Coursework Assignment Brief

Assessment - Postgraduate

Academic Year 2024-25

Module Title: Cyber-Physical Systems Security			
Module Code: CMP7240			
Assessment Type Coursework	**Level** 7	**Weighting** 100%	**Word Count/Workload** 4000 words
Submission Date Week 12	**Submission Time** 1500	**Module Leader** Junaid Arshad	**Time Limit** N/A

Assessment Information	
Assessment Summary (with type)	To conduct a thorough cyber security review of a connected manufacturing system.
Assessment Title	Analysis of Cyber Security within a CPS Scenario
Things to include:	Review, design, and critical analysis in the form of a report.

Completion of this assessment will address the following learning outcomes:	
1	Critically evaluate current threat landscape for Cyber-Physical Systems and articulate commonalities and differences with contemporary computing systems
2	Apply learned concepts, methods and techniques to address cybersecurity challenges within a given CPS context
3	Discuss the impact of the techno-social context in a cybersecurity programme considering regulations, criticality of requirements, the environment, etc.

Submission Information

Present any written aspects of the assessment using font size 11 and using 1.5 spacing to allow for comments and annotations to be added by the markers.

Complete the appropriate cover sheet for this assessment and append your work.

This assessment will be marked anonymously and should show your student number only.

Submit this coursework assessment task via Moodle.

Late Submission

Assessments must be submitted in the format specified in the assessment task, by the deadline and to the submission point published on Moodle. Failure to submit by the published deadline will result in penalties which are set out in Section 6 of the Academic Regulations, available at: https://icity.bcu.ac.uk/Quality-Enhancement-and-Inclusion/Quality-Assurance-and-Enhancement/Academic-Regulations

Word Count

The maximum word count for this module assessment is shown on Page 1. A +10% margin of tolerance is applied, beyond which nothing further will be marked. Marks cannot be awarded for any learning outcomes addressed outside the word count.

The word count refers to everything in the main body of the text (including headings, tables, citations, quotes, lists etc.). Everything before (i.e. abstract, acknowledgements, contents, executive summaries etc.) and after (i.e. references, bibliographies, appendices etc) is **not** included in the word count limit.

Referencing Style

- BCU Harvard

More information on referencing is available here: https://www.bcu.ac.uk/library/services-and-support/referencing

Use of Artificial Intelligence

Whilst AI tools can be helpful in assisting learning, when it comes to assessment, the Academic Misconduct Procedure is clear that this should be a student's own original work and not the work of other people or AI tools.

The Use of AI Tools – Student Guidelines document follows the same guidelines your lecturers use. If you are unsure of whether AI is appropriate within your work, please read the guidelines or ask your lecturer. For advice and guidance around academic writing, please visit the Centre for Academic Success.

Academic Integrity Guidance

Academic integrity is the attitude of approaching your academic work honestly, by completing and submitting your own original work, attributing and acknowledging your sources when necessary. Understanding good academic practice in written and oral work is a key element of academic integrity. It is a positive aspect of joining an academic community, showing familiarity with and acknowledging sources of evidence. The skills you require at higher education may differ from those learned elsewhere such as school or college.

You will be required to follow specific academic conventions which include acknowledging the work of others through appropriate referencing and citation as explicitly as possible. If you include ideas or quotations that have not been appropriately acknowledged, this may be seen as plagiarism which is a form of academic misconduct. If you require support around referencing, please contact the Centre for Academic Success

It is important to recognise that seeking out learning around academic integrity will help reduce the risk of misconduct in your work. Skills such as paraphrasing, referencing and citation are integral to acting with integrity and you can develop and advance these key academic skills through the Centre for Academic Success (CAS).

To learn more about academic integrity and its importance at university, you can access CAS resources on Moodle. Furthermore, you can book on to workshops and request 1-2-1 support around key academic skills.

Academic Misconduct

Academic misconduct is conduct that has or may have the effect of providing you with an unfair advantage by relying on dishonest means to gain advantage and which therefore compromises your academic integrity.

The Academic Misconduct procedure sets out the process we will follow, and the penalties we may apply, in cases where we believe you may have compromised your academic integrity by committing academic misconduct. The Academic Misconduct Procedure and information about academic support is available at: https://icity.bcu.ac.uk/Student-Affairs/Appeals-and-Resolutions/Academic-Misconduct-Procedure

Task: To conduct a thorough cyber security review of a connected industrial system

Style: Report

Rationale: To apply knowledge and skills learnt through this module in a real-life scenario.

Description: SmartFab Industries is a hypothetical mid-sized manufacturing company specializing in precision components for the automotive sector. Leveraging a fully connected manufacturing ecosystem, SmartFab integrates IoT-enabled machinery, cloud-based ERP systems, and AI-driven analytics. On the factory floor, machines automatically report performance data in real time, triggering predictive maintenance alerts before breakdowns occur. Inventory levels are monitored and replenished automatically via smart sensors, while production schedules adjust dynamically based on supply chain inputs and customer demand. Engineers and managers access live dashboards remotely, enabling faster decision-making and enhanced collaboration across departments and sites.

However, with the rising number of attacks and vulnerabilities targeting connected devices and infrastructures in recent year, SmartFab is cautious and intends to conduct a thorough review to understand any implications of adopting these technologies.

As an expert within Cyber-Physical Systems Security, SmartFab need your help to achieve this transformation while preserving security and privacy of their patients.

To aid them, you are required to complete the following:

- Conduct a review of state of the art to identify and understand the threat landscape for connected manufacturing infrastructures.
- Develop a high-level architecture for the proposed infrastructure and conduct threat modelling for three critical components.
- Based on the outcome of threat modelling, produce a secure network design along with justification for your design choices. Please also include a discussion of appropriate countermeasures/mitigation strategies to protect against the identified threats which should highlight how these measures can protect against specific threats. You can include countermeasures such as network segmentation, cryptography, vulnerability scanning, and intrusion detection system.

Additional information:

Element 1 – Threat Landscape and Review (1000 words)
For this element, you are required to conduct a review of state of the art to identify and understand the threat landscape for the scenario provided above. You can consult academic literature such as published articles, conference papers and books etc as well as technical reports and other public sources of data to: identify specific characteristics of connected infrastructures; understand the impact of these characteristics on security requirements for such infrastructures, and assess the scale of cyber threats for the scenario presented above.

Element 2 – Threat Modelling (1000 words)
For this element, you are required to use methods such as STRIDE to conduct threat modelling for the given scenario. You will be expected to develop a high-level technical architecture for the scenario presented above which will include identifying critical components of the proposed system. You will perform threat modelling exercise for three critical components of the system using STRIDE method. Please include your assessment and reasoning to accompany the threats identified.

