Securing Sheffield's Fun Run: A Comprehensive Analysis of the S-FUN Drone Monitoring System

Group: H - COM6017 Security of Control and Embedded Systems
Team Member: Yan Kong, Ridza Adhandra, Xuantong Zhang, Weiqi Zhang, Mukta Choudhury

Date: 12 May, 2024

1. Introduction

1.1 Overview of the Sheffield Fun Run Monitoring System (S-FUN)

The Sheffield Fun Run Monitoring System (S-FUN) is designed to ensure the safety and smooth operation of fun runs held in Sheffield. These events often involve thousands of runners participating in extended runs around the city, typically to raise money for charitable causes. To facilitate these events, parts of the city's road infrastructure are temporarily closed to vehicle traffic, ensuring the safety of the participants.

The S-FUN system employs a fleet of 12 drones, with 10 operational at any given time and 2 held in reserve. These drones are continuously monitored and controlled from a headquarters (HQ) located at Sheffield Town Hall. The HQ is staffed by three drone pilots, who can operate the drones either locally or remotely via high-speed broadband connections.

A map was made on how the S-FUN is going to take place in Sheffield. Please note that a lot of assumptions were used when the map was designed.

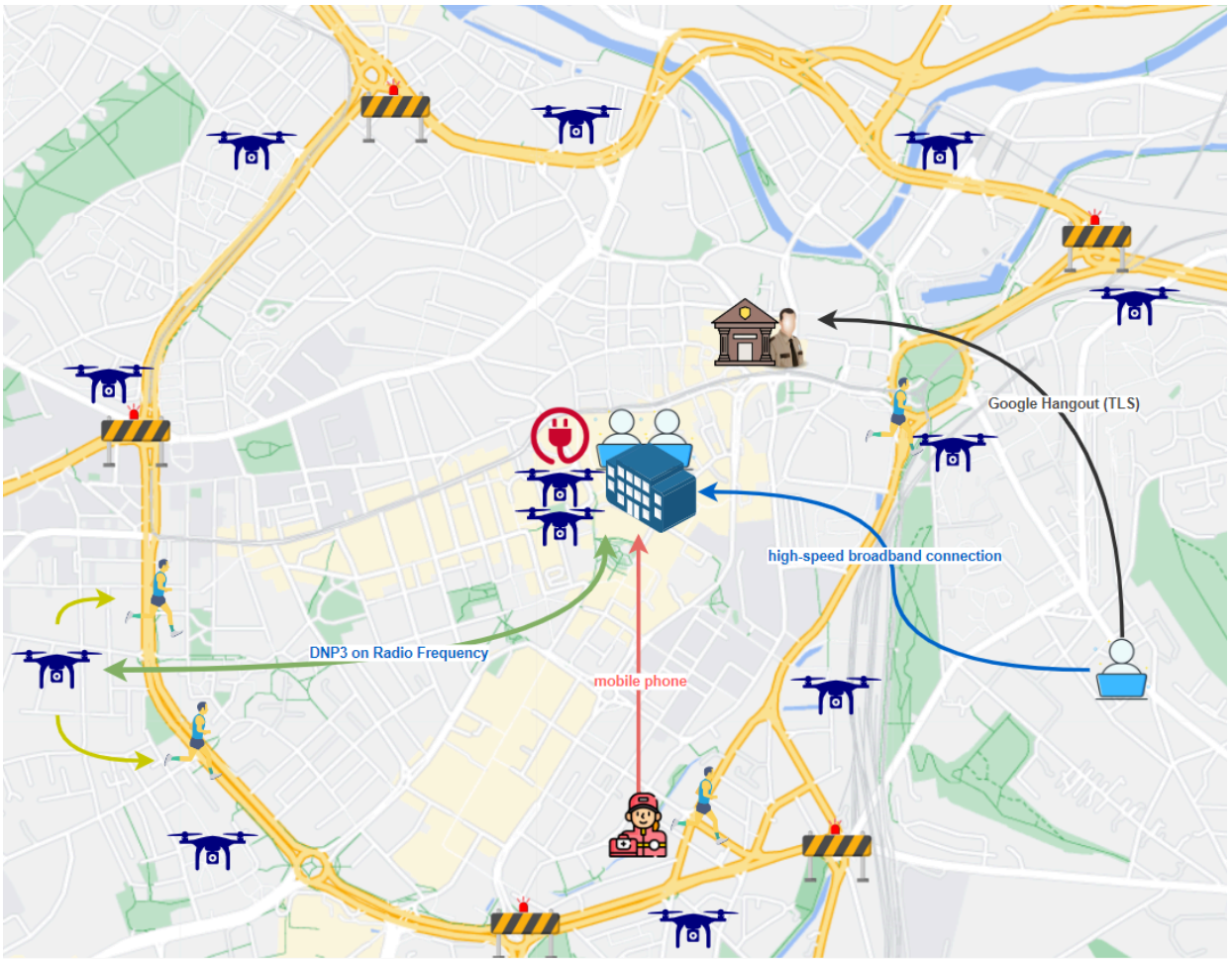

Figure 1: S-FUN Map of Sheffield

2. Identification of the System

The system identification of S-FUN as a fun runs monitoring system will be based on The OWASP Foundation Security Threat Modelling. The Identification will start with the trust level, a documentation of Cybersecurity-relevant Roles that have access rights to the system, both physical and abstract assets. Then this trust level will be cross referenced with the list of the assets of the system. [1]

