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.

The team is also adding a quality management team member to our financial estimates to account for the resources it will take to implement the above-mentioned tools. This quality manager will work cohesively with our existing teams to assure they are all aligned with our standards. We have allocated $160,000 of our budget to the quality manager, using their estimated annual salary of $100,000 for the duration of 18months it will take to complete the project.

# **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:

1. **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.
2. **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.
3. **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.
4. **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.
5. **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.
6. **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
7. **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
8. **Licensing Risks:** This possesses a substantial risk in an IoT drone project, especially considering the project's complexity, which often involves both hardware and software components that may be subject to specific licensing requirements or restrictions.
9. **Collision Risk**s: Drones operate in physical environments where they can interact with objects, other drones, people, and infrastructure, making risk management essential. Effectively managing this risk is vital for ensuring both safety and operational efficiency.
10. **Market Competition:** entry of new competitors in market, pressurizes the company's market share and makes adjustment in prices to compete with the competition. 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.
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. **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.
13. **Signal Interference:** when unwanted signals disrupt drone communication, causing control loss, data errors, and reduced range which is cause includes environmental obstructions, electromagnetic interference, frequency overlap, and adverse weather.
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)
15. **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.
16. **Human resources risk**: Human Resources Risks include skill shortages, where finding qualified personnel to operate and maintain drones can be challenging. High turnover rates can lead to a loss of expertise and disrupt project continuity. Additionally, training costsfor new employees can strain resources, and employee burnout from high workloads can reduce productivity and morale.
17. **Health and Safety Risks:** Prolonged exposure to drone communication signals could pose health risks to operators or nearby individuals. Accidents involving drones can cause physical injuries or property damage
18. **Market entry risks:** Market entry risks in the drone industry refer to the challenges faced when attempting to introduce drone products or services into new geographical or sectoral markets. These can include navigating local regulations, understanding consumer preferences, and overcoming established competition. Additionally, cultural differences and varying acceptance of drone technology can complicate successful market penetration and adoption.
19. **Data Overload**: Data overload in the drone industry occurs when the volume of information collected by drones exceeds an organization’s capacity to process and analyze its effectiveness. As a result, valuable data may become underutilized, diminishing the potential benefits of drone operations.
20. **Ethical risks:** Ethical concerns in the drone industry include privacy violations, as drones can capture data without consent, leading to surveillance issues. The use of drones by law enforcement raises questions about excessive monitoring and potential abuse of power. Additionally, there are worries about data security, informed consent, and the environmental impact on wildlife and ecosystems. Addressing these concerns is crucial for fostering public trust and ensuring responsible drone operations.
21. **Weaponization of Drones:** The recent development of drones for military purposes presents ethical challenges regarding their use in warfare, including collateral damage, civilian casualties, and the psychological impact on those involved in drone warfare.
22. **Dependency on Connectivity:** Drones heavily depend on reliable internet and GPS signals for navigation, data transmission, and control. If connectivity is lost due to factors like poor network coverage, environmental interference, or technical malfunctions it can lead to significant operational disruptions

# **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 by applying FMEAprocess, FMEA offers a systematic framework for identifying and prioritizing potential failure modes within a system, enabling early detection of issues and facilitating proactive risk mitigation. By quantifying risks based on severity, occurrence, and detection, FMEA enhances cross-functional communication and informed decision-making. Additionally, it promotes continuous improvement and efficient resource allocation, ultimately contributing to increased product reliability and quality. This structured approach fosters a culture of risk awareness, optimizing overall project outcomes and compliance with industry standards.

### **Likelihood Levels**

### 1 = Very Unlikely (1-10%)

3 = Possible (30-50%)

5 = Very Likely (70-100%)

**Impact(I)**:

2 = Minor (20-30%)

5 = Significant (60-80%)

7 = severe (60-80%)

10 = disastrous (>90%)

**Detection(D)**:

1= very likely (>90%)

3=Possible (30-50%)

5=Very unlikely (<10%)

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk Type** | **Cause** | **Likelihood**  **(L)** | **Effect** | **Impact**  **(I)** | **Detection**  **(D)** | **RPN number (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 | 7 | 3 | 84 |
| Regulatory and Compliance Risks | Change in govt laws | 3 | Legal issues | 8 | 3 | 72 |
| Supply Chain and Vendor Risks | Supplier issues, lack of alternatives | 3 | Project delays, increase in costs | 7 | 3 | 63 |
| Privacy concerns | data collection, continuous monitoring | 4 | Ethical and legal concerns, violation of privacy laws | 6 | 2 | 48 |
| Latency in data processing | Slow processing speeds | 4 | Delayed data processing | 6 | 2 | 48 |
| Performance Risks | Poor sensor quality, connectivity issues with 5G | 2 | Low performance | 5 | 4 | 40 |
| Limited Communication Range | Hardware Limitations | 3 | Lower distance range which directly impact the sales | 6 | 2 | 36 |
| Licensing  Issues | Non-compliance with licensing agreements | 2 | Legal issues | 6 | 3 | 36 |
| Collision Risks | Malfunction in LiDAR sensor | 2 | Drone damage | 4 | 4 | 32 |
| Quality assurance failures | Inadequate quality control processes | 2 | Product defects | 4 | 3 | 30 |
| Market competition | Increase in number of competitors | 3 | Loss of market share | 5 | 2 | 30 |
| Brand Reputation Risks | Negative media coverage, public perception | 2 | Loss of trust with consumer | 5 | 2 | 20 |
| Financial risks | lack of funding | 1 | Project failure | 5 | 4 | 20 |

In deriving the table, we considered the impact by evaluating the potential consequences of each risk on the project. For detection, we rated how easily each risk could be identified and mitigated and for likelihood, we considered several factors. we reviewed historical data from similar projects to see how often each risk had occurred. We also consulted with team members to gather their insights and experiences in handling drones.

***Conclusion from the risk matrix***

Technological risk, cybersecurity risk, security risk. These risks have the highest RPNs, indicating they have a significant impact, high likelihood, and are challenging to detect. Addressing these should be a priority to mitigate potential issues effectively and increase the efficiency of the drone.

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**.**

# **Handling strategies for risks**

|  |  |  |
| --- | --- | --- |
| **Risk Type** | **Risk Description** | **Handling Strategy** |
| **Security Risks** | Unauthorized access, data breaches, and interception of communications between drones and control systems. | Implement end to end encryption, Real time threat detection, and Regular security audits |
| **Privacy concerns** | |  | | --- | |  |  |  | | --- | | Unintentional data capture and potential surveillance issues, leading to legal and ethical challenges | | Limit data collection to project needs, privacy alerts based on GPS, and clear privacy policies |
| **Regulatory and compliance** | Compliance risks with airspace restrictions and data protection laws, especially in high-regulation areas. | Geo-fencing to avoid restricted areas and build relationships with aviation authorities. |
| **Operational and performance** | Risks in network connectivity, power management, and performance impacts from environmental factors. | Backup power systems and proposed regular maintenance for sensors. |
| **Cybersecurity** | Vulnerabilities in IoT connections that could lead to malware, service attacks, or firmware exploits. | Multi layers security measures, develop response plan for malicious attacks, routine vulnerability tests |
| **Technological** | Software bugs, compatibility issues with IoT platforms, and latency that affects real-time decision-making. | Rigorous testing |
| **Supply chain and vendor** | Component shortages and dependence on third-party vendors, potentially delaying production and deployment. | Diversify suppliers to reduce dependency, vet vendors thoroughly |
| **Financial** | Cost overruns and uncertainty in ROI if performance doesn’t meet expectations or if scaling is challenging. | Develop detailed budget and contingency plan, prioritize ROI based features |
| **Project Management** | Scope creep, skill gaps, and delays due to regulatory approvals or team capability limitations. | Develop clear project scope and agile methods, identify skill gaps and hire contractors/consultants |
| **Licensing** | Challenges in obtaining the necessary licensing for drone operations | Research licensing requirements early in the project, regularly monitor licensing update to ensure compliance |
| **Collision** | Risk of drones colliding into building or other personal property resulting in damage or injury | Implement collision avoidance sensors and real time alerts for drone operators |
| **Brand Reputation** | Negative public backlash from issues such as data breaches/ accidents | Ensure transparency with stakeholders and maintain high standards in security and compliance |
| **Latency in Data processing** | Delays in data processing, impacting real time data control | Utilize the edge of the 5g network to reduce latency |
| **Limited communication range** | Restricted range of communication, limiting operational distance from control centers, 5g access points | Utilize signal boosters on board to activate on demand only when needed to reduce power consumption |
| **Signal interference** | Interference from environmental factors that may disrupt communication and control of drones | Develop protocols for safe recovery in case of signal loss |

