CYBERSECURITY AUTOMATION FOR AN INDUSTRY 4.0 GARMENT MANUFACTURING SYSTEM

Project Id: 2021-011

Final Project Thesis

P.A.U.T. De Alwis

B.Sc. (Hons) Degree in Information Technology Specialization in Cyber Security

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

October 2021

CYBERSECURITY AUTOMATION FOR AN INDUSTRY 4.0 GARMENT MANUFACTURING SYSTEM

Project Id: 2021-011

Final Project Thesis

B.Sc. (Hons) Degree in Information Technology Specialization in Cyber Security

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

October 2021

DECLARATION

"I declare that this is our own work and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to Sri Lanka Institute of Information Technology, the nonexclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books)."

Name	Student ID	Signature
P.A.U.T. De Alwis	IT18136098	

The above candidates are carrying out research for the undergraduate Dissertation under my supervision.

Signature of the supervisor : Prof. Pradeep Abeygunawardhana

Date:

Signature of the co-supervisor : Ms. Wellalage Sasini Nuwanthika

Date:

ABSTRACT

Digital transformation of Industry 4.0 towards Internet of Things (IoT) focuses on productivity rather than security, therefore often face cyber security challenges. To overcome such, a centralized security solution focusing on four major areas 1) standardization, 2) security configurations with update management, 3) authentication and physical access control and 4) intrusion detection was applied to a Cyber Physical System (CPS) based garment manufacturing system to overcome the security gap. Security policies based on ISO 27001:2013 and IEC 62443 security standards were applied to the security configuration management system in the design stage to achieve 'security by design' concept. Security and audit configurations as well as security update management were applied using Ansible for the automated tool that can be customized based on requirements. The proposed system enhances security, reaching for a cost-effective, efficient, reusable solution, and provides a comprehensive security solution for potential challenges of current and future smart manufacturing. The system is secured in terms of strategy, design, and operations rather than securing the system after deployment, especially through the compliance with standardization and policy implementation.

Keywords—Industry 4.0, Internet of Things (IoT), standardization, cyber security, Cyber Physical System (CPS)

ACKNOWLEDGEMENT

I wish to acknowledge the help provided by Dr. Asela Kulatunga, Head of Department of Manufacturing and Industrial Engineering in University of Peradeniya for giving us the opportunity to visit Peradeniya University to study CNC machine and robotic applications workflow which was a good initialization point for our research project. I wish to show my gratitude to Mr. Wijeweera, owner of Wijeweera Knit Wear (Private) Limited for letting us visit the garment factory to analyze requirements for our project in the initialization stage.

I wish to show my appreciation for our external Supervisor Chartered Eng. P.A. Gamini De Alwis for guiding us in the correct direction, throughout our research project by providing experience the manufacturing field, Dr. Darshi De Saram for sharing knowledge and experience and providing comments to make our project a success. I wish to acknowledge Ms. Archana Nair for the verification of policies.

I wish to thank my Supervisor Professor Pradeep Abeygunawardana and Co-supervisor Ms. Sasini Wellalage for supervising us throughout an entire year for our final year research. I would like to acknowledge the Faculty of Computing academic staff, specially the Department of Computer Systems Engineering for support given to make this project a success. Last but not least, I would like to thank research module coordinators of Sri Lanka Institute of Information Technology for all the knowledge taught and giving opportunities for a research to make us learn and grow.

TABLE OF CONTENTS

Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Description
CIA	Confidentiality, Integrity and Availability
CNC	Computer Numerical Control
CoAP	Constrained Application Protocol
CPPS	Cyber Physical Product Systems
CPS	Cyber Physical Systems
DCS	Distributed Control Sensors
DNP3	Distributed Network Protocol
DoS	Denial of Service
EN	European Standards
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
HMI	Human Machine Interface
IACS	Industrial Automation and Control Systems
ICT	Information and Communication Technology
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
ISA	International Society of Automation
ISO	International Organization for Standardization
ISCN	Information Security Continuous Monitoring
ISMS	Information Security Management System
ISVS	IoT Security Verification Standard
JTC	Joint Technical Committee
LAN	Local Area Network
M2M	Machine to Machine
MitM	Man in the Middle
MTCS	Multi-Tier Cloud Security

NC	Numerical Controller
NIST	National Institute of Information Technology
OCTAVE	Operationally Criticalthreat Asset and Vulnerability Evaluation
OWASP	Open Web Application Security Project
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SAM	Standard Allowed Minutes
SCADA	Supervisory Control and Data Acquisition
SDLC	Secure Development Life Cycle
SHODAN	Sentient Hyper-Optimized Data Access Network
SMV	Standard Allowed Value
SN	Sensor Network
SOA	Statement of Applicability
SP	Special Publication
SU	Sub Committee
TCP	Transmission Control Protocol
TR	Technical Requirements
TS	Technical Specifications
WG	Working Group

1. INTRODUCTION

The modernization brought on by Industry 4.0 began to saturate the manufacturing sector with heterogeneous technologies and a large percentage of physical actuation components making the automation process more complex. .Industrial Internet of Things (IIoT) combines smart computing and network technologies in automation and data transmission to create more extensive, better connected, and productive systems, in line with the ongoing trend of manufacturing and industrial practices, including Cyber Physical Systems (CPS) and Internet of Things (IoT). The Internet of Things (IoT), as well as data analytics and machine learning, are used in smart manufacturing to provide a link between the digital and physical worlds. Despite the fact that these technologies have been in development for some time, integrating them with industrial systems presents new problems as well as possible benefits like enhanced efficiency.

Standardization is a solution for the various problems encountered when implementing a complex IoT system. Also, standardization and frameworks provide a guide for the protection of the system. Until recently, the primary goal of digital transformation has been to integrate network and smart devices into current production environments in order to boost productivity, and direct human labor and resources are reduced. Capabilities in CPS require sophisticated algorithms and infrastructure, which frequently result in new security vulnerabilities and operational risks. As cyber-attacks are no longer a question of "if," but rather "when" in today's hyper-connected world, manufacturers and their supply networks will remain unprepared in the face of threats unless they take targeted, decisive, and energetic actions to improve security. As a result, as a pro-active measure implementation of effective policies according to globally recognized standards and frameworks is one of Industry 4.0's main enablers. Not only the current literature in the field but also, the results of the research shows that standardization and frameworks save time and costs as they guide towards risk reduction managing risks through best practices. The importance is that standardization can help implement long term security procedures, can be used as a bench mark for compliance with cyber security laws and protocols, can allow the market to attain its full potential by opening up new opportunities in new areas.

The integration of sophisticated smart manufacturing technologies dramatically widens the scope of industrial espionage and sabotage attempts, because industrial 4.0 manufacturing systems are driven by a focus on functionality rather than security,. As a result of poor security design and unmet cyber security standards, the volume and sophistication of cyber-attacks in

industrial automation systems is increasing. Observation is that standardization in IoT systems design, implementation and maintenance has to be focused because of the following.

- IoT is gaining in importance on a technical, social, and economic level.
- Large amounts of data are generated by intelligent devices. This information must be managed, processed, transferred, and stored securely in accordance with industry standards.
- IoT has brought vast industrial revolution also known as industrial 4.0 or smart manufacturing and has helped automate many processes within organisations using many trending technologies.
- Smart manufacturing is based on the construction of a link between the digital and physical worlds via IoT, in conjunction with enhancements such as data analytics, machine learning, Cyber Physical Systems, wireless sensor networks, augmented reality, cloud computing, 3D printing, system integration, and, most crucially, cyber security are all examples of emerging technologies.
- The integration of complicated smart manufacturing technologies vastly expands the scope of attacks aimed at industrial espionage and sabotage, because industrial 4.0 manufacturing systems are driven by a focus on utility rather than security,
- Due to poor security design, methods, and requirements, the volume and sophistication of cyber-attacks in industrial automation systems is increasing.
- The lack of effective regulation, standards, and governance has resulted in a steady decline in the security of IoT networks and devices, and there have been plenty of privacy concerns.

The creation of a secure environment for smart systems that use The CPS platform is a large project that is currently hampered by a number of issues such as collaborating between different systems, centralized security management, secure communication, and insecure data, resulting in design and security model conflicts, additional cost, low product quality, CIA violations, and difficulties adhering to laws and regulations.

Novel changes in Industry 4.0 lead to a passion for manufacturing plants with productivity, customization features, flexibility, operational efficiency [1] and SAM/SMV (Standard Allowed Minute/Standard Minute Value) rather than security. The integration of complex smart manufacturing technologies lead to increased intercommunication and data density, thus

massively expand the scope of attacks pointing at industrial espionage and sabotage [1], because Industrial 4.0 are implemented targeting the functionality than security [2].

CPS are used to gain higher productivity in manufacturing [3], and to usher innovation due to their potential to integrate technology from different sectors for the implementation of real world processes [1][2]. Manufacturing automation is becoming a part of critical infrastructure in the present and future context. CPS is designed and implemented to be easily extendable and scalable as the structure includes heterogeneous communication technologies. The integration of IoT devices combined with various technologies is a complex task and implementing security for those systems is more complex task. As a result, cyber security has become a serious problem. The goal of the research is to develop a cyber-security solution for an Industry 4.0 garment manufacturing system that complies to security standards in order to illustrate the cyber security gap and discuss solutions to apply in the apparel industry while comparing and contrasting current security aspects in current industrial 4.0 automated systems in the industry.

A comprehensive, cost effective and efficient security solution for garment manufacturing systems to overcome the potential challenges of the smart system is proposed with a centralized security approach with four major cyber security aspects such as,

- Standardization
- Centralized security configurations and update management
- Authentication and Physical Access Control
- Intrusion detection

This dissertation focus on the cyber security aspect of the following:

1) Standardization

2) Update management.

The reminder of the paper is followed by a background review, analysis of the current literature on IoT, CPS and Network devices and their challenges, current literature on standardization the field, objectives and sub objectives of the project.

1.1. Background Review

The development of steam power, which was the greatest breakthrough for human productivity, started the first industrial revolution. Fabric was created using inventions such as the spinning

machine and looms. The textile manufacturing began with the invention of the first mechanical sewing machine. The first industrial revolution was powered by coal, water, and steam, whereas the second was accelerated by electricity. The sewing machines began to be produced in a serial manner as a result of the revolution in the apparel industry. Partial automation with Programmable Management Systems ushered the third industrial revolution. Developments in microprocessors, software, fiber optic cables, and telecommunication domains made the digital revolution a success. The German Federal Government first announced the Industrial Revolution 4.0 at the Hannover Fair in 2011. The physical world is created in a virtual environment, and cyber physical systems are linked and communicate with one another in real time to make decisions without human intervention, with the goal of developing new internet services and business models that provide efficiency, transparency, fault detection, flexibility, monitoring, and, most importantly, productivity while lowering costs. The use of IoT in industrial applications and the technological convergence of CPS will feature value generation and commercial methods, as well as modular frameworks that can adapt to changing needs and strategies.

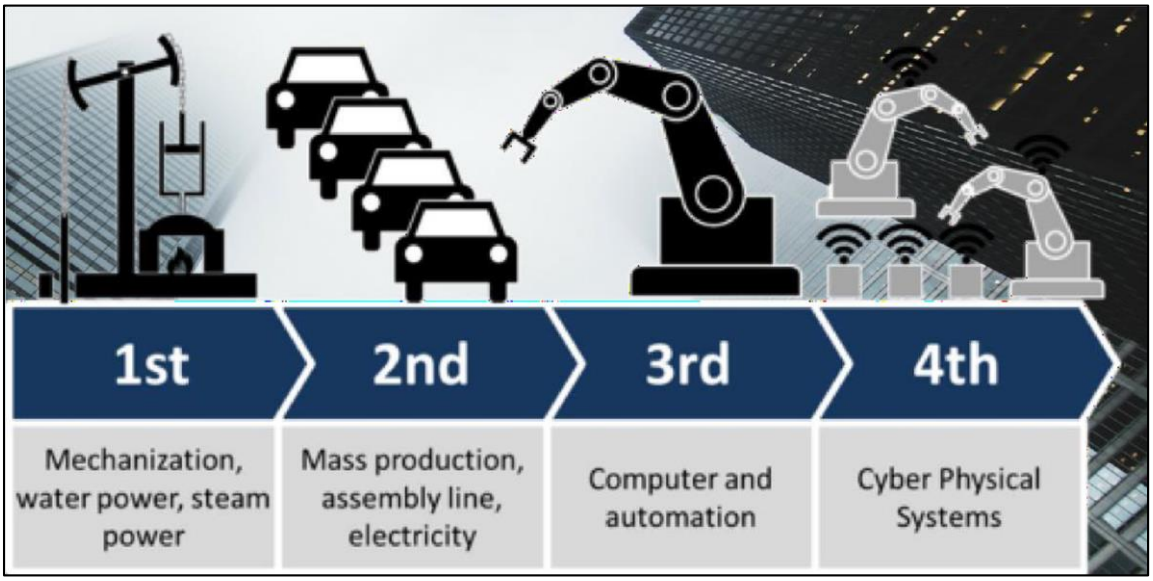


Figure 1.1: Industrial revolution

Industry 4.0 foresee the development of IIoT and the integration of smart computers and networking in manufacturing processes for automation. The Internet of Things (IoT) is a technology that allows computers and computer-related equipment to communicate with one another in order to improve intelligence, profitability, and effectiveness, as well as safety [4]. While IoT refers to a network of interconnected computing devices that communicate with one another and with people in real time, it is most typically utilized in consumer applications, IIoT

is employed in industrial applications such as manufacturing. In contrast to IoT, IIoT has more unique categories that include smart devices, networking approaches, command control, and service requirements.

Since the beginning of the first revolution, the apparel manufacturing industry has grown to be an important part of the global manufacturing industry. The apparel fashion industry has become extremely competitive. As a result, industry-wide integrated technologies are fast evolving, enabling for new manufacturing methods. Industry 4.0 features include scalability, product customization, customer happiness, control, and visibility, all of which are important in the garment industry. Nonetheless, the majority of automation systems are centered on the clothing sector.

In an apparel factory, the basic flow of production processes comprises designing the product according to marketing demands and consumer requirements, selecting suitable clothing material, and assembling the product. Creating layers out of clothing materials, cutting various forms with minimal material waste, various sewing operations, finishing, product quality assurance, packing, storing, and distribution.

Because of the wastage problem, availability and accessibility, labor dependency, and the fact that it is an expensive operation, the cutting process plays a significant part in the garment automation sector. Die cutters, first introduced in the 1900s, improved cutting efficiency and quality. Numerical Controller (NC) machines, introduced in the 1940s, allowed for continuous cutting, allowing for more production flexibility and material utilization [5]. The digital revolution gave birth to CNC (Computer Numerically Controlled) machinery. Cutting has become the most technologically advanced area in the apparel industry as a result of this improvement. There are a variety of cutting technologies available, including computer controlled knives, lasers, plasma, ultrasound, and markers. Since the development of the first fully automated cutting system, existing cutting technologies have improved in terms of productivity, adaptability, and pattern matching capabilities [5]. Cutting processes, such as CNC machines, are part of the industry 4.0 revolution, which is addressing solutions for labor-intensive problems, waste, and cost reduction [5].

In the IIoT, or fourth industrial revolution, the concept of digitalization and integration has been highlighted, and CNC technology plays a critical role in automating cutting garment production systems. The CNC serves as a hub through which vital information flows. CNC controllers in Industry 4.0 should be able to support integration, sensors, and cloud servers.

The transition from traditional hardware-based controllers to smart automation software architecture is a difficulty. Security issues develop as a result of today's industrial 4.0 automation's concentration on functionality rather than security. Lack of security may result in an increase in, a loss of production, or even death. Existing measures' shortcoming poor levels of awareness. Readiness for upcoming confrontations is important that is the reason for security should be important underpinning the development in industry 4.0. If industrial 4.0 manufacturing automation developers could discover cyber security requirements that haven't been fully captured in automation and design systems that address all security aspects in automation, the developing automation systems would be theoretically risk-free and secure. For industrial 4.0 automation production systems, CPS play a critical role in cyber security.

The foundation of industrial 4.0 should enable garment cutting manufacturing automation including CNCs to deliver best possible performance based on security. It must also embrace the most accepted open security standards other than industrial best practices and standards which adhere to security laws and regulations to enhance safety as well as the security while designing the automated manufacturing systems. This also should be flexible enough to adopt to changing requirements and standards as well as strategies in the future of apparel industry.

Manufacturing standards, are a challenge that IoT has to overcome. Manufacturers devote insufficient time and resources to security. Lack of compliance, lack of secure update mechanisms leads to various security threats [6]. They are very industry specific and mostly suggested best practices. IoT Devices lack having guidance for security policy enforcement and policies are not been focused to enforce in the design stage.

In industry 4.0, network and wireless connections necessitate a standard, a widely accepted digital fieldbus. EtherCAT, or Ethernet for Control Automation Technology, is one such standard. It is an Ethernet-based fieldbus system. This is standardized in International Electro technical Commission (IEC) 61158 and can be used for both hard and sift real-time automation requirements. Both PROFINET and Sercor 3 standards could also be used. For Programmable Logic Controller (PLC), PLCCopen IEC 61131 standard is valid. Data sharing systems and standards, innovative education and training, laws and regulations should be considered as enabling factors in the design stage. As previously discussed, Industrial Control Systems employ different insecure communication protocols, including PROFINET, Modbus, Distributed Network Protocol 3 (DNP3), and EtherCAT. Even though DNP3 and Modbus

started out as serial protocols, they have been enhanced to work with Ethernet and Transmission Control Protocol (TCP)/Internet Protocol (IP). They are now widely used to connect devices across field buses and networks. Therefore, systems lack the security mechanisms required to support packet authentication integrity, anti-repudiation, and anti-replay. Poor security policies and practices can frequently introduce vulnerabilities into manufacturing systems [7].

Many companies are also already using collaborative robots (co-robots) to lead and unload part to a CNC system. Even small manufacturing sites and systems can take advantage from co-bots as it reduces integration cost.

Patch management is a continuous process of identifying, prioritizing, and resolving vulnerabilities. Delays in prioritizing and applying patches can result in security vulnerabilities. While patching remains one of the most significant obstacles to more efficient cyber security risk mitigation, using a patch management solution to implement a standard, repeatable procedure greatly decreases the response time associated with vulnerability assessment and patch management procedures reducing exploits and breach risks. Update management, Benefits of patch management include gain insight to risks and vulnerabilities, optimize performance by minimizing the downtime,

Future trends in industrial 4.0 manufacturing systems includes, Simulators and test beds, intrusion detection and attack generation, security policy specification and enforcement and forensics.

