



Sri Lanka Institute of Information Technology

PROJECT REGISTRATION FORM

(This form should be completed and uploaded to the Cloud space on or before XXXXXXXXX)

The purpose of this form is to allow final year students of the B.Sc. (Hon) degree program to enlist in the final year project group. Enlisting in a project entails specifying the project title and the details of four members in the group, the internal supervisor (compulsory), external supervisor (may be from the industry) and indicating a brief description of the project. The description of the project entered on this form will not be considered as the formal project proposal. It should however indicate the scope of the project and provide the main potential outcome.

PROJECT TITLE (As per the accepted topic assessment form)	Cyber security automation for an industrial 4.0 garment manufacturing system
--	--

RESEARCH GROUP (as per the Topic assessment Form)	Internet of Things
--	--------------------

PROJECT NUMBER		(will be assigned by the lecture in charge)
----------------	--	---

PROJECT GROUP MEMBER DETAILS: (Please start with group leader's details)

	STUDENT NAME	STUDENT NO.	CONTACT NO.	EMAIL ADDRESS
Format	Perera C.D.D	ITxxxxxxx	0712345678	itxxxxxxx@my.sliit.lk
1	H.H. Dasunpriya kalhara	IT18139440	0775494315	it18139440@my.sliit.lk
2	P.A.U.T De Alwis	IT18136098	0776713691	it18136098@my.sliit.lk
3	A.D.H Jinadasa	IT18132410	0772562889	it18132410@my.sliit.lk
4	R.P.R.D Randunu	IT18133578	0765420261	it18133578@my.sliit.lk

SUPERVISOR Name	CO-SUPERVISOR Name
Dr. Pradeep Abeygunawardhana	Ms.Sasini Wellalage
Signature	Signature
Attach the email as Appendix 1	Attach the email as Appendix 2
Date	Date

SUPERVISOR, CO_ SUPERVISOR Details**EXTERNAL SUPERVISOR Details** (if any, may be from the industry)

Eng. P.A. Gamini De Alwis	Head of pump Division, Richard Pieris & Company PLC. Technical Director, Glide.	283/A, Lumbini Place, Hokandara Road, Thalawathugoda	0773489617 0112776700	Attach the email as Appendix 3
Name	Affiliation	Contact Address	Contact Numbers	Signature/Date

ACCEPTANCE BY CDAP MEMBER (This part will be filled by the RP team)

Name	Signature	Date

PROJECT DETAILS

Brief Description of your Research Problem: (extract from the topic assessment form)

When automating a manual system or semi – automated system towards the fourth industrial revolution (Industry 4.0) smart computing is integrated 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:

The development of the secure network environment

The network environment in industry 4.0 is developing using a CPPS platform using CPS technology. Building the CPPS platform is a complex project that is currently limited by various conditions, such as following CPS challenges,

1) Collaboration between different systems

A Collaborative model between physical devices and computer systems is essential for exchanging information, [1] store information, documentation, decision making, corrective and preventive action.

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]. Physical devices environment, software, and hardware platforms, and other functional and non-functional must consider in a typical CPS model in addition to CPS modeling language [1].

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.

4) Insecure Data

Lack of system integrations to ensure data security for the manufacturing companies during the implementation of Industry 4.0. The IoT-based CPSs that are connected to many of embedded sensors and communication devices pose a significant risk linked with the growth of data usage and the much higher risks of system breaches [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 implement the architecture as per the business needs considerable initial investment in the matter of cost and time is required [5].

6) Lack of strategy to Industry 4.0

Lack of dynamic strategic plan to support the migration to Industry 4.0 in the manufacturing Industry [6].

[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] 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.

[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.

[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.

Description of the Solution: (extract from the topic assessment form)

Design and implement an automated system focusing cyber security aspects to the identified micro-enterprise manual garment manufacturing business, according to the external supervisor's advice from the manufacturing field, while considering security threats and drawbacks of current automated garment manufacturing systems in the local industry. After designing and implementing the automated system, consider the problems encountered while implementing the system and analyze whether those security problems are encountered in the current local industrial automated systems, in order to find the security gap between the current industrial automated garment manufacturing systems currently available locally and the proposed system for the research.

Develop security policies, considering industrial guidelines, procedures and standards in order to implement the automated system securely. Design and implement a private network with a firewall and an intrusion detection system to improve network monitoring and security. Establish secure communications between IoT devices to use ansible to automate device management with the help of an ansible controller in order to centralize device security and configuration management.

Main expected outcomes of the project: (extract from the topic assessment form)

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 industry standards, that has authentication and access monitoring for the utilized IoT devices, automated security configurations using ansible, security updates using ansible and intrusion detection system.

WORKLOAD ALLOCATION (extract from the topic assessment form after correcting the suggestions given by the topic assessment panel.)

(Please provide a brief description about the workload allocation)

MEMBER 1

Create playbooks to configure IoT devices and other devices in the network and automate device configuration using ansible. Create a tool to harden IoT devices to make the devices more resilient against attacks and check compliance according to industry standards. Add audit and remediation scripts to the tool based on industrial guidelines. Add report generating functionality to the tool. Design methodology to achieve specification, modeling and analysis for the CPS based on supervisors' advice.

