Airspace Security

EXECUTIVE SUMMARY

With the rapid pass that drones are evolving from a technology and business process application perspective, so are the possible threats, ranging from a harmless intrusion until a possible terrorist attacks. All this makes drone detection a more urgent agenda point in various industries in the world, as all standard security messieurs are bypassed by this new technology. Also one thing is sure, drones are here to stay.

Petrochemical are using drones for infrastructure inspection, but also are understanding the cost of a shutdown due to a rogue drone.

Renewable Energy are using drones for infrastructure inspection, but also understanding the cost of a shutdown and repairs of rogue drones

Power plant are using drones for infrastructure inspection, but also understanding the cost of a shutdown and repairs of rogue drones

R&D facilities are protecting themselves against espionage and hackers, who can use drones as a tool to infiltrate vulnerable networks or dropping malicious payloads.

Corporations are protecting themselves against espionage and hackers, who can use drones as a tool to infiltrate vulnerable networks or dropping malicious payloads.

Legal directive summary

In the following years, the number of industry use cases will unfold and entering into the global market. Whether drones are used for commercial, governmental, military or personal use. Most governments are catching up with this new phenomenon from a legislation and regulation perspective. The current legislation and regulations in Belgium are very restrictive, reducing commercial usage of drones mostly to class 1A and 1B drone pilots, or indoor usage.

European legislation and regulations are currently in there final stage, the EASA (European Aviation Safety Agency) has submitted a final opinion to the European Commission end of 2017 taking into account all received feedback to its proposal. The target is to have a common low-level airspace regulation in place by 2019, covering altitudes of up to 150 meters. This space will be governed by a system similar to existing air traffic control management, using e-identification and geofencing, providing governmental bodies the capability to have access to drone information. The common-law will cater as well for future usage of autonomous drones usage, as of today the flying BLOS (Beyond Line of Side) with a (autonomous) drone isn't allowed in most EU countries, it's mainly reserved only for governmental bodies (e.g. military, law-enforcement…).

Drone safety and security

Drone safety and security conversation is still in his infant state, as more emerging issues and loopholes are discovered. Drone manufactures, drone professionals and enthusiasts will continue to out-pace official instances, as they are struggling to keep up from a drone technology and capability perspective, as well from a payload perspective.

Intrusion detection & geofencing

The conversation on drone intrusion detection and geofencing, is still in his starting blocks, as the awareness within public sector or private sector isn't present on what the possibilities are to protect themselves against unwanted drone intrusion, throughout geofencing or types of protections to overcome these type of treats.

Conclusion

The technology and capabilities of drones increases in a rapid pass, as well the commercial applications, means that drones are her to stay and will be come part of the daily operations within the industry. As there are no physical barriers in our airspace to prevent interruptions or attacks, additional regulations will follow, but implementation of intrusion detection and geofencing technology will be required to provide warning of the presence of unauthorized drones.

Petrochemical

Introduction

Petrochemical industries are beginning to implement drone programs globally, providing engineers an early opportunity to use smart sensors to detect leaks, locate faults with precision, inspect facilities, equipment, pipelines, and assess structural health or damage.

Drones are quicker and easier to deploy, than the classical inspections, providing a live imaging and surveying. Dangerous and cost-inefficient detection tactics, such as scaffolding or deploying helicopter operations, can be taken completely out or become a second-response solution if required.

Safety is top of mind for all petrochemical operators. Spills and leaks have been of extreme concern throughout the history of the industry, with safety of the environment and people the most critical part of a manufacturer's infrastructure. Combined with the rise and availability of drone technology, these organizations have taken note of how to advance their facility and risk programs, and integrate drone maintenance to help prevent disasters and avoid costly interruptions to their operations.

Petrochemical corporations are investing in drones for maintenance and surveillance, and are also considering the unique and specific risks drone hardware poses to the physical infrastructure of their facilities. Wherever a drone operates to support a structure's safety program, there must also be a security procedure to ensure proper use and entry of drones in the airspace.

Risk

As of today, the petrochemical industry relies the classical inspection methods to detect damage and threats on their fix assets and rolling stock, at a significant financial cost. Therefor the industry need to consider how rogue drones fit into their security equation, avoiding possible damages or disasters caused by a rogue drone.

Conclusion

The risk of the wrong drone near a petrochemical facility could be deadly and cause serious financial cost and possible reputation damages, in case of an environmental disaster or lost of lives.

Such drones must be detected before they enter protected airspace and cause damage. When the drone is known, and comes to work at petrochemical, whether it be, the need to have an aerial protection and safety program in place is required.

Renewable Energy

Introduction

The Renewable Energy industry, is one of the early adopters of drone technology and using it for a significant amount of time, providing engineers an early opportunity to use smart sensors to detect structural health or damage early, avoiding any possible major incidence, (piece of a windmill flying away or misalignment of solar tower mirror).

As drones are not only easy to deploy, they are also programmable, allowing them to fly a certain inspection path, reducing the inspection time, and possible downtime (e.g. stopping a windmill or solar tower). Hands drones allows provides the industry the capability schedule more often inspections, as necessity of expensive inspection equipment (e.g. helicopter) isn't required anymore, except for specific specialized inspections.

Safety is top priority for all renewable energy operators. Structural damages have been of extreme concern throughout the history of the industry, with safety of the surroundings and people in dense populated areas the most critical part. Combined with the rise and availability of drone technology, these organizations have taken note of how to advance their risk programs.