1.2. Literature Review

Security has become a secondary concern rather than an important component in industry 4.0 automation systems, posing a significant risk in the rush for flexibility, quality, and efficiency. This problem leads to a variety of security flaws and attacks., mostly network related attacks such as Denial of Service (DoS) attacks, MitM (Man in the Middle) attack, eavesdropping attacks, false data injection attack, replay attack, spoofing attack, side channel attack, covert channel attack, zero day attack, physical attacks, malware as well as machine learning related attacks and data analytics related attacks [7]. The majority of security has been shared with a third party, and manufacturers must rely on the third party's confidence. There could be insider attacks, a loss of data governance, and plenty of other dangers. Existing systems have different vulnerabilities but this issue has been poorly understood. As manufacturing automated systems are evolving rapidly new vulnerabilities would arise if security is not been a primary concern in design. Most literature focus on functionality of industrial 4.0 automated systems and security is considered as a secondary concern or a characteristic.

In bygone days, manufacturing security was performed by tactics like Isolation based on physical access control. Nowadays, since remote working capability which arose due to Covid–19 pandemic Ethernet, IP controls are a core part in networking. As a result, there is a significant threat level and an increased number of vulnerabilities. PLC, Remote Terminal Unit (RTU) systems, and Supervisory Control and Data Acquisition (SCADA) servers were all searched using Sentient Hyper-Optimised Data Access Network (SHODAN), a custom IoT search engine. Servers for Human Machine Interface (HMI) and DCS (Distributed Control Sensors) have been targeted [7].

Because automation deals with large amounts of data, the demand for high-speed data has been rapidly increasing in the industrial network. As a result, Ethernet technology provides advantages like increased efficiency, reduced operation, real-time data sharing, and device control. One of the difficulties in designing secure systems in smart manufacturing is a scarcity of skilled security personnel. With the shift to IIoT systems, this will become increasingly important. It's not easy to come up with practical and usable security policies. Policies affect both the performance of the system as well as adaptability. Users may refuse to follow security policies and procedures if they become a burden to them, and they may intentionally abuse the system [7]. Personal awareness is also necessary to highlight the importance of security as a human issue as well as we pay attention for technical issues. If Ethernet allows possibilities of

CIA violation, it is a threat to the system so that new security concept involve security standards.

1.2.1. IoT security frameworks

International Organization for Standardization (ISO)/IEC Joint Technical Committee (JTC) 1/ Sub Committee (SC) 27

1) Working Group WG1 Requirements, security services, and guidelines
    - WG2 Techniques and Mechanisms
    - WG3 security evaluation criteria
2) Standards ISA-Special Publication (SP0 99 Manufacturing and Control Systems Security Founded in 2002 ISA-TR99.00.01-2004(TR1) Published on March 12, 2004, ISA-TR99.00.02-2004(TR2) Published on April, 2004 [8].

Table 1.1: Industrial standards and guidelines comparison

	IEC 62443	**ISO/IEC 27000**	**ISO/IEC 15408**	**VDI/VDE 2182**
Purpose	- Industrial communication networks - Network and system security	- Information Technology - ISMS	- Evaluation criteria for IT security	- Risk-based selection of controls and countermeasures
Structure of Documentation	- 1 Standard - 4 Categories - 12 Parts	-1 Standard Family - 5 Categories - 16 Standards	- 1 Standard - 3 Parts	- 1 General Model - 6 Application Examples - 1 Set of Recommendations
Procedure	- Domain-tailored concepts	- 4 cyclic steps	- One-time approach	- 8 cyclic steps
Viewpoint	- Policies & procedures - (Technical) systems & components	- Management & organisation - Processes	- TOE	- Risks & threats - Countermeasures
Target Audience	- System Integrator (SI) - Product Supplier (PS) - Asset Owner (AO)	- Organizations of all types and sizes using IT	- Developers - Evaluators - Consumers	- Vendors - Machine Manufacturers - Plant Managers
Protection	- Defense in depth - Segmentation (zones & conduits) - Risk assessment (VDI/VDE 2182) - ISMS (ISO/IEC 27000)	- Security controls - Audit - Certification	- Protection profiles - Security components - Assurance components - Audit	- Asset identification - Risk assessment - Countermeasure use - Process audit
Metrics	- 4 Security Levels (SLs) - 7 Foundational Requirements (FRs) - 2-13 System Requirements (SRs) - 4 Maturity Levels (MLs) - 4 Protection Levels (PLs)	- Nothing relevant specified	- 7 Evaluation Assurance Levels (EAL)	- $\geq$3 classification levels (e.g. low, medium & high) - Probability & occurrence - Damage & impact

Table 1.2: Best practices for industrial Information security

Best Practice	General Description and Purpose
NIST Cybersecurity Framework [12]	Framework for Improving Critical Infrastructure Cybersecurity
BSI ICS Security Compendium [13]	General Recommendations for Industrial Control System Security
IIC Security Framework [14]	Industrial Internet of Things Security Framework
IEEE 1686 Standard [15]	IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities
IEEE Security Recommendations [16]	Practice for Privacy Considerations for IEEE 802 Technologies
NIST SP 800-30 [17]	Guide for Conducting Risk Assessments
NIST SP 800-53 [18]	Security and Privacy Controls for Information Systems and Organizations
NIST SP 800-82 [19]	Guide to Industrial Control Systems (ICS) Security
DHS Catalog [20]	Recommendations for Standards Developers of Control System Security
IEC 61508 Standard [21]	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
NERC CIPs [22]	Securing assets within the Critical Infrastructure Protection (CIP)
NIST IR 7628 [23]	Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements
ISACA COBIT [24]	Control Objectives for Information and Related Technology
CIS CSC [25]	Critical Security Controls as the basis for security audits

As illustrated in [9, Tab. 1.1] and [9, Tab. 1.2] there are several standards, guidelines and best practices in use for industrial information security.

The absence of effective regulation, standards and weak governance has led to a continual downward trend in the security of IoT networks and devices, as well as given rise to a broad range of issues including privacy. Especially, privacy challenges lead to providing legal frameworks, although there are significant efforts such as General Data Protection Regulation (GDPR), unexpected data breaches continue to plague the industry. Although technologies have been in development for years, their integration with industrial systems leads to new challenges as well as potential benefits such as productivity. Security in design concept is important and IoT frameworks and standards take a massive importance when it comes to the security in design concept.

Various information security frameworks exist to cover IoT concepts and deployments in various verticals, classified according to the area of concern [10]. Therefore, when securing IoT systems there should be a clear strategy. Research is being done to identify current security frameworks, but there are relatively few initiatives that have been developed to be used in CPS.

When referring to literature reviews of IoT security frameworks and standards, *IoT security Framework*, *IoT security* and *IoT Information security governance* are keywords. Systematic reviews are done according to sources such as application and system layer protection, secure booting & secure firmware updates, business layer, secure communication, data at rest protection, embedded firewall & intrusion detection security, key and certificate management, Authentication & Authorization controls, integration with security management systems which includes security policy management, reporting incidents, security compliance of frameworks for security policies and standards such as IT Security Policies, network security policies, access control policies, Information and Communication Technology (ICT) Security

Standards, and Multi-tier Cloud security (MTCS). In an occurrence of security non-compliance, the security framework, must address security risk assessment and controls to mitigate the risk while abiding with standards and needs [11].

Cisco's proposed security implications for IoT/Machine to Machine (M2M) constructions are extensive, necessitating the deconstruction of a workable IoT/M2M security framework that may be used to execute security in IoT contexts. ISA (International Society of Automation)/IEC 62443 cyber security standards for Industrial Automation and Control Systems (IACS) compliance can be obtained by Floodgate Security Framework. Constrained Application Protocol (CoAP) Frameworks to handle security and trust issues of IoT environments, OSCAR security framework, explores a novel approach to the problem of End to End (E2E) security in IoT [11]. There is literature on aiming to minimize development and testing time in industrial environment using a framework for rapid integration.

1.3. Research Gap

1.3.1. Standardization

Industrial 4.0 transaction from hardware based controllers architecture to a secure smart automation software architecture is a challenge. When, implementing security, there are decentralized and layered approaches as solutions for the implementation and maintenance of smart manufacturing systems. Our approach is a centralized management system including major cyber security aspects; security configurations, intrusion detection and authentication and access control. The standardization for the centralized smart system will be focusing on the major cyber security aspects mentioned above. Based on the major aspects a step by step standardization approach for policy management is implemented and integrated for each aspect for the centralized system.

There are several IoT security frameworks in various stages of development. (European Telecommunications Standards Institute (ETSI) European Standards (EN) 303 645, IoT Security Compliance Framework, Open Web Application Security Project (OWASP) IoT Security Verification Standard (ISVS), European Network and Information Security Agency (ENISA), National Institute of Standards and Technology (NIST))[12][13]. IEC 62443 standard is arising as the popular IoT framework, a series of standards including technical reports to secure IACS. It provides a systematic and practical approach to cyber security for industrial systems. Comparison of the security standards and best practices for the different

industrial automation domains are available [14]. The challenge was to compare, contrast and choose the effective IoT security standards and frameworks suitable to the system.

The research focus on designing an automated system focusing centralized cyber security approach to the manufacturing system for configuration and update management, intrusion detection and access control aligned with standardization. The security threats and drawbacks of the manufacturing system are evaluated according to risk assessments. A solution to eliminate risks and threats after evaluating the problems encountered while implementing security to the system was encouraged. Through past literature, analyzing what approaches were taken to overcome those security problems are encountered. It was observed that the layered and decentralized security approaches were common among the literature, but those approaches affected for the decreased efficiency of the overall smart system. Therefore to increase the efficiency a comprehensive centralized security solution was implemented and tested for industrial automated systems. Clearly the found security gap which affected to the system's efficiency of the industrial automated garment manufacturing system was closed by choosing the effective security standards and creating policies for implementation and integration of major cyber security aspects to overcome the current security challenges. Standard verification and policy creation verification for the manufacturing system were evaluated by an industry expert to ensure that the standardization solution were effective enough to close the gap.

1.3.2 Update management

Security patching process and updates are not easy to manage. Lack of security awareness is one of the main reasons for neglecting security update management. Updates could break systems that works fine, applying updates disturbs the business process and there could be fear for functionality changes. Therefore, the update management system is aligned with the security configuration management system through Ansible while giving a centralized update management approach.

Rather than downloading and installing apps from a server repository on all client systems every time, it is effective to save all applications on a Local Area Network (LAN) server and distribute them to client systems as needed. Using a local repository is a very quick and efficient method because all essential apps are transferred from the local server via a fast LAN connection. As a result, it saves Internet bandwidth and, as a result, lowers the annual Internet cost.

1.4. Research Problem

Smart manufacturing integrate many technologies. Most developers do not fully recognize the cyber security challenges in designing, implementing or maintaining an industrial 4.0 automated system as there are many inter connected devices and technologies. Also vendors and manufactures are focused on productivity rather than security. The research was to identify the application of cyber security requirements which are not been thoroughly captured in automation of garment manufacturing and give a comprehensive security solution to overcome security challenges through a centralized management system with effective strategies for standardization.

Challenges:

For the creation of a safe network environment a Cyber Physical Production System (CPPS) platform based on CPS technology is being used to improve the network environment in Industry 4.0. Building the CPPS platform is a difficult task that is currently hampered by a number of factors, including the need to adhere to CPS challenges.

1.4.1. Collaboration between different systems

Physical devices and computer systems working together for a collaborative model is essential for exchanging information, [15] store information, documentation, decision making, corrective and preventive action.

1.4.2. Centralized security management

Creating CPS models to apply security configurations and updates to physical devices and monitor physical devices using a centralized control system such as SCADA to maximize efficiency is a challenge [16]. In addition to the CPS modeling language, physical devices, software, and hardware platforms, as well as other functional and non-functional factors, must be included in a typical CPS model [15].

1.4.4. Secure communication

CPS that use the SCADA systems is connected to the internet over TCP/IP protocols without additional protection [17], which have known vulnerabilities.

1.4.5. Insecure data

During the implementation of Industry 4.0, there would be a lack of system integrations to ensure data security for manufacturing firms. IoT-based CPSs, which are connected to a large

number of embedded sensors and communication devices, pose a major risk due to the increase in data usage and the increased risk of system breaches. [18].

1.4.6. Initial Cost

Migration to industry 4.0 is not an instantaneous process, in a manufacturing company will result in end-to-end integration to design and incorporate architecture in accordance with business requirements In terms of cost and time, a significant initial investment is required. [19]

1.4.7. Industry 4.0 plans and strategies are lacking.

In the manufacturing industry, there is a lack of a dynamic strategic plan to support the transition to Industry 4.0 [20].

Main focus for the standardization aspect arise the questions such as how to identify and create security policies, how to integrate security strategies suitable for IoT and CPS devices, are there IoT security standards which can be implemented to the implementation, integration and maintenance of the smart system, which standards are suitable for the policy creation, how to choose effective security standards according to the project requirements and how to implement proper security update mechanisms. Developing industrial security policies, considering industrial guidelines, procedures and standards which adhere to laws and regulations is essential when automating the system towards industrial 4.0 automated garment manufacturing system. In order to implement the automated system securely, chosen security standards should be verified and the security policies should be according to the best practices aligned with the effective standards.

How to manage updates using Ansible to automate device management with the help of an Ansible controller in order to centralize device security and configuration management are other focused areas to overcome the security gap through the research. Patch management should be a priority of a healthy security approach to maintain the quality and to mitigate threats to the automated system.

1.5. Research Objectives

1.5.1. Main objectives

Main objective of the overall research project is security implementation for the potential challenges of the smart garment manufacturing system. An automated garment manufacturing

system which has been securely implemented to overcome the potential security challenges in the garment manufacturing industry according to the security standards, which is also verified for authentication and access control for the utilized IoT devices, automated centralized security configurations using Ansible, security updates using Ansible and intrusion detection system.

Identifying the components and devices and conducting risk assessment to identify current and future threats and security policy creation for different components using security and industrial standards to secure the industry 4.0 garment manufacturing system is the main objective of standardization component.

Update Management will be used for the update management configurations giving a solution for increased use of internet bandwidth while downloading and updating software for each devices. Objective is to come up with a solution to lower the use of internet bandwidth while updating deices reducing the cost.

1.5.2. Sub objectives

Create and develop security policies for the major cyber security aspects in the project including, centralized security configuration management, intrusion detection and access control such as privacy policy, password policy, network policy, audit policy, authorization and access control, backup policy according to industrial guidelines and standards which are verified by an industrial expert to design, implement and maintain the secured automated system safely. Come up with procedures and methods to implement the identified security policies if needed. Verify the security policies before implementing for the accountability of the research. Evaluate and give solutions for the problems encountered when implementing security policies.

2. METHODOLOGY

2.1. System Diagram

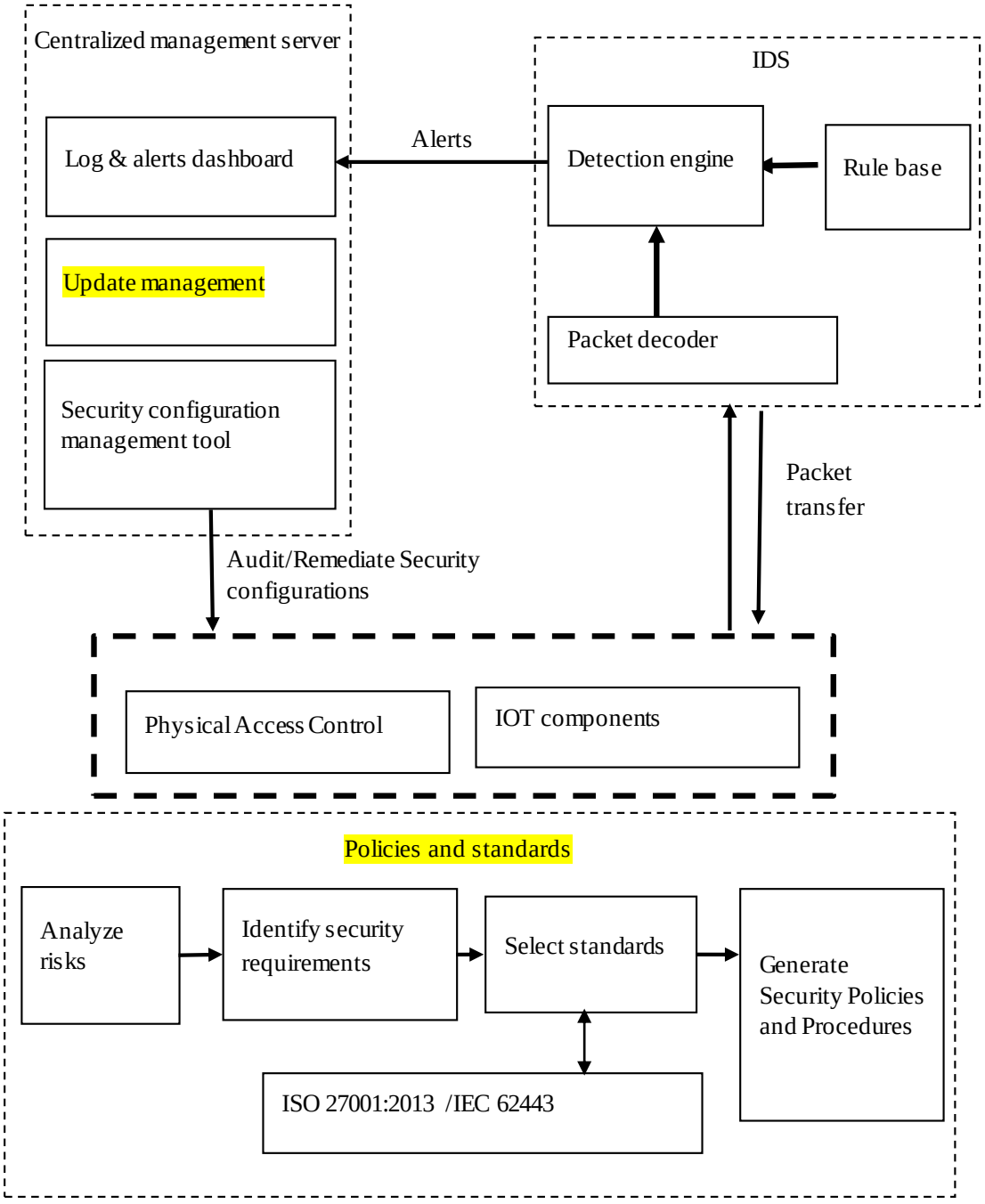


Figure 2.1: Overall System Diagram

As highlighted in the above overall system diagram, update management is done using Ansible playbook templates, the update management system server is connected to Ansible controller which is associated with the device inventory.