2.1 Cybersecurity-Relevant Roles (Trust Level)

ID	Name	Description
1	HQ Control System Admin	The administrator who can configure the S-FUN control system and server at the HQ.
2	Drone Pilot	The pilot who flies the drone directly from the HQ. They need a password to access the system.
3	Remote Drone Pilot	The pilot who accesses the HQ control system remotely. They need a password to access the system remotely.
4	Maintenance Staff	Maintenance of the drones who have direct access to the drones.
5	Sheffield Town Hall staff	Town hall staff who may have direct physical access to the system.
6	Police	Police can be contacted by pilots through a dedicated Google Hangouts meeting secured by passwords and TLS. They have indirect access to the system.
7	Paramedics	They communicate with HQ via mobile phones to respond to runners in distress. They have indirect access to the system

Table 1: Trust level of the S-FUN

2.2 Physical Devices and Systems

The list of inventories will include numbers indicate the trust level of the system:

ID	Name	Description	Trust Level
1	Drones	12 total, including 2 spares. Used for monitoring the event. Key for surveillance and ensuring the safety of participants.	2, 3, 4
2	Drone Batteries	20 total batteries, 10 for spares. Drones need these batteries to fly. It takes 30 minutes to charge a battery to full	4
3	Battery Charging Stations	Used to recharge drone batteries	4
4	HQ server	A server for control terminal and to store video and audio stream from the drones	1, 2, 3
5	Mobile Device	Mobile Devices for contacting the paramedics	1, 2, 7
6	Remote Computers	Remote computers for remote pilots	2

Table 2: Inventory of Physical Devices and Systems of S-FUN

2.3 Software Platforms and Applications

The list for software and applications also will include trust level. The list as follows:

ID	Name	Description	Trust Level
1	Drone Control Software	Allows pilots to control and monitor drones.	1, 2, 3
2	HQ Control Terminals	Where drone pilots monitor video feeds and control drones.	1, 2, 3
3	HQ Storage Server	Stores video and audio streams from the drones.	1, 2, 3
4	HQ server	A server for control terminal and to store video and audio stream from the drones	1, 2, 3
5	Remote Access Software	Allows pilots to control drones and access video feeds remotely.	3
6	Google Hangout	Software to communicate with the police	1, 2, 3, 6

Table 3: List of software and applications of S-FUN

2.4 Data Flow Diagram and Pseudocode of DNP3

The data flow diagram will show the data flow between all parties involved.

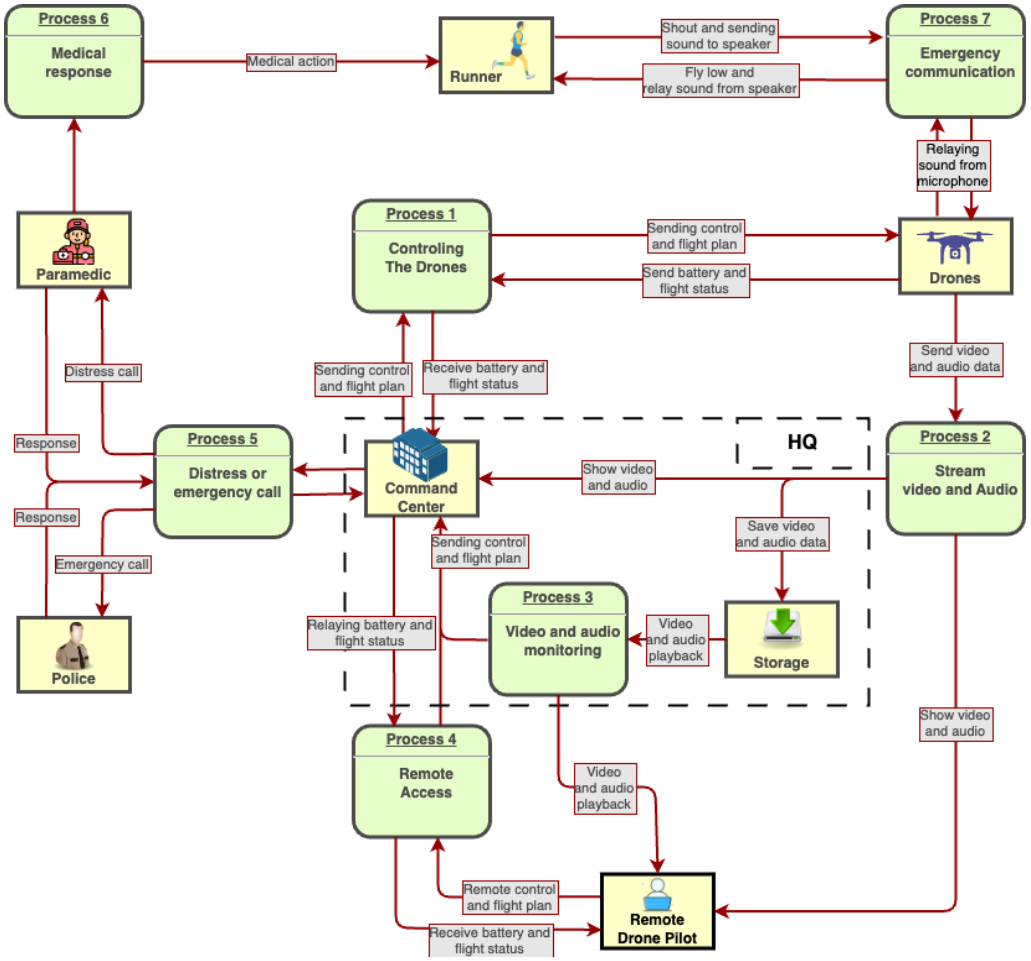

Figure 2: Data Flow Diagram of S-FUN

Both the command centre and storage server are located in the HQ (Town Hall). The pilots control the drones and receive battery and flight status from the drones, for on-site pilots' data stream happens from the HQ while remote pilots happen through remote access (process 1 and 4). On the Other hand, the drones also send video and audio streams to pilots, both in control centre and remote pilots, and to storage servers (process 2). If needed, the pilots can replay video and audio from the server (process 3). The command centre may send a distress call and ask for help (process 5). If there is a security emergency, Google Hangout will be used to communicate with the police. If something happens with the runner, the pilots can see and communicate with the runner through the drones (process 7). Mobile phones will be used by the pilots to call paramedics if the runner is in need. Then the paramedics will give medical treatment to the runner (process 6).

The data flow within S-FUN relies heavily on the Distributed Network Protocol (DNP3) for communication between the drones and the HQ control system. DNP3 is a set of communication protocols used for secure and reliable communication in supervisory control and data acquisition (SCADA) systems. [3] In S-FUN, DNP3 facilitates the transmission of control commands from the HQ to the drones and the continuous streaming of video and status updates from the drones back to HQ. The use of DNP3 ensures robust and efficient communication, which is critical for real-time monitoring and control during the event.

Here is a simplified pseudocode description of the DNP3 protocol's basic operation:

Python

```
Initialize DNP3 protocol
Establish RF communication channel

While system is operational:
    For each drone in operation:
        Send control commands to drone via DNP3
        Receive status updates and video streams from drone
        If communication with drone is lost:
            Attempt to re-establish communication for up to 5 minutes
            If communication is not restored:
                Command drone to return to HQ and land

    Monitor DNP3 communication for anomalies
    If anomaly detected:
        Alert system administrator
        Log details of the anomaly for further investigation
```

Figure 3: pseudocode of DNP3

2.5 External Information Systems

External information systems are external information systems to the S-FUN that may pose a threat to the system. These systems are technically still within the control of the organisation, but possibly not within the control of the development team [7].

These are the external information systems that were integrated with S-FUN:

- With the assumption that HQ server is not developed by the S-FUN developers, the HQ server will depend on its operating system. Although it is possible some modifications were made to the OS of the server to suit the S-FUN purpose.
- Assume that all the drones were bought from external parties, then the control system of the drones should be made by the same party. S-FUN developers may adjust the control system to suit their needs.
- The communication between S-FUN system operators and the paramedics will depend on the mobile network.
- The Google Hangouts over TLS will be used to make communication with the police.

3. Identification of Security Threats (STRIDE Framework)

To identify and analyse potential security threats to S-FUN, we applied the STRIDE framework. STRIDE categorises threats into six types: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. This method ensures a comprehensive assessment of vulnerabilities and risks associated with the system.

Threat Category	Threat	Potential Attack Method	Mitigation Strategies
Spoofing	Unauthorised Drone Control via GPS Spoofing	Attackers can exploit the drone's reliance on GPS for navigation by manipulating GPS Signals. This could be done using: Overt Spoofing: Transmitting a stronger GPS signal to override the legitimate signals, leading to incorrect drone positioning or behaviour. Covert Spoofing: Gradually replacing the legitimate GPS signal with a fabricated one, causing the drone to follow an incorrect path without detection.	Integrated Multi-Navigation Systems: Equip drones with a combination of GPS and other navigational aids like inertial measurement units (IMUs) and visual navigation systems to validate GPS data and detect discrepancies. Encryption and Signal Authentication: Implement encryption measures and signal authentication to safeguard against unauthorised GPS signal interference. Regular Security Audits and Firmware Updates: Ensure that drone software is up to date with the latest security patches that address vulnerabilities to GPS spoofing. Use of Radar and Advanced Detection Systems: Employ radar systems capable of detecting unusual drone flight patterns or deviations from pre-set routes, indicating potential spoofing. Implement digital beamforming techniques to enhance the detection capabilities.

