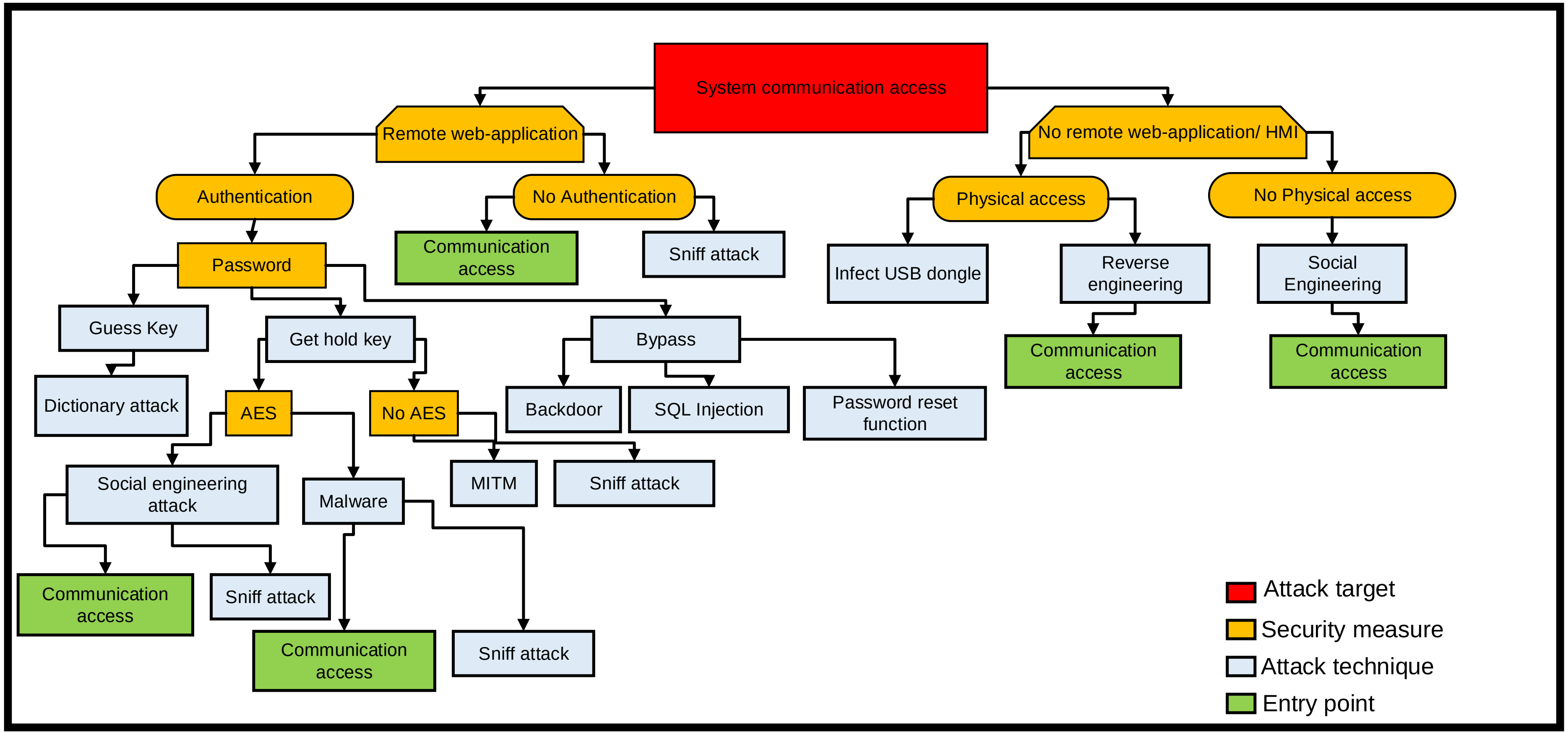


Figure 16: System communication access attack tree

An attack tree analysis for this threat goal is shown in Figure 15. If there is no authentication requirement, an attack can easily succeed to gain access. Instead if an authentication is required, an attack may seek to guess the access key by the dictionary attack method, or bypass the password using a backdoor secret method, such as chipset, cryptosystem and an algorithm Structured Query Language (SQL) injection, a code injection technique, used to attack data-driven applications [174]. When encryption is employed, the attack can obtain the key through a social engineering method or malware injection. Systems without any encryption can be attacked with a Man-In-The-Middle (MITM) method, where the attacker can spoof the system identity, waiting for a user to login and then save the credentials for future access. On the other hand, if physical access to the HMI is gained, the attacker can use an infected USB dongle to compromise the control system [175] or can employ a reverse engineering method to gain access to the communication. One possibility to gain communication access without physical access to the machine is the social engineering method.

5.2.3 Data Acquisition (DAQ) unit access

The modular DAQ unit operates in intranet or extranet control for machine data. Therefore, it is a primary target for compromising manufacturing systems. Figure 16 displays the attack tree to acquire access to the modular IoT DAQ unit. The side-channel method is one of the simplest ways to acquire DAQ unit access to make changing into the hardware asset as well as installing new firmware or patch. Using the network, the attacker can use SQL injection [176] for accessing to the user device or gain authentication to it in order to infect the DAQ unit with malware, viruses, and through the replay attack to spoof information. Furthermore, the attacker can target gaining remote access to the DAQ unit, after remotely logging in credentials, and launch a Denial of Service attack to flood the available bandwidth. Alternatively, by accessing the sensors, the attacker can compromise hardware or software components to tamper the sensor in order to compromise the normal operation of the DAQ unit.

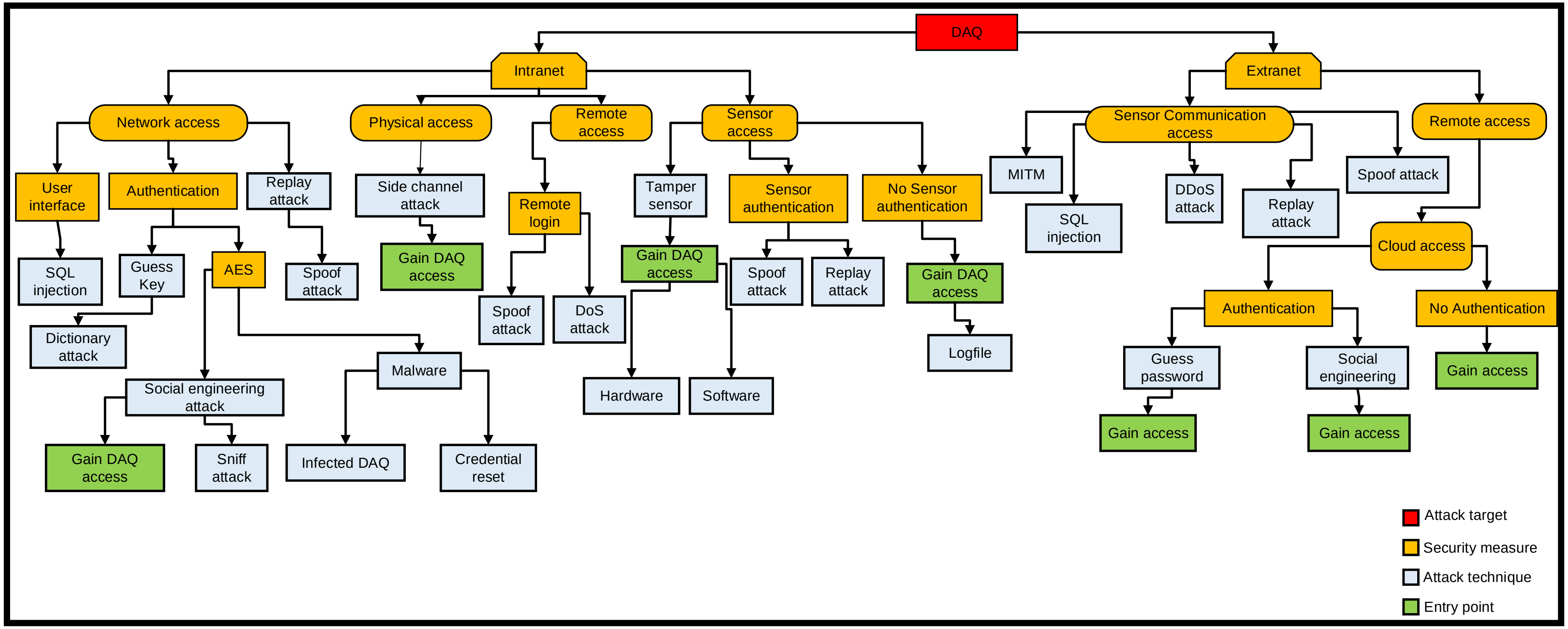


Figure 17: DAQ unit access attack tree

If the sensor authentication is not employed, the attacker can gain direct access to the DAQ unit using logfiles to spoof data. From the extranet side, the attacker can gain access to the DAQ unit via sensor communication access by Man-In-The-Middle method, SQL injection, or spoofing sensor information, replay attack method, or through the Distributed Denial of Service (DDoS) technique. Also, the attacker can remotely gain authentication to the cloud and control the DAQ unit.

5.3 Risk-based impact assessment

The possible impacts of these three attack goals, namely network, system communication, and DAQ unit access, their various potential functional impacts are described with the reliability-oriented approach Failure Mode and Effects Analysis (FMEA) in Table 7.

Table 7: Attack goals and impacts

Attack Goal	Effect Description	Severity	Function codes
Network access	Inability to communicate with the DAQ unit	M	I, U
	Inability to communicate with the Cloud	H	U
	Inability to communicate with the SCU	L	C, U
	Inability to communicate with the User Devices	H	I, U
	Inability to upgrade firmware	L	I
System communication access	Inability to use the HMI	M	I, U, Pr
	Inability to use the DAQ unit modules	H	I, C
	Inability to use the legacy production machinery	M	Pr, Sr
DAQ unit access	Inability to collect correct sensor data	H	C, I
	Inability to protect sensor data	H	C, I
	Inability to send data correctly	H	C, I U

The table identifies potential failure modes in a system and their causes and effects. In particular, the severity level is identified as follows:

- Low (L): minor issues are mentioned which is most likely to be ignored by the user.

- Medium (M): causes dissatisfaction to the user due to degradation in performance.
- High (H): causes instability in the process to such an extent which may cause accidents, and high dissatisfaction to the customer due to a significant impact on performance.

In addition, impacts could affect different functions, which in the case of a production machine could be stated as [177]:

- Pr: Primary, affecting functions required to fulfil the machinery intended output (e.g., production of an item);
- Sr: Secondary, supporting the primary function (e.g., managing coolant in a machine tool);
- C: Control and protective, affecting the ability to control a process (e.g., adjusting feed rate in machining) or protecting workers, equipment, or the environment (e.g., stopping machining after tool breakage);
- I: Information, affecting ability to provide monitoring information for a function (e.g., failure to provide or display temperature reading); and
- U: Interface, affecting the interaction interface between two items.

This makes the understanding of the potential consequences of an attack achieving its goals more tangible and enables the design and development of impact mitigation mechanisms when moving to specific implementation instantiations of the new approach. The above impacts imply that the integrity of the monitoring infrastructure is compromised by such attacks and as a result the monitoring functionality is itself compromised. The system is exposed for example to DoS attacks, which can be set up from different entry points (cloud, external interfaces, user interfaces, local SCU and environment). In this case, the network system is flooded by excessive messages asking the server to authenticate requests that have invalid return addresses. Likewise, the equipped legacy production machine with external devices is exposed to other risks linked to the physical interaction. Performing an attack tree modelling constitutes a structured methodology for approaching security issues and facilitates the design and implementation of appropriate mitigation mechanisms. The next section presents the implementation of the proposed approach in designing, developing and testing the methodology for IoT device security on the pilot case of legacy machine tool monitoring.

5.4 Chapter summary

This chapter presents the third step of the design thinking approach. The abstract application model for legacy production machinery consists of local and remote architecture sub-systems, which may represent attack entry points. Such an abstract model that uses data flow diagram (DFD) to model threats to specific applications and interfaces. This model maps the transfer of data between subsystems by classifying them as input and output elements and data storage elements. Having a clear understanding of the abstract application model make it easier to define potential attack targets, and consequently, design mitigation mechanisms. In order to design mitigation mechanisms, modelling with attack tree diagrams is used to define the main goals of an attacker, which for this research is gaining access to the network, to the communication, and to the DAQ unit. Finally, the FMEA analysis is used to describe the possible attack impact for each attack goal. The next chapter takes into consideration such analysis of threats and introduces application-specific modelling for developing and testing IoT endpoint device security in legacy production machinery monitoring.

6 IMPLEMENTATION OF THREAT MITIGATION MECHANISMS FOR IoT-ENABLED SYSTEMS

This chapter introduces a modular security approach for industrial monitoring operations by decomposing the device into multiple components, each of which contributes to greater security, instead of adding complexity to an existing global security control mechanism. This new approach is managed through an innovative authentication protocol based on the concept of increasing the complexity necessary for the success of an attack while remaining simple to implement and includes the following steps:

- Identification of attack risk mitigation mechanisms for industrial monitoring system.
- A novel design of a modular IoT device for supervisory and monitoring operations.
- A novel authentication protocol, which cascades the complexity of compromising the IoT device security.

6.1 Threat mitigation when introducing IoT in production machinery monitoring

Currently, traditional integrated monitoring systems processes data from production machinery for supporting enterprises decision making. Through monitoring services companies are not just enabled to react immediately on machine failures but also to pre-empt any potential failures through forecasting. Industrial data acquisition solution devices are able to supervise, process, and store data collected from the sensors attached to the production machine. Although, these devices are compact in capabilities and dimensions, most of the time are missing important security provisions. End point security can substantially benefit from the Industrial Internet Security Framework (IISF) [49] principle of component or subsystem isolation. The current market offers monitoring solutions where all functional aspects such as data input and output, data processing, error handling and user interface are all intertwined, rather than containing architecturally separate components. This limit exposes devices to a large list of threats, especially for network and communication categories which in most cases involves the inability to use the entire system and the device itself. The majority of these devices encompass sensors, CPU, and network hub, opening the opportunity for the system to be physical compromised, replaced and cloned in all hardware and software components, if an attacker gains access to the device. Therefore, a new thinking approach is needed for the design of safe monitoring devices that consider the reliability and delivery of the expected functionality of the system as the ultimate requirement.

6.2 Concept prototyping

The proposed modular solution derives from an initial single integrated circuit solution designed for monitoring spindle vibrations, as shown in Figure 18, which includes an accelerometer sensor (Figure 18 – heptagon 1), a dongle USB for Wi-Fi connectivity (Figure 19 - heptagon 2), the single-board computer Raspberry pi 2 as CPU unit (Figure 19 - heptagon 3) in order to facilitate direct monitoring of operations, and a 3300 mAh battery used to power the system unit (Figure 19 - heptagon 4). Furthermore, to protect the system from unauthorised tampering, a protective cover has been designed which protects sensors and CPU unit integrated circuits.

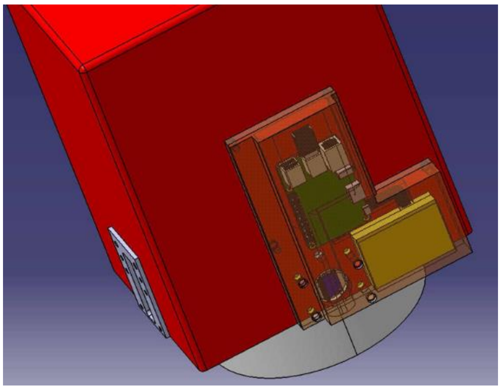


Figure 18: Monolithic IoT data acquisition unit for production machinery

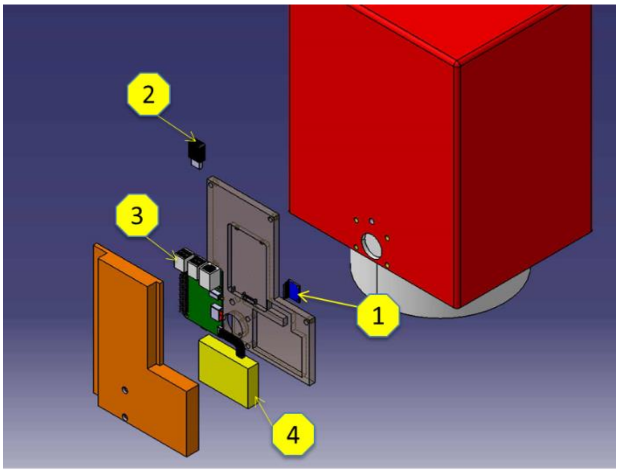


Figure 19: Exploded view of the monolithic IoT data acquisition unit for production machinery

The system is attached to the spindle of the DMG model machine tool and used during machining operations. Although this solution is reconfigurable, smaller in size than industrial monitoring systems, memory is limited (1 GB of integrated RAM) for managing different sensors. Also, a single board solution can be compromised if a module is compromised, for example through a cloning attack.

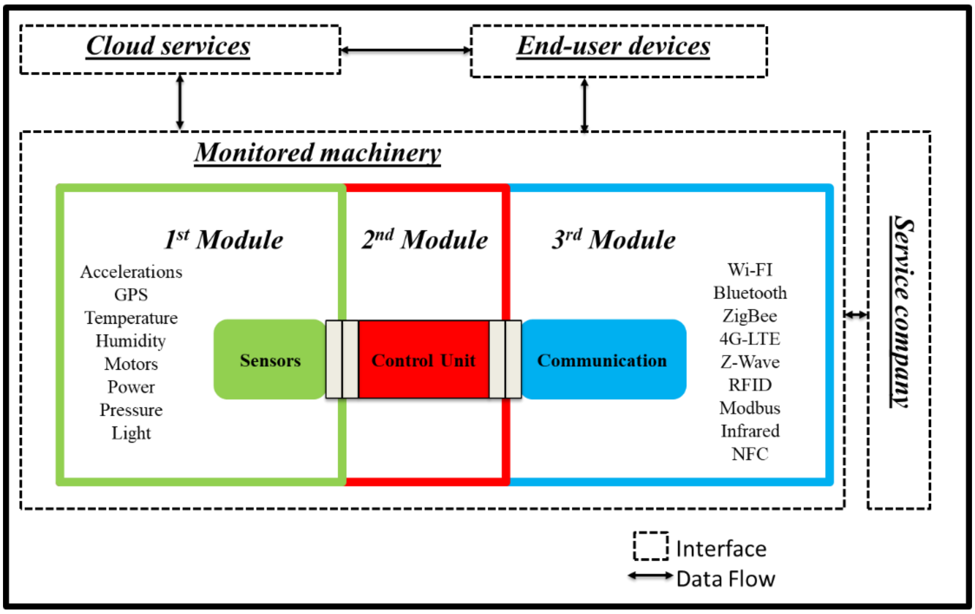


Figure 20: Design of the modular IoT data acquisition unit for production machinery

The proposed design integrates a modular security approach, by de-composing a single-board device into several components, each one contributing additional security, instead of adding complexity to an existing overall security control mechanism. Figure 20 shows the concept of the proposed modular IoT device without yet introducing additional security provisions. The design structures of the device consist of singular modules, indicated as the sensor module or 1st module, the control unit module or 2nd module, and the communication module or 3rd module. This design fitted for legacy production machines including different sensors module and communication protocols. This architecture can be connected to the services as cloud, end-user devices and in local way to the service company. Each module uses the encrypted communication and authentication for both local network and cloud network. The connection diagram of each module of the modular IoQ DAQ unit is presented in Appendix B. The modular prototype IoT DAQ unit is intended to support industry challenges in designing secure IoT units. It consists of a standardised communication interface that uses a hardware and software authentication protocol that allows data access only to authorised users. In addition, the proposed modular device communicates at the Machine-2-Machine (M2M) level and is suitable for cloud interaction. The approach is designed to be auditable so that any misuse can be identified. The proposed concept has the advantage this increases the complexity needed for an attack to succeed, while remaining simple to implement [178]. Consequently, end point security and the principle of isolation is respected, as well as the trustworthiness requirements. If one of the end points fails, the whole system will not be affected but will be still able to be isolated from the current threats and delivery the intended functionality. Collected data or processed information, such as alerts, can be shared with available applications via end-user devices or sent to the cloud or a service provider. The modular IoT DAQ unit uses only a single sensor or actuator and a single communication component at a time. Therefore, limiting the size, power and memory to process data is critical, offering the modular IoT DAQ unit the opportunity to flexibly configure hybrid solutions.

6.3 Modular IoT DAQ unit developed concept

The proposed modular design (Figure 21) supports security by introducing additional modules managed by a dedicated authentication protocol.

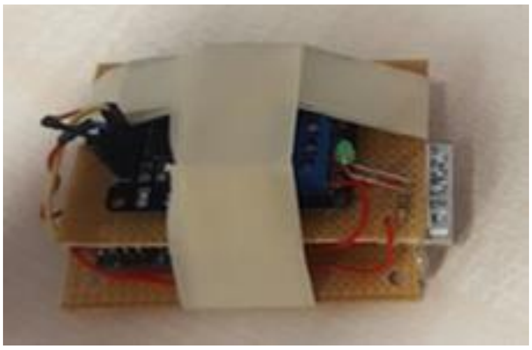


Figure 21: Modular IoT DAQ unit device hardware - Sensor module

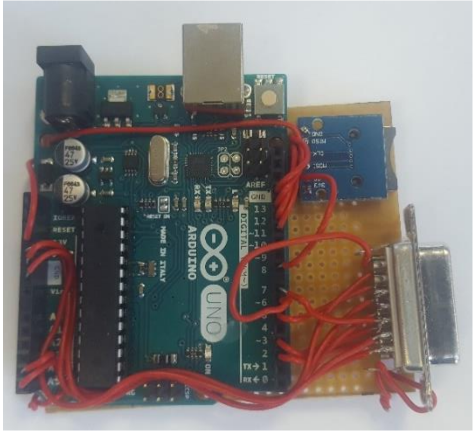


Figure 22: Modular IoT DAQ unit device hardware - Control Unit module

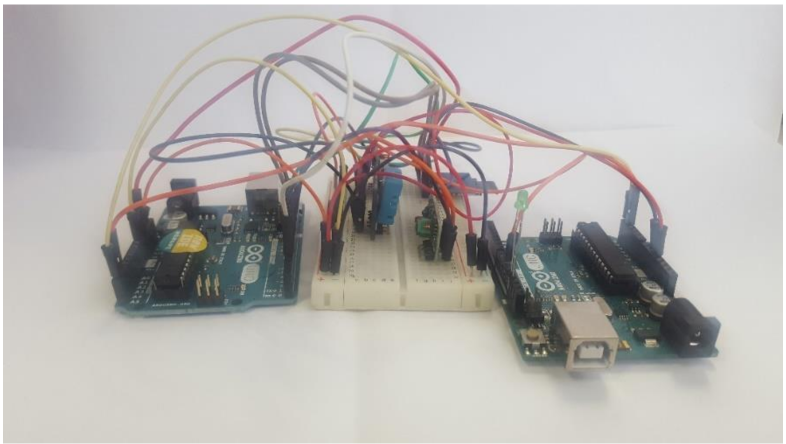


Figure 23: Modular IoT DAQ unit device hardware – Communication module

This design consists of a sensor module or 1st module (Figure 21) equipped with I / O ports, a communication module or 3rd module (Figure 23) with various communication technologies (e.g. InfraRed (IR), Radio Frequency (RF), Bluetooth) and a control unit module or 2nd module (Figure 22) which consist of CPU and memory and the power options . Each of the modules may be considered to extend the functionality of the previous one, however, in integrated IoT devices, their trust boundary encompasses them all together. Furthermore, one of the key features of the developed modular IoT DAQ unit is that it can work as a switch between different communication protocols, as presented later. In addition, multi-connectivity can be further exploited, not only as an alternative communication means, but also as a mechanism to increase security, by enabling the device to react when detecting a threat via switching communication protocols, each one featuring its one security provisions. In addition, the modular IoT DAQ unit has the advantage of being easy to maintain or replace. These features allow building a practical and custom monitoring IoT device with security provisions

6.4 The New LCCA Authentication protocol

The proposed modular IoT DAQ unit employs an authentication protocol which cascades the complexity of compromising its own security while allowing access for authorised users. The type of such modular security barriers may be adaptive, adding further complexity to the task of any mechanism designed to attack an IoT-enabled solution. Figure 24 and Figure 25 describe the authentication protocol for the IoT modular DAQ unit. In detail, the flowchart in Figure 24 defines the process flow, while the data flow is showed in Figure 25 via DFD. The protocol is divided into four main phases called: Log identity authentication, encrypted Communication, secure Connection, and Authentication, and will be referred to as LCCA. Each of these phases of the LCCA protocol employs AES cryptography and contributes additional security to the system. If one of these phases does not work, results in issuing a security alert. An alarm will be sent to warn the service company about malfunctioning of modular IoT Unit. The LCCA protocol includes a set of passwords, baud rates, keycodes and frequency values used to advance through the four phases and can also be applied for communication between the control module and the other two modules.

