

# **CYBERSECURITY AUTOMATION FOR AN INDUSTRY 4.0 GARMENT MANUFACTURING SYSTEM**

Project Id: 2021-11

Project Proposal Report

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

March 2021

# **CYBERSECURITY AUTOMATION FOR AN INDUSTRY 4.0 GARMENT MANUFACTURING SYSTEM**

2021-11

Project Proposal Report

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

Department of Computer Systems Engineering


Sri Lanka Institute of Information Technology

Sri Lanka

March 2021

## DECLARATION

We 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.

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

The supervisor/s should certify the proposal report with the following declaration.

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**

Industrial Internet of Things (IIoT) or smart manufacturing are other terms for Industry 4.0 which integrate smart computing as well as network technologies in automation and data transmission according to the ongoing trend of manufacturing and industrial practices, including Cyber Physical Systems(CPS), Cyber Physical Product Systems(CPPS), Internet of Things (IoT), robotics to create more extensive, better connected and productive systems. Smart manufacturing relies on the Internet of Things (IoT) to create a link between the digital and physical worlds, as well as data analytics and machine learning. Although these technologies have been in development for some time, integrating them with industrial systems introduces new challenges as well as potential advantages such as increased efficiency.

The integration of sophisticated smart manufacturing technologies vastly expands the scope of industrial espionage and sabotage attacks because industrial 4.0 manufacturing systems are driven by focusing on the development of functionality rather than security. Therefore, the volume and sophistication of cyber threats in industrial automation systems are growing due to poor security design and cyber security requirements are not been captured. The development of the secure environment for the smart systems using The CPPS platform is a large project that is currently hampered by a number of issues like, collaborating between different systems, centralized security Management, secure communication and insecure data leading to, conflicts in design model and security model, additional cost, low product quality, violation of Confidentiality, Integrity and Availability (CIA) and difficulties in adhering to laws and regulations. Therefore, designing and automating a Computer Numerical Control cutting machine into the direction of industry 4.0 which adapts with security standards to illustrate the cyber security gap and discuss solutions to apply in the apparel industry while comparing and contrasting with current security aspects in the current industrial 4.0 automated systems in the industry is the objective of the research.

Key words – Industrial Internet of Things, Cyber Physical Systems, Cyber Physical Product Systems, Computer Numerical Control

## TABLE OF CONTENTS

<b>DECLARATION.....</b>	<b>3</b>
<b>ABSTRACT.....</b>	<b>4</b>
<b>LIST OF FIGURES .....</b>	<b>7</b>
<b>LIST OF TABLES .....</b>	<b>7</b>
<b>1.INTRODUCTION.....</b>	<b>8</b>
1.1 Background Review .....	8
1.2 Literature Review .....	13
1.3 Research Gap.....	16
1.4 Research Problem.....	17
1.4.1. Collaboration between different systems .....	17
1.4.2. Centralized security management .....	17
1.4.3. Secure communication.....	17
1.4.4. Insecure data .....	18
1.4.5. Initial cost.....	18
1.4.6. Lack of strategy to industry 4.0 .....	18
<b>2.OBJECTIVES .....</b>	<b>19</b>
2.1 Main Objectives .....	19
2.2 Sub Objectives.....	19
<b>3.METHODOLOGY.....</b>	<b>20</b>
3.1 System Diagram .....	20
3.2 Individual components .....	20
3.2.1. Security standards and policy development.....	20

3.2.1.1 Identify the connected devices .....	21
3.2.1.2 Conduct a risk assessment .....	21
3.2.1.3 Identify the specific standards, procedures and guidelines .....	22
3.2.1.4 Choose the most suitable standards and frameworks .....	23
3.2.1.5 Verify the chosen standards and frameworks .....	23
3.2.1.6 Determine the types of policies that are needed .....	23
3.2.1.7 Verify policy creation .....	23
3.2.1.8 Implement policies for the components .....	23
3.2.2 Update Management .....	24
3.2.2.1 Setup local repositories .....	25
3.2.2.2 Configure package manager .....	25
3.2.2.3 Configure Iot devices to access previously setup local repository .....	25
3.2.2.4 Test local repositories .....	25
3.2.2.5 Verify update .....	25
3.2.2.6 Mechanisms for roll back .....	25
3.3 Requirements .....	26
3.4 Gantt Chart .....	27
<b>4.DESCRPTION OF PERSONAL AND FACILITIES .....</b>	<b>28</b>
<b>5.BUDGET AND BUDGET JUSTIFICATION .....</b>	<b>29</b>
<b>REFERENCE LIST .....</b>	<b>30</b>