Here we will discuss how we determined development strategies for each of these risks. We used a few different types of methods which would help with avoidance, mitigation, and to the best of our ability transfer the risk to the consumer. While we completed a bit of research behind our handling strategies and looked at similar scenarios, we also used the basic risk mitigation skills developed with the experienced people on our team. One key takeaway from risk mitigation is that everyone will see each risk differently and may categorize or rank them differently. It is important to note that every person is unique and has different priorities, as a project manager it is important to consider everyone’s viewpoints, however it is crucial to keep the end goal in mind.

Here are some of our risks and the handling strategies associated with real life examples to help support our decision making:

***Security risk***

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 80,000 drones’ 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 then started to have Encryption and Security Protocols (McNabb Miriam, 2024). To avoid this type of situation this is something we plan to include with the launch of our product.

***Supply chain and vendor risks***

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. This helps ensure we do not create too much dependency on one vendor.

***Technological Risks***

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 by frequently giving software 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. ex: White House Crash (Schmidt, M. S 2015.)

***Regulatory and Compliance Risks***

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 (Kesteloo, H 2019). The drone interfered with air traffic, prompting an investigation by the Federal Aviation Administration (FAA). Our solution is to avoid these by educating and giving training to the user to avoid these issues and having geo fencing integrated in the drones**.**

***Cybersecurity Threats***

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 (Sussman, B. 2022). 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) using multiple layers and conducting routine vulnerability tests. This helps prevent interception of sensitive information and multifactor authentication in every stage of accessing the data

***Licensing issues***

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***

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 continuous customer assistancefor the customers.

***Quality Assurance Failures***

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.

***Economic Instability***

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. We also considered unexpected costs during the development and maintenance phases which can lead to an increase in the project budget, potentially resulting in financial challenges. However, given our project's initial budget and the 10% cushion, we can accommodate a slight increase in our budget however, a complete depression would ultimately result in the going over the budget

# 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).

***FMEA***

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 electronics industries since these require high levels of safety, precision, and risk mitigation (Kerzner, 2022, pp. 874-875). Since our drones are expected to sometimes overlap areas with airspace restrictions, this strategy will effectively protect our stakeholder’s interests in which they expect a robust, fault-tolerant drone.

***Six Sigma***

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.

This strategy, like the previous one, is also an established standard in industries where precision and low defect rates are critical. These industries include aerospace, electronics, and telecommunications (Kerzner, 2022, pp. 987-989). Our IoT Drones' capabilities fall under all these industries, so this is a great strategy to assure high levels of accuracy and efficiency from our drone.

***Continuous improvement***

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.

This is another strategy that is widely adopted in technology and manufacturing industries, which require fast-paced technological advancements that stakeholders expect out of our product (Kerzner, 2022, pp. 832-833).

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 Management Plan***

1. **Objectives**

* To ensure the IoT Drone meets high standards of reliability, accuracy, and performance.
* To proactively identify and mitigate potential points of failure.
* To maintain continuous improvements that assure the drone and its capabilities are up to date with the latest industry advancements.
* To achieve high precision and minimal defect rates in data handling and operational functionality.

1. **Scope**

* This plan covers all stages of the IoT Drone project, including design, development, testing, production, and post-launch maintenance.
* This plan applies to both hardware (components, sensors, and connectivity) and software (data processing, communication protocols, and control systems) components of the drone.

1. **Quality Standards**

* Reliability: The drone must maintain consistent connectivity, perform accurate sensor readings, and operate consistently under diverse environmental conditions.
* Data Accuracy: Data transmission and sensor readings should meet industry standards with minimal errors.
* Safety and Compliance: All drone components and software must meet industry standards for IoT devices.
* Continuous Improvement: Regular performance reviews and iterative adjustments should be implemented to enhance performance over time.

1. **Quality Management Strategies**

* Failure Mode and Efffect Analysis (FMEA)
  + Objective: Identify and address potential failure points in hardware and software.
  + Implementation steps: perform FMEA in the design phase, then rank each identified risk, and develop mitigation plans for high-priority risks.
  + Monitoring: FMEA results should be reviewed periodically, usually before testing phases to adjust the mitigation measures as needed.
* Six Sigma
  + Objective: To ensure high data accuracy, minimal defect rates, and operational consistency in hardware and software.
  + Implementation steps: Use this methodology to analyze data collection and processing, conduct testing to optimize hardware and software configurations, set defect rate targets and implement improvements based on data analysis.
  + Monitoring: Regular reviews should be scheduled, especially during testing and production stages to ensure alignment with the quality goals.
* Continuous Improvement (Kaizen)
  + Objective: To keep our product’s technology and capabilities up to date to ensure it remains competitive in the market by adapting to technical advancements.
  + Implementation steps: Implement regular review cycles in which the team identifies areas of improvement, establish feedback loops with stakeholders and field testers, and allocate time in each phase for assessing and implementing small improvements.
  + Monitoring: Continuous improvement reviews should be conducted quarterly by the team.
* Quality Control (QC) and Quality Assurance (QA)
  + Objective: Ensure that all components and software meet quality functions.
  + Implementation steps: Apply rigorous testing of hardware and software components to ensure compliance with quality standards, establish protocols for standardized procedures for testing and production, and conduct pre-launch audits on hardware and software to ensure compliance and quality standards are met.
  + Monitoring: QA procedures will be revisited at major milestones, while QC checks should be ongoing throughout the development and production phase.

1. **Roles and Responsibilities**

* Quality manager: Oversees all quality management activities and ensures adherence to this quality management plan.

1. **Documentation and Reporting**

* FMEA Reports: Generated at the end of each FMEA session, documenting risks and mitigation measures taken.
* Six Sigma Data Reports: Regular reports detailing the outcomes of the Six Sigma analyses and improvements.
* Continuous Improvement Log: Logs of suggestions, feedback, and changes made.
* QC/QA Checklists: Checklists documenting compliance with quality standards for each component, updated at each project stage.

1. **Review and Revision**

* Our team’s plan will be reviewed at the end of each major project phase to ensure that our project remains aligned with our set goals and any changes in industry standards or stakeholder expectations.

***Quality Policy***

1. **Policy Statement**

* The IoT Drone project is committed to delivering a high-quality, reliable, and innovative product that meets industry standards, and exceeds stakeholder expectations. We are dedicated to maintaining rigorous quality management throughout the entire project lifecycle, from design and development to testing and production.

1. **Core Principles**

* Reliability and Safety: Our primary goal is to produce a drone that operates safely and reliably under various conditions while meeting the highest standards for IoT and drone aviation technology.
* Accuracy and Consistency: We prioritize data accuracy and operational consistency by leveraging Six Sigma methodologies, minimizing variability, and ensuring that each component performs as intended.
* Continuous Improvement: With the Kaizen philosophy, we embrace continuous improvement by implementing incremental changes and advancements that keep the drone competitive and relevant.
* Proactive Risk Management: With FMEA, we proactively identify, assess, and mitigate potential risks.
* Quality Assurant and Control: We are committed to rigorous QC and QA practices to ensure each phase of development meets our defined quality benchmarks and complies with industry standards.

***Commitment to Quality***

The IoT Drone Project team is dedicated to:

* Implementing robust quality management processes to produce a safe, reliable, and high-performing product.
* Meeting or exceeding industry standards by adhering to proven quality methods, such as FMEA, Six Sigma, Continuous Improvement, and QC/QA.
* Continuously improving the project’s quality through regular reviews, feedback, and iterative enhancements based on technological advancements and stakeholder input.