Element 3 – Secure Design and Countermeasures (2000 words)

In this element, you are required to develop a secure network design along with justification for your design choices. Please also include a discussion of appropriate countermeasures/mitigation strategies to protect against the identified threats which should highlight how these measures can protect against specific threats. You can include countermeasures such as network segmentation, cryptography, vulnerability scanning, and intrusion detection system

For advice on writing style, referencing and academic skills, please make use of the Centre for Academic Success: Centre for Academic Success - student support | Birmingham City University (bcu.ac.uk)

Transferable skills:

- Research skills
- Analytical Thinking
- Critical Thinking
- Organisational Skills
- Written Communication
- Time Management
- Problem Solving
- Technical Proficiency
- Professionalism

Marking Criteria:

Table of Assessment Criteria and Associated Grading Criteria

Learning Outcomes	1	2	3
Assessment Criteria →	**Threat Landscape and Review**	**Threat Modelling**	**Secure Design and Countermeasures**
Weighting:	20%	30%	50%
Grading Criteria **0 – 20% Fail**	Unable to identify characteristics impacting security requirements for the proposed system. Unable to conduct the review and analysis of the state of the art. Unable to critically analyze and assess the scale of cyber threats for the given scenario. Unable to consult and reference existing academic and other public resources.	Unable to develop a high-level architecture of the proposed system. Unable to understand and apply the STRIDE method Unable to identify critical components and threats specific to these components along with appropriate reasoning.	Unable to develop a secure network design. Unable to include a discussion of appropriate countermeasures / mitigation strategies to protect against the identified threats. Unable to include discussion on countermeasures.
20 – 39% Fail	Limited effort to identify characteristics impacting security requirements for the proposed system. Limited review and analysis of the state of the art. Poor critical analysis to assess the scale of cyber threats for the given scenario. Some evidence of consulting and reference existing academic and other public resources.	Limited effort to develop a high-level architecture of the proposed system. Basic understanding of the STRIDE model and its limited application to identify threats. Unable to identify critical components and threats specific to these components. Basic or no reasoning included.	Limited effort to develop a secure network design along. No justification for design choices included. Limited discussion of appropriate countermeasures/mitigation strategies to protect against the identified threats Limited or no discussion on countermeasures which may not be relevant to identified threats.
40 – 49%	Identification of some characteristics impacting security requirements for the proposed system. Limited effort to conduct the review and analysis of the state of the art. Poor quality of critical analysis to assess the scale of cyber threats for the given scenario. Some references to existing academic and other public resources.	A basic architecture of the proposed system presented but with important components missing. Limited understanding of the STRIDE model and its limited application to identify threats. Identification of some critical components and some relevant threats. Limited reasoning included.	Some effort to develop a secure network design along. Limited justification for design choices included. Limited discussion of appropriate countermeasures/mitigation strategies to protect against the identified threats Limited discussion on countermeasures relevant to identified threats.

	50 – 59%	Identification of characteristics impacting security requirements for the proposed system. Fair effort to conduct the review and analysis of the state of the art. Decent quality of critical analysis to assess the scale of cyber threats for the given scenario. Some evidence of use of existing academic and other public resources.	An architecture of the proposed system presented with some important components included. Understanding of the STRIDE model and its application to identify some threats. Identification of some critical components and some relevant threats. Some reasoning included.	Decent effort to develop a secure network design along. Some justification for design choices included. Some discussion of appropriate countermeasures/mitigation strategies to protect against the identified threats Decent discussion on countermeasures relevant to identified threats.	
	60 – 64%	Identification of characteristics impacting security requirements for the proposed system along with appropriate reasoning. Good effort to conduct the review and analysis of the state of the art. Good quality of critical analysis to assess the scale of cyber threats for the given scenario. Evidence of use of existing academic and other public resources.	An architecture of the proposed system presented with important components included. Good understanding of the STRIDE model and its application to identify some threats. Identification of critical components and some relevant threats. Decent reasoning included.	Good effort to develop a secure network design along. Good justification for design choices included. Good discussion of appropriate countermeasures/mitigation strategies to protect against the identified threats Good discussion on countermeasures relevant to identified threats.	
	65 – 69%	Identification of characteristics impacting security requirements for the proposed system along with very good reasoning. Very good effort to conduct the review and analysis of the state of the art. Very good quality of critical analysis to assess the scale of cyber threats for the given scenario. Evidence of use of range of existing academic and other public resources.	An architecture of the proposed system presented with important components included. Very Good understanding of the STRIDE model and its application to identify threats. Very good effort to identify critical components and relevant threats. Good reasoning included.	Very good effort to develop a secure network design along. Very good justification for design choices included. Very good discussion of appropriate countermeasures/ mitigation strategies to protect against the identified threats Very good discussion on countermeasures relevant to identified threats.	

70 – 79%	Identification of characteristics impacting security requirements for the proposed system along with excellent, in-depth reasoning. Excellent effort to conduct the review and analysis of the state of the art. Excellent quality of critical analysis to assess the scale of cyber threats for the given scenario. Evidence of use of range of existing academic and other public resources and high quality argument underpinned by them.	A high-level architecture of the proposed system presented with important components included. Excellent understanding of the STRIDE model and its application to identify threats. Excellent effort to identify critical components and relevant threats. Very good reasoning included.	Excellent effort to develop a secure network design along. Excellent justification for design choices included. Excellent discussion of appropriate countermeasures/ mitigation strategies to protect against the identified threats Excellent discussion on countermeasures relevant to identified threats.
80 – 89%	Identification of characteristics impacting security requirements for the proposed system along with outstanding, in-depth reasoning. Outstanding effort to conduct the review and analysis of the state of the art. Outstanding quality of critical analysis to assess the scale of cyber threats for the given scenario. Evidence of use of range of existing academic and other public resources and high quality argument underpinned by them.	Outstanding effort to develop a high-level architecture of the proposed system with important components included. Outstanding understanding of the STRIDE model and its application to identify threats. Outstanding effort to identify critical components and relevant threats. Excellent reasoning included.	Outstanding effort to develop a secure network design along. Outstanding justification for design choices included. Outstanding discussion of appropriate countermeasures/ mitigation strategies to protect against the identified threats Outstanding discussion on countermeasures relevant to identified threats.
90 – 100%	Identification of characteristics impacting security requirements for the proposed system along with world-class, in-depth reasoning. World-class effort to conduct the review and analysis of the state of the art. World-class quality of critical analysis to assess the scale of cyber threats for the given scenario. Evidence of use of range of existing academic and other public resources and world-class argument underpinned by them.	World-class effort to develop a high-level architecture of the proposed system with all important components included. World-class understanding of the STRIDE model and its application to identify threats. World-class effort to identify critical components and relevant threats. World-class reasoning included.	World-class effort to develop a secure network design along. World-class justification for design choices included. World-class discussion of appropriate countermeasures/ mitigation strategies to protect against the identified threats World-class discussion on countermeasures relevant to identified threats.

Submission Details:

Format:

Report

- Submit Written assignment to Moodle via electronic upload
- Submissions should be provided in Microsoft word (.docx) or (text-based) PDF format.

