

FINAL SUBMISSION-2500527

by Tuscany Crowther-Snow

Submission date: 09-Jan-2026 03:45AM (UTC+0000)

Submission ID: 272625364

File name: 66771_Tuscany_Crowther-Snow_FINAL_SUBMISSION-2500527_712285_1469944980.docx (1.08M)

Word count: 3018

Character count: 17109



Cyber Risk and Computer System design

Computer systems fundamentals

B.Eng (Hons) Embedded Electronic systems

B.Eng (Hons) Electrical and Electronic Engineering



Tuscany Crowther-Snow
2500527

Table of contents//

section	pages
Task 1	
Component list	3-5
Shopping list (table)	6-15
Task 2	
introduction	16
Risk and impact analysis	16-17
Risk protection	18
Holistic identification	19
Incident identification plan	20
Applicable cybersecurity standards	21
Summary	21
bibliography	22

Task 1:

CPU: Intel Core i7-13700

This CPU would be the perfect  choice due to its reliable single core performance, as well as its high multi core capacity. The software named in the brief (SolidWorks, PSpice, LabVIEW etc) will need fast individual cores for accurate interaction, as well as simulations and background tasks which the multi-thread processors will be able to handle with ease. This CPU is perfect for multitasking without degrading the performance of the computer.

It also has a much better processing capability compared to other mid-range processors (Intel core i5, Ryzen 5 etc).  Although there are more powerful high-end CPUs available (Core i9), they are much  higher in price, and the i7 is powerful enough for the tasks required in the brief.

Motherboard: Intel Z790 ATX

This motherboard provides a stable  form compatible with 13th-generation intel processors. It supports DDR5 memory, multiple expansion slots, and modern connectivity options, ensuring long-term convenience and upgrade potential.

In comparison to other chipsets, the Z790 offers better power delivery and expandability, making it more suitable for professional workloads, without the cost of higher-end alternatives. 

RAM: 32GB DDR5

I have chosen 32GB of DDR5 RAM to accommodate the memory-intensive applications and multitasking that engineering work entails. CAD software will require a large amount of memory, especially when handling intricate design.

Although 16GB might be adequate for basic work-from-home setups, it may limit the performance of engineering software. On the other hand, 64GB would be excessive for the tasks named in the brief. DDR  memory also has higher efficiency compared to DDR4.

Storage: 1TB NVMe SSD, 2TB HDD.

The NVMe SSD will provide fast boot times and rapid access to software and projects which will improve the overall productivity. The 2TB HDD secondary storage offers cost-effective storage for archives.

The mix of storage will be more effective than HDD-only systems and more economical compared to large-capacity SSDs alone.

Input/output ports:

The system will include USB-C, USB-3.2, DisplayPort, audio ports, and gigabit Ethernet. These will support multiple peripherals, dual-monitor setups and reliable audio/video communication.

This configuration is more flexible and efficient compared to systems with limited I/O.

GPU: NVIDIA RTX 3060

This GPU provides dedicated graphics processing that enhances rendering and visual performance in SolidWorks and similar software. It will allow smooth interaction with complex schematics and supports high-res displays.

Integrated graphics lack sufficient performance for CAD software, while higher end GPUs may offer higher performance, but at a much higher cost. The RTX3060 is a perfect balance between performance and affordability.

Case/power supply: Mid Tower ATX and 750W 80+ gold PSU

This mid-tower case ensures good air flow and thermal control for sustained workloads. The power supply delivers reliable and efficient power, supporting current components and potential upgrades.

Lower rated power supplies might compromise stability, while higher-wattage units are unnecessarily for this setup.

Monitor/peripherals: 27-inch QHD IPS display

This monitor provides a large, high-resolution display suitable for detailed software and simulations. Compared to full HD monitors, it improves productivity and reduces eye strain.

A 1080p webcam, ergonomic keyboard, and precision mouse will support effective communication and long-term comfort during extended work sessions.

Network connectivity:

Gigabit Ethernet ensures a stable a high-speed wired connection for video calls and file transfers, while Wi-Fi 6 provides a fast and reliable wireless alternative. This dual-connectivity approach improves reliability compared to wireless-only systems.

Required software:

Windows 11 Pro is perfect for its compatibility with engineering software and enhanced security features. Engineering applications and professional-grade security software ensure a secure, efficient and collaborative work environment.



