

Computer System Fundamentals Assignment

by Benjamin Newbury-Davies

Submission date: 08-Jan-2026 09:10PM (UTC+0000)

Submission ID: 272600121

File name: 66119_Benjamin_Newbury-
Davies_Computer_System_Fundamentals_Assignment_712285_433823177.docx (3.22M)

Word count: 2419

Character count: 13475

B.Eng (Hons) Embedded Electronic Systems
B.Eng (Hons) Electrical and Electronic Engineering

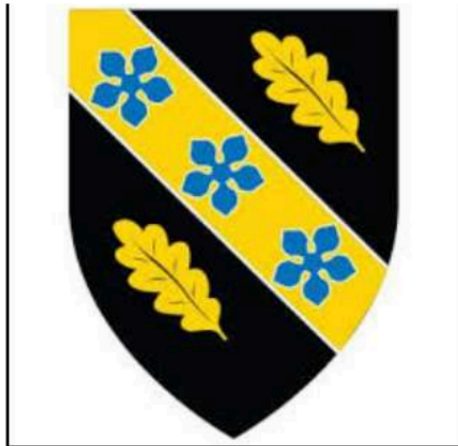
Module: Computer System Fundamentals

Module Code: ACCA4028

Assignment title: Cyber Risk and Computer Design

Name: Benjamin Newbury-Davies

Student ID: 2517508





Task 1

Introduction



In this report, the written content will be based on the two tasks and scenarios. In task one, the written content will critically analyse the design of a desktop computer to meet the specification needs of an Electrical Engineer, whilst adhering to the specific functions and regulations that the desktop computer needs to fit with the criteria of the scenario and instructions that have been set. This will include a 'shopping list' style table, outlining the key factors for each component needed to suit the task and scenario; also, this report will show the comparison but contrast of each specified component, from the listed table, to highlight and examine the best fit for the desktop computer, based on the specified task and scenario.

Hardware Components Shopping List



Type of Component	Component Name	Specification	Price	Image (If Available)
CPU	AMD's Ryzen 9 9950 X	Cores – 16 Threads – 32 Base Consumption – 170 W [1]	£463.69	
Motherboard	Intel Xeon W7-3565X	Cores – 32 Threads – 64 Cache – 82.5MB L3 Memory – DDR5, [3]	~~£2056.54~~	
RAM	DDR5	Maximum capacity – 16-32GB Clock speed – 4800 MT/s to 6400 MT/s Bandwidth – 51.2 GB/s [3]	£217.99	
Non-Volatile Storage	PCIe 5.0 NVMe Solid State Drive (SSD)	Form factor – compact M.2 2280 Capacities – 1TB – 8TB [4]	£158.95	



Input/Output ports	USB 4/Thunderbolt 4 USB 3.2 Gen 2/2x2 2.5 Gigabit/Ethernet (RJ-45) Wifi-7	USB 4/Thunderbolt 4 – Bandwidth of 40 Gbps, USB 3.2 Gen 2/2x2 Connecting standard peripherals 2.5 Gigabit/Ethernet (RJ-45) - Large simulation files Wifi-7 – Stability and speed [2,10]	Included from Motherboard	
Graphics Card	NVIDIA RTX 6000 Generation	Memory – 48GB GDDR6 ECC Max Power - 300W [2]	£700.30	
Case/Power Supply	80 Plus Platinum-certified ATX 3.0	Wattage – 1000W-1200W Efficiency – 80 plus platinum [4]	£79.99	
Monitor (including mouse, keyboard and webcam)	1.4K UHD IPS Monitor (BenQ PD series) 2. 3D connexion CAD Mouse pro wireless 3. Logitech MX Key S	1. Resolution – 4K UHD (3840 pixels x 2160 pixels) 2 Connectivity – HDMI, Display port, USB-C, Quick zoom, Bluetooth LE 3. Wireless keyboard, Bluetooth LE,	1. 157.60 2. 62.80 3. £83.90	  

		[6, 6, 6]		
Network Connectivity	Wired Ethernet	Define speeds, cable types and common categories [10]	Cat6a/7 - £1-£3 per metre	
Required Software	Windows 11	Microsoft Software's (CAD, MATLAB) [4]	£5.99 	

CPU

To run the computer for an Electrical Engineer, the CPU that is chosen is the AMD's Ryzen 9 9950 X. This CPU will be able to withhold multi-threaded tasks. This CPU is a better fit choice for the computer, compared to the Intel Core i5-12400, as it is a more advanced, being able to withstand more multi-threaded tasks [1]. This CPU will work well as it can run software's like SolidWorks electrical, PSpice and LabVIEW [6].

