A close up of a logo

Description automatically generated

**Module 04**

**IE 5329 – Project Management, Fall Semester 2024**

Dr. Jennifer Cross

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Internet of Things Drones Integration

**Team 3**

Mohammed Noor Alabbasi, Project Lead

Arsalan Habib

Emila Lopez

Victoria Velasquez

Arun Chandana

Dhana Gandham

Loic Wega

# Introduction and Updates:

In this module, we advance our project management skills by addressing the essentials of risk and quality management for the IoT drone integration project. Effective risk management safeguards project objectives, guiding the team in identifying, evaluating, and responding to potential risks that could affect cost, schedule, and performance. This module emphasizes a proactive approach, helping the team assess and implement handling strategies to minimize potential project disruptions.

In addition, Module 4 introduces quality management techniques, equipping the team with strategies to ensure consistent project standards and achieve high-quality outcomes. Quality management here is more than preventing defects; it also establishes clear, measurable criteria to monitor project success and improve processes.

**Key Updates from Previous Modules**

In this module, we build on prior learnings by examining risk in greater depth, with a focus on risks specific to IoT drone integration, such as cybersecurity vulnerabilities, data privacy, regulatory compliance, and operational reliability. We introduce tailored handling strategies like risk avoidance, mitigation, transfer, and acceptance, providing a comprehensive framework for addressing each key risk.

To support consistent quality, the module also introduces advanced quality management tools like Failure Mode and Effect Analysis (FMEA) and Six Sigma, essential for proactively identifying potential points of failure and ensuring continuous improvement. These techniques are complemented by quality metrics that allow the team to gauge project success in real time, ultimately ensuring that both risk and quality management efforts lead to the project’s goals.

# Identification of Key Project Risks

Identifying key risks in our IoT drone project is crucial to ensure the project’s success and address challenges proactively. On the surface “Key concerns include limited battery life, explosion risks, and potential damage to assets and individuals” (Dauren Askerbekov et al.,2024) but that only scratches the surface so in this portion, we will identify the risks in detail.

The risks are as follows in no specific order:

1. **Security Risks:** From data breaches to hacking to weak encryption, if communication between the drone and control systems is not properly encrypted, it could be intercepted. It can also lead to loss of control or manipulation of the drone’s activities or unauthorized access to sensitive data collected by the drones, such as videos, images, or sensor data.
2. **Privacy Concerns**: Drones may collect data unintentionally from individuals or places without the proper permissions, raising ethical and legal concerns. Surveillance issues arise from continuous monitoring or surveillance and could violate personal or corporate privacy laws, especially in areas with strict data protection regulations.   
     
    Privacy can be resolved when the drone is programmed for a specific use case for example the use of multi-spectral cameras “primarily for agricultural use cases to help anticipate the health of vegetation. In the solar industry, this can be used to determine the health of turfgrass and surrounding vegetation” (Drone, 2023).
3. **Regulatory and Compliance Risks**: Compliance with Aviation Laws and Restricted Areas go hand in hand as there are regulations for drones not allowed within protected airspace such as military bases, airports, or government facilities. Failure to adhere can and will lead to legal consequences or penalties.
4. **Operational and Performance Risks**: Communications failures are most definitely a high risk because IoT drones rely heavily on stable communication networks) Wi-Fi, LTE, 5G), and disruptions could result in loss of control or loss of data.    
      
   Battery and power issues are also an issue because they have a limited life, and it can lead to incomplete flight missions, crashes, or loss of data if the drone were to run out of power mid-flight. Sensor malfunctions due to faulty sensors could lead to inaccurate data collection or impaired decision-making by autonomous drones.    
      
   A performance risk that is outside of our control would have to be environmental factors from the weather (e.g., high winds, rain, extreme temperatures) could affect drone performance and lead to crashes or damage.
5. **Cybersecurity Threats**: IoT vulnerabilities are no surprise since drones have internet connectivity that can be vulnerable to malware, denial-of-service attacks, or exploitation of IoT protocol weaknesses. Firmware exploits or insecure/outdated firmware in the drone’s hardware can be targeted by attackers.
6. **Technological Risks**: Software bugs and glitches come as no surprise in the software controlling the drone’s navigation, data collection, or processing could lead to malfunction or crashes.    
      
