University of Sheffield

# COM6017 Security of Embedded and Control Systems

# Group Report : Analysis of a Drone System


Group Report Team 7: Abrar Alhejaili, Adeleke Adelaja, Anna Liu, Jagpreet Jakhar, Jiaqi Gu

Department of Computer Science

May 17, 2023

## Declaration

The team agrees that all members of the team have made reasonable contributions to the work recorded in the report.

# Abstract

In completing this team assessment, our team extensively utilized remote collaboration tools, mirroring the collaborative dynamics commonly observed in real-world scenarios. We were given the flexibility to choose the specific tools that best suited our needs. The primary objective was to produce a comprehensive report that documented the following key elements: Firstly, we conducted an in-depth analysis to identify security threats to the system, drawing upon available threat models and presenting our findings in a structured manner using STRIDE threat modelling. Secondly, we formulated a set of security requirements encompassing physical, logical (electronic), and procedural aspects that should be implemented within the system. Moreover, we explored and identified the major challenges associated with privacy, proposing feasible approaches to address them. Similarly, we examined the significant challenges related to safety and dependability, outlining practical strategies to mitigate these risks. Reflecting on our collaborative efforts, we assessed the factors that either facilitated or hindered our teamwork. Specifically, we highlighted the collaborative tools we employed, such as shared calendars and remote conferencing platforms like Blackboard Collaborate, Google meet, WhatsApp Communities and evaluated their success. Furthermore, we briefly suggested improvements that could enhance the efficacy of such tools. To accurately summarize the individual contributions made by each team member, we reached a consensus statement affirming that all members had made reasonable contributions or indicating any discrepancies. Additionally, we provided a table summarizing how each team member contributed.

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Report

## 1.1 Identification of security threats to the system. You should use available threat models to inform your work where possible and present your work in a suitably structured way. You should not address privacy concerns at this point

According to [1] threat modeling is a core task that analyzes the applicable threats to elicit security requirements early in a system's life cycle. The goal is to identify threats from the attacker and the defense perspective and to establish communication and coordination between all stakeholders to mitigate risks. Hence, a structured approach to threat modeling presents the advantage of adequately identifying, quantifying and mitigating the system risks. As such, the *STRIDE* methodology is applied to address the use case presented in the report.

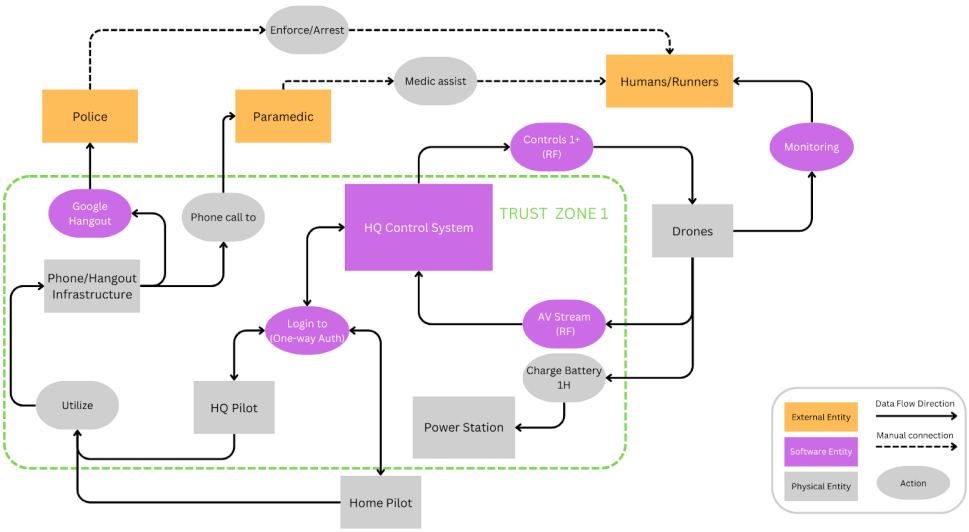


**Figure 1.1:** *System Data Flow Diagram (DFD)*

- **Entry Points** are interfaces that potential attackers can use to exploit the system:

**Table 1.1:** *Entry Points*

| SN | Name | Description | Trust Levels |
|---|---|---|---|
| 1 | Login System | Pilots must log in to the control system hosted in HQ | 1.Anonymous user<br>2.Authorized user with valid login<br>3.Adversary with invalid login |
| 2 | RF protocol | Streaming communication between drone and HQ | 1.Anonymous user<br>2.Authorized user in HQ<br>3.Adversary outside HQ |
| 3 | Mobile phone | Communication between Paramedics and HQ | 1.Anonymous user<br>2.Paramedics<br>3.Authorized user in HQ<br>4.Adversary outside HQ |
| 4 | Drone Audio Visual | Audio Visual (AV) service is used to capture and monitor motion and sound and stream them to HQ | 1.Anonymous user<br>2.Authorized user in HQ<br>3.Adversary outside HQ |

- **Assets** are systems, devices, and non-digital entities that a potential attacker is interested in and are classified as the following asset types:

**Table 1.2:** *Assets*

| ID | Asset Type | Description |
|---|---|---|
| 1 | Software Related | Login and control center<br>Server<br>Key Management System<br>Mobile communication service<br>Internet and Internet Services (Google Hangout)<br>RF Comms Services |
| 2 | Electrical Power | Battery<br>Battery Charging Station |
| 3 | External Entity | Authorities (Paramedics and Police)<br>Humans (runners, pedestrians, travellers, and residents)<br>Weather |
| 4 | Physical Process | Access to mobile communication.<br>Access to the battery storage and charging station.<br>Aerial access to the routes.<br>Access to drone audio-visual components.<br>Entry to city council and data centre. |
| 5 | Information Asset | Identity and Access Management data<br>Flight plans<br>Surveillance (Audio/Visual) data |

- **Assumptions**

  As we analyze the security of our headquarters, we assume that the staff are trustworthy and operating within security guidelines. However, it is important to note that there is a single trust boundary, which means that a threat adversary could potentially operate from within if they gained physical access. This is especially concerning since the trust boundary is located in a public space. When examining the authorized physical and logical access to different system components, we must consider external entities that have indirect control over the system. We have identified three operator groups - paramedics, police, and pilots working from home - who pose potential security risks. It is crucial to recognize that all parties' devices could be compromised, even those of pilots working from home. For example, an adversary could steal or hijack a pilot's device and use social engineering tactics to conceal their true intentions and exploit the system.

- ***STRIDE* Approach to Threats**

  *STRIDE*[2] is a methodology for threat modeling. It consists of the initials of the following six threats: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

  *Spoofing* is a dangerous threat in which attackers can send harmful messages to important services like paramedics, pilots, drones, and the police by gaining unauthorized access to phone lines, RF signals, and internet connections. There are two ways this can happen: the attacker can pretend to be the HQ and deceive pilots with fake feedback or impersonate paramedics with virtual phone numbers and fabricated news. This can cause confusion and lead to dispatching police by mistake. Any channel without proper encryption is at risk of this type of attack.

  *Tampering* with data and *Information Disclosure* are two other potential threats. Attackers who gain unauthorized access can manipulate drone data, flight plans, audio-visual signals, system logs, and other confidential data. If the drone is accidentally captured, personal data breaches or undetectable data tampering can occur. Physical damage to the drone's storage is also possible. IoT devices are also vulnerable if attackers can gain privileged access to relevant hosts within the subnet. For example, attackers can tamper with the charging status, which will mislead pilots in charge of battery exchange, or they can collect the status and inform their accomplices when to perform the DoS attacks.

  *Repudiation* is when attackers compromise the system to cover their tracks. This can happen in the preparation phase by malicious implantation. Attackers can then send authenticated but unexpected commands to the system, which may cause disorder or damage to the system that is non-traceable.

  *Denial of Services* occurs when attackers physically damage the RF receivers to force all drones back to HQ, eventually denying the service. They can use RF devices to flood the communication system between drones and the HQ. A compromise of the battery charging dock can also prevent battery recharging, leading to a degradation of service as fewer drones will fly at any time to conserve battery.

  *Elevation of Privilege* is when attackers escalate their limited access to root access, giving them control of the entire system. This can happen through attacks like SQL injection, password enumeration, or exploitation of vulnerable protocols. Attackers can find the IP address of the HQ or any other relevant host within one network using dedicated search engines like Shodan or Zoomeye.

## 1.2 A set of security requirements that the system should implement. These should include physical, logical (electronic), and procedural aspects.

Following are the recommended security requirements based on the perceived threats analyzed above :

- **Physical Security**

  Physical security is a constantly evolving and domain-specific concept. In this scenario, physical security refers not only to protecting assets from fire, water, static electricity damage, or similar risks, but also to protecting the system by using guards, security gates, and monitoring systems[3].

**Table 1.3:** *Physical Security Objectives and Requirements*

| Security Objective | Assets/Personnel | Security Requirement |
|---|---|---|
| Monitoring | Drones, pilots, paramedics, and other staff | All places where personnel activities exist must be fully covered by monitoring cameras, human surveillance, and alarm systems. |
| Flight Security | Drones | Flight plans must be preapproved with Multi-Factor Authentication. Define and enforce collision and proximity rules for the drones to avoid crashing with other objects or accessibility to human reach[4]. |
| Access Control | ID cards (keys), and profile storage | ID cards for all personnel must be properly allocated and their profile must be safely stored and validated. Any unauthorized entry must be refused by using barriers (e.g., turnstiles). |
| Environment Control | Landing pad, charging station, equipment storeroom | All venues where equipment is kept or stored must be dry, free of static electricity, and free of explosion risks. |
| Intrusion Detection | All physical assets | All malicious entities need to be detected to prevent them from further cyberattacks or causing physical damage. |

- **Logical Security**

  In this scenario, logical security is closely related to information (data) security, although the two are not equivalent. Logical security consists of four concepts: data confidentiality, data integrity, data authenticity, and non-repudiation. This definition is system-specific and distinguishable from other kinds of security [5] Principle 3. [1]

[1] In addition to data in the traditional sense, "data" here also refers to firmware, software, operating systems, and other content stored in digital form.

**Table 1.4:** *Logical Security Objectives and Requirements*

| Security Objective | Assets | Security Requirement |
|---|---|---|
| Data Confidentiality | Any data in transmission or storage | All data must be applied with proper encryption and can only be accessed by authorized people. |
| Data Integrity | Any data in transmission or storage | Any tampering with the data must be detectable by using hash or signature algorithms. |
| Data Authenticity | Any data in transmission or storage | Only authenticated personnel or devices can be the source of data. |
| Non-Repudiation | Actions recordings systems | Any modification and query of data must be traceable to a specific person or device. |

- **Procedural Security**

  Procedural security refers to policies, terms, and codes of conduct specified to assist in achieving other security requirements.

**Table 1.5:** *Security Objectives and Requirements*

| Security Objective | Assets/Personnel | Security Requirement |
|---|---|---|
| Access Control | Pilots, paramedics, and other staff | Access rights must be clearly defined and all access actions must follow the restraint. Access to critical infrastructure must only be possible by authorized personnel and role-restricted. |
| Authentication | Drones, pilots, paramedics, and other staff | Multi-factor authentication should be used to increase the system's robustness. |
| Security Skill and Awareness Training | Pilots, paramedics, and other staff | All personnel must be trained properly to ensure that they will not become a breakthrough point of potential cyber-attacks. |
| Incident Response | Drones, servers, pilots, paramedics, and other staff | An incident response strategy must be specified, documented, and simulated prior with stakeholders to mitigate any attack that is not prevented. |

## 1.3 Identification of the major challenges to privacy posed by the system above. Indicate how these are or can reasonably be addressed.