The LCCA flow for the communication between the sensor and the control unit module is described below.

Phase 0: Start

The system is in sleep mode (START), waiting for the first connection. Therefore, the system initialises the set of keycodes, passwords, baud rate, and frequency relationships to be used.

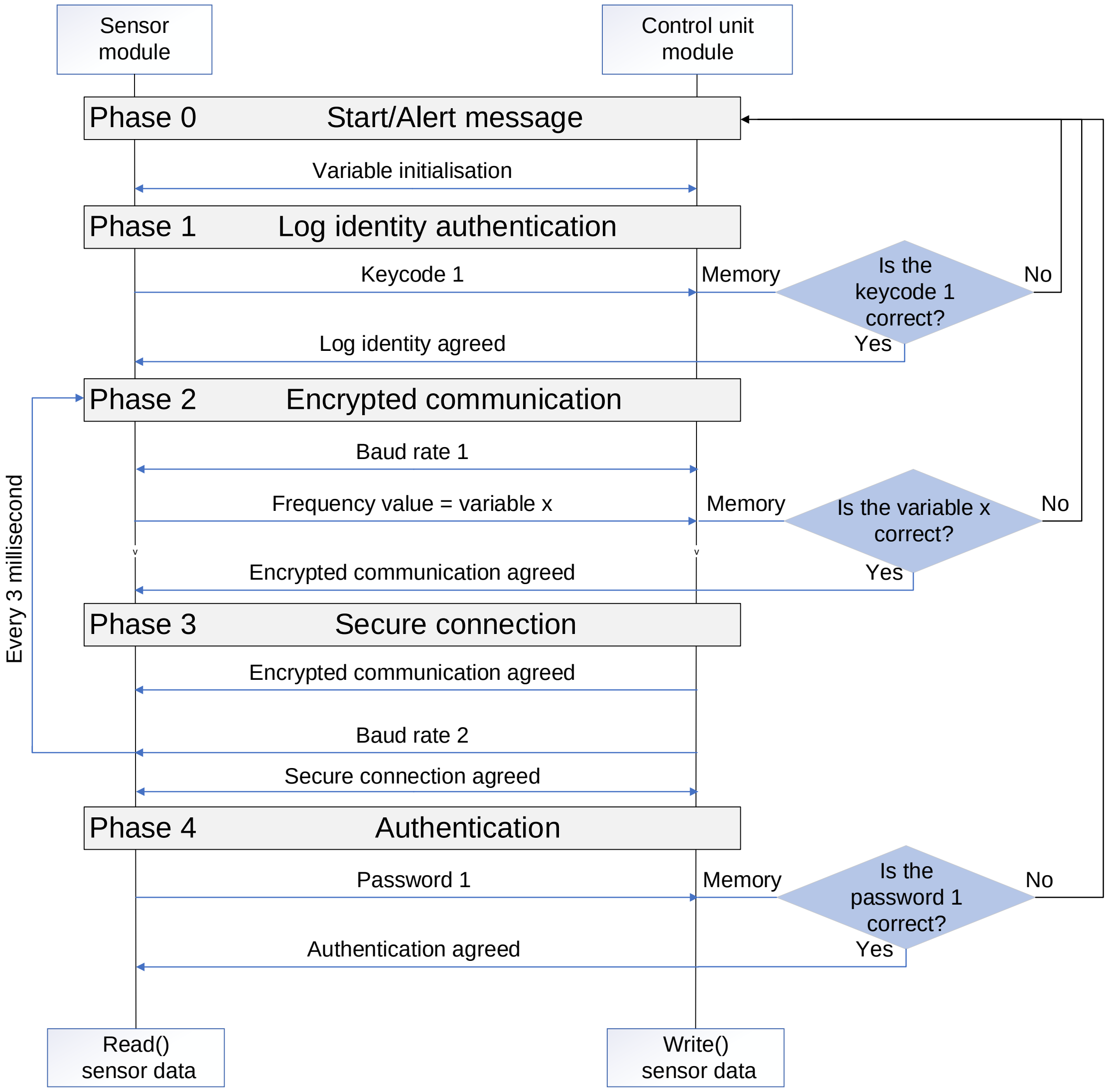


Figure 24: Log identity authentication, encrypted communication, secure connection, and authentication (LCCA) protocol

Phase 1: Log identity authentication

This phase handles the log identity between the modules. Specifically, if the control unit module recognises the sensor module log identity, the protocol proceeds, otherwise the process freezes.

For this example, the identities of the registers (and for the same purpose baud rate, frequency values and passwords) are pre-stored in a dictionary built into each module, but algorithmic approaches to dynamically create them could be employed instead. With this first phase the approach mitigates common issues associated with physical attacks where the attacker can try to get physical access to the hardware device and manipulate or change its parameters. In the case of a cloned or stolen identity, the control unit module can generate a new sensor or communication module keycodes which can be distinguished between the original sensor and the cloned sensor.

Phase 2: Encrypted communication

This step consists of setting the control unit module to an agree baud rate value with the sensor module, otherwise the control unit module will close the connection and set the system to sleep mode. This allows to share signals, information and a common password. The baud rate is expressed in bit/s, representing the rate of which information is transferred through a communication channel between two modules. The LCCA algorithm sets the initial speed (baud rate 1) at fixed time intervals (in this example, 3 ms) which changes the frequency of the control unit with a new speed value (baud rate 2), based on (using previous frequency value as shown in Figure 24) a formula agreed in advance between the modules. Upon agreement, data exchange progresses, and all data transfers are encrypted. Any mismatch between the two, which may arise as a result of a security breach, will pause communication and set the system to sleep mode, issuing an alert. To prevent a vulnerability, the baud rate needs to change each time a new step is running. With the agreed communication, the protocol moves onto the next phase, otherwise it closes the connection and returns to phase 1. Two approaches can be used to control the baud rate value. One approach is recording the value within a processor register device. The second requires that the rules for setting the new baud rate must be updated every few seconds. Therefore, the second approach offers advanced protection because it will be more difficult for someone to gain access to data if the rules used are unknown.

Phase 3: Secure Connection

This phase is the connection between the control unit and sensor module. Once the encrypted communication is established, the control module will receive a frequency value from the sensor module to set a new connection rate at predetermined intervals (set here every 3 milliseconds). If the frequency value is recognised by the control unit module, the protocol continues to the next phase. If the frequency value is not recognised, the control unit will pause communication, set the system into sleep mode and issue an alert. If recognised, the modules are instantly connected, and the control unit sends the new frequency in a continuous loop employing the baud rate agreed in phase 2.

Phase 4: Authentication

This phase consists of controlling the sensor module alphanumeric password by the control unit module. These modules are pre-set with an admissible alphanumeric password which is a combination of a minimum of eight characters, including lowercase and uppercase, numbers, and symbols. Additional measures prevent using the same password twice; dictionary words, or sequences; usernames or information that might become publicly associated with the user. If the control unit module does not recognise the password, authentication ends unsuccessfully, and the process moves back to step 3. Figure 25 shows a detailed version of Figure 14 to illustrate the data flow through the trust boundaries when the IoT device is equipped with the added security provisions. Instead of the single trust boundary around the IoT device, there are now three trust boundaries, one for each module, and an overall boundary is highlighted for the whole machine equipped with the IoT device. The implementation of the LCCA authentication protocol in presented in Appendix C.

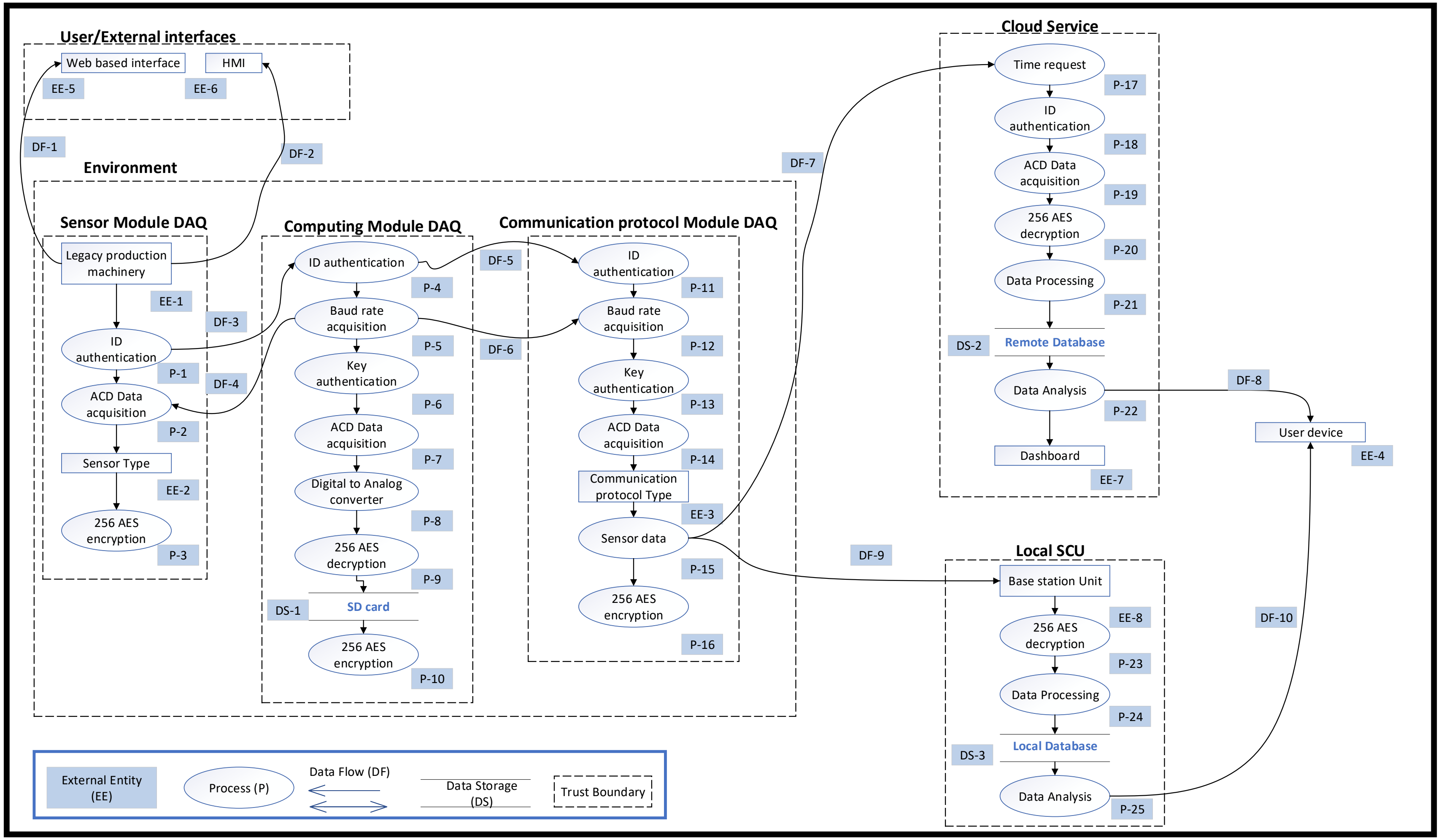


Figure 25: Data flow diagram of the connected legacy production machinery

6.5 Chapter Summary

This chapter responds to the aim and objectives of the threat mitigation phase of the design thinking approach. The proposed IoT modular design is for a sealed unit that offers a standardised communication interface that uses hardware and software authentication protocols between the modules. This new design allows data access only for authorised users and communicates at the M2M and cloud level. In addition, it is limited to the use of a single sensor or actuator and a single communication component at a time to avoid vulnerability and overload of the network and communication. While devices consisting of all hardware components included in a single module, increasing the risks of network, communication and physical attacks, the modular IoT DAQ unit offers the opportunity to customise and manage the configuration of the device and replace the individual modules without compromising the entire device. In addition, the approach is designed to be verifiable so that any abuse can be identified.

Overall, the proposed modular IoT DAQ unit employs an authentication protocol which cascades the complexity of compromising its own security while allowing access for authorised users. It comprises four main stages, namely Log identity authentication, encrypted Communication, secure Connection, and Authentication (LCCA). All four phases of the LCCA protocol employ AES cryptography and each phase contributes additional security. The next section presents the implementation of the above protocol concept as part of an IoT-enabled machine monitoring pilot instantiation.

7 PILOT TESTING AGAINST SELECTED ATTACK

The final phase of the systematic design thinking approach delineates mitigation mechanism for the DoS and clone attack which are scored with high impact in the earlier analysis (Table 6) and considered typical threats for manufacturing environments integrated with embedded devices.

The prerequisite for this chapter is that of a successful DoS or clone attack, through several intermediate targets that follow the attack tree shown to access the DAQ unit in Chapter 5. The scope of these tests was to perform an end to end functional testing without fully emulating DoS or clone attack or its mitigation mechanism. The aim was to clarify how the isolation principle was applied through the LCCA protocol to reduce relevant security risks. The functional test output can be returned to improve the effectiveness of the mitigation mechanism. The attacks aim to deprive the IoT device of resources and compromise monitoring data. Specifically, this chapter explains how advanced modular IoT functionality equipped with the LCCA protocol can prevent the attacker from manipulating device and network data after gaining access to the architecture from two different entry points. For the experiments was employed an industrial DMG Mori NTX 1000/W CNC Mill Turn Centre (twin-spindle turning centre with five-axes milling capability). Finally, this chapter describes the physical instantiation of the IoT DAQ unit and the mitigation mechanisms testing DoS and cloning attacks.

7.1 Modular IoT DAQ unit vs DoS attack

The first scenario is that the DMG production machinery is under DoS attack. The modular IoT DAQ unit is used to monitor the accelerations and temperature from the spindle of the DGM machine during machining operations on an aluminium sample. The sensor data is encrypted and sent to a cloud platform developed with a Raspberry pi 2 accessible only by authorised users. The attack goal aims to exhaust battery life or communications and gain access to the sensors data. The attacker attempts to get information from the sensors to modify, jam the data traffic, or get machine parameters such as the spindle temperature and acceleration. The attack tree in Figure 16, shows the steps that the attacker must take to achieve the target. The implementation consists of the control unit module which is equipped with a 32 GB SD card to store data and its CPU to run the authentication protocol.

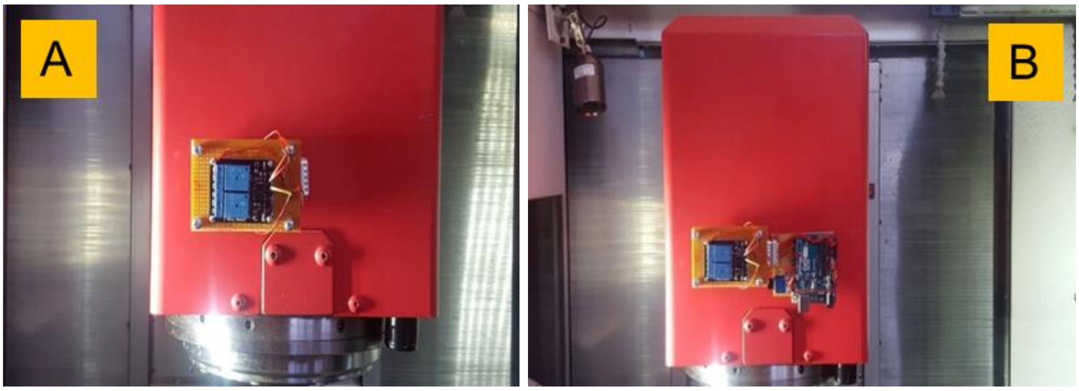
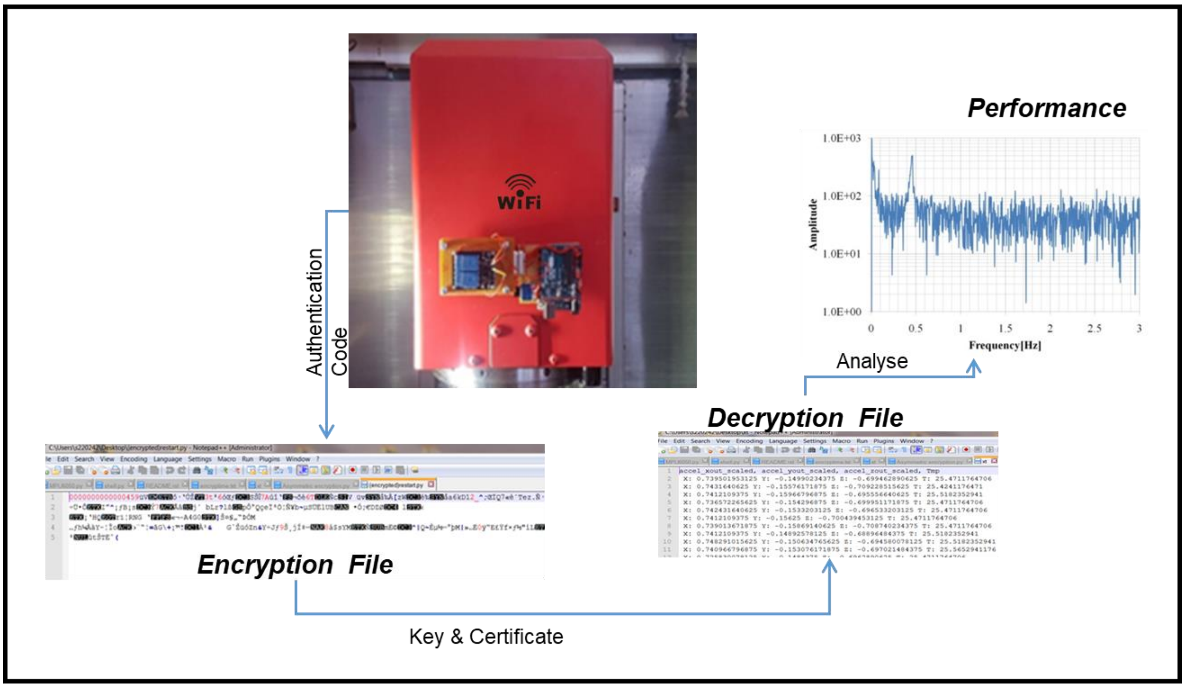


Figure 26: Prototype implementation of modular IoT DAQ unit

A snapshot of the user device screen during monitoring real-time data is shown in Figure 26, where current data are shared with end-user devices and are visualised. In detail, the sensor module is tightly integrated with the legacy machine tool (Figure 26 - picture A), while the transmitter module is preserved and attached to the machine by the users assigned to check the health of the machine (Figure 26- picture B).



```
accel_xout_scaled, accel_yout_scaled, accel_zout_scaled, Tmp
 X: 0.739501953125 Y: -0.14990234375 Z: -0.699462890625 T: 25.4711764706
 X: 0.7431640625 Y: -0.15576171875 Z: -0.709228515625 T: 25.4241176471
 X: 0.7412109375 Y: -0.15966796875 Z: -0.695556640625 T: 25.5182352941
 X: 0.736572265625 Y: -0.154296875 Z: -0.699951171875 T: 25.4711764706
 X: 0.742431640625 Y: -0.1533203125 Z: -0.696533203125 T: 25.4711764706
 X: 0.7412109375 Y: -0.15625 Z: -0.700439453125 T: 25.4711764706
 X: 0.739013671875 Y: -0.15869140625 Z: -0.708740234375 T: 25.4711764706
 X: 0.7412109375 Y: -0.14892578125 Z: -0.68896484375 T: 25.5182352941
 X: 0.748291015625 Y: -0.150634765625 Z: -0.694580078125 T: 25.5182352941
 X: 0.740966796875 Y: -0.153076171875 Z: -0.697021484375 T: 25.5652941176
```

Figure 27: Modular IoT DAQ unit operational process

The sensor module comprises of two layers. The bottom layer includes the sensors, the CPU and memory of the control module and the battery to supply the IoT unit during data acquisition and protocol execution. The top layer includes a relay board used as an electronic switch that allows sensor data to pass through it only if in input a specific signal is recognised. The control unit module collects sensor data and stores them into an encrypted file, which only an authorised end user equipped with the appropriate key and certificate can decrypt and read the file content (Figure 27). The control unit module calculates the CPU and RAM usage of the sensor module. In addition, if the control unit module does not detect the correct credentials, i.e. valid keycode between either the sensor or the communication module, the data acquisition operations are interrupted, therefore it sends an alert message to the user-device specify the anomaly. The webserver, cloud or end-user device exposes the modular IoT DAQ unit to the typical Denial of Service (DoS) attack aiming to take down the operational capacity of the device.

7.1.1 The DoS attack scenario and path

The DoS attack emulation scenario is shown in Figure 28 which consists of:

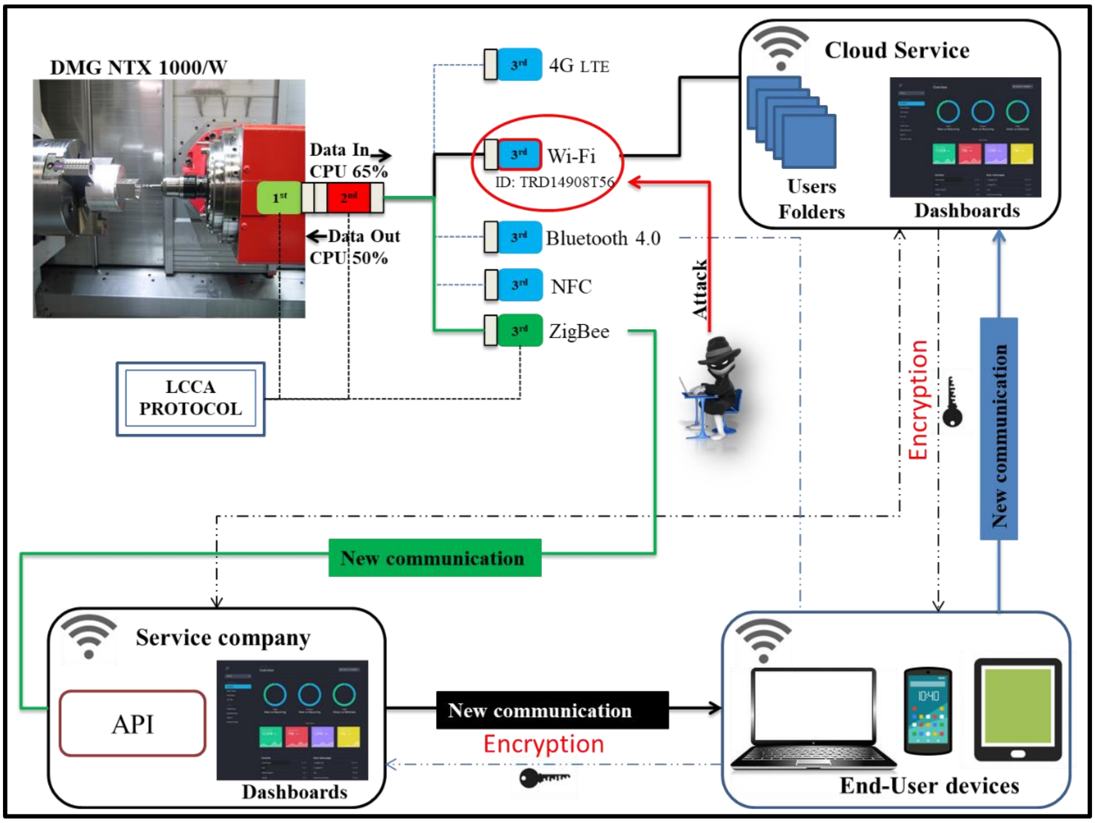


Figure 28: DoS attack emulation scenario

1. The milling machine tool equipped with the sensor module on the spindle.
2. The network hub for the monitoring service provider equipped with the API to monitor the status and the performance of the machine tool.
3. The end-user devices used to monitor the machine tool anywhere and anytime.
4. The own cloud service, for processing, analysing and planning the maintenance interventions.