	Identity Theft	Identity theft can occur when attackers gain unauthorised access to the credentials of drone operators or system administrators. This can be achieved through various methods including: Phishing Attacks: Trick users into providing login information. Brute Force Attacks: Use automated software to generate and try a large number of credentials. Keylogging: Malware that records keystrokes to capture credentials. Spoofing Trusted Networks: Creating fake Wi-Fi networks to intercept data transmitted by users.	Robust Authentication Protocols: Implement multi-factor authentication systems that require more than one piece of evidence to verify a user's identity. Regular Security Training: Educate staff about the risks of phishing and other social engineering tactics. Advanced Encryption Standards: Encrypt data transmissions to prevent unauthorised interception and access. Continuous Monitoring and Detection: Use security software that detects and alerts on unusual access patterns or unauthorised access attempts.
	Communication Spoofing in Google Hangouts	Communication spoofing can occur when attackers gain unauthorised access to video conferencing sessions. This could be achieved through: Intercepting Communications: Using network sniffing tools to capture unencrypted data transmitted during a conference. Account Hijacking: Gaining access to conference controls by stealing host credentials through phishing attacks or malware. Fake Video/Audio Injection: Injecting misleading content into a live session to manipulate the event outcomes or to disseminate false information.	Strong Authentication Measures: Implement multi-factor authentication for all users accessing the conference system. End-to-End Encryption: Use encryption protocols to secure all forms of communication within Google Hangouts. Continuous Monitoring: Deploy network monitoring tools to detect and respond to unusual activities, which could indicate a spoofing attempt. User Education: Regularly train users on identifying phishing attempts and securing their account credentials.
Tampering	Data Manipulation	Attackers may intercept and alter the data transmitted from drones to HQ. This involves changing video, audio, or sensor data to present false information or hide genuine threats.	End-to-end encryption: Encrypting data at the source (drone) and decrypting it only at the destination (HQ) ensures that the data intercepted during transmission cannot be read or altered without detection. Checksums or hashing: Using this for data integrity ensures that any alteration of the data during transit can be detected before the data can be processed. Anomaly detection systems: Using machine learning algorithms to detect patterns or anomalies in incoming data can alert operators to potential tampering. This system can flag unexpected changes in data patterns that might indicate manipulation.

	Command Tampering	Altering commands sent from HQ to drones via interception of DNP3 communications by: Packet Sniffing: Using tools to capture DNP3 traffic and analyse command structures. Command Injection: Crafting and sending altered commands to drones. Man-in-middle-attacks: Intercepting and modifying commands in transit. Replay Attacks: Resending valid commands with malicious modifications or timings.	Encryption: Secure DNP3 communications to prevent interception and alteration. Authentication and Integrity Checks: Ensure commands are authenticated and unaltered before execution. Anomaly Detection: Monitor for patterns indicating MitM or replay attacks. Network Segmentation: Isolate control systems to limit access to critical communications.
	Battery Information Tampering	Manipulation of battery status data to mislead operators about drone power levels. Data Interception and Alteration: Attackers intercept the communication between the drone and the control system that transmits battery status data. Using a man-in-the-middle attack, they can alter this data before it reaches the operator. Exploitation of Software Vulnerabilities: Using a buffer overflow or SQL injection on the server handling the data, an attacker might alter stored values of battery levels.	Encryption: Utilise strong encryption protocols for all communications involving battery data to prevent unauthorised interception and alteration. Authenticated Messages: Implement message authentication codes (MAC) or digital signatures to verify the integrity and authenticity of battery status data received.
Repudiation	Untraceable Actions	Log Deletion or Modification: Attackers or malicious insiders can delete or modify logs or erase evidence of their actions. This could involve accessing log management systems to alter or remove logs that record their unauthorised activities. Use of Non-Traceable Tools: An attacker uses a live OS on a USB drive to access a system, leaving no traces on the hard drive after removal.	Immutable Logging: Implement systems where logs cannot be altered or deleted. Comprehensive Monitoring: Use real-time monitoring tools to detect changes to logging settings. Regular Audits: Conduct frequent security audits to review and verify logs and system configurations.

Information Disclosure	Leakage of Sensitive Data	Interception of Data Transmissions: Attackers could intercept unencrypted or poorly encrypted data as it travels from drones to the control system. This could include live video feeds or audio communication. Example: This could be done using packet sniffers. Access Through Compromised Accounts: Attackers use stolen credentials to access the drone's archival storage, downloading past mission videos containing sensitive location data. Exploitation of Software Vulnerabilities: Software flaws can be used to gain unauthorised access to data streams or stored data. Physical Access to Storage Media: Direct physical access to drones to extract data.	Encrypt Data: Use strong encryption for data at rest and in transit. Robust Access Controls: Regularly update and manage permissions and credentials. Patch and Update Software: Regularly update software to fix vulnerabilities. Enhance Physical Security: Secure drone storage and handling areas.
	Communication Interception	Eavesdropping on drone communication channels to steal operational data or personal information.	Secure Communication Protocols: Implement protocols like SSL/TLS or WPA3 for encrypted communications. Regular Security Updates: Continuously update and patch systems to defend against known vulnerabilities. Network Segmentation and Monitoring: Use network segmentation to restrict access to critical communication channels and monitor for unauthorised access points.
Denial of Service (DoS)	Network Flooding	Overloading HQ's network with traffic to disrupt communications and drone operations.	Implement anti-DDoS solutions, segregate network traffic, ensure redundant connectivity for critical systems.
	Drone Deactivation	Disabling drones through signal jamming, exploiting software vulnerabilities, or physical attacks, e.g. Using jammers to block or interfere with the communication frequencies used by drones.	Use anti-jamming technologies like frequency hopping, update drone software regularly, and enforce physical security.

Elevation of Privileges	System Takeover	Exploiting Vulnerabilities: Using known or zero-day vulnerabilities in the system to escalate privileges. Phishing Attacks: Deceiving system administrators into granting access or downloading malware that gives attackers elevated privileges. Credential Stuffing: Using stolen account credentials to gain unauthorised access to systems.	Regularly patch systems, conduct penetration testing, limit administrative access.
	Unauthorised Access to Restricted Areas	Bypassing Physical Security: Manipulating or bypassing physical security measures like locks or surveillance systems. Network Intrusion: Breaching network security to access restricted digital resources. Social Engineering: Tricking employees into providing access to restricted areas or systems.	Implement strong access controls, use surveillance and alarms, and conduct security audits regularly.