MEMBER 2

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

MEMBER 3

Implement firewall and intrusion detection system to provide edge network protection with real time monitoring. An efficient firewall will allow to ward off attacks against the network. In addition to network security, conducting hazard analysis, defining safety constraints, asset loss assessment is planned to design to ensure the system security. lastly to guarantee the interoperability of the components by using ansible modules.





MEMBER 4

Authenticate users when connecting between IoT devices and ansible controllers to enable secure access to the services. Moreover, monitor and filter the user behavior on the system to prevent unauthorized access and to prevent malicious attacks on the networks. And also build the strong security and encryption method to safeguard the system. In addition, design a methodology to production improvement and do modifications of production flow paths.

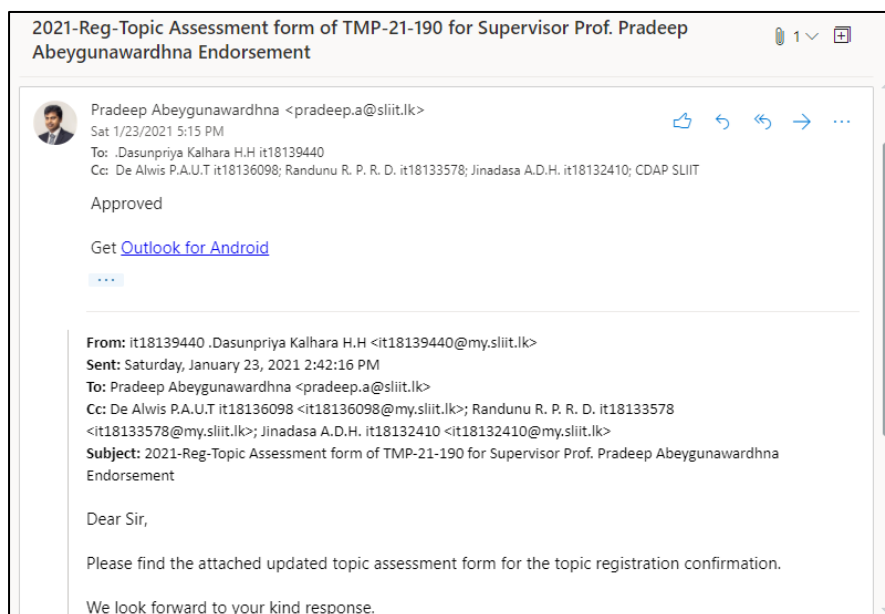
DECLARATION (Students should add the Digital Signature)

"We declare that the project would involve material prepared by the Group members and that it would not fully or partially incorporate any material prepared by other persons for a fee or free of charge or that it would include material previously submitted by a candidate for a Degree or Diploma in any other University or Institute of Higher Learning and that, to the best of our knowledge and belief, it would not incorporate any material previously published or written by another person in relation to another project except with prior written approval from the supervisor and/or the coordinator of such project and that such unauthorized reproductions will construe offences punishable under the SLIIT Regulations.

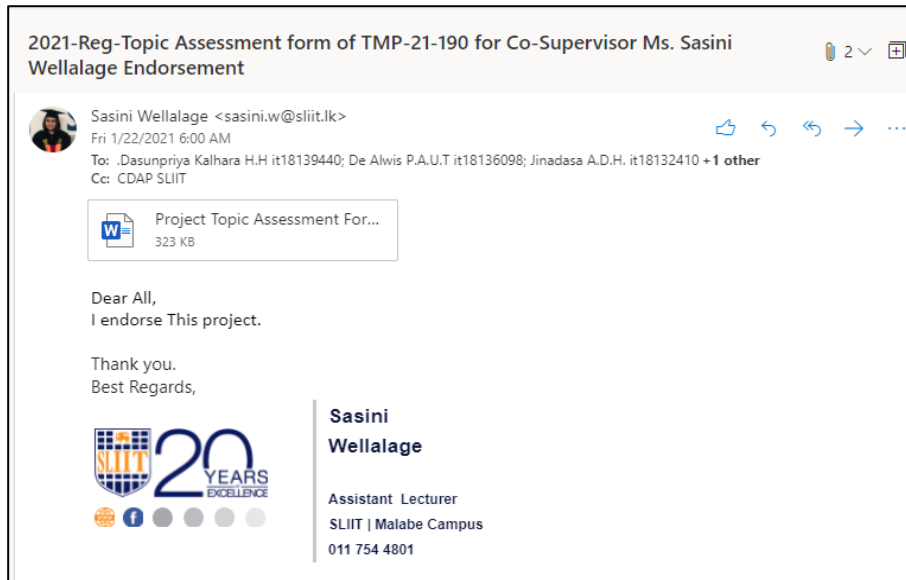
We are aware, that if we are found guilty for the above mentioned offences or any project related plagiarism, the SLIIT has right to suspend the project at any time and or to suspend us from the examination and or from the Institution for minimum period of one year”.

	STUDENT NAME	STUDENT NO.	Signature
1	H.H. Dasunpriya kalhara	IT18139440	
2	P.A.U.T De Alwis	IT18136098	
3	A.D.H Jinadasa	IT18132410	
4	R.P.R.D Randunu	IT18133578	

Appendix 1:



Appendix 2:



Appendix 3:

