Assignment Guidance and Front Sheet
This sheet is to be populated by the Module Tutor, checked by the Programme Team, and uploaded to Moodle for students to fill in their ID and submit with their assessment.

Student ID or IDs for group work	1921983

Module Title & Code	WM267 Cyber Risks in Organisations
Module Owner	Dr Gregory Epiphaniou
Module Tutor	William Afrifah
Module Marker	Dr Gregory Epiphaniou
Assessment type	Coursework
Date Set	26/02/2021
Submission Date (excluding extensions)	29/03/2021
Marks return date (excluding extensions)	26/04/2021
Weighting of mark	60%

Assessment Detail	The coursework examines the process of identifying, measuring and ranking threats in a smart energy environment. It introduces the students to formal methods to measure the impact of threats and deploy cost-effective mitigation plans successfully.
Additional details	2,000 words (+-10%)
Module learning outcomes (numbered)	Demonstrate the ability to design, implement and test information security processes in Information security management systems to increase their resilience and conformance with legal and regulatory functions Provide a systematic understanding of knowledge and awareness of information and systems and network security management processes Assess, analyse and synthesise tools, techniques and approaches to quantify threat landscapes and provide mitigation plans in a variety of organisational contexts. Systematically apply knowledge on how to design and implement information security policy programs fully aligned to legal and regulatory compliance frameworks

Learning outcomes assessed in this assessment (numbered)	Provide a systematic understanding of knowledge and awareness of information and systems and network security management processes Assess, analyse and synthesise tools, techniques and approaches to quantify threat landscapes and provide mitigation plan in a variety of organisational contexts.
Marking guidelines	Please see attached marking scheme at the end of the coursework brief.

	The University of Warwick 20-point marking scale as a default for Undergraduate assessment.
Submission guidance	N/A
Academic Guidance	Where further help may be received, link to handbook, details of feed forward, workshops, seminars etc
Resubmission details	The University policy is that students should be given the opportunity to remedy any failure at the earliest opportunity. What that "earliest opportunity" means in terms of timing and other arrangements is different depending on Programme (i.e., Undergraduate, Full Time Masters, Part Time Postgraduate, or Overseas). Students are advised to consult your Programme Team or intranet for clarity.
Late submission details	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late.

U1921983

Project Daedalus Threat Modelling

Contents

Executive Summary........3

Core Findings........3

Remarks........4

Trust Boundaries........4

TD (1)........4

TD(2)........5

Data Flow Diagrams........5

DFD(1)........5

DFD(2)........6

Data Flow Descriptions........6

Threat Modelling........7

Threat Identification........7

STRIDE........9

Threat Ranking........9

DREAD........9

Threat Mitigation Plan........11

Plan Derivation........11

Incident Response........12

Risk Mitigation........14

Actions........14

Conclusion........16

Bibliography........16

Executive Summary

Core Findings

As the Threat Modeller, I will provide the Daedalus Project with a systematic and structured security identification, ranking and mitigation plan which shall be exploited to meet the high priority security objects shown below. The threat model shall inform decisions in design, development and implementation of software and hardware while prioritising safety (Adepu et al., 2020).

My core findings for threats within the two defined trust domains are as follows. Firstly, with regards to the wireless module, we must ensure that the most up-to-date protocols are being used (WPA2-PSK – see mitigation plan). The wireless module will be providing internet access to the M400 management module while also being used to transfer data from the ESP8266 to the management module. For these reasons, a robust plan must be implemented to ensure data integrity and restrict access to the internal workings of the Daedalus panel.

An Incident Response Plan (IRP) has been developed to provide a robust framework for the Daedalus Project team to work from.

Remarks

Daedalus' high priority security objectives are as follows (Kravets et al., 2020):

- Confidentiality – Development must ensure that all data is safely transmitted and received. Using cryptographic controls will allow for this.
- Integrity – Data must be validated on receipt and transmission to ensure it is not altered or injected from an attacker. By using verification and validation techniques like signed software and checksums this can be ensured.
- Availability – The smart panel and its interfacing components must be available at all times. By developing a DDoS response plan this shall be mitigated.
- Authentication – Particularly in the domain of software updates is authentication a high priority. By enforcing signed software techniques, you can avoid old software being installed on components.

The investigation has found that there is a high concentration of threats within two trust boundaries and the M400 management module. The wireless module will allow attackers to gain access from anywhere in the world if not secured properly. Subsequently, due to the poor security with regards to the local software updates combined with the wireless module vulnerability, the panel shall be permanently vulnerable without proper mitigation (CISCO, 2014).

Trust Boundaries

TD (1)

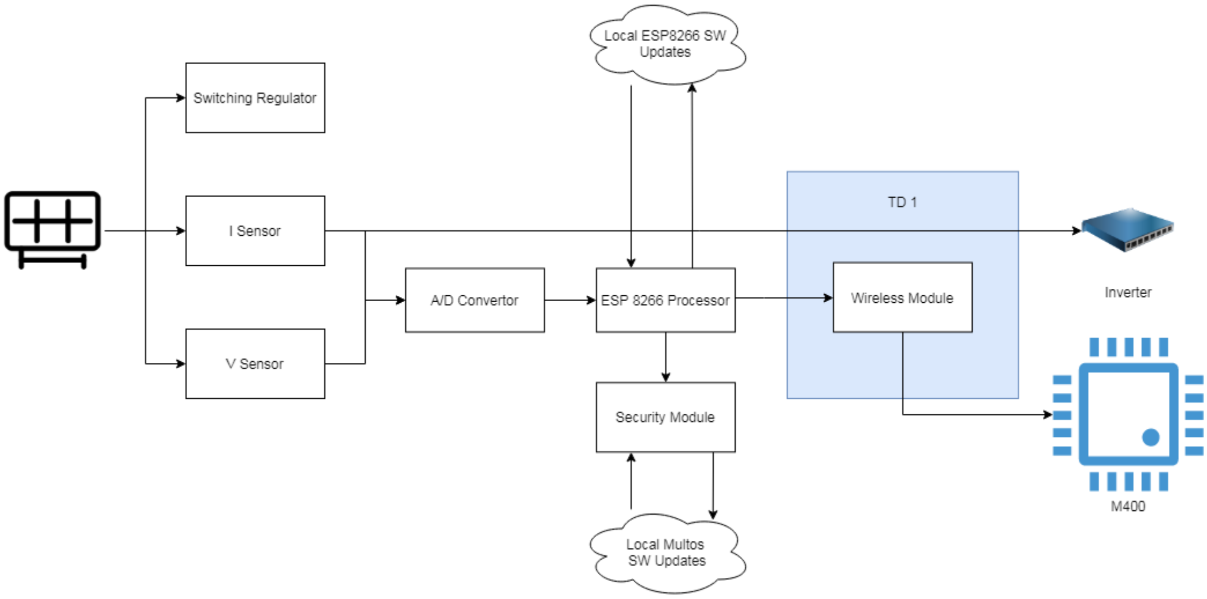


Figure 1: Wireless Module Trust Domain

Trust domain 1 is the communication between the Wireless Module and the database via the M400 management module.

TD(2)

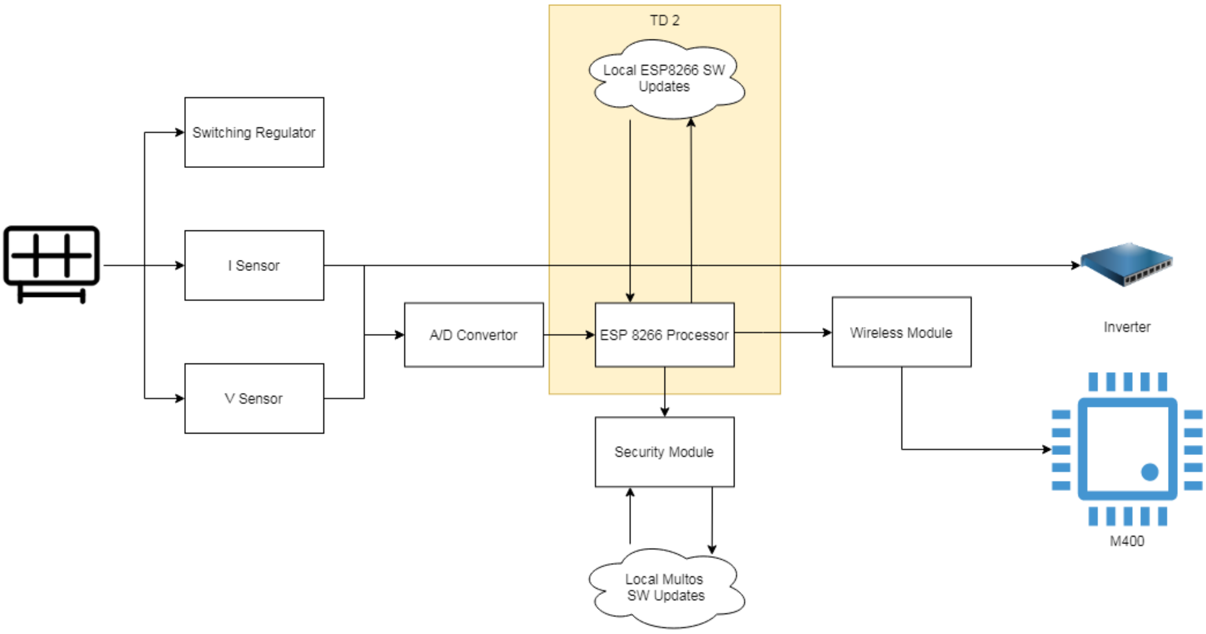


Figure 2: ESP 8266 Software Update Trust Domain

Trust domain 2 encompasses the communication between the ESP 8266 and its software update repository.

Data Flow Diagrams

DFD(1)

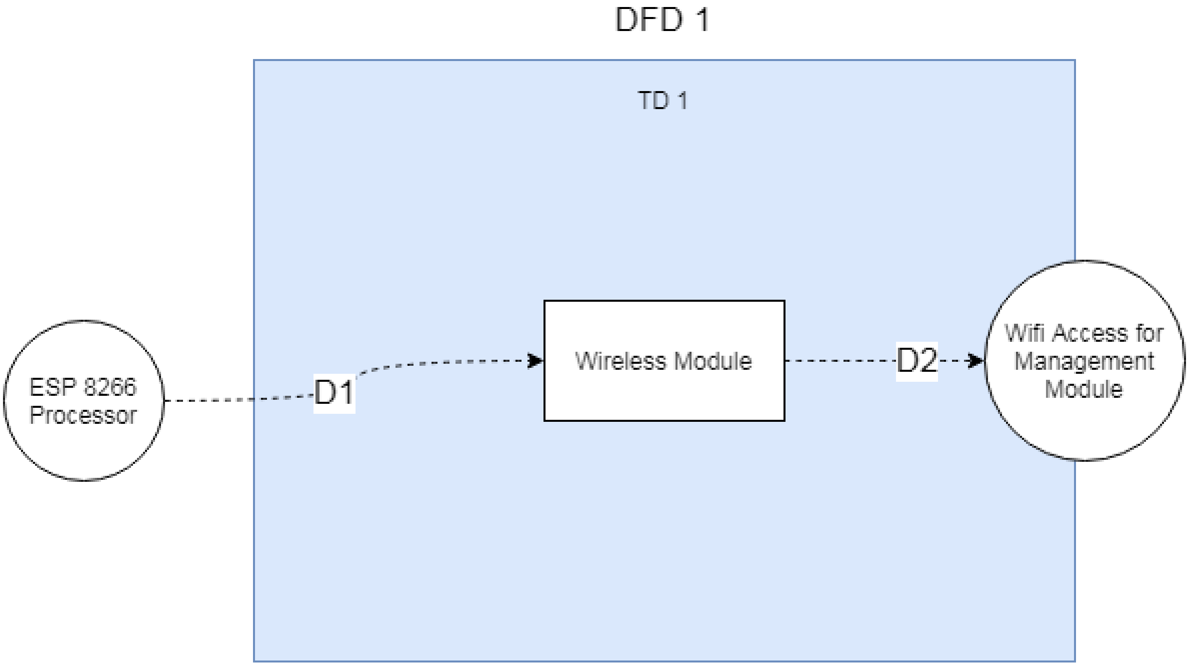


Figure 3: DFD for TD1 (Wireless Module)

DFD(2)

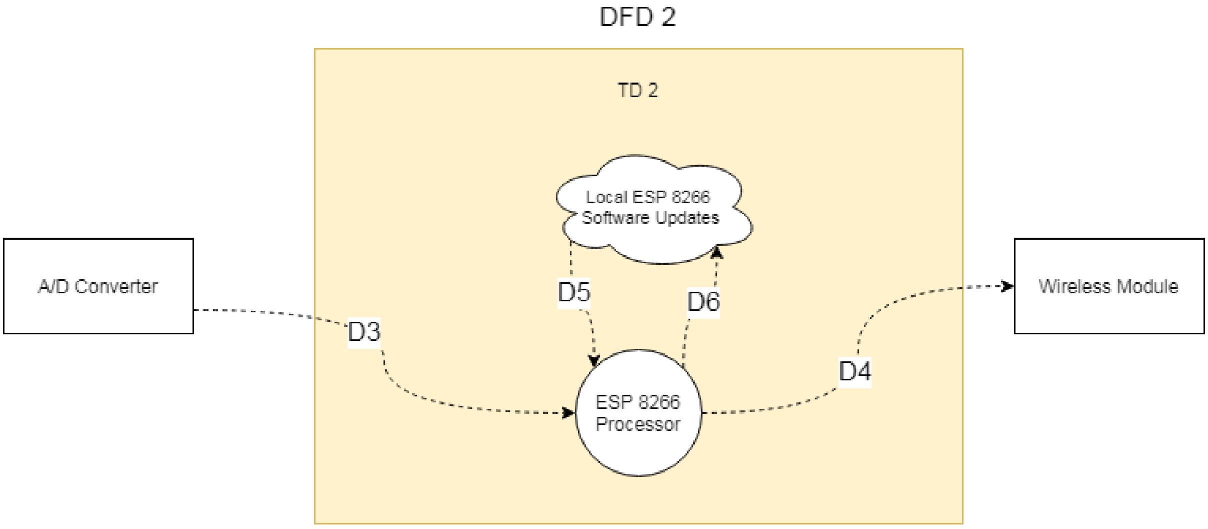


Figure 4: DFD for TD2 (ESP 8266 & SW Updates)

Data Flow Descriptions

Table 1 details all data flows, their descriptions, which trust domain it is associated with and the threat entries (Trubnikov et al., 2019).

Table 1: Data Flow Descriptions

DF ID	DF Description	Trust Domain	Threat Entry/Exit
D1	Data Transmission to Wireless Module from ESP 8266	TD1 & 2	Wireless Module
D2	Data Transmission from Wireless Module	TD1	Wireless Module
D3	Data from A/D Converter	TD2	ESP 8266
D4	See D1	TD1 & 2	Wireless Module
D5	Local SW Update	TD2	ESP 8266 Processor & Local ESP8266 Software updates
D6	Local SW Update Request	TD2	ESP 8266 Processor & Local ESP8266 Software updates

Threat Modelling

The threat modelling process will follow a strict plan outlined below:

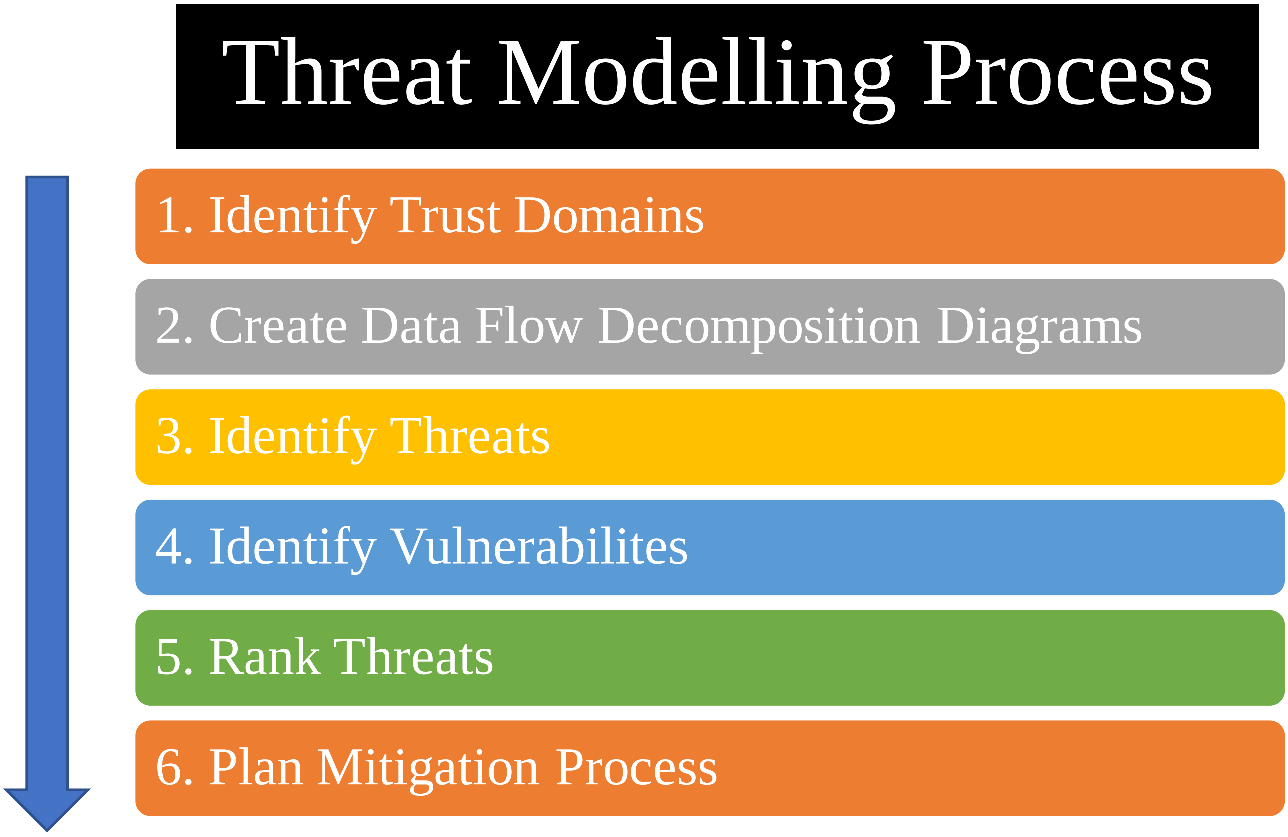

Threat Modelling Process
1. Identify Trust Domains
2. Create Data Flow Decomposition Diagrams
3. Identify Threats
4. Identify Vulnerabilites
5. Rank Threats
6. Plan Mitigation Process

Figure 5: Threat Modelling Process

Threat Identification

As threat modellers, we have identified TD1 and TD2 as the high-level vulnerabilities within the Daedalus project. We will focus on the data flowing between the Local SW Update Database to the ESP 8266, and the Wireless Module to the management module (M400). All flows in DFD1 and DFD2 will be examined thoroughly and then threats within them will be classified against the STRIDE methodology (Griffor, 2017). Where STRIDE (Flammini and SpringerLink, 2019) is:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

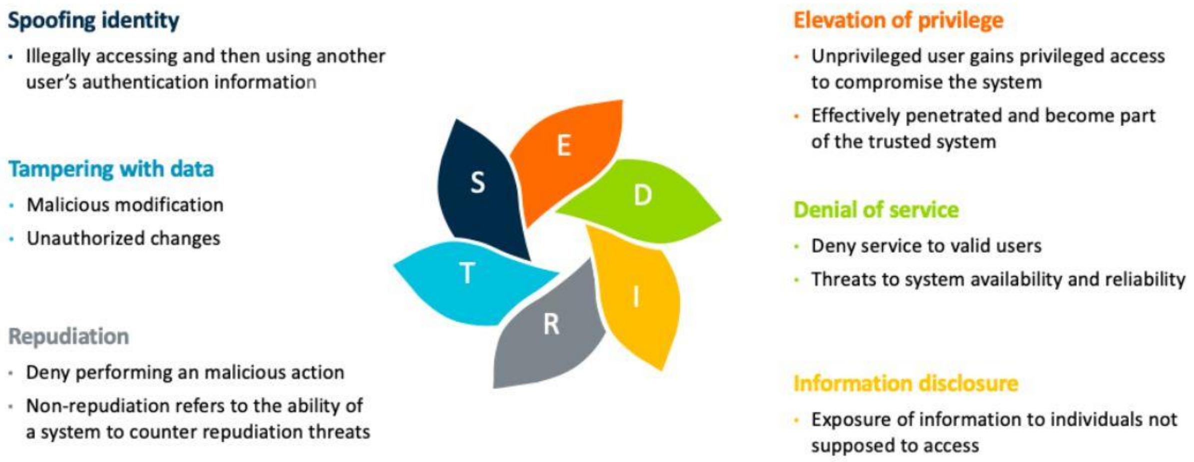

Spoofing identity
Illegally accessing and then using another user's authentication information
Tampering with data
Malicious modification
Unauthorized changes
Repudiation
Deny performing an malicious action
Non-repudiation refers to the ability of a system to counter repudiation threats
S
E
D
T
R
I
Elevation of privilege
Unprivileged user gains privileged access to compromise the system
Effectively penetrated and become part of the trusted system
Denial of service
Deny service to valid users
Threats to system availability and reliability
Information disclosure
Exposure of information to individuals not supposed to access

