## Research Proposal

## Research Title

## The Design and Development of a sports stadium monitoring and management system to provide early threat detection and prevention of cyber threats to Cyber Physical Systems (CPS).

## Supervisors

* First Supervisor: Cathryn Peoples
* Second Supervisor: Doug Millward

## Introduction

Currently, there exists risks to data confidentiality, integrity and availability (CIA) and to human life within sports stadiums (Benslimane, 2022; Wan et al., 2021). CPS are growing in numbers globally, however the security measures in sports stadiums in which to protect them are not keeping pace (Baker, 2020). Manufacturers and sports organisations are producing these effective and efficient devices, including CCTV cameras, access control systems, and alarm systems, without having sufficient foresight to the consequences of them being breached. In a sports stadium, where many people gather, the results could be devastating. Breached devices could be maliciously used to lure crowds into danger, while access to turnstiles could result in them being locked, keeping patrons in bottle necked areas makes it easier to launch subsequent terrorist attacks. Denial of service (DoS) attacks could be launched to render systems inoperable, causing loss of revenue, dissatisfaction amongst fans and reputational damage to the organisation. Compromise of in-game CPS or Internet of Things (IoT) technology could be used to influence the outcome of a game, and insecure apps and networks could result in patron data being compromised, leading to identity fraud and resulting in heavy fines for the organisation.

Attackers able to successfully breach a sport stadium device, data or network, could potentially access any other device connected to that network (Melander, 2017), or even the corporate network from such a foothold. Corporate networks in sports stadiums are generally much better protected than IoT, Operational Technology (OT) or CPS networks (NCSC, 2020), as the effects of malicious activity is well understood and documented. While this is important, it is equally necessary to protect all connected devices.

Sports stadiums are particularly vulnerable targets due to their capacity to hold several thousand people in a relatively concentrated area. Additionally, sports mega events are often televised and international tournaments may bring increased attention from hacktivists or provoke politically driven attacks from nation states (Benslimane, 2022).

The National Center for Spectator Sports Safety and Security (NCS4), an academic organisation dedicated to protecting spectators of sport (NCS4, N.D.), have teamed with the Cybersecurity and Infrastructure Security Agency (CISA, N.D.) to provide a diagram where twelve example sports stadium vulnerabilities are described (CISA, N.D.). These vulnerabilities are listed in Table 1.

Table 1: Vulnerabilities and Consequences

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Name | Device | Vulnerability | Consequence |
| 0 | monitor | Central Control Monitor | No way to detect devices, such as online status | > Availability issues AND delays in detecting an attack |
| 1 | pos | Point of Sale (POS) | Outdated and unpatched firmware / software | > Attacker disables POS systems, resulting in loss of revenue and dissatisfaction among patrons |
| 2 | kiosk | Stadium Kiosk | No password to software / firmware | > Attacker shuts down ticketing system, causing unrest among patrons due to the inability to purchase tickets or be granted admission |
| 3 | entrance | Stadium Entrance Equipment | Device software lacks strong password protection | > Attacker hacks into control system and locks turnstiles, preventing entrance into the stadium. This causes mass gathering that makes the crowd vulnerable to a mass attack such as a bombing or an active gunman |
| 4 | cctv | CCTV | No segmented access controls and ACL | > Attacker disrupts CCTV and telecommunications, impairing communications with emergency services |
| 5 | telecomms | Telecommunications | Not segmented | > Attacker disrupts telecommunications with emergency services resulting in delayed response times |
| 6 | hvac | Heating, Ventilation, and Air-Conditioning (HVAC) | Not segmented | > Attacker raises temperature in server room causing servers to become overheated and shutdown |
| 7 | suas | Small Unmanned Aircraft System (sUAS) | No encrypted data link AND weak/no encryption keys | > Attacker introduces malware that distributes DOS attack, congesting networks and rendering dependent systems inoperable |
| 8 | smartgrid | Smart Grid | Smart grid meter memory, containing admin credentials, lacks encryption | > Attacker manipulates meter settings resulting in power outage (stadium / critical systems) |
| 9 | videoboard | Video Board and Public Address (PA) System | Control system is unsecured, leaving its video boards and PA system vulnerable | > Attacker displays or announces a threatening message, causing crowds to panic |
| 10 | fireandemergency | Fire and Emergency Management | Unmonitored | > Hacker sets off fire alarm system, causing patrons to panic and rush out of stadium |
| 11 | lights | Automated Lighting Controls | Fails to restrict remote access authorization to a need-to-have basis | > Attacker shuts down lighting in stadium causing patrons to rush out of the stadium, endangering lives |
| 12 | evcharging | Electric Vehicle Charging Station | No firewall | > Attacker steals patrons' credit card information > Displays threatening message on charging station, causing patrons to panic |

Proposed security controls to mitigate these include:

* Firewall – Control access and prevent unauthorised traffic entering the system.
* Segregated subnets – Provide an additional level of protection for devices, or secure access to the public without compromising the security of the main network. Common implementations of these in the real world include extranets, demilitarised zones (DMZ), virtual local area networks (VLAN) or guest networks, and could be achieved using firewalls and switches.
* Encrypted data links – Although data encryption is listed only by two or three examples in the diagram, due to a stadium’s relatively small size it makes sense that all traffic within a stadium network is encrypted, especially when any breach of data transmissions could result in the whole network being compromised.
* Firmware upgrade utility – Outdated firmware offers exploitable vulnerabilities discovered over time.
* Local logins for firmware – Hashed secure passwords are required to restrict access to the firmware
* Network log ins to software, with input validation applied to protect against injection attacks.
* Remote access capability for restricted users
* Monitoring capabilities – A monitoring device is important to watch continuously for important events across the other devices, including disconnections, reconnections, and alarms, where security personnel can be alerted in real time to ensure maximum uptime and safe operation of all connected devices.

More inter-connected devices make for a more immersive patron experience, however it also increases the stadium network attack surface. Therefore, it is imperative they are protected in line with expansion.

## Research Questions

1. How can the safety and security of cyber-physical systems in sports stadiums be improved?

## Aim

## To design and develop a prototype sports stadium management system which monitors cyber-physical systems in sports stadiums and provides pre-emptive detection and protection against DoS, Man in the Middle (MITM), sniffing, password cracking, vulnerability exploits, and identity theft cyber-attacks.

## Objectives

* To protect the CPS against DoS attacks and compromise within the sports stadium domain
* To create a prototype of the model, producing mitigations to the twelve risk examples listed in NCS4 and CISA’s integrated security considerations diagram
* To create a detailed report on the findings of the research

The model will be designed in accordance with the twelve example vulnerabilities, and as a result will provide an early detection mechanism for the following types of attacks:

* DoS / Distributed Denial of Service (DDOS)

The majority of security issues related to CPS in sports stadiums relate to DOS attacks. This is highlighted by the twelve examples of vulnerable devices listed in CISA and NSC4’s diagram. CPS devices often do not contain data that attackers will want to access. More crucially it is critical they remain available and operating in a safe and proper way to ensure patron safety in and around the stadium. Therefore, DoS attacks are a major concern for smart sports stadiums.

Detection of DoS attacks will be achieved through the monitoring facility to detect when remote cyber-physical systems are offline or otherwise not reporting properly.

The prototype will prevent the following attacks:

* Man in the Middle (MITM) – by encrypting the data in transit
* Sniffing – by encrypting the data in transit
* Password Cracking – by enforcing secure passwords
* Vulnerability Exploits – by providing a firmware update facility, firewall functions, and several other mitigations
* DoS / DDoS – which can also be prevented through a combination of all mitigations employed, together with network segregation to prevent intruders accessing sensitive system controls
* Identify theft – prevented in the case of the electric vehicle charging station by implementing a local firewall

Additional bonus features which are not necessarily related to the twelve examples include prevention of the following attacks:

* SQL Injection

Literature Review

The literature review is intended to follow a structure similar to the following:

# Introduction (1250 words)

* An introduction to IoT and its types
* CPS’s use in the modern world
* Security challenges in sports stadiums

# Smart stadiums and Cyber Security (1250 words)

* Which devices in a stadium are smart
* Consequences of compromise
* Examples of historic compromise

# IoT Technology and Cyber Security in sports (1500 words)

* The various current IoT technology uses and deployment methods
* The importance of securing IoT in sports stadiums
* How CPS is currently secured in sports stadiums?
* Ways in which CPS is lacking security in sports stadiums, and why

# Word count

Total estimated: (4000 words)

Methodology

Because the artefact will be created using software tools, the project will follow the scientific method (Figure 1), will require deductive reasoning, and quantitative data will be used to test the hypothesis (Miessler, 2020).

