

Computer Systems Fundamentals ACCA4028 Assignment - David Reynard

by David Reynard

Submission date: 10-Apr-2025 02:43PM (UTC+0100)

Submission ID: 255365067

File name: 59372_David_Reynard_Computer_Systems_Fundamentals_ACCA4028_Assignment_-_David_Reynard_659655_2121326500.docx (221.13K)

Word count: 2398

Character count: 13111

Cybersecurity and Computer System Design Assignment

David Reynard

Student No: 2419240

L4 – Computer Systems Fundamentals

ACCA4028

Embedded Electronics Systems
Engineering Degree Apprenticeship

Contents

Task 1 – Custom computer design for an engineer 3

1 - Introduction 3

2 - Establishing minimum requirements 3

2.1 - SOLIDWORKS 3

2.2 - PSpice 3

2.3 - LabVIEW 3

3 - Hardware decision 4

3.1 – CPU 4

3.2 – GPU 4

3.3 – RAM 4

3.4 – Storage 4

3.5 – Coolant 5

3.6 – PSU 5

3.7 – Motherboard 5

3.8 – Case 5

3.9 – Monitor 5

3.10 - Peripherals & Additions 5

4 – Software Requirements 6

5 – Breakdown 6

Task 2 – Cybersecurity 7

1 – Current Risk Priority 7

1.1 - Highest risk: Lack of training 7

1.2 - Default passwords 8

1.3 – Outdated Software/Firmware 8

1.4 – Use of Less ‘Secure by design’ Products 8

2 – Security Strategy 8

2.1 – Training Plan 8

2.2 – Update Schedules 9

2.3 – Liability Systems 9

3 – Incident Response Plan 9

References 10

Task 1 – Custom desktop computer design for an engineer

1 - Introduction

A number of technical considerations need to be made when designing a custom build PC, all dependant on the system use case. In this case, the end-user is an engineer who has specified a number of application and security requirements that must be met. To best suit these requirements, they should be translated into technical specifications.

2 - Establishing minimum requirements

The customer has specified a list of CAD (computer aided design), collaborative and presentative software that will be required for their day-to-day work. CAD software is the most resource intensive category of item in the list, as such the bulk of hardware minimums should be established based off the software providers' self-assessments.

Out of the list provided, the following were deemed to be the most demanding and a good representation of hardware minimums.

2.1 - SOLIDWORKS

SOLIDWORKS publishes limited requirements beyond RAM (Random Access Memory) requirements, and driver supported GPUs (Graphics Processing Unit), most of which are units made for industry.

2.2 - PSpice

Pspice also doesn't provide minimum hardware specifications, however, FlowCAD recommends the following for PSpice:

- "Intel Core™ i7 4.30 GHz or AMD Ryzen™ 7 4.30 GHz with at least 4 cores
- 16 GB RAM
- 50 GB free disk space (SSD recommended)
- 1920 x 1200 display resolution with true color (at least 32-bit color)
- A dedicated graphics card supporting OpenGL, min 2 GB"

[1]

2.3 - LabVIEW

Labview provides a set of minimum requirements from 2019, but no set of optimal system requirements. They are quoted as follows:

- "Pentium 4 G1 (or equivalent) or later (64-bit)
- 1GB RAM
- 1024 x 768 pixels screen resolution
- Windows 10 (version 1809)/8.1 Update 1²/7 SP1³
- 5GB Disk space
- You must have Adobe Reader 7.0 or later installed to search PDF versions"

[2]

3 - Hardware decision

Minimums for the major components required for the build have been mostly covered, but minimum specification for a GPU is missing. In principle, the CPU will be more important than the GPU due to lesser requirement for on-screen graphics processing, this will be used to decide the GPU.

For benchmark equivalents, UserBenchmark [3] will be used, the score generated will also be used to choose above minimum spec by a relative amount. In order to help with compatibility and pricing comparison, PCPartPicker [4] will be used.

3.1 – CPU

The Intel Core i5-14600KF would satisfy our previously defined requirements, increasing performance above the minimum spec by 78%, at a cost increase of 58% for that component. Anything more would significantly drop the cost/performance coefficient.

3.2 – GPU

The GPU only needs to support the engineering applications without causing the CPU to be bottlenecked. As per the SOLIDWORKS recommendation, an industrial card of medium spec. The RTX 4000 Ada generation (20GB VRAM) is a SOLIDWORKS supported card that will more than sufficiently support SOLIDWORKS and the rest of the system operation.