Regulations:

- The minimum pass mark for a module is 50%
- Re-sit marks are capped at 50%

Full academic regulations are available for download using the link provided above in the IMPORTANT STATEMENTS section

Late Penalties

If you submit an assessment late at the first attempt, then you will be subject to one of the following penalties:

- if the submission is made **between 1 and 24 hours** after the published deadline the original mark awarded will be reduced by **5%**. For example, a mark of 60% will be reduced by 3% so that the mark that the student will receive is 57%.
- if the submission is made between **24 hours** and **one week (5 working days)** after the published deadline the original mark awarded will be reduced by 10%. For example, a mark of 60% will be reduced by 6% so that the mark the student will receive is 54%.
- **if the submission is made after 5 days following the deadline, your work will be deemed as a fail and returned to you unmarked.**

The reduction in the mark will not be applied in the following two cases:

- the mark is below the pass mark for the assessment. In this case the mark achieved by the student will stand
- where a deduction will reduce the mark from a pass to a fail. In this case the mark awarded will be the threshold (i.e., 50%)

Please note:

- **If you submit a re-assessment late then it will be deemed as a fail and returned to you unmarked.**

Feedback:

Marks and Feedback on your work will normally be provided within 20 working days of its submission deadline.

Where to get help:

Support hours will be shared during the semester based on timetable.

Students can get additional support from the library support for searching for information and finding academic sources. See their iCity page for more information: http://libanswers.bcu.ac.uk/

The Centre for Academic Success offers 1:1 advice and feedback on academic writing, referencing, study skills and maths/statistics/computing. See their iCity page for more information: https://icity.bcu.ac.uk/celt/centre-for-academic-success

Additional assignment advice can be found here: https://libguides.bcu.ac.uk/MA

Fit to Submit:

Are you ready to submit your assignment? Review this assignment brief and consider whether you have met the criteria. Use any checklists provided to ensure that you have done everything needed.

Assignment Checklist

Run through this simple tick list before submitting your work!

Report

Well prepared materials make your work look more professional and easier to understand.

Item	Action	Done
1	I have used the spellchecker and proofread the work correcting errors several times.	
2	I have checked that all material is directly related to the assignment tasks.	
3	I have checked that all the required information has been included in the work.	
4	The work is professionally presented using consistent headings, fonts and layout.	
5	All tables and images are numbered and captioned.	
6	I have used the structure specified in the assignment.	

Referencing and Originality

Your work will be subjected to checks to ensure it is not copied. Derivative work may leave you subject to penalties, including in extreme cases, expulsion from the University.

Item	Action	Done
1	All images and tables are fully referenced.	
2	I have not copied any material from anywhere else. All sentences have been paraphrased into my own words.	
3	All references appear in the references section at the end of the presentation.	
4	All references are cited in the text in the form of (author, year). See https://www.bcu.ac.uk/library/services-and-support/referencing for more details.	
5	If I have used quotes, these are fully referenced, appear in quotation marks and form only a small part of my work.	

Content

Is your work complete? Have you included all the required elements?

Ite	Action	Done
1	I have given an analysis of problem.	
2	I have explained why I chose the strategic tools that I have used and used references to support my decisions.	

CYBER SECURITY ANALYSIS FOR SMARTFAB'S INDUSTRIES CONNECTED MANUFACTURING ECOSYSTEM

.

First A. Author, *Fellow, IEEE*, Second B. Author, and Third C. Author, Jr., *Member, IEEE*

Abstract—The report presents a detailed cybersecurity analysis of the connected manufacturing infrastructure of SmartFab industries. It examines the modern threats of cyber-physical systems (CPS) threats that include ransomware, advanced persistent threats, and IoT risks. Threat modelling was performed on IoT-enabled Computer Numeric Control (CNC) machinery, a cloud-based ERP system, and a predictive maintenance analytics system using the STRIDE framework. Results of the study highlight a secure network architecture that was suggested, a part of which includes network segmentation, encryption, IDS/IPS, access control, and resilience. To conclude, by providing strategic guidelines on continuous monitoring and patching, as well as the training of staff as a part of long-term operational security and robustness.

Index Terms— SmartFab, Cyber Security, CPS Manufacturing, STRIDE Threat Model, Cloud System

I. INTRODUCTION

SmartFab Industries is a fictional mid-sized production company specialising in precision parts used in the automotive industry (SmartFab, 2025). The company maintains the interconnected production system, which incorporates IoT-powered equipment, a cloud-hosted Enterprise Resource Planning (ERP) system, and AI-powered analytics. Such an ecosystem allows real-time monitoring of the performance, predictive maintenance, automatic inventory handling, and dynamic production scheduling. Although such developments bring greater efficiency, productivity, and more effective decision-making, they pose enormous threats when it comes to cybersecurity. The unification of oil and gas operational technology (OT) and information technology (IT) widens the risk of attack, exposing critical systems to ever-changing cyber threats. This report aims to evaluate those risks by analysing the active threat environment and developing a threat model of the systems.

II. Threat Landscape and Review

A. Characteristics of Connected Manufacturing Infrastructure

The infrastructures of connected manufacturing integrate the operational technology (OT) and the information technology (IT). It also produces an integrated situation that combines the workings of physical machinery and digital systems (Berardi, et al., 2023). OT systems, including industrial control systems and programmable logic controllers, are now connected to enterprise IT networks, permitting the free transfer of data and synchronised activities. One important characteristic is the use of IoT devices on the production floor to monitor and automate an area and to provide predictive maintenance. The gadgets gather sensor readings, monitor the performance, and cause automatic actions during operational variations. Generated data is usually stored and processed in cloud-based computing systems, thus data allows multi-level analytics, optimisation through AI, and distant collaboration. Cloud integration promotes scalability and accessibility, but with it comes a degree of dependency on third-party infrastructure (Almutairi & Sheldon, 2025). Moreover, remote access functionalities enable engineers and managers to keep track of systems, look at the dashboard, and modulate operations anywhere. Although these features increase efficiency, flexibility, and responsiveness in the systems tremendously, they also increase the potential attack surface, resulting in emerging cybersecurity issues in connected manufacturing systems.

B. The impact of Characteristics on Security Requirements

The nature of connected manufacturing infrastructures poses a highly demanding set of security requirements since their operations are safety-critical in nature.

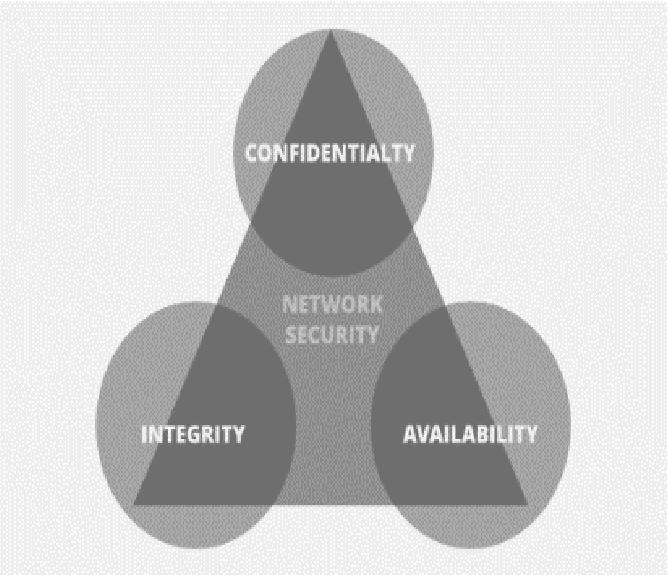


Fig. 1: Network Security (GeeksforGeeks, 2018).