The project will be delivered using the Lean Software Development method. This is beneficial for solo projects, which facilitates regular communication and feedback with supervisors, possible changing requirements, small teams, and minimises waste by creating one piece of quality work at a time whilst minimising delays (MHZ Studio, 2021).

Although the planning approach will follow an Agile philosophy, a GANTT chart has also been created to help map the project’s progress, and work packages and milestones included to break the project into more manageable chunks (UOEO, N.D.).

An extensive literature review will then be undertaken to understand the extent of the problem and current state of the art. Once this is complete, the artefact will be more focused.



Figure 1: Scientific Method (sciencenotes.org, 2023)

The final report will also explain transparently how verification and validation were applied, including continuous dialogue with the project supervisors and testing of security controls. Furthermore, a project evaluation will be undertaken after the artefact has been created, including critically appraising the design, methods, and implementation of the project and artefact, with a final evaluation of the project outcomes including any limitations and deviations from the original plan.

The following project tasks will need to be executed:

1. State the problem and provide an overview of the subject area
2. List the requirements of the software
3. Design the software
4. Implement the software
5. Test the software
6. Write the report

## Hypothesis

That a successful model is created which monitors the status of CPS devices deployed in sports stadiums, using secure transmissions, providing an early warning of possible threats or malfunction, and mitigations to the defined vulnerabilities.

## Project Schedule

Both the 13,000-word report and artefact are expected to take approximately ten weeks each. The project timeline is shown in Figure 3.

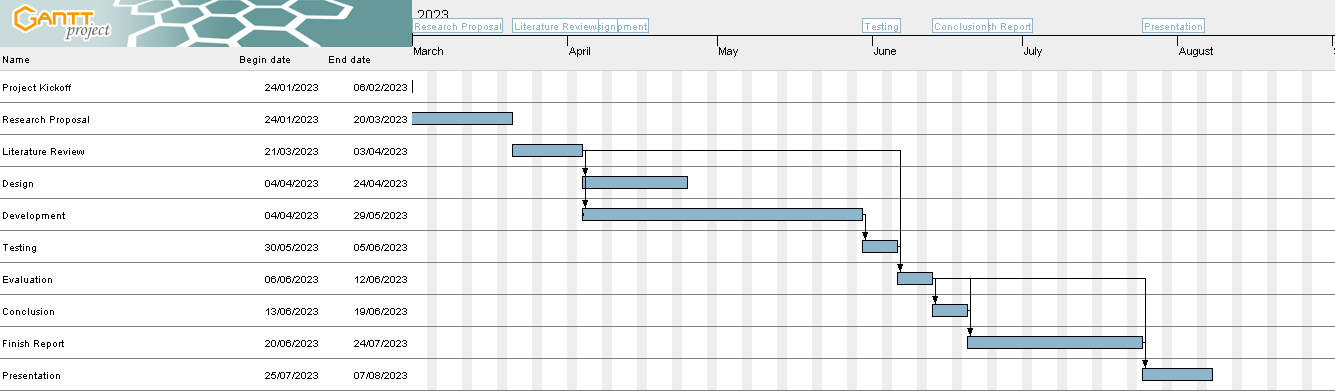


Figure 3: Project Timeline

## Project Breakdown

The project will be organised into work packages as shown in Figure 2.