3.3 – RAM

In line with the Pspice requirements, 32GB of RAM should provide sufficient memory to run the required engineering applications, as well as the background system and professional/presentative applications. Although DDR4 is not the most up to date standard, it will save on cost for the memory and the motherboard. The quantity of memory should make up for the quality.



3.4 – Storage

A 1TB m.2 SSD should provide the speed and storage necessary to store the vast majority of applications, operating system and frequently accessed files. A larger 4TB HDD should be present to store project files and other documents to preserve the SSD.



3.5 – Coolant

A CPU cooler, as well as some case airflow fans will be required. A Noctua NH-D15 is a well rated air based CPU cooler that mounts directly to the chip for optimum thermal transfer. The number and position of internal fans will be determined by the case.



3.6 – PSU

The PSU (Power supply unit) will provide power for system. PCPartPicker takes into consideration the system power requirement and will offer PSUs that fit the bill. As such, an 850w, 80+ platinum grade Corsair SF850 has been chosen as it is above the requirement for futureproofing. The reliable platinum grade is proof of high efficiency.



3.7 – Motherboard

PCPartPicker will also flag compatible motherboards for slots, RAM technology etc. The Gigabyte B760M offers a compact, high memory capacity board with built in WIFI capability at a reasonable price.



3.8 – Case

To fit the form-factor, the In Win EM048 will provide a MicroATX form factor, offering and input and an output airflow with dust filtering for optimised cooling. The case has a number of 3.2 USB A and C inputs for external connectivity.



3.9 – Monitor

For use with CAD software, a larger and more detailed monitor will help with the finer details of design work. It is also a good idea to enlist the use of a secondary monitor for interacting with the professional and presentative software, as well as reducing eye strain. 2x ViewSonic VX3276-2K-MHD will provide high quality display on a larger 32" screen. This monitor is supported by the GPU through the use of Mini-DisplayPort, which the GPU supports 4 of.



3.10 - Peripherals & Additions

A mouse, keyboard and webcam will be required for optimal use of the system. Ergonomic equipment should be used to reduce the risk of repetitive strain injury and other display screen equipment risks. The following are suitable, standard office ergonomic options:

- Logitech MX Master 3S - £99.99
- HP 960 Ergonomic Wireless Keyboard - £109.99

The Logitech BRIO 100 is an economic 1080p USB webcam with built in microphone for collaborative interactions as was requested in the requirements.

Although the motherboard has built in WIFI, a wired network should be used where possible for stability and security. The TP-Link TX201 will provide 1 RJ45 connection port to provide connection to the internet. A network switch can be employed where more direct connections are required.

4 – Software Requirements

Software additional to the CAD software previously mentioned will be required for team collaboration, presentation, and security as well as an operating system to allow interaction with the system.

The latest version of Windows 11 Pro will be appropriate for compatibility and security. It's backwards compatibility will ensure legacy software will still function as intended, and being the latest instance of Windows will mean that security patches and system upgrades will be supported.

The SOLIDWORKS Standard with Cloud services pack is most suited to the customer requirements due to the already sufficient CAD tools and support.

A perpetual professional Labview license is recommended due to the further inclusion of extra tools such MS Office integration, database connectivity and advanced signal processing toolkits.

Microsoft 365 Business Premium will provide the majority of non-engineering software for a broad range of business collaboration through the use of MS Teams, Outlook, SharePoint and OneDrive as well as providing word processing, presentation and budgeting software like MS Word, PowerPoint and Excel. The package also provides access to Microsoft defender for an extra layer of security.

Malwarebytes is a good addition to security as a fall back option in a scenario where it is suspected the system may be infected.

5 – Breakdown

The following quoted from PCPartPicker is the full build:

<https://uk.pcpartpicker.com/list/xjRvmC>

The cost breakdown is as follows:

PC Hardware

- CPU: £180.47
- CPU Cooler: £106.46
- Fans: 2x £9.03 = £18.06
- Motherboard: £122.99
- RAM: £44.99
- Storage: £85.80 + £87.99 = £173.79
- GPU: £1,438.65
- Case: £160.68

David Reynard – 2419240
University of Wales Trinity St David
Cybersecurity and Computer System Design

- PSU: £169
- NIC: £27.24

Total: £2 442.33

Peripherals:

- Monitor: 2x £209.99 = £419.98
- Mouse: £99.99.
- Keyboard: £109.99
- Webcam: £49.99

Total: £679.95

Software:

- Microsoft 365 business premium: £238.80 /year
- Malwarebytes standard: £29.99 /year
- Solidworks: £2 820 /year
- Labview: £9 210
- Pspice: Free
- Windows 11 Pro: £178.45

Total: £9 388.45 flat + £3 088.79 /year

Grand total: £12 510.73 flat + 3 088.79 /year

Task 2 – Cybersecurity

The business in the provided scenario is, in its current state, is extremely vulnerable to cyber-attack through a number of different means. This due to a wide variety of existing hardware, training and general attitude/awareness problems. The solution lays in targeting specific deficiencies with business policy changes which should improve personnel risk-aversion and reduce system vulnerability.