Security standards are focused on the overall system based on authentication and access control, security configurations, and network security.

2.2. Methodology of Individual Components

2.2.1. Security standards and policy development

Compare and contrast security standards and choose suitable standards to create and develop security policies such as privacy policy, password policy, network policy, audit policy, authorization and access control, backup policy according to the guidelines on standards to design, integrate and implement the centralized secured automated system securely. Come up with procedures and methods to implement the identified security policies if needed.

Below shows the work break down structure for security standards and policy development.

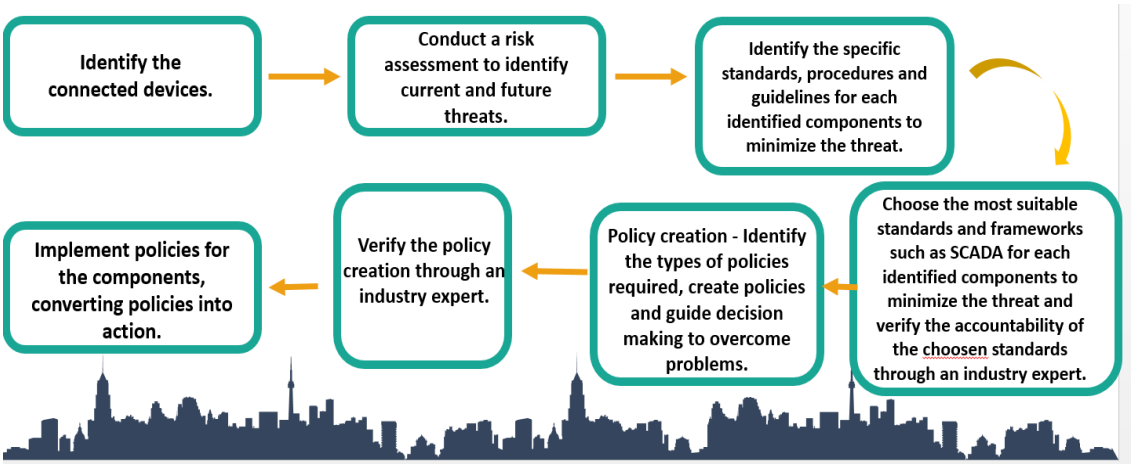


Figure 2.2: Individual Workflow Diagram- Security standards and policy development

2.2.1.1 Identify the connected devices

After going through the current literature regarding the topic, it was essential to have a better understanding about the current local apparel industry and CNC machines.

Therefore, a field visit to a local knit wear garment manufacturing factory was arranged to get a better idea about the apparel industry and local garment manufacturing machines. The processes were manual but, the workflow of the garment factory was observed. Each machinery for production processes was observed. A better idea about the cutting process and its machinery was taken by the factory visit. The requirements and customer-partner relationships were noted down to document the requirements, limitations, costs and benefits of the research.

Figure 2.3: Visit to observe CNC devices - Robotic device

Figure 2.4: Observation of CNC devices 1

Figure 2.5: Observation of software related to CNC machines

Figure 2.6: Observation of CNC device 2

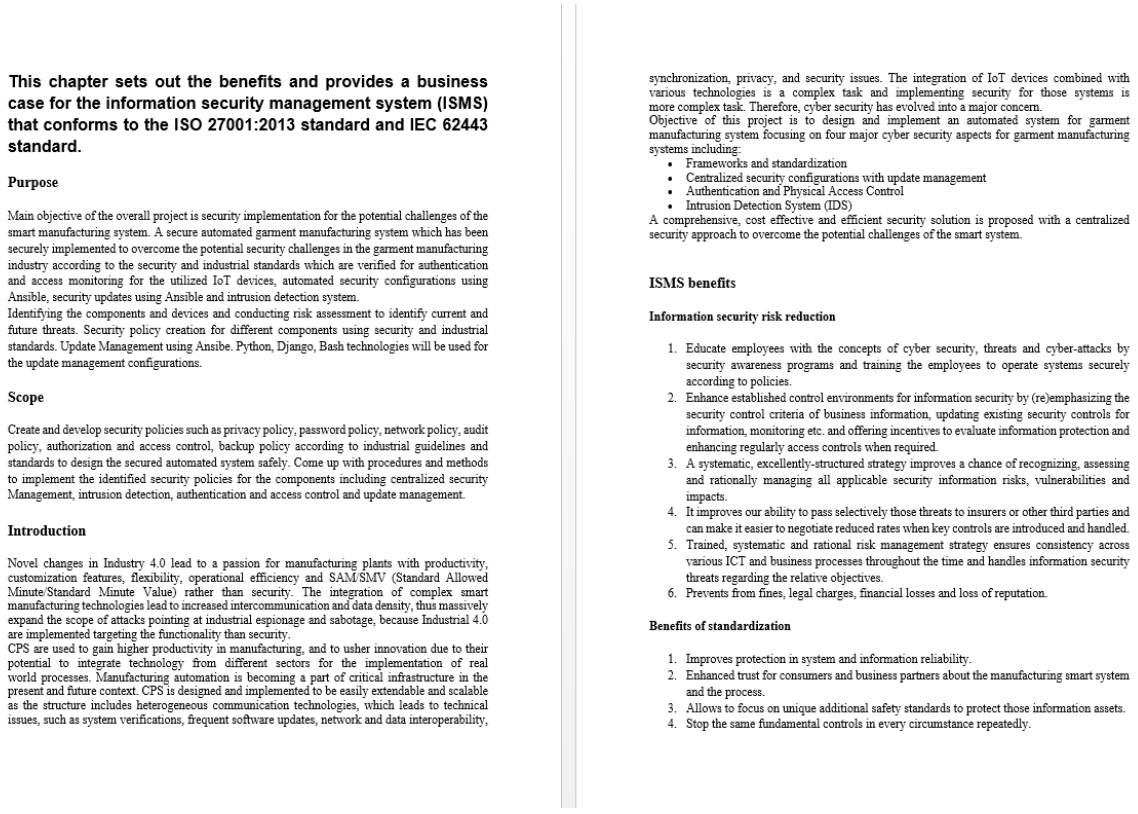
As shown in the above figures, a field visit to the Peradeniya Engineering Faculty, Sri Lanka was arranged to get a better idea about how the CNC machines work and how to collaborate IoT and cyber security for the available local CNC systems. The industrial visit gave us a thorough observation of the following:

- CNC machine workflow
- The current security aspect of the CNC machines
- What components we should specially focus
- How to secure access terminals

- What are the related software and hosted operating systems
- Engineering point of view for the security of CNC machines
- Gaps between IT and engineering applications of CNC machines
- How the machines are operated

Most importantly we got a good initialization point for our research project to have an accurate direction to the research as a detailed idea about the fundamental concept of the topic for the research was taken by the visit. The more we progress in-depth of the research, the more we understand the importance of the visit to Peradeniya Engineering faculty thanks to the support as well as the detailed explanation given by your academic staff members.

A business case was documented by analyzing business requirements, understanding future customer-partner requirements, defining the scope and the purpose of the project while analyzing ISMS benefits and costs.



This chapter sets out the benefits and provides a business case for the information security management system (ISMS) that conforms to the ISO 27001:2013 standard and IEC 62443 standard.

Purpose

Main objective of the overall project is security implementation for the potential challenges of the smart manufacturing system. A secure automated garment manufacturing system which has been securely implemented to overcome the potential security challenges in the garment manufacturing industry according to the security and industrial standards which are verified for authentication and access monitoring for the utilized IoT devices, automated security configurations using Ansible, security updates using Ansible and intrusion detection system.
Identifying the components and devices and conducting risk assessment to identify current and future threats. Security policy creation for different components using security and industrial standards. Update Management using Ansibe. Python, Django, Bash technologies will be used for the update management configurations.

Scope

Create and develop security policies such as privacy policy, password policy, network policy, audit policy, authorization and access control, backup policy according to industrial guidelines and standards to design the secured automated system safely. Come up with procedures and methods to implement the identified security policies for the components including centralized security Management, intrusion detection, authentication and access control and update management.

Introduction

Novel changes in Industry 4.0 lead to a passion for manufacturing plants with productivity, customization features, flexibility, operational efficiency and SAM/SMV (Standard Allowed Minute/Standard Minute Value) rather than security. The integration of complex smart manufacturing technologies lead to increased intercommunication and data density, thus massively expand the scope of attacks pointing at industrial espionage and sabotage, because Industrial 4.0 are implemented targeting the functionality than security.
CPS are used to gain higher productivity in manufacturing, and to usher innovation due to their potential to integrate technology from different sectors for the implementation of real world processes. Manufacturing automation is becoming a part of critical infrastructure in the present and future context. CPS is designed and implemented to be easily extendable and scalable as the structure includes heterogeneous communication technologies, which leads to technical issues, such as system verifications, frequent software updates, network and data interoperability, synchronization, privacy, and security issues. The integration of IoT devices combined with various technologies is a complex task and implementing security for those systems is more complex task. Therefore, cyber security has evolved into a major concern.
Objective of this project is to design and implement an automated system for garment manufacturing system focusing on four major cyber security aspects for garment manufacturing systems including:

- Frameworks and standardization
- Centralized security configurations with update management
- Authentication and Physical Access Control
- Intrusion Detection System (IDS)

A comprehensive, cost effective and efficient security solution is proposed with a centralized security approach to overcome the potential challenges of the smart system.

ISMS benefits

Information security risk reduction

1. Educate employees with the concepts of cyber security, threats and cyber-attacks by security awareness programs and training the employees to operate systems securely according to policies.
2. Enhance established control environments for information security by (re)emphasizing the security control criteria of business information, updating existing security controls for information, monitoring etc. and offering incentives to evaluate information protection and enhancing regularly access controls when required.
3. A systematic, excellently-structured strategy improves a chance of recognizing, assessing and rationally managing all applicable security information risks, vulnerabilities and impacts.
4. It improves our ability to pass selectively those threats to insurers or other third parties and can make it easier to negotiate reduced rates when key controls are introduced and handled.
5. Trained, systematic and rational risk management strategy ensures consistency across various ICT and business processes throughout the time and handles information security threats regarding the relative objectives.
6. Prevents from fines, legal charges, financial losses and loss of reputation.

Benefits of standardization

1. Improves protection in system and information reliability.
2. Enhanced trust for consumers and business partners about the manufacturing smart system and the process.
3. Allows to focus on unique additional safety standards to protect those information assets.
4. Stop the same fundamental controls in every circumstance repeatedly.

Figure 2.7: Screen shot of the first two pages of Business case documentation.

The business case was documented according to ISO 27001:2013 standard. The overall business case states the purpose, scope, Information Security Management Systems (ISMS) benefits, how to reduce information security risks, benefits of standardization for ISO 27001:2013 and IEC 62443, benefits of structured approach, benefits of getting certifications,

benefits of being compliant to the standards, ISMS implementation costs, operation and maintenance costs, training costs (see Appendix 1). Analyzing the business requirements for the system were done and documented.

Discussing aspects of security CIA and how they might apply to the standardization requirements of cyber security in the system and identifying each security aspect were done. Categorization of the aspects according to ISO 27001:2013 were done and controls/reasons for the controls are justified with the overview of implementing each security aspect in Statement of Applicability(SOA) documentation. For each aspect the controls/control objective, whether the current controls are fully applied or applied to some extent is analyzed and highlighted. If the controls are not in place remarks with justification were stated. The selected controls and reasons for selection is marked according to the aspects of business requirements or results of risk assessments. The overview of implementation for each aspect is documented through the Statement of Applicability (SOA).

The SOA documentation is demonstrated in the below screen shots.

P.A.U.T.De Alwis (IT18136098), H.H.DKalhara(IT18139440), A.D.H Jinadasa (IT18132410), R.P.R,D Randunu (IT18133578)

Statement of Applicability Current as of: 07/06/2021

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Annex A controls			Current controls	Remarks (with justification for exclusions)	Selected controls and reasons for selection				Remarks (overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	Sec	Control Objective/Control							
	5.1	Management direction for information security							
Security Policies	5.1.1	Policies for information	TSE				x		As for the manufacturing automation ISMS to be controlled while preserving CIA to protect against cyber-attacks, it was clear that visible information policy for the automation system's entire life cycle has to be developed as best practice to demonstrate the outcome of the well secured system.
	5.1.2	Review of the policies for information security	Y				x		By reviewing current general policies, their weakness can be indentified and strenghtened. The Intrusion detection and prevention, authentication and access control, security configurations and audit components have implemented according to general policies. Reviewing them should be done to develop the policies to preserve CIA.

Figure 2.8: SOA for security policies

	6.1	Internal organisation							
	6.1.1	Information security roles and responsibilities	Y				x		Dividing security roles and destributing responsibilties simplify the workflow. The information security responsibilities are divided according to the components: Authentication and access control, policy development, Intrusion detection, security configurations.
Organisation of information security	6.1.2	Segregation of duties	Y				x		Decrease conflict of interest in roles
	6.1.3	Contact with authorities	Y		x				By consulting authorities for legal advice.
	6.1.4	Contact with special interest groups	Y				x		By maintaining contact with interst groups
	6.1.5	Information security in project management	Y				x		assessing the risks involed.
	6.2	Mobile devices and teleworking							
	6.2.1	Mobile device policy	N	Not applicable for now.				x	
	6.2.2	Teleworking	Y				x		The manufacturing system is IoT based, remote working is essential for the system. Update Management will be done accordng to a centralized Management system using ansible through internet.

Figure 2.9: SOA for organization of information security

Human resource security	7.1	Prior to employment							
	7.1.1	Screening	Y				x		Running background verification checks on all developers, operators and other, in accordance with applicable laws, legislation and ethics.
	7.1.2	Terms and conditions of employment	Y		x				Users of the system may consent and sign the terms and conditions of the before operating or developing the software.
	7.2	During employment							
	7.2.1	Management responsibilities	Y				x		Assign compliance duties by ensuring that people responsible for operating and identifying the risks for thr protection of the system, weaknesses and controls applicable to their job positions. Training the employees to adhere to guidelines and maintanance of policies and procedures. Get necessary certifications.
	7.2.2	Information security awareness, education and training	Y				x		Holding sufficient preparation courses for operation of the system. Train to adhere to policies, procedures and guidelines.
	7.2.3	Disciplinary process	Y		x				Should be encountered when there is a critical damage to the system.
	7.3	Termination and change of employment	Y						Policies should be adhered to when terminating.
	7.3.1	Termination or change of employment responsibilities	Y		x				Ensuring the information is secure after an individual or contractor exits the company This is particularly critical, since individuals have data about the systems such as passwords.

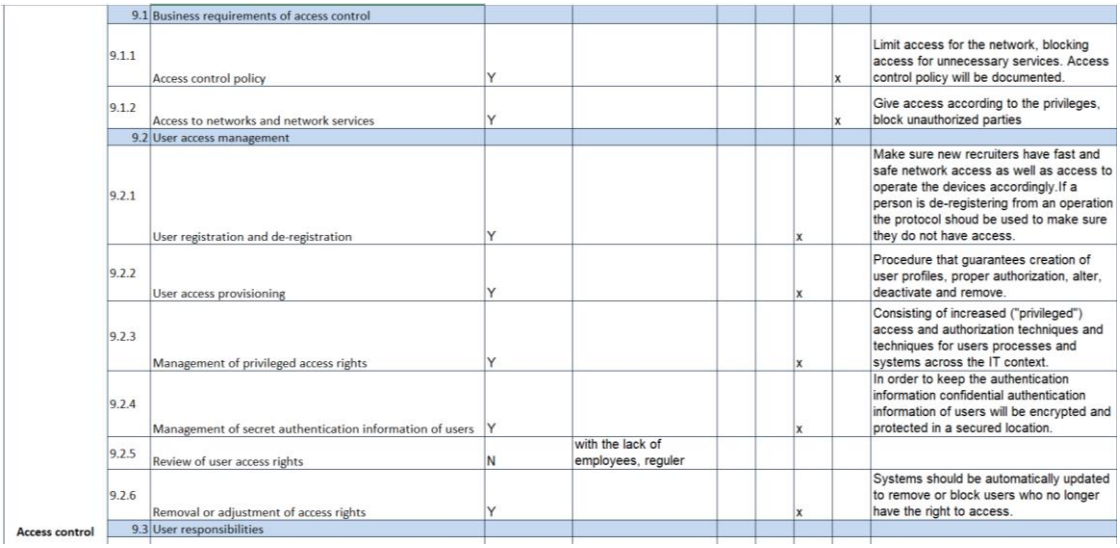
Figure 2.10: SOA for Human resource security

	8.1	Responsibility for assets							
	8.1.1	Inventory of assets	Y				x		It is important to bring together a register or inventory of such assets that demonstrates how they are handled and regulated depending on their value. The products are intended to sell according to the value.
	8.1.2	Ownership of assets	Y				x		Ownership shall be determined upon formation of the assets. The asset owner is responsible for handling the asset efficiently over the entire lifecycle of the asset. In this project there are mainly 4 components. Therefore, the assets belonging for the specific components will be handled by the respective person who is responsible for the component. Mainly The components include, intrusion detection, access control, security configurations and policies and procedures.
	8.1.3	Acceptable use of assets	Y			x			The guidelines for appropriate usage shall be taken into account for staff, contractors, operators, developers and other parties where applicable, and all the information properties to which they have access will be determined and documented in policies. Routine training and knowledge sharing sessions will be done for awareness of acceptable use.
	8.1.4	Return of assets	N	to be carried out from the premises.					

Figure 2.11: SOA for Asset Management – part 1

Asset management	8.2	Information classification							
	8.2.1	Classification of information	Y				x		Information must be categorized according to importance, criticality and severity from the risk assessments, according to information protection and classification policies.
	8.2.2	Labeling of information	Y				X		An acceptable collection of information marking protocols must be established and enforced in compliance with the organization's approved information classification policies.
	8.2.3	Handling of assets	Y				x		Procedures for managing objects must be established and applied in compliance with the scheme for classifying information.
	8.3	Media handling							
	8.3.1	Management of removable media	Y				x		The removable media must be tested for risks periodically, specific risk evaluations will need to be carried out. Awareness for use of removable media shoud be given through trainings, storage and access for the media should be logged.
	8.3.2	Disposal of media	Y					x	If no longer needed media have to be disposed of by following recorded protocols securely. These protocols mitigate the risk of disclosure to unauthorized parties to classified information.
	8.3.3	Physical media transfer	Y					x	Encrypting the classified media information in transit, Wrapping should be sufficient to protect the products during transit from any physical damage, and maintain records.