   Integration challenges may arise such as compatibility when drones need to integrate with IoT platforms, cloud services, and analytics systems. Latency in real-time communication from delays in transmitting data to the control system or cloud serves can affect real-time decision-making, especially in time-sensitive applications.
7. **Supply Chain and Vendor Risks**: Component shortages on a global scale in key components such as semiconductors or sensors could delay production and deployment. Vendor reliability namely relying on third-party hardware, software, or service providers introduces risks if they fail to meet expectations or go out of business.
8. **Financial Risks**: Cost overruns from unexpected costs in development, deployment, or maintenance can strain the project budget. Return on investment (ROI) uncertainty if the drones don’t perform as expected or cannot scale, the expected benefits may not justify the costs.
9. **Project Management Risks**: Scope creep may take hold as stakeholders might request additional features or functionalities, the project could expand beyond the original scope, leading to delays and cost overruns.  Team skill gaps due to a lack of expertise in IoT systems, drone technology or cybersecurity could slow down progress or lead to flawed implementations. Time delays from failure to meet project deadlines due to development issues, testing challenges, or regulatory approvals can derail the project.
10. **Licensing Risks:** It can be a significant risk in an IoT drone project, especially because a project of this magnitude often involves both hardware and software that may have specific licensing requirements or restrictions.
11. **Brand Reputation**: The product involves public-facing technology and potentially sensitive use cases. Brand reputation risks can affect user trust, market adoption, and overall project success.
12. **Collision Risk**s: This is another significant risk particularly because drones operate in physical spaces where they can interact with objects, drones, people, and infrastructure. This is a risk that is crucial to manage for both safety and operational efficiency.
13. **Latency in data processing**: Latency in data processing refers to the delay between the moment data is generated or received and the moment it is processed or made available for use. In the context of IoT-enabled drones, latency can significantly impact performance and decision-making
14. **Limited Communication Range:** Limited range is the restricted ability of drones to maintain effective connectivity with their control systems or networks or operator. This can significantly impact the drone's operation, data transmission, overall performance and the sales of the product (the longer the range higher the expected sales)

In the next section, our team will analyze each of the risks in greater detail to get to the root of the problem and discuss the potential impact and financial impact the risks will have on our project.

Analysis of Key Project Risks

This risk matrix is drawn from DJI companies past failures, highlights critical risks that the company faces along with their likelihood and potential impact as an example in some cases. By assessing these risks from DJI, we can develop targeted strategies to mitigate them, ensuring better operational stability and customer confidence.

  The risk matrix was drawn using FMEA process

The risks are categorized based on the historical failures of similar drone companies, alongside a sensitivity analysis of the project and team input. This structured approach ensures a comprehensive understanding of potential vulnerabilities and informs effective risk management strategies tailored to the specific challenges faced in the drone industry.

### **Likelihood Levels**

1=Very Unlikely (1-10%)

2=Unlikely (10-30%)

3=Possible (30-50%)

4=Likely (50-70%)

5=Very Likely (70-100%)

**Impact(I)**:

1= Negligible (0-10%)

2=Minor (20-30%)

3=Moderate (30-50%)

4=Noticeable (50-60%)

5=Significant (60-80%)

6=Major (80-90%)

7=severe (60-80%)

8=critical (70-80%)

9=catastrophic (80-90%)

10=disastrous (>90%)

Where I considered

Insignificant risk (1)

Low risk (2-3)

Moderate risk (4-6)

High risk (7-9)

Critical (>9)

**Detection(D)**:

1= very likely (>90%)

2=likely (60-80%)

3=Possible (30-50%)

4=unlikely (10-30%)

5=Very unlikely (<10%)

**Risk priority number (R)= L\*I\*D**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk Type** | **Cause** | **Likelihood**  **(L)** | **Effect** | **Impact**  **(I)** | **Detection**  **(D)** | **RPNnumber**  **(R)** |
| Technological Risks | Coding errors | 4 | System malfunction | 8 | 3 | 96 |
| Cybersecurity Threats | Weak encryption, poor access control | 5 | Unauthorized access, data loss | 9 | 2 | 90 |
| Security Risk | Weak encryption | 4 | Data tampering | 8 | 3 | 72 |
| Regulatory and Compliance Risks | Change in govt laws | 3 | Legal issues | 8 | 3 | 72 |
| Economic Instability | economic downturns | 3 | Decrease in revenue | 8 | 3 | 72 |
| Supply Chain and Vendor Risks | Supplier issues, lack of alternatives | 4 | Project delays, increase in costs | 7 | 2 | 56 |
| Latency in data processing | Slow processing speeds | 3 | Delayed data processing | 6 | 2 | 36 |
| Performance Risks | Poor sensor quality, connectivity issues with 5G | 2 | Low performance | 5 | 3 | 30 |
| Licensing  Issues | Non-compliance with licensing agreements | 2 | Legal issues | 6 | 2 | 24 |
| Collision Risks | Malfunction in LiDAR sensor | 2 | Drone damage | 4 | 2 | 16 |
| Quality assurance failures | Inadequate quality control processes | 2 | Product defects | 4 | 2 | 16 |
| Brand Reputation Risks | Negative media coverage, public perception | 2 |  | 5 | 2 | 20 |
| Financial risks | lack of funding | 1 |  | 5 | 4 | 20 |

|  |
| --- |
|  |
|  |

This section presents a concise overview of the identified risks, highlighting parallels with similar products and their observed challenges. Additionally, it outlines potential solutions informed by the experiences of other industry players, offering critical insights for effective risk management and informed decision-making**.**