As the renewable energy operators getting more acquainted with drone technology and their capability, they should also considering the unique and specific risks drone hardware poses to the physical infrastructure of their assets. Wherever a drone operates to support a structure's safety program, there must also be a security procedure to ensure proper use and entry of drones in the airspace.

Risk

As, the renewable energy industry relies significantly on drone inspection methods to detect structural damage and threats, the industry need to consider how rogue drones fit into their security equation, avoiding possible damages or disasters caused by a rogue drone.

Conclusion

The risk of the wrong drone near a renewable energy area could cause serious financial cost and possible shutdown of the asset in case the rogue drone causes structural damages.

Such drones must be detected before they enter protected airspace and cause damage. When the drone is known, and comes to work at the premises, whether it be, the need to have an aerial protection and safety program in place is required.

Power plant

Introduction

Energy manufacturers are beginning to implement drone programs globally, providing engineers an early opportunity to use different payloads to detect possible leaks, locate faults with precision, inspect facilities, equipment, pipelines, and assess structural health or damage. Drones are quick and easy to deploy providing live imaging and surveying.

Dangerous and cost-inefficient detection tactics, such as scaffolding or deploying other time and costly operations. Safety is top priority for all utility operators. Spills and leaks have been of extreme concern throughout the history of the industry, with safety of the environment and people the most critical part of a manufacturer's infrastructure. Combined with the rise and availability of drone technology, these organizations have taken note of how to enhance their facility, risk and security programs, and integrate drone maintenance to help prevent disasters and avoid costly interruptions to their operations.

Energy corporations are investing in drones for maintenance and surveillance, and are also considering the unique risks drone hardware poses to the physical infra- structure of their facilities. Wherever a drone operates to support a structure's safety program, there must also be a security procedure to ensure proper use and entry of drones in the airspace

Risk

The Energy industry relies primary on the classical inspection methods to detect damage and threats on their assets, at a significant financial cost. Therefor the industry need to consider how rogue drones fit into their security equation, avoiding possible damages or disasters caused by a rogue drone.

Conclusion

The risk of the wrong drone near an Power plant facility could be deadly and cause significant infrastructure and environmental damages from a financial perspective. Rogue drones must be detected before they enter protected airspace and cause damage. When the drone is known, and comes to work at a power plant, whether it be, the need to have an

R&D Facilities

Introduction

As drones have the ability to discretely spy on corporate operations, risking information leaks. For R&D facilities, lost of information, implicates a security breach not only from a physical, intellectual property right and copyright infringement perspective. All these issues will lead to financial damages, including losses investors, customers, diminish brand image and prompt a loss of investors and client confidence. All European country has very specific privacy laws, as well drone laws strictly forbid to operate drones above private property without admission. As R&D facilities are main targets for industrial espionage and hacking, it's a must to pro-actively protect their airspace and vulnerable buildings from unauthorized drone activity.

Risk

An unauthorized drone will lead to possible security breach on intellectual property right and copyright infringement perspective. All these issues will lead to financial damages, including losses investors, customers, diminish brand image and prompt a loss of investors and client confidence.

Conclusion

Drone protection for R&D facilities is no longer fiction, it's a practice in place today since any drone user is capable of causing millions in damages throughout industrial espionage or hacking. With an understanding of the threat that drones pose, as well as a proactive plan in place to protect critical infrastructure.

Cooperations

Introduction

Not only do drones have the ability to discretely spy on corporate operations, risking information leaks, but also an interruption of corporate operation can cause system malfunctions and server failures. Financial damages, including losses by customers, diminish brand image and prompt a loss of client confidence. Drones are enabling new avenues for hackers and industrial spies, who can use drones to carry payloads of any kind. All European country has very specific privacy laws, as well drone laws strictly forbid to operate drones above private property without admission. As certain corporations are targets for industrial espionage and hacking, it's a must to pro-actively protect their airspace and vulnerable buildings from unauthorized drone activity.

Risk

An unauthorized drone will lead to possible security breach an cause system malfunctions and server failures. All these issues will lead to financial damages, including losses investors, customers, diminish brand image and prompt a loss of investors and client confidence.

Conclusion

Drone protection for corporations is no longer fiction, it's a practice in place today since any drone user is capable of causing millions in damages throughout industrial espionage or hacking. With an understanding of the threat that drones pose, as well as a proactive plan in place to protect critical infrastructure.

Conclusion

Drone detection and safety is an emerging market, and is becoming a prominent issue as new regulations and drone incidents unfold. Drones were first introduced to the public as a military resource, and the technology has since been adapted and evolved for widespread commercial and personal use. With the introduction of any new technology, a learning curve is presented, and new applications outside of their initial intention unfold as they become more prominently usage in agriculture and land surveying, wildlife monitoring, search and rescue operations, for arts and entertainment.

As the drone market and capabilities will continue to grow, so will the incidents like drones carrying contraband into prisons, crashing into people and buildings, causing physical harm and damage. Drones were also being used as surveillance, inspections, locate missing persons.
As the technology was initially only accessible to the governmental agencies or military, can now procured and used by any consumer, whether for good or bad.

The number of use cases for drones, are growing on a daily basis, and regardless of the intention of a drone pilot, a rogue drone can cause significant damage. Drones are here to stay, and the European union expects a significant increase of drones entering the market over the next few years. All known classical security implementations to protect valuable assets, people and buildings requires an update to protect them against drone intrusions. As proactive aerial equivalent detection technologies are available on the market, it's up to security personnel, governments, and private citizens to determine how they want to protect their airspace from drone threats.