Figure 2.12: SOA for asset management-part 2

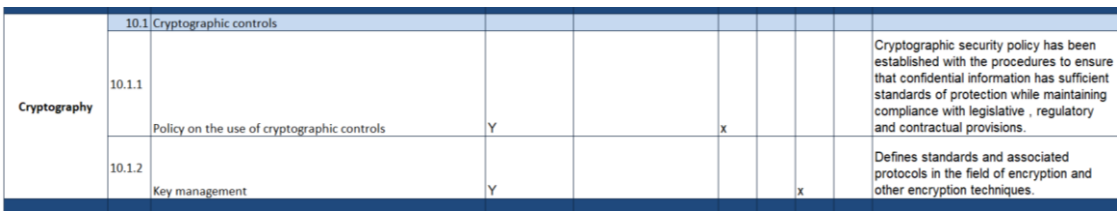


	9.1	Business requirements of access control							
	9.1.1	Access control policy	Y					x	Limit access for the network, blocking access for unnecessary services. Access control policy will be documented.
	9.1.2	Access to networks and network services	Y					x	Give access according to the privileges, block unauthorized parties
	9.2	User access management							
	9.2.1	User registration and de-registration	Y				x		Make sure new recruiters have fast and safe network access as well as access to operate the devices accordingly.If a person is de-registering from an operation the protocol shoud be used to make sure they do not have access.
	9.2.2	User access provisioning	Y				x		Procedure that guarantees creation of user profiles, proper authorization, alter, deactivate and remove.
	9.2.3	Management of privileged access rights	Y				x		Consisting of increased ("privileged") access and authorization techniques and techniques for users processes and systems across the IT context.
	9.2.4	Management of secret authentication information of users	Y				x		In order to keep the authentication information confidential authentication information of users will be encrypted and protected in a secured location.
	9.2.5	Review of user access rights	N	with the lack of employees, reguler					
	9.2.6	Removal or adjustment of access rights	Y				x		Systems should be automatically updated to remove or block users who no longer have the right to access.
Access control	9.3	User responsibilities							

Figure 2.13: SOA for access control-part 1

Access control	9.2.6	Removal or adjustment of access rights	Y				x		Systems should be automatically updated to remove or block users who no longer have the right to access.
	9.3	User responsibilities							
	9.3.1	Use of secret authentication information	Y			x			The assignment of user access rights from initial user login to removal if no longer necessary, including special access control rights restrictions and password management, should be monitored.
	9.4	System and application access control							
	9.4.1	Information access restriction	Y				x		User rights of access to data and systems should be compatible with business requirements and job requirements identified and reported.
	9.4.2	Secure log-on procedures	Y					x	Encrypt all administrative non-console accesses. For web-based administration and other operational accesses, use technologies such as SSH, VPN or SSL / TLS.
	9.4.3	Password management system	Y				x		The set of standards and best practices that users adopt during the effective storage and management of credentials to avoid unauthorized usage according to the password policy.
	9.4.4	Use of privileged utility programs	Y				x		The device and application functions capable of overriding shall be limited and regulated closely.
	9.4.5	Access control to program source code	Y				x		Confirm that the workers in charge of bringing the program to production and the personnel in charge of the implementation of the software have a reasonable dividing line.

Figure 2.14: SOA for Access control-part 2



	10.1	Cryptographic controls							
Cryptography	10.1.1	Policy on the use of cryptographic controls	Y		x				Cryptographic security policy has been established with the procedures to ensure that confidential information has sufficient standards of protection while maintaining compliance with legislative , regulatory and contractual provisions.
	10.1.2	Key management	Y				x		Defines standards and associated protocols in the field of encryption and other encryption techniques.

Figure 2.15: SOA for Cryptography

	11.1	Secure areas	y						
	11.1.1	Physical security perimeter	y					x	Protected physical assets can be accessed only by authorized personal.
	11.1.2	Physical entry controls	y					x	Authorize access by key cards to the premises, fingerprint access for manufacturing systems, CCTV cameras to monitor, door-locks, security guards,walls and barriers
	11.1.3	Securing office, room and facilities	y					x	Alarms, CCTv camera, locks
	11.1.4	Protecting against external end environmental threats	y					x	Awareness and training to act when external threats occurs, fire exits and alarms
	11.1.5	Working in secure areas	y				x		Restriction process for unauthorized people, securing the area with a security officer.
Physical and environmental security	11.1.6	Delivery and loading areas	y				x		Seperate areas for delivery and loading
	11.2	Equipment	y			x			
	11.2.1	Equipment siting and protection	y				x		Protection of workspace and best practices and policies

Figure 2.16: SOA for physical and environmental security-part 1

Physical and environmental security	11.1.6	Delivery and loading areas	y				x		Seperate areas for delivery and loading
	11.2	Equipment	y			x			
	11.2.1	Equipment siting and protection	y				x		Protection of workspace and best practices and policies
	11.2.2	Supporting utilities	y				x		Securing utilities by good practices
	11.2.3	Cabling security	y					x	securing cables with relevent and quality materials
	11.2.4	Equipment maintenance	y				x		Policies and procedures for equipment maintanance
	11.2.5	Removal of assets	y				x		Assets should be removed onlyaccording to removal protocols.
	11.2.6	Security of equipment and assets off-premises	y					x	Signing agrrements to ensure security of off premises equipment
	11.2.7	Secure disposal or re-use of equipment	y					x	sensitive data in papers should be disposed using shredders, Bins for recycling plastic equipments
	11.2.8	Unattended user equipment	y				x		Policies for cleaning and removal of unattended equipments
	11.2.9	Clear desk and clear screen policy	y					x	Awareness and training courses and policies.

Figure 2.17: SOA for physical and environmental security-part 1

	12.1	Operational procedures and responsibilities							
	12.1.1	Documented operating procedures	Y				x		Creating and updating SOPs(Standard operating procedures) for the requrements.
	12.1.2	Change management	Y				x		Change management according to the new trends or if the systems should be develped according to new technologies, business transformations.
	12.1.3	Capacity management	Y					x	By defining parameters and SOPs to prevent system from crashing
	12.1.4	Separation of development, testing and operational environments	Y				x		Seprate enviroment for further improvements, separate environments for testing because it would ommit unnesessary risks.
	12.2	Protection from malware							
	12.2.1	Controls against malware	Y					x	Using anti virus software, update management
	12.3	Backup							
	12.3.1	Information backup	Y				x		backing up information regularly or periodically.
Operations security	12.4	Logging and monitoring							
	12.4.1	Event logging	Y				x		maintaining event logs to track events
	12.4.2	Protection of log information	Y				x		assigning permission to log files
	12.4.3	Administrator and operator logs	Y				x		logging commands issued by administrators
	12.4.4	Clock synchronisaton	Y				x		helps to keep track of time that an event occured

Figure 2.18: SOA for operations security-part 1

	12.4.4	Clock synchronisaton	Y				x		helps to keep track of time that an event occured
	12.5	Control of operational software							
	12.5.1	Installation of software on operational systems	Y					x	Installation can only be done with prior approval by authorized personal.
	12.6	Technical vulnerability management							
	12.6.1	Management of technical vulnerabilities	Y						Patch update compliance
	12.6.2	Restrictions on software installation	Y					x	Policies for restriction processes, Only administrators can install softwares into organization devices. Restrict the users to install softwares.
	12.7	Information systems audit considerations							
	12.7.1	Information systems audit controls	Y				x		Comply with specific standards based on laws and regulations

Figure 2.19: SOA for operations security-part 2

	13.1	Network security management							
	13.1.1	Network controls	Y					x	Intrusion detection system. By defining firewall policies and network policies, blocking access using ACLs.
	13.1.2	Security of network services	Y					x	By hardening ssh, http and other network services
Communications security	13.1.3	Segregation in networks	Y					x	By planing the network according to the requirement.
	13.2	Information transfer							
	13.2.1	Information transfer policies and procedures	Y					x	How to transfer sensitive data, using encryption.
	13.2.2	Agreements on information transfer	Y		x				When transfering confidential data
	13.2.3	Electronic messaging	Y				x		By using internal email services, only usng authorized services for message sharing.
	13.2.4	Confidentiality or non-disclosure agreements	Y		x				For confidential data and documents

Figure 2.20: SOA for communications security

	14.1	Security requirements of information systems							
	14.1.1	Information security requirements analysis and specification	Y				x		Octave risk assessment, ISO 27001 and IEC 62443 security standards
	14.1.2	Securing applications services on public networks	Y		x				Encrypted communication
	14.1.3	Protecting application services transactions	Y		x				Encrypted communication
	14.2	Security in development and support processes							
	14.2.1	Secure development policy	Y					x	Using SDLC development cycle
	14.2.2	System change control procedures	Y				x		System changes are only done by authorized personnel, creating SOPs/policies for system changes
System acquisition, development and maintenance	14.2.3	Technical review of applications after operating platform changes	Y				x		Audits to ensure system runs without any crashes.
	14.2.4	Restrictions on changes to software packages	Y				x		Deny access to change software packages for operators and users. Allow access for authorized engineers.
	14.2.5	Secure system engineering principles	Y					x	Secure system development standards
	14.2.6	Secure development environment	Y					x	secure software development standerds
	14.2.7	Outsourced development	N	Not applicable					
	14.2.8	System security testing	Y					x	external and internal penetration testing
	14.2.9	System acceptance testing	Y				x		Black box testing
	14.3	Test data							
	14.3.1	Protection of test data	y					x	encrypted when stroring

Figure 2.21: SOA for system acquisition, development and maintenance

	14.3	Test data							
	14.3.1	Protection of test data	y					x	encrypted when stroring
	15.1	Information security in supplier relationships							
Supplier relationships	15.1.1	Information security policy for supplier relationships	Y				x		An effective strategy details the segmentation, collection, administration, exit of suppliers, how knowledge assets are managed around suppliers to minimize the associated risks.
	15.1.2	Addressing security within supplier agreements	Y			X			Signing agreements
	15.1.3	Information and communication technology supply chain	Y				x		A strong system procedure for entire garment production life cycle in the context of IoT
	15.2	Supplier service delivery management							
	15.2.1	Monitoring and review of supplier services	Y					x	A good audit defines how companies track, evaluate and inspect their service supply periodically.
	15.2.2	Managing changes to supplier services	Y				x		An effective monitoring explains how any improvements to vendors' supply of services are handled and enhancement of existing information management practices, processes and controls.
	16.1	Management of information security incidents and improvements							
	16.1.1								A successful procedure explains how the management defines roles and processes to ensure a swift, efficient and organized response to operations and resolve

Figure 2.22: SOA for supplier relationship

	16.1	Management of information security incidents and improvements							
	16.1.1	Responsibilities and procedures	Y		x				A successful procedure explains how the management defines roles and processes to ensure a swift, efficient and organized response to operations and resolve vulnerabilities, accidents and incidents of carelessness or deliberate offenses.
	16.1.2	Reporting information security events	Y				x		Good monitoring means that accidents and activities related to information security can be recorded as quickly as possible across relevant management channels for quick responses.
	16.1.3	Reporting information security weaknesses	Y					x	The monitoring is focused solely on accidents and events but may be handled accordingly according to risk management and event management policies as well as business continuity plan.
Information security incident management	16.1.4	Assessment of and decision on information security events	Y					x	Information security events need to be reviewed, and then it should be determined if they can be categorized as information security accidents, vulnerability, events according to the octave risk assessment framework.

Figure 2.23: SOA for Information security incident management

Information security incident management	16.1.4	Assessment of and decision on information security events	Y					x	Information security events need to be reviewed, and then it should be determined if they can be categorized as information security accidents, vulnerability, events according to the octave risk assessment framework.
	16.1.5	Response to information security incidents	Y					x	It is still important to appoint members, be transparent on actions and timescales and maintain the details for audit purposes, as with all for ISO 27001.
	16.1.6	Learning from information security incidents	Y					x	This is an essential regulation, and the strategy needs to show the expertise gained by evaluating and addressing events relating to information security. The weaknesses should be analyzed and the best solutions should be implemented while making sure the same incident will not occur again.
	16.1.7	Collection of evidence	Y					x	The organization should collect data periodically and have a log system which can be used as evidence, must identify and enforce controls for the identification, collection , acquisition and retention of information.

Figure 2.24: SOA for Information security incident management

Information security aspects of business continuity management	17.1	Information security continuity							
	17.1.1	Planning information security continuity	Y					x	Maintaining access control, having a business continuity plan
	17.1.2	Implementing information security continuity	Y					x	Implement specific procedures
	17.1.3	Verify, review and evaluate information security continuity	Y					x	Through audits
	17.2	Redundancies							
	17.2.1	Availability of information processing facilities	Y					x	Keep track on information security processing facilities, log reviews

Figure 2.25: SOA for Information security aspects of business continuity management

management	17.2	Redundancies							
	17.2.1	Availability of information processing facilities	Y					x	Keep track on information security processing facilities, log reviews
	18.1	Compliance with legal and contractual requirements							
Compliance	18.1.1	Identification of applicable legislation and contractual requirements	Y		x				keeping upto date with legislation, regulatory and contractual requirements
	18.1.2	Intellectual property rights	Y		x				Appling for IP rights and paitents gives legal benifits
	18.1.3	Protection of records	Y			x			protecting records are company's obligation
	18.1.4	Privacy and protection of personally identifiable information	Y			x			Company is obligated to protecting PII
	18.1.5	Regulation of cryptographic controls	Y					x	Using recommended cryptographic mechanisms
	18.2	Information security reviews							
	18.2.1	Independent review of information security	Y				x		when regularly reviewing policies independently helps to identify significate changes.
	18.2.2	Compliance with security policies and standards	Y			x			Regularly reviewing policies and standards
	18.2.3	Technical compliance review	Y			x			Regularly reviewing technical controls that enforces policies and standards

Figure 2.26: SOA of compliance

2.2.1.2 Conduct a risk assessment

Determined issues which has to be addressed, also to which instance or degree should the issues be addressed in the overall system, coordinated activities for directing and controlling risks.

The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) risk assessment framework is a methodology for identifying and assessing asset information security risks. OCTAVE is highly personalized, self-directed, and adaptable. Octave could be customized according to the requirements. Therefore, the risk assessment was conducted using OCTAVE Allegro. The following aspects are highlighted in Octave:

- Determine the importance of vital assets.
- Concentrate risk analysis on the most critical assets.
- Think about the connections between critical assets.
- To reduce risk, develop a practice-based protection strategy and risk mitigation plans.

Risk assessment was conducted for identified assets and each critical asset was evaluated through OCTAVE Allegro worksheet 8 and OCTAVE Allegro worksheet 10.

1. Allegro worksheet 8: Critical information asset profile – For each critical asset rationale for selection, stating why information asset is important to the organization, agreed description for the critical asset, who owns the asset, CIA security requirements and other requirements are stated along with the most important security requirement.
2. Allegro worksheet 10: Information asset risks are identified for each critical asset. The threats were identified with the area of concern and the actor, means, motive, outcome, security requirements and probability of occurrence and consequences for the threat were identified. The severity was scored in a 1-10 scale according to the impact area to finally, get the relative risk score for each threat. Refer Appendix 2 for the critical information asset profile and Information asset risks for the critical asset, CNC machine.

According to the information gathered from OCTAVE risk assessment, a heat map was generated for the critical assets to determine which threats are most likely to occur in the system.

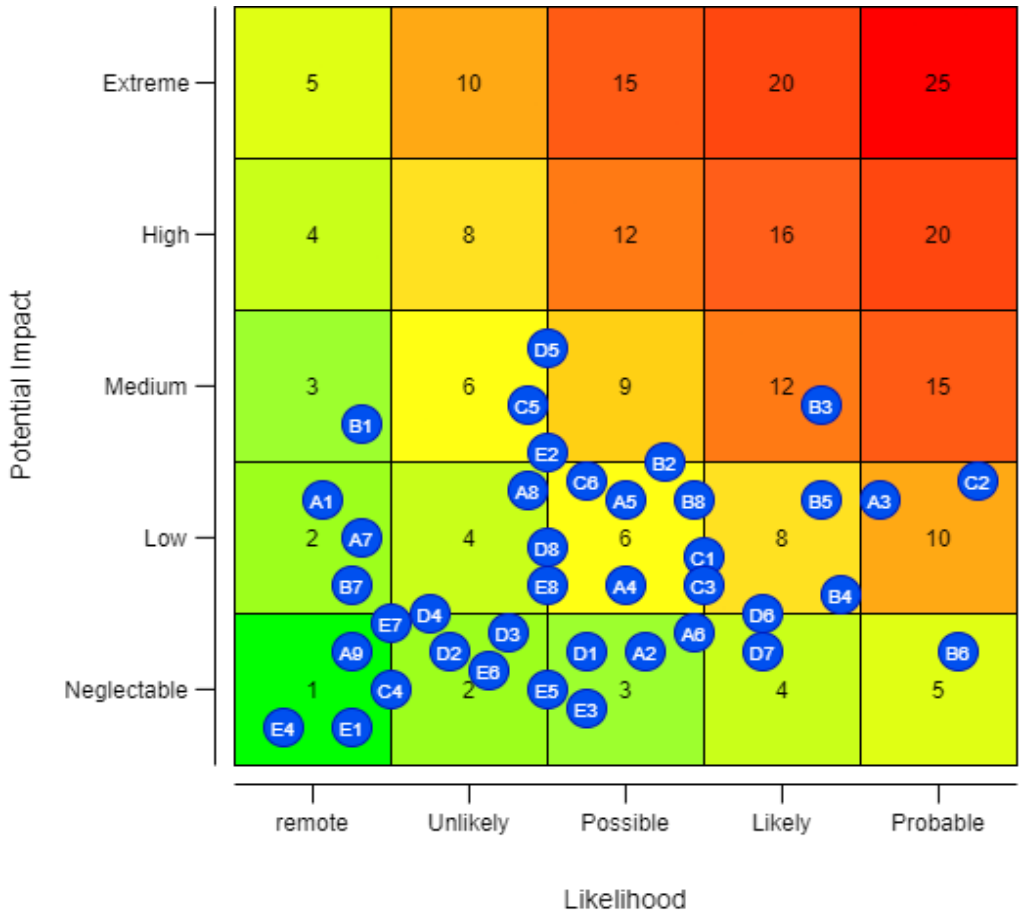


Figure 2.27: Heat map

Table 2.1: Threats and related devices

ID	Name
A1	Unauthorized access to Ansible controller via network - Ansible controller
A2	Disclosure of access credentials - Ansible controller
A3	Denial of service attacks - Ansible controller
A4	Unauthorized access to ansible controller via console - Ansible controller
A5	Ransomware - Ansible controller
A6	Spyware - Ansible controller
A7	Power outage - Ansible controller
A8	Trojan - Ansible controller
A9	Overloading system storage - Ansible controller
B1	Overheat - IOT
B2	Ransomware - IOT
B3	Unauthorized access to ansible controller via network - IOT
B4	Disclosure of access credentials - IOT
B5	Denial of service attacks - IOT
B6	Spyware - IOT

B7	Power outage - IOT
B8	Overloading system storage - IOT
C1	Unauthorized network scans and reconnaissance attacks - Internal network
C2	DOS attack - Internal network
C3	Unauthorized connected devices - Internal network
C4	Backdoors - Internal network
C5	Malware - Internal network
C6	Brute force attacks - Internal network
D1	Automated CNC machines can be left unattended - CNC
D2	power failure - CNC
D3	Natural disaster - CNC
D4	Overheat - CNC
D5	Hardware failure - CNC
D6	Unauthorized access through network - CNC
D7	Unauthorized connected devices - CNC
D8	Malware - CNC
E1	Power outage - Sensors

E2	Hardware failure - Sensors
E3	Unauthorized access through an unsecured network - Sensors
E4	Unauthorized access through outdated and insecure devices - Sensors
E5	Tamper a network physically - Sensors
E6	Natural disaster - Sensors
E7	Overheat - Sensors
E8	Unauthorized connected devices - Sensors

2.2.1.3 Identify the specific standards, procedures and guidelines for each identified components and overall system.

An overview of overall cyber security and IoT security standards and frameworks were identified and evaluated after searching via the internet blogs, articles, research papers, journals and digital libraries. Suitable frameworks and standards for the project was thoroughly researched, identified and evaluated for policy creation. The information about suitable standards and frameworks were gathered through internet and literature found in research libraries such as Google scholar and Institute of Electrical and Electronics Engineers (IEEE). They provided information about frameworks as well as standards in development as well as the standards and frameworks widely popular around the world articles and blogs from the internet provided significantly important and necessary information about suitable IoT security standards.