1 – Current Risk Priority

Below is an evaluation of risk/impact severity, ranking from 1.1 being the highest and 1.4 being the lowest.

1.1 - Highest risk: Lack of training

Staff being unaware of what constitutes as a security risk is the subsequent cause of the majority of issues to be mentioned. Any single person within the business has the power to compromise it, through incompetence, complacency, or social engineering and is the number 1 cause of cyber-attacks. Lack of training has a high likelihood to result in an attack, and has the potential to affect any single protected asset within the company to a catastrophic level.

1.2 - Default passwords

Default passwords are often listed in software manuals, and will often allow user admin-level access said program, meaning should a bad actor have access to the internal software, they can manipulate the system in whatever way the developers have provided the highest level user. Use of default passwords has a high likelihood to result in an attack on any externally networked systems, providing high level permissions to the attacker on that system and the extended network.

1.3 – Outdated Software/Firmware

With outdated software/firmware, a bad actor can simply use previously discovered (and patched) exploits to damage, access or manipulate the systems in question without even coming up with their own ideas.

Firewall exploits can also be found online and can lead to traffic being overlooked, possibly allowing viruses, Trojans etc. to enter the system undetected. Due to the accessibility of these exploits, outdated software/firmware has a medium likelihood of resulting in a cyber-attack with the possibility to do a medium amount of damage, depending on what the exploit entails.

1.4 – Use of Less ‘Secure by design’ Products

Less secure products will more often have more possible exploits. Although suboptimal, it isn't a critical downfall in this scenario due to the additional risks.

Similarly to firewall exploits, effort and skill is required for discovering new exploits, but for products they are less common to find. Additionally, the bad actor would have to possess knowledge and understanding of the systems used within the facility, which isn't always easy to come by.

These combined points make less secure products a low causation risk by comparison. Should the system be compromised however, medium damage can be done through manipulation and further access to the network.

2 – Security Strategy

In order to amend these glaring issues, improvements must be made in policy to ensure these risks monitored and mitigated regularly.

2.1 – Training Plan

As previously mentioned, lack of staff training and awareness is the greatest risk to cyber integrity. A regular course, taken every 1-2 years should be provided ALL staff. This course should include basics on standard cyber-attack methods, such as phishing, malware and man-in-the-middle attacks, as well as signs the dangers and signs of social engineering.

A more advanced course should be present for system administrators, which should include more advanced detail of the ‘basic’ course mentioned, as well as content on their responsibilities when it comes to updating software, maintaining up-to-date system access and ensuring the presence and security of strong passwords. This should be completed every year.

2.2 – Update Schedules

System admins should be briefed on staying informed of critical and major system updates, and should be given time to check and complete any and all updates regularly every 2-4 weeks depending on the amount and size of systems in their jurisdiction.

2.3 – Liability Systems

Not much can be done retrospectively in regards to poorly secured/supported systems other than to purchase from reputable businesses that offer security assurances. Briefing staff on general awareness of possibly liable systems, paying extra care and attention to known exploits and system use.

3 – Incident Response Plan

In the case of a cyber-attack or security incident, it is crucial to have a premeditated standard operating procedure to avoid panic and execute a sound of mind plan.

The first thing to do once an incident has taken place, according to the NCSC (National Cyber Security Centre) is to report the incident to Action Fraud which will be further escalated to the (NFIB) National Fraud Intelligence Bureau [5]. Their advice should supersede all of the following steps.

If they are unable to help, isolate the suspected system from the network so as to prevent rapid spread. Then, attempt to run anti-virus and anti-malware to see if there is any malicious software present and if it can be quarantined. Built in operating system checks should also be completed to help find/resolve the issue. All passwords associated with the system should change, as well as duplicates. Expert help should then be sought before continuing to use the system if a factory reset isn't viable.