## **LIST OF FIGURES**

Figure 1.1: Industrial revolution	09
Figure 3.1: Overall System Diagram	20
Figure 3.2: Individual Workflow Diagram- Security standards and policy development	21
Figure 3.3: Individual Workflow Diagram- Security Updates	24
Figure 3.4: Gantt Chart	23

## **LIST OF TABLES**

Table 1.1: Comparison of industrial standards and guidelines	15
Table 1.2: Summary of best practices for industrial security	15
Table 4.1: Description of Personal and Facilities	28
Table 5.1: Budget and Budget Justification	29

## **LIST OF ABBREVIATIONS**

<b>Abbreviation</b>	<b>Description</b>
CNC	Computer Numerical Control
CPPS	Cyber Physical Product Systems
CPS	Cyber Physical Systems
DoS	Denial of Service
IIoT	Industrial Internet of Things
IoT	Internet of Things
MitM	Man in the Middle

# **1. INTRODUCTION**

## **1.1 Background Review**

The first industrial revolution commenced with the discovery of steam power which was the greatest breakthrough for human productivity. Invention such as spinning machine, looms to make fabric made appearance. The first mechanical sewing machine was invented marking the beginning of the textile industry. As the first industry revolution was driven by coal, water and steam the second revolved around electricity. Gas and oil. The impact of the revolution in apparel sector is the sewing machine began to be produced in a serial manner. Third industrial revolution also known as digital revolution began with partial automation through Programmable Management Systems. 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 the virtual environment and cyber physical systems are connected, communicated with one another and with human in real time to ultimately make decisions without human involvement, aiming to develop new internet services and business models providing efficiency, transparency, fault detection, flexibility, monitoring and most importantly productivity while reducing costs. The use of IoT in industrial applications and the technological convergence of Cyber Physical Systems will have value creation and business models, modular structures which adopt to rapidly changing requirements. Industry 4.0 garment manufacturing systems are based on IoT and other technologies and used to build a bridge between the digital and physical worlds. Cyber Physical Systems, wireless sensor networks, Machine Learning, Data analytics, augmented reality, cloud computing, 3D printing, system integration, cyber security are such technologies.