Frameworks such as NIST, ISO, IEC, and SCADA can be used according to the different aspects of IoT, therefore a thorough research was done to identify what standards and frameworks are most important to each critical asset for the smart system. There are many Information security management standards and IoT security standards which are implemented in different organizations and systems globally.

2.2.1.3.1. Standards identified for critical aspects in the research.

2.2.1.3.1.1 Firewall and network security

Using NIST Special Publication 800-4, Guidelines on Firewalls and Firewall Policy, create a firewall policy that specifies how firewalls can handle inbound and outbound network traffic. Creates firewall rules, as well as picking, configuring, inspecting, installing, and managing firewalls, with step-by-step instructions. The NIST - US has released a free special publication for firewall security aspect.

2.2.1.3.1.2. CPS

CPS are at the heart of the next generation of industrial control systems. Framework for Cyber-Physical Systems, NIST Special Publication 1500-201. The IEC 61499 standard adds a higher level of design, allowing for the versatile combination of software components while maintaining hardware independence. On top of Raspberry Pi boards, this work addresses the design of applications using the IEC 61499 standard.

2.2.1.3.1.3. Authentication and access monitoring

Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST Special Publication 800-137, is a NIST special publication for authentication and access monitoring, and NIST SP 800-92 is a guide to Computer Security Log Management. Electronic authentication rules are outlined in NIST SP-800-63-1.

Cyber security standards are techniques that are commonly set out in published materials that are intended to protect a user's or organization's cyber environment. Users, networks, computers, software, processes, information in storage or transit, applications, facilities, and systems that can be linked directly or indirectly are all part of this area to be protected. ISO 27001 for information security management systems, IEC 62443 which defines processes, techniques and requirements for Industrial Automation and Control Systems, NIST framework and ISO/IEC 30163:2021 standard which specifies the system requirements of an Internet of Things (IoT)/Sensor Network (SN) technology-based platform for chattel asset are some of the standards that could be used for the research. The Software Development Life Cycle (SDLC) is a well-defined approach for producing high-quality, low-cost software in the shortest possible amount of time framework.

A document which provides a brief overview of standards and frameworks that could be used in the research project about cyber security automation of industrial 4.0 garment manufacturing system was created.

Written norms are expected to render cyber security initiatives clear therefore the standard identification document was prepared according to all suitable security standards and frameworks after a discussion with the group members and a security policy developer's instructions were taken. Cyber security standards, are generic collections of prescriptions for the best implementation of specific steps, created by industry experts. Therefore, Methods, protocols, reference structures, and other items may be included in the specifications. It ensures security reliability, promotes integration and interoperability, and allows for practical measure comparison. As a regulation, a guideline, or a description, a written specification that establishes a common language, includes a technical specification or other detailed requirements, and is intended to be followed consistently. The goal of security standards is to improve the security of information technology (IT) systems, networks, and critical infrastructures.

2.2.1.3.2. Evaluation for the identification of most suitable standards and frameworks

2.2.1.3.2.1 ISO 27000 Series

The International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) created a set of information security standards to provide a globally recognized foundation for best information security management practices. It aids the firm in safeguarding its information assets, such as personnel information, financial data, and intellectual property.

Because of the risk of cyber-attacks that enterprises confront, the ISO 27000 series is required. Cyber-attacks are becoming more common by the day, posing a persistent threat to any sector that relies on technology. ISMS is a systemic approach to risk management, including measures to address people, processors and technology.

2.2.1.3.2.1.1 ISO 27001

This standard enables us to demonstrate to clients and stakeholders that any company is maintaining their personal data and information with the utmost care. This standard outlines a method for establishing, implementing, running, monitoring, maintaining, and upgrading our ISMS that is based on processes. ISO IEC 27001: 2013 is the only standard in the series that

can be audited and certified against. ISO 27001 based ISMS can demonstrate many efficiencies and other benefits such as;

• Improved system dependability and security: Security is often defined as protecting the Confidentiality, Integrity, and Availability of an asset. If a system or an organization uses a standards-based strategy to ensure that adequate controls, processes, and procedures are in place, the stated objectives will be met. By default, meeting the CIA's security objectives will improve the system's dependability, availability, and accessibility. Having stable, secure, and reliable systems means that system interruptions are kept to a minimum, enhancing availability and productivity. In addition to the foregoing, a standards-based approach to data security is recommended.

• Reduced Costs: Standards based approach to information security ensures that all controls are measured and managed in a structured manner. As a result, processes and procedures become more simplified and effective, minimizing expenses. Companies have realized they can better manage the tools they have in place by consolidating redundant systems or re-assigning other systems from assets with low risk to those with higher risk.

• Legislation compliance: Having a well-structured Information Security Management System in place makes compliance considerably easier.

• Better Management: Knowing what's in place and how it should be managed and safeguarded makes it easier to manage information resources inside a company.

• Improved Customer and Partner Relationships: Customers and trading partners can interact with the company with confidence knowing that the company has taken an independently verifiable approach to information security risk management.

ISO 27001 can be adopted as a framework for an organization to work against, or the organization can seek certification against the standard. An organization's certification to ISO/IEC 27001 shows that it has designed and implemented best-practice information security processes. Certification will be benefited when gaining new clients and improve competitiveness, enhancing reputation, improve structure and focus.

2.2.1.3.2.2. IEC 62443

The IEC 62443 cyber security standard defines processes, techniques and requirements for Industrial Automation and Control Systems (IACS). Its documents are the result of the IEC

standards creation process where all national committees involved agree upon a common standard. Targets at three main roles:

• Product suppliers that develop, distribute and maintain components or systems used in automated solutions.

• System integrators that design, deploy and commission the automated solution.

• Asset owners that operate, maintain and decommission the automated solution.

Planned and published IEC 62443 work products for IACS Security. All IEC 62443 standards and technical reports are organized into four general categories called General, Policies and Procedures, System and Component.

1. The first category includes foundational information such as concepts, models and terminology.

2. The second category of work products targets the Asset Owner. These address various aspects of creating and maintaining an effective IACS security program.

3. The third category includes work products that describe system design guidance and requirements for the secure integration of control systems. Core in this is the zone and conduit design model.

4. The fourth category includes work products that describe the specific product development and technical requirements of control system products.

2.2.1.3.2.3. ISO/IEC 30163:2021

This standard specifies the system requirements of an Internet of Things (IoT)/Sensor Network (SN) technology-based platform for chattel asset monitoring supporting financial services.

2.2.1.3.2.4. NIST Cyber Security Framework

To assist firms in managing their cyber security risks, the Framework incorporates industry standards and best practices. It establishes a common vocabulary that enables employees at all levels of a company and at all points in the supply chain to acquire a shared awareness of their cyber security threats. The Framework not only helps organizations understand their cyber security risks. Improve the security of the essential infrastructure, shielding it from both internal and external threats. NIST Cyber Security Framework describes five functions that manage the risks to data and information security which are identify, protect, detect, respond,

and recover. The primary components consist of the Core, Profiles, and Implementation Tiers. The Core offers guidance to organizations wanting to get better protection for their information systems.

IDENTIFICATION OF POTENTIAL CYBER SECURITY STANDARDS, PROCEDURES, GUIDELINES AND FRAMEWORKS FOR THE CYBER SECURITY AUTOMATION OF INDUSTRIAL 4.0 GARMENT MANUFACTURING SYSTEM

Abstract

Cyber security standards are techniques that are commonly set out in published materials that are intended to protect a user's or organization's cyber environment. Users, networks, computers, software, processes, information in storage or transit, applications, facilities, and systems that can be linked directly or indirectly are all part of this area to be protected. ISO 27001 for information security management systems, IEC 62443 which defines processes, techniques and requirements for Industrial Automation and Control Systems, NIST framework and ISO/IEC 30163:2021 standard which specifies the system requirements of an Internet of Things (IoT)/Sensor Network (SN) technology-based platform for chattel asset are some of the standards that could be used for the research. The Software Development Life Cycle (SDLC) is a well-defined approach for producing high-quality, low-cost software in the shortest possible amount of time framework. This document provides a brief overview of standards and frameworks that could be used in the research project about ***cyber security automation of industrial 4.0 garment manufacturing system***

I. Introduction

Written norms are expected to render cyber security initiatives clear. These requirements are referred to as cyber security standards, and they are generic collections of prescriptions for the best implementation of specific steps, created by industry experts. Methods, protocols, reference structures, and other items may be included in the specifications. It ensures security reliability, promotes integration and interoperability, and allows for practical measure comparison. A written specification that defines a common language, includes a technical specification or other precise requirements, and is intended to be used consistently, as a law, a guideline, or a description. The aim of security standards is to make information technology (IT) systems, networks, and essential infrastructures more secure.

Figure 2.28: Screen shot of the standard identification documentation

Please refer Appendix 3 for the overall documentation of most suitable standard identification and evaluation documentation for the smart system

2.2.1.4 Choose the most suitable standards and frameworks

The most suitable standards and frameworks were chosen after evaluating the details for each component and their requirements. Two security standards were chosen after discussing and evaluating the details of most suitable standards with group members and policy developers in the industry. The most practical standards to implement in the research project was chosen according to the system requirements. Therefore, the research needed a standard for information security management and IoT security. The chosen standards were compared and documented.

2.2.1.4.1. ISO 27001:2013

This International Standard provides requirements for establishing, implementing, maintaining and continually improving an information security management system to support strategic decisions for needs and objectives, security requirements, system processes used, size of the audience and structure in ISMS. Also a comparison of chosen cyber security standards for the cyber security automation of industrial 4.0 garment manufacturing system were conducted.

2.2.1.4.2. IEC 62443

Developed to secure industrial automation and control systems (IACS) throughout their lifecycle. It currently includes nine standards, technical reports (TR) and technical specifications (TS). IEC 62443 was initially developed for the industrial process sector but IACS are found in an ever-expanding range of domains and industries.

IACS technologies are central to critical infrastructure. Implementing IEC 62443 can help to lessen the effects of cyber-attacks and even avoid them. It can improve security and lower expenses throughout the lifecycle.

IEC 62443 covers not just the technology that makes up a control system, but also the processes, countermeasures, and people working in it.

Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program.

2.2.1.4.3. Importance of using both standards

There are significant variations between Operational Technology (OT) and Information Technology (IT) systems. One of the most notable differences is that industrial process failures frequently have an impact on the physical world, they might impair human health and welfare, risk the environment by spilling hazardous materials, or have an economic impact, such as in the case of severe power outages. In addition, the emphasis on basic security objectives. IT emphasizes data confidentiality, whereas OT prioritizes system availability; the security goals of both domains are thus diametrically opposed.

IEC 62443 lays forth the specific requirements of IACS while also building on existing best practices. This means that sections of IEC 62443 were written with ISO 27001 under reference, but they also take into account the distinctions between IACS and IT systems. In addition, the standard not only outlines how to design a management system, but it also specifies precise functional and process requirements for both individual IACS components as well as complete control systems. As a result, IEC 62443 has a far broader scope than ISO 27001 and is more customized to the needs of IACS.

Both can be used together in a sense that ISO 27001 practices can help protect the information used to implement IACS and ensure the development process is effective in implementing the security practices defined by IEC 62443. Addressing the cyber security of these systems using a customer service management system that meets the requirements laid out in IEC 62443.

Table 2.2: Comparison of chosen security standards for the research

	ISO 27001	**IEC 62443**
Organizations involved on creating the standard	ISO (the International Organization for Standardization) and IEC (the International Electro technical Commission)	The International Electro technical Commission (IEC)
Directives	Drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.	This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.
Scope	Information Security Management Systems	Cyber Security Management System (CSMS) for industrial automation and control systems (IACS)
Certifications	Yes	Yes. Number of organizations offering the certifications are smaller, some of the most prominent players are TÜV, exida, CertX, UL, DEKRA and ISASecure.
Controls	114 controls in 14 categories	Thirteen documents which are organized into four groups: General, Policies and Procedures, System, and Component.

2.2.1.4.4. Relationship between IEC 62443 standard and ISO/IEC 27001

Much of the content in the ISO standard is applicable to IACS as well. The IEC 62443 standard emphasizes the need for consistency between the practices to manage IACS cyber security with the practices to manage business/information technology systems cyber security. Economies will be realized by making these programs consistent. IEC 62443 standard builds on the guidance in the ISO/IEC standards. It addresses some of the important differences between IACS and general business/information technology systems. It introduces the important concept that cyber security risks with IACS.

2.2.1.5 Verify the chosen standards and frameworks

Verified the accountability of the chosen standards and frameworks whether they could be accountable to the automated manufacturing system through the advice from industrial experts. Industrial security standards verification was done through external supervisor. Security standards were verified through a security industry expert.

2.2.1.6 Determine the types of policies that are needed.

Identify the types of policies needed to the automation system such as password policies, network and authentication and access control policies, security update policies, acceptable use policies, encryption policies, vulnerability management policies according to standards and legislations. This information about policy creation was also gathered through various blog sites about standardization which determined how to implement ISO 27001:2013 and IEC 62443. The two standards were thoroughly analyzed and according to the system requirements the policies were identified. Each policy was created combining the two standards giving a customized policy creation according to the two standards. The policy documentation were done according to the steps to implement ISO 27001. The ISO 27001 toolkit documentation lead to a better understanding how to implement the policies. For example, see Appendix 4 for audit policy and password policy.

2.2.1.7 Verify policy creation

Created information security policies can be verified by the security expert from the industry before implementing the policies. So that we could be sure that our implemented security policies are secure.

2.2.1.8 Implement policies for the components

Properly installed and set up all of the key technologies and tools in the system, prepare the actual policies and procedure documents, import the initial set of policies, customize rule sets ensuring that the policies are adhered to in the tools to enforce policies accordingly.

2.2.1.9 Testing results

The policy creation was verified by an industry expert. Furthermore, after implementing the policies members who are responsible for each component conducted testing, auditing to ensure and verify that the applied policies are secured. The results were successful without error.

2.2.2 Update management

Create a centralized security update management system using local repositories.

Below shows the work break down structure for the update management component.

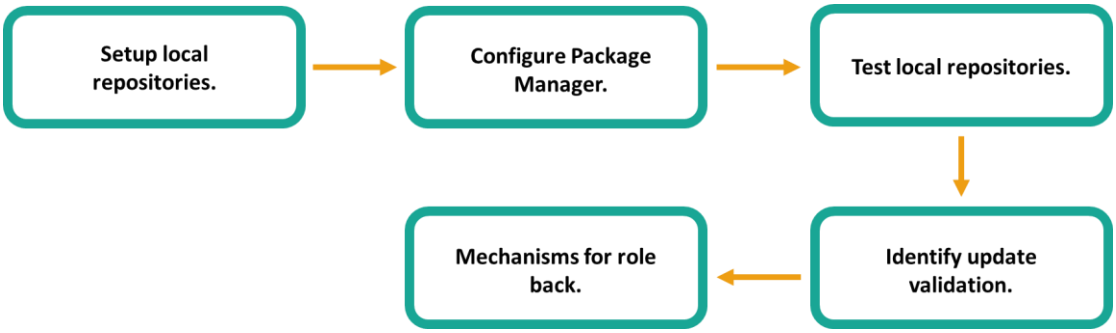


Figure 2.29: Individual Workflow Diagram- Security Updates

2.2.2.1 Setup local repositories

System administrators should always install software, security updates for all the devices. It is consuming a lot of internet bandwidth. As a solution to this above mentioned issue, instead of downloading software each time to all systems, all applications are saved in a local server in the LAN and distributed among clients when required in the same time. This solution is fast and efficient because the LAN connections are faster. This saves the internet bandwidth reducing the cost for internet.

Creating a local repository is advantages when the devices are connected and have to install more software. Setup a central local repository in the server, so that the clients can install, update and upgrade the packages from the central repository without using internet.

Host the created repo using apache server.

Add required packages to the local repository frequently. Pull the packages from public repositories from the package server and save locally. Install apt-mirror.

2.2.2.2 Configure package manager

Create a directory in the hard disk to save all packages. Go to the latest mirror package repository and run apt-mirror to get all the packages in the repository.

