White paper:
Integrated counter-UAV solution for airports

Can you ensure efficient management of drone incursions across all stakeholders?

Many drones fulfil a useful purpose, but unregistered and non-cooperative drones can cause security concerns and even major damage. As UAV traffic increases, airports, law enforcement and air navigation service providers (ANSPs) face new challenges in both safety and security.

To protect passengers and cargo from harm and disruption, to ensure integrity of airport operations, and to sustain undisrupted air traffic, **all stakeholders must find ways to safely integrate the handling of non-cooperative unmanned traffic into their operations**, while maintaining high efficiency.

To achieve this goal, stakeholders must first step back and consider the bigger picture. Rather than deploying piecemeal technology solutions, the best-practice approach is to pinpoint the specific operational requirements, model the necessary flow of information and communication across all stakeholders, and finally implement the appropriate working practices and technologies to support that flow of information.

The model should cover the full scope of activities from the detection of Unmanned Aerial Vehicles (UAVs) through to post-incident documentation and investigation. It should take into account at every stage the required coordination between different organisations.

Critically, it is the information flow that should determine technology decisions, rather than the other way around.

A big-picture view enables efficient cross-agency management, reduced response times and exceptional safety levels. Looking to the future, this will also lay the groundwork for advanced incident management, helping to ensure that all stakeholders are prepared for challenges and opportunities to come.

FREQUENTIS

Welcome new airspace users—not all of them friendly

The global UAV market is growing even faster than expected, with industries developing solutions ranging from drone taxis to international parcel delivery. As the number and variety of drones increase, so does the pressure on airports to adopt new working practices to ensure that general aviation and unmanned air traffic can share airspace safely.

Not all drones operate in accordance with the agreed rules, whether due to technical failure, though negligence or ignorance, or even intentionally. Permitting the uncontrolled flying of drones is naturally not an option, as shown by recent high-profile and high-cost cases of disruption. If improperly managed, unmanned traffic could cause security incidents and ultimately even harm to property, aircraft or people. Due to their size, speed and agility, drones give airports limited time to respond once they enter controlled airspace, which raises the importance of building a responsive approach to countering non-cooperative UAVs.

Current standalone drone-detection solutions are costly and imperfect. The solutions are limited by the capability of sensors, difficulty in classifying and differentiating drones, and a lack of integration across systems, processes and agencies.

Even when drones can be successfully detected, incident handling is fragmented today: legal frameworks, responsibilities, and operational procedures are unclear, and agencies struggle to coordinate their activities at speed and across large areas. Furthermore, detected drones need to be classified. UAVs may have good reasons to fly around airports. Therefore, we need to be able to distinguish collaborative drones from non-collaborative ones, including the classification by integration of UAS Traffic Management (UTM).

The onus is on airports to create integrated cross-agency solutions in coordination with ANSPs and law-enforcement agencies. These solutions must provide an accurate picture of the shared airspace for quick decision making by integrating all available information sources, including reports and visual observations, existing or new Air Traffic Management (ATM), UAS Traffic Management (UTM) and drone detection systems. The coordination of stakeholders is critical, raising the complexity of the challenge and taking it from the technological arena into the organisational arena.

Taking control

Given the urgency, many airports begin investing in technological systems such as drone sensor systems without first considering how to integrate them into operational and organisational environments. As a result, airports end up investing time, effort and considerable capital resources into systems that will likely never deliver the hoped-for capabilities—not least because those capabilities have not been clearly defined.

To create an integrated solution that works, connecting organisations, processes and technology, airports need to target a broader vision.

First, they must define their own operational requirements and performance targets, which will shape their response to the challenge. For example, a small regional airport will be able to tolerate short interruptions in service much better than a large global hub.

Next, they should model the complete flow of information and communications across all stakeholders involved from all relevant agencies. The complete model includes all phases from detection to post-incident investigation.

The best-practice tool for this purpose is “Information Stream Design”.* This tool summarises the actors, systems and resources, and visualises individual process steps and the cooperation between actors and systems.