Table 4: Identification of Security Threats of S-FUN [4]

4. Security and System Requirements

Each asset within the system must be protected against potential threats, especially considering the intelligence received about possible disruptions from the Anti-Fun Alliance. This section aligns the system's assets with the NIST Cybersecurity Framework's PROTECT function subcategories to establish a comprehensive security posture. [2]

Category	Subcategory	Assets Addressed	Justification
Identity Management, Authentication, Access Control	Identity, credential management	HQ Control Server, Remote Access Systems, Drone Control Software	Strict identity and credential management ensure that only vetted and verified individuals can access critical systems, crucial for maintaining control and preventing unauthorised command executions.
	Physical access to assets protected	Drones, Battery Charging Stations, HQ Server	Restricting physical access is essential to prevent sabotage, theft, or unauthorised alterations, directly safeguarding the operational integrity of the entire monitoring system.
	Remote access to assets managed	Remote Access Systems, Drone Control Interfaces	Managing remote access through robust authentication protocols ensures that drone operations are controlled securely, mitigating risks of unauthorised access and manipulation from external threats.
	Access permissions and authorization managed	Drone Control Software, HQ Control Terminals, Remote Access Systems	Detailed access control policies are crucial for delineating clear operational boundaries, ensuring users can only access systems and data necessary for their roles, thus minimising potential security breaches.
	Network integrity protected	DNP3 Communication Systems, TLS-secured Networks	Ensuring network integrity protects against interception and manipulation of sensitive control and communication data, maintaining reliable and secure operational flows critical for event safety.
	Identities proved and bound to credentials	All User Devices and Control Systems	Binding identities to robust credentials ensures that each action within the system can be traced to an authenticated user, enhancing accountability and security.
	Users, devices, and assets authenticated	Drones, HQ Control Systems, Mobile Communication Devices	Implementing multi-factor authentication across devices and systems ensures that access is strictly controlled and verified, significantly reducing the risk of unauthorised access or spoofing attacks.
Awareness and Training	Users are informed and trained	All Staff (Pilots, Maintenance, HQ Personnel)	Comprehensive training on security protocols and operational procedures ensures all staff are equipped to handle security incidents, reinforcing system integrity and response capabilities.

	Privileged users understand roles and responsibilities	System Administrators, Drone Pilots	Empowering users with privileged access to understand their critical roles and responsibilities ensures they are vigilant and proactive in maintaining the system's security posture.
	Third-party stakeholders understand their roles	Paramedics, Police, External Support Teams	Educating all third-party stakeholders on their security roles and communication protocols enhances coordination and ensures a unified response to incidents, bolstering overall event security.
	Senior executives understand their roles and responsibilities	HQ Senior Management	Involving senior executives in understanding their oversight roles in security policy enforcement and resource allocation ensures top-down support and adherence to security practices.
	Physical and cyber security personnel understand their roles	HQ Security Staff, IT Support Teams	Clearly defined roles for security personnel ensure a cohesive and informed response to both physical and digital threats, maintaining a secure environment for the monitoring operations.
Data Security	Data at rest protected	HQ Video Storage, Mobile Devices, Backup Storage Devices	Protecting data at rest with encryption and access controls prevents unauthorised disclosure and manipulation of stored data, essential for maintaining the confidentiality and integrity of operational information.
	Data in transit protected	Drone Video/Audio Feeds, Mobile Communications	Encrypting data in transit shields it from eavesdropping and tampering, ensuring that real-time operational data remains confidential and integral during transmission.
	Assets formally managed (removal, transfers, disposition)	Drones, Batteries, Mobile Devices	Proper lifecycle management of physical assets prevents unauthorised reuse or disposal, ensuring that all components remain secure throughout their operational life.
	Adequate capacity to ensure availability	Network Infrastructure, Server Capacity	Maintaining adequate system and network capacity prevents bottlenecks and failures, ensuring reliable and continuous operation critical for real-time monitoring and response.

	Protections against Data Leaks	All Networked Systems and Storage Devices	Implementing stringent controls and monitoring for data leaks ensures that sensitive information remains within the secured network perimeter, protecting against external breaches and insider threats.
	Integrity checking mechanisms (software, firmware, information)	Control Software, Communication Protocols, Servers	Regular integrity checks validate the authenticity and unchanged state of the system's software and firmware, crucial for detecting and mitigating the impact of malicious modifications.
	Development and testing environments are separate	Development and Operational Software Environments	Isolating development from production environments prevents inadvertent exposure of vulnerabilities and ensures stable, secure deployment of technologies.
	Integrity checking mechanisms verify hardware	Drones, HQ Control Equipment	Frequent hardware inspections ensure that physical components are not compromised, maintaining operational trustworthiness and security against tampering.

Table 5: Security and System Requirements of S-FUN using NIST Protect Functions [5]

By systematically aligning each asset of the S-FUN system with the NIST PROTECT function subcategories, we can create a robust security framework that mitigates potential risks. This proactive approach not only safeguards the system against known threats but also enhances its overall resilience.

5. Privacy Challenges

5.1 Identification of Privacy Attack

The identification will be focusing on the privacy challenges that S-FUN faced, followed by the attack scenario that hypothetically could happen. This attack then will be analysed with the DREAD threat modelling framework.