Figure 6: STRIDE (Avotis, 2021)

Table 2 shows threats that are assigned a STRIDE category and Threat ID along with a description of the threat. Table 2 shows all threats related to TD1 and TD2 for Daedalus. This threat assessment is based on public knowledge of cyber threats and cyber physical systems, no experts were consulted.

Each threat will then be evaluated through the DREAD methodology.

STRIDE

Table 2: STRIDE Threats for Wireless Module and Local SW Updates and ESP 8266

Data Flow	Trust Domain	Threat Entry	Threat ID	STRIDE	Threat Event
D1&D2	TD1	Wireless Module	1	S	IP Spoofing
D1&D2	TD1	Wireless Module	2	S	Client Imitation
D1&D2	TD1	Wireless Module	3	S	Credential Theft
D1&D2	TD1	Wireless Module	4	T	Data Replay
D1&D2	TD1	Wireless Module	5	T	Packet Injection
D1&D2	TD1	Wireless Module	6	I	Key Reinstallation Attack
D1&D2	TD1	Wireless Module	7	D	WIFI Jamming
D1&D2	TD1	Wireless Module	8	D	DDoS Attack
D1&D2	TD1	Wireless Module	9	E	Unauthorized Admin Access
D4	TD2	ESP8266	10	S	Unauthorized Access to Data Packets
D5	TD2	Local SW Repo	11	S	Copied Signed Software Signatures
D6	TD2	ESP8266	12	T	Unscheduled Update Requests
D5	TD2	ESP8266	13	T	SQL Injection [1]
D5	TD2	ESP8266	14	R	Unsigned Software Package
D5	TD2	ESP8266	15	I	Unauthorized Access to Software Repository

[1] Assumption made that Software Versions will be stored in an SQL compatible database.

Following threat identification, the Threat Modeller shall identify vulnerabilities which shall subsequently inform threat ranking via the DREAD methodology and will develop security test cases that can be used in development/improvement stages (Mittal and Tolk, 2020).

Threat Ranking

DREAD

DREAD is used to rank identified threats to then construct a robust mitigation plan. An average will be taken of all the categories to calculate an overall threat ranking. Table 3 shows my DREAD rankings for threats against Daedalus. Where DREAD (Jagannathan, 2020) is:

- Damage Potential
- Reproducibility
- Exploitability
- Affected Users
- Discoverability

Table 3: DREAD Ranking

Threat ID	STRIDE	Threat Event	Risk/Vulnerability	1 = Low, 5 = High					
				D	R	E	A	D	Average
1	S	IP Spoofing	Unauthorized Access through whitelisted IPs	3	2	3	5	1	2.8
2	S	Client Imitation	Impersonation of a legitimate account	5	4	5	1	2	3.4
3	S	Credential Theft	Access to legitimate account	5	5	5	5	1	4.2
4	T	Data Replay	Can allow intruder to view encrypted data or locate login details	3	2	1	1	1	1.6
5	T	Packet Injection	Gain access to data and network	5	3	1	1	1	2.2
6	I	Key Reinstallation Attack	Confidential information will be exposed	5	1	2	1	3	2.4
7	I	Eavesdropping	Stolen Credentials	4	2	3	2	2	2.6
8	D	WIFI Jamming	Attack will restrict WIFI access and will have access to block transmissions	3	5	2	5	1	3.2
9	D	DDoS Attack	Abuse of resources – will reduce capacity of processors	4	5	3	5	1	3.6
10	E	Unauthorized Admin Access	Run commands and access files that would otherwise be unauthorized	5	5	1	1	1	2.6
10	S	Unauthorized Access to Data Packets	Could be used to identify confidential info or to craft malicious packets	5	5	3	1	1	3

11	S	Copied Signed Software Signatures	ESP8266 would assume the SW is correct and safe when it is not – could lead to intrusion	5	3	1	5	1	3
12	T	Unscheduled Update Requests	ESP8266 could update to old software with vulnerabilities allowing access to attackers	5	2	1	5	1	2.8
13	T	SQL Injection [1]	Unauthorized command execution, table creation, deletion	5	5	5	5	1	4.2
14	R	Unsigned Software Package	Can lead to the loss of data, integrity and privacy. It also can allow attackers to gain privileges and hide from security controls	5	5	5	5	1	4.2
15	I	Unauthorized Access to Software Repository	Malicious code could be added to the repository and sent to ESP8266	5	5	5	5	1	4.2