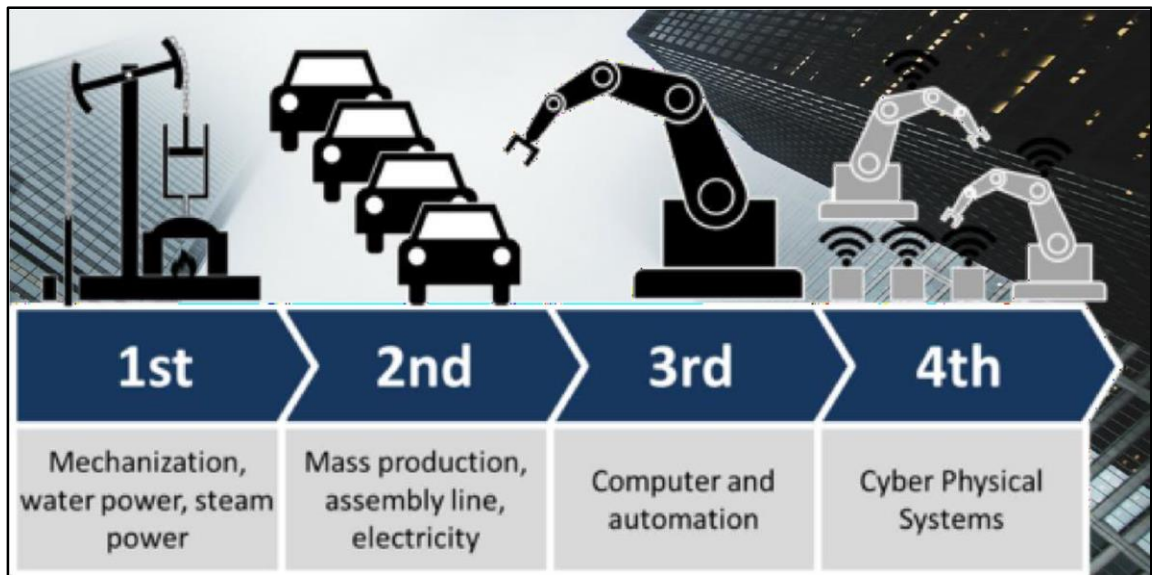


Figure 1.1: Industrial revolution image

Development of IIoT to the integration of smart computing and networking in manufacturing processes for automation is the vision of industry 4.0. IoT adopts enabling the interconnection of computers and computer related equipment to improve intelligence, profitability, and effectiveness as well as safety[10]. While IoT refers to system of interrelated computing devices which communicating with each other and with people in real time it is most commonly used for consumer usage, IIoT is used for industrial purpose such as manufacturing. Unlike IOT, IIoT has more distinctive types incorporated smart devices, networking techniques, command control as well as service requirements.

The apparel manufacturing industry has become a vital field in the world's manufacturing field since the beginning of the first revolution. Textile field has a great history and it keep on developing due to the high adaptability for new arising technologies such as IIoT. Apparel fashion industry has become a highly competitive industry. Therefore, integrated technologies within the industry are rapidly advancing allowing innovations in the manufacturing processes. Industry 4.0 allows characteristics such as scalability, customization in massive scale, customer satisfaction and control and visibility which

place a significance value in apparel industry. Nevertheless most automation systems are evolving around garment industry.

The basic flow of the production processes in a clothing and apparel factory includes design the product according to the marketing demands and customer requirements, selecting suitable clothing material, Forming layers from the clothing materials, Cutting various shapes by minimizing the wastage of materials, different sewing operations, finishing, product quality assurance, packing, storing and distribution.

Cutting process plays a huge role in garment automation industry because of the wastage problem, availability and accessibility, labor dependency and it is an expensive process. Introduced in 1900s die cutters increased cutting efficiency and quality, Numerical Controller (NC) machines appeared in 1940s and made continuous cutting possible, leading to a greater flexibility in production and more use of material. Computer Numerically Controlled (CNC) machines was created in the digital revolution. This technological advancement made cutting the most advanced sector in apparel field. Various cutting devices such as computer controlled knives, laser, plasma, ultrasound and markers are available. Since the first fully automated cutting system matured with enhancement in technology the existing cutting technologies developed with the aspect of productivity, versatility and pattern matching capability. Cutting processes which includes CNC machines are currently ongoing industry 4.0 revolution while addressing solutions for labor intensive problems, wastage problems and cost cutting [8].

The concept of digitalization and integration has been pointed out in IIoT or fourth industrial revolution which CNC technology plays a vital part when automating cutting garment manufacturing systems. The CNC is a hub which important data are flowing. In industry 4.0 CNC controllers should be capable of supporting integration, sensors, and cloud servers. A challenge is the transaction from traditional hardware based controllers architecture to a smart automation software architecture. The security related problems arise as today's industrial 4.0 automation is driven by focusing on the functionality rather than security. Lack of security might lead to increasing economic damages, loss of

production and even loss of life. As we know, IoT depends between digital and physical environment through IoT with other technologies, industrial espionage and sabotage is massively increasing over the past years. Existing measures' shortcoming poor levels of awareness. Readiness for upcoming confrontations is vital that is the reason for security should be important underpinning the development of the development in industry 4.0. If the industrial 4.0 manufacturing automation developers could identify the application of cyber security requirements which are not been thoroughly captured in automation and develop systems addressing all the security aspects in automation, the developing automation systems would be potentially free of huge risks and would be safe. Cyber physical systems play a crucial role in cyber security for industrial 4.0 automation manufacturing systems.