Conclusion:

This specification presents a balanced and cost-effective desktop environment tailored to the graphical, technical, and security requirements of a work-from-home Electrical Engineer. Each component has been selected to maximise performance and reliability while avoiding unnecessary cost and complexity.

Component name	Image	Specification	Price
Intel core i7-13700		Manufacturer Intel Part # - BX8071513700K - i7-13700K Series Intel Core i7 Microarchitecture Raptor Lake Core Family Raptor Lake Socket LGA1700 Core Count 16 Thread Count 24 Performance Core Clock 3.4 GHz Performance Core Boost Clock 5.4 GHz Efficiency Core Clock 2.5 GHz Efficiency Core Boost Clock 4.2 GHz L2 Cache 24 MB L3 Cache 30 MB TDP 125 W Integrated Graphics Intel UHD Graphics 770 Maximum Supported Memory 192 GB ECC Support Yes Includes Cooler No Packaging Boxed Lithography 10 nm Includes CPU Cooler No Simultaneous Multithreading Yes: Hyper-Threading	£349.99
MSI MAG Z790 TOMAHAWK WIFI ATX LGA1700 Motherboard		Manufacturer MSI Part # - MAG Z790 TOMAHAWK WIFI 7D91-009R	£179.99

		• 911-7D91-010 Socket / CPU LGA1700 Form Factor ATX Chipset Intel Z790 Memory Max 256 GB Memory Type DDR5 Memory Slots 4 Memory Speed • DDR5-4800 • DDR5-5000 • DDR5-5200 • DDR5-5400 • DDR5-5600 • DDR5-5800 • DDR5-6000 • DDR5-6200 • DDR5-6400 • DDR5-6600 • DDR5-6800 • DDR5-7000 • DDR5-7200 Color Black PCIe x16 Slots 2 PCIe x1 Slots 1 M.2 Slots • 2260/2280/22110 M-key • 2260/2280 M-key • 2242/2260/2280 M-key • 2242/2260/2280 M-key • 2230 E-key SATA 6.0 Gb/s Ports 7 Onboard Ethernet 1 x 2.5 Gb/s Ports (Intel) Onboard Video Depends on CPU USB 2.0 Headers 2 USB 3.2 Gen 1 Headers 1 USB 3.2 Gen 2 Headers	
--	--	---	--

		1 Supports ECC No Wireless Networking Wi-Fi 6E RAID Support Yes Uses Back-Connect Connectors No	
(RAM) 32 GB (2x16 GB) DDR5-6000		Manufacturer Kingston Part # KF556C36BBEK2-32 Speed DDR5-5600 Form Factor 288-pin DIMM (DDR5) Modules 2 x 16GB Price / GB £10.693 Color Black First Word Latency 12.857 ns CAS Latency 36 Voltage 1.25 V ECC / Registered Non-ECC / Unbuffered Heat Spreader Yes	£194.20
Gigabyte AORUS Gen4 7300 1 TB M.2-2280 PCIe 4.0 X4 NVME Solid State Drive		Manufacturer Gigabyte Part # AG4731TB N Capacity 1 TB Price / GB £0.130 Type SSD Cache 1024 MB Form Factor M.2-2280	£129.95

		Interface M.2 PCIe 4.0 X4 NVME Yes	
Seagate Surveillance HDD 2 TB 3.5" 5400 RPM Internal Hard Drive		Manufacturer Seagate Part # ST2000VX003 Capacity 2 TB Price / GB £0.069 Type 5400 RPM Cache 64 MB Form Factor 3.5" Interface SATA 6.0 Gb/s NVME No	£137.50
NVIDIA Founders Edition GeForce RTX 3060 Ti 8 GB Video Card		Manufacturer NVIDIA Part # 900-1G142-2520-000 Chipset GeForce RTX 3060 Ti Memory 8 GB Memory Type GDDR6 Core Clock 1410 MHz Boost Clock 1670 MHz Effective Memory Clock 14000 MHz Interface PCIe x16 Color Black / Silver Frame Sync G-Sync Length 242 mm TDP 200 W	£529.00