Privacy Challenges

The primary privacy challenge of S-FUN is the risk of unauthorised surveillance. The drones are able to capture continuous video and audio from public spaces, these video and audio may include privacy for individuals such as runners, and raises concerns over how this data is handled, stored, and accessed. There is potential of data misuse.

The unauthorised surveillance may cause the leak of the private information. Such as leading to scenarios where individuals' movements and actions are monitored, recorded, and potentially exploited without their knowledge or consent. [6]

As the DNP3 protocol lacks the identity authentication mechanism [7] impersonators can obtain DNP3 response messages by eavesdropping to obtain PLC and CS communication addresses, causing malfunction. An attacker can exploit a CS vulnerability to obtain native sensitive information, send a malicious command to the PLC, and tamper with the response message of the PLC.

The following figure shows an abstraction of typical data flow in a similar system.

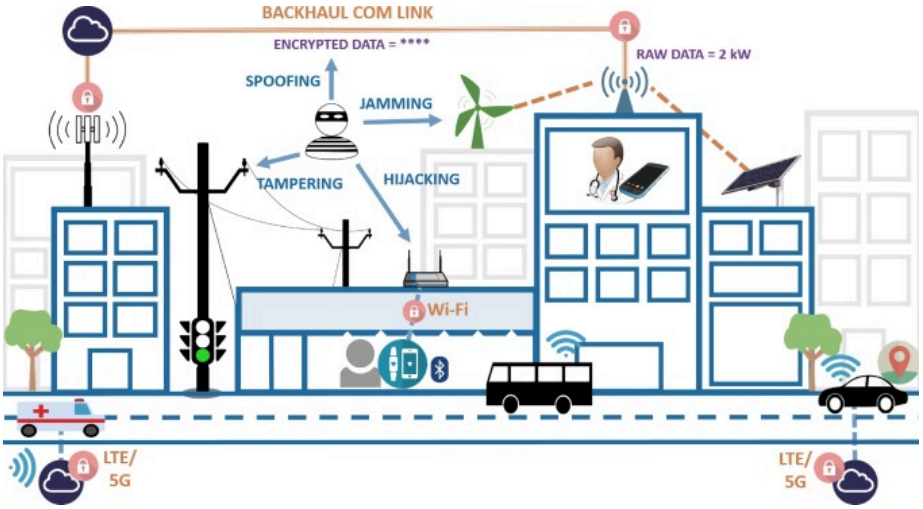

Figure 4: The adversary can target the system during sensing, transferring, and processing of data. The complexity of the system structure provides more opportunities for the adversary. [8]

Hypothetical Attack Scenario: Unauthorised Access to Video Sources

One plausible privacy attack involves an external attacker gaining unauthorised access to live video feeds or stored video archives from the drones. This could occur through exploiting vulnerabilities in the communication protocol (DNP3) used by the drones. Attackers can exploit a configuration software (CS) vulnerability to obtain native sensitive information. According to Bagaria (2011) [3], if the attacker steals the pre-set key through the controlled CS, the DNP3-SA security improvement protocol based on the authentication of both parties can't prevent such attacks.

5.2 DREAD Scoring and Justifications

1) Damage Potential (8/10): If an attacker gains access to video feeds, the damage could be significant. It could lead to the invasion of privacy of thousands of runners and spectators, with sensitive personal information potentially being exposed or misused.
2) Reproducibility (6/10): The complexity of the attack depends on the security measures in place. However, given enough technical skill and knowledge of the DNP3 protocol, an attacker could potentially replicate the attack.
3) Exploitability (5/10): While exploiting the system requires specific knowledge and skills, vulnerabilities in older protocols or unpatched systems could lower the difficulty for experienced attackers.

4) Affected Users (9/10): The number of affected individuals could be extensive, including all runners and any individuals caught in the drones' video feeds. This widespread impact amplifies the severity of the privacy breach.
5) Discoverability (7/10): Given the increasing awareness and tools available for cybersecurity exploits, the chance of attackers discovering vulnerabilities in the system is significant. [9]

6. Anomaly Detection

An established security method with many applications is anomaly detection [10]. It may be used to detect misuse in online social networks, identify possible insider threats within businesses, and protect server applications in high-risk contexts. Technical challenges faced by anomaly detection systems include the requirement to accurately recognise a variety of typical patterns and reduce the number of false positives. They also use similar methods for evaluation and detection, such dimensionality reduction, experimental assessment, and feature extraction.

Machine learning is used to use sophisticated techniques to extract meaningful, novel, potentially useful, and successful patterns from (often large) datasets in a particular subject of interest [11]. When faced with new or unseen data instances, machine learning algorithms seek to identify complex patterns within data sets to support well-informed decision-making or predictions. Bhattacharyya uses machine learning techniques to find anomalous properties in computer systems connected in a network. This includes a study of the vulnerabilities that networks face at various layers due to flaws in protocols or other reasons. He used probabilistic learning, combinatorial learners, supervised learning, unsupervised learning, soft computing, and probabilistic learning to handle network intrusions. To provide a clear understanding of each strategy's capabilities, a thorough analysis and assessment of these strategies is included.