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 [13]. 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 IEC 61158 and can be used for both hard and soft real-time automation requirements. Both

PROFINET and Sercor 3 standards could also be used. For PLC, PLCOpen IEC 61131 standard 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 use a variety of insecure communication protocols, including PROFINET, Modbus,, DNP3, and EtherCAT. Although DNP3 and Modbus started out as serial protocols, they have both been enhanced to work with Ethernet and TCP/IP, and they're now widely used to connect devices across field buses and networks. These 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 load 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 testbeds, 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, time delay attack, data tampering 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]. Mostly security has been shared with a third party, and the manufacturers should rely on the trust of the third party. There could be insider threats, loss of governance of shared data and many more threats. 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 primarily focus only on functionality of industrial 4.0 automated systems and security is been 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 (Programmable Logic Controller), RTU (Remote Terminal Unit) systems, and SCADA servers were all searched using SHODAN, a custom IoT search engine. Servers for HMI (Human Machine Interface) 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 CIS violation, it is a threat to the system so that new security concept involve security standards.

Many working groups are working on factory automation, and some standards have already been published, as shown below.

#### ISO/IEC TC 1/SC 27

- 1) Working Group WG1 Requirements, security services, and guidelines  
WG2 Techniques and Mechanisms  
WG3 security evaluation criteria
- 2) Standards ISA-SP99 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. [9].

Table 1.1: Comparison of industrial standards and guidelines

	IEC 62443	ISO/IEC 27000	ISO/IEC 15408	VDI/VDE 2182
<b>Purpose</b>	- Industrial communication networks - Network and system security	- Information Technology - ISMS	- Evaluation criteria for IT security	- Risk-based selection of controls and countermeasures
<b>Structure of Documentation</b>	- 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
<b>Procedure</b>	- Domain-tailored concepts	- 4 cyclic steps	- One-time approach	- 8 cyclic steps
<b>Viewpoint</b>	- Policies & procedures - (Technical) systems & components	- Management & organisation - Processes	- TOE	- Risks & threats - Countermeasures
<b>Target Audience</b>	- 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
<b>Protection</b>	- 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
<b>Metrics</b>	- 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

Source : 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](https://doi.org/10.1109/IECON.2019.8927559). [11]

Table 1.2: Summary of best practices for industrial 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

Source: 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](https://doi.org/10.1109/IECON.2019.8927559). [11]

### **1.3 Research Gap**

Industrial 4.0 transaction from traditional hardware based controllers architecture to a secure smart automation software architecture is a challenge.

The security related problems arise as today's Industrial 4.0 automation is driven by focusing on the functionality and SAM/SMV (Standard Allowed Minute/ Standard Minute Value) rather than security. There are few IoT security frameworks in various stages of development. (ETSI (European Telecommunications Standards Institute) EN 303 645, IoT Security Compliance Framework, OWASP ISVS, ENISA, NIST)[14][15].

Comparison of the security standards and best practices for the different industrial automation domains are available.[16] There hasn't been a powerful enough push to make universal IoT security standards.

The research focus on designing an automated system focusing cyber security aspects to the identified manufacturing system, while considering security threats and drawbacks of current automated garment manufacturing systems in the local industry. After designing the automated system, will consider the problems encountered while implementing security to the system and analyze whether those security problems are encountered in the current local industrial automated systems. So that we could clearly find the security gap between the current industrial automated garment manufacturing systems currently available locally and the proposed system for the research. Security standards verification and policy creation verification for the manufacturing system will be done by an industry expert to close the gap.

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.



## **1.4 Research problem**

When automating a manual system or semi – automated system towards the Industry 4.0 smart computing will integrate with technologies including IoT, cognitive computing, machine learning and data analytics. Most system developers do not entirely recognize the cyber security challenges when designing an industrial 4.0 automated system. The research is to identify the application of cyber security requirements which are not been thoroughly captured in automation.

Challenges:

For the creation of a safe network environment a 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, [1] store information, documentation, decision making, corrective and preventive action.

### **1.4.2 Centralized security management**

Creating CPS models to apply security configurations/updates to physical devices and monitor physical devices using a centralized control system such as Supervisory control and data acquisition (SCADA) to maximize efficiency [2]. 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. [1].

### **1.4.3 Secure communication**

CPS that use the SCADA systems is connected to the internet over TCP/IP protocols without additional protection [3], which have known vulnerabilities.