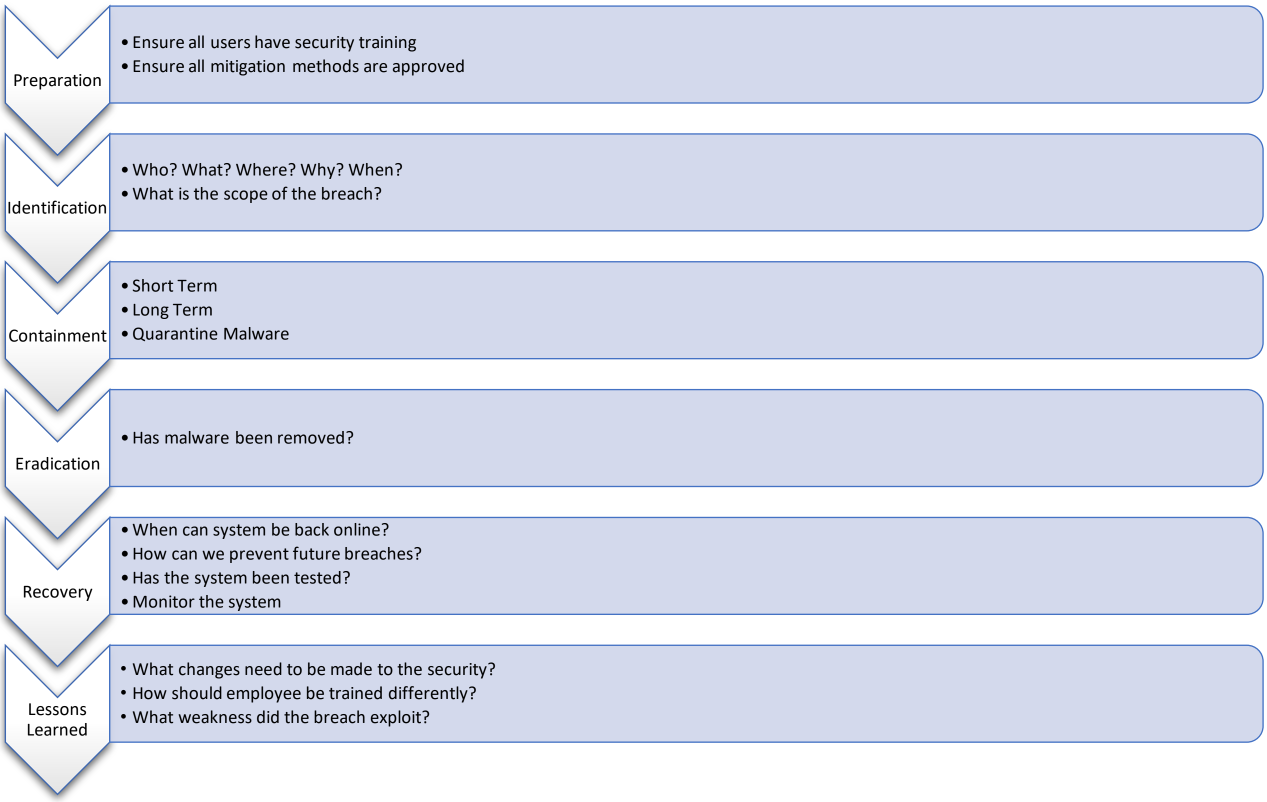
Threat Mitigation Plan

Plan Derivation

The plan will refer to and define security policies and processes which shall reduce impact of security threats. Threat mitigation can be broken down into three components, or layers of mitigation (Stroud, 2021):

- **Threat prevention:** Best practices and policies that protect corporate applications and data from being threatened by threat actors
- **Threat identification:** Security tools and management to identify active security threats
- **Threat remedy:** Strategies and tools to reduce the impact of active security threats that have gotten past corporate security defences and infiltrated the network by isolating or containing the threat.

Incident Response



Preparation
• Ensure all users have security training
• Ensure all mitigation methods are approved
Identification
• Who? What? Where? Why? When?
• What is the scope of the breach?
Containment
• Short Term
• Long Term
• Quarantine Malware
Eradication
• Has malware been removed?
Recovery
• When can system be back online?
• How can we prevent future breaches?
• Has the system been tested?
• Monitor the system
Lessons Learned
• What changes need to be made to the security?
• How should employee be trained differently?
• What weakness did the breach exploit?

Figure 7: Incident Response Cycle

Figure 5 shows the basis of an incident response plan (IRP) using the SANS Institute's 6 steps (Cassetto, 2018). These steps then inform the design of Figure 6 (Below) which shows are more tailored approach to an IRP for Daedalus. By acting before, during and after an attack you ensure the system in constantly monitored and allow for continuous improvement to be followed using agile best practices. Each section of the IRP relates to a distinct event within the threat modelling landscape and provides a clear framework to be followed.