Fig.1 shows that System integrity and availability can be as critical as data confidentiality in this type of situation. A cyber-event could halt production, including damaging machinery and equipment or impairing employee safety. These demands are also increased by real-time operational constraints and sensitivity to latency. Manufacturing invariably involves real-time, time-sensitive control communications between sensors, controllers, and equipment. The outage or interruption (either generated by a cyber-attack or a systems malfunction) can lead to costly production losses or dangerous situations. There are also the multi-layered attack surfaces that are formed through the combination of disparate components. Each of these, including sensors, industrial controllers, communication, cloud platforms, and remote access interface, has its vulnerability, which can be exploited by adversaries (Pedreira, et al., 2021). Hackers can exploit vulnerable situations in the IoT firmware, alter the controls, or just capture data between devices in transmission.

C. Current Threat Landscape in CPS Manufacturing

The global manufacturing industry of cyber-physical systems (CPS) is hit by an extremely dynamic threat situation as the attackers exploit both the cyber and physical risks. The typical vulnerabilities are viruses and ransomware that could either encrypt the data or interrupt control systems, triggering system downtime and numerous expenses. State-sponsored Advanced Persistent Threats (APTs) present a significant potential threat in the long run (Yusof, 2024). They can integrate into networks without being noticed to steal intellectual property or sabotage vital infrastructure. Supply chain attacks use vulnerabilities present in third-party components, software updates, or third-party access, whereas insider abuse can be done by deliberately disabling security or accidentally breaking security. Direct attacks on actual physical attack, e.g., tampering with sensors or mechanical attempts, are still a problem in CPS conditions.

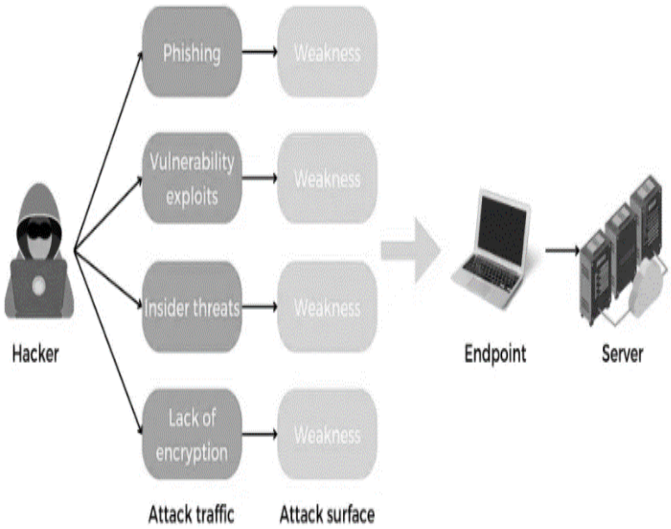


Fig. 2: Cyber Attacks Vectors (Dilmegani, 2025).

Fig. 2 shows that Network exploitation is done by finding a vulnerable, insecure protocol or a poorly configured firewall. In these exploitations, ERP application systems or manufacturing execution software vulnerabilities may also be used as a hiding place by attackers. IoT firmware attacks use vulnerable authentication or unpatched systems so that the industrial equipment can be manipulated. Phishing and spear-phishing are forms of social engineering that exploit human individuals in order to divulge credentials or permit access to the system.

These threats can be illustrated through a number of headline-making cases. In 2017, the NotPetya ransomware attack caused destruction to the manufacturing processes of companies around the world and resulted in losses of hundreds of millions of dollars (Lubin, 2021). In 2021, a ransomware attack was one of the largest automotive suppliers, of a reduction of 71% indicating both financial and operational costs of downtime (Blackkite, 2021). The malware had the potential to cause physical destruction of industrial equipment via cyber-attacks. The consequences of such incidents would highlight the need to practice evident segmentation between IT and OT networks, frequent patching, the quality of access control, and contingent employee awareness practices.

D. CPS Threats vs Traditional IT Threats

The nature of cybersecurity threats, goals, and consequences between Cyber-Physical Systems (CPS) and traditional IT systems is distinct, even though a few similar cybersecurity issues are found between them. In a classical IT landscape, the attacks are usually targeted at either data confidentiality, financial reward, or service abuse. In CPS manufacturing, the ultimate goals, however, might be physical destruction, production shutdown, or the interference of safety-critical processes. This makes risk prioritisation shift more to safeguarding of systems' integrity, availability, and continuity of operation rather than simple data confidentiality.

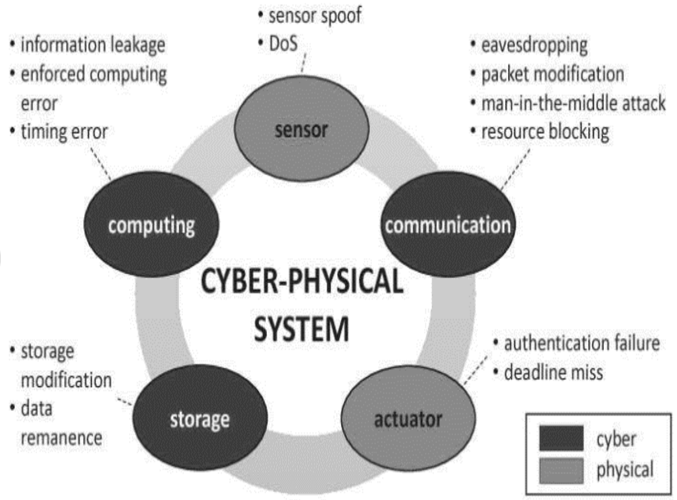


Fig 3: Attack surface of Cyber-Physical System (CPS) (Onik, et al., 2019).

Fig. 3 shows that Physical processes being integrated also create new CPS vulnerabilities that do not pose a threat in purely digital systems. As an example, compromising a programmable logic controller (PLC) may change the way the machine behaves, resulting in flawed products, equipment failure, or safety compromises. In contrast to IT systems, the constituents of CPS must be real-time responsive with low latency, and time lag should not be a prominent feature (Habib & Chimsom., 2022). In addition, CPS infrastructures may include legacy OTs with old security controls, thereby exploitable. Threats, once breached, can spread to not only the digital but also the physical layer of operation, to increase their impact. As a result, the cybersecurity of CPS must have a dual aim, protecting digital assets and the physical processes. They regulate in order to maintain both operational safety and resilience to the changing threats.