All sub-systems are equipped with AES 256 encryption.

The test aimed to simulate a Denial of Service attack (DoS) via the network. The attacker gained network access and is ready to generate connection requests via the communication module (Wi-Fi) using its source address rather than directly attacking the target system. In this way, the communication module responds affirmatively to the connection request not by the attacker but to the target of the attack. As a result, the attacker enters a vicious circle that will quickly exhaust the targeted resources and flood the network with traffic.

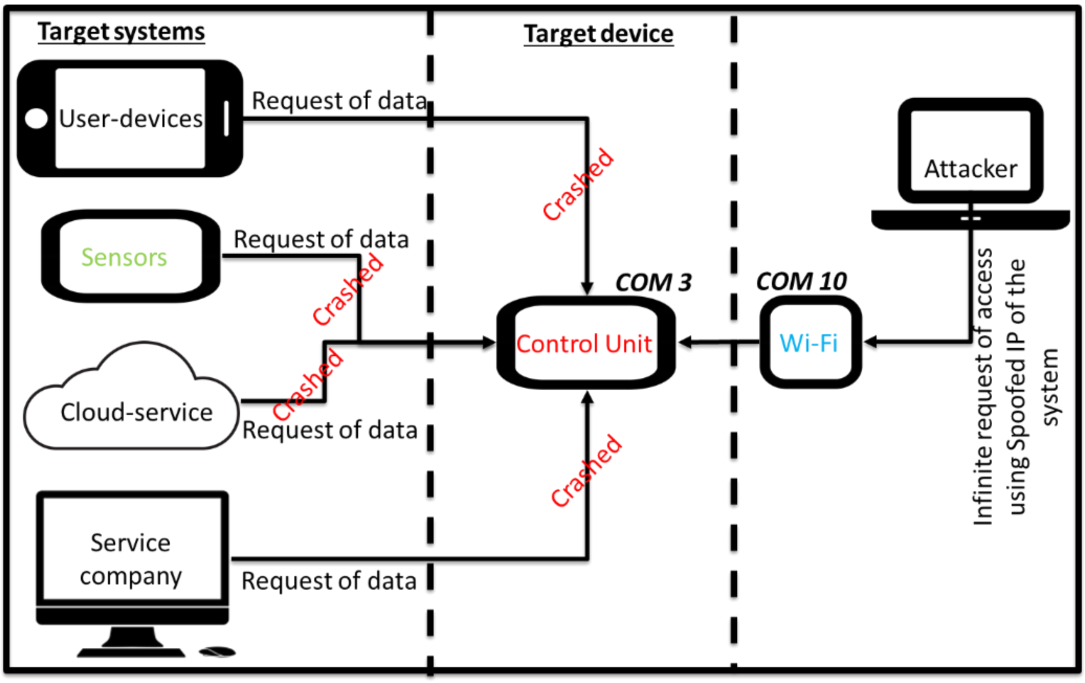


Figure 29: DoS attack path (without defence)

The attacker generates an infinite request for access after spoofing the IP of the system. At the same time, the targeted system attempts to access the data when the sensor module is trying to exchange condition monitoring data with the control unit module. The large number of responses from the control unit module exhausts the bandwidth and ultimately leads to the system crashing. This employs an Arduino Uno unit for generating a connection request to the transceiver module, so as to affect the targeted device. The control unit module is connected to the sensor module via COM3 port and the transceiver through the COM10 port (Figure 29). Therefore, the attacker gains network access for managing the control unit module generating functions for infinite access requests, delay services and reducing the battery life of the module. As a result of this DoS attack emulation the modular IoT DAQ unit is able to calculate the value of the CPU usage in percentages for the control unit module. The CPU utilisation procedure includes two phases:

- Phase 1: The real-time operating clock (RTOC) is used to estimate CPU/core utilisation. The scheduler system tick is used for this purpose, as it is based on timer interrupt, which is considered as a relatively accurately measure of elapsed time.
- Phase 2: Counting maximum idle count; an estimation is obtained through observing idle counts during a measurement period. If no task is performed (besides the timer interrupt) this represents the maximum number of idle counts and corresponds to 0% utilisation. Estimation accuracy errors tend to become insignificant when the CPU utilisation measurement period is sufficiently large. After calculation of maximum idle counts, no code or task can be added to the idle task.

CPU utilisation provides a total load of all CPU cores, especially a single-core processor which is 100% of a core. CPU usage allows you to analyse CPU load peaks and identify overactive CPU usage, particularly for unnecessary background processes or applications. In this case, the modular IoT DAQ unit consists of a single-core processor that uses 71% of the CPU core during the implementation of the LCCA protocol. The modular IoT DAQ unit can run smoothly in the range of 30% to 71% load, but at 72% it becomes much slower and process collisions increase exponentially, which means that something is overloading the system.

Although the proposed modular DAQ is an autonomous system that operates without updates and is controlled through a corporate network, this system is able to detect network attacks, in particular for the DoS scenario.

In order to perform a CPU analysis able to react over time to a possible overload, this modular single-core IoT DAQ unit is composed of three CPU bands: between 1% and 30% which represents the initialization stage in which the CPU interacts with the hardware components on the modular IoT DAQ; between 30% and 71%, which is the operating band for the modular IoT DAQ, and finally between 72% and 100%, which is the problematic band for the proposed modular system.

In this case, the DoS attack occurs by running the application through a host device on the intranet. The control unit and transmitter module exchange information using the LCCA protocol to detect significant deviations from the expected standard operation. If the DoS attack occurs on the channel currently available for data exchange (for example, on the Wi-Fi module circled in red in Figure 28), the control module recognises the attack and interrupts the current communication path.

The scope of this test was to perform an end to end functional testing without fully emulating DoS attacks or its mitigation mechanism. The aim was to clarify how the isolation principle is applied through the LCCA protocol to reduce relevant security risks. The simple detection technique can, however, be replaced by a more sophisticated mechanism, following a similar isolation principle in the communication between the modules.

7.2 Modular IoT DAQ unit vs Cloning attack

In the second case the attacker gains access to the communication module by the social engineering method bypassing a firewall. The control unit module controls the authentication key and CPU percentage, therefore, if some of the software or hardware parameters change (e.g. current, system memory, voltage, CPU, IDs) the control unit module closes the current connection with the malicious hardware or software parts and discovery a different way for exchanging data with the target.

7.2.1 The cloning attack scenario and path

Figure 30 shows the Denial of Service (DoS) attack by an infected USB dongle for upgrading an infected kernel inside of the machine. Such an attack may employ multiple attacking machines, which together form a botnet.

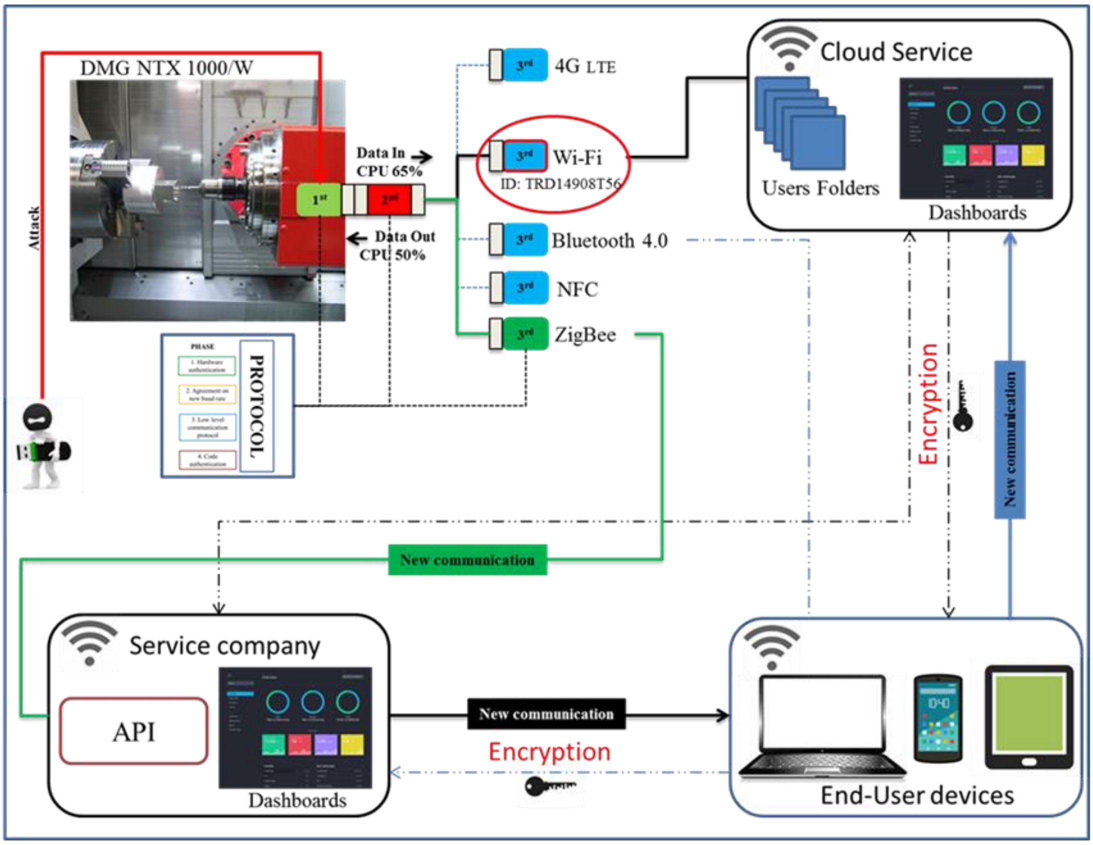


Figure 30: Cloning attack

A botnet is a network controlled by a master bot and is made up of devices infected by specialised malware, known as bots or zombies [179]. In this scenario, the attacker gains physical access to the sensor module and clones it using fake modules equipped with reprogrammed firmware. The control unit module calculates the CPU percentage usage from each module if some hardware parameters have changed, the control unit module is able to identify such a modification.

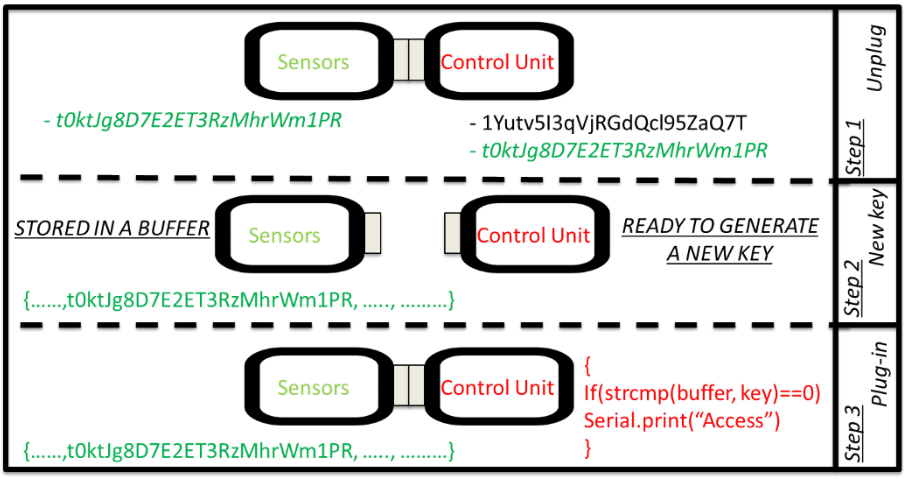

Sensors
Control Unit
- t0ktJg8D7E2ET3RzMhrWm1PR
- 1Yutv5I3qVjRGdQcl95ZaQ7T
- t0ktJg8D7E2ET3RzMhrWm1PR
Step 1
Unplug
STORED IN A BUFFER
Sensors
Control Unit
READY TO GENERATE A NEW KEY
{......,t0ktJg8D7E2ET3RzMhrWm1PR, ..., ...}
Step 2
New key
Sensors
Control Unit
{
If(strcmp(buffer, key)==0)
Serial.print("Access")
}
{......,t0ktJg8D7E2ET3RzMhrWm1PR, ..., ...}
Step 3
Plug-in

Figure 31: Authentication process between control unit module and sensor or communication module

Figure 31 describes the authentication process between the sensor and the control unit module.

- Step 1 - for each connection between the two modules the control unit module generates a unique authentication key.
- Step 2, the authentication key is stored in a buffer of characters under a private class that does not allow modifications by other users within the sensor module. In addition, the control unit module is ready to generate a new authentication key for the next connection.
- Step 3 checks the sensor unique key and compares it to the one in the control unit module buffer. If the sensor's unique key matches the key inside the control buffer unit, the sensor module will gain access to phase 2 of the authentication protocol (Figure 24).

The control module compares single characters of the authentication key to make sure that it is the unique key. If the sensor authentication key matches the key inside the control unit module buffer, the sensor module will gain access to phase 2 of the authentication protocol (Figure 24).

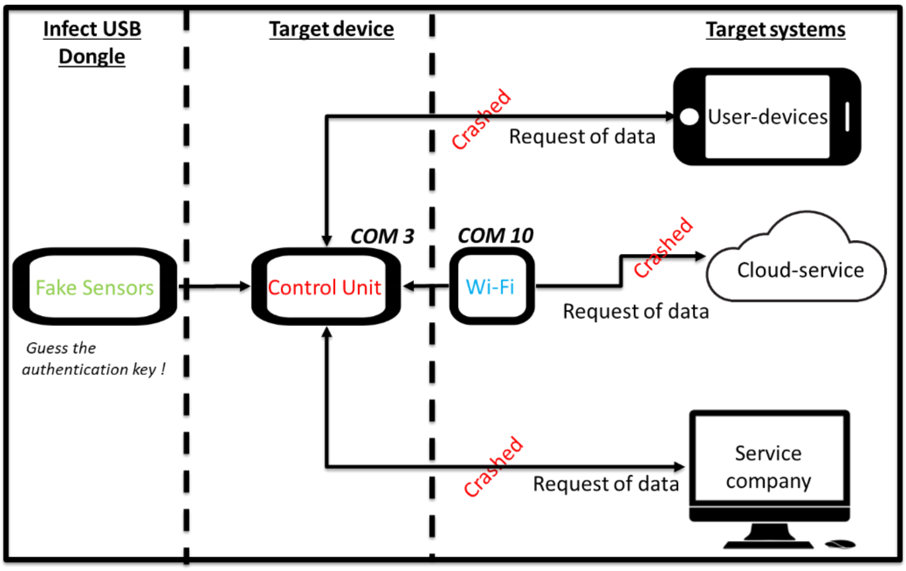
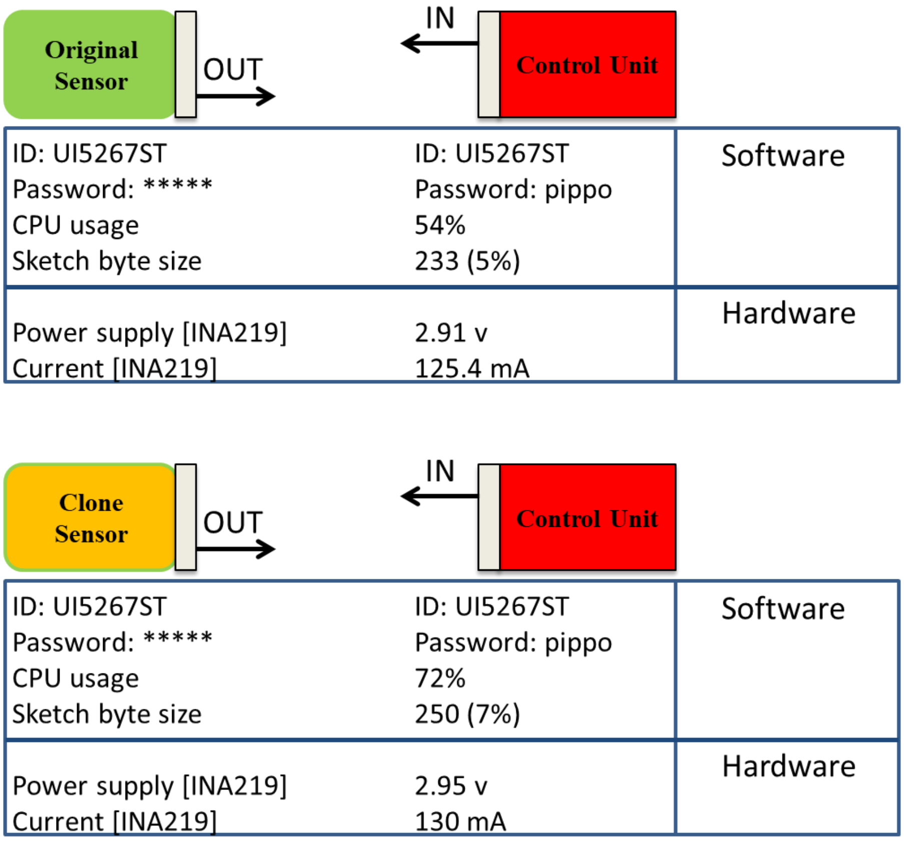


Figure 32: Authentication method vs. the DoS attack by infected USB dongle

Figure 32 shows the DoS attack by an infected USB dongle which is employed for upgrading an infected kernel inside of the machine [179]. If the attacker correctly guesses the authentication key, and reprograms the sensor firmware, the attacker initiates the DoS attack and crashes the whole network. In a cloning attack of a wireless sensor network architecture, once a sensor node is compromised, the attacker can easily capture other sensor nodes and deploy several clones that have legitimate access to the network (legitimate IDs, passwords, and other security credentials) [180]. The control unit module processes and analyses data from the sensor and communication modules for each connection. Therefore, the control unit module detects variations between the original and the clone sensor. If a clone sensor is detected, the control unit module disables all communication with it.

Figure 33 shows two different cases of sensor communication. In the first case the control unit module is plugged into the original sensor (green module), reading software parameters, such as ID, password, CPU usage, static RAM (SRAM) byte sketch size; and hardware parameters through a INA219 sensor (power supply and current measurement). In the second case, the clone sensor (yellow module) shows the same hardware and software of the original sensor but the malicious code for compromising the monitoring system is also included. In case of a cloning attack, the attacker aims to reprogram the kernel module by adding code lines to compromise the modular IoT DAQ unit.



ID: UI5267ST Password: ***** CPU usage Sketch byte size	ID: UI5267ST Password: pippo 54% 233 (5%)	Software
Power supply [INA219] Current [INA219]	2.91 v 125.4 mA	Hardware

ID: UI5267ST Password: ***** CPU usage Sketch byte size	ID: UI5267ST Password: pippo 72% 250 (7%)	Software
Power supply [INA219] Current [INA219]	2.95 v 130 mA	Hardware

Figure 33: Reading byte between two modules

Against such an attack, the control unit module is able to monitor any change in the CPU usage, the power supply and current, and compare them against typical parameter values for the connection. In addition, the control unit module controls the sketch size in bytes as an identification mechanism of the original sensor module. This sketch byte size is the real-time value stored in the static RAM of the device. In order to prevent an attacker from cloning a module, the control unit module by means of the sketch byte size and the static RAM value is able to identify non-original modules in order not to share information with it. In addition, physical parameters can help understand some early hardware changes such as power supply and current reading by an add-on to the modular IoT DAQ unit.

The authentication ID control mechanism brings down the probability of successful cloning threat events to a lower level, and consequently reduces also the level of impact.

7.3 Chapter summary

This chapter describes the validation tests for the design thinking approach which refers to the mitigation mechanism for DoS and clone attack which are classified with a high impact index in Table 6 and are considered typical threats to production environments integrated with embedded devices. The experimentation is set up using a DGM milling machine used for validation with respect to two case studies. The attacks aim to deprive the IoT device of resources in order to compromise the monitoring data.

The first attack scenario aims to compromise battery life or IoT device communications and gain access to sensor data from a DoS attack, in order to modify data traffic or obtain machine parameters. The second attack scenario aims to infect a USB dongle kernel for updating the DGM machine. Such an attack can employ multiple machines, which together form a botnet. The mitigation mechanism focused on the isolation principle which is applied through the LCCA protocol to reduce significant security risks. The introduced protocol monitors any changes to the authentication, communication and overall connection between the modules. Therefore, if any changes are detected, the modular IoT DAQ unit closes the current connection with the harmful hardware or software parts and detects a different way of exchanging data with the destination. This chapter describes the successful development and application of the design thinking approach proposed with validation. The next chapter presents the discussions and the conclusion of the thesis.

8 DISCUSSION AND CONCLUSION

This chapter presents the summary of the findings of the research in fulfilment of the research aim and objectives. This thesis addresses security and integrity risks when incorporating IoT within manufacturing environment by introducing a step by step design thinking approach for IoT-enabled monitoring of legacy production machinery incorporating security by design features. This chapter consists of many sections. Section 8.1 provides a summary of the main research results and is followed by Section 8.2 which provides a summary of the research results in the application of the methodologies proposed in this Thesis. In Section 8.3 research methodology to the body of knowledge are highlighted. Section 8.4 discusses the new design thinking approach and 8.5 the future work for the extension of the work done in this Thesis is presented. Finally, Section 8.6 presents the conclusions of the research with respect to the objectives of the research.

8.1 Key Research Findings and Observations

There has been little attention to security methods and approaches for integrating IoT technology within a legacy manufacturing environment, especially for control and monitoring operations. In addition, such an integration is managed by authentication mechanisms often heavy in terms of processing capabilities which focus only on the software aspects of the IoT application. Classic IT security mechanisms integrated with new advanced connectivity suitable for industry supervision and control require a better understanding of uncertainties such as the context of the application and identification threat models. The presence of these uncertainties if not adequately explained can lead to unreliable projects that are unable to satisfy their own design requirements.

This research aims to introduce a design thinking approach for security when upgrading legacy machinery with IoT through a new method within well-understood research areas, rather than generating a new theory in a new domain. In addition, this research presents a novel lightweight authentication protocol with real-time functionality, which increases the complexity required by any attack approach to compromise the IoT device and monitoring via hardware and software functionality.

A literature review and selection of industry case study were undertaken to identify gaps in the legacy sector that motivates the propositions in this research and provides the basis for selecting the security mechanisms managed by the novel authentication protocol. This review was conducted for studies on security approaches for integrating IoT technology into a legacy production environment. In addition, a review of the studies on the security mechanisms of industrial supervision and control systems, in particular in the case of access to the network, system communications and data acquisition unit. The combination of the results from literature, in particular of the identified gaps and of the acquired knowledge, has led to the proposal of a new approach to security to systematically integrate and design hardware and software for the remote monitoring of IoT data with security provisions for legacy production machinery and managed by a lightweight authentication protocol. The following section presents the strategy and development of the approach used.

8.2 Analysis of the proposed methodology

The applied research methodology by using existing information, methods and techniques that already exist in the body of knowledge to solve an industry need. Such a methodology explores new insights into strategies to develop a novel endpoint method for systematically integrate and design robust secure IoT data acquisition hardware and software for monitoring legacy production machinery remotely. The study employs a mixture of the qualitative and quantitative research design approach. During the study, both qualitative and quantitative data must be sought, hence the combined approach. The collection of information on the research domain in relation to the selection of the case study to reflect current practice is presented and is carried out through the use of questionnaires, interviews, analysis and semi-structured and unstructured observations will be used as strategies to clarify the knowledge necessary to achieve the purpose of this research. The requirements of surveys are the motivation of the selected research design approach and the data collection methodologies. In this research, a new approach based on a risk-averse design for endpoint security is presented through the development of an innovative implementation of IoT device security, following the principle of isolating modularity, including a new lightweight authentication protocol. The approach is focused on the monitoring aspect of a legacy machine tool and identifies the risk of attack for the end-user.

These attack targets are the inability to communicate with the Cloud, the system control unit (SCU), user devices, the inability to update the firmware, the inability to use the human interface. machine (HMI), the inability to collect correct data from the sensors, to protect the sensor data and send the data correctly. The validation phase employed functional tests for the selected case study using hardware experiments to characterise the physical functioning of the authentication protocol for the modular IoT DAQ unit and computer simulations to replicate the behaviour of a system starting from a conceptual model.