2.2.2.3 Configure IoT devices to access previously setup local repository

Web server is needed to be able to access the repo from other devices. Configure the Apache server. Create a link. Add repository source in other devices to fetch the repository and packages.

2.2.2.4 Test local repositories

Install packages using added local repository

2.2.2.5 Verify update

Verify updates using GPG keys to identify rogue updates.

2.2.2.6 Mechanisms for roll back

Keep previous version of packages to roll back or downgrade updates.

2.3. Commercialization aspect of the product

The standardization aspect could be commercialized after developed as a customized security framework for industrial 4.0 manufacturing systems at a reasonable price.

The overall security system could be successfully tested and promote as a cost-effective solution for small to medium businesses, targeting towards businesses who are migrating towards Industry 4.0.

3. RESULTS, RESEARCH FINDINGS AND DISCUSSION

3.1. Standardization

3.1.1 Identify the specific standards and comparison of chosen security standards

Before identifying the standards and the research indicated it was important to learn the difference between security standards and frameworks. As a result, it was important to have an idea about the difference between standards and frameworks. Then as per the discussion with the group members and professionals two standards were chosen ISO 27001:2013 and IEC 62443, but when followed and the policies were made according to the security standards NIST cyber security framework special publications were needed to create policies.

Table 3.1: Security standard Vs. Security framework

Security Standard	Security Framework
A cyber security standard defines both functional and assurance requirements within a product, system, process, or technology environment. Well-developed cyber security standards enable consistency among product developers and serve as a reliable metric for purchasing security products. • Best-known practice. • Defines the steps and procedures involved. • Internationally recognized standards mean that the same procedure is followed throughout the globe to perform a certain task if that particular standard has been adopted. • Ensures that all companies follow the bare-minimum requirements to keep their client's data safe.	A security framework is a compilation of state-mandated and international cyber security policies and processes to protect critical infrastructure. It includes precise instructions for companies to handle the personal information stored in systems to ensure their decreased vulnerability to security-related risks. • Structure underneath or beyond a system. • Not defined to the point. • Gives an outline.
IOT Security Standards examples: European Telecommunications Standards Institute	IoT security Frameworks examples:

(ETSI) EN 303 645 - ETSI TS 303 645 V2.1, provisions for the security of consumer devices that are connected to a network, ENISA Baseline security recommendations for IoT in the context of Critical Information Infrastructures, The National Institute of Standards and Technology's (NIST's) set of basic IoT security practices for manufacturers, OWASP Internet of Things Security Verification Standard (ISVS) provides security requirements for IoT applications.	IoT security Compliance framework, from the IoT security foundation, IEC 62443

After identifying and comparing, the most suitable security standards were chosen and those standards were followed for policy creation.

3.1.2 Policy creation

The ISO 27001:2013 toolkit was followed as a guide for policy creation, but as it is mostly used for organizational processes, only the parts required for the smart system was considered. The asset registry and the business case documentation was created and they were useful for the risk assessment to identify requirements and assets.

3.1.3 Implementation of policies

3.1.3.1 Password policy

According to the ISO 27001 standard, the password policy should include an interactive password management system that ensures quality passwords.

According to IEC 62443 there are three main password requirements highlighted:

1. Password-based authentication's strength
2. Password generation and lifetime constraints
    - Human users
    - Software processes and devices
3. All users' passwords have a lifetime limit (humans, software processes, devices)

Human users should be identified for all access to components. The authentication passwords are used when authenticating to the Linux centralized security management system and the firewall is password protected when authenticating via interface.

The standard requires multi factor authentication for authentication of all access components. Limitations are that the multi factor authentication is costly. A key management server is required if using tokens for authentication. There also could be security overhead, if multi factor authentication in each IoT device. Instead, the access through the smart lock is authenticated through biometrics using finger prints. The smart lock is connected to the security management system through console, but the security management system is also password protected. The password less accounts are automatically locked through root. The biometric smart lock is the first layer of defense of the physical security for the smart system. An Identifier such as an ID for the user or a physical key can be used for physical security as multi factor authentication for smart lock. In our proposed system, only the critical assets are password protected based on the cost, but for future endeavors tokens can be used for multi factor authentication. The security management system has group based authentication. The permissions granted to the identified human user must be followed. The authentication enforcement is further discussed under Authentication and authorization policies. Passwords are always stored with hash function, not in plain text.

According to IEC 62443 NIST SP 800-63-1 password guidelines were used to enforce password security policies.

Guidelines for password entropy and throttling have been simplified. Please refer to Appendix 4 for the policy details.

3.1.3.2 Audit policy

According to ISO 27001 standard audits at predetermined intervals should determine whether the information security management system complies with information security management system requirements, the requirements of this International Standard while being implemented and maintained effectively.

The audit policy should plan, establish, administer, and maintain audit programs, including frequency, methodology, responsibilities, planning requirements, and reporting. The audit programs must take into account the importance of the processes in question as well as prior audit results determining the audit criteria and scope for each audit. Choose auditors is also an

important task according to the standard. There should be feedback of the ISMS including trends in audit results.

According to IEC 62443 standard, system usage such as monitoring, recording and subject to audit should be notified via a system usage notification, but in our system when auditing, the system is in a down state as auditing of the systems are been audited at a chosen time for all devices reducing the interruption for each device. Scheduled audits take place four times a year. When there are more devices through the network, when the audits are done in a centralized manner in the same time the cost and the redundancy is reduced. It is the system administrators' responsibility to maintain and control the audits.

Components shall support a supervisor manual override for a configurable time or sequence of events. In our system the administrator can log for specific events and they are logged and monitored, whether those logins were failed/successful, what commands were used.

According to IEC 62443, audit records on write-once media is a requirement, but in our system this mechanism is not used. Instead, only the root user can read audit records. The audit records are written in system level and nobody can access or modify the records. Programming access to audit logs is only given by the logs of a centralized system. All notifications of tampering shall be logged. Active monitoring would not be done as it would be unnecessary for the system. The performance will be decreased when actively monitoring the environment.

3.2. Update Management

Update Management system was implemented in Ubuntu. For testing a Raspberry Pi Operating system was used as client.

Refer Appendix 5 for security configurations for update management system.

4. CONCLUSION

Objective of this project is to design and implement an automated system for garment manufacturing system focusing on four major cyber security aspects including, frameworks and standardization, centralized security configurations with update management, authentication and Physical Access Control and Intrusion Detection System (IDS). A comprehensive, cost effective and efficient security solution is proposed with a centralized security approach to overcome the potential challenges of the smart system based on standardization.

Security standards are chosen according to the results of OCTAVE risk assessment, and specific standards are evaluated. The comparison of chosen security standards is done according to the security requirements of the research. Frameworks and standards identified are according to standardization. According to project requirements for the manufacturing system, two standards were chosen to create policies. International Organization for Standardization (ISO) 27001:2013 provides requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) and IEC 62443 developed to secure industrial automation and control systems (IACS) throughout their lifecycle. The comparison and importance of why both standards should be implemented together are evaluated and documented. Next step is to identify and document important policies to use them in implementation. ISO 27001 guidelines were useful to determine the above. The technical requirements of IEC 62443 were useful when implementing the policies for IoT. There were limitations and repercussions when implementing according to the IEC 62443 standard, but they were addressed and solutions were given. After policy creation, the implementation of policies were done accordingly and the results and limitations were discussed.

An update management system was created giving a solution for consuming internet bandwidth when updating client devices often with security updates. Each time there is an update administrators should download software and update the client devices very often. A smart option to save all applications on a local server on LAN and distribute them to other client systems as needed, using a local repository was implemented. It is a very quick and efficient method, as all essential apps are transferred over a fast LAN connection from local server and

minimize the bandwidth required if there are multiple instances of client devices to update which will also reduce the cost of internet.

The research highlighted the fact that, IoT security standards should be chosen carefully according to the requirements, as there are many IoT security standards addressing different areas. The best solution is to customize a framework based on proper standardization according to the requirements of the system. The research showed that if proper standardization is used according to effective standards or frameworks the smart system will be more secure reducing the scope for attacks. Standardization is a proactive measure for reducing threats for an IoT smart system. The threats can be reduced through proper standardization while increasing efficiency and the quality of the smart system.

5. DESCRIPTION OF PERSONAL AND FACILITIES

Table 5.1: Description of Personal and Facilities

Registration no	Name	Task Description
IT18136098	P.A.U.T. De Alwis	• Security standards and policy development Conduct a risk assessment Choose suitable framework and standards Policy creation Policy verification • Update management Create a tool to provide security updates to IoT devices.

6. REFERENCE LIST

[1] K. Zhou, Taigang Liu, and Lifeng Zhou, " Industry 4.0: Towards future industrial opportunities and challenges," in 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Zhangjiajie, China, Aug. 2015, pp. 2147–2152, doi: 10.1109/FSKD.2015.7382284.

[2] H. Xu, W. Yu, D. Griffith, and N. Golmie, " A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective," IEEE Access, vol. 6, pp. 78238–78259, 2018, doi: 10.1109/ACCESS.2018.2884906.

[3] A. Bhattacharjee, S. Badsha, and S. Sengupta, " Blockchain-based Secure and Reliable Manufacturing System," IEEE Green Computing and Communications (GreenCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), Rhodes, Greece, Nov. 2020, pp. 228–233. doi: 10.1109/iThings-GreenCom-CPSComSmartData-Cybermatics50389.2020.00052.

[4] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective," IEEE Access, vol. 6, pp. 78238–78259, 2018, doi: 10.1109/ACCESS.2018.2884906.

[5] M. Suh, "Automated Cutting and Sewing for Industry 4.0 at ITMA 2019," p. 13, 2019.

[6] "Top 10 IoT Security Issues: Ransom, Botnet Attacks, Spying," Intellectsoft Blog, Jul. 30, 2020. https://www.intellectsoft.net/blog/biggest-iot-security-issues/ (accessed Mar. 07, 2021).

[7] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," Journal of Manufacturing Systems, vol. 47, pp. 93–106, Apr. 2018, doi: 10.1016/j.jmsy.2018.04.007.

[8] Mitsuo Harada, "Security management of factory automation," in SICE Annual Conference 2007, Takamatsu, Japan, Sep. 2007, pp. 2914–2917, doi: 10.1109/SICE.2007.4421488.

[9] M. Ehrlich, H. Trsek, L. Wisniewski, and J. Jasperneite, "Survey of Security Standards for an automated Industrie 4.0 compatible Manufacturing," in *IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society*, Lisbon, Portugal, Oct. 2019, pp. 2849–2854, doi: 10.1109/IECON.2019.8927559

[10] N. Tuptuk and S. Hailes, " Security of smart manufacturing systems," Journal of Manufacturing Systems, vol. 47, pp. 93–106, Apr. 2018, doi: 10.1016/j.jmsy.2018.04.007.

[11] M. Irshad, " A Systematic Review of Information Security Frameworks in the Internet of Things (IoT)," in 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, Australia, Dec. 2016, pp. 1270– 1275. doi: 10.1109/HPCC-SmartCity-DSS.2016.0180.

[12] "What Are the IoT Security Standards?," SDxCentral. https://www.sdxcentral.com/5g/iot/definitions/what-are-iot-security-standards/ (accessed Mar. 07, 2021)."Comparison of IoT Security Frameworks," Comparison of IoT Security Frameworks. https://www.eurofins-cybersecurity.com/news/comparison-iot-securityframeworks/ (accessed Mar. 07, 2021).

[13] "Comparison of IoT Security Frameworks," Comparison of IoT Security Frameworks. https://www.eurofins-cybersecurity.com/news/comparison-iot-securityframeworks/ (accessed Mar. 07, 2021).

[14] M. Ehrlich, H. Trsek, L. Wisniewski, and J. Jasperneite, “Survey of Security Standards for an automated Industrie 4.0 compatible Manufacturing,” in IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society, Lisbon, Portugal, Oct. 2019, pp. 2849–2854, doi: 10.1109/IECON.2019.8927559.

[15] K. Zhou, Taigang Liu, and Lifeng Zhou, “Industry 4.0: Towards future industrial opportunities and challenges,” in 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Zhangjiajie, China, Aug. 2015, pp. 2147–2152, doi: 10.1109/FSKD.2015.7382284.

[16] H. Xu, W. Yu, D. Griffith, and N. Golmie, “A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective,” IEEE Access, vol. 6, pp. 78238–78259, 2018, doi: 10.1109/ACCESS.2018.2884906.

[17] S. R. Chhetri, N. Rashid, S. Faezi, and M. A. Al Faruque, “Security trends and advances in manufacturing systems in the era of industry 4.0,” in 2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Irvine, CA, Nov. 2017, pp. 1039–1046, doi: 10.1109/ICCAD.2017.8203896.

[18] Kamble, S., Gunasekaran, A. and Gawankar, S., 2020. Sustainable Industry 4.0 Framework: A Systematic Literature Review Identifying The Current Trends And Future Perspectives.

[19] Lins, Theo & Rabelo, Ricardo & Correia, Luiz & Sá Silva, Jorge. (2018). Industry 4.0 Retrofitting. 8 -15. 10.1109/SBESC.2018.00011. [6]Moktadir, M., Ali, S., Kusi-Sarpong, S. and Shaikh, M., 2019. Assessing Challenges For Implementing Industry 4.0: Implications For Process Safety And Environmental Protection.

[20] Moktadir, M., Ali, S., Kusi-Sarpong, S. and Shaikh, M., 2019. Assessing Challenges For Implementing Industry 4.0: Implications For Process Safety And Environmental Protection.

7. APPENDICES

Appendix 1: Business Case

This chapter sets out the benefits and provides a business case for the information security management system (ISMS) that conforms to the ISO 27001:2013 standard and IEC 62443 standard.

1. Purpose

Main objective of the overall project is security implementation for the potential challenges of the smart manufacturing system. A secure automated garment manufacturing system which has been securely implemented to overcome the potential security challenges in the garment manufacturing industry according to the security and industrial standards which are verified for authentication and access monitoring for the utilized IoT devices, automated security configurations using Ansible, security updates using Ansible and intrusion detection system.

Identifying the components and devices and conducting risk assessment to identify current and future threats. Security policy creation for different components using security and industrial standards. Update Management using Ansibe. Python, Django, Bash technologies will be used for the update management configurations.

2. Scope

Create and develop security policies such as privacy policy, password policy, network policy, audit policy, authorization and access control, backup policy according to industrial guidelines and standards to design the secured automated system safely. Come up with procedures and methods to implement the identified security policies for the components including centralized security Management, intrusion detection, authentication and access control and update management.

3. Introduction

Novel changes in Industry 4.0 lead to a passion for manufacturing plants with productivity, customization features, flexibility, operational efficiency and SAM/SMV (Standard Allowed Minute/Standard Minute Value) rather than security. The integration of complex smart manufacturing technologies lead to increased intercommunication and data density, thus massively expand the scope of attacks pointing at industrial espionage and sabotage, because Industrial 4.0 are implemented targeting the functionality than security.

CPS are used to gain higher productivity in manufacturing, and to usher innovation due to their potential to integrate technology from different sectors for the implementation of real world processes. Manufacturing automation is becoming a part of critical infrastructure in the present and future context. CPS is designed and implemented to be easily extendable and scalable as the structure includes heterogeneous communication technologies, which leads to technical issues, such as system verifications, frequent software updates, network and data interoperability, synchronization, privacy, and security issues. The integration of IoT devices combined with various technologies is a complex task and implementing security for those systems is more complex task. Therefore, cyber security has evolved into a major concern.

Objective of this project is to design and implement an automated system for garment manufacturing system focusing on four major cyber security aspects for garment manufacturing systems including:

- Frameworks and standardization
- Centralized security configurations with update management
- Authentication and Physical Access Control
- Intrusion Detection System (IDS)

A comprehensive, cost effective and efficient security solution is proposed with a centralized security approach to overcome the potential challenges of the smart system.

4. ISMS benefits

4.1 Information security risk reduction

1. Educate employees with the concepts of cyber security, threats and cyber-attacks by security awareness programs and training the employees to operate systems securely according to policies.
2. Enhance established control environments for information security by (re)emphasizing the security control criteria of business information, updating existing security controls for information, monitoring etc. and offering incentives to evaluate information protection and enhancing regularly access controls when required.
3. A systematic, excellently-structured strategy improves a chance of recognizing, assessing and rationally managing all applicable security information risks, vulnerabilities and impacts.

4. It improves our ability to pass selectively those threats to insurers or other third parties and can make it easier to negotiate reduced rates when key controls are introduced and handled.
5. Trained, systematic and rational risk management strategy ensures consistency across various ICT and business processes throughout the time and handles information security threats regarding the relative objectives.
6. Prevents from fines, legal charges, financial losses and loss of reputation.

4.2 Benefits of standardization

1. Improves protection in system and information reliability.
2. Enhanced trust for consumers and business partners about the manufacturing smart system and the process.
3. Allows to focus on unique additional safety standards to protect those information assets.
4. Stop the same fundamental controls in every circumstance repeatedly.
5. It is widely applicable and thus interchangeable across various divisions, roles, business units and organizations.
6. Improves the company brand value and market shares with the help of world-class and well-respected safety standards.(ISO 27001:2013 combined with IEC 62443)

4.3 Benefits of structured approach

1. ISMS improves structure and focus. It helps to develop specific obligations in the field of information risk.
2. Increases ability to rebound and carry on business as normal.
3. Provides a logically coherent and fairly detailed framework for varying controls in information security.
4. Establishes a comprehensive collection of policies, protocols and standards for information security, customized to the smart system and officially accepted by the industry

4.4 Benefits of certification

1. Cyber-attacks are on the rise in the world, and our company and its credibility can have a huge impact. An ISMS accredited according to ISO 27001 helps secure the reputation.

2. It allows company to escape the expensive fines related to non-compliance with data security standards and the financial damages arising from data breaches.
3. Develop working partnerships, and attract current customers and employees.
4. It also offers us a proven marketing advantage over our competitors.
5. Increase competition, trust and guarantee on domestic and international markets.
6. Shows dedication to information security in the organization, at all levels.

4.5 Benefits of compliance

1. ISO 27001 certification is recognized internationally and proves successful compliance, eliminating the need for regular customer audits.
2. Generate a proactive position focused on information security.
3. Our organization is expected to comply with various data security, privacy and IT governance regulations, then ISO 27001 will implement the most efficient methodology to do so.