#### **1.4.4 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. [4].

#### **1.4.5 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. [5]

#### **1.4.6 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. [6].

Main focus for the component arise the questions such as how to identify and create security policies, how to integrate security strategies suitable for IoT and CPS devices, Which standards are suitable for the policy creation, 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 CNC machine towards industrial 4.0 automated garment manufacturing system. In order to implement the automated system securely, used security standards should be verified. 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 layered security approach to maintain the quality and to mitigate threats to the automated system.

## **2. OBJECTIVES**

### **2.1 Main Objectives**

Main objective of the overall research 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 Ansible. Python, Django, Bash technologies will be used for the update management configurations.

### **2.2 Sub Objectives**

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 which are verified by an industrial expert to design the secured automated system safely. Come up with procedures and methods to implement the identified security policies. Verify the security policies before implementing for the accountability of the research.

### 3. METHODOLOGY

#### 3.1 System Diagram

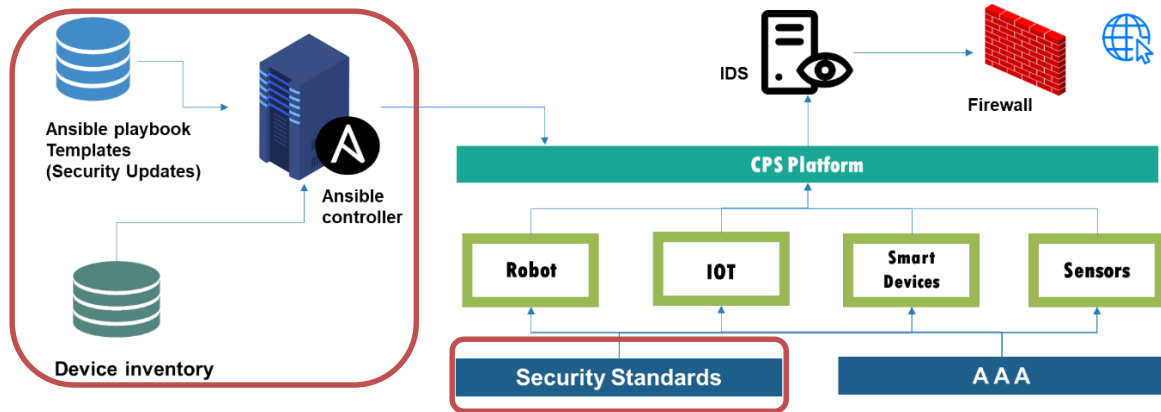


Figure 3.1: Overall System Diagram

As highlighted in the above overall system diagram, update management component is done using Ansible playbbok templates and Ansible controller which is associated with the device inventory. Security standards component is focused for IoT devices, sensors and the network.

#### 3.2 Individual Components

##### 3.2.1 Security standards and policy development

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.

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

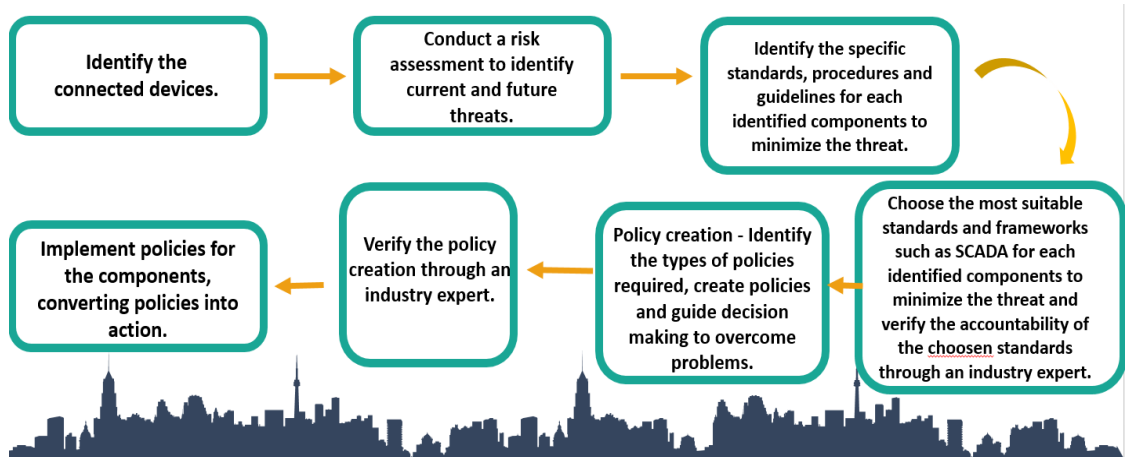


Figure 3.2: Individual Workflow Diagram- Security standards and policy development