It is critical to start with a focus on the collaboration between organisations before considering the underlying technology, because the completed information stream design will be the basis for system design and system requirements. Ultimately, the selection, design and integration of technological solutions should be informed by the information stream design to ensure that the deployed system is fit for purpose.

*“Information Stream Design” was developed by Frequentis in cooperation with the Fraunhofer Institute, adopting key principles from “Value-Stream-Analysis”. The method is used to map, analyse, optimize and ensure a user- and business process-centric design. Frequentis Control Room Consulting department has successfully used this methodology with numerous customers to clarify operational needs and to derive technical requirements for systems and control rooms.

Information Stream Design

In information stream design, the starting point is the creation and analysis of user scenarios, including the definition of roles and responsibles involved at every step from the detection of a drone all the way through verification, alerting, risk assessment, decision making, intervention, all-clear, legal documentation and finally post-incident investigation.

Consider a typical user scenario: the incursion of a drone into restricted airspace next to an airport. Several eyewitnesses may notice the entry of the drone and report it to the responsible office at the airport. At the same time, the drone may be flagged up by automated drone detection systems, subsequently classified as unidentified and non-cooperative, leading to the triggering of an alert chain. Automated risk analysis may then lead to a decision to close the airport and surrounding airspace, then the deployment of countermeasures and/or human-led response teams. Once the drone is successfully intercepted and it is confirmed that there is no wreckage on the runway or further disturbances anticipated, the airspace may be reopened. Before closing off the incident, all evidence will be recorded and a final report created, before an investigation is launched to prevent future occurrences and to implement any learnings.

The user scenario can be divided into the following phases: Detection, Verification & Risk Assessment, Alerting, Decision, Intervention, Check & All-Clear, Documentation, and Investigation.

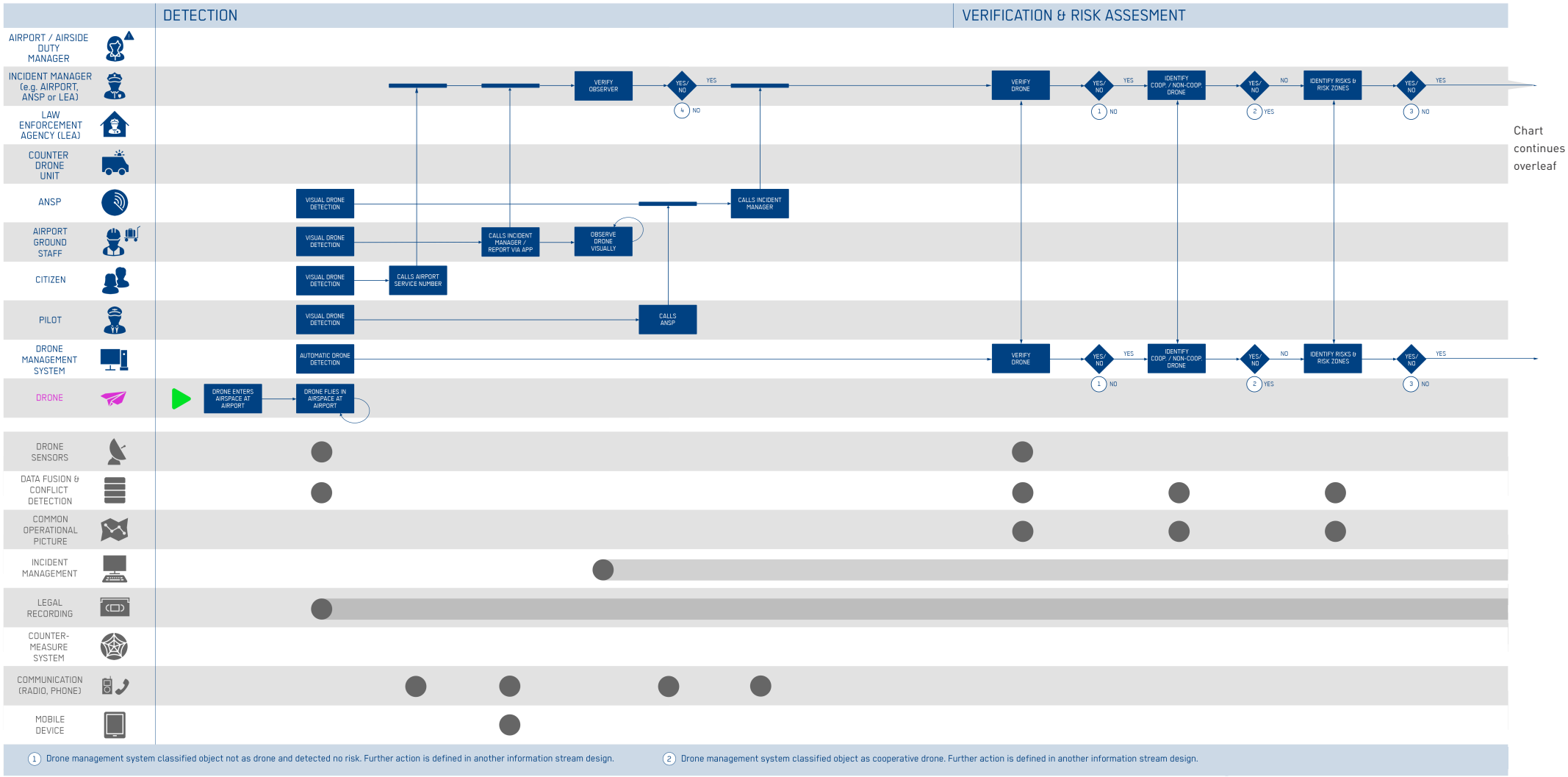
Sample roles and responsibilities:

In the following example, the names, roles and responsibilities are generalized to represent different airports from different countries. Actual names, roles, and responsibilities may differ.

- Airport / Airside Duty Manager: authority and decision maker for all safety concerns
- Incident Manager: responsible for coordinating (drone) incidents with all involved parties. This role may be undertaken by an airport, an ANSP or a law-enforcement agency, or it may be a shared responsibility
- Law Enforcement Agency (LEA): responsible for coordination of countermeasures
- Counter Drone Unit: directed by LEA to intercept drones and locate and arrest the drone operator
- ANSP: ensures ongoing air traffic safety during drone incidents, including the separation and efficient movement of aircraft and vehicles operating on and around the airport
- Airport Ground Staff, Citizen, Pilot: possible sources for reporting unauthorized drone activities in an airport environment

Systems:

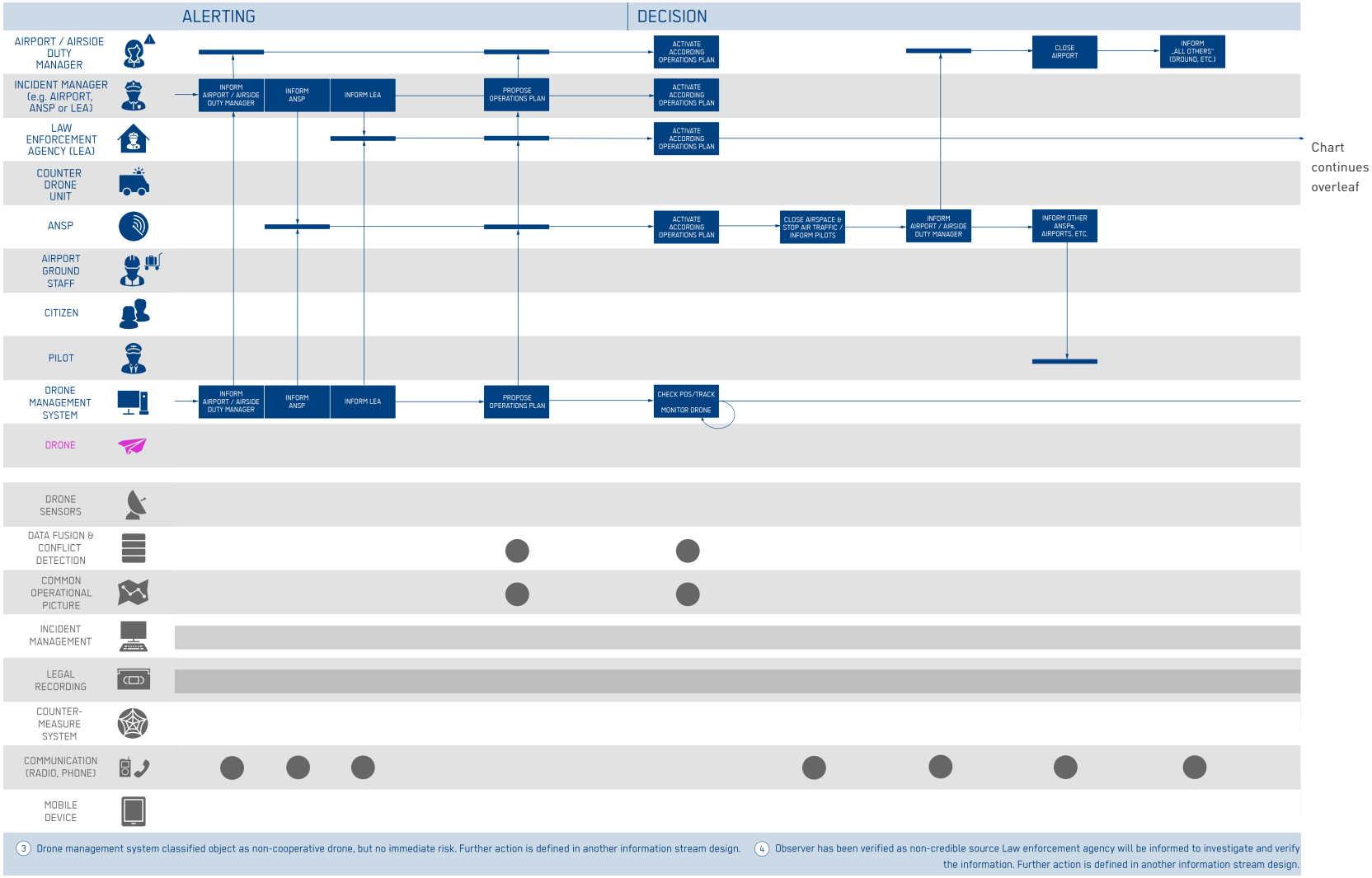
- Drone: an unmanned aerial vehicle (UAV)
- Drone Management System: an intelligent computer system integrating and automating drone detection, risk assessment, decision making and intervention
- Drone sensors: technical sensors for detection of UAVs in a defined area
- Data fusion & conflict detection (ATM/UTM/Drone Detection): data exchange platform integrating drone detection sensors, UAS traffic management systems (for classification cooperative/uncooperative), ATM systems (for risk analysis and deconfliction) and law enforcement systems (for blue force tracking)
- Common operational picture: geographical information system displaying and correlating cooperative drones, non-cooperative drones, aircraft, blue forces and geo-referenced elements; with definition of protected airspaces, integration and correlation of flight plans and communication (click-to-dial)
- Incident management: workflow management and decision support tools to automate and streamline standard operating procedures and cross agency collaboration
- Legal Recording: voice and data recording for legal, audit and training purposes
- Counter-measure system: approved for the airport environment to intercept non-cooperative drones
- Communication (Radio, Phone): voice communication systems in use at airport to connect stakeholders
- Mobile device: providing situational awareness in reporting and tracking drone incursions



Best-practice information stream design

Phase 1: Detection: Drones can be detected technically with specialised drone sensors, or visually through human sources. The characteristics of a robust drone detection solution include a multi-sensor fusion and the ability to integrate visual observations from ground staff, pilots, police forces and other sources.