8.3 Application of the proposed methodology

The systematic design thinking methodology introduced comprises five key steps. Feedback from each phase may reveal the need to reconsider the choices of analysis, modelling, design and implementation of all the previous phases.

- Baseline and context: this phase requires an understanding of the application context and the interfaces of system components, which can be exposed to security threats.

- Threat analysis: this phase involves an analysis of security problems and vulnerabilities that can create a negative impact on the integrity of the industrial IoT monitoring system. A threat of taxonomy and impact risk assessment are produced.
- Application and threat modelling: this phase produces a more detailed model of the target system's application context, along with its interfaces and functionality. DFDs are implemented to understand the permeation of data trust between components and the systematic modelling of threats through attack trees.
- Threat mitigation: this phase covers the design and implementation of security threat mitigation mechanisms. An instance of the overall process is created and applied to the real-time monitoring application related to production environments.
- Testing and validation: this phase include testing and validation of mitigation mechanisms against selected threats. The results of functional and penetration tests can be returned to improve the effectiveness of mitigation.

The design thinking approach is an abstract conceptual model that does not correspond well to the increase in the complexity of application cases. MBSE and security meta-models could be relevant for moving from such an abstract model to a specific application case in a practical way to support a manual diagnosis of security vulnerabilities. MBSE helps to ensure a more complete, coherent and traceable system design while allowing the communication and reuse of system information [147] for others in reusing and extending the results of this thesis research.

8.4 Contribution to knowledge

This research helped to systematically integrate a design thinking approach for IoT security in IoT-enabled legacy production environments. This contribution provided an application methodology for designing and analysing optimisation for secure IoT monitoring devices, which allows for the mapping and prioritisation of threats and risks in a domain-specific application-oriented way, which, in turn, allows the identification of priorities to intervene with a mitigation approach and reduces the risks of integrity. The contributions to the knowledge of this Thesis can, therefore, be summarised as follows:

- The proposal for a new approach to endpoint security design to address security problems when updating production machinery with IoT connectivity to provide monitoring of conditions on real-time for legacy manufacturing machinery. The proposed approach has also been demonstrated through application to two case studies (DoS attacks and clones). The approach, therefore, provides the isolation principle to reduce security-relevant risks.
- Developed a new authentication protocol implementing in effect the isolation principle at the IoT endpoint subsystem level.
- The proposed methodology can be applied to assess the risks and vulnerabilities related to any industrial environment related to monitor industrial production environment

The overall contribution has opened a new section within the scientific community regarding the security integration of IoT within legacy production environments, especially for control and monitoring applications. Research institutions and companies can benefit from these contributions which can be applied to different industry sectors to assess risks and vulnerabilities for integrating IoT. In detail, the new design thinking approach can be used as a starting point for a conceptual evaluation of IoT technology within manufacturing environments. The multistage authentication protocol can be customised following the specific input from the manufacturer for controlling parameters useful to discover possible endpoint vulnerabilities from monitoring and controlling IoT devices integrated into the corporate network. The modular IoT DAQ defines new guidelines on how to design IIoT devices for the industry. Such a modular IoT DAQ can control many sensor modules connected to different production machines within the shop floor. The hardware equipment does not require any wires for communication and connection between modules.

8.5 Further Research Work

Although this systematic step-by-step approach draws parallels with previous and ongoing activities (e.g. PASTA, LINDUUN, STRIDE), it is positioned towards the concrete context of retrofitting legacy production machinery with monitoring capabilities enabled by IoT connectivity, with particular attention IoT endpoint security. Based on the above, there are other areas of research within this research problem domain that can be avenues for further research. The recommended future research is presented as follows:

- Comprehensive list of intentional and unintentional threat types which cover the range of attackers. Attack threat models should be integrated for identifying potential threat motivations.
- Comprehensive mitigation mechanisms for the range of threats identified. The research presented includes specific examples of relevant mitigation mechanisms to prevent DoS and clone attack threats, any alternative and more comprehensive mechanism can be used, but should still be included in the context of a global design approach for IoT security.
- The research intention reported was to present the multistage design thinking approach for security arrangements. Any final implementation of the solutions adopted must be preceded by thorough and systematic tests against attacks.
- The step-by-step approach is an abstract conceptual model that can be further strengthened in specific application cases combining it with a systematic MBSE methodology. Further work could involve the implementation of MBSE systematically analysing systemic security

risks, identifying both high and low-level vulnerabilities to generate attack trees for manual diagnosis [181].

- Risk quantification introduced was only indicative and qualitative in nature. Further work is needed in the direction of systematic risk quantification, including evidence-based data and approaches for risk quantification [182].
- Organisations seeking to adopt design-based security approaches would benefit from methodologies and tools that help inappropriately prioritise any security-related updates. Future work should examine how to best place a design-based approach, such as the one presented in this document, in the context of managing overall organisational security maturity.

8.6 Conclusion

In conclusion, this research proposed a novel approach for IoT-enabled monitoring of legacy production machinery, which consist of five stages, incorporating security by design features. The fist two steps of this approach which analyse current monitoring practices and security and vulnerability issues related to the application domain, while the remain three steps which make the domain-relevant analysis to become application specific. These include a detailed model of the application context on legacy production machinery monitoring, together with its interfaces and functionality, implementing threat mitigations combined with a new modular IoT DAQ unit mechanism, validated by functional tests against Denial of Service (DoS) and clone attacks. For each step of the design thinking approach there has been design DFD's and attack trees for upgrading legacy production machine with the IoT technology. The main concepts of the new approach are the adoption of the isolation principle and the development of a new LCCA multistage and light authentication protocol, which increases the complexity required by DoS and clone attacks to reach a compromise of the IoT device and of monitoring and production associated. Functional tests were created and validated to show the performance of the modelling methodology. The results obtained identified how the isolation principle is applied through the LCCA protocol to reduce significant security risks. The overall design thinking approach has been empirically tested but further systematic validation with larger studies, including longitudinal and expert opinion, and data gathering in specific application contexts are needed. These should include a deeper and application-focused risk analysis to quantify the threats. The implementation of the LCCA protocol in such applications can be further logically examined for errors using automated verification technology and tested more thoroughly with extensive and automated tests done by third parties involved in security [183].

REFERENCES

1. Singer, P. THE 600 GROUP Table of contents Available online: https://www.hardmanandco.com/wp-content/uploads/2018/11/600-Group-Interims-November-2018.pdf (accessed on Nov 20, 2018).

2. Farinha, J.T.; Galar, D.; Shagluf, A.; Longstaff, A.P. Maintenance strategies to reduce downtime due to machine positional errors. In Proceedings of the Maintenance Performance Measurement and Management (MPMM) Conference 2014; Coimbra, Portugal, 2014; pp. 111–118.

3. Al-Sarawi, S.; Anbar, M.; Alieyan, K.; Alzubaidi, M. Internet of Things (IoT) communication protocols: Review. *ICIT 2017 - 8th Int. Conf. Inf. Technol. Proc.* **2017**, 685–690.

4. Rojko, A. Industry 4.0 concept: Background and overview. *Int. J. Interact. Mob. Technol.* **2017**, *11*, 77–90.

5. Rohm, T. How IoT will dramatically impact Enterprise Resource Planning (ERP) systems Available online: https://www.itworldcanada.com/article/how-iot-will-dramatically-impact-enterprise-resource-planning-erp-systems/420874 (accessed on Aug 19, 2019).

6. Nylander, S.; Wallberg, A.; Hansson, P. Challenges for SMEs entering the IoT world - Success is about so much more than technology. In Proceedings of the ACM International Conference Proceeding Series; Linz Austria, 2017; pp. 1–7.

7. Chae, H.; Shahzad, Aa.; Irfan, M.; Lee, H. Industrial Control Systems Vulnerabilities and Security Issues and Future Enhancements. *Adv. Sci. Technol. Lett.* **2015**, *95*, 144–148.

8. Hascoet, J.-Y.; Rauch, M. Enabling Advanced CNC Programming with openNC Controllers for HSM Machines Tools. *High Speed Mach.* **2016**, *2*, 1–14.

9. Janak, L.; Stetina, J.; Fiala, Z.; Hadas, Z. Quantities and Sensors for Machine Tool Spindle Condition Monitoring. *MM Sci. J.* **2016**, *2016*, 1648–1653.

10. Elghazel, W.; Bahi, J.M.; Guyeux, C.; Hakem, M.; Medjaher, K.; Zerhouni, N. Dependability of Sensor Networks for Industrial Prognostics and Health Management. *Comput. Ind.* **2015**, *68*, 1–15.

11. Deshpande, A.; Pieper, R. MSEC2011-50019. In Proceedings of the ASME 2011 International Manufacturing Science and Engineering Conference MSEC2011; ASME: Corvallis, Oregon, USA, 2011; pp. 1–8.

12. Karpinski, R. The expanding and changing impact of IoT data on IT infrastructure Available online: https://www.i-scoop.eu/internet-of-things-guide/iot-it-infrastructure/ (accessed on Jun 9, 2020).

13. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A Survey on Security and Privacy Issues in Internet-of-Things. **2017**, *4*, 1250–1258.

14. Zhou, L.; Yeh, K.; Hancke, G. Security and Privacy for the Industrial Internet of Things: An Overview of Approaches to Safeguarding Endpoints. *IEEE Signal Process. Mag.* **2018**, *35*, 76–87.

15. Murakami, K.; Suemitsu, H.; Matsuo, T. Classification of Repeated Replay-Attacks and Its Detection Monitor. In Proceedings of the IEEE 6th Global Conference on Consumer Electronics (GCCE); IEEE: Nagoya, Japan, 2017; pp. 2–3.

16. Patil, D.S.; Patil, S.C. A Novel Algorithm for Detecting Node Clone Attack in Wireless Sensor Networks. *2017 Int. Conf. Comput. Commun. Control Autom.* **2017**, 1–4.

17. Fernández-caramés, T.M.; Fraga-lamas, P.; Suárez-albela, M.; Castedo, L. Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications. *Sensors* **2017**, *28*, 1–31.

18. Ogiela, L.; Ogiela, M.R. Insider Threats and Cryptographic Techniques in

Secure Information Management. *IEEE Syst. J.* **2017**, *11*, 405–414.

19. Iqbal, M.A.; Bayoumi, M. A Novel Authentication and Key Agreement Protocol for Internet of Things Based Resource- constrained Body Area Sensors. In Proceedings of the IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW); IEEE: Vienna, Austria, 2016; pp. 315–320.

20. Abawajy, J. Enhancing RFID tag resistance against cloning attack. In Proceedings of the NSS 2009 - Network and System Security; IEEE: Gold Coast, QLD, Australia, 2009; pp. 18–23.

21. Ray, B.; Huda, S.; Chowdhury, M.U. Smart RFID reader protocol for malware detection. In Proceedings of the 12th ACIS International Conference on Software Engineering, Artificial Intelligence Networking and Parallel Distributed Computing, SNPD 2011; 2011; pp. 64–69.

22. Deng, C.; Guo, R.; Zheng, P.; Liu, C.; Xu, X.; Zhong, R.Y. From Open CNC Systems to Cyber-Physical Machine Tools: A Case Study. *Procedia CIRP* **2018**, *72*, 1270–1276.

23. Boyang, M.; Maoyue, L.; Xianli, L.; Lihui, W.; Liang, S.Y. Open architecture CNC system based on soft-integrated communication. *Procedia CIRP* **2018**, *72*, 671–676.

24. Shostack, A. *Threat Modeling : Designing for Security*; Wiley, 2014; ISBN 9781118810057.

25. UcedaVelez, T.; Morana, M.M. *Risk Centric Threat Modeling_ Process for Attack Simulation and Threat Analysis*; Wiley, 2015; ISBN 0470500964, 9780470500965.

26. Gupta, K.; Shukla, S. Internet of Things: Security challenges for next generation networks. In Proceedings of the 1st International Conference on Innovation and Challenges in Cyber Security, ICICCS 2016; IEEE: Noida, India, 2016; pp. 315–318.

27. He, H.; Maple, C.; Watson, T.; Tiwari, A. The Security Challenges in the IoT enabled Cyber-Physical Systems and Opportunities for Evolutionary Computing & Other Computational Intelligence. In Proceedings of the 2016 IEEE Congress on Evolutionary Computation (CEC); IEEE: Vancouver, BC, Canada, 2016; pp. 1015–1021.

28. Brandner, M. Why in Industry 4.0 manufacturing needs to be better prepared for cyber attacks Available online: https://www.iottechnews.com/news/2016/jul/01/why-industry-40-manufacturing-needs-be-better-prepared-cyber-attacks/ (accessed on Jul 1, 2016).

29. Watteyne, T.; Handziski, V.; Vilajosana, X.; Duquennoy, S.; Hahm, O.; Baccelli, E.; Wolisz, A. Industrial Wireless IP-Based Cyber – Physical Systems. *Proc. IEEE* **2016**, *104*, 1025–1038.

30. Korolov, M. Attacks against industrial control systems double _ CSO Online Available online: https://www.csoonline.com/article/2911160/attacks-against-industrial-control-systems-double.html (accessed on Apr 17, 2015).

31. Hassan, Q.F. *Internet of Things: Technologies and applications*; Wiley-IEEE.; John Wiley & Sons, 2018; ISBN 1119456746, 9781119456742.

32. Koene, I.; Viitala, R.; Kuosmanen, P. Internet of Things Based Monitoring of Large Rotor Vibration with a Microelectromechanical Systems Accelerometer. *IEEE Access* **2019**, *7*, 92210–92219.

33. Gao, S.; Zhang, X.; Du, C.; Ji, Q. A multichannel low-power wide-area network with high-accuracy synchronization ability for machine vibration monitoring. *IEEE Internet Things J.* **2019**, *6*, 5040–5047.

34. Fidler, B.; Currie, M. The production and interpretation of ARPANET maps. *IEEE Ann. Hist. Comput.* **2015**, *37*, 44–55.

35. Mercer, D. Strategy Analytics_ Internet of Things Now Numbers 22 Billion

Devices But Where Is The Revenue_ _ Business Wire Available online: www.strategyanalytics.com (accessed on May 16, 2019).

36. Remotti, L.A.; Hartmann, C.; Jussila, A. Study on mapping Internet of Things innovation clusters in Europe Available online: https://ec.europa.eu/digital-single-market/en/internet-of-things/clusters (accessed on Jun 19, 2019).

37. Kaur, K. A Survey on Internet of Things - Architecture, Applications, and Future Trends. In Proceedings of the 1st International Conference on Secure Cyber Computing and Communication, ICSCCC 2018; IEEE: Jalandhar, India, 2018, 581–583.

38. Yeo, K.S.; Chian, M.C.; Wee Ng, T.C.; Tuan, D.A. Internet of things: Trends, challenges and applications. In Proceedings of the 14th International Symposium on Integrated Circuits, ISIC 2014; IEEE: Singapore, Singapore, 2015; pp. 568–571.

39. Conne3tion Top IoT Trends in 2019 – Conne3ion Available online: https://connexion3.gr/top-iot-trends-in-2019/ (accessed on Feb 13, 2019).

40. CISCO Cisco Visual Networking Index : Forecast and Trends , Available online: https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1955935 (accessed on Nov 27, 2018).

41. MacGillivray, C.; Torchia, M.; Bisht, A.; Crook, S.; Kalal, M.; Leung, J.; Membrila, R.; Sivier, A.; Torisu, Y.; Wallis, N. Worldwide Internet of Things Forecast, 2018–2022 Available online: https://webcache.googleusercontent.com/search?q=cache:g3mad0qnI8wJ:https://www.idc.com/getdoc.jsp%3FcontainerId%3DUS44755019+&cd=4&hl=en&ct=clnk&gl=uk (accessed on Jun 18, 2020).

42. Pramod, B. IoT Security Market Statistic-2026 Available online: https://www.alliedmarketresearch.com/automotive-tire-market (accessed

on Jan 20, 2020).

43. Yan, Z.; Zhang, P.; Vasilakos, A. V. A survey on trust management for Internet of Things. *J. Netw. Comput. Appl.* **2014**, *42*, 120–134.

44. Xu, L. Da; He, W.; Li, S. Internet of Things in Industries : A Survey. *IEEE Trans. Ind. INFORMATICS* **2014**, *10*, 2233–2243.

45. Borgia, E. The internet of things vision: Key features, applications and open issues. *Comput. Commun.* **2014**, *54*, 1–31.

46. ITU-T *Overview of internet of things*; 2018; Vol. 10.

47. ISO/IEC *Information technology – Internet of Things Reference Architecture (IoT RA)*; Switzerland, 2018; Vol. 20.

48. iiconsortium *The Industrial Internet of Things Volume G1: Reference Architecture*; 2019;

49. iiconsortium *Industrial Internet of Things Volume G4 : Security Framework*; 2016;

50. Hankel, M.; Rexroth, B. *The Reference Architectural Model Industrie 4.0 (RAMI 4.0)*; 2015;

51. Bauer, M.; Boussard, M.; Bui, N.; Walewski, W.J.; Carrez, F.; Jardak, C.; De Loof, J.; Magerkurth, C.; Meissner, S.; Nettstrater, A.; et al. *Internet of Things – Architecture Final architectural reference model for the IoT v3 . 0*; 2013;

52. IEEE SA IEEE Standards Activities in the Internet of Things (IoT) Overview Available online: https://standards.ieee.org/initiatives/iot/stds.html (accessed on Nov 14, 2018).

53. Basavanthappa, N. *Microsoft Azure IoT Reference Architecture*; 2018.

54. INTEL *The Intel® IoT Platform Architecture Specification White Paper*

Internet of Things (IoT); 2016.

55. Malessa, M.; Schmerbauch, R.; Obermeier, T. SAP on IBM i Reference Architecture Available online: https://www.sap.com/documents/2015/08/fc338289-5b7c-0010-82c7-eda71af511fa.html (accessed on Oct 4, 2017).

56. Jiang, X.; Chen, X.; Yang, W.; Xu, L. Reference Architecture for IBM Cloud Pak for Data with Lenovo ThinkSystem Servers and Storage Available online: https://lenovopress.com/lp1229-ibm-cloud-pak-for-data-reference-architecture (accessed on Oct 14, 2019).

57. ENISA 2018 CTI-EU | Bonding EU Cyber Threat Intelligence. Available online: https://www.enisa.europa.eu/events/2018-cti-eu-event (accessed on Nov 5,2018).

58. Alhalafi, N.; Veeraraghavan, P. Privacy and Security Challenges and Solutions in IOT: A review. In Proceedings of the International Conference on Smart Power & Internet Energy Systems; Melbourne, Australia, 2019; Vol. 322, pp. 1–5.

59. Minoli, D.; Sohraby, K.; Kouns, J. IoT Security (IoTSec) Considerations , Requirements , and Architectures. In Proceedings of the 14th IEEE Annual Consumer Communications & Networking Conference (CCNC); IEEE: Las Vegas, NV, USA, 2017; pp. 1006–1007.

60. Liu, D.; Gao, Y. Fingerprint identification simulation system. In Proceedings of the 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, DCABES 2010; IEEE: Hong Kong, China, 2010; pp. 533–538.

61. Park, Y.H.; Lee, H.C.; Park, K.R.; Tien, D.N.; Lee, E.C.; Kim, S.M.; Kim, H.C. A multimodal biometric recognition of touched fingerprint and finger-vein. In Proceedings of the International Conference on Multimedia and Signal Processing, CMSP 2011; IEEE: Guilin, Guangxi, China, 2011; Vol.

1, pp. 247–250.

62. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A survey of internet of things (IoT) authentication schemes. *Sensors (Switzerland)* **2019**, *19*, 1–43.

63. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Commun. Surv. Tutorials* **2018**, *20*, 3453–3495.

64. Filder, P.D. Was Stuxnet an Act of War? Decoding a Cyberattack. *IEEE Secur. Priv.* **2011**, *9*, 56–59.

65. Zetter, K. Is It Possible for Passengers to Hack Commercial Aircraft? Available online: https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/ (accessed on May 26, 2015).

66. Panchal, A.C.; Khadse, V.M.; Mahalle, P.N. Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures. In Proceedings of the IEEE Global Conference on Wireless Computing and Networking, GCWCN 2018; IEEE: Lonavala, India, 2018; pp. 124–130.

67. Symantec *Internet Security Threat Report 23 Volume*; 2018.

68. Hemsley, K.E.; Fisher, R.E. *History of Industrial Control System Cyber Incidents*; Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.

69. Poongodi, M.; Vijayakumar, V.; Al-Turjman, F.; Hamdi, M.; Maode, M. Intrusion Prevention System for DDoS attack on VANET with reCAPTCHA Controller using Information based metrics. *IEEE Access* **2019**, *7*, 1–1.

70. Kamhoua, A.G.; Pissinou, N.; Iyengar, S.S.; Beltran, J.; Kamhoua, C.; Hernandez, L.B.; Njilla, L.; Makki, A.P. Preventing Colluding Identity Clone Attacks in Online Social Networks. In Proceedings of the IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW); IEEE: Atlanta, GA, USA, 2017; pp. 187–192.

71. Larson, M. 6 critical issues facing the Internet of Things Available online: https://www.networkworld.com/article/3026315/6-critical-issues-facing-the-internet-of-things.html (accessed on Feb 1, 2016).

72. Columbus, L. 2018 Roundup Of Internet Of Things Forecasts And Market Estimates Available online: https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/#eee4aca7d838 (accessed on Dec 13, 2018).

73. ICO. Guide to the General Data Protection Regulation (GDPR) Available online: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (accessed on Jun 22, 2019).

74. Nelson, K. The List_ Best and Worst Countries for Cybersecurity Available online: https://www.secureworldexpo.com/industry-news/countries-dedicated-to-cybersecurity (accessed on Nov 13, 2019).

75. HM Government National Cyber Security Strategy 2016-2021 Available online: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (accessed on Sep 11, 2017).

76. National Security & Defense A budget for amrica's future Available online: https://www.whitehouse.gov/omb/analytical-perspectives/ (accessed on Jul 31, 2018).

77. Sadowsky, G.; Dempsey, J.X.; Mack, B.J.; Schwartz, A. *Information Technology security handbook*; Washington, DC: World Bank, 2003; ISBN 0974788805.

78. ENISA Guidelines for SMEs on the security of personal data processing Available online: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing (accessed on Jan 27, 2017).

79. Dumont, D. Cyber security concerns of supervisory control and data acquisition (SCADA) systems. In Proceedings of the IEEE International Conference on Technologies for Homeland Security, HST 2010; IEEE: Waltham, MA, USA, 2010; pp. 473–475.

80. Shukla, S.K. Cyber Security of Cyber Physical Systems: Cyber Threats and Defense of Critical Infrastructures. In Proceedings of the 9th International Conference on VLSI Design and 2016 15th International Conference on Embedded Systems (VLSID); IEEE: Kolkata, India, 2016; pp. 30–31.

81. Babu, B.; Ijyas, T.; Muneer, P.; Varghese, J. Security issues in SCADA based industrial control systems. In Proceedings of the International Conference on Anti-Cyber Crimes, ICACC 2017; IEEE: Abha, Saudi Arabia, 2017; pp. 47–51.

82. Wolf, M.; Serpanos, D. Safety and security in cyber-physical systems and internet-of-things systems. *Proc. IEEE* **2018**, *106*, 9–20.

83. Goodin, D. First known hacker-caused power outage signals troubling escalation Available online: http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/%5Cnhttp://arstechnica.co.uk/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/ (accessed on Apr 1, 2016).

84. Ortiz, E.; Costello, T.; Shamlian, J. United Airlines Flights No Longer Grounded, Delays Remain Available online: http://www.msnbc.com/msnbc/united-airlines-passengers-say-flights-grounded-nationwide (accessed on Aug 7, 2015).

85. Perez, E. FBI: Hacker Chris Roberts claimed to hack into flights - CNN.com Available online: https://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html (accessed on May 19, 2015).

86. Falliiere, N. Stuxnet Introduces the First Known Rootkit for Industrial

Control Systems | Symantec Connect Community Available online: http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices (accessed on Aug 6, 2010).

87. Conklin, W.A. IT vs OT Security : A Time to Consider a Change in CIA to Include Resilience. In Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS); IEEE: Koloa, HI, USA, 2016; pp. 2642–2647.

88. Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges. *Proc. - IEEE Symp. Comput. Commun.* **2016**, 180–187.

89. Xu, Y.; Koide, H.; Vargas, D.V.; Sakurai, K. Tracing MIRAI malware in networked system. In Proceedings of the 6th International Symposium on Computing and Networking Workshops, CANDARW 2018; IEEE: Takayama, Japan, 2018; pp. 534–538.

90. Dudley, S. Top market pressures driving manufacturers to the IoT Available online: https://www.ibm.com/blogs/internet-of-things/iot-top-manufacturers-pressures/ (accessed on Jun 14, 2017).

91. Karnouskos, S. Stuxnet worm impact on industrial cyber-physical system security. *IECON Proc. (Industrial Electron. Conf.* **2011**, 4490–4494.

92. ptsecurity INDUSTRIAL COMPANIES Available online: https://www.ptsecurity.com/ww-en/analytics/ics-attacks-2018/ (accessed on May 3, 2018).

93. Symantec *Internet Security Threat Report Volume 24 | February 2019*; 2019; Vol. 24.

94. Taylor, E. 2019 Forcepoint Cybersecurity Predictions Report Available online: https://www.forcepoint.com/newsroom/2018/forcepoint-reveals-cybersecurity-predictions-2019-trusted-interactions-critical (accessed on Nov 13, 2018).

95. Robles, R.J.; Choi, M. Assessment of the Vulnerabilities of SCADA , Control Systems and Critical Infrastructure Systems. *Int. J. Grid Distrib. Comput.* **2009**, *2*, 27–34.

96. Stouffer, K.; Falco, J.; Kent, K. Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology. *Nist Spec. Publ.* **2008**, *800*.

97. Basseville, M. Statistical methods for change detection. In *Control Systems, Robotics and Automation*; Unbehauen, H., Ed.; Encyclopedia of Life Support Systems (EOLSS), 2009; Vol. XVI, pp. 130–145 ISBN 978-1-84826-605-6.

98. Pajic, M.; Member, S.; Mangharam, R.; Sokolsky, O.; Arney, D.; Goldman, J.; Lee, I. Model-Driven Safety Analysis of Closed-Loop. *IEEE Trans. Ind. Informatics* **2014**, *10*, 3–16.

99. Mitchell, R.; Chen, I. Behavior Rule Based Intrusion Detection for Supporting Secure Medical Cyber Physical Systems. In Proceedings of the 21st International Conference on Computer Communications and Networks (ICCCN); IEEE: Munich, Germany, 2012; pp. 1–7.

100. Chesebrough, D.; Hallman, W. The NDIA Cybersecurity for Advanced Manufacturing Joint Working Group (CFAM JWG) October Available online: https://www.ndia.org/divisions/working-groups/cfam (accessed on Oct 23, 2017).

101. Naval, S.; Laxmi, V.; Rajarajan, M.; Member, S. Employing Program Semantics for Malware Detection. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2591–2604.

102. Tirado, E.; Turpin, B.; Beltz, C.; Roshon, P.; Judge, R.; Gagneja, K. Future Network Systems and Security. In Proceedings of the Future Network Systems and Security. FNSS 2018. Communications in Computer and Information Science, Springer, Cham; Springer International Publishing,

Paris, France, 2018; Vol. 878, pp. 117–127.

103. Devi Kanchan, K.; Arumugam, S. Password Cracking Algorithm using Probabilistic Conjunctive Grammar. In Proceedings of the IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS); IEEE: Tamilnadu, India, 2019; pp. 1–4.

104. Huda, S.; Abawajy, J.; Alazab, M. Hybrids of support vector machine wrapper and filter based framework for malware detection. *Futur. Gener. Comput. Syst.* **2016**, *55*, 376–390.

105. Dong, W.; Liu, X. Robust and Secure Time-Synchronization Against Sybil Attacks for Sensor Networks. *IEEE Trans. Ind. Informatics* **2015**, *11*, 1482–1491.

106. Huda, S.; Abawajy, J.; Islam, R. A fast malware feature selection approach using a hybrid of multi-linear and stepwise binary logistic regression. *Concurr. Comput. Pract. Exp.* **2017**, *29*, 1–18.

107. Hurtaud, S. Global Cyber Executive Briefing Lessons from the front line Available online: https://www2.deloitte.com/content/dam/Deloitte/nz/Documents/risk/cyber-executive-briefing-nz.pdf (accessed on Nov 8, 2019).

108. Liptak, A. Renault shut down several French factories after cyberattack - The Verge Available online: https://www.theverge.com/2017/5/14/15637472/renault-nissan-shut-down-french-uk-factories-wannacry-cyberattack (accessed on May 14, 2017).

109. Ylmaz, E.N.; Ciylan, B. Cyber Security in Industrial Control Systems : Analysis of DoS Attacks against PLCs and the Insider Effect. In Proceedings of the 2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG); IEEE: Istanbul, Turkey, 2018; pp. 81–85.

110. Langer, R. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Secur. Priv.*

2011, *9*, 49–51.

111. Chen, T.M.; Abu-Nimeh, S. Lessons from Stuxnet. *Computer (Long. Beach. Calif).* **2011**, *44*, 91–93.

112. Moubarak, J.; Filiol, E. Comparative Study of Recent MEA Malware Phylogeny. In Proceedings of the 2nd International Conference on Computer and Communication Systems; IEEE: Krakow, Poland, 2017; pp. 16–20.

113. Kim, H.; Broman, D.; Lee, E.A. An Architectural Mechanism for Resilient IoT Services. In Proceedings of the 1st ACM Workshop on the Internet of Safe Things; Delft, Netherlands, 2017; pp. 1–7.

114. Elhabashy, A.E.; Wells, L.J.; Camelio, J.A.; Woodall, W.H. A cyber-physical attack taxonomy for production systems : a quality control perspective. *J. Intell. Manuf.* **2019**, *30*, 2489–2504.

115. Do, Q.; Martini, B.; Choo, K.R. Is the data on your wearable device secure ? An Android Wear smartwatch case study. *Softw. Pract. Exp.* **2017**, *47*, 391–403.

116. Ibrahim, A.; Tsudik, G. DARPA : Device Attestation Resilient to Physical Attacks. In Proceedings of the WiSec '16: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks; ACM Digital Library: Darmstadt Germany, 2016; pp. 171–182.

117. Johnson, C. Securing Safety-Critical SCADA in the Internet of Things. In Proceedings of the 11th International Conference on System Safety and Cyber Security (SSCS 2016), Securing Safety-Critical SCADA in the Internet of Things; IEEE: London, UK, 2016; pp. 1–6.

118. Zetter, K. Why Firmware Is So Vulnerable to Hacking, and What Can Be Done About It Available online: https://www.wired.com/2015/02/firmware-vulnerable-hacking-can-done/ (accessed on Feb 24, 2015).

119. Selander, G.; Mattsson, J.; Palombini, F.; Seitz, L. Object Security for

Constrained RESTful Environments (OSCORE) Available online: https://tools.ietf.org/id/draft-ietf-core-object-security-05.html (accessed on Sep 29, 2017).

120. Karmakar, K.K.; Varadharajan, V.; Nepal, S.; Tupakula, U. SDN enabled secure IoT architecture. In Proceedings of the IFIP/IEEE Symposium on Integrated Network and Service Management, IM 2019; IEEE: Arlington, USA, 2019; pp. 581–585.

121. Porambage, P.; Schmitt, C.; Kumar, P.; Gurtov, A.; Ylianttila, M. PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications. *Int. J. Distrib. Sens. Networks* **2014**, 1–14.

122. Cromwell, B. Massive Failures of Public-Key Infrastructure (PKI) Available online: https://cromwell-intl.com/cybersecurity/pki-failures.html (accessed on Feb 9, 2020).

123. Beck, K.; Beedle, M.; Van Bennekum, A.; Cockburn, A.; Cunningham, W.; Fowler, M.; Grenning, J.; Highsmith, J.; Hunt, A.; Jeffries, R.; et al. Manifesto for agile software development twelve principles of agile software Available online: http://www.agilemanifesto.org (accessed on Jun 22, 2020).

124. OWASP OWASP Available online: https://owasp.org/about/ (accessed on Jul 26, 2019).

125. OWASP OWASP Internet of Things Project - OWASP Available online: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab.3DIoT_Attack_Surface_Areas (accessed on Nov 1, 2019).

126. OWASP Internet of Things Top Ten Available online: https://owasp.org/www-project-internet-of-things/ (accessed on Nov 1, 2019).

127. Khan, R.; Mclaughlin, K.; Laverty, D.; Sezer, S. STRIDE-based Threat

Modeling for Cyber-Physical Systems. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe); IEEE: Torino, Italy, 2017; pp. 1–6.

128. Charney, S. Trustworthy Computing Next Available online: http://webcache.googleusercontent.com/search?q=cache:pMC_lkBPZrYJ:download.microsoft.com/download/e/3/3/e33d31c2-e075-44ca-b4e8-dacdbc8882e7/trustworthy%2520computing%2520next%2520white%2520paper.pdf+&cd=1&hl=en&ct=clnk&gl=uk (accessed on Feb 28, 2012).

129. Saini, V.K.; Duan, Q.; Paruchuri, V. Threat modeling using attack trees. *J. Comput. Sci. Coll.* **2008**, *23*, 124–131.

130. Aksu, M.U.; Dilek, M.H.; Tatli, E.I.; Bicakci, K.; Dirik, H.I.; Demirezen, M.U.; Aykir, T. A Quantitative CVSS-Based Cyber Security Risk Assessment Methodology For IT Systems. In Proceedings of the International Carnahan Conference on Security Technology; IEEE: Madrid, Spain, 2017; pp. 1–8.

131. Luna, J.; Suri, N.; Krontis, I. Privacy-by-Design Based on Quantitative Threat Modeling. In Proceedings of the 7th International Conference on Risks and Security of Internet and Systems (CRiSIS); IEEE: Cork, Ireland, 2012; pp. 1–8.

132. Saitta, P.; Larcom, B.; Eddington, M. Trike v . 1 Methodology Document Available online: https://www.octotrike.org/papers/Trike_v1_Methodology_Document-draft.pdf. (accessed on Jul 13, 2005).

133. Mead, N.R.; Shull, F.; Vemuru, K.; Villadsen, O. A Hybrid Threat Modeling Method Available online: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=516617 (accessed on Mar 18, 2018).

134. Alberts, C.J.; Behrens, S.G.; Pethia, R.D.; Wilson, W.R. *Operationally Critical Threat , Asset , and Vulnerability (OCTAVE) Framework , version 1.0*, 1999.

135. Camarinha-matos, L.M. SCIENTIFIC RESEARCH Unit 1 : INTRODUCTION Some key questions, Uninova - Instituto Desenvolvimento de Novas Tecnologias, 2009.

136. Shuttleworth, M.; Wilson, L.T. Definition of Research Available online: https://explorable.com/definition-of-research (accessed on Feb 7, 2020).

137. Creswell, J.W. *Research design: qualitative, quantitative, and mixed methods approaches*; 4th ed.; Sage Publications: Los angeles: University of Nebraska–Lincoln, 2014; ISBN 9781452226095.

138. Bailey, K. *Methods of Social Research*; Free Press: New York, United States, 2008; Vol. 1; ISBN 13: 9781416576945.

139. Kumar, R. *Research methodology: a step-by-step guide for beginners*; 3rd ed.; Sage Publications, 2005; ISBN 9781849203005.

140. Robson, C. *Real world research: a resource for social scientists and practitioner-researchers*; 3rd ed.; John Wiley & Sons, 2002; ISBN 978-1405182409.

141. Wisker, G. *The postgraduate research handbook: succeed with your MA, MPhil, EdD and PhD*; Palgrave: Basingstoke, 2001; ISBN 0333747771.

142. Gummesson, E. *Qualitative Methods in Management Research*; 2nd ed.; Sage Publications: London, 2000; ISBN 0761920145, 9780761920144.

143. Walliman, N.; Bousmaha, B. *Your research project: a step-by-step guide for the first-time researcher*; 2nd ed.; Sage: London, 2005; ISBN 1412901324.

144. Yin, R.K. *Case study research: design and methods*; 4th ed.; Sage Publications: London, 2003; Vol. 5; ISBN 1412960991, 9781412960991.

145. Cohen, L.; Manion, L.; Morrison, K. *Research methods in education*; 5th ed.; Routledge: London, 2002.

146. BS ISO 13372:2012 Condition monitoring and diagnostics of machines —

Vocabulary Available online: https://shop.bsigroup.com/ProductDetail/?pid=000000000030218267 (accessed on Nov 30, 2012).

147. Rashid, M.; Anwar, M.W. System Engineering for Embedded Systems. In Proceedings of the System of Systems Engineering Conference (soSE); IEEE: Kongsberg, Norway, 2016; pp. 1–6.

148. Blank, M.R.; Gallagher, D.P. Guide for Conducting Risk Assessments Available online: https://webcache.googleusercontent.com/search?q=cache:0NORUNg2snIJ:https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf+&cd=1&hl=en&ct=clnk&gl=uk (accessed on Sep 12, 2012).

149. Schmalenberg, F.; Vandenhouten, R. An advanced data processing environment based on data flow diagrams with a flexible triggering and execution model. In Proceedings of the IEEE 14th International Symposium on Applied Machine Intelligence and Informatics - Proceedings; IEEE: Herl'any, Slovakia, 2016; pp. 159–164.

150. Xu, H.; Su, J.; Zong, X.; Yan, L. Attack identification for software-defined networking based on attack trees and extension innovation methods. In Proceedings of the IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2017; IEEE: Bucharest, Romania, 2017; Vol. 1, pp. 485–489.

151. BS EN 13306:2017 Maintenance — Maintenance terminology Available online: https://shop.bsigroup.com/ProductDetail?pid=000000000030324472 (accessed on Dec 21, 2017).

152. Werner, A.; Mehta, P.; Mears, L. Msec2011-50132 Development of a Condition Based Maintenance Program for a Cnc. *Signal Processing* **2011**, 1–9.

153. Mori, M.; Fujishima, M.; Komatsu, M.; Zhao, B.; Liu, Y. Development of remote monitoring and maintenance system for machine tools. *CIRP Ann. - Manuf. Technol.* **2008**, *57*, 433–436.

154. Emmanouilidis, C.; Bertoncelj, L.; Bevilacqua, M.; Tedeschi, S.; Ruiz-Carcel, C. Internet of Things - Enabled Visual Analytics for Linked Maintenance and Product Lifecycle Management. *IFAC-PapersOnLine* **2018**, *51*, 435–440.

155. Mehnen, J.; He, H.; Tedeschi, S.; Tapoglou, N. Practical Security Aspects of the Internet of Things. In *Cybersecurity for Industry 4.0*; 2017; pp. 1–33 ISBN 978-3-319-50659-3.

156. ENISA *Good Practices for Security of Internet of Things in the Context of Smart Manufacturing*; ENISA, 2018; ISBN 9789292042615.

157. ISO/IEC ISO / IEC 27001 Information Security Management System Available online: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en (accessed on Oct 10, 2013).

158. ISO/IEC Information technology — Security techniques — Information security risk management Available online: https://www.iso.org/standard/75281.html (accessed on Jul 1, 2018).

159. Zhang, X.; Wuwong, N.; Li, H.; Zhang, X. Information Security Risk Management Framework for the Cloud Computing Environments. In Proceedings of the 10th IEEE International Conference on Computer and Information Technology; IEEE: Bradford, UK, 2010; pp. 1328–1334.

160. Ajgaonkar, A.; Kapellmann, D.; Kothari, D.; Chiang, D.; Vhitiprolu, M.; Maregowda, S.T. *JPMorgan Chase & Co. Risk Assessment based on the 2014 Data Breach*; 2014;

161. Das, A.; Memik, G.; Zambreno, J.; Choudhary, A. Detecting / Preventing Information Leakage on the Memory Bus due to. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE

2010); IEEE: Dresden, Germany, 2010; pp. 861–866.

162. Becher, A.; Benenson, Z.; Dornseif, M. *Tampering with motes: Real-world attacks on wireless sensor networks*; Clark, J.A., Paige, R.F., Polack, F.A.C., Brooke, P.J., Eds.; Springer, Berlin, Heidelberg: Berlin, Germany, 2006; Vol. 3934; ISBN 978-3-540-33377-7.

163. Fachkha, C.; Bou-Harb, E.; Debbabi, M. Inferring distributed reflection denial of service attacks from darknet. *Comput. Commun.* **2015**, *62*, 59–71.

164. Soundararajan, S.; Arthur, J.D.; Balci, O. A methodology for assessing agile software development methods. *Proc. - 2012 Agil. Conf. Agil. 2012* **2012**, 51–54.

165. ACSC Australian Government Information Security Manual: Executive Companion Available online: https://www.cyber.gov.au/ism (accessed on Mar 2, 2020).

166. Daud, M.; Rasiah, R.; George, M.; Asirvatham, D.; Rahman, A.F.A.; Halim, A.A. Denial of service: (DoS) impact on sensors. In Proceedings of the 4th International Conference on Information Management, ICIM 2018; IEEE: Oxford, UK, 2018; pp. 270–274.

167. Meyer, D.; Haase, J.; Eckert, M.; Klauer, B. A threat-model for building and home automation. In Proceedings of the IEEE International Conference on Industrial Informatics (INDIN); IEEE: Poitiers, France, 2017; pp. 860–866.

168. Kang, D.J.; Lee, J.J.; Kim, S.J.; Park, J.H. Analysis on cyber threats to SCADA systems. In Proceedings of the IEEE Transmission and Distribution Conference and Exposition: Asia and Pacific; IEEE: Seoul, South Korea, 2009; pp. 1–4.

169. Young, N.; Drees, R. Cyber security for automatic test equipment. *IEEE Instrum. Meas. Mag.* **2018**, *21*, 4–8.

170. Gulati, R. The Threat of Social Engineering and Your Defense Against It.

SANS Readinng room **2003**, 1–12.

171. Rai, K.K.; Asawa, K. Impact analysis of rank attack with spoofed IP on routing in 6LoWPAN network. In Proceedings of the 10th International Conference on Contemporary Computing, IC3 2017; IEEE: Noida, India, 2017; pp. 1–5.

172. Anugurala, A.; Chopra, A. Securing and preventing man in middle attack in grid using open pretty good privacy (PGP). In Proceedings of the 4th International Conference on Parallel, Distributed and Grid Computing, PDGC 2016; IEEE: Waknaghat, India, 2016; pp. 517–521.

173. Nakhila, O.; Zou, C. Parallel active dictionary attack on IEEE 802.11 enterprise networks. In Proceedings of the IEEE Military Communications Conference MILCOM; IEEE: Baltimore, MD, USA, 2016; pp. 265–270.

174. Maraj, A.; Rogova, E.; Jakupi, G.; Grajqevci, X. Testing Techniques and Analysis of SQL Injection Attacks. In Proceedings of the 2nd International Conference on Knowledge Engineering and Applications; IEEE: London, UK, 2017; Vol. 5, pp. 55–59.

175. Leyden, J. Viruses infect vital control systems at TWO US power stations Available online: https://www.theregister.co.uk/2013/01/16/us_power_plant_malware/ (accessed on Jan 16, 2013).

176. Sa, P.K.; Sahoo, M.N. *Progress in Intelligent Computing Techniques : Theory , Practice , and Applications*; Kacprzyk, J., Ed.; Springer International Publishing, 2016; Vol. 518; ISBN 9789811033728.

177. Márquez, A.C. *The Maintenance Management Framework: Models and Methods for Complex Systems Maintenance*; illustrate.; Springer Science & Business Media, 2007; ISBN 1846288215, 9781846288210.

178. Thames, L.; Schaefer, D. *Cybersecurity for industry 4.0: Analysis for Design and Manufacturing*; 2017; ISBN 1617795631.

179. Oliveira, J.; Frade, M.; Pinto, P. System protection agent against unauthorized activities via USB devices. In Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018); Madeira, Portugal, 2018; pp. 237–243.

180. Ansari, M.H.; Vakili, V.T. Detection of clone node attack in mobile wireless sensor network with optimised cost function. *Int. J. Sens. Networks* 2017, *24*, 149–159.

181. Whiting, D.; Sorokos, I.; Papadopoulos, Y.; Regan, G.; O'Carroll, E. Automated model-based attack tree analysis using HiP-HOPS. *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)* **2019**, *11842 LNCS*, 255–269.

182. Sanders, A.; Sun, T.; Pan, Y.; Yuan, B. Correlating risk findings to quantify risk. In Proceedings of the 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust and 2012 ASE/IEEE International Conference on Social Computing, SocialCom/PASSAT 2012; IEEE: Amsterdam, Netherlands, 2012; pp. 752–759.

183. Clarke, E.M.; Henzinger, T.A.; Veith, H.; Bloem, R. *Handbook of model checking*; Springer link, 2018; ISBN 9783319105758.

APPENDICIES

Appendix A – Questionnaire

Questionnaire

The main objective of this questionnaire is to collect data regarding the common failure modes and the root causes of failure for CNC machines found in industrial environments.

(The data collected through this questionnaire will be the basis of a statistical study for a PhD in Remote Monitoring. This study focuses on the causes of degradation in CNC machines. If you provide your email address, a brief report containing the results of the survey will be sent to you through email. Please notice that all data will be treated anonymously)

1) *Part Discussion Guide:*

Project Name: **Condition Monitoring Module**

Structure: **Interviews/Observations**

Date:

Site Name/Location:

Name (optional):

Email (optional):

Affiliation (name of the company or a description of the company you work for):

Job title:

Job description:

Years of relevant experience on machines tools:

2) *Part 2 Degradation Questions:*

Research questions

1) When you come to the shift, how are you informed of what you will be responsible to complete on your shift? Does it change frequently?

2) Is there anything that you need to check on a daily basis? If yes, what machine, which

3) What's your machine reliability? What's the method to measure it (paper, software)? On a scale from 1 – 5 how, 5 being greatest, how would you rate the influence of unexpected machine breakdowns on delivery delays?

4) According to your experience, what functional parts of a machine tool are subject to increased maintenance during the life cycle?

Functional Groups	***Tick box if you consider this***	***Why?***
Spindle group		
Worktable system		
Axis control system		
Tool magazine		
Tool change system		
Refrigeration system		
Lubrication system		
Functional Groups	***List them***	***Why?***
Other:		
Other:		
Other:		

5) What are the common causes associated with the degradation mechanisms of these functional parts?

Common causes	***Tick box if you consider this***
Vibrations	
Overstressing	
Torsion	
Mechanical seizing	
Mechanical stress	
Thermal stress	

Wear	
Other:	

6) Which of the common causes you listed above occur more frequently?

Parameter	***Common causes***
Once a week	
Once a month	
Once a year	
Less than once a year	
Other:	

7) Research in relevant literature shows that one of the most critical components of milling machines is the spindle. Which of the causes of damage listed below can be considered as critical against the life of the spindle? (Please complete the table below in response to this question)

Parameter	***Tick box if you consider critical***	***Why***
Wear of the components of the spindle		
Improper lubrication		
Axial and radial impacts		
Improper maintenance		
Other:		

8) What are the failure components for the spindle group of a machine tool?

Functional group	***Function***	***Subset***	***Component***	***Tick box if you consider this***
Spindle group	Tool motion	Motor	Bearings	
			Windings	
		Transmission system	Sensor range change	
			Solenoid valves	
			Hydraulic circuit	
		Control system Spindle	Boards actuation	
			Encoder orientation	
			Electrical circuit	

		Other:		

9) What is the frequency of diagnostic procedure used to identify damage in the spindle?

Functional group	***Description***	***Time***						
		During work	***Each day***	***Each month***	***Less every six months***	***Plus every six mounths***	***Each years***	***Other***
Spindle group	Inspection sensory noise							
	Inspection by analysing the vibration							
	Revision engine							
	Other:							

10) Who do you report to for maintaining these machine components?

Functional Groups	***Intern Expert/External Expert/Remote Service***
Spindle group	
Worktable system	
Axis control system	
Tool magazine	
Tool change system	
Refrigeration system	
Lubrication system	
Functional Groups	***List them***
Other:	
Other:	
Other:	

External expert technician	
Internal expert technician	
Remote service company	

Other:	

11) How is data collection on machine tool done? (measurement of temperature, vibration, noise)

Database internal to the machine	
Data acquisition unit connected to Cloud system	
Data acquisition unit external to the machine	
Other:	

12) Preventive maintenance can prevent machine breakdowns but reduce machine uptime. How would you rate the overall efficiency of PM method on a scale of 1-5, 5 being the greatest?

1	*2*	*3*	*4*	*5*
Comment	*Comment*	*Comment*	*Comment*	*Comment*

13) Do you use any software for maintenance work? Will it help if all preventive maintenance schedules for different machines are shown in one software?

14) If there is software that can generate maintenance orders based on actual health condition of machines, on a scale from 1 – 5, 5 being greatest, how willing would you be to implement the orders?

1	*2*	*3*	*4*	*5*
Comment	*Comment*	*Comment*	*Comment*	*Comment*

15) Who do you think should provide this software? Do you think cutting tool companies are good fit to develop this software?

16) How is the security of communication with the data acquisition unit ensured?

Password	
Cryptography	

Identification process	
Other:	

17) The project involves the development of a data acquisition unit. In your view, what are the most sensitive parameters that you would like to monitor? Please list below. Example (vibration, temperature, noise, other)

Thank you

Survey results

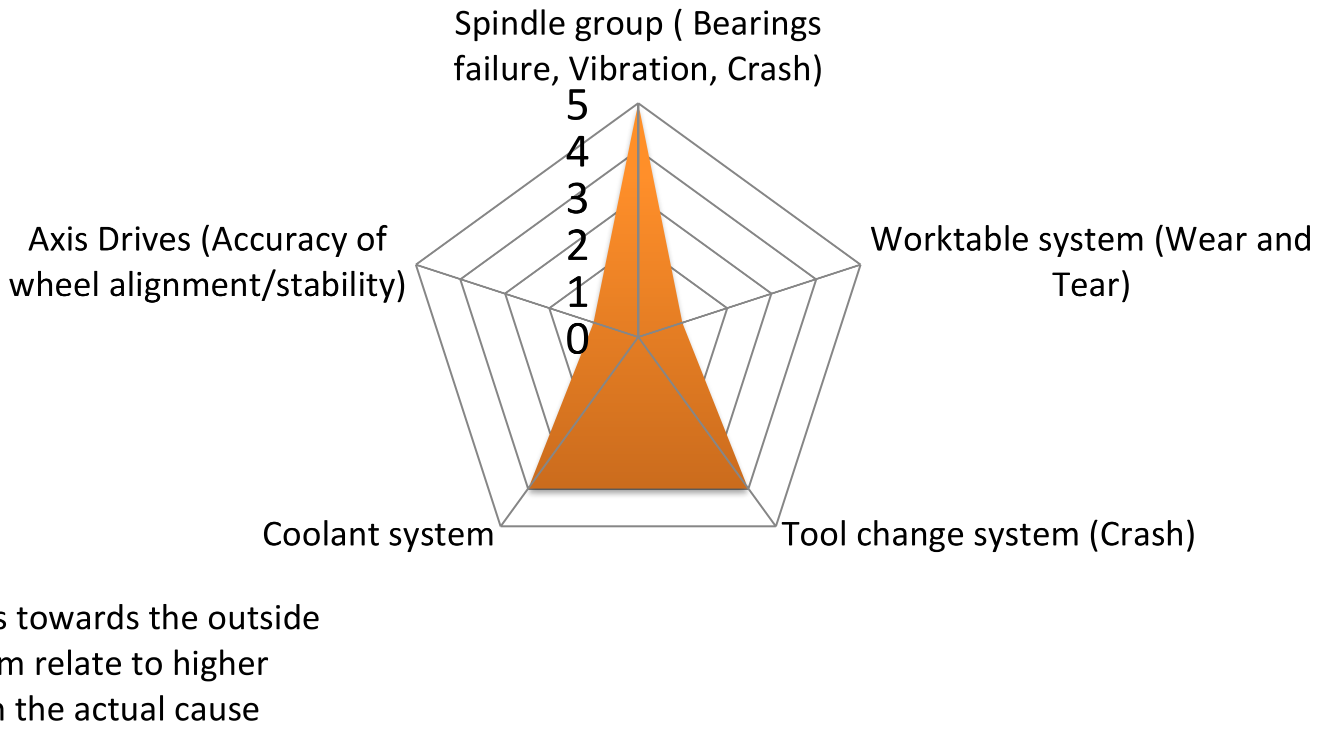
The purpose of this series of questions is to acquire expert knowledge about common failure modes and the root causes of failure for CNCs in industrial environments. The section allows experts to provide their knowledge based on their experience in the sector. The transcribed questions and answers produced are those necessary to support the research objective.

Part 1 Discussion Guide

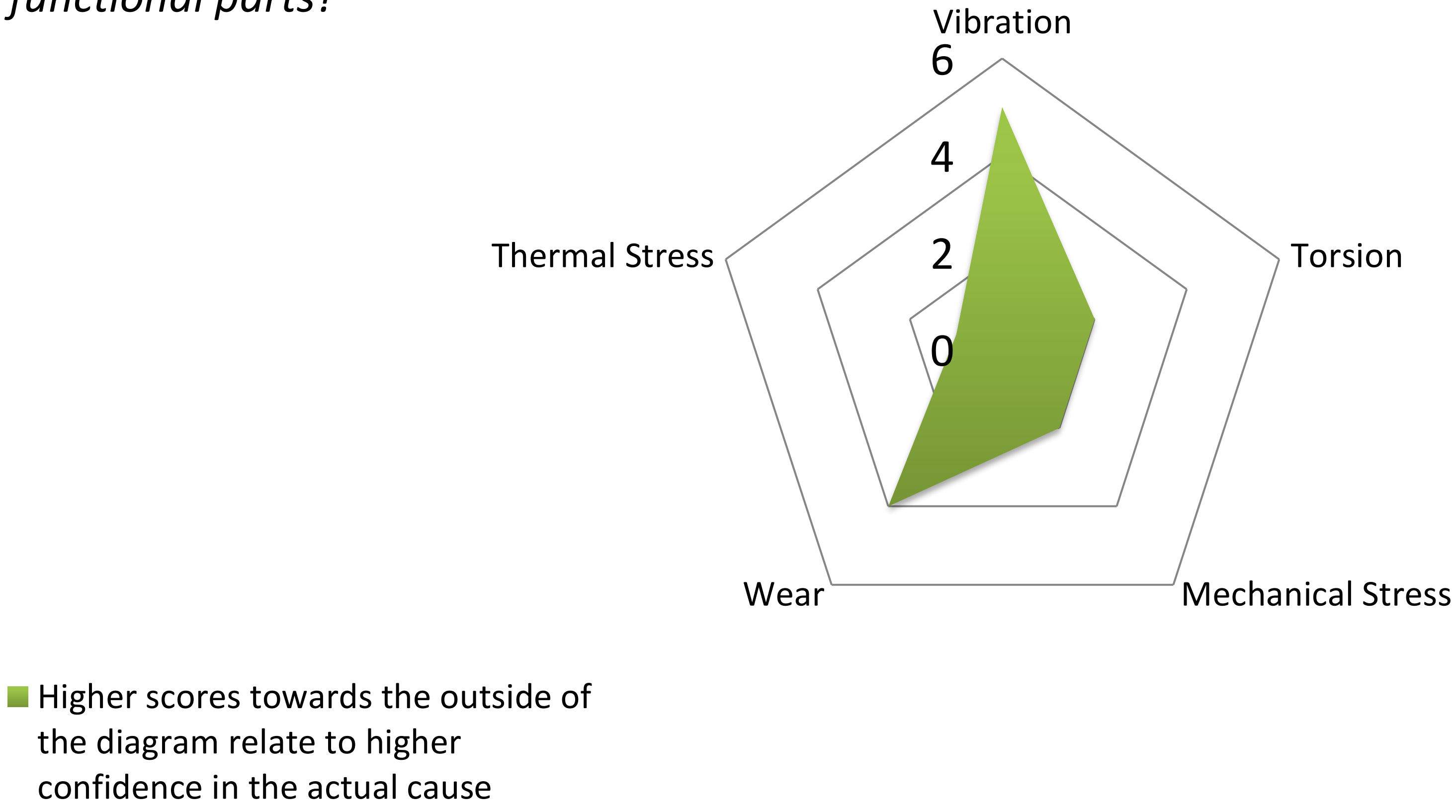
Company	Rolls-Royce Plc	DMG MORI	A.M.R.C. (PTG Group)	Cranfield University	BAE-Systems	PowerKut
Job title	**Machining Specialist**	**Application Engineer**	**Factory Manager**	**Research fellow**	**Engineer**	**Specialist**
Experience	**21**	**33**	**35**	**9**	**12**	**20**

Part 2 Degradation questions

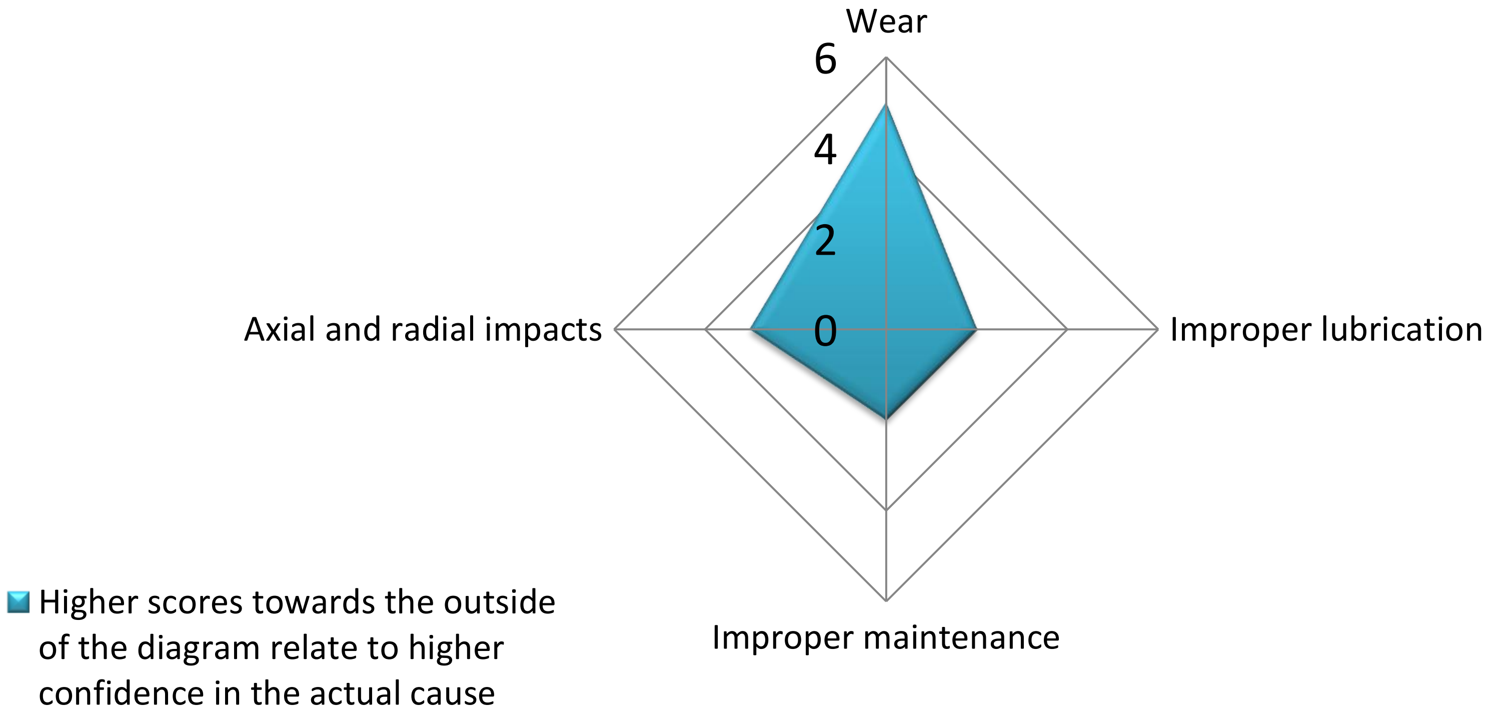
1. *According to your experience, what functional parts of a machine tool are subject to increased maintenance during the life cycle?*



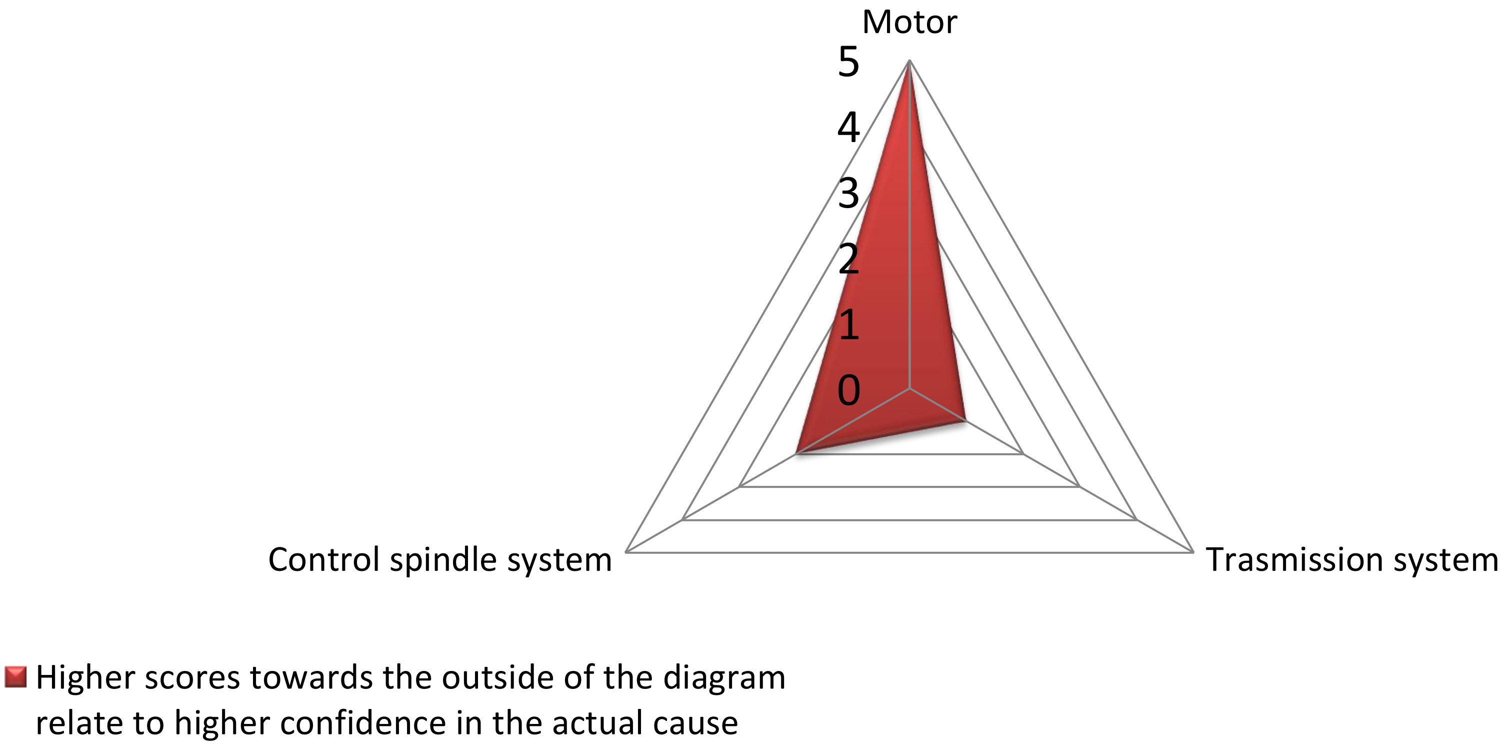
2.What are the common causes associated with the degradation mechanisms of these functional parts?



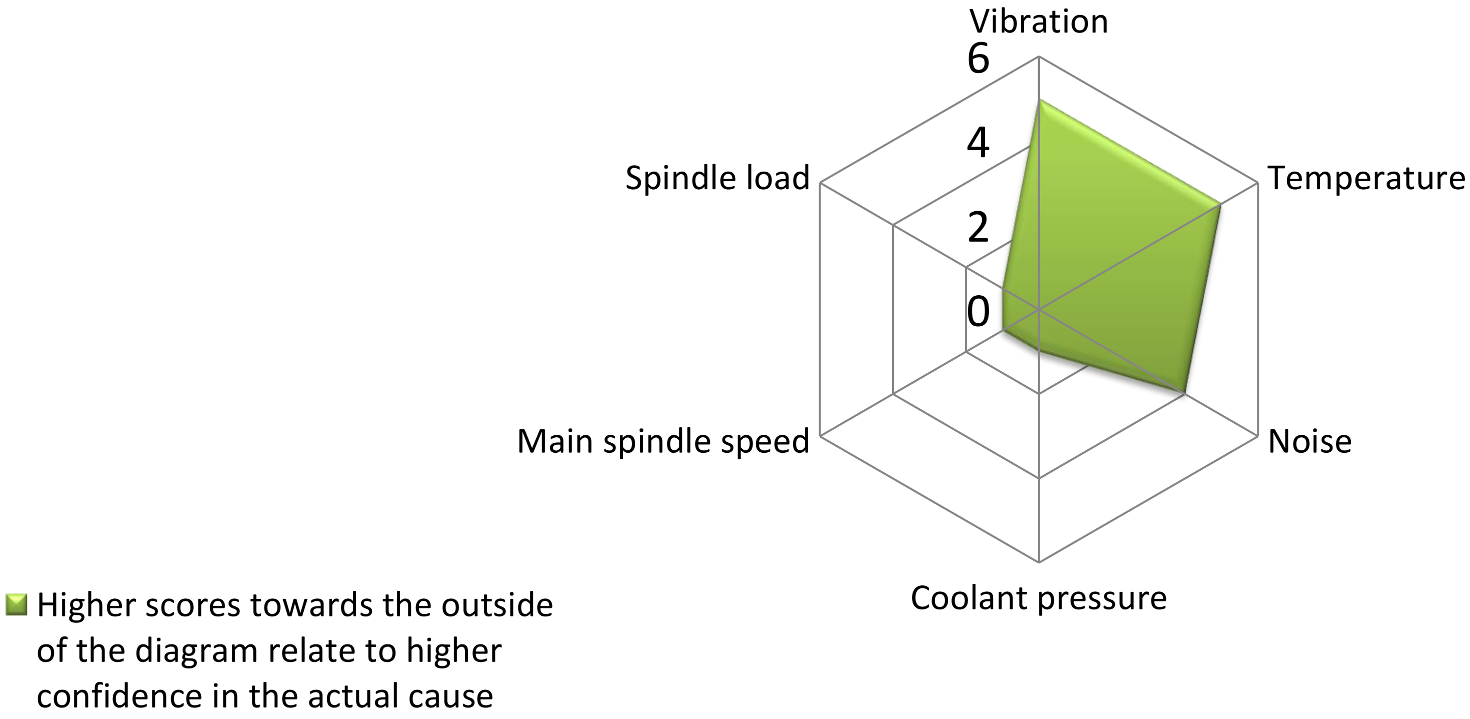
3.Research in relevant literature shows that one of the most critical components of milling machines is the spindle. Which of the causes of damage listed below can be considered as critical against the life of the spindle?

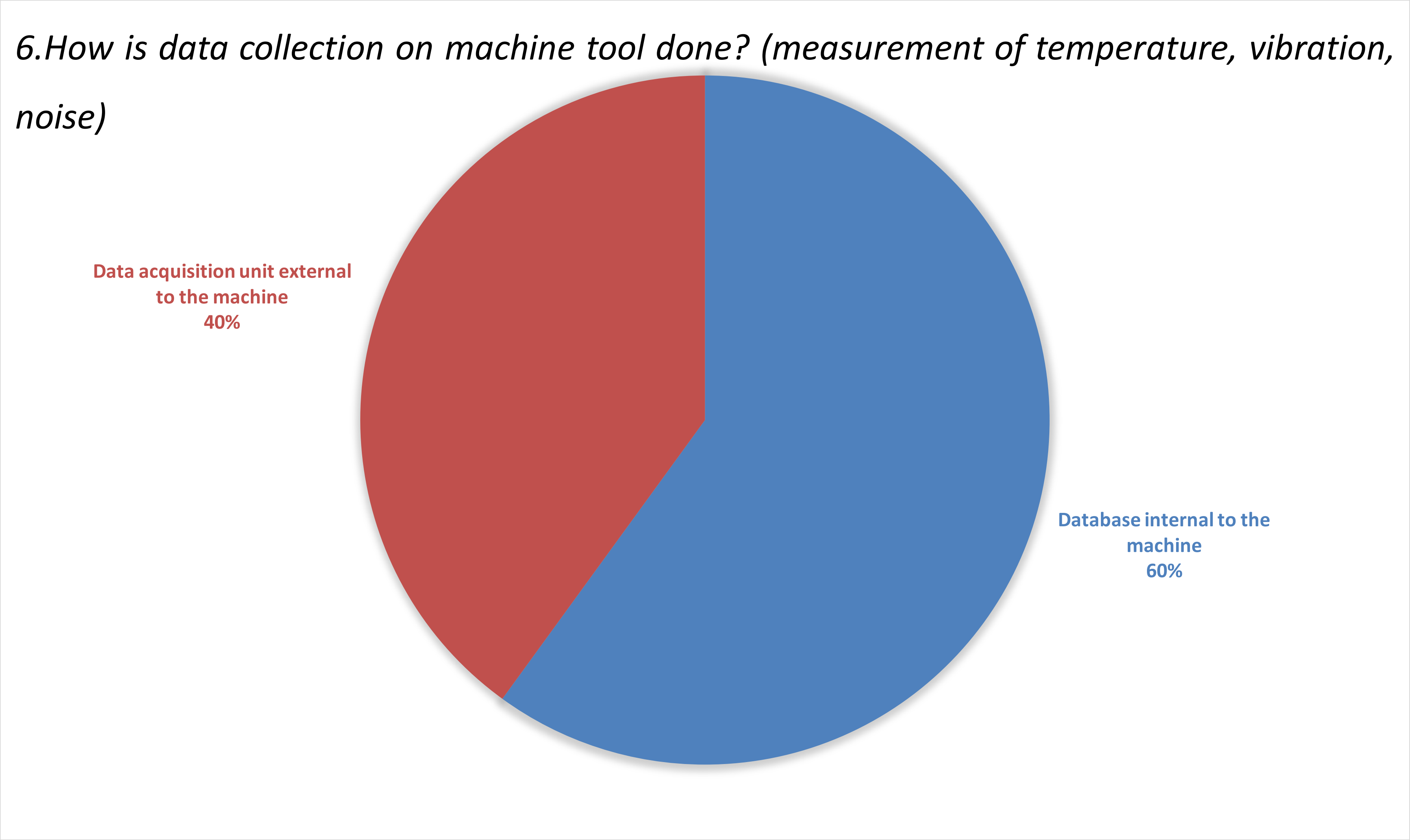


4.What are the failure components for the spindle group of a machine tool?