### 3.2.1.1 Identify the connected devices

Analyze business requirements, understand customer-partner requirements, and discuss aspects of security CIA (Confidentiality, Integrity, and Availability) and how they might apply to this requirement and identify devices according to the requirements and categorize the devices.

### 3.2.1.2 Conduct a risk assessment

Determine issues which has to be addressed in the document but also to which instance or degree should the issues be addressed. According to ISO 9001, must determine to what degree a method is critical to the quality control and then decide whether or not to log it. According to the ISO 31000:2018 standard, which provides guidelines and a common approach to managing any type of risk, a risk is usually expressed in terms of risk sources, possible events, their consequences, and their probability. Risk

management is defined in this standard as a set of coordinated activities for directing and controlling risks.

The Octave risk assessment framework is a methodology for identifying and assessing asset information security risks. Octave is highly personalized, self-directed, and adaptable.

- Determine the importance of vital assets.
- Concentrate risk analysis on the most critical assets.
- Think about the connections between critical assets, threats to assets, and vulnerabilities that expose assets to threats. Assess risks in a real-world setting.
- To reduce risk, develop a practice-based protection strategy and risk mitigation plans.

### **3.2.1.3 Identify the specific standards, procedures and guidelines for each identified components.**

Suitable frameworks and standards should be identified and chosen for policy creation. Frameworks such as NIST, ENISMA, SCADA frameworks can be used accordingly for the policy creation purpose.

### **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 National Institute of Standards and Technology - United States has released a free special publication.

## **CPS**

CPSs (cyber-physical systems) 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.

### **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.

#### **3.2.1.4 Choose the most suitable standards and frameworks**

Choose the most suitable standards and frameworks after evaluating each component and their requirements.

#### **3.2.1.5 Verify the chosen standards and frameworks**

Verify 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 could be done through external supervisor. Security standards could be verified through a security industry expert.

#### **3.2.1.6 Determine the types of policies that are needed.**

Identify the types of policies needed to the automation system such as password policies, network and physical access policies, security update policies, acceptable use policies,

encryption policies, vulnerability management policies according to standards and legislations.

#### **3.2.1.7 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.

#### **3.2.1.8 Implement policies for the components**

Properly install 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. After implementing the policies members who are responsible for each component could conduct testing, auditing to ensure and verify that the applied policies are secured.

### **3.2.2 Update management**

Create a tool to provide security updates to IoT devices using Ansible roles.

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

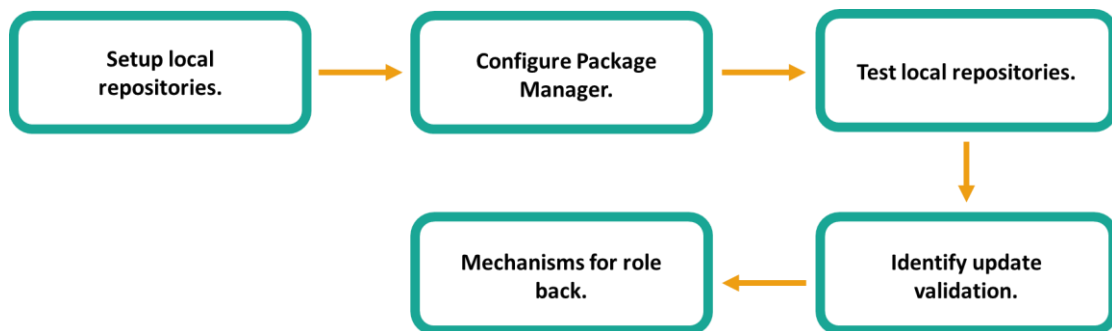


Figure 3.3: Individual Workflow Diagram- Security Updates



### **3.2.2.1 Setup local repositories**

Setup a local repository in the server. Creating a local repository is advantageous when the devices are connected and have to install more software, security updates are often happened in all systems saving internet bandwidth and decreasing internet cost.