		Case Expansion Slot Width 2 Total Slot Width 2 Cooling 2 Fans External Power 1 x PCIe 12-pin DisplayPort Outputs 3 HDMI Outputs 1	
Montech XR ATX Mid Tower Case		Manufacturer Montech Part # • XR-B • XR (B) Type ATX Mid Tower Color Black Power Supply None Side Panel Tempered Glass Power Supply Shroud Yes Front Panel USB • USB 3.2 Gen 2 Type-C • USB 3.2 Gen 1 Type-A Motherboard Form Factor • ATX • Micro ATX • Mini ITX Maximum Video Card Length • 420 mm • 16.535" Drive Bays • 2 x Internal 3.5" • 2 x Internal 2.5" Expansion Slots 7 x Full-Height Fan Support • Rear: 1 x 120 mm / 1 x 140 mm • Top: 3 x 120 mm / 2 x 140 mm • Motherboard Tray: 2 x 120 mm	£50.04

		• PSU Shroud: 3 x 120 mm Included Fans • Rear: 1 x 120 mm (ARGB PWM) • Motherboard Tray: 2 x 120 mm (Reversed ARGB PWM) Radiator Support • Rear: 140 / 120 mm • Top: 360 / 240 / 140 / 120 mm Dimensions • 435 mm x 230 mm x 450 mm • 17.126" x 9.055" x 17.717" Volume • 45.023 L • 1.59 ft³	
Segotep GM 750 W 80+ Gold Certified Fully Modular ATX Power Supply		Manufacturer Segotep Part # CP-PSU-ST-GM750 Type ATX Efficiency Rating 80+ Gold Wattage 750 W Length 140 mm Modular Full Color Black Fanless No ATX 4-pin Connectors 0 EPS 8-pin Connectors 2 PCIe 16-pin 12VHPWR/12V-2x6 Connectors 1 PCIe 12-pin Connectors 0 PCIe 8-pin Connectors 0 PCIe 6+2-pin Connectors 4	£84.99

		PCIe 6-pin Connectors 0 SATA Connectors 8 AMP/Molex 4-pin Connectors 3	
Microsoft Windows 11 Pro Retail - Download 64-bit		Manufacturer Microsoft Model Windows 11 Pro 64-bit (Download) Part # FQC-10572 Mode 64-bit Version Windows 11 Pro Maximum Supported Memory 2048 GB	£181.97
Gigabyte GC- WBAX210 802.11a/b/g/n/ac/ax PCIe x1 Wi-Fi Adapter		Manufacturer Gigabyte Part # GC-WBAX210 Protocol Wi-Fi 6E Interface PCIe x1 Color Black / Silver	£42.74
Asus TUF Gaming VG27AQ 27.0" 2560 x 1440 165 Hz Monitor		Manufacturer Asus Model TUF Gaming VG27AQ Part # • VG27AQ • 90LM0500-B01370 • 90LM0500-B03370 Screen Size 27" Resolution 2560 x 1440 Refresh Rate 165 Hz Response Time (G2G) 1 ms Panel Type IPS	£271.00

		Aspect Ratio 16:9 Color Black Brightness 350 cd/m² Pixel Pitch 0.233 mm Widescreen Yes Curved Screen No Frame Sync • FreeSync • G-Sync Compatible Built-in Speakers Yes Viewing Angle 178° H x 178° V Inputs • 1 x DisplayPort • 2 x HDMI	
Kensington Pro Fit Ergo Wireless Ergonomic Keyboard		Manufacturer Kensington Model Pro Fit Ergo Part # K75400US Style Ergonomic Mechanical No Layout English (US) Backlit None Tenkeyless No Connection Type Wireless Color Black Mouse Included No	£65.48

Razer Viper V3 Pro Wireless/Wired Optical Mouse		Manufacturer Razer Part # • RZ01-05120100-R3U1 • RZ01-05120100-R3A1 • RZ01-05120100-R3G1 Tracking Method Optical Connection Type • Wired • Wireless Maximum DPI 35000 Hand Orientation Right Color Black	£126.99
Creative Labs Pebble 2.0 4.4 W Speakers		Manufacturer Creative Labs Model Pebble 2.0 Part # 51MF1680AA000 Configuration 2.0 Total Wattage 4.4 W Frequency Response 100 Hz - 17 kHz Color Black Power (Front, Each) 2.2 W	£21.99
Anker PowerConf C200 Webcam		Manufacturer Anker Model PowerConf C200 Part # • A3369 • A3369011 Resolution • 2k • 1080p • 720p Connection USB 3.2 Gen 1 Type-C Focus Type Auto	£39.99