Motherboard

The selected motherboard desktop computer is the Intel Xeon W7-3565X. This motherboard will run a cache of 82.5MB, which has high storage. This supports the CPU as it offers excellent network features, helping with the task of video conferencing and reliable network connection [3]. This works better than the Core i9 as it offers a more versatile package and USB ports to benefit the Electrical Engineer, at a more justified price.

RAM

For the computer, the RAM DDR5 was selected. This gives a high storage capacity of 32GB. This capacity of storage fits the computer as it will enable tasks to be completed by the Electrical Engineer such as running the SolidWorks Electrical software, allowing software to run smoothly [3]. This was chosen as it offers good of performance and cost compared to a 16GB RAM. The 64GB RAM isn't cost efficient for an at home desktop computer.

Non-Volatile Storage

The non-volatile storage PCIe 5.0 NVMe Solid State Drive (SSD), was chosen. This storage caters for the factors of different professional software's needed by the Electrical Engineer. This storage allows multiple software's to be compatible,

compared to HDD [4]. The PCIe 5.0 NVMe Solid State Drive (SSD) is more expensive, but it's a better option as its aspects allow for more advanced work.

Input/Output Ports

For the computer, inputs and outputs will be fitted. USB 4 ports are fitted to connect sources; these are, storage drives and docking stations [2]. These ports will offer extremely high support, so it'll run smoothly and more compatible with the computer, giving the engineer an advantage of specific tasks. The USB 3.2 ports will be included for effective equipment needed, like keyboards, mouse and webcam. These ports will ensure that data transfer is kept high, with a simple design. The 2.5 Gigabyte Ethernet port allows the computer to have strong internet connections, allowing efficient work. [10]

Graphics Card

The selected graphics card is the NVIDIA RTX 6000 Generation. This works with the set-up as it allows the completion of tasks on professional software such as SolidWorks, with precise detail. It also has an affordable price. [2]

Monitor, Webcam, Mouse and Keyboard

For the computer, a monitor with a screen size of 3840 pixels x 2160 pixels was chosen as this can further ability to work with a larger screen, fit for the purpose of handling multiple tasks at once. A 1080p webcam allows clear videocalls. The keyboard and mouse allow the computer to run smoothly, with Bluetooth.

Network Connectivity

To help with the computer, ethernet cables are fitted. Ethernet cables are a beneficial factor as they offer fast data transfer, crucial when large projects need to be sent [10]. Ethernet cables supply high security protection; they're a harder source for hackers to tap into. When WIFI 7 is included, they provide an overall secure network source.

Required Software

Windows 11 is the software used. Windows 11 holds SolidWorks electrical, PSpice and LabVIEW. Windows 11 allows everyday functional use. Windows 11 allows the Electrical Engineer to access software like CAD Design and MATLAB [4,5,6]. It gives a high sense of security as it is a modern software, fit with regular updates to ensure it is secure from viruses.

Task 2

Introduction

The manufacturing company has a large supply chain producing and supplying power distribution equipment, industrial control systems and embedded electronic

controllers. The company undertakes roles in supplying key utilities, transportation, energy and manufacturing, internationally. Cyber security is a key aspect in the company's operating system as the professional engineering work, should be run with no interruption, protecting intellectual property and customer data.

In this report, the content will be based on the cybersecurity threats that pose in the given task and scenario, with a mitigation strategy used to counterattack these actions. This report will identify the impacts of cybersecurity threats, prioritising these risks in accountable order. A holistic cybersecurity risk plan will be set regarding the specified content. Applicable cybersecurity standards will be identified and how strategies proposed, align with these standards. [7,8,9]

Identification and Risks Evaluation

The lack of updated firewall rules and segregation increase the risk of unauthorised personal access. Firewall rules and segregation hold important information to the company such like IP addresses and destination ports; penetration of these systems can lead to the compromising of important control systems, leading to the disruption of vital equipment and therefore damaging the financial situation of the company. [7]