4.6 Executive summary - benefits

An ISMS is a collection of rules, protocols, processes and structures that handle the risks of information, such as cyber threats, hacking, data breaches or theft. Educate employees by security awareness programs, improves protection in organizational computer systems and information reliability, allows the company to focus on unique additional safety standards, provides a logically coherent and fairly detailed framework for varying controls in information security, helps secure our reputation as an organization, develop working partnerships, and attract current customers and employees, proves successful compliance, eliminating the need for regular customer audits are some of the top benefits for our organization to implement and deploy the ISO 27001 information security management framework.

5. ISMS costs

5.1 ISMS implementation project management costs

- Team members' wages working on the project.
- Hardware and software tools, materials, equipment and legal permits identification for the project.

- Identifying use of workspaces for the project.
- Tasks which facilitates projects completion in given time.
- Research, design and installation processes to complete the projects.
- Risk assessments and vulnerability assessments for the project.
- Assign, manage and track each project resources.
- Tracking progress updates of projects.
- Project plan implementation and integrating Internet of Things (IoT) components.
- Project data management influencing storage and servers.
- Overall change controls in project.
- Activity duration estimation and schedule controls for projects.
- Quality assurance and controls in project.
- Project information distribution.

5.2 Other ISMS implementation costs

Training and awareness for ISMS such as certification courses or tests for measuring the training's effectiveness would be necessary for system operators, developers and employees.

Developing and maintaining record details of inventory information assets such as asset type, location, backup information, license information, business value.

Assess information security risks by comparing risks against risk criteria and selecting controls.

Review and update information security policies through industry experts.

5.3 Certification costs

Certification audit cost - $35000 (includes Assess and select a suitable certification body + Pre-certification visits and certification audit/inspection by an accredited ISO/IEC 27001 certification body)

Risk of failing to achieve certification at first application - $3000 - $5000

Recertification audit cost - $35000

Takes 15 working days for certification audit.

5.4 Ongoing ISMS operation and maintenance costs

Internal audit cost (once a year after certificate acquisition or certificate renewal) - $20000

Surveillance audit cost - $20000

Refer:

https://www.pivotpointsecurity.com/blog/iso-27001-cost-estimate-48000-information-security-confidence-priceless/

https://ismsalliance.com/trends/iso-27001-certification-audit/audits-and-associated-costs-needed-to-gain-and-maintain-iso-27001-certification/

https://www.itgovernance.co.uk/iso27001-certification-costs

5.5 Executive summary - cost

The system's current policies and standards should be implemented according to the ISO 27001 standards for ISMS and IEC 62443 IoT security standard. Therefore, overall design and implementation of ISMS project will be costly, but we are trying to adopt security policies according to the standards as a customized framework. After Implementation certification would be acquired for ISO 2700. It will take $52000 per year to maintain the certification and standards and reacquire certificate after 3 years.

6. Conclusion

Assurance of information security utilizes frameworks based on specific standards such as ISO 270001:2013 and IEC 62443. We can fulfill their ultimate goals such as better management strategies, information security governance, compliance with laws and regulations, improving market share, competing with other successful organizations by justifying information security costs for information security management systems and illustrating the benefits of having best practices for information security management systems.

Appendix 2: Critical asset profile and Information asset risks for CNC machine

	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset *What is the critical information asset?*	**(2) Rationale for Selection** *Why is this information asset important to the organization?*	**(3) Description** *What is the agreed-upon description of this information asset?*
CNC(Computer Numerically Controlled) cutting machine	Important for the primary operational function to cut precise designs into sheet materials with minimal material wastage, reducing operating costs and improving efficiency.	High automation and efficiency, high precision CNC smart garment cutting machine. Help improve productivity by automating cutting application with better cost performance. Cutting speed varies to the one material to another. The interface is based on Linux operating system. CNC machine includes with secure sensor solutions. Automated cutting process is more accurate.
(4) Owner(s) *Who owns this information asset?*		
Third party organization		
(5) Security Requirements *What are the security requirements for this information asset?*		
❑ **Confidentiality**	Only authorized personnel can view this information asset, as follows:	**Operators of the machine and developers of the software**
❑ **Integrity**	Only authorized personnel can modify this information asset, as follows:	**Developers of the software**
❑ **Availability**	This asset must be available for these personnel to do their jobs, as follows:	Operators
	This asset must be available for __12___ hours, __7___ days/week, and __52___ weeks/year.	
❑ **Other**	This asset has special regulatory compliance protection requirements, as follows:	Safety requirements Quality assurance Maintenance
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		

❑ Confidentiality	❑ Integrity	❑ Availability	❑ Other

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk	Information Asset	CNC machine	
	Area of Concern	*Automated CNC machines can be left unattended*	
	Threat — (1) Actor *Who would exploit the area of concern or threat?*	insider	
	Threat — (2) Means *How would the actor do it? What would they do?*	Physically or network	
	Threat — (3) Motive *What is the actor's reason for doing it?*	accidental	
	Threat — (4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**	
	Threat — (5) Security Requirements *How would the information asset's security requirements be breached?*	disclosed to unauthorized individuals and lose of integrity	
	Threat — (6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium** ❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
	Reputation & Customer Confidence	8	4
	Financial	2	1
	Productivity	2	1
	Safety & Health	-	-
	Fines & Legal Penalties	2	1
	User Defined Impact Area	-	-
		Relative Risk Score	**7**

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET		
Information Asset Risk — Threat	Information Asset	CNC machine	
	Area of Concern	*power failure*	
	(1) Actor *Who would exploit the area of concern or threat?*	Natural	
	(2) Means *How would the actor do it? What would they do?*	Physical (Power loss to the CNC machine)	
	(3) Motive *What is the actor's reason for doing it?*	Accidental	
	(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**	
	(5) Security Requirements *How would the information asset's security requirements be breached?*	Loss of availability	
	(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium** ❑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
	Reputation & Customer Confidence	6	1.5
	Financial	2	0.5
	Productivity	8	2
	Safety & Health	-	-
	Fines & Legal Penalties	--	-
	User Defined Impact Area	-	-
	Relative Risk Score		**4**

Allegro - Worksheet 10	Information Asset Risk Worksheet

Information Asset Risk

Threat

Information Asset	CNC machine
Area of Concern	*Natural disaster*
(1) Actor *Who would exploit the area of concern or threat?*	Natural
(2) Means *How would the actor do it? What would they do?*	Physical
(3) Motive *What is the actor's reason for doing it?*	Accidental
(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**
(5) Security Requirements *How would the information asset's security requirements be breached?*	Loss of availability
(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** ❑ **Medium** ❑ **Low**

(7) Consequences

What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?

(8) Severity

How severe are these consequences to the organization or asset owner by impact area?

Impact Area	Value	Score
Reputation & Customer Confidence	4	1
Financial	8	2
Productivity	8	2
Safety & Health	-	-
Fines & Legal Penalties	-	-
User Defined Impact Area	-	-

Relative Risk Score **5**

Allegro - Worksheet 10	Information Asset Risk Worksheet

Information Asset Risk

Threat

Information Asset	CNC machine
Area of Concern	*Overheat*
(1) Actor *Who would exploit the area of concern or threat?*	Natural
(2) Means *How would the actor do it? What would they do?*	Physically (overheated because of room temperature or workload)
(3) Motive *What is the actor's reason for doing it?*	Accidental
(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**
(5) Security Requirements *How would the information asset's security requirements be breached?*	Loss of availability
(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** ❑ **Medium** ❑ **Low**

(7) Consequences

What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?

(8) Severity

How severe are these consequences to the organization or asset owner by impact area?

Impact Area	Value	Score
Reputation & Customer Confidence	6	1.5
Financial	2	0.5
Productivity	8	2
Safety & Health	2	0.5
Fines & Legal Penalties	-	--
User Defined Impact Area	-	-

Relative Risk Score **4.5**

Allegro - Worksheet 10	Information Asset Risk Worksheet

Information Asset Risk

Threat

Information Asset	CNC machine
Area of Concern	*Hardware failure*
(1) Actor *Who would exploit the area of concern or threat?*	Natural
(2) Means *How would the actor do it? What would they do?*	Physical
(3) Motive *What is the actor's reason for doing it?*	Accidental
(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**
(5) Security Requirements *How would the information asset's security requirements be breached?*	Loss of availability
(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** ❑ **Medium** ❑ **Low**

(7) Consequences

What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?

(8) Severity

How severe are these consequences to the organization or asset owner by impact area?

Impact Area	Value	Score
Reputation & Customer Confidence	6	3
Financial	8	4
Productivity	8	4
Safety & Health	-	-
Fines & Legal Penalties	2	1
User Defined Impact Area	-	-

Relative Risk Score **12**

Allegro - Worksheet 10	Information Asset Risk Worksheet

Information Asset Risk

Threat

Information Asset	CNC machine
Area of Concern	*Unauthorized access through network*
(1) Actor *Who would exploit the area of concern or threat?*	insiders and outsiders
(2) Means *How would the actor do it? What would they do?*	Network (The actor gets, modify or remove data)
(3) Motive *What is the actor's reason for doing it?*	deliberate
(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**
(5) Security Requirements *How would the information asset's security requirements be breached?*	disclosed to unauthorized individuals and lose of integrity
(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** ❑ **Medium** ❑ **Low**

(7) Consequences

What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?

(8) Severity

How severe are the consequences to the organization or asset owner by impact area?

Impact Area	Value	Score
Reputation & Customer Confidence	8	4
Financial	4	2
Productivity	4	2
Safety & Health	-	-
Fines & Legal Penalties	2	1
User Defined Impact Area	-	-

Relative Risk Score **9**

Allegro - Worksheet 10	Information Asset Risk Worksheet

Information Asset Risk

Threat

Information Asset	CNC machine		
Area of Concern	*Unauthorized connected devices*		
(1) Actor *Who would exploit the area of concern or threat?*	Insider		
(2) Means *How would the actor do it? What would they do?*	Network or Physical (connected to the open ports of the CNC machine)		
(3) Motive *What is the actor's reason for doing it?*	Deliberate		
(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure**	❑ **Destruction**	
	❑ **Modification**	❑ **Interruption**	
(5) Security Requirements *How would the information asset's security requirements be breached?*	disclosed to unauthorized individuals and lose of integrity		
(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium**	❑ **Low**

(7) Consequences

What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?

(8) Severity

How severe are these consequences to the organization or asset owner by impact area?

Impact Area	Value	Score
Reputation & Customer Confidence	6	3
Financial	6	3
Productivity	6	3
Safety & Health	-	-
Fines & Legal Penalties	2	1
User Defined Impact Area	-	-

Relative Risk Score **10**

Allegro - Worksheet 10	Information Asset Risk Worksheet

Information Asset Risk

Threat

Information Asset	CNC machine
Area of Concern	*Malware*
(1) Actor *Who would exploit the area of concern or threat?*	Insider or outsider
(2) Means *How would the actor do it? What would they do?*	Network or physical
(3) Motive *What is the actor's reason for doing it?*	Deliberate
(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Destruction** ❑ **Modification** ❑ **Interruption**
(5) Security Requirements *How would the information asset's security requirements be breached?*	Loss of data or availability
(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High** ❑ **Medium** ❑ **Low**

(7) Consequences

What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?

(8) Severity

How severe are these consequences to the organization or asset owner by impact area?

Impact Area	Value	Score
Reputation & Customer Confidence	6	3
Financial	5	2.5
Productivity	8	4
Safety & Health	-	-
Fines & Legal Penalties	2	1
User Defined Impact Area	-	-

Relative Risk Score 10.5

Allegro - Worksheet 10	Information Asset Risk Worksheet

Information Asset Risk

Threat

Information Asset				
Area of Concern				
(1) Actor *Who would exploit the area of concern or threat?*				
(2) Means *How would the actor do it? What would they do?*				
(3) Motive *What is the actor's reason for doing it?*				
(4) Outcome *What would be the resulting effect on the information asset?*	❑ **Disclosure** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**		
(5) Security Requirements *How would the information asset's security requirements be breached?*				
(6) Probability *What is the likelihood that this threat scenario could occur?*	❑ **High**	❑ **Medium**	❑ **Low**	

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
	Reputation & Customer Confidence		
	Financial		
	Productivity		
	Safety & Health		
	Fines & Legal Penalties		
	User Defined Impact Area		
		Relative Risk Score	

Appendix 3: Standard evaluation document

Identification of potential cyber security standards, procedures, guidelines and frameworks for the cyber security automation of industrial 4.0 garment manufacturing system

ABSTRACT

Cyber security standards are techniques that are commonly set out in published materials that are intended to protect a user's or organization's cyber environment. Users, networks, computers, software, processes, information in storage or transit, applications, facilities, and systems that can be linked directly or indirectly are all part of this area to be protected. ISO 27001 for information security management systems, IEC 62443 which defines processes, techniques and requirements for Industrial Automation and Control Systems, NIST framework and ISO/IEC 30163:2021 standard which specifies the system requirements of an Internet of Things (IoT)/Sensor Network (SN) technology-based platform for chattel asset are some of the standards that could be used for the research. The Software Development Life Cycle (SDLC) is a well-defined approach for producing high-quality, low-cost software in the shortest possible amount of time framework. This document provides a brief overview of standards and frameworks that could be used in the research project about cyber security automation of industrial 4.0 garment manufacturing system.

1. INTRODUCTION

Written norms are expected to render cyber security initiatives clear. These requirements are referred to as cyber security standards, and they are generic collections of prescriptions for the best implementation of specific steps, created by industry experts. Methods, protocols, reference structures, and other items may be included in the specifications. It ensures security reliability, promotes integration and interoperability, and allows for practical measure comparison. A written specification that defines a common language, includes a technical specification or other precise requirements, and is intended to be used consistently, as a law, a guideline, or a description. The aim of security standards is to make information technology (IT) systems, networks, and essential infrastructures more secure.

2. EVALUATION

2.1 ISO 27000 Series

It is the family of information security standards which is developed by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) to provide a globally recognized framework for best information security management practices. It helps the organization to keep their information assets secure such as employee details, financial information, and intellectual property.

The need of ISO 27000 series arises because of the risk of cyber-attacks which the organizations face. The cyber-attacks are growing day by day making hackers a constant threat to any industry that uses technology. ISMS is a systemic approach to risk management, including measures to address people, processes and technology.

2.1.1 ISO 27001

This standard allows us to prove the clients and stakeholders of any organization to managing the best security of their confidential data and information. This standard involves a process-based approach for establishing, implementing, operating, monitoring, maintaining, and improving our ISMS. The only standard in the series that can be audited and certified against is ISO IEC 27001: 2013.

ISO 27001 based ISMS can demonstrate many efficiencies and other benefits such as;

• Improved system dependability and security:

Security is frequently characterized as safeguarding an asset's Confidentiality, Integrity, and Availability. The stated objectives will be satisfied if a standards-based strategy is used in a system or an organization, which ensures that proper controls, processes, and procedures are in place. By default, achieving the CIA's security goals will increase the dependability, availability, and accessibility of the system. Having stable, secure and reliable systems ensures that interruptions to those systems are minimized, thereby increasing their availability and productivity. In addition to the above, a standards based approach to information security demonstrates to customers that the company can be trusted with their business. This can increase profitability by retaining existing, and attracting new, customers.

• Reduced Costs:

Standards based approach to information security ensures that all controls are measured and managed in a structured manner. As a result, processes and procedures become more simplified and effective, minimizing expenses. Companies have realized they can better manage the tools they have in place by consolidating redundant systems or re-assigning other systems from assets with low risk to those with higher risk.

• Legislation compliance:

Having a well-structured Information Security Management System in place makes compliance considerably easier.

• Better Management:

Knowing what's in place and how it should be managed and safeguarded makes it easier to manage information resources inside a company.

• Improved Customer and Partner Relationships:

Customers and trading partners can interact with the company with confidence knowing that the company has taken an independently verifiable approach to information security risk management.

• ISO 27001 can be adopted as a framework for an organization to work against, or the organization can seek certification against the standard. An organization's certification to ISO/IEC 27001 shows that it has designed and implemented best-practice information security processes. Certification will be benefited when gaining new clients and improve competitiveness, enhancing reputation, improve structure and focus.

2.2 IEC 62443

The IEC 62443 cyber security standard defines processes, techniques and requirements for Industrial Automation and Control Systems (IACS). Its documents are the result of the IEC

standards creation process where all national committees involved agree upon a common standard.

Targets at three main roles:

- Product suppliers that develop, distribute and maintain components or systems used in automated solutions.
- System integrators that design, deploy and commission the automated solution.
- Asset owners that operate, maintain and decommission the automated solution.

Planned and published IEC 62443 work products for IACS Security.

All IEC 62443 standards and technical reports are organized into four general categories called *General, Policies and Procedures, System* and *Component*.

1. The first category includes foundational information such as concepts, models and terminology.
2. The second category of work products targets the Asset Owner. These address various aspects of creating and maintaining an effective IACS security program.
3. The third category includes work products that describe system design guidance and requirements for the secure integration of control systems. Core in this is the zone and conduit design model.
4. The fourth category includes work products that describe the specific product development and technical requirements of control system products.

2.2.1 General

Part 1 covers topics that are common to the entire series:

- 1-1 (TS): Terminology, concepts and models

2.2.2 Policies and procedures

Part 2 focuses on methods and processes associated with IACS security:

- 2-1: Establishing an IACS security program
- 2-3 (TR): Patch management in the IACS environment
- 2-4: Security program requirements for IACS service providers

2.2.3 System

Part 3 is about requirements at the system level:

- 3-1: Security technologies for IACS
- 3-2: Security risk assessment for system design
- 3-3: System security requirements and security levels

2.2.4 Components and requirements

Part 4 provides detailed requirements for IACS products:

- 4-1: Secure product development lifecycle requirements
- 4-2: Technical security requirements for IACS components

The elements of the 62443 series are shown in Figure 1.