		Operating System • Windows • OS X FOV Angle 95° Focal Length 150 mm Sensor Pixels 5 MP Privacy Shutter Yes Built-In Lighting No	
--	--	--	--

 12 **cost: £2405.82**

Task 2:

Introduction:

Cybersecurity in a manufacturing company is vital, being the foundation for the safety of both the employees and the customers. With large-scale business comes lots of vulnerabilities, and attackers could easily take advantage of there in order to gain access to sensitive information. In order to keep attacks at bay, there are many different methods available to protect the company. In this report, I will be identifying different risks and impacts, as well as giving solutions and action plans to help keep cyber attacks to a minimum.

i: risk and impact analysis

 13 outdated firewall rules and lack of segmentation between corporate and operational systems, increasing the risk of unauthorised access.

Potential impact:  14

Without proper segmentation between the corporate and operational systems, the likelihood of external attackers or insiders gaining access to the internal systems greatly increases. If this happens, it would be easy for the attacker to move into industrial control systems, which would massively increase the scale of possible damage. As well at this, compromised operational systems could lead to disruption for production lines, deliveries, and financial loss, alongside the chance of making **operating conditions unsafe, which heightens risks for staff. All of this could then lead to legal consequences and penalties for the company.**

References: [1], [6]

Risk: embedded devices having outdated firmware and default passwords.

Potential impacts:

Attackers may be able to gain control of the embedded systems, meaning they can make changes to the devices or disable safety features. This could then cause the devices to make errors when taking measurements, or cause faulty outputs, leading to faulty products. If users passwords are compromised, important files and materials such as emails could be stolen, breaching the privacy of many people and this material could then be reused by competitors or sold on by attackers. Once again, this could then lead to legal consequences.

References: [6], [7]

Risk: components being sourced from international suppliers, some of which **don't** follow secure development or validation practices. 

Potential impacts:

As the suppliers aren't completely trustworthy, there is a risk of the suppliers introducing malicious code or hardware into the components to intentionally compromise the company. This code could cause the devices to malfunction, crash or even become completely inoperable. If they gain access of the devices, it may lead to other attacks such as DDoS attacks, as seen with the Mirai botnet in the past. A single vulnerable component could be used in multiple systems, causing a larger-scale risk. These risks can then reduce the trust of the customers, meaning that the company could lose money if they lose customers.

References: [3], [4]

Risk: workstations running outdated operating systems which **don't** receive secure development or validation patches. 

Potential impacts:

As the workstations don't have secure patches, the exposure to malware could increase. This could lead to files and data being encrypted, leaked or stolen. Also, if a workstation is compromised this could be a gateway into wider corporate and operational networks. Customer data could then be leaked or stolen, as well as their personal information such as email addresses and home addresses, which poses a risk to their safety.

References: [2], [8]

Risk: employees **haven't** received adequate cybersecurity training, leading to successful phishing attacks and increased risk of malware spreading within systems. 

Potential impacts:

Phishing attacks that are successful may lead to employees accidentally disclosing login details or sensitive information. Clicking malicious links can infect systems and compromised employee accounts may attack systems with trusted access. If employees' accounts are used to contact others, suspicious activity may not be recognised promptly, posing a serious threat.

References: [4], [9]

ii) Risk Prioritisation

Priority	Risk	Justification
High	Network segmentation weaknesses	Allows attackers to move from corporate to operational systems, potentially disrupting production, risking safety. This would impact the infrastructure greatly.
High	Outdated operating systems	Compromising unsupported operating systems can lead to malware and exploitation. This could lead to data loss and access to wider networks.
Medium/High	Embedded device vulnerabilities	Embedded devices can be exploited and interfere with the manufacturing process. Although it is serious, attacks are less frequent against workstations.
Medium	Supply chain risks	Supply chain weaknesses might bring hidden issues into systems. These risks would have a lower likelihood of fast exploitation.
Medium	Lack of employee training	More phishing and social attacks would happen, however it is easily fixed and is smaller-scale compared to the other risks.

iii) Holistic strategies

1: Improve the network security

- Separate the office networks from the manufacturing systems.
- Regularly update the firewall rules.
- Regularly monitor the network activity and check for suspicious.

These will help the problem as it will limit how far potential attackers can move within the company.

2: secure the embedded devices

- Update the device's software regularly.
- Change all of the default passwords.
- Keep a list of all the connected devices.