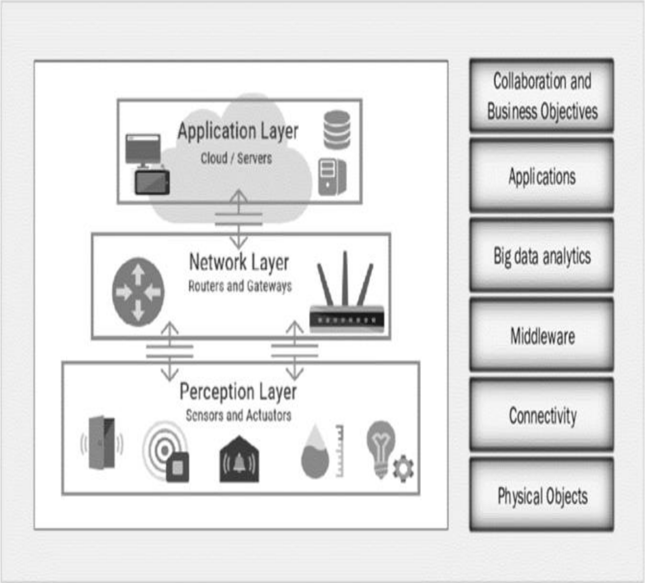
E. Summary of Threat Review

The shift of SmartFab to a connected manufacturing ecosystem presents new risks in terms of cyber risks. IoT devices, cloud ERP, and AI analytics integration also widen the attack surface, exposing the company to the risk of ransomware, advanced persistent threats, supply chain attacks, and insider abuse. Exposure is further compounded by weak firmware on IoT devices, unpatched systems, and insecure network settings. Manufacturing processes are sensitive to threats, which means that any slight disruptions can have significant operational and safety consequences. These threats require threat modelling, including the IT-OT interdependencies and multi-layered CPS vulnerabilities, before providing a secure design with robust artefacts, strong access control, and constant monitoring to protect the operations and assets.

III. Threat Modelling

A. CPS Architecture of SmartFab at high-level

Cyber-Physical System (CPS) SmartFab architecture will be defined in several layers, with each layer accomplishing some roles during manufacturing operations.



Fig, 4: SmartFab's Cyber-Physical System (CPS) Architecture Layers (Tavana, et al., 2020)

Fig.4 shows that the bottom layer is the sensor/actuator layer that consists of machinery and smart sensors and controls real-world processes in real time, enabled by IoT. Higher will be the control layer that may contain industrial controllers like Programmable Logic Controllers (PLCs) and Supervisory. Control and Data Acquisition (SCADA) computer systems that will execute automated instructions and maintain process stability.

Operational data in the control lay will be gathered to be analysed at the data processing layer. Predictive health maintenance systems run on AI, which will detect anomalies in the performance and will predict equipment failure (Calabrese, et al., 2021). The processed information will be relayed to the cloud-based ERP system that allows integrating manufacturing information and maintenance of supply chain, inventory, and business management. The remote user interface layer will allow the engineers, managers, and executives to access dashboards and analytics safely and wherever they are.

Connections between OT and IT environments will be connected via secure gateways and firewalls, where data can move between shop-floor equipment (OT) and cloud and enterprise systems (IT) without a loss of safety. Such connections will allow end-to-end visibility, but they will pose a potential attack surface and will require segmentation and security controls, as part of the system design.

B. Selection of Critical Component for Analysis

Threat modelling has chosen three critical components as they are key to SmartFab connected manufacturing processes and the ramifications that occur once they are breached.

1) IoT-enhanced CNC machining Equipment

IoT-enhanced CNC machining equipment will be part of the central production processes. It will be based on particularly accurate automated control, and a breakage might stop the manufacturing process or spoil materials, or it may affect the quality of products (Pandey, et al., 2023). Being directly linked with the network, it will also be prone to the threats aimed at IoT devices and industrial processes.

2) Cloud-Based EPR

The cloud-based ERP will mix production information with purchasing, stock, and supply chain control (Chinta, 2022). It will be the working frame of decision-making and coordination. The breach may lead to loss of data, the interruption of business operations, and competitive advantage.

3) Predictive Maintenance Analytics

The predictive maintenance analytics platform will schedule maintenance and predict equipment breakdowns, and directly affect efficiency and uptime. The manipulation of its outputs will cause some unnecessary downtime or disastrous equipment failure.

The above components will be selected on the basis of their being high-value targets that are operationally and financially important. Failure to protect any of them may propagate to affect all production or business processes within SmartFab; thus, such would be of high priority to undergo a comprehensive assessment of threats using the STRIDE framework.

C. STRIDE-Based Modelling for Each Component

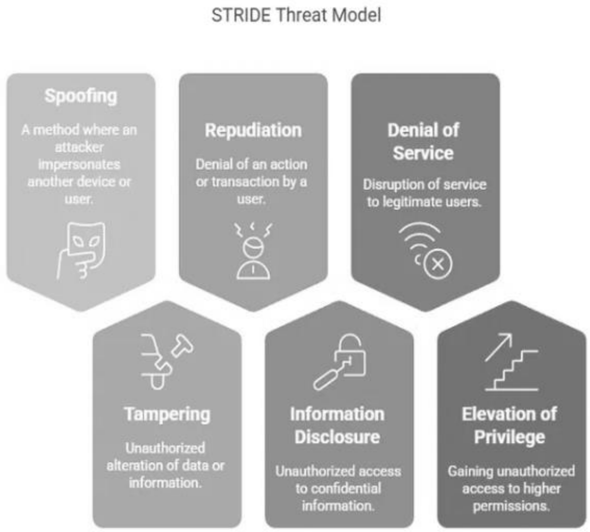

STRIDE Threat Model
Spoofing
A method where an attacker impersonates another device or user.
Repudiation
Denial of an action or transaction by a user.
Denial of Service
Disruption of service to legitimate users.
Tampering
Unauthorized alteration of data or information.
Information Disclosure
Unauthorized access to confidential information.
Elevation of Privilege
Gaining unauthorized access to higher permissions.

Fig 5: STRIDE Threat Model (Charlie Klein, 2025).

Fig. 5 shows that the STRIDE Threat Model is an organised method to detect and classify many security threats in software systems. This model was created by Microsoft to have teams methodically examine potential threats; it subdivides them into six categories:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service (DoS)
- Elevation of Privilege

1) CNC Machining Smart Equipment

Spoofing: Insertion of an invalid sensor measurement, hence erroneous machining parameters.

Tampering: Hiding machine control commands to create defective parts or damage the equipment.

Repudiation: Scarcity of enough logging, which enables malicious deeds by the attackers (Javed, et al., 2023).

Information Disclosure: interception of machining codes in the transfer of information.

Denial of Service (DoS): Loading the control network to a level that will stop production.

Elevation of Privilege: The use of the weakness in IoT firmware to attain administrative rights on the controllers.

2) Cloud-based ERP system

Spoofing: the use of hacking credentials to pretend to be authorised users.

Tampering: It can entail altering the inventory or monetary information, disturbing planning in the supply chain.

Repudiation: Risks are exposed in the case of auditing trails that are not complete, so that any undesirable changes can be made without accountability.