Embedded devices have outdated firmware and passwords, making them easy targets. These risks are easy targets for hackers to move easily around main company control systems, importing malware proliferation, leading to stolen credentials, stopping mass production and increasing the risk of ransomware attacks. This can lead to high reputational damage. [9]

Components that are internationally sourced, follow insecure development processes. This poses as a risk for hackers to halt productions lines as poor product quality can be introduced, with legal trade laws not being met, leading to overall mistrust between companies as the mass production standards are low; causing huge financial loss. [8]

Outdated operating systems and workstations receive no security patches. These risks allow hackers to tap into operating systems, making them prone to crashing and malfunctioning as they are an easy target to malware and exploits. This can result in loss of mass product and financial issues as production outages will occur. [7]

The lack of cybersecurity training, undertaken by employees. This is a huge risk to the company as the lack of employee cybersecurity training can result in safety risks to staff and the company. If the under a cyber security attack, hackers can impose malfunctions and tamper with safety systems; with an employee not trained on cybersecurity, this puts mass amounts of employees and equipment in danger as working conditions are unsafe. [8]

Risk Prioritisation

The risk with highest prioritisation is the embedded devices that have outdated firmware. The likelihood of this is very high with it being a very severe risk as it has a direct impact production and credentials. [9]

The risk with second highest prioritisation is the lack of firewall rules and segregation. With this risk the likelihood of this is at medium risk; the severity is very high as it can impact the widespread of vital company information. [7]

The risk with the third highest prioritisation is outdated operating systems. The likelihood of this risk is high, with a high severity as it is linked the finances and mass production of the company. [7]

The risk with the fourth highest prioritisation is the lack of employee training. The likelihood of this is very high; the severity of this is a medium risk, being a common occurrence in hacking patterns, so companies are now learning how to deal with this risk. [8]

The risk with the least prioritisation is the components that are internationally sourced, with insecure development processes. The likelihood of this is a medium risk; the severity of this is, is high as it interferes with product quality. This risk is last on the in the order of prioritisation as it has is a harder risk to exploit as there are more safety regulations in place. [8]

Holistic Cybersecurity Mitigation Strategy

Outdated Firewall Rules and Lacks Segregation:

To identify all assets, conduction of a risk assessments should be undertaken. A least privilege approach should be adopted where all traffic is blocked unless manually approved. The risk mitigation for this risk is that lateral movement is under control for all areas of the risk and if one area is compromised, lateral movement is limited. [7]

Embedded Devices have Outdated Firmware and Outdated Passwords:

Regular firmware system updates should be put into place to update security factors, alongside good vendor communication to recognise when updates are needed. The use of strong authentication passwords is reinforced, with strong device access control. The risk mitigation for this risk company control systems cannot be exploited. [9]

Components that are Internationally Sourced, with Insecure Development Processes:

The continuous monitoring of third-party activities allows objective insights for vendor performance. Service Level Agreements and clauses are put into place to recognise security standards. The risk mitigation for this risk is that all legal trade laws are met, with legal agreements in place, reinforcing these laws. [8]

Outdated Operating Systems and Workstations Receive No Security Patches:

The access of the operating systems should be limited to essential personnel. The deployment of Intrusion Prevention Systems, should be in place, monitoring network trafficking. The risk mitigation for this is that all services have backed up security network services, reducing assets from dangerous malware. [7]

The Lack of Cybersecurity Training, Undertaken by Employees:

Each employee should undertake a continuous training programme, tailored to their specific job role to grasp the full concept of their roles and responsibilities. Real-world threats and scenarios should be implemented into daily working activity giving colleagues on the job training. The risk mitigation for this is that it creates a secure work environment as the vulnerability of employees is reduced. [8]

Incident Response Plan

The first step of the plan is preparation. This includes overall risk assessments to identify vulnerabilities, creating an incident response team, assigning specific roles to specific employees based on the working environment. [7]



The second step of the plan is the identification. This includes the monitoring of potential issues, identifying them in severity classes, based on the impact they can cause. [7]

The third step of the plan is containment. This includes the limitation of damage by promoting the segment network to prevent lateral movement and isolation of highlighted affected systems. [7]

The next step of the plan is eradication. This is the main process of addressing the root cause, patching vulnerabilities; leading to the removing of malware. [7]

The next step of the plan is recovery. This is aimed at restoring operating systems by re-testing to monitor the risk of re-infection and that the verification of vital production systems is confirmed. [7]

Finally, the last step of the plan is any lessons learned. This is to be set for post incident, identifying root causes of issues, backing up policies and creating new control systems stopping further issues from occurring. [7]

Alignment of Cybersecurity Standards

Standard	Alignment
NIST SP 800-61 [7]	Cybersecurity risk management handling, incident response and handling.
ISO 27001 (Annex A 5.24) [8]	Managing security information, communicating roles and responsibilities.