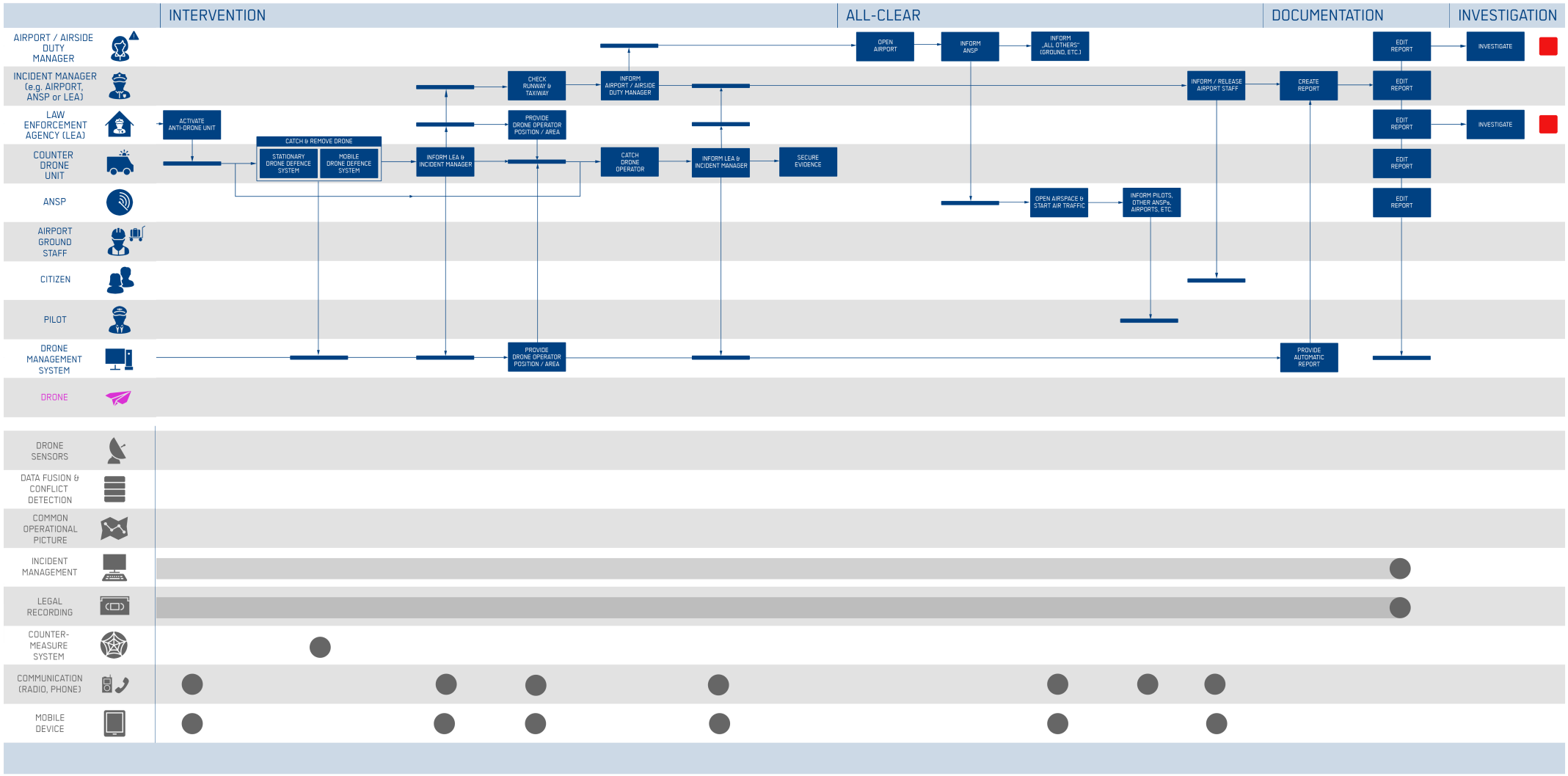
Phase 2: Verification & Risk Assessment: During this stage, the drone is identified as cooperative or non-cooperative, and an evaluation of the risk is undertaken to evaluate the potential threat based on pre-defined risk zones and characteristics of the drone (flight characteristics, type, payload, etc). Key elements are the link to the UTM system to distinguish between non-cooperative and cooperative drones, and the link to existing ATM systems to detect conflicts between general aviation and non-cooperative drones.