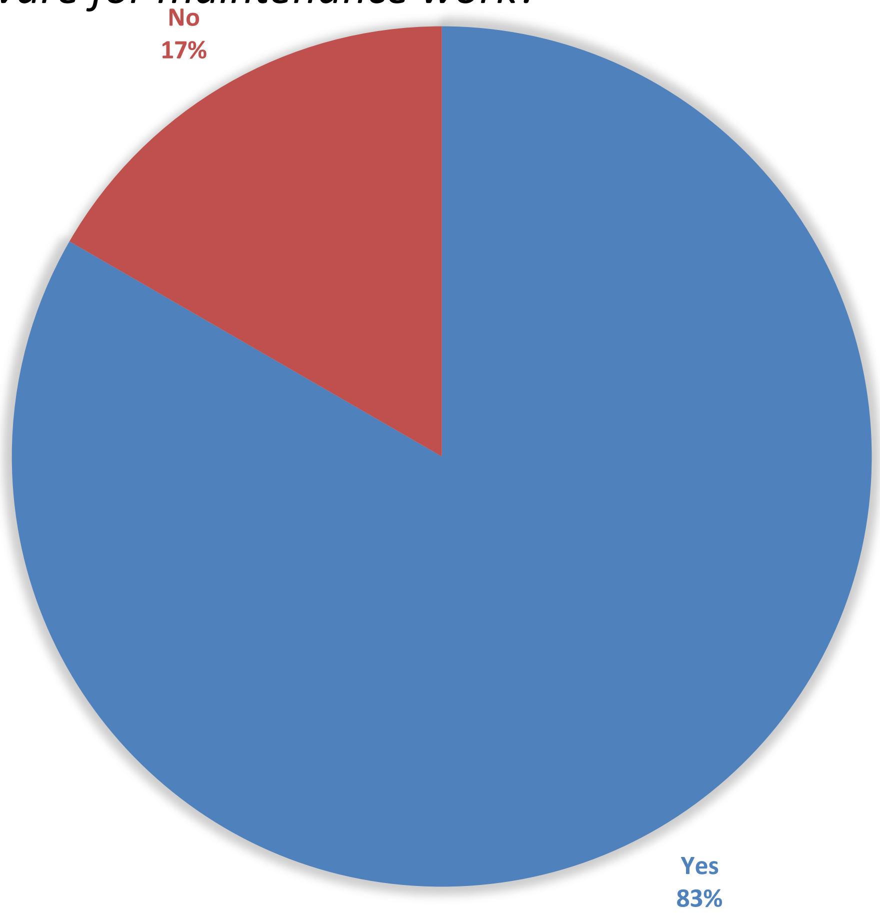
5.The project involves the development of a data acquisition unit. In your view, what are the most sensitive parameters that you would like to monitor? Please list below. Example (vibration, temperature, noise, other)



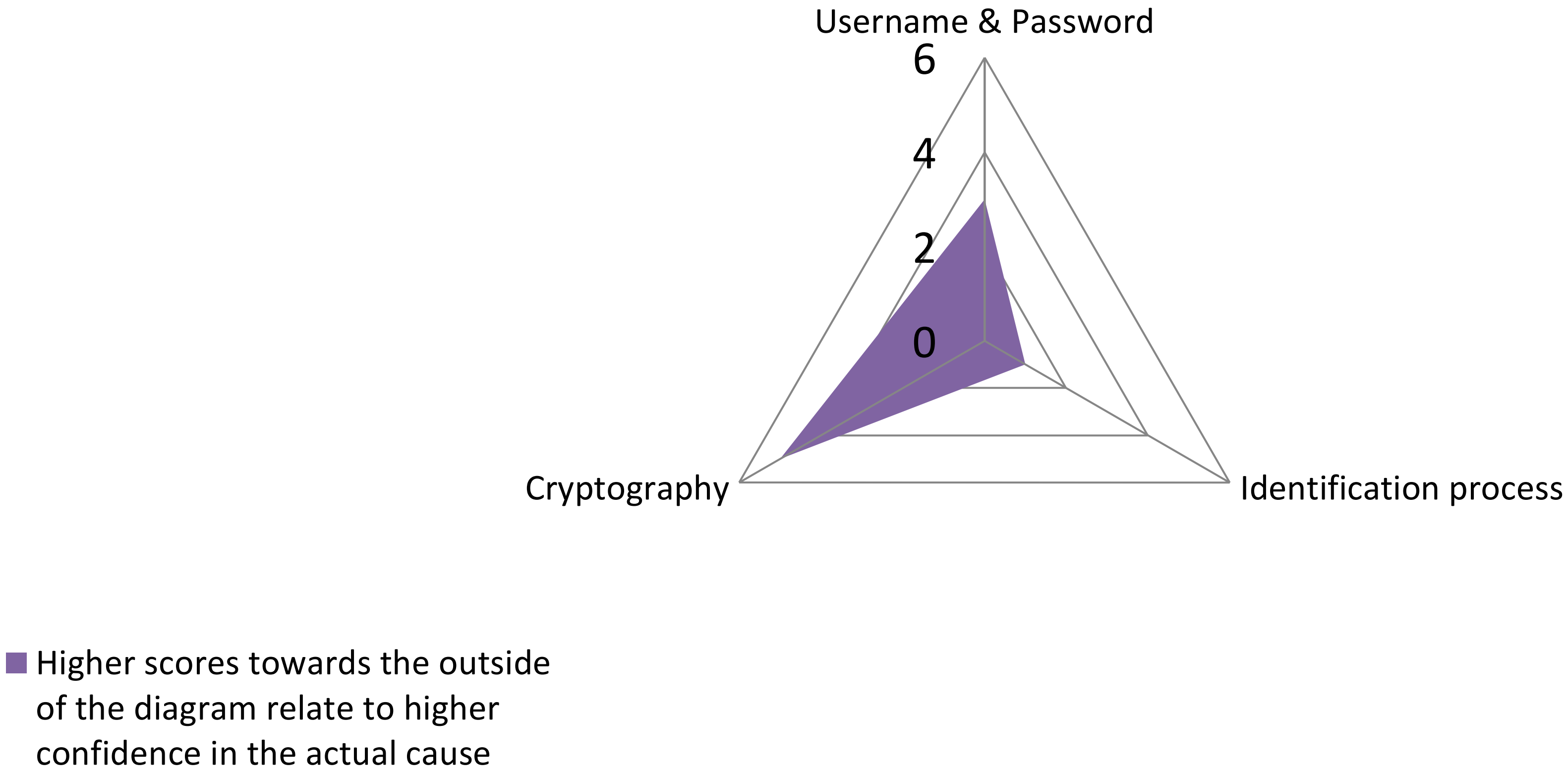


6.How is data collection on machine tool done? (measurement of temperature, vibration, noise)

7.Do you use any software for maintenance work?



8.How is the security of communication with the data acquisition unit ensured?

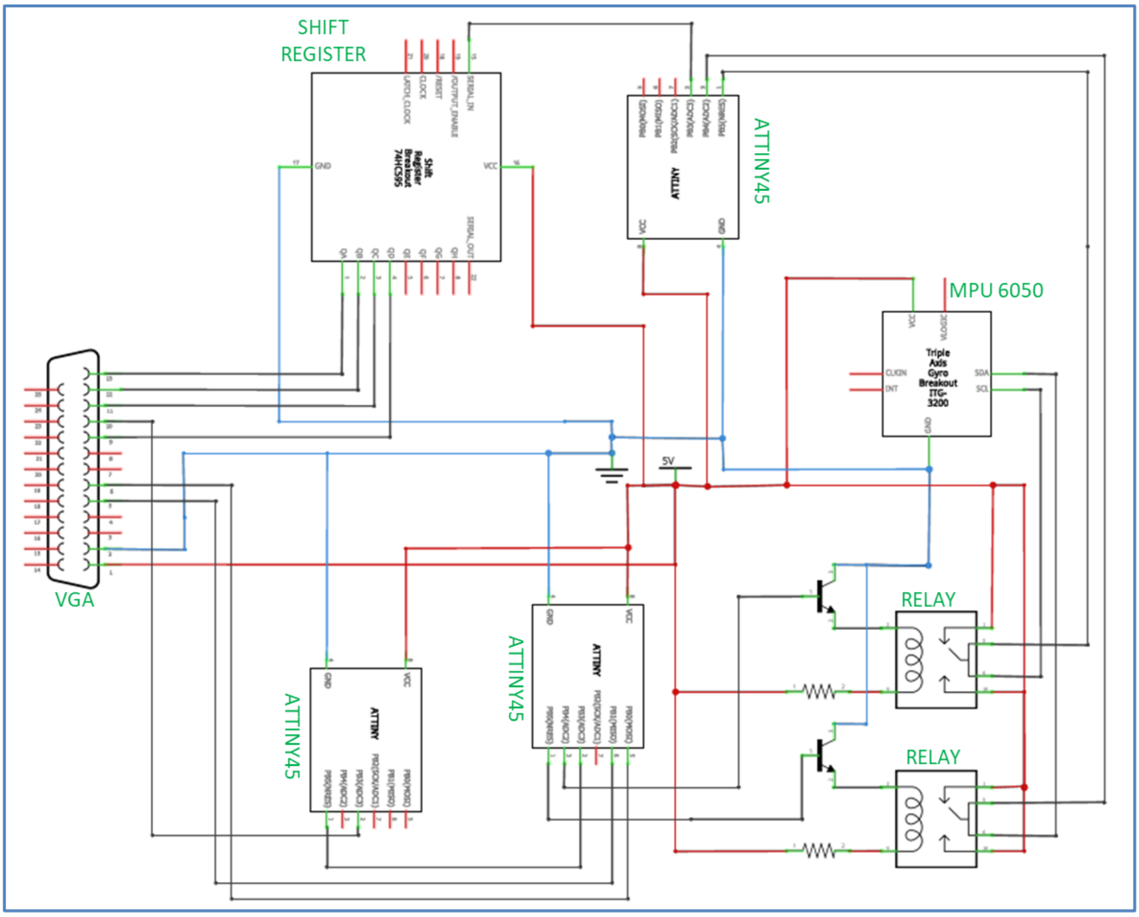


Summary

- ✓ The parts most subject to maintenance in a machine tool are: *spindle group, coolant system, tool change system.*
- ✓ The common causes associated with the degradation mechanisms of these functional parts are *vibration and wear*.
- ✓ The causes of damage considered as critical against the life of the spindle are: *wear*.
- ✓ The failure components for the spindle group are: *motor.*
- ✓ The parameters to be monitored are: *vibration, temperature and noise*.
- ✓ The data within the machine tool are collected with *data base internal to the machine.*
- ✓ Almost all of them use a *maintenance software*.
- ✓ Everyone says that software that helps predict the health of the machine tool would help the production.
- ✓ For communications security should be used *cryptography and password*.

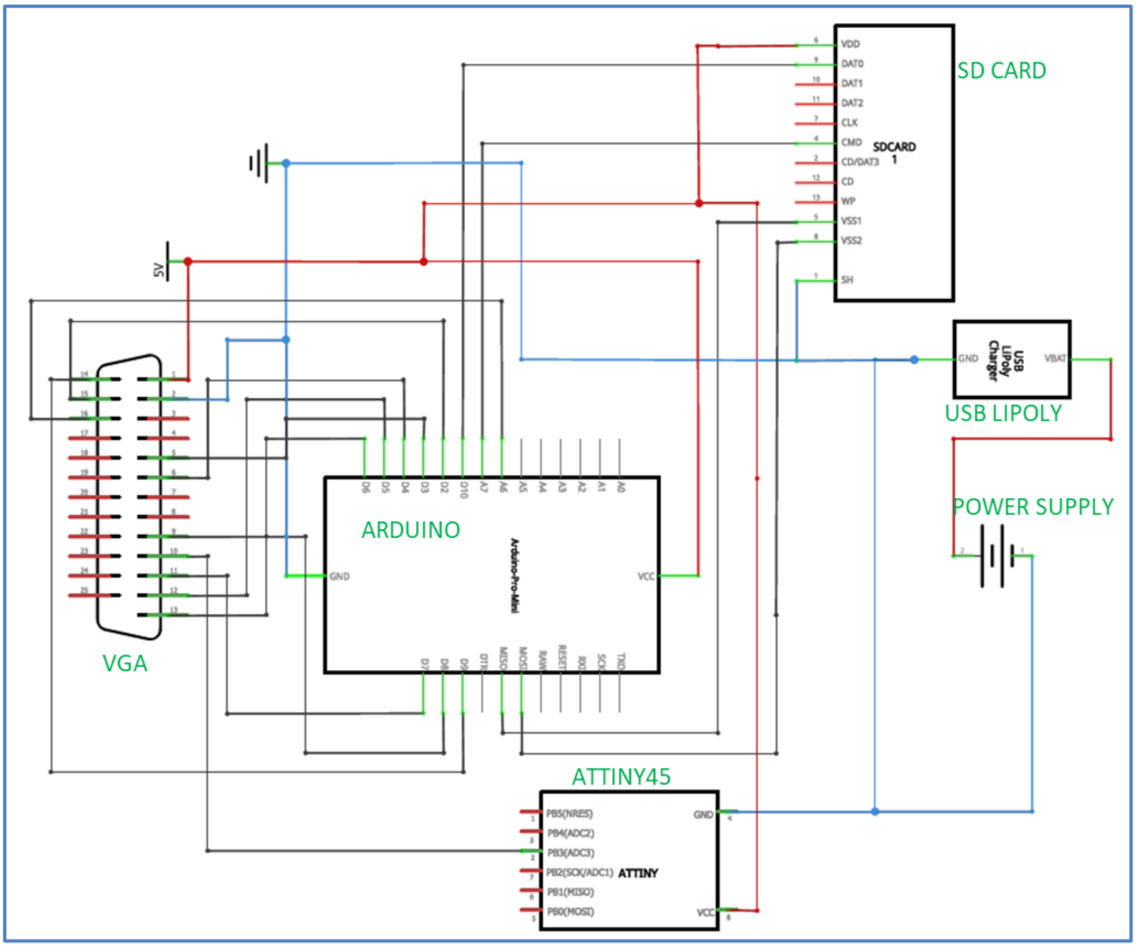
Appendix B – The connection diagram of each module of the modular IoT DAQ unit

Figure B-1 shows the sensor module or 1st module scheme, which consists of a Video Graphics Array (VGA) connector female db25, three Attiny45, two relays modules, a shift register 74HC165, and a MPU 6050 sensor.



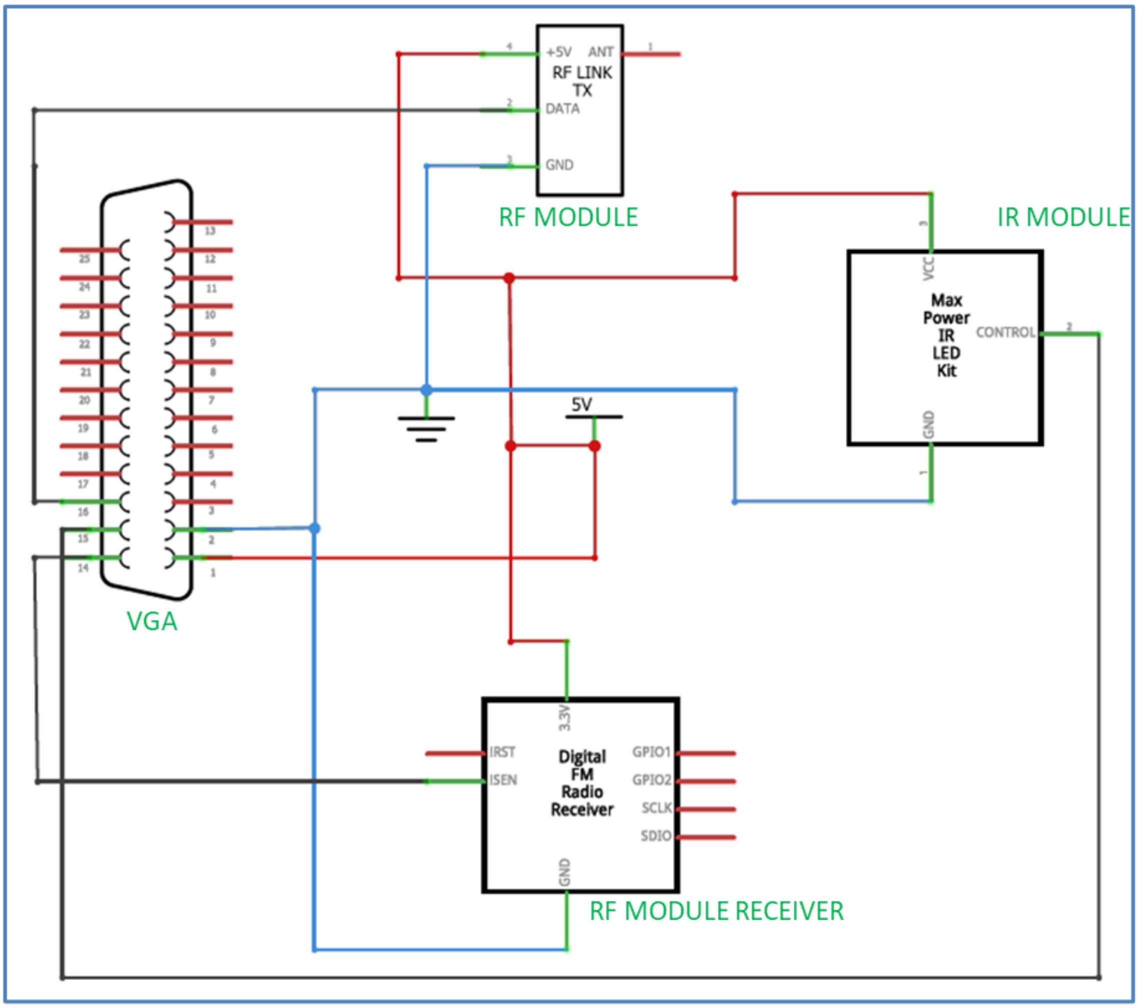
34**Figure B- 1: Intelligent sensor module**

Each component contributes to the proposed authentication protocol to increase the high-security level of the modular IoT device. A VGA connector is present for the transfer of signals between modules. The module consists of three Attiny45 for controlling parts of the authentication protocol, such as the encryption and decryption mechanisms and the hardware authentication process. The two-channel relay modules are used as electronic switches for the control unit module to transfer signals, baud rates, passwords, frequencies and keycodes to the sensors module. The shift register 74HC165 increases the number of the inputs in parallel and uses a serial output. For this particular case, it is used to generate noise and split the signal string into many pieces (sent through four outputs Oa, Ob, Oc, Od) which are then reconstructed into SCU or the cloud through a specific decryption algorithm.



35**Figure B- 1: Control unit module**

Figure B-2 shows the control unit module or 2nd module scheme which consists of a VGA connector male db25, an Arduino Pro mini, an Attiny45, SD module, an USB LIPOly charger and power supply. An Arduino Pro mini is in charge of the authentication protocol initialisations. It does not include physical external access on the single board. The Attany45 controls encryption and decryption mechanisms and the inputs for the hardware authentication step. A LIPOly charger is used for recharging the battery via solar panel while, an SD module is used to store temporary encrypted data.

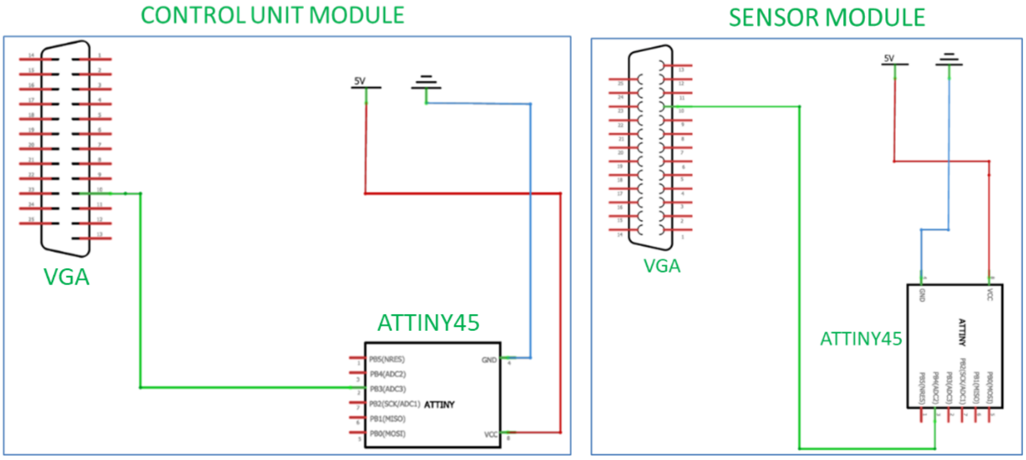


36**Figure B- 3: Communication module**

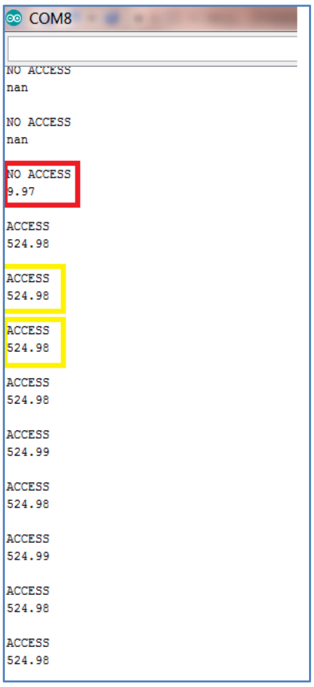
Finally, the communication module or 3rd module scheme is presented in figure B-3, which consists of a VGA connector female db25, a RF module 433 MHz to transmit and receive data and an infrared IR module for the user password.

Appendix C – Implementation of the LCCA authentication protocol

This section introduces the implementation tests of the authentication protocol. Each phase is described in detail through the physical connection diagram used for tracking the signal path during each step of the authentication protocol.



37**Figure C- 1: Log identity authentication physical phase - components involved**

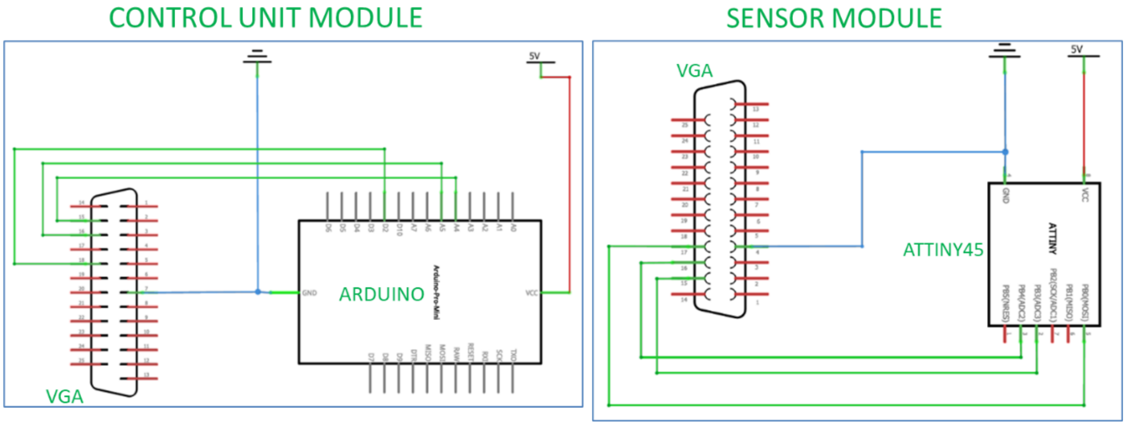


```
NO ACCESS
nan

NO ACCESS
nan

NO ACCESS
9.97

ACCESS
524.98

ACCESS
524.98

ACCESS
524.98

ACCESS
524.98

ACCESS
524.99

ACCESS
524.98

ACCESS
524.99

ACCESS
524.98

ACCESS
524.98
```

38**Figure C- 2: Log identity authentication - test ACCESS/NO ACCESS**

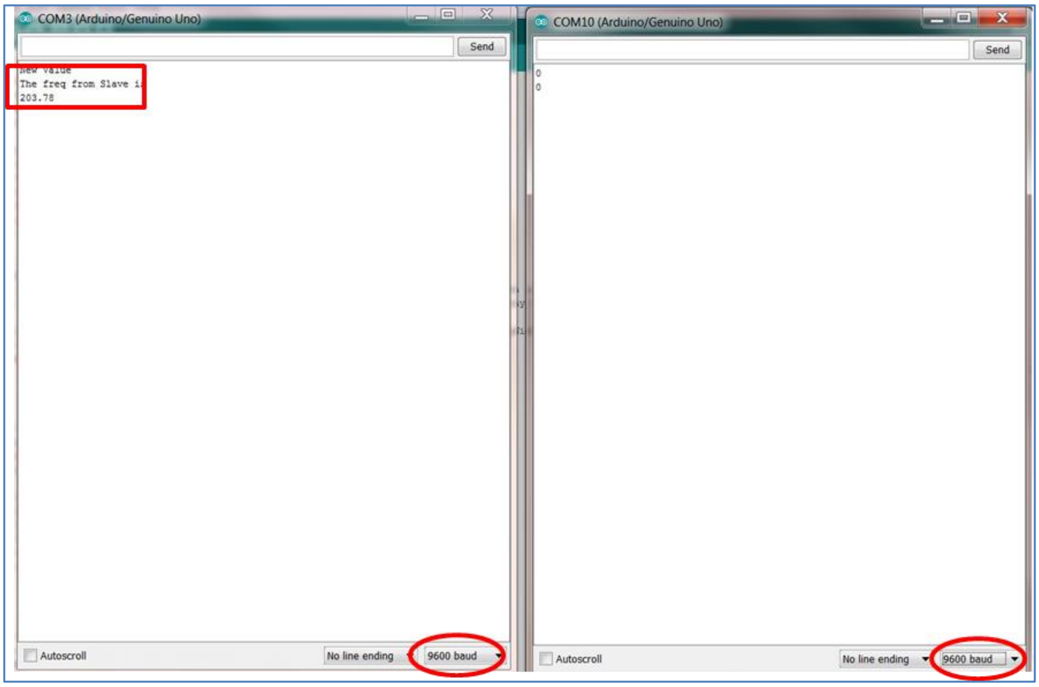
Figure C-1 shows the physical components involved in the first step of the authentication protocol, which are two Attiny45 one for each module.