IEC 62443 [9]	Control system security and industrial automation.
---------------	--

The incident response plan aligns with various international standards and procedures. This allows the manufacturing company to use the best practices for vital infrastructure systems.

Conclusion

To conclude, this report analysed and evaluated key factors of a desktop computer for an Electrical Engineer and assessed different vital cybersecurity risks for a manufacturing company. The precise selection of hardware and robust cybersecurity strategies help mitigate the threat of malware, protecting key operational and company data from further cyber threats.

References

11

[1] AMD, *AMD Ryzen 9 Desktop Processors*, AMD, 2024. (Online): <https://www.amd.com>

[2] NVIDIA Corporation, *NVIDIA RTX 6000 ADA Generation GPU*, NVIDIA, 2024. (Online): <https://www.nvidia.com>

[3] Intel Corporation, *Intel Xeon W Processor Family*, Intel, 2024. (Online): <https://www.intel.vom>

[4] Microsoft, *Windows 11 Security and Productivity Overview*, Microsoft, 2024. (Online): <https://microsoft.com>

[5] MathWorks, *MATLAB and Simulink for Engineers*, MathWorks, 2024. (Online): <https://www.mathwork.com>

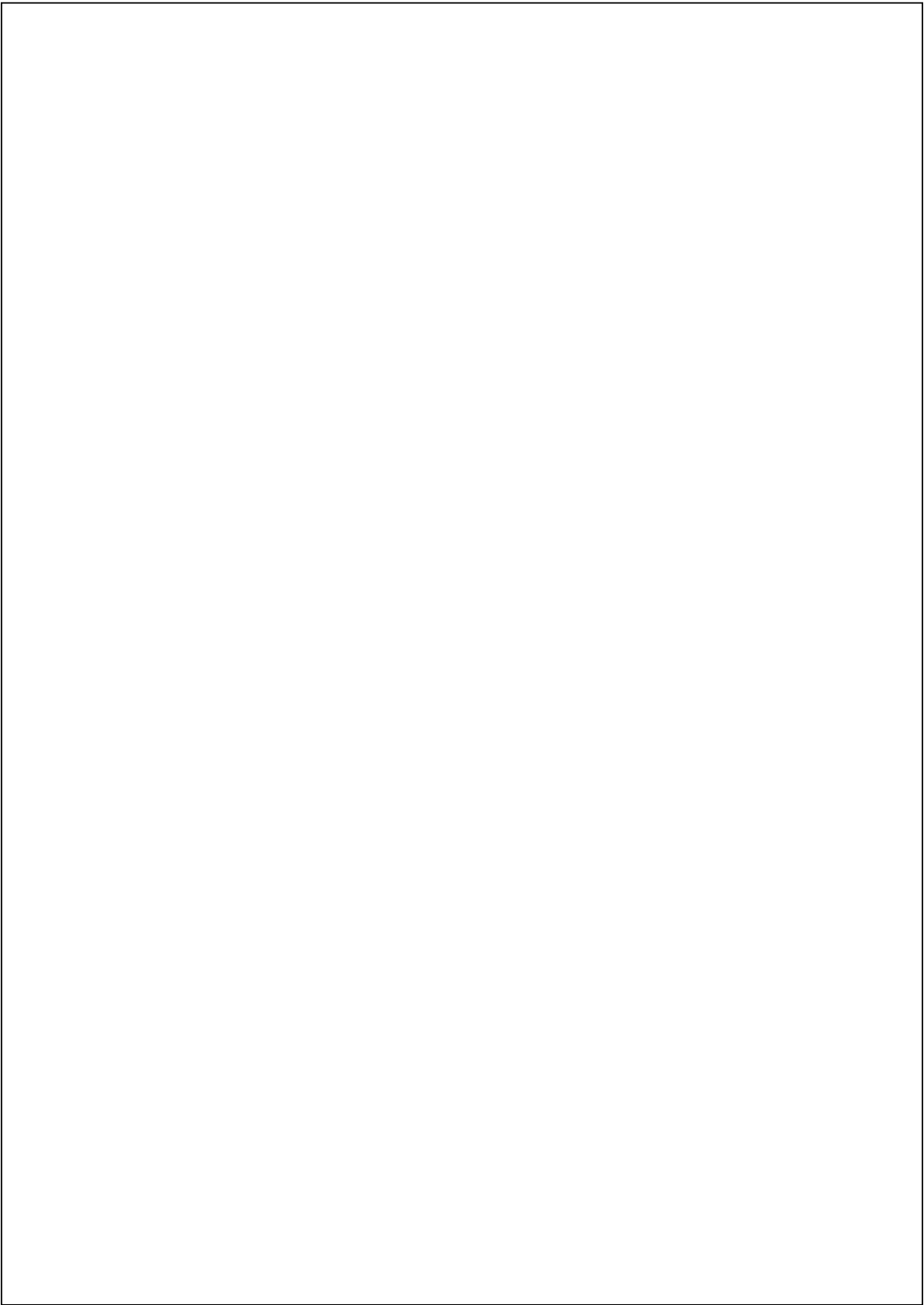
[6] Dassault Systems, *SolidWorks Electrical Documentation*, Dassault Systems, 2024. (Online): <https://www.solidworks.com>