Phase 3: Alerting: As soon as a drone has been identified as a potential threat to the airport, all relevant stakeholders will be alerted immediately and given the available information to activate the respective operational plans.

Phase 4: Decision: Depending on the degree of risk, the relevant stakeholders will implement respective operations plans to prepare for intervention, including closure of air traffic and airports.

Note: In a fully integrated drone management system with trusted drone-detection sensors, phases 1, 2, 3 are fully automated and controlled by the drone management system.



Phase 5: Intervention: An intercept of the drone and arrest of the operator is coordinated by law enforcement. Intelligence is collected by the incident manager and shared to mobile devices.

Phases 6: Check & All Clear: When the drone has been captured, airport staff ensure that normal operations can resume, including re-opening of airport and air space.

Phases 7 and 8: Documentation and Investigation: Building a report based on shared experiences is crucial to enabling ongoing optimisation of the response to similar incidents in the future, while investigations can help with the prosecution of drone pilots (acting as a deterrent for the future).

Note: Throughout these stages, multiple parties must keep each other informed to pinpoint the location of the drone and uphold safety levels.

Understanding the benefits

By following this top-down or big-picture approach, airports, ANSPs and police forces can enable efficient cross-agency incident management based on agreed responsibilities and procedures. The technology and processes will be designed to support the people involved in drone detection, intervention and response, rather than the other way around, enabling easier uptake and better outcomes.

By integrating drone sensor and detection systems with UTM, ATM and law enforcement via a data exchange platform, all stakeholders have access to a common situational picture in real time. As a result, they can respond faster and more effectively to drone incidents, maintaining exceptional safety levels alongside high operational efficiency. The data can be shared securely with new and existing systems to visualise cooperative drones (collected via UTM systems), non-cooperative drones (detected through sensors and visual observations), air situation (provided by ATM) and ground situation (provided by police and/or military) including de-confliction of air traffic, all based on Asterix and AIXM standards.

Airports have the option to build on their existing infrastructure by deploying selected components where it makes sense, helping to minimise costs and to avoid vendor lock-in. By basing the architecture on open standards, airports can ensure interoperability and future scalability with evolving sensor and effector technologies. Further cost savings can be achieved through synergies created when drone sensor systems can also support other airport/ANSP use cases such as bird detection, remote tower or perimeter protection.

In general, drone incidents are just another type of incident that may happen in an airport environment. Integration with incident and crisis management software in an airport operation centre, or within an incident and crisis management control room, can create synergies in personnel, increase operational efficiency and enable the provision of drone detection as a service to multiple airports at once.

Conclusion

Working with Frequentis, airports, ANSPs and law enforcement agencies can draw on the market leader's extensive experience and deep domain knowledge to optimise their plans for counter-UAV solutions. Specifically, they can take advantage of the expertise of the Frequentis Control Room Consulting (CRC) team to apply superior methodology that is proven in multiple customer engagements and within research programs.

The Information Stream Design from Frequentis CRC embodies deep understanding of KPIs, responsibilities and procedures for drone detection and intervention at airports. Frequentis counter-drone solutions are based on state-of-the-art approaches to data fusion, integration and incident & crisis management, used worldwide in both civilian and military contexts.

Frequentis solutions support over 30,000 working positions for more than 500 customers worldwide. With long experience in serving not only ANSPs but also military and blue-light customers, Frequentis has the necessary breadth of understanding and experience to deliver integrated cross-agency solutions that span the full requirements of a counter-UAV solution in an airport environment.

FREQUENTIS AG
Innovationsstraße 1
1100 Vienna, Austria
Tel: +43-1-811 50-0
www.frequentis.com

2_CRO_IntegratedCounterUAV_0220