Information Disclosure: It may include customer information theft, supplier agreements, and production plans.

Denial of Service (DoS): The DoS attacks might render the ERP platform unreachable, halting the business (Efe, 2024).

Elevation of Privilege: It could include various attacks on the application, trying to get administrative rights.

3) Predictive maintenance analytics platform

Spoofing: It may involve providing incorrect performance info to AIs to produce erroneous maintenance plans (Androjna, et al., 2021).

Tempering: It may include the manipulation of algorithms to cause unnecessary shutdowns.

Repudiation: The risks involve the impossibility of verifying logs concerning changes to the model. Information Disclosure: It may include a spill of information on the performance of operations.

Denial of Service (DoS): The DoS attacks might result in the inability to get timely maintenance notifications, thus creating a likelihood of equipment failure.

Privilege Escalation: It could be possible that the analytics server is compromised, so that all systems connected could be controlled.

D. Threats Reasoning

The threats that were identified have different likelihoods and potential business impacts, and all have to be prioritized to inform the selection of mitigation strategies. Spoofing and tampering of SmartFab threat ranks highly because the IoT-connected CNC machinery is a basic operating system functionality exposed to the network, and firmware lacks many security measures. These attacks might lead to poor production quality, equipment destruction, and major idle time, which translates to direct sales and consumer confidence. Information disclosure and escalation of privilege pose a danger to the cloud-based ERP system (Alwaheidi & Islam, 2022). A successful penetration may reveal commercially valuable information or give the attacker control over critical operations, which interferes with the supply chain. These threats are not very common, as the basic malware is; however, they pose serious financial and reputational effects.

Examples of the moderate threats that are likely to affect this predictive maintenance analytics platform are spoofing of performance data, which may result in wrong maintenance scheduling. Although they do not cause dire effects instantly, these risks may lead to inefficiency in operations in the long run or sudden breakdowns. With a criterion based on this valuation, the highest priorities should be the securing of IoT devices, segmentation of networks to minimize vectors of attack, hardening the ERP access controls, and integrity checks of input into analytics. The high-impact, high likelihood threats will achieve the most significant overall reduction in the level of cyber risks faced by SmartFab.

IV. Secure Design and Countermeasures

A. Secure Network Design for SmartFab

A strong, secure network design is imperative to protect the manufacturing environment in SmartFab against internal and external threats through the network connection.

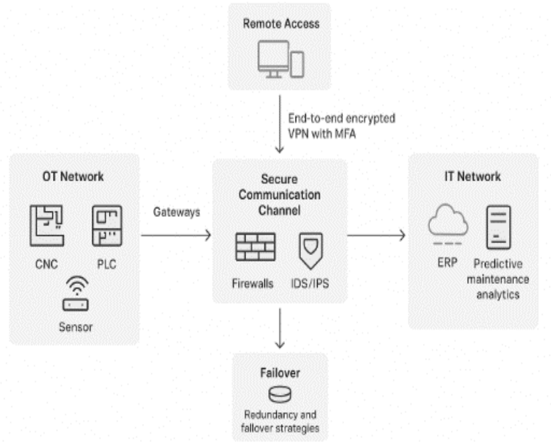

Remote Access
End-to-end encrypted VPN with MFA
OT Network
CNC
PLC
Sensor
Gateways
Secure Communication Channel
Firewalls
IDS/IPS
IT Network
ERP
Predictive maintenance analytics
Failover
Redundancy and failover strategies

Fig 6: Secure Network Design for SmartFab

Fig.6 shows that the network starts with an explicit distinction in Operational Technology (OT) and Information Technology (IT) networks (Felser, et al., 2019). OT machines (they include CNC machines, PLCs, sensors) do their work in a separate, segmented zone of the network. OT-IT communication channel is implemented by secure gateways deployed with firewalls, intrusion detection/prevention systems (IDS/IPS), and access control policy. This segregation minimizes the threat of cross-infection by adversaries and isolates possible breaches by dragging the potential breach to isolated zones.

The ability of engineers and managers to monitor systems and make changes remotely is important and requires secure remote access. An end-to-end encrypted Virtual Private Network (VPN) with Multi-Factor Authentication (MFA) is also available to secure remote connections and identify users (Otta, et al., 2023). This reduces the chances of stolen credentials and unauthorized access to sensitive systems by unauthorized users. Planners also use redundancies and failover plans to provide essential components like ERP servers, control systems, and network gateways with a means of ensuring continuity of operations in the event of failures. Guaranteed fast recovery to the secondary data centres is provided by using redundant paths on the network, spare power back-ups, and mirrored systems that can facilitate a quick switch over, in case of hardware failure, cyberattacks, or any disruptive event.

The design makes SmartFab intrinsically stronger in terms of security and ensures continuity of manufacturing operation by way of network segmentation, secure access control, and resilient infrastructure. It also falls under best practices in ISA/IEC 62443 and NIST Cybersecurity Framework, which guarantees compliance and strong defence against emerging cyber threats.

B. Justification for Design

The suggested secure network architecture of SmartFab complies with the standards on industrial automation and control systems security, ISAIEC 62443, and the NIST Cybersecurity Framework. ISA/IEC 62443 focuses on network segmentation and least privilege as well as layered defences that boil down to OT and IT network separation, controlled gateways, and access controls based on roles (Cindrić, et al., 2025). In the same way, the identification, protection, responding, and recovering are core areas of NIST framework that can be translated into intrusion detection/intrusion prevention systems, VPN with MFA access facilities, and redundancy to provide a quick recovery.

Cost-wise, the design always strikes a balance between good security and efficient operation. Secure gateways and network segmentation leverage as the existing infrastructure, and fewer hardware upgrades are needed. VPN and MFA are less costly to implement than the possible losses when production stops, or a cyber-attacker hacks your data.

IoT devices or production lines can also be added to the segmented network zones, not affecting the ongoing operations. Resource scalability as businesses increase demands is possible with cloud-based ERP and analytics (Gooda, et al., 2025). Although redundancy plans should also be developed to provide the benefits of those resiliency measures with the newest systems. The approach focuses on ensuring the operational feasibility within constraints. The implementation does not impact the manufacturing process as far as possible by means of phased deployment and by ensuring that security measures are compatible with current OT equipment. Remote access can allow persistent operational control during a maintenance or upgrade period without affecting safety or control when it is done securely.

The design will be a viable, future-proof, and highly scalable security solution that aids the effectiveness of operations and is a cost-efficient solution that makes SmartFab more resilient to the current and future cyber-physical challenges.

C. Countermeasure Strategies and Implementation

Multi-layered defence system should be adopted to defend the SmartFab connected manufacturing ecosystem against various threats in cyberspace. The next stage has identified some countermeasures that are critical in achieving system integrity, availability, and confidentiality, as well as reducing operational friction.