**Security risk: (critical risk factor)**

 This can have significant implications for both the operational integrity of the drone and the security of the data it collects including personal data tampering. In October 2022 DJI faced serious security issues around 80000 drone data was leaked in the dark wed. then DJI started to store the data of the us citizens within USA by set data base in USA without transmitting back to China and the started to have an **Encryption and Security Protocols.**

<https://dronelife.com/2024/01/25/djis-thorough-rebuttal-safeguarding-data-privacy-and-cybersecurity-amid-national-security-concerns-over-chinese-drones/>

**supply chain and vendor risks: (medium risk factor)**

The global shortage of semiconductors has significantly affected various industries including the drone manufacturing industries. These shortages can delay production timelines and lead to increased costs, as companies scramble to secure necessary components**.  We are planning to diversify the supplier base and maintain inventory buffers to ensure production continuity based on the sales**

**Technological Risks: (medium risk factor)**

Software controlling a drone’s navigation, data collection, or processing can have bugs or glitches. These issues can lead to malfunctions, crashes, or unintended behavior during flights. In 2020, a drone delivery service faced significant challenges when trying to integrate its fleet with a new cloud-based logistics platform, this incompatibility between the drone software and the platform led to delays in the deliveries and operational malfunctions. We can overcome this issue    **frequently   giving the updates to the drone.**

 Bugs in the software: Software controlling a drone’s navigation, data collection, or processing can have bugs or glitches. These issues can lead to malfunctions, crashes, or unintended behavior during flight. In 2019, a DJI drone experienced a software glitch that caused it to crash during a routine flight. The drone lost connection with its controller and failed to execute a return-to-home command, resulting in a crash. Which are used as terror attacks, ex: **White House Crash (2015)**

[A Drone, Too Small for Radar to Detect, Rattles the White House - The New York Times](https://www.nytimes.com/2015/01/27/us/white-house-drone.html)

**Regulatory and Compliance Risks: (high risk factor)**

Drones operate in a complex regulatory environment, particularly concerning aviation laws and restricted air spaces. Managing these regulations is crucial to ensure safety and avoid legal problems.  Many regions have no-fly zones to protect sensitive areas. Drones entering these zones can pose security risks and disrupt operations. In 2019, a drone operator in the U.S. was fined $20,000 for flying a drone near an airport without authorization. The drone interfered with air traffic, prompting an investigation by the Federal Aviation Administration (FAA).  **To avoid these   by educating and giving training to the user to avoid these issues and having geo fencing integrated in the drones.**

[Drone pilot fined $20,000 after DJI Phantom 3 lands at McCarran Airport](https://dronedj.com/2019/11/24/drone-pilot-fined-20000-mccarran-airport-las-vegas/)

**Cybersecurity Threats: (high risk factor)**

Drones often rely on IoT connectivity, making them susceptible to various cyber threats. Attackers can exploit weaknesses in IoT protocols or use malware to gain unauthorized access to drone systems. In a notable incident with DJI, a financial firm experienced a cyberattack involving drones that breached their corporate network. Attackers used modified drones equipped with devices that spoofed the firm’s Wi-Fi network. **This issue can be solved by usage of encrypted communication channels (e.g., TLS/SSL) to protect data transmitted between the drone and its control systems**. This helps prevent interception of sensitive information and multifactor authentication in every stage of accessing the data

[The Drone Cyberattack That Breached a Corporate Network](https://blogs.blackberry.com/en/2022/10/the-drone-cyberattack-that-breached-a-corporate-network)

**Financial Risks**: **(low risk factor)**

Unexpected costs during the development and maintenance phases can lead to an increase in the project budget, potentially resulting in financial challenges. However, **given our project's initial budget**, we can accommodate a slight increase in our budget.

**Licensing issues:(moderate risk factor)**

Licensing for drones is crucial for the company’s operations. To obtain these licenses from the government, it is essential to maintain accurate documentation in accordance with regulatory requirements. Additionally, the company must ensure that all software is consistently updated and upgraded to meet government standards. This involves regular audits and compliance checks to adhere to the evolving regulations governing drone usage. By prioritizing these practices, the company can facilitate a smoother licensing process and mitigate the risk of penalties or operational disruptions due to non-compliance, ultimately supporting its long-term success in the industry.

**Performance Risks:(moderate risk factor)**

Even after a lot of quality and production trails we can face a small number of drones causing performance risks after reaching the consumers which can solved by **giving better customer assistance** for the customers.