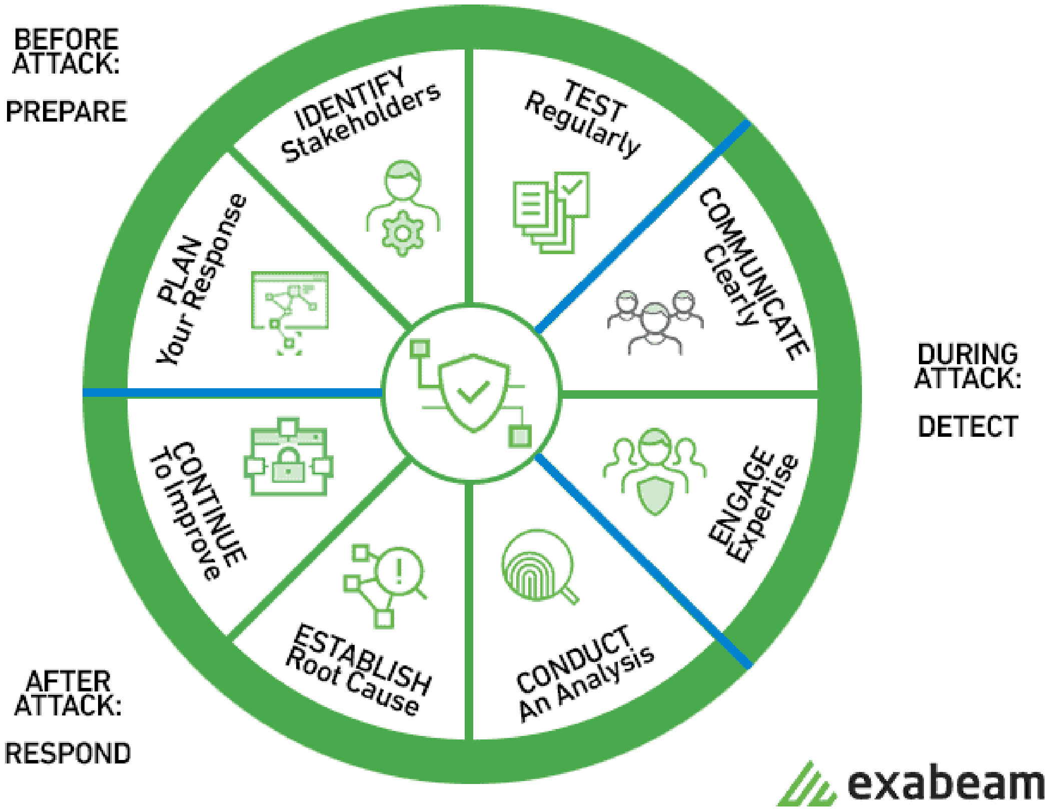
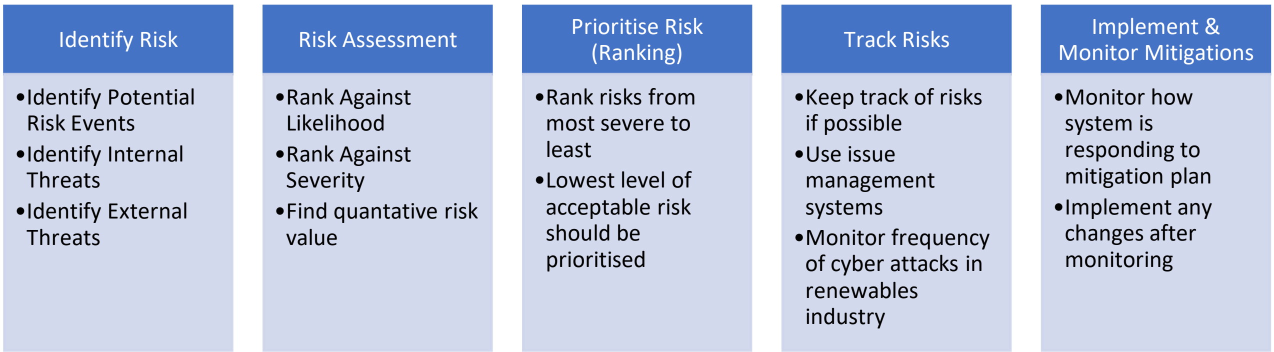


Figure 8: Elements of Incident Response (Cassetto, 2018)

IRP Rationale

1. PLAN – By planning we ensure a framework is followed that all users and systems can adopt to enforce consistency within the Daedalus Project.
2. IDENTIFY – By identifying stakeholders we ensure that all areas of the trust domains are covered with 100% coverage leading to a confident and accurate threat landscape.
3. TEST – By testing regularly we will allow for CI/CD and therefore will improve systems constantly and consistently without exposing new or old vulnerabilities.
4. COMMUNICATE – During an attack, by communicating clearly (which applies to humans and also Daedalus components) we will be able to identify threats and locate attackers or malware with ease.
5. ENGAGE – By engaging with experts and suitable software we shall be able to stop attacks more efficiently
6. CONDUCT – After the attack by conducting an analysis we will be able to visually view how the system was infiltrated and where our vulnerabilities lie and then mitigate those risks appropriately.
7. ESTABLISH – By finding the root cause, we can track the vulnerability back to its source which shall allow for more consistent threat detection.
8. CONTINUE – By combining our findings from point 6 and 7 we will be able to develop better security software and implement more efficient security measures to continually improve the Daedalus system.