1) Network segmentation

Network segmentation segregates the high-risk modules of the infrastructure from the rest of it to avert any type of lateral movement caused by the hacker. In a design in SmartFab, the Operational Technology (OT) systems, like IoT-enabled CNC machines, PLCs, and industrial sensors, are coupled to a different network zone than Information Technology (IT) systems (Kasiviswanathan, et al., 2024). They are incorporating the ERP and cloud analytics systems. Data flow between the segments is controlled by the use of controlled gateways and firewall rules. This lowers the chances of a breach in one zone finding its way to other zones, as well as offers an improved containment of incidents.

2) Cryptography

Communication channels, as well as the data that is stored, are secured via cryptographic measures. Data during transit between OT devices, cloud systems, and remote access points will use end-to-end encryption (e.g., TLS 1.3) (Zhou, et al., 2024). So that intercepted messages will not be usable and remain unreadable and unmanipulable. Information that is held at rest, including manufacturing specifications, operation log, and analytic output, is secured through tough encryption such as AES-256. Major management practices are centralised and guarded by stringent access controls lest they be misused.

3) Vulnerability Scanning and Patch Management

Through frequent vulnerability scans, IoT firmware, industrial control systems, and ERP applications identify weaknesses (Bakhshi, et al., 2024). The use of automated scanning tools as well as manual reviews is an excellent way to keep exploitable holes at bay. Upon identification, vulnerabilities get prioritized with the most severe addressed first and patched as soon as possible, but using a controlled change management process that does not interfere with production. This preventive measure limits the attack surface by a considerable margin and minimizes threats of known exploits.

4) Intrusion Detection and Prevention System

Intrusion Detection and Prevention Systems (IDP/IPS) are installed on major network entry points to analyse the traffic and look for anomalous behaviour, malicious access attempts, and patterns of recognised attacks (Chang, et al., 2022). Anomaly-driven detection plays a vital role in OT settings where it can detect a behavior outside the normal operation, including unanticipated machine commands or unusual sensor readings. Automatic detection of malicious activity, followed by blocking the offending traffic by IPS components, can either prevent damage or disruption.

5) Access Control and Authentication

Access control is very strict and based on Role-Based Access Control (RBAC). So that only systems that they require according to their functions can be used. Multi-Factor Authentication (MFA) provides a second measure of security to all privileged (Ometov, et al., 2018). The remote accounts create a hard layer of security that seriously limits the potential of stolen credentials, resulting in unauthorized access to an account. Least-privileged principles are used to eliminate privileged escalation, and administrative rights are introduced on a need basis only, and those administrative rights are monitored carefully.

6) Security Awareness Training

The issue of security breaches due to human error is one of the most widespread. Security awareness training is routinely offered to every employee at every level, complete with identifying phishing, good password habits, and proper handling of sensitive information. Training sessions are held specifically on OT systems with the staff and centre on the industrial needs specific to cybersecurity (Hatzivasilis, et al., 2020).

By applying these countermeasures in a joint manner, SmartFab can have a layered security in place that is able to cover technical and human vulnerabilities. This consolidated defence serves not only to safeguard against the present threats but also establishes a sturdy security stance that has a chance at evolving against changing dangers to the manufacturing sector.

D. Linking Countermeasures to Threat

The countermeasures in SmartFab secure network design should be made directly to respond to the threats of the STRIDE analysis, and each of the respective risks is countered.

Spoofing: Strong authentication mechanisms, like Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC), will prevent spoofing threats, because spoofing entails false inputs on sensor values, or stolen credentials (Abduhari, et al., 2025). Communications will also be encrypted so that intercepted credentials or information should not be usable to impersonate.

Tempering: Network segmentation and encrypting data on transit will minimise the danger of tampering, an unauthorised alteration of the machine control commands or ERP records. Integrity checks and change management procedures are also effective in avoiding detection and prevention of unauthorized changes.

Repudiation: The threat of repudiation will be addressed by using specific logging and a safer audit trail in OT and IT systems. The records will not be edited and are associated with the verified user activities, so they can be held accountable.

Information Disclosure: It may involve theft of proprietary data or production schedules. This will be mitigated by encryption of stored and transferred data, tight control of access to data, and patching of known vulnerabilities to eliminate any exploitable holes.

Denial of Service (DoS): DOS attacks, which may cause production to stop or ERP services to be unavailable, will be deterred by an intrusion detection/prevention system (IDS/IPS) that will block the traffic (Wang, et al., 2025). The use of redundancy and failover plans keeps operations going in the event of an incident.

Elevation Privilege: Continuous vulnerability scanning will identify exploitable vulnerabilities before being used to escalate access by the attacker counter the EoP threats.

Through a mapping of every STRIDE , SmartFab also offers a fully layered defence-in-depth approach to cybersecurity. It also minimising the risk and severity of cyber incidents and still allowing the business to operate resiliently.

E. Residual Risks and Improvement

Strong security cannot prevent some threats. The defences can still be evaded by zero-day vulnerabilities, advanced persistent threats (APTs), and insider misuse (Zhang & Tenney, 2023). Also, patching or replacement may be constrained by operational requirements and inherent legacy OT infrastructure. The residual risks can only be dealt with through constant monitoring of network traffic, system logs, and user activity. Periodic security tests are able to detect new vulnerabilities, whereas incident response training is useful in ensuring the team is ready to manage. Incorporating an adaptive security posture will allow SmartFab to change its defence measures according to the shifting threat environments and preserve long-term business and operational resilience.

V. Conclusion

In conclusion, the evaluation proposed that SmartFab faces high risks of cyber hacking during its move to smart manufacturing, such as ransomware, supply chain, ERP systems, and predictive analytics-based platforms. STRIDE threat modelling revealed high priorities in attack vectors and helped inform the drafting of a secure network architecture built around segmentation, encryption, IDS/IPS, and other strong access controls. These precautions place SmartFab in a firm security footing of connected operations. Yet, resilience needs constant observation, prompt patching, in-time audits, and employee training on awareness in order not to be broken. Planned investments in adaptive defences and equipping Incident preparedness will make SmartFab a secure and competitive company in a changing cyber-physical threat environment.

Acknowledgment

I would like to thank my mentors, colleagues, and peers once again because of their effective guidance and helpful feedback. They support me during the research and the preparation of this cybersecurity review which has significantly contributed to the readability, richness, and the quality of this work.