Host the created repo using apache HTTPD 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.

### **3.2.2.2 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.

### **3.2.2.3 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 symlink. Add repository source in other devices to fetch the repository and packages.

### **3.2.2.4 Test local repositories**

Install packages using added local repository

### **3.2.2.5 Verify update**

Verify updates using GPG keys to identify rogue updates.

### **3.2.2.6 Mechanisms for roll back**

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

### **3.3 Requirements**

- Meeting stakeholder requirements
- Risk identification and assessment
- Security policy development and privacy by design
- Hardware root of trust

### 3.4 Gantt Chart



Figure 3.4: Gantt chart

#### 4. DESCRIPTION OF PERSONAL AND FACILITIES

Table 4.1: Description of Personal and Facilities

Registration no	Name	Task Description
IT18136098	P.A.U.T. De Alwis	<ul style="list-style-type: none"><li>• Security standards and policy development</li></ul> Conduct a risk assessment Choose suitable framework and standards Policy creation Policy verification <ul style="list-style-type: none"><li>• Update management</li></ul> Create a tool to provide security updates to IoT devices using Ansible roles.

## 5. BUDGET AND BUDGET JUSTIFICATION

Table 5.1: Budget and Budget Justification

Item(s)	Cost (LKR)
Web server hosting	5000.00
Firewall + IDS/IPS hardware	18000.00
Physical security system hardware	5000.00
Raspberry Pi 3	12000.00
<b>Total</b>	<b>40000.00</b>

## 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](https://doi.org/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](https://doi.org/10.1109/ACCESS.2018.2884906).
- [3] 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](https://doi.org/10.1109/ICCAD.2017.8203896).
- [4] Kamble, S., Gunasekaran, A. and Gawankar, S., 2020. Sustainable Industry 4.0 Framework: A Systematic Literature Review Identifying The Current Trends And Future Perspectives.
- [5] Lins, Theo & Rabelo, Ricardo & Correia, Luiz & Sá Silva, Jorge. (2018). Industry 4.0 Retrofitting. 8 -15. [10.1109/SBESC.2018.00011](https://doi.org/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.
- [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.
- [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](https://doi.org/10.1016/j.jmsy.2018.04.007).
- [8] M. Suh, “Automated Cutting and Sewing for Industry 4.0 at ITMA 2019,” p. 13, 2019.
- [9] 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](https://doi.org/10.1109/SICE.2007.4421488).
- [10] 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](https://doi.org/10.1109/ACCESS.2018.2884906).
- [11] 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](https://doi.org/10.1109/IECON.2019.8927559).

[13]“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).

[14]“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-security-frameworks/> (accessed Mar. 07, 2021).

[15]“Comparison of IoT Security Frameworks,” *Comparison of IoT Security Frameworks*. <https://www.eurofins-cybersecurity.com/news/comparison-iot-security-frameworks/> (accessed Mar. 07, 2021).

[16]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](https://doi.org/10.1109/IECON.2019.8927559)

# APPENDICES

## Appendix A : Turnitin similarity Score

feedback studio

Udara De Alwis IT18136098\_Project Proposal Report

**CYBERSECURITY AUTOMATION FOR AN INDUSTRY 4.0  
GARMENT MANUFACTURING SYSTEM**

Project Id: 2021-11

Project Proposal Report

P.A.U.T. De Alwis

Page: 1 of 31 Word Count: 5351

Text-only Report High Resolution On

**Match Overview**

**20%**

1	www.glacier-project.de	Internet Source	2%	>
2	Nilufer Tuptuk, Stephen...	Publication	2%	>
3	Submitted to Sri Lanka ...	Student Paper	2%	>
4	Submitted to University...	Student Paper	2%	>
5	Mitsuo Harada, "Securi...	Publication	1%	>
6	Submitted to Middlese...	Student Paper	1%	>
7	erevistas.uaqj.mx	Internet Source	1%	>
8	Yury N. Kofanov, Svetla...	Publication	1%	>
9	Garcia, Marcelo V., Fed...	Publication	1%	>