As this is a public event and spread over at least 10km this may raise many issues relating to the privacy of citizens, some of which are:

- **Legal Issues**[6]
  - Several Laws may affect the operation of drones in this event such as the Data Protection Act 2018, the Surveillance Camera Code of Practice under the Protection of Freedoms Act 2012, and Civil Aviation Authority (CAA) Regulations.

  The operation of drones must be with principles of lawfulness, fairness, transparency, and purpose limitation, among others.

- **Consensual Issues**
  - Consent for Recording must be sought from participants and non-participants, and also consent for Recording in Public Spaces. The heights of drones must be calibrated according to CAA regulations depending upon the number of people.

  Following CAA guidelines and Informing individuals about the drone's presence, purpose, and the recording of personal data is crucial. Clear signage or public announcements can help raise awareness and allow individuals to make informed decisions.

- **Invasion of Privacy**[7]
  - Invasion of people who are not participating, for example, residents in their homes who may be recorded during the event.
  - Illegal recording by drones compromised by Anti-Fun Alliance.

  Drone flights should be planned to not invade privacy by the use of blurring or other processing techniques to safeguard their privacy.

- **Data Protection and Storage**
  - Data Security: The data stored at HQ must be encrypted and secured, and the transfer of data from drones to HQ should also be secured to prevent eavesdropping. However, the security need may need to be balanced against latency and operational needs
  - Data Minimisation: Data collected should be kept to a minimum and only the data which is within the scope of monitoring the S-FUN.
  - Data Storage: Data Stored on the HQ may be stored on a server located outside the jurisdiction of the UK, for example, the USA, which may raise privacy concerns.
  - Retention Period: Data collected during the event should not be kept for a long time, and if the event passes without any incidents should be deleted.

## 1.4 Identification of the major challenges to safety and dependability posed by the system above. Indicate how these are or can reasonably be addressed.

Drone accidents accounted for 18% of all accident reports according to Air Accident Investigation Branch's(AAIB) Annual Safety Report 2022[8]. The following are the challenges to safety and dependability :

- **Physical Safety**
  - According to AAIB, 53% of losses were caused by loss of control in flight. As drones weigh 15kg, they can hit with significant kinetic power to cause injuries.
  - Timing of closure and reopening of barriers to vehicles can cause accidents as 3 pilots may be controlling 10 drones and de-synchronisation may happen.
  - Evacuation by paramedics may be hampered due to road closures
- **Battery Issues**
  - The frequent need to replace drone batteries could affect the constant monitoring.
  - Faster Battery depletion due to windy conditions.
- **Weather Conditions**
  - Damage to drone components and functionality due to rain or water exposure.
- **Communication Loss**
  - Safety risks if drones operate without human control due to communication loss.
  - Automatic return to HQ after a period of lost communication.
- **Piloting Issues[9]**
  - 3 Pilots controlling 10 drones may cause stress and lack of situational awareness.
  - Unaccounted obstacles such as power lines for trams or trees can cause loss of drones[10].

The following measures can be taken to tackle the above challenges[10]:

- Proper Pre-flight Planning and pre-flight checks to ensure functioning equipment and clear flight paths and synchronize barrier placement.
- Separating Flight and monitoring teams for stress management and increasing situational awareness
- Drone hover and automatic return in case of communication loss is a good measure.
- Preempting the need for battery replacement to ensure continuous monitoring of events.
- Planning evacuation and emergency routes for ambulances, and paramedics.

## 1.5 A reflection on what helped team collaboration and what hindered it. In particular, you should indicate what tools you used to collaborate and assess the success of their use. Briefly suggest how such tools can be improved.