Risk Mitigation



Identify Risk
- Identify Potential Risk Events
- Identify Internal Threats
- Identify External Threats

Risk Assessment
- Rank Against Likelihood
- Rank Against Severity
- Find quantative risk value

Prioritise Risk (Ranking)
- Rank risks from most severe to least
- Lowest level of acceptable risk should be prioritised

Track Risks
- Keep track of risks if possible
- Use issue management systems
- Monitor frequency of cyber attacks in renewables industry

Implement & Monitor Mitigations
- Monitor how system is responding to mitigation plan
- Implement any changes after monitoring

Figure 9: Risk Mitigation Plan

Actions

Table 4: Threat Action Table

Threat ID	**Threat Event**	1 = Low, 5 = High						**Action**
		D	**R**	**E**	**A**	**D**	**Average**	
1	IP Spoofing	3	2	3	5	1	2.8	Deploy Packet Filtering Systems, Utilization of firewalls, Upgrade to IPv6.
2	Client Imitation	5	4	5	1	2	3.4	Secure network with WPA2-PSK.
3	Credential Theft	5	5	5	5	1	4.2	Encrypt data using high level hashing algorithms. Strong encryption, strong passwords, adequate password policy.
4	Data Replay	3	2	1	1	1	1.6	Establish random session keys and implement timestamping methods
5	Packet Injection	5	3	1	1	1	2.2	Employ packet sniffing methods – i.e., Wireshark. Reject packets originating from outside your local network that claim to originate from within.
6	Key Reinstallation Attack	5	1	2	1	3	2.4	Disable EAPOL-Key frame re-transmission during key installation.

7	Eavesdropping	4	2	3	2	2	2.6	Authenticate incoming packets Use standards and protocols that provide authentication. TLS & SSL
8	WIFI Jamming	3	5	2	5	1	3.2	There are no ways to avoid this. Suggested action is to locate attacker.
9	DDoS Attack	4	5	3	5	1	3.6	Develop a DoS response plan, Practice early threat detection
10	Unauthorized Admin Access	5	5	1	1	1	2.6	Minimize number of admin accounts and disable any root or default accounts
10	Unauthorized Access to Data Packets	5	5	3	1	1	3	Access to raw data
11	Copied Signed Software Signatures	5	3	1	5	1	3	Implement single use software signatures
12	Unscheduled Update Requests	5	2	1	5	1	2.8	Encrypt update requests using hashing and salting to confirm authenticity of requests
13	SQL Injection [1]	5	5	5	5	1	4.2	Input Sanitation
14	Unsigned Software Package	5	5	5	5	1	4.2	Reject any unsigned packages
15	Unauthorized Access to Software Repository	5	5	5	5	1	4.2	Implement firewalls and credential keys.

Table 4 displays the advised actions to secure the Daedalus Project from cyber or physical attack. Each action will then be monitored following the Incident Response Plan and the Risk Mitigation Plan defined above.

Conclusion

The majority of threats identified in TD1 and TD2 have a vulnerability associated with them that can be avoided or mitigated by including more robust encryption techniques and following cyber security, risk management and threat modelling best practices. The highest ranking threats are SQL Injection, Access to SW Repository, Unsigned Software Package and Credential Theft. These should not be accepted risks and should be mitigated properly. In total there were 5 counts of *Spoofing*, 4 counts of *Tampering*, 2 counts of *Information Disclosure*, 2 counts of *Denial of Service* and 1 count of *Elevation of privilege*. Spoofing is a major concern for the Daedalus Project.

In general, the countermeasures address all properties of CIA. Confidentiality will be ensured via cryptographic controls. Integrity will be ensured by validating incoming data and software updates via the method of check sums and similar methods. Availability will be ensured by minimizing the chance of DDoS attacks.

Bibliography

ADEPU, S., BRASSER, F., GARCIA, L., RODLER, M., DAVI, L., SADEGHI, A. & ZONOUZ, S. Control Behavior Integrity for Distributed Cyber-Physical Systems. 2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS), 21-25 April 2020 2020. 30-40.

AVOTIS. 2021. *Threat Modelling* [Online]. Available: https://avotis.com.sg/threat-modelling/ [Accessed 5th April 2020].

CASSETTO, O. 2018. *Incident Response Plan 101: How to Build One, Templates and Examples* [Online]. Available: https://www.exabeam.com/incident-response/incident-response-plan/ [Accessed 30th March 2021].

CISCO. 2014. *The Internet of Things Reference Model* [Online]. Available: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf [Accessed 20 March 2020].

FLAMMINI, F. & SPRINGERLINK 2019. *Resilience of Cyber-Physical Systems From Risk Modelling to Threat Counteraction*.

GRIFFOR, E. 2017. Handbook of system safety and security : cyber risk and risk management, cyber security, threat analysis, functional safety, software systems, and cyber physical systems.

JAGANNATHAN, V. 2020. *Threat Modeling* [Online]. OWASP Foundation. Available: https://owasp.org/www-pdf-archive/AdvancedThreatModeling.pdf [Accessed 25th March 2020].

KRAVETS, A. G., BOLSHAKOV, A. A. & SHCHERBAKOV, M. V. 2020. Cyber-Physical Systems: Industry 4.0 Challenges.

MITTAL, S. & TOLK, A. 2020. Complexity challenges in cyber physical systems : using modeling and simulation (M & S) to support intelligence, adaptation and autonomy.

STROUD, F. 2021. *Cyber Security Threat Mitigation* [Online]. Available: https://www.webopedia.com/definitions/cyber-security-threat-mitigation/ [Accessed 28th March 2021].

TRUBNIKOV, I. V., MINAKOVA, O. V. & KURIPTA, O. V. Framework for Building Data Flow Diagramm Based Applications. 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), 1-4 Oct. 2019 2019. 1-5.