Bibliography

1. Abduhari, E. S. et al., 2025. "Access Control Mechanisms and Their Role in Preventing Unauthorized Data Access: A Comparative Analysis of RBAC, MFA, and Strong Password. Natural Sciences Engineering and Technology Journal, 5(1), pp. 1-13.
2. Almutairi, M. & Sheldon, F. T., 2025. IoT–Cloud Integration Security: A Survey of Challenges, Solutions, and Directions. Electronics, 14(7), p. 1394.
3. Alwaheidi, M. K. & Islam, S., 2022. Data-driven threat analysis for ensuring security in cloud-enabled systems. Sensors, 22(15), pp. 1-24.
4. Androjna, A., Perkovič, M., Pavic, I. & Mišković., J., 2021. AIS data vulnerability indicated by a spoofing case study. Applied Sciences, 11(11), p. 5015.
5. Bakhshi, T., Ghita, B. & Kuzminykh, I., 2024. A review of IoT firmware vulnerabilities and auditing techniques. Sensors, 24(2), pp. 1-28.
6. Berardi, D. et al., 2023. When operation technology meets information technology: challenges and opportunities. Future Internet, 15(3), p. 95.
7. Blackkite, 2021. RANSOMWARE RISK: AUTOMOTIVE MANUFACTURING IN 2021. [Online]
8. Available at: https://blackkite.com/wp-content/uploads/2021/06/Ransomware-Risk-_-Automotive-Manufacturing-in-2021.pdf
[Accessed 10 August 2025].
9. Calabrese, F. et al., 2021. Predictive maintenance: A novel framework for a data-driven, semi-supervised, and partially online prognostic health management application in industries. Applied Sciences, 11(8), pp. 1-28.
10. Chang, V. et al., 2022. "A survey on intrusion detection systems for fog and cloud computing. Future Internet, 14(3), p. 89.
11. Charlie Klein, 2025. STRIDE Threat Model: A Complete Guide. [Online]

12. Available at: https://www.jit.io/resources/app-security/stride-threat-model-a-complete-guide [Accessed 10 August 2025].
13. Chinta, P. C. R., 2022. Enhancing Supply Chain Efficiency and Performance Through ERP Optimisation Strategies.. Journal of Artificial Intelligence & Cloud Computing, 1(4), pp. 1-7.
14. Cindrić, I., Jurčević, M. & Hadjina., T., 2025. Mapping of Industrial IoT to IEC 62443 Standards. Sensors (Basel, Switzerland), 25(3), p. 728.
15. Dilmegani, C., 2025. Most Common Cyber Attack Vectors in 2025. [Online]
16. Available at: https://aimultiple.com/most-common-cyber-attack-vectors [Accessed 10 August 2025].
17. Efe, A., 2024. Risk modelling of cyber threats against MIS and ERP applications. Pamukkale Üniversitesi İşletme Araştırmaları Dergisi, 11(2), pp. 1-18.
18. Felser, M., Rentschler, M. & Kleineberg., O., 2019. Coexistence standardisation of operation technology and information technology. Proceedings of the IEEE, 107(6), pp. 1-5.
19. GeeksforGeeks, 2018. What is the CIA Triad?. [Online] Available at: https://www.geeksforgeeks.org/computer-networks/the-cia-triad-in-cryptography/ [Accessed 10 August 2025].
20. Gooda, S. K. et al., 2025. Cloud-Based Solutions for Scalable Enterprise Resource Planning Systems: Benefits and Implementation Strategies. ITM Web of Conferences, 76(1), pp. 1-11.
21. Habib, M. K. & Chimsom, C., 2022. CPS: Role, characteristics, architectures, and future potentials. Procedia Computer Science, 200(1), pp. 1-12.
22. Hatzivasilis, G. S. I. M. S. et al., 2020. Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. Applied Sciences, 10(16), pp. 1-26.
23. Javed, H. et al., 2023. "Blockchain-based logging to defeat malicious insiders: The case of remote health monitoring systems.. IEEE Access, 12(1), pp. 1-18.
24. Kasiviswanathan, S., Gnanasekaran, S., Thangamuthu, M. & Rakkiyannan, J., 2024. Machine-learning and Internet-of-Things-driven techniques for monitoring tool wear in the machining process: a comprehensive review. Journal of Sensor and Actuator Networks, 13(5), p. 53.
25. Lubin, A., 2021. Public policy and the insurability of cyber risk. JL & Tech. Tex, 5(1), pp. 1-65.
26. Ometov, A. et al., 2018. Multi-factor authentication: A survey.. Cryptography, 2(1), pp. 1-31.
27. Onik, M. M. H., KIM, C.-S. & Yang, J., 2019. Personal Data Privacy Challenges of the Fourth Industrial Revolution. International Conference on Advanced Communication Technology (ICACT, 1(1), pp. 1-9.
28. Otta, S. P., Panda, S., Gupta, M. & Hota, C., 2023. "A systematic survey of multi-factor authentication for cloud infrastructure. Future Internet, 15(4), p. 146.
29. Pandey, V. K. et al., 2023. Machine Learning algorithms and fundamentals as Emerging Safety Tools in Preservation of fruits and vegetables: a review.. Processes, 11(6), pp. 1-17.
30. Pedreira, V., Barros, D. & Pinto, P., 2021. A review of attacks, vulnerabilities, and defenses in Industry 4.0 with new challenges on data sovereignty ahead. Sensors, 21(151), pp. 1-21.
31. SmartFab, 2025. Discover, understand, and act faster on the insights hidden in your production data. [Online] Available at: https://www.smartfab.ai/ [Accessed 10 August 2025].
32. Tavana, M., Hajipour, V. & Oveisi, S., 2020. IoT-based enterprise resource planning: Challenges, open issues, applications, architecture, and future research directions. Internet of Things, 11(1), pp. 1-10.
33. Wang, F. et al., 2025. A Survey of Integrated Multi-Layer Security for Continuous-Process Industrial Control Systems: Insights from a Steel Manufacturing. SSRN, 1(1), pp. 1-41.
34. Yusof, Z. B., 2024. Exploration of advanced persistent threats: techniques, mitigation strategies, and impacts on critical infrastructure.. International Journal of Advanced Cybersecurity Systems, Technologies, and Applications, 8(12), pp. 1-9.
35. Zhang, J. & Tenney, D., 2023. The evolution of integrated advanced persistent threat and its defence solutions: A literature review.. Open Journal of Business and Management, 12(1), pp. 1-46.

Assignment Checklist

Run through this simple tick list before submitting your work!

Report

Well prepared materials make your work look more professional and easier to understand.

Item	Action	Done?
1	I have used the spellchecker and proofread the work correcting errors several times.	✓
2	I have checked that all material is directly related to the assignment tasks.	✓
3	I have checked that all the required information has been included in the work.	✓
4	The work is professionally presented using consistent headings, fonts and layout.	✓
5	All tables and images are numbered and captioned.	✓
6	I have used the structure specified in the assignment.	✓

Referencing and Originality

Your work will be subjected to checks to ensure it is not copied. Derivative work may leave you subject to penalties, including in extreme cases, expulsion from the University.

Item	Action	Done
1	All images and tables are fully referenced.	✓
2	I have not copied any material from anywhere else. All sentences have been paraphrased into my own words.	✓
3	All references appear in the references section at the end of the presentation.	✓
4	All references are cited in the text in the form of (author, year). See https://www.bcu.ac.uk/library/services-and-support/referencing for more details.	✓
5	If I have used quotes, these are fully referenced, appear in quotation marks and form only a small part of my work.	✓

Content

Is your work complete? Have you included all the required elements?

Ite	Action	Done
1	I have given an analysis of the problem.	✓
2	I have explained why I chose the strategic tools that I have used and used references to support my decisions.	✓