The following helped the team collaboration:

- Consultation regarding division of work, and providing timely and constructive feedback to work of team members.
- Effectiveness of communication, between members working on the same question, and the team as a whole.
- Openness to receiving feedback.
- Competency of every team member to tackle the assignment.
- Punctuality of all team members
- Availability of tools which allowed remote collaboration.

Only Hindrance was comparably lower productivity when working remotely, as work was done more efficiently when meeting in person, and non-availability of Group Study Rooms in The Diamond at appropriate times.
During our team collaboration, we utilized a variety of tools to facilitate communication and cooperation. These tools played a crucial role in our collaboration efforts, enabling us to overcome geographic barriers during Easter Holidays and work efficiently together.

- Blackboard Collaborate
    1. This was our primary tool for remote meetings, file sharing, and reading through the assignment which worked well.
    2. The video and audio quality can be improved upon and also sharing and displaying a shared document can be made more user friendly
- WhatsApp
    1. We used it quite successfully to arrange meetings, maintain workflow and keep ourselves updated.
    2. Adding a shared calendar feature to Groups would make organising meetings and workflow easy.
- Google Docs
    1. We used google docs to prepare initial drafts for our questions and brainstorming, Its feature to allow multiple simultaneous updates in the document was quite handy.
    2. Improvements can be made by adding more features such as producing flowcharts or other visualisation tools easily.

## 1.6 A table summarizing how each team member contributed.

| Team Member | Question a | Question b | Question c | Question d | Question e |
|---|---|---|---|---|---|
| Abrar Alhejaili | | | X | X | |
| Adeleke Adelaja | X | X | | | |
| Anna Liu | | | X | X | |
| Jagpreet Jakhar | | | X | X | X |
| Jiaqi Gu | X | X | | | |

**Table 1.6:** *Summary of Team Members' Contributions and Feedback*

# Bibliography


[1] S. M. Khalil, H. Bahsi, H. O. Dola, T. Korõtko, K. McLaughlin, and V. Kotkas. Threat modeling of cyber-physical systems - a case study of a microgrid system. *Computers & Security*, 124:102950, 2023. doi: 10.1016/j.cose.2022.102950.

[2] Michael Howard and Steve Lipner. *Threat Tree Patterns*. Microsoft Press, Redmond, WA, 2006.

[3] S. H. Weingart. Physical security devices for computer subsystems: A survey of attacks and defenses. In *Cryptographic Hardware and Embedded Systems — CHES 2000*, pages 302–317, 2000. doi: 10.1007/3-540-44499-8_24.

[4] K. A. Gromada and W. M. Stecz. Designing a reliable uav architecture operating in a real environment. *Applied Sciences*, 12(1):294, 2022. doi: 10.3390/app12010294.

[5] G. Stoneburner, C. Hayden, and A. Feringa. *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A*. 2004. doi: 10.6028/nist.sp.800-27ra.

[6] UK Government. Drones: Uk public dialogue. `https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/579550/drones-uk-public-dialogue.pdf`, 2016. Accessed: [Insert Access Date].

[7] UK Civil Aviation Authority (CAA). Protecting people's privacy. `https://register-drones.caa.co.uk/drone-code/protecting-peoples-privacy`, 2021. Accessed: [Insert Access Date].

[8] Air Accident Investigation Branch. AAIB - Annual Safety Report 2022, 2022. URL `https://assets.publishing.service.gov.uk/media/64492a1ef12683000cca68b6/AAIB_Annual_Safety_Review_2022.pdf`.

[9] UK Civil Aviation Authority (CAA). You have control - cap2507. `https://www.caa.co.uk/media/qofdwzb4/acrobrwex_you-have-control-cap2507-january-2023-pdf_adwf432-tmp.pdf`, 2023. Accessed: [Insert Access Date].

[10] Civil Aviation Authority. Drone Educational Safety Article 02: Preventing Technical Failures, 2023. URL `https://www.caa.co.uk/media/eesisp22/drone-educational-safety-article-02-preventing-technical-failures-1.pdf`.

# Appendices