**Quality Assurance Failures :(high risk factor)**

Quality assurance is essential, as issues identified post-deployment can negatively impact the company's brand value. If defects or shortcomings are discovered after the product is released, they can lead to customer dissatisfaction and tarnish the company's image. To address this concern effectively, it is advisable to **establish an independent quality assurance team dedicated to overseeing the product's quality throughout its lifecycle**. This team will conduct thorough assessments and ensure that standards are consistently met, helping to prevent potential problems and maintain the company’s reputation for delivering reliable and high-quality products to its customers.

**Collision risks:(low risk factor)**

These types of risk occur rarely in the running stage as different trail tests are done before the deployment of the drone. This occurs due to the malfunction in the LiDAR sensors. This can be solved by **replacing the sensor in the failed unit.**

**Brand Reputation Risks:(moderate risk)**

Implementing proactive PR strategies is essential for managing brand reputation risks, especially in the drone industry, where public perception can be significantly impacted by failures. In the past, GoPro faced a major setback with the recall of its Karma drones due to power loss issues. The company’s delayed response and lack of clear communication worsened the situation, degrading the brand value.

[GoPro Announces Karma Recall and Refund Program | GoPro Inc.](https://investor.gopro.com/press-releases/press-release-details/2016/GoPro-Announces-Karma-Recall-and-Refund-Program/default.aspx)

**Economic Instability:(high risk factor)**

Given our reliance on drones for project income, it's crucial to diversify our operations across different countries and in different sectors. This approach will enhance economic stability and mitigate risks associated with dependence on a single market or region. Parrot, a French drone manufacturer, initially focused on consumer drones but faced declining sales due to intense competition. The company’s lack of diversification into more profitable sectors like commercial and industrial drones led to financial difficulties

[Historical-Performance-of-the-UAS-Industry-Final.pdf](https://droneanalyst.com/wp-content/uploads/2020/08/Historical-Performance-of-the-UAS-Industry-Final.pdf)

# Handling strategies for risks

|  |  |  |
| --- | --- | --- |
| **Type of Risks** | **Risk Description** | **Handling Strategy** |
| Security | Unauthorized access, data breaches, and interception of communications between drones and control systems. |  |
| Privacy Concerns | |  | | --- | |  |  |  | | --- | | Unintentional data capture and potential surveillance issues, leading to legal and ethical challenges | |  |
| Regulatory and compliance | Compliance risks with airspace restrictions and data protection laws, especially in high-regulation areas. |  |
| Operational and performance | Risks in network connectivity, power management, and performance impacts from environmental factors. |  |
| Cyber security Threats | Vulnerabilities in IoT connections that could lead to malware, service attacks, or firmware exploits. |  |
| Technological | Software bugs, compatibility issues with IoT platforms, and latency that affects real-time decision-making. |  |
| Supply chain and Vendor | Component shortages and dependence on third-party vendors, potentially delaying production and deployment. |  |
| Financial | Cost overruns and uncertainty in ROI if performance doesn’t meet expectations or if scaling is challenging. |  |
| Project Management | Scope creep, skill gaps, and delays due to regulatory approvals or team capability limitations. |  |
|  |  |  |
|  |  |  |
|  |  |  |

* **Assumption (retention)**
* **Avoidance**
* **Control (mitigation)**
* **Transfer**

# Quality Management Strategies

For our IoT Drones product, the best quality management strategies we’ve chosen to implement are Failure Mode and Effect Analysis (FMEA), Six Sigma, Continuous Improvement (Kaizen), and Quality Control (QC) and Quality Assurance (QA).

The FMEA was a strategy best suited for our IoT Drones due to the complex components and critical safety implications. This is done by systematically identifying potential failure points in the drone’s components. These components can include failure points in the sensors, data transmission modules, and power sources. This strategy would help the team to assess what would be the direct impact of each potential failure and prioritize preventative measures.

This is a strategy recognized as best practice in aerospace and electronic industries

The Six Sigma strategy is also well suited for our project, it has a data-driven approach which is essential for maintaining the precision and consistency which would be required in the IoT data transmission and drone navigation. Having our data accurate is imperative to our drone’s real-time performance and operational accuracy.

The Continuous Improvement (Kaizen) strategy is just as it sounds in the way that it is meant to be implemented as the project is moving along. Projects that are highly involved in technology, like ours, need to stay up to date and continuously improve our processes and product. This approach, while difficult to always consider, will help to adapt to new insights or emerging technologies, ensuring our drone’s design and performance remain current and competitive.

Lastly, another strategy with great potential to assist our project is Quality Control (QC) and Quality Assurance (QA). This strategy provides various checks and verification throughout the project lifecycle. These quality checks ensure the drone’s design and functionality align with set standards. QC often requires hands on testing components and performance metrics, while QA focuses on the processes and standards that guide development. Combined, QC and QA will allow our team to catch issues early on, keep consistent quality levels, and ensure adherence to the design specifications.

# Quality related metrics