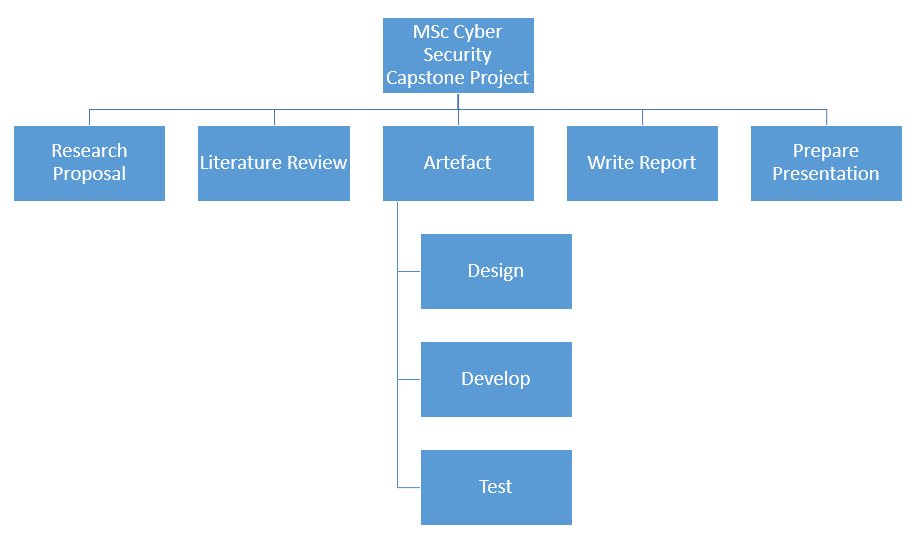


Figure 2: Project Work Packages

## Risks

Project risks include:

## Insufficient knowledge of the technologies required to create a working model. To counteract this, substantial research into the technologies likely to be used will be conducted, focusing on areas which are applicable to the project. This will be achieved using resources such as LinkedIn Learning, YouTube, and the Internet generally.

## Insufficient time to complete either the model or report. To counteract this:

## A project plan in the form of a Gantt chart will be created. This will help keep the project on track, act as a reminder for remaining work, and combat any procrastination. Redundancy will be built into the schedule to protect against unforeseen circumstances.

## A work / study / life balance will need to be achieved. For this, a strict regime will need to be followed, allowing for breaks and daily domestic duties. Redundant time will be used where possible to focus on completing the project in good time.

## Misinterpretation of the requirements. To counteract this, regular contact with the assigned supervisors, who have invaluable experience and expertise, will be maintained.

## Not enough information to create the report. This will likely mean that the research is not likely to meet the requirements of a master’s level dissertation. Obvious counteractions to this would be to:

## Carry out more research

## Make use of the available capstone project resources

## Regularly consult with the assigned supervisors

1. Data loss. To counteract for this, regular backups of the data will be made.

Artefact

The artefact will be produced using a mixture of technologies including Python and MQTT, and encapsulated in containers held on Docker Desktop to simulate the various CPS devices within a stadium. UML diagrams and a network diagram will be used for the design.

The model will include a variety of security controls which aim to mitigate each of the twelve vulnerabilities described by the NCS4 and CISA in their integrated security considerations diagram. The prototype model will also include a central monitoring node to check all systems are reporting ok, and all data sent between devices and the central monitoring screen will be encrypted.

It is possible that only some examples will be taken from the full quota of twelve, due to likely time constraints. The decisions on which vulnerabilities will be mitigated in the prototype model will be chosen using the MoSCoW approach (Monday, 2022).

As this module requires a computing artefact to be created, the type of project will therefore be software development (UOEO, N.D.).

A test plan will be created to test the quality of the code, the effectiveness of the security controls and the system as a whole. This will be recorded to video once complete and uploaded with the rest of the documentation.

Finally, the project will be critically evaluated, and then written up with full conclusions and referenced using the Harvard referencing style.

## Project Resources

The following technologies will be used to develop the artefact: MQTT, Python, Linux, Docker Desktop.

## CyBOK

This project research aims to help further the Infrastructure Security CyBOK Category and the associated Cyber-Physical Systems Security Knowledge Area (NCSC, 2019).

## References

Baker, P. (2020) The Rise of Cyberthreats in Sports. Available from: <https://professional.uchicago.edu/stories/master-science-threat-and-response-management/rise-cyberthreats-sports> [Accessed 06 March 2023].

Benslimane, K. (2022) Protecting global stadiums and events with Self-Learning AI. Available from: <https://darktrace.com/blog/protecting-global-stadiums-and-events-with-self-learning-ai> [Accessed 27 February 2023].

Bukey, D. (2020) Argonne scientists lead push to strengthen cybersecurity in sports stadiums. Available from: https://www.anl.gov/article/argonne-scientists-lead-push-to-strengthen-cybersecurity-in-sports-stadiums [Accessed 18 February 2023].

Cybersecurity & Infrastructure Security Agency. (N.D.) About CISA. Available from: <https://www.cisa.gov/about> [Accessed 06 March 2023].