***Responsibility and Accountability***

All team members are responsible for upholding this Quality Policy in their roles and are encouraged to actively participate in quality improvement initiatives. The Quality Manager oversees the policy’s implementation and ensures all quality practices align with the project’s goals and industry standards.

***Quality Plan Related Matrix***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Quality Objective** | **Quality Activity** | **Metric/Standard** | **Responsible Team Member** | **Frequency** |
| Reliability | Conduct Failure Mode and Effect Analysis (FMEA) | Identified and mitigated high-priority risks | FMEA Coordinator (Quality Manager) | Design Phase, Reviews |
|  | Integrate controlled and redundant systems for critical components | Redundancy in key components | Engineering Team | Ongoing |
| Data Accuracy and Consistency | Apply Six Sigma to reduce process variability | Defect rate below 0.1% | Six Sigma Specialist (Quality Manager) | Testing, Production |
|  | Implement feedback from stakeholders | ≥ 95% accuracy in sensor readings | Quality Control QC Inspector (Quality Manager) | Bi-weekly |
| Continuous Improvement | Conduct Kaizen sessions for ongoing enhancements | Number of improvements implemented per quarter | Continuous Improvement Leader (Quality Manager) | Quarterly |
|  | Implement stakeholder feedback | ≥80% positive feedback on improvements | Continuous Improvement Leader (Quality Manager) | Post-feedback |
| Proactive Risk Management | Perform FMEA at design phase and update before beginning testing phase | Complete risk assessment for each phase | Quality Manager | Design, before testing |
|  | Document and review risks and mitigation steps | 100% documentation of identified risks and mitigation actions | Quality Manager | Quarterly |
| Quality Assurance (QA) | Develop standardized QA protocols for calibration | Compliance with QA protocols (100%) | QA Inspector (Quality Manager) | Before production |
| Quality Control (QC) | Inspect components and subsystems to verify compliance | 95% or higher compliance with quality standards | QC Inspectors (Quality Manager) | Each production batch |
| Stakeholder Satisfaction | Gather and analyze feedback from users | Stakeholder satisfaction ≥90% | Quality Manager | Post-release review |
| Compliance with Industry Standards | Ensure all hardware and software meet IoT and safety regulations | Full compliance with regulatory standards | Quality Manager and Engineering Team | Pre-release |

# Quality related metrics

To ensure our IoT Drone project meets quality standards and stakeholder expectations, we have identified measurable quality metrics and their corresponding methods for continuous monitoring and improvement. The quality and success of our IoT Drone project will be assessed based on: battery performance and longevity, security compliance/data accuracy, and user satisfaction. Each metric is defined with specific targets that, when achieved, indicate project success and alignment with stakeholder expectations.

***Battery Performance and Longevity***

Battery life – measured as the average operational time per change cycle, travel distance, and yearly degradation rate – is a foundational metric to ensure our drone operates efficiently during demanding conditions. High battery performance minimizes maintenance costs and the need for frequent recharging or replacement.

* Quality Target: Achieve an average flight time of 45 minutes to an hour per charge, with no more than a 10% annual degradation in capacity.
* Monitoring: Integrated sensors will provide real-time data on battery levels and performance indicators, transmitted to a centralized dashboard for continuous observation.
* Reporting: Weekly summaries will track trends in battery life and degradation, with automated alerts if performance drops below target thresholds.

“High-end and professional drones can fly for 45 minutes to an hour. Industrial drones, using advanced battery technologies and optimized designs, can exceed 2 hours of flight time” Gibson, E. (Powering Autos, 2024). The average drone battery life is influenced by several factors, primarily including battery capacity, drone weight, altitude, weather conditions, and flight mode.

***Security Compliance/Data Accuracy***

Given the sensitive data handled by our IoT system, security compliance is crucial. This metric focuses on the frequency of security incidents or vulnerabilities detected in our software, aiming for a “zero incidents” target, which reflects compliance with security protocols and encryption standards. Achieving this benchmark reduces risk to user data and risks to operational integrity.