These methods reduce easy access points for attackers.

3: Strengthen the supply chain security.

- Begin performing supplier security assessments and requirements.
- Check components using code reviews
- require a software bill of materials (SBOM) from suppliers.

This will reduce the risk of hidden problems entering the systems and products and make sure that the suppliers are trustworthy.

4: update the operating systems.

- Update the unsupported operating systems that need to be updated.
- Isolate the legacy systems that cant be upgraded.
- Require strict access control for the engineering workstations.

Doing this will minimise the exposure of valuable assets and reduce exploitability.

5: improve employees knowledge of risks.

- Make employees attend regular cybersecurity awareness training.
- Perform regular phishing simulations and other targeted training.
- Require multi-factor authentication onto all accounts.

This will reduce human-based attacks and improves early detection of attacks.

iv) Incident identification plan

1: preparation

- Create an incident response team
- Keep a log of all incident responses
- Make sure all staff are trained to deal with potential attacks

2: analysis

- Use alerts, reports and monitoring tools to detect incidents.
- Arrange the incidents in order of severity and the system affected.
- Identify what methods have to be used to solve the problem.

3: regulation

- Isolate the affected systems and networks
- Disable the accounts which have been compromised.
- Prevent the spread to production or customer systems

4: removal

- Remove the malware and remove the compromised credentials.
- Patch the vulnerabilities and recompose the systems securely.
- Check the integrity of the embedded devices and firmware.

5: reflection

- Conduct post-incident reviews.
- Update the policies and controls.
- Update training.
- Report the incident to management and stakeholders.

v) applicable cybersecurity standards.

ISO/IEC 27001 – Information Security Management Systems

ISO/IEC 27001 provides a risk based framework for protecting systems, data and customer information. This would be good for the scenario as it also has a structured risk assessment method, access control, supplier management, incident response plans and employee awareness. It is a foundation for the companys overall governance and makes sure that cybersecurity risks are managed across the company.

NIST SP 800-61 – Computer Security Incident Handling Guide

This standard supports incident response plans by splitting it into different phases (preparation, detection, containment, eradication, recovery and lessons learned). This makes sure that security incidents are handled in the right way, while making sure that it is efficient.

ISO/IEC 27036 – Supply Chain Security

This would apply really well as it is critical for third party risks. It requires supplier security assessments, contractual security obligations and component validation. This will help to prevent insecure components from being put into the products/customer environments.

Summary:

In this report, I have analysed cybersecurity risks affecting the companys networks, embedded devices, supply chain, systems, and employees. These risks pose serious threat to the company, and by prioritising them and later removing them, the organisation can greatly reduce its exposure to cyber threats. There are many different standard that align with what I have written in this report, and all-together, they can easily be handled and fixed.

Bibliography

- [1] National Institute of Standards and Technology (NIST), *Cybersecurity Framework (CSF) 2.0*, 2024.
- [2] NIST, *Computer Security Incident Handling Guide (SP 800-61 Rev. 2)*, 2023.
- [3] NIST, *Secure Software Development Framework (SP 800-218)*, 2022.
- [4] ISO/IEC, *ISO/IEC 27001: Information Security Management Systems*, 2022.
- [5] ISO/IEC, *ISO/IEC 27005: Information Security Risk Management*, 2018.
- [6] International Electrotechnical Commission, *IEC 62443: Industrial Communication Networks – Network and System Security*, 2018.
- [7] ENISA, *Cybersecurity of Industrial Automation and Control Systems*, 2023.
- [8] CISA, *Cross-Sector Cybersecurity Performance Goals*, 2023.
- [9] Verizon, *2024 Data Breach Investigations Report*, 2024.

72

/100

PAGE 1

PAGE 2

PAGE 3



Comment 1

The introduction of a report is crucial as it sets the stage for the entire document. Introduction should include several key elements to ensure that the reader understands the purpose, scope, and structure of the report



Comment 2

Good work. However, it would be better to include a reference to support your claim.

To justify why the selected processor is better than the alternatives, please include an appropriate reference as evidence.



Comment 3

It is better to number each heading



Comment 4

Good work. However, it would be better to include a reference to support your claim.



Comment 5

Good work. However, it would be better to include a reference to support your claim.



Comment 6

It is better to include page number

PAGE 4



Comment 7

Line
spacing between heading and para, between lines, between paragraphs should be uniform.