Cybersecurity & Infrastructure Security Agency. (N.D.) STADIUM SPOTLIGHT: CONNECTED DEVICES AND INTEGRATED SECURITY CONSIDERATIONS. Available from: <https://www.cisa.gov/stadium-spotlight-connected-devices-and-integrated-security-considerations> [Accessed 06 February 2023].

Darling, G. (2021) IoT vs. Edge Computing: What’s the difference?. Available from: <https://developer.ibm.com/articles/iot-vs-edge-computing> [Accessed 18 February 2023].

Khalifa, N.A (2020) IDENTIFICATION AND PREVENTION OF EXPECTED CYBERSECURITY THREATS DURING 2022 FIFA WORLD CUP IN QATAR. Journal of Poverty, Investment and Development. 5(1): 49-84. DOI: <https://doi.org/10.47604/jpid.1135>

Melander, B. A. (2017). Smart stadiums: An illustration of how the “Internet of things” is revolutionizing the world. *Sports & Entertainment Law Journal Arizona State University.* 6(2): 350-382. Available from: <https://asuselj.org/wp-content/uploads/2017/08/Melander-Smart-Stadiums.pdf> [Accessed 18 February 2023].

MHZ Studio. (2021) Applying Lean in Software Development. Available from: <https://www.youtube.com/watch?v=uZ_uG28ZQSM> [Accessed 25 February 2023].

Miessler, D. (2020) The Difference Between Deductive and Inductive Reasoning. Available from: <https://danielmiessler.com/blog/the-difference-between-deductive-and-inductive-reasoning> [Accessed 14 February 2023].

Monday.com. (2022) The MoSCoW prioritization method explained. 22 September 2022. *project-management.* Available from: https://monday.com/blog/project-management/moscow-prioritization-method/#:~:text=The%20acronym%20MoSCoW%20stands%20for,to%20resolve%20conflicts%20between%20stakeholders. [Accessed 14 February 2023].

NCS4. (N.D.) National Center for Spectator Sports Safety and Security. Available from: <https://ncs4.usm.edu> [Accessed 06 March 2023].

NCSC. (2019) CyBOK The Cyber Security Body of Knowledge. <https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf> [Accessed 14 February 2023].

NCSC. (2020) The Cyber Threat to Sports Organisations. Available from: https://www.ncsc.gov.uk/files/Cyber-threat-to-sports-organisations.pdf [Accessed 06 March 2023].

Roberts, F. S. (2019) From Football to Oil Rigs: Risk Assessment for Combined Cyber and Physical Attacks. *Journal of Benefit-Cost Analysis.* 10(2): 251 - 273. DOI: https://doi.org/10.1017/bca.2019.15

Sciencenotes.org. (2023) Steps of the Scientific Method. Available from: <https://sciencenotes.org/steps-scientific-method> [Accessed 14 February 2023].

Solovev, A. & Petrova, A. (2020) Reasons and Peculiarities of Choosing MQTT Protocol for Your IoT Devices. September 10, 2020. *Integra Sources Blog.* Available from: <https://www.integrasources.com/blog/mqtt-protocol-iot-devices> [Accessed 06 March 2023].

University of Essex Online. (UOEO) (N.D.) Software Development. Available from: <https://www.my-course.co.uk/Computing/Cyber%20Security/CYSPROJ/CYSPROJ%20Lecturecast%204/content/index.html#/lessons/b-geZlb5JM4I0hp9xRVXjcGltldoYPCD> [Accessed 14 February 2023].

University of Essex Online. (UOEO) (N.D.) Work Packages. Available from: <https://www.my-course.co.uk/Computing/Cyber%20Security/CYSPROJ/CYSPROJ%20Lecturecast%203/content/index.html#/lessons/lnP5c3GVPaYQjzvjuFbnhrI_P5BpWCKZ> [Accessed 14 February 2023].

Wan, B., Xu, C., Prasad Mahapatra, R. & Selvaraj, P. (2021) Understanding the Cyber‑Physical System in International Stadiums for Security in the Network from Cyber‑Attacks and Adversaries using AI. *Wireless Personal Communications*. 127: 1207-1224. DOI: https://doi.org/10.1007/s11277-021-08573-2