* Quality Target: Maintain zero incidents of security breaches or vulnerabilities.
* Monitoring: Real time threat-detection software and periodic security assessments will monitor system vulnerabilities, with immediate alerts if security thresholds are breached.
* Reporting: Daily security status reports will summarize threat detection activities, with comprehensive weekly and monthly security audits to ensure compliance.

***User Satisfaction Rating***

User satisfaction, measured by customer feedback on cost, technology capabilities, data quality, ease of use, and reliability, is integral to market success. A high user satisfaction rate reflects our alignment with customer expectations and fosters further market adoption.

* Quality Target: Maintain a user satisfaction rate of 85% or higher.
* Monitoring: User feedback will be collected post-deployment via surveys and analyzed for insights into performance.
* Reporting: Monthly reports will aggregate satisfaction data, identify improvement areas, and highlight achievements in alignment with the satisfaction target.

***Quality Related Metrics Conclusion***

To ensure our IoT Drone project meets high-quality standards, we’ve defined and structured our key performance metrics: Battery Performance, Security Compliance/Data Accuracy, and User Satisfaction. Each metric has specific, measurable targets that indicate project success and guide continuous improvement.

Real-time monitoring and bi-weekly audits will proactively track these metrics, while weekly reports highlight performance trends. Monthly quality reviews and end of phase audits with stakeholders provide an opportunity to address any persisting issues and align on progress.

This approach to monitoring, reporting, and regular review reinforces our commitment to quality, supports operational efficiency, and positions our drone for successful market adoption.

**Conclusion and Next Steps**

In conclusion, this module provided a comprehensive approach to managing risk and ensuring quality in our IOT drone project. By focusing on the key risks like cyber security and technological reliability we applied methodologies such as FMEA, Sic Sigma and other continuous improvement practices to further mitigate any risks. This module has allowed our team, systematically through risk and quality management on the IoT drone integration project, to strongly put into practice proactive identification and handling of risks with the implementation of high-standard quality management. We have done thorough analyses of technological, cybersecurity, and regulatory and supply chain risks, so we can now be well-placed to safeguard our project against disruptions that may come unexpectedly to meet project goals and stakeholder expectations.

Next, we will focus on the upcoming module, diving into the details of Human Resource Management. We will determine which type of organizational structure is best, develop a staffing plan for filling each key position, and determine the minimum expectations and salary ranges for the positions.

# Citations

Kerzner, H. (2002). *Project management: A systems approach to planning, scheduling, and controlling* (13th ed.). John Wiley & Sons.

McNabb Miriam McNabb is the Editor-in-Chief of DRONELIFE and CEO of JobForDrones. (2024, February 1). *DJI’s rebuttal: Safeguarding Data Privacy and Cybersecurity*. DRONELIFE. <https://dronelife.com/2024/01/25/djis-thorough-rebuttal-safeguarding-data-privacy-and-cybersecurity-amid-national-security-concerns-over-chinese-drones/>

Schmidt, M. S., & Michael. (2015, January 26). *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

Kesteloo, H. (2019, November 24). *Drone pilot fined $20,000 after fly-away DJI Phantom 3 lands at McCarran Airport in Las Vegas*. DroneDJ. https://dronedj.com/2019/11/24/drone-pilot-fined-20000-mccarran-airport-las-vegas/

Sussman, B. (2022, October). The drone cyberattack that breached a corporate network. https://blogs.blackberry.com/en/2022/10/the-drone-cyberattack-that-breached-a-corporate-network

Gibson, E. (2024, October 29). *How Long Does the Average Drone Battery Last? Tips for Extending Battery Life*. PoweringAutos. <https://poweringautos.com/how-long-does-the-average-drone-battery-last/>

Füellenbach, G. (2023, July 5). The Impact of Customer Experience on Drone Business Growth. DRONEPROS. <https://www.dronepros.co/post/the-impact-of-customer-experience-on-drone-business-growth>