Total body word count: 2134

References

[SOLIDWORKS, "SOLIDWORKS Hardware Benchmarks," 28th September 2008. [Online]. Available:
1 <https://www.solidworks.com/support/hardware-benchmarks>. [Accessed 18th March 2025].
]

[NI Emerson, "LabVIEW 2019 Readme for Windows," March 2019. [Online]. Available:
2 [https://www.ni.com/pdf/manuals/374715l.html?srsId=AfmBOoph2_q2tEkp0IOLe4ulelze7VH8L](https://www.ni.com/pdf/manuals/374715l.html?srsId=AfmBOoph2_q2tEkp0IOLe4ulelze7VH8LEbYSwl7s3oElpuU2Cb9zMBq#requirements)
] EbYSwl7s3oElpuU2Cb9zMBq#requirements. [Accessed 18th March 2025].

[". t. o. s. a. engineers", "UserBenchmark," [Online]. Available:
3 <https://www.userbenchmark.com/>. [Accessed 03 2025].
]

[PcPartPicker, "Pick Parts. Build Your PC. Compare and Share.," [Online]. Available:
4 <https://uk.pcpartpicker.com/>. [Accessed 03 2025].
]

[National Cyber Security Centre (NCSC), "Small Business Guide: Response & Recovery," [Online].
5 Available: <https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery>.
] [Accessed 10 04 2025].

[FlowCAD, "Quick Start OrCAD PSpice," 18th August 2020. [Online]. Available:
6 https://www.flowcad.de/AN/PSpice_Quickstart_EN.pdf. [Accessed 18th March 2025].
]

Computer Systems Fundamentals ACCA4028 Assignment - David Reynard

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

78/100

PAGE 1

PAGE 2



Comment 1

Good Work

PAGE 3



Comment 2

Good Work

PAGE 4



Comment 3

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

PAGE 5



Comment 4

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

PAGE 6



Comment 5

Good Work, It would have been better with the a table and specification

PAGE 7

PAGE 8

PAGE 9



Comment 6

It would have been better with a conclusion

GRADING FORM: GRADING

DAVID REYNARD

77.60

ENGAGEMENT WITH LITERATURE

The report should be supported by credible sources relevant to cybersecurity and computer systems design in engineering. Sources may include academic journal articles, textbooks, government and industry guidelines, and reputable websites. Recent materials (within the last five years) on cybersecurity, and hardware specifications are encouraged. Proper referencing with in-text citations and a reference list is essential to show the breadth and relevance of research.



Wide and appropriate reading demonstrated, with strong selection of sources. Referencing is consistent. Proper in-text citations and a reference list are used. Include more peer-reviewed or technical publications to enhance depth. Consider expanding to a broader range of literature types.

6.8

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 scenarios, supporting a balanced approach to risk mitigation by protecting 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 stronger with reference to cybersecurity

23.4

frameworks and more detailed explanations for hardware choices.

COGNITIVE AND INTELLECTUAL

The report must include evaluation of the cybersecurity risks and hardware specifications relevant to the scenario. This involves comparing alternatives and assessing cost-effectiveness. Logical reasoning and clear arguments should illustrate why each decision is suitable, ensuring a proportionate response to security risks.



Excellent evaluation of the underlying concepts and principles of computer systems. The report demonstrates an excellent ability to construct arguments using evidence and make appropriate, valid judgements. Alternatives in hardware design are considered, and the use of a risk priority matrix is commendable. However, the incident response plan, while reasonable, lacks a critical evaluation of its effectiveness. A good approach to mitigating security risks is demonstrated, with consideration given to both technical and organisational measures.

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.



There is 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 careful selection of components for the computer. The PC build is technically sound, realistic, and well-costed. However, the response would benefit from a clearer explanation of component compatibility. The design could also be improved by addressing potential future upgrades and system scalability, which are important for long-term usability. Additionally, it would be beneficial to consider the inclusion of backup or disaster recovery solutions as part of the overall system strategy.

20

TRANSFERABLE SKILLS FOR LIFE

The report should display clear and professional communication, with high presentation quality, including well-organised sections, diagrams, and tables to convey technical information effectively. It should demonstrate the ability to complete tasks, reflecting readiness for professional practice, and emphasise clarity, accuracy, and fluency in technical writing.



The report exhibits a high level of structure and coherence. The presentation is clear, contributing to a very good overall quality. It demonstrates strong transferable skills for both life and professional practice. However, it would benefit from careful proofreading and the replacement of informal phrases with more formal academic language

8.4