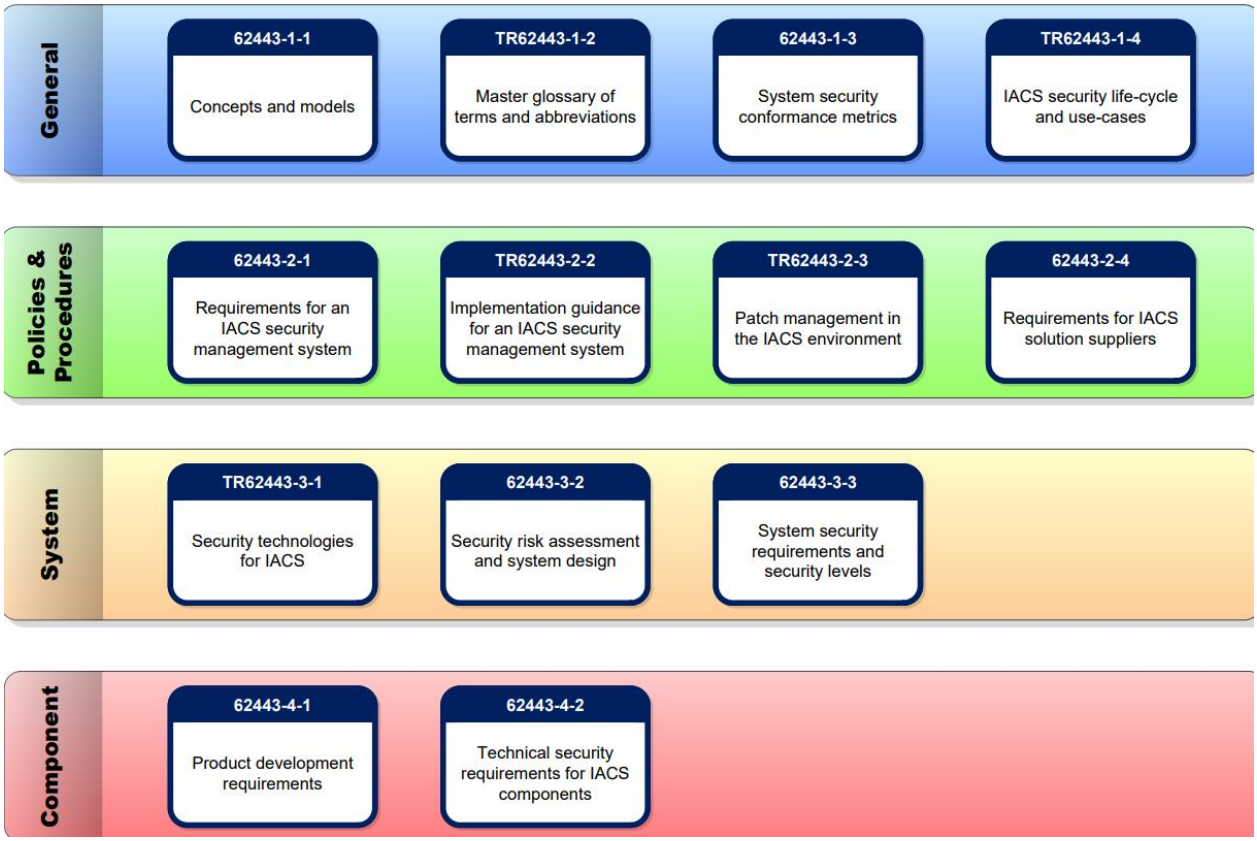


Figure 1 – 62443 Elements.

Focused area:

Part 2-1: Establishing an industrial automation and control system security program. This section of the standard is aimed at operators of automation solutions and defines requirements for how security during the operation of plants is to be considered.

Part 4-1: Secure product development lifecycle requirements. Section 4-1 of IEC 62443 defines how a secure product development process should look like. It is divided into eight areas: management of development, definition of security requirements, design of security solutions, secure development, testing of security features, handling of security vulnerabilities, creation and publication of updates and documentation of security features.

Part 4-2: Technical security requirements for IACS component

Cyber security technical requirements for components that make up an IACS, specifically the embedded devices, network components, host components, and software applications. The standard, which is based on the IACS system security requirements of ISA/IEC 62443-3-3, System Security Requirements and Security Levels, specifies security capabilities that enable a component to mitigate threats for a given security level without the assistance of compensating countermeasures.

2.3 ISO/IEC 30163:2021 IoT standard

This standard specifies the system requirements of an Internet of Things (IoT)/Sensor Network (SN) technology-based platform for chattel asset monitoring supporting financial services, including: - System infrastructure that describes functional components; - System and functional requirements during the entire chattel asset management process, including chattel assets in transition, in/out of warehouse, storage, mortgage, etc.; - Performance requirements and performance specifications of each functional component; - Interface definition of the integrated platform system. This document is applicable to the design and development of IoT/SN system for chattel asset monitoring supporting financial services.

One of the most difficult challenges in the IoT evolution is standardization. Without global standards, the complication of machines that need to connect and interact with one another (along with automation, service quality, data repository, and so on) would skyrocket. The Internet of Things promises lots of interconnected devices, which would necessitate universal standards in order to function at a degree of complexity that is appropriate, scalable, and manageable.

In a world dominated by smart devices, security is very important. This is why IoT standardization is necessary. Many have proposed that a common model for the Internet of Things could help us solve some of the industry's current problems. Laws and limitations can aid in defining the scope of data protection and determining when and how data can be purchased or exchanged. It can also help to dispel any misunderstandings about collection of data and information manipulation.

It is possible to monitor the flow of data and prevent it from reaching the hands of the wrong people by controlling the IoT industry. As a result, standardization of the IoT industry is essential for ensuring that we can continue to benefit from IoT.

IoT devices would not be a simple task to standardize. The procedure, along with the enforcement of the regulations, will be hampered by challenges and obstacles. Despite the fact that there is no single body involved in developing IoT standards, significant attempts are being taken at the national and international levels, as well as at the government and organizational levels. Many domestic and multinational corporations have established alliances to agree on shared IoT standards and technologies.

2.4 NIST Cyber Security Framework

To assist firms in managing their cyber security risks, the Framework incorporates industry standards and best practices. It establishes a common vocabulary that enables employees at all levels of a company—and at all points in the supply chain—to acquire a shared awareness of their cyber security threats. The Framework not only helps organizations understand their cyber security risks. Improve the security of the essential infrastructure, shielding it from both internal and external threats. NIST CSF describes five functions that manage the risks to data and information security which are identify, protect, detect, respond, and recover. The primary components consist of the Core, Profiles, and Implementation Tiers. The Core offers guidance to organizations wanting to get better protection for their information systems.

3. Conclusion

Among the standards discussed above the most relevant standards to our project ISO 27001 standard and IEC 62443 standard is the most suitable as both covers information security requirement as well as IoT automation life cycle requirements.

Appendix 4: Password Policy and audit policy (Examples for created policies)

Password Policy

1. Policy Statement

When restricting access, the systems should be safeguarded with passwords that are difficult to guess or derive. The importance of passwords in computer security cannot be underestimated. They serve as the first line of defense for systems. The entire system could be hacked if the password system is not strong. Therefore, secure password policy should be implemented in accordance with the guidelines indicated below. Password management systems must be interactive and ensure that passwords are of high quality.

2. Purpose

Ensure that security practices are introduced, implemented and maintained by all employees with respect to password-protected information infrastructure according to the standards ISO 27001:2013 and IEC 62443.

3. Scope

3.1 Applicability

The policy is applicable to the smart manufacturing system

3.2 Documentation

The documentation shall consist of Password Policy and related guidelines.

3.3 Document Control

The Password Policy document and all other referenced documents shall be controlled.

3.4 Records

Records being generated as part of the Password Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.

3.5 Distributions and Maintenance

The Password Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned.

4. Privacy

The Password Policy document is to be treated as "confidential" and only given to those who need it with suitable access control. This document's further changes and revisions will be monitored

5. Responsibility

The password policy shall be implemented by administrator accordingly.

Users should:

- Recognize their obligations for password security
- Use data in accordance with job function and business policy
- Recognize the ramifications of failing to follow the laws and policies governing information resources.
- Notify right away if the password has been hacked.

6. Policy

6.1 General

a. Password policy shall ensure that all user accounts are protected by strong passwords and that the strength of the passwords meets the security requirements of the system.

b. The concept of aging shall be used for passwords. Passwords on their expiry shall cease to function.

c. Users shall be educated about password protection and the password policy shall be implemented to ensure that users follow best practices for password protection.

d. IT systems shall be configured to prevent password reuse. For critical information systems, account lockout strategy shall be defined. This shall be based on a risk analysis of the system as well as the costs to be incurred in case such a strategy is implemented.

e. The password management system:

- Allow users to select and change their own passwords and include a confirmation procedure to allow for input errors.
- Force users to change their passwords at the first log-on.
- Enforce regular password changes and as needed.
- Maintain a record of previously used passwords and prevent re-use.
- Not display passwords on the screen when being entered.
- Store password files separately from application system data.
- Store and transmit passwords in protected form.

f. Passwords must not be shared, used, or divulged to anyone else and no generic or group passwords are allowed.

g. Passwords should be memorized by the user. They should be not written on paper or electronic media.

6.2 Access Authorization Requirements

• Access to the system shall be based on an approval.

• Individuals shall be granted access only to those information systems necessary for the performance of their official duties with approval. This requirement includes contracted employees and who have been granted access.

• Lock-out feature shall suspend accounts after three invalid attempts to log on, manual action by a security system administrator is required to reactivate the ID.

6.3 Password Parameters

All user passwords of the system and account passwords, should meet the following characteristics:

- Minimum password length is eight characters
- Complexity is four, consisting at least one upper key, at least one digit, at least one symbol and at least one lower key.
- Password history shall be five passwords.

- Maximum attempts before account lock is three.
- Password has used will be sha512
- Maximum password age will be sixty days
- Minimum age before password change will be one day.

Passwords should not be:

- Dictionary words
- Portions of associated account names (e.g., user ID, log-in name)
- Character strings (e.g., ABC or 123)

6.4 Password and Account Security

- Password accounts not used for 90 days will be disabled and reviewed for possible deletion. Accounts disabled for 60 days will be deleted.
- Accounts for contractors shall terminate on the expiration date of their contract.
- The auto-lock policy for locked accounts must be released after 24 hours only
- Users should immediately change their password if they suspect it has been compromised.
- Passwords may not be embedded in automated programs, utilities, or applications, such as autoexec.bat files, batch job files, terminal hotkeys.
- Passwords may be not visible on a screen, hardcopy printouts, or any other output device

7. Enforcement

Unauthorized personnel is not allowed to see or obtain sensitive data. Any employee found to have violated this policy may be subjected to disciplinary action.

Information Systems Audit Policy

1. Policy Statement

Audit controls and adequate security precautions are to prevent, control, and eliminate risks that can negatively impact the system and expose sensitive data. The policy confirms that the Information system is effectively implemented and maintained.

2. Purpose

The goal of this policy is to ensure that security configuration management system is configured in accordance with the security standards ISO 27001 and IEC 62443 as well as the best practices. The policy is also to confirm internal audits at planned intervals to provide information on whether the information security management system, conforms to requirements for its information security management system. Servers and other configuration devices must be audited four times a year and in accordance with appropriate regulatory compliance to ensure the integrity, confidentiality, and availability of information and resources. It also reduce risks of information systems, the data it manages, and the users it services.

3. Scope

3.1 Applicability

The policy is applicable to the smart manufacturing system and applies to all involved in the creation, deployment, operations, or support of the system.

3.2 Documentation

The documentation shall consist of information systems audit Policy and related guidelines.

3.3 Document Control

The information systems audit Policy document and all other referenced documents shall be controlled.

3.4 Records

Records being generated as part of the information systems audit Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators.

3.5 Distributions and Maintenance

The information systems audit Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned.

4. Privacy

The policy hereby provides its consent to allow internal Audits to access its servers and resources to the extent necessary to allow perform scheduled and ad hoc audits of all servers of the system. Components shall protect audit information, audit logs, and audit tools (if present) from unauthorized access, modification and deletion.

4.1 Specific Concerns

Smart system support critical business functions and store sensitive information. Improper configuration of servers could lead to the loss of confidentiality, availability or integrity of the system.

5. Responsibility

The audit configurations shall be implemented and maintained by the system administrator accordingly. The responsibility of the audit configurations and the audit policy is handled by system administrator. The auditing will be done internally by the auditors and a third party will conduct necessary evaluations.

6. Policy

6.1 General

a) Plan, execute, and maintain audit programs, including frequency, methodology, responsibilities, planning requirements, and reporting. The audit programs must take into account the importance of the processes in question as well as the findings of prior audits.

b) For each audit the identification of the audit criteria, requirements and scope should be done. Audit scope can be included with security vulnerabilities, risk evaluation, automated assessment tools, procedures and controls and penetration testing if necessary.

c) Choose auditors and conduct audits in a way that ensures the audit process' objectivity.

d) Ensure that the audit results are communicated to the appropriate entities.

e) Keep documentation of the audit results as evidence.

f) Feedback on the information security performance including audit results should be taken.

6.2 Audit procedures

3.2 Requirements

When deploying server systems, approved and standard configuration templates must be utilized including:

- All system logs are handled through a central system.
- All administrator actions must be logged.
- A central patch deployment system is used.
- Antivirus must be installed and updated in each client.
- Network scan to ensure only necessary network ports and network shares are in use.
- Verify administrative group membership.

Generating audit records relevant to:

- Access control
- Request errors
- Control system events
- Backup and restore events
- Configuration changes
- Audi log events

Audit records shall include:

- Timestamps

- Source originated
- Category
- Type
- Event ID
- Event result

Audit backups will be restored once a month or backup log files according to capacity. Allocating audit record storage capacity with log management with warnings when audit record storage capacity threshold reached.

Audit processing failures for software errors are logged.

Time synchronization mechanism for protection of time stamp integrity shall be provided to detect unauthorized alterations.

6. Enforcement

Staff members found in policy violation may be subject to disciplinary action or termination.

Appendix 5: Update management security configurations

Update Management Configurations

1. Update Management

1.1. Importance of local repositories

- System administrators have to install software, security updates and fixes often in all systems which consumes internet bandwidth.
- Rather than downloading and installing apps from the Ubuntu repository often on all systems, it is a smart option to save all applications on a local server on LAN and distribute them to other Ubuntu systems as needed.
- Using a local repository is a very quick and efficient method, as all essential apps are transferred over a fast LAN connection from local server.
- Setting up a local apt repository server will minimize the bandwidth required if there are multiple instances of Ubuntu to update which will reduce the cost of internet.

1.2. Set up local APT repository server on Ubuntu.

Reason - To minimize the bandwidth require, if having multiple instances to updates. Accessible to all local clients and update all system over LAN from local repository.

Setup a central local repository in the server, so that the clients can install, update and upgrade the packages from the central repository without using internet.

Login to Ubuntu as root and update the system

>apt-get update && apt-get upgrade

Install essential packages to set up the local repository

>apt-get install build-essential

Create a local Apache Web Server to server all packages to the clients.

>sudo apt-get install apache2

>sudo systemctl enable apache2

Test whether Apache is working

>http://10.0.2.15

Create A directory to store all packages - Create a folder called packages in the apache root document folder. (/var/www/html/)

>mkdir /var/www/html/packages

Create additional directories under /var/www/html/packages/ to save packages depending upon system's architecture.

>mkdir /var/www/html/packages/amd64

Copying all DEB files from installation media

>mount /dev/cdrom /media/cdrom

>find /media/cdrom/pool/ -name "*.deb" -exec cp {} /var/www/html/packages/amd64 \;

>umount /media/cdrom

Mount all remaining CD/DVD one by one and copy the .deb files

>http://10.0.2.15/packages/amd64/

Create Catalog file for APT use in directory i.e /var/www/html/packages/amd64/

Run the below command so that Synaptic Manager or APT will fetch the packages from local repository. Otherwise the packages in the local repository will not be shown in Synaptic and APT.

This command will scan all deb files and create the local repository in the Debian server.

>dpkg-scanpackages . /dev/null | gzip -9c > Packages.gz

Note- Whenever adding a new deb file in this repository, the above command should be run to create catalog file.

A catalog is a directory of information about data sets, files, or a database . A catalog usually describes where a data set, file or database entity is located and may also include other information, such as the type of device on which each data set or file is stored.

Configure Server sources list

After creating the catalog file, Open /etc/apt/sources.list file in the server(local) system.

>vi /etc/apt/sources.list

1.3 Testing

1.3.1. On server configurations

$ sudo apt-get install dpkg-dev apache2 dpkg-sig

$ sudo systemctl enable apache2

$ sudo systemctl start apache2

$ sudo mkdir /var/www/html/packages/

$ sudo mkdir /var/www/html/packages/amd64

$ sudo mkdir /var/www/html/packages/i386

$ sudo find /deb-location -name "*_amd64.deb" -exec cp {} /var/www/html/packages/amd64 \;

$ sudo find /deb-location -name "*_i386.deb" -exec cp {} /var/www/html/packages/i386 \;

$ sudo find /deb-location -name "*_all.deb" -exec cp {} /var/www/html/packages/i386 \;

$ sudo find /deb-location -name "*_all.deb" -exec cp {} /var/www/html/packages/amd64 \;

$ cd /var/www/html/packages/amd64/

$ sudo dpkg-scanpackages . /dev/null | gzip -9c > Packages.gz

$ sudo dpkg-scanpackages . /dev/null > Release

$ cd /var/www/html/packages/i386/

$ sudo dpkg-scanpackages . /dev/null | gzip -9c > Packages.gz

$ sudo dpkg-scanpackages . /dev/null > Release

1.3.2. Configurations on client devices

$ sudo nano /etc/apt/source.list

Add following line if system is 64bit

deb [trusted=yes] http://server-ip/packages/amd64/ /

Add following line if system is 32bit

deb [trusted=yes] http://server-ip/packages/i386/ /

$ sudo apt-get update

Appendix 6: Gantt Chart

#	Task Name	Duration	Start	ETA
Complete project execution		40 weeks	10-01-21	01-11-21
1	Online project Registration	1 week	10-01-21	17-01-21
2	Topic Assessment Form submission	1 week	18-01-21	22-01-21
3	Project Charter submission	1 week	08-02-21	12-02-21
4	Proposal report draft submission	2 weeks	15-02-21	26-02-21
5	Proposal presentation	1 weeks	28-02-21	08-03-21
6	Proposal report	2 weeks	08-03-21	21-03-21
7	Security standards and policy development	28 weeks	22-03-21	18-10-21
7.1	Identify the connected devices	2 weeks	22-03-21	05-04-21
7.2	Conduct a risk assessment	3 weeks	05-04-21	26-04-21
7.3	Identify the specific standards, procedures and guidelines	2 weeks	26-04-21	10-05-21
7.4	Choose and verify suitable standards	2 weeks	10-05-21	24-05-21
7.5	Policy creation	7 weeks	24-05-21	12-07-21
7.6	Verify policy creation	2 weeks	12-07-21	26-07-21
7.7	Implement policies for the components	10 weeks	26-07-21	18-10-21