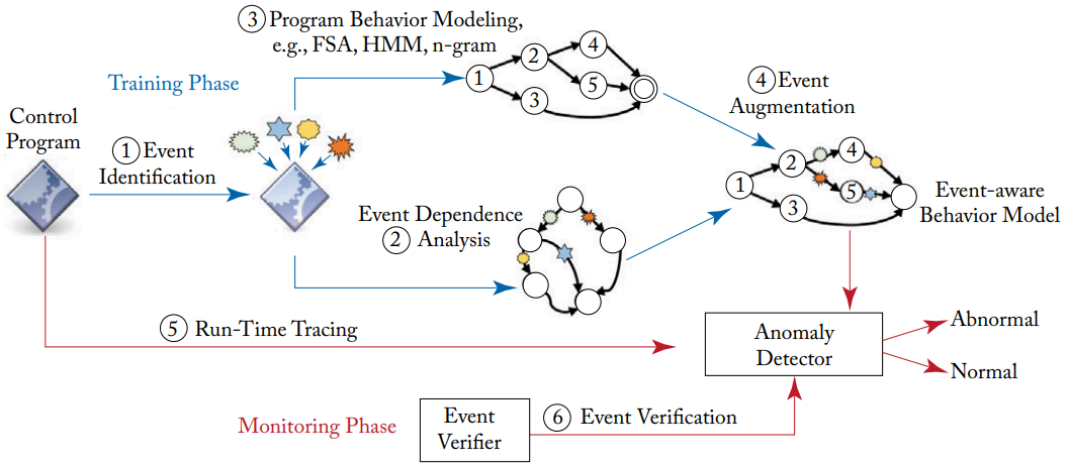

Figure 5: Workflow of the event-aware anomaly detection framework. [12]

To maintain the security and integrity of S-FUN, a variety of technologies can be used to identify unusual or malicious activity. Anomaly detection based on machine learning is one such technology. Here's how it could be implemented:

1) Monitoring and Gathering Data

Make use of the drones' current data streams, including telemetry, audio, and video feeds. To create a baseline of regular behaviour, gather data on normal operations from past fun runs.

2) Feature Extraction

Identifying and separating relevant traits from the collected data is the process of feature extraction. Analysing drone activity entails tracking flying patterns and altitude variations. Strange flight paths or unusual height changes are a couple of examples of anomalies.

Initial task: Monitor and record user login behaviours, the frequency with which instructions are received, and other relevant activity. Unusual command sequences or occurrences of unauthorised logins are two examples of abnormalities.

Communication mode: Keep an eye on the communication's frequency and protocol. Atypical data transmission or irregular communication channels are examples of abnormalities.

3) Machine Learning Model Training

Depending on whether labelled data is present, train a machine learning model using the obtained data, emphasising either supervised or unsupervised anomaly detection techniques.

Supervised Learning: A supervised model, such as Support Vector Machines or Random Forests, may be trained to classify occurrences as normal or anomalous when there is tagged data, such as known assaults or anomalies.

In situations when labelled data is scarce, unsupervised learning is employed. To find deviations from the predicted normal behaviour in such cases, techniques such as Gaussian Mixture Models, Autoencoders, and Isolation Forests can be used.

4) Real-Time Anomaly Detection

Use the trained model to watch incoming data in real-time, continually. Signal as possible anomalies any departures from the established regular behaviour. Among the anomalies might be: Drones that drastically deviate from their approved flying routes Abrupt discontinuation or modification of communication habits. Unusual activities (such as hostile behaviour directed at runners or unauthorised access to the route) discovered in video or audio feeds. Suspicious network traffic suggesting cyberattacks.

5) Reaction Mechanism

Upon detecting an anomaly, initiate the relevant steps to alert the drone pilot or control centre staff to the issue. Take the specified security actions—such as rerouting drones, turning on additional security, and alerting law enforcement—to deal with the anomaly. If necessary, automatically isolate or shut down problematic components to stop further harm or compromise.

6) Model Refinement

Refine the anomaly detection model iteratively by adding new data and refining existing ones with input from users. Incorporate feedback from security professionals and system operators to improve the model's responsiveness and accuracy. Through the use of Machine Learning-based Anomaly Detection,

S-FUN enhances the security and reliability of the fun run monitoring system by precisely recognising and responding to anomalous or malevolent acts.

7. Team Collaboration Tool

We use **Google Space** as a collaboration tool which we found to be very useful. It significantly enhanced our team's communication and project management.

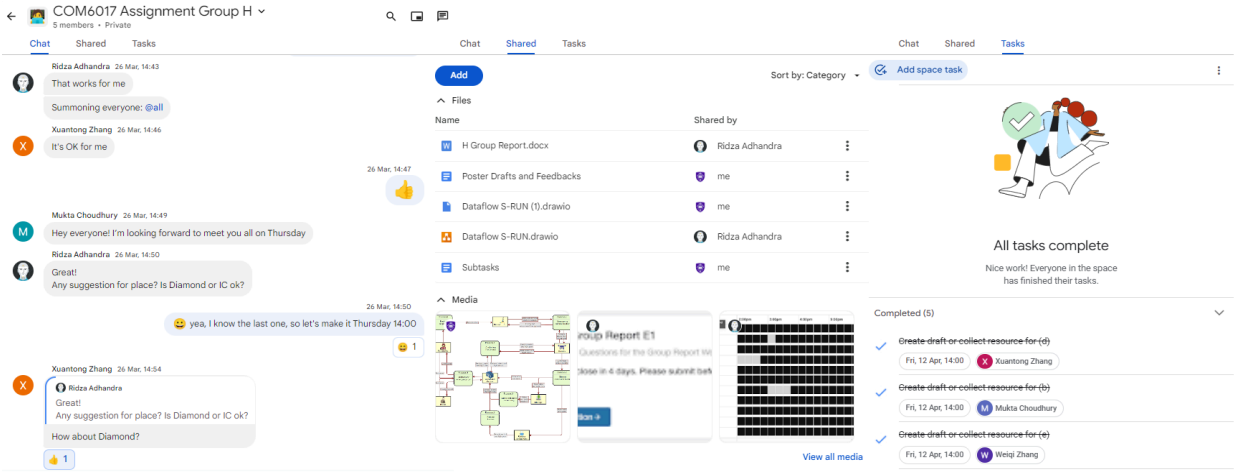

Figure 6: Our Team Collaboration in Google Space (Chat, Shared Docs, Tasks)