The first connection is in place and the control unit module reads the private identity for the sensor module. If the identity of the sensor is recognised, the communications initialise. If the identity is not recognised the control unit module freezes the communication. Figure C-2 shows the keycode value generated by the control unit module and stored in each module. In detail, the control unit module has a record of keycodes for access which are recognised (values in the yellow squares) and not recognised (values in the red squares).



39**Figure C- 3: Encrypted communication phase – components involved**

Figure C-3 shows the physical components used during the second phase. The second phase involves the agreement of the new baud rate between the control unit module and the sensor module An Arduino pro mini and an attiny45 are used to achieve this.



```
New Value
The freq from Slave i
203.78
```

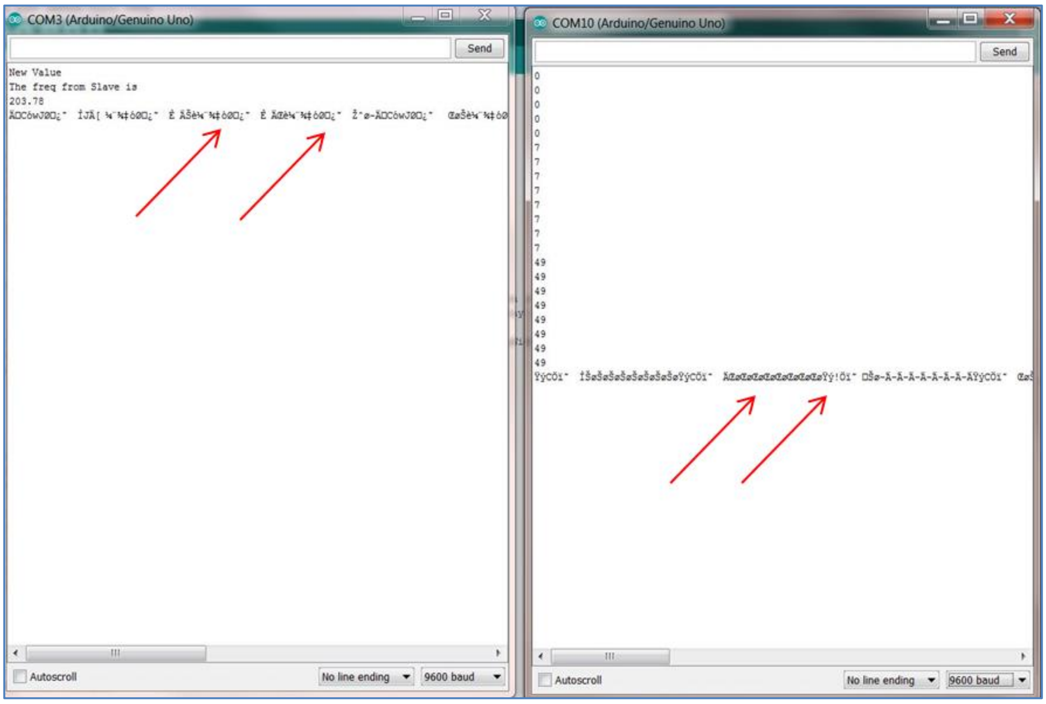
No line ending, 9600 baud

```
0
0
```

No line ending, 9600 baud

40**Figure C- 4: Log identity authentication**

During the first connection, the control unit module (COM3) recognises the keycode from the sensor module (COM10) and sets the new baud rate (Figure C-4).



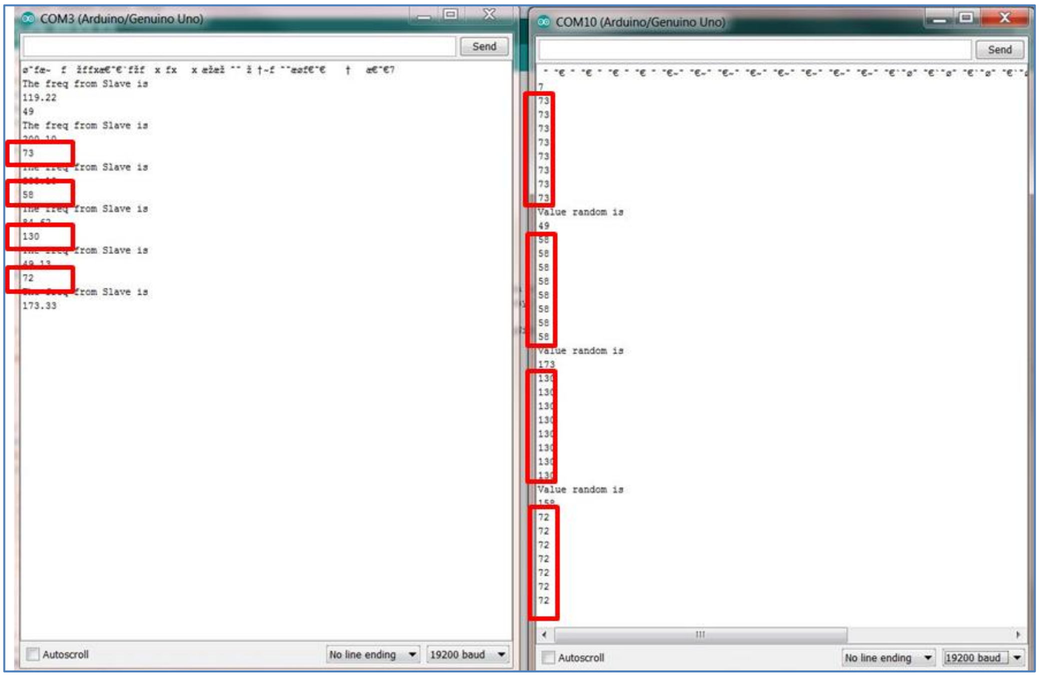
```
New Value
The freq from Slave is
203.78
ÃÜCówJØÜ¿˝  İJÃ[ ¼¨¾‡óØÜ¿˝  Ė ÃŠè¼¨¾‡óØÜ¿˝  Ė ÃŒè¼¨¾‡óØÜ¿˝  Ž˝ø-ÃÜCówJØÜ¿˝  Œøšè¼¨¾‡óØ
```

No line ending, 9600 baud

```
0
0
0
0
0
7
7
7
7
7
7
7
7
49
49
49
49
49
49
49
49
ŸýCÖı˝  İŠøŠøŠøŠøŠøŠøŠøŸýCÖı˝  ÃŒøŒøŒøŒøŒøŒøŒøŒøŸý!Öı˝ ÜŠø-Ã-Ã-Ã-Ã-Ã-Ã-Ã-ÃŸýCÖı˝  Œøš
```

No line ending, 9600 baud

41**Figure C- 5: New encrypted keycode value**

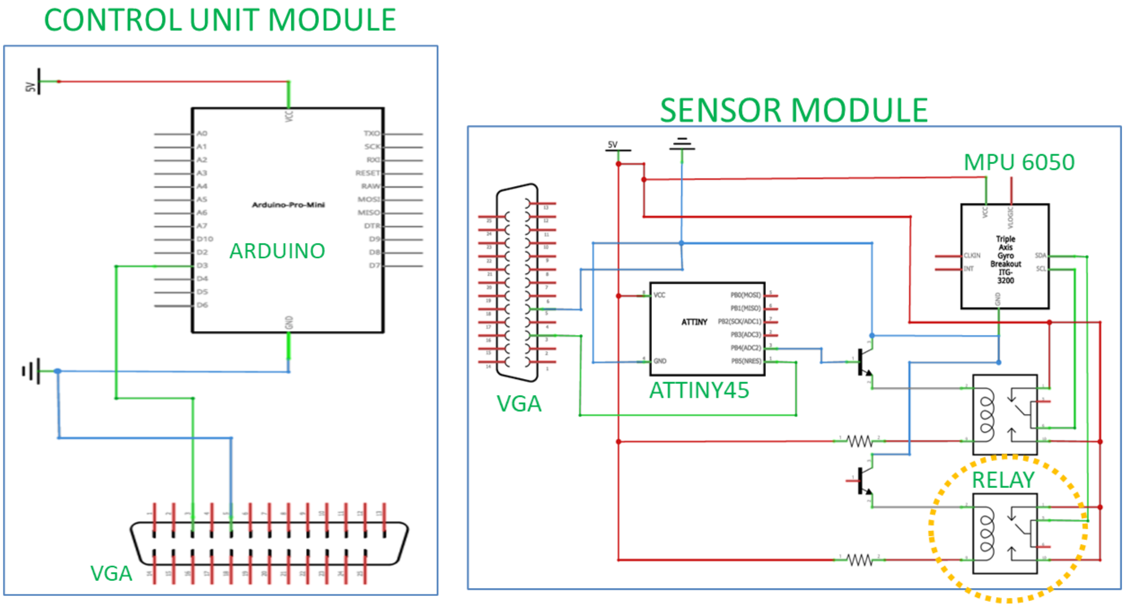


```
ø˜fæ-  f  žffxæ€˜€˙fžf  x fx   x æžæž ˜˜ ž †~f ˜˜æøf€˜€    †   æ€˜€7
The freq from Slave is
119.22
49
The freq from Slave is
200.10
73
The freq from Slave is
200.10
58
The freq from Slave is
84.62
130
The freq from Slave is
49.13
72
The freq from Slave is
173.33
```

```
˜ ˜€ ˜ ˜€ ˜ ˜€ ˜ ˜€ ˜ ˜€~˜ ˜€~˜ ˜€~˜ ˜€~˜ ˜€~˜ ˜€~˜ ˜€~˜ ˜€~˜ ˜€˙˜ø˜ ˜€˙˜ø˜ ˜€˙˜ø˜ ˜€˙˜
7
73
73
73
73
73
73
73
73
Value random is
49
58
58
58
58
58
58
58
58
Value random is
173
130
130
130
130
130
130
130
130
Value random is
158
72
72
72
72
72
72
72
```

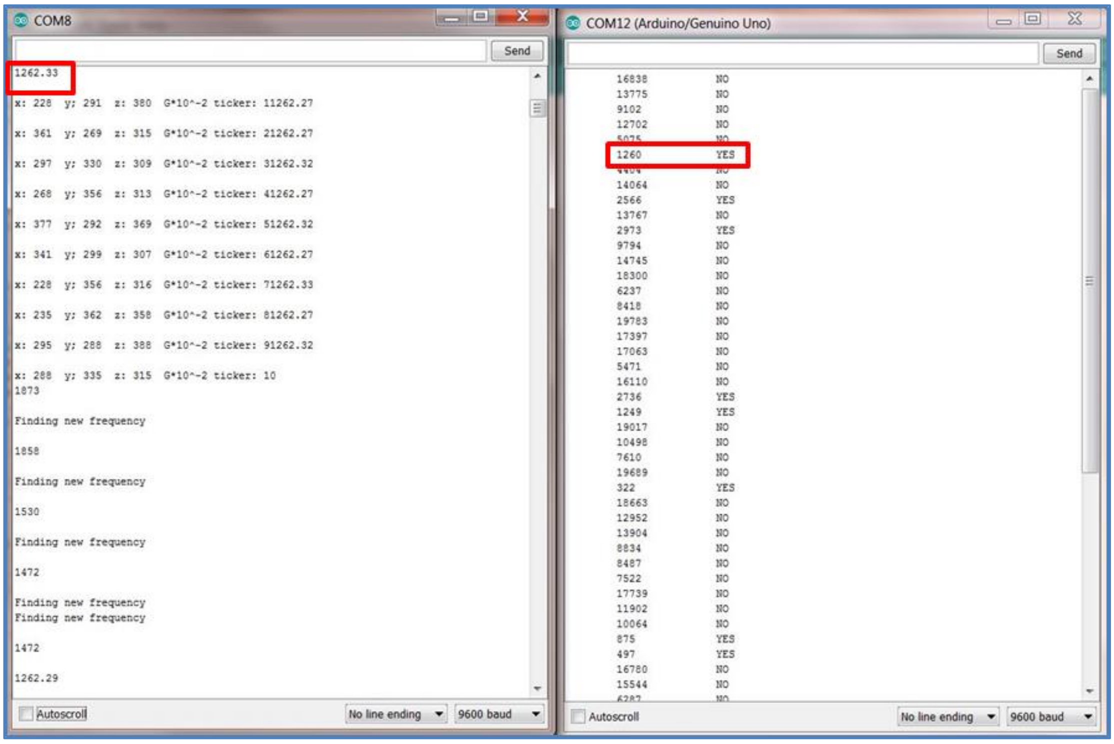
42**Figure C- 6: The new baud rate agreement**

In addition, the control unit module also generates a new encrypted keycode value as the new access value for the new sensor module baud rate (Figure C-5). Therefore, when the sensor module receives the new keycode it will generate a new frequency value for the control unit. If the control unit recognises the new frequency value from its own record value database a new baud rate will be set. The new baud rate generates a frequency value used for the next transmission rate agreement session. All these combinations occur in a few milliseconds and are continuous. (Figure C-6).



43**Figure C- 7: Secure connection – components involved**

Figure C-7 shows the required components for the connection step of the LCCA authentication protocol.



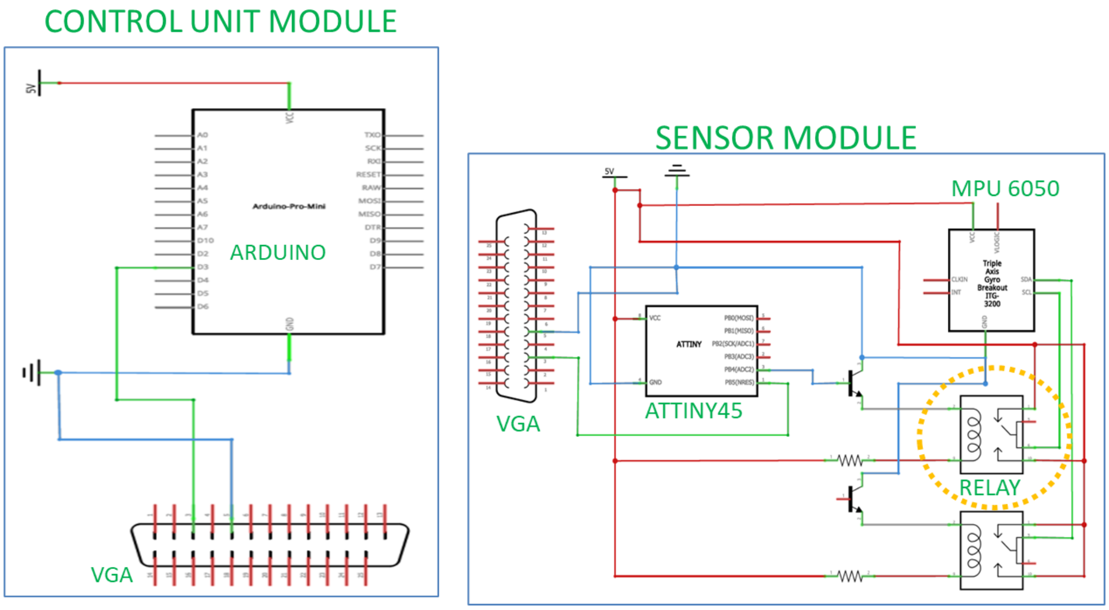
```
1262.33

x: 228  y: 291  z: 380  G*10^-2 ticker: 11262.27

x: 361  y: 269  z: 315  G*10^-2 ticker: 21262.27

x: 297  y: 330  z: 309  G*10^-2 ticker: 31262.32

x: 268  y: 356  z: 313  G*10^-2 ticker: 41262.27

x: 377  y: 292  z: 369  G*10^-2 ticker: 51262.32

x: 341  y: 299  z: 307  G*10^-2 ticker: 61262.27

x: 228  y: 356  z: 316  G*10^-2 ticker: 71262.33

x: 235  y: 362  z: 358  G*10^-2 ticker: 81262.27

x: 295  y: 288  z: 388  G*10^-2 ticker: 91262.32

x: 288  y: 335  z: 315  G*10^-2 ticker: 10
1873

Finding new frequency

1858

Finding new frequency

1530

Finding new frequency

1472

Finding new frequency
Finding new frequency

1472

1262.29
```

```
16838        NO
13775        NO
9102         NO
12702        NO
5075         NO
1260         YES
4404         NO
14064        NO
2566         YES
13767        NO
2973         YES
9794         NO
14745        NO
18300        NO
6237         NO
8418         NO
19783        NO
17397        NO
17063        NO
5471         NO
16110        NO
2736         YES
1249         YES
19017        NO
10498        NO
7610         NO
19689        NO
322          YES
18663        NO
12952        NO
13904        NO
8834         NO
8487         NO
7522         NO
17739        NO
11902        NO
10064        NO
875          YES
497          YES
16780        NO
15544        NO
6287         NO
```

44**Figure C- 8: Frequency value agreement**

During this phase the control unit module generates a new frequency value for the sensor module as key agreement for starting the connection. Physically, the bottom relay in figure C-7 is the switch to access to the sensor data.

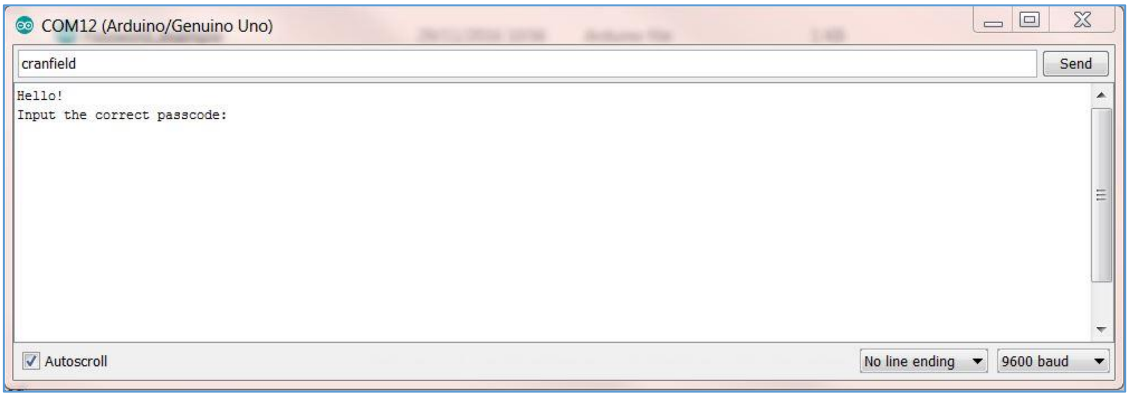
In detail, the control unit module generates a random frequency value in a specific range. The sensor module recognises the frequency value and authorises the control unit module to access the sensor data via relay. This collection is limited to 10 seconds, after which the sensor module will wait for receive a new frequency value as shown in Figure C-8.



45**Figure C- 9: Authentication -components involved**

Finally, the last phase of the LCCA protocol consists of the authentication. Figure C-9 shows the required components for the authentication phase. Authorised users may get access to the sensor data via an alphanumeric password.

If the control unit module recognises the user password, it will send a specific frequency value to the sensor module to switch-on the above relay (Figure C-9).



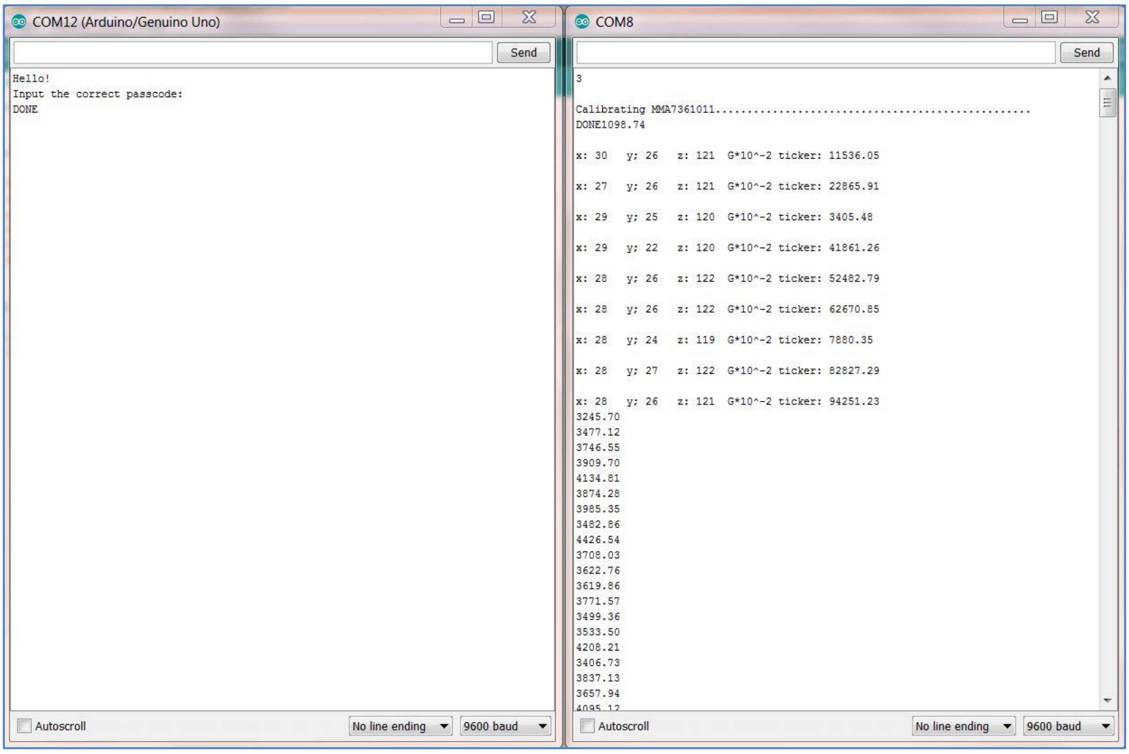
cranfield

```
Hello!
Input the correct passcode:
```

☑ Autoscroll   No line ending   9600 baud

46**Figure C- 10: User passcode**

Figure C-10 shows the control unit module which requires the user passcode to access the sensor data.



```
Hello!
Input the correct passcode:
DONE
```

□ Autoscroll   No line ending   9600 baud

```
3

Calibrating MMA7361011...............................................
DONE1098.74

x: 30   y; 26   z: 121  G*10^-2 ticker: 11536.05

x: 27   y; 26   z: 121  G*10^-2 ticker: 22865.91

x: 29   y; 25   z: 120  G*10^-2 ticker: 3405.48

x: 29   y; 22   z: 120  G*10^-2 ticker: 41861.26

x: 28   y; 26   z: 122  G*10^-2 ticker: 52482.79

x: 28   y; 26   z: 122  G*10^-2 ticker: 62670.85

x: 28   y; 24   z: 119  G*10^-2 ticker: 7880.35

x: 28   y; 27   z: 122  G*10^-2 ticker: 82827.29

x: 28   y; 26   z: 121  G*10^-2 ticker: 94251.23
3245.70
3477.12
3746.55
3909.70
4134.81
3874.28
3985.35
3482.86
4426.54
3708.03
3622.76
3619.86
3771.57
3499.36
3533.50
4208.21
3406.73
3837.13
3657.94
4095.12
```

□ Autoscroll   No line ending   9600 baud

47**Figure C- 11: Authentication**

Figure C-11 shows that the control unit module recognises the passcode and invites the sensor module to authorise the user access to the sensor data. Finally, the sensor module activates the sensor and starts to collect data.

This section shows the main tasks of the authentication protocol and highlights the contribution to the security that this protocol can give to the device proposed.

All authentication protocol phases are managed in the control unit module CPU. By doing this, all architecture becomes flexible and all other modules can be easily replaced.