[7] National Institute of Standards and Technology (NIST), *Computer Security Incident Handling Guide (SP 800-61 Rev 2)*, NIST, Gaithersburg, MD, USA 2012

[8] International Organisation for Standardization, *ISO/IEC 27001:2022 – Information Security Management Systems*, ISO, Geneva, Switzerland, 2022

[9] International Electrotechnical Commission, *IEC 62443: Industrial Communication Networks – Network System Security*, IEC, Geneva, Switzerland, 2018

[10] Cisco Systems, *Ethernet Cabling Standards and Performance*, Cisco, 2023. (Online): <https://www.cisco.com>



Computer System Fundamentals Assignment

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

67 /100

PAGE 1

PAGE 2



Comment 1

It is better to include table of content



Comment 2

It is better to number each sub headings



Comment 3

It is better to
provide a numbered title for the table



Comment 4

why it is too expnesive



Comment 5

It would have been better with the page number

PAGE 3

PAGE 4



Comment 6

what is the total cost?



Comment 7

Recommended to avoid
contractions

PAGE 5

PAGE 6

PAGE 7



Comment 8

It would have been better if the risks are listed in table

PAGE 8



Comment 9

it is better to include references with in the text



Comment 10

It is better to
provide a numbered title for the table

PAGE 9



Comment 11

It is
advisable to include more references from peer-reviewed journals.

PAGE 10

GRADING FORM: CSF RUBRICS

BENJAMIN NEWBURY-DAVIES

67.60

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.



Wide and appropriate reading is demonstrated, with a strong selection of sources. Referencing is generally consistent. Including more peer-reviewed or technical publications would enhance the depth of the work. Greater consistency in citation style would further improve the quality. Consider expanding the review to include a broader range of literature types.

6.7

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.



Clear and accurate knowledge of computer components and cybersecurity, with strong contextual application. Exhibits good understanding of the fundamentals of computing, which is evident through the description. Demonstrates a solid understanding of hardware 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 stronger with reference to cybersecurity

21.1

frameworks and more detailed explanations for hardware choices.

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 good comparative analysis and clear justification for component selection. The report demonstrates logical reasoning in prioritising cybersecurity threats and risk assessments are well-structured, format could be enhanced to be clearer to non-technical readers. It would have been better if each component had been compared with alternatives and justified and the total cost of the computer is mentioned. A good approach to mitigating security risks is demonstrated.

19

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. The context of the application is well considered and insightful. Practical skill is evident through the selection of computer components, which are highly practical, and reasonably priced. The work would be further improved by including some

14.1

consideration of data backup and upgradable strategies.

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 with good coherence, contributing to a strong presentation. Overall quality is good, demonstrating effective transferable skills. Consider Minor refinements such as ensuring proper text alignment would further enhance the polish of the report. It would also benefit from proper text alignment, appropriate placement of table captions, and inclusion of page number, table of content to enhance the readability of the report.

6.7