How it helped us:

1) Integration: Google Space's all-in-one platform integrates various functionalities, facilitating communication and project management without the need to switch between different applications.

2) Real-Time Communication: The instant messaging feature and the ability to create different chat rooms for various aspects of the project fostered timely discussions and decision-making.

3) Task Management: The tasks feature allowed for clear assignment and tracking of responsibilities and deadlines within the same environment used for communication.

4) Meeting Scheduling and Integration: Direct integration with Google Calendar made it easier to schedule meetings and ensure everyone was aware of upcoming deadlines and discussions.

Areas for improvement:

1) Project Management: While Google Space integrates various tools, it lacks a dedicated project management function for more complex project tracking and visualisation.

   Suggestion: Integrating or linking with a dedicated project management tool like Trello or Asana could enhance tracking project progress, dependencies, and milestones more effectively.

2) Engagement and Formality: Depending on the team's discipline, the chat-based platform might lead to less formal communication, which can affect the seriousness with which tasks are approached.

   Suggestion: Establishing clear communication guidelines can help maintain a professional tone.

8. Summary of Contributions

Both Ridza Adhandra and Yan Kong shared responsibility for overseeing the overall project, working in a complementary manner. All team members were very cooperative and actively participated in the group work. It was a very pleasant experience, with everyone contributing effectively to achieve our common goals.

Team Member	**Contribution**	**Note**
Yan Kong	Identification of the System and assets	Coordinated the overall project and managed team meetings. Compiled the final report.
Ridza Adhandra	NIST PROTECT function analysis	
Xuantong Zhang	DREAD threat modelling for privacy challenges	
Weiqi Zhang	Anomaly detection recommendations	
Mukta Choudhury	Threats analysis using STRIDE framework	

9. References

[1] Almuhammadi, Sultan, and Majeed Alsaleh. "Information security maturity model for NIST cyber security framework." Computer Science & Information Technology (CS & IT) 7.3 (2017): 51-62. https://www.csitcp.com/paper/7/73csit05.pdf

[2] Greer, Chris, et al. "NIST framework and roadmap for smart grid interoperability standards, release 3.0." (2014). https://doi.org/10.6028/NIST.SP.1108r3

[3] Bagaria, Sankalp, Shashi Bhushan Prabhakar, and Zia Saquib. "Flexi-DNP3: Flexible distributed network protocol version 3 (DNP3) for SCADA security." 2011 International Conference on Recent Trends in Information Systems. IEEE, 2011. https://doi.org/10.1109/ReTIS.2011.6146884

[4] Yao, Danfeng, et al. Anomaly detection as a service: challenges, advances, and opportunities. Morgan & Claypool, 2018. https://link.springer.com/book/10.1007/978-3-031-02354-5

[5]Bhattacharyya, D.K., Kalita, J.K., 2014. Network anomaly detection: a machine learning perspective. Boca Raton: CRC Press, Taylor & Francis Group, 2014, Boca Raton.

[6] Greer, C., Wollman, D.A., Prochaska, D., Boynton, P.A., Mazer, J.A., Nguyen, C., FitzPatrick, G., Nelson, T.L., Koepke, G.H., Jr, A.R.H., Pillitteri, V.Y., Brewer, T.L., Golmie, N.T., Su, D.H., Eustis, A.C., Holmberg, D., Bushby, S.T., 2014. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. NIST.

[7] Threat Modelling Process | OWASP Foundation [WWW Document], n.d. URL https://owasp.org/www-community/Threat_Modeling_Process (accessed 5.7.24).

[8] Yao, D. (Daphne), Shu, X., Cheng, L., Stolfo, S.J., 2022. Anomaly Detection as a Service: Challenges, Advances, and Opportunities, 1st ed. Netherlands: Springer Nature, Netherlands.

[9] Bhattacharyya, Dhruba Kumar, and Jugal Kumar Kalita. Network anomaly detection: A machine learning perspective. Crc Press, 2013.

[10] OWASP. (n.d.). Threat Modeling Process. Retrieved May 11, 2024, from https://owasp.org/www-community/Threat_Modeling_Process#determine-and-rank-threats

[11] UK Government. (2022). Conducting a STRIDE-based Threat Analysis. Retrieved May 11, 2024, from https://www.gov.uk/government/publications/secure-connected-places-playbook-documents/conducting-a-stride-based-threat-analysis

[12] Bernabe, J. B., & Skarmeta, A. (2022). Introducing the challenges in cybersecurity and privacy: The European research landscape. In Challenges in Cybersecurity and Privacy-the European Research Landscape (pp. 1-21). River Publishers. eBook ISBN9781003337492