Comment 8

Good Work, How you came to a conclusion it requires 750W. I would have been better with calculation



Comment 9

Line
spacing between heading and para, between lines, between paragraphs should be uniform.

PAGE 5



Comment 10

Line
spacing between heading and para, between lines, between paragraphs should be uniform.

PAGE 6



Comment 11

It is
better to provide a numbered title for the table, as it clearly indicates the table's content and purpose, making it easier for readers to understand its context and relevance.

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12



Comment 12

it would have been better if the cost was included in the description.



Comment 13

It is better to number each heading



Comment 14

It is better to include the type of cyber attack as a sub heading



Comment 15

It is beter to include citation within the text/ description.



Comment 16

Recommended to avoid
contractions like "don't." Instead, use the full form of the phrase,
which in this case is "do not



Comment 17

Recommended to avoid
contractions like "don't." Instead, use the full form of the phrase,
which in this case is "do not



Comment 18

Recommended to avoid
contractions like "haven't." Instead, use the full form of the phrase,
which in this case is "have not



Comment 19

caption
should be added for the table, so the reader will get an idea about the table



Comment 20

Compose
the report from a third-person perspective.



Comment 21

Compose
the report from a third-person perspective.

PAGE 22

GRADING FORM: CSF RUBRICS

TUSCANY CROWTHER-SNOW **71.80**

ENGAGEMENT WITH LITERATURE

The report should be supported by credible sources on cybersecurity and computer systems design in engineering. These may include academic journals, textbooks, official guidelines, and peer-reviewed or recognised online publications. Use of recent materials (from the past five years) on cybersecurity and hardware is encouraged. Proper referencing, with in-text citations and a reference list, is essential.



Engagement with a wide range of literature, including sources retrieved independently and with strong selection of sources. Include more peer-reviewed or technical publications to enhance depth. It would have been better if citation is included in task 1.
Citations and referencing require improvement

6.5

KNOWLEDGE AND UNDERSTANDING

The report should demonstrate knowledge of key cybersecurity principles and hardware specifications relevant to the scenario. Understanding should be shown through explanations of how these principles apply to real-world situations, supporting a balanced approach to risk mitigation that protects data integrity, confidentiality, and availability.



Excellent knowledge and understanding of the basic underlying concepts and principles of computer systems is evident through the description. Demonstrates a solid understanding of hardware compatibility, application requirements, and security risks. It also includes real-world considerations, such as legacy compatibility, realistic training cycles, and varying levels of attack risk. The analysis would be even better with more description about the choices made in task 1 with proper referencing.

23

COGNITIVE AND INTELLECTUAL

The report must evaluate cybersecurity risks and hardware specifications relevant to the scenario, comparing alternatives and assessing cost-effectiveness. Logical reasoning and clear justification should support each decision, demonstrating a holistic and proportionate response to security risks.



Excellent evaluation of the underlying concepts and principles of computer systems. There is a good comparative analysis and clear justification for component selection. The report demonstrates logical reasoning in prioritising cybersecurity threats through the use of a matrix, and risk assessments are well-structured, format could be enhanced to be clearer to non-technical readers. The report clearly demonstrates the adoption of a holistic and proportionate approach to mitigating security risks by addressing technical, organisational, and human factors, aligned with the severity and likelihood of each risk.

21.2

PRACTICAL SKILLS

Practical application of theoretical knowledge is expected, with clear demonstrations of how hardware choices are suited to the given scenarios. Solutions should be realistic, feasible, and contextually appropriate, showing a direct link between theory and practical implementation.



A very good application of a range of taught, basic methods, materials, tools, and techniques is

14.4

demonstrated. The context of the application is well considered and insightful. Practical skills are evident through the selection of components for the computer. The response would benefit from a good explanation of component compatibility. The design would also be improved by considering potential future upgrades or system scalability, which is important for long term usability.

TRANSFERABLE SKILLS FOR LIFE

The report should demonstrate professional communication and high-quality presentation, with well-organised sections, diagrams, and tables to convey technical content, as well as clarity and fluency in technical writing.



The report is well structured and demonstrates good coherence, contributing to a solid overall presentation. The quality of the work is good and shows effective transferable skills. Minor refinements could further improve the presentation, such as numbering each heading, maintaining uniform line spacing between paragraphs, including captions for tables, and ensuring the introduction section is clearly presented.

6.7