2020 INFOCUS Safety & Security

Aviation industry insights

Safety and surveillance • Airspace protection • Training
• Passenger and baggage screening • Cyber security

An HMG Aerospace publication

Rapiscan® systems
An OSI Systems Company

SEE INSIDE THE FUTURE

With ever-increasing global threats and new regulations being introduced, the 920CT gives you state of the art technology designed to meet the strictest of current and future regulations all within a contemporary design.

920CT can easily integrate with Rapiscan® Systems security checkpoint Tray Return System (TRS™).

The harmonious combination of 920CT and TRS creates a seamless experience for airports by strengthening security, increasing passenger throughput and staff efficiency.

EU ECAC C2 APPROVED

EU ECAC C3 APPROVED

www.rapiscansystems.com/920CT

One Company, Total Security

Contents

4 Welcome
6 Surveillance solutions
8 KID-Systeme
12 Dallmeier
14 Airspace protection
16 Passenger and baggage screening
18 Cyber security
20 Argus Cyber Security
22 Miltope
24 Training
26 Air Partner
28 ACI World
30 Events calendar

100 unmanned aircraft sightings reported each month by FAA.

5,000 trainees around the globe who benefited from ICAO training in 2019.

100,000 flights taking to the sky and landing without incident every day.

$860m the anticipated value of the commercial aircraft video surveillance systems market by 2023.

EDITORIAL
Editor / Chloë Greenbank
chloe@hmgaerospace.com

ADVERTISING SALES & MARKETING
Sales Manager / Toby Walton
toby@hmgaerospace.com

Sales & Business Development Manager / Jannie Boxall
janine@hmgaerospace.com

Marketing and Communications Specialist / Emma Walker
emma@hmgaerospace.com

PRODUCTION & DESIGN
Graphic Designer / Paul Firth
paul@hmgaerospace.com

Production and Design Editor / Steve Lodewyke
steve@hmgaerospace.com

MANAGEMENT
publishing@hmgaerospace.com
Publisher / Mark Howells
Director / Becky Howells

HMG Aerospace Ltd,
The Hub, Fowler Avenue,
Farnborough
Business Park,
Farnborough, GU14 7JF
United Kingdom
Tel: +44 1252 545993

www.hmgaerospace.com

Welcome to INFOCUS Safety & Security 2020

Every day approximately 100,000 flights take to the sky and land without incident, according to the International Air Transport Association (IATA). It's an impressive figure, especially when you consider the different factors threatening to disrupt the industry. From terrorist strikes, disease outbreaks, geopolitical posturing and cyberattacks to mechanical faults, disruptive passengers, data breaches and airspace protection, there are numerous risks to overcome for both airports and airlines.

However, despite these challenges, air transport is cited as the safest form of travel today and security remains at the heart of the industry's concerns. It's incumbent on stakeholders across the aviation sector from airlines and airports to governments and industry associations to ensure it remains so. Alexandre de Juniac, IATA's Director General and CEO, asserts that "on average, a passenger could take a flight every day for 241 years before experiencing an accident with one fatality onboard." He adds: "We remain committed to the goal of having every flight take-off and land safely."

Integral to modern life, aviation is a key driver of global economic development, but the big challenge looking forward is the forecasted double-digit growth in air traffic over the next two decades. Prior to the current coronavirus outbreak it had been anticipated that in 2020 alone, 4.72bn passengers will be flying high. As human beings we've only been travelling by powered flight for just over 100 years, but we're already crowding the skies, putting pressure on infrastructure and seeing increasing demands from passengers. All of this is resulting in constantly evolving challenges that threaten to disrupt the industry's safety and security record. In recent times, the industry has battled to recover from tragic incidents and restore public confidence. Accidents such as the two Boeing 737 MAX airline crashes, attacks at Zaventem Airport in Belgium and Ataturk Airport in Turkey, the US airstrike at Baghdad and the COVID-19 outbreak that continues to disrupt the global aviation industry are etched in the travelling public's consciousness.

Now emerging technologies combined with aviation's digital transformation and its growing reliance on cyber, as well as the changing character of war, mean that industry stakeholders are having to adapt fast to new and rapidly evolving threats.

Although the framework and procedures currently in place form a base layer, looking forward there needs to be new strategies in place to mitigate the threats we don't yet know about. And we need to factor in that the passenger or customer journey no longer begins on the aircraft or at the airport, it begins as soon as a booking is made. And that's where safety and security policies must start also.

"We remain committed to the goal of having every flight take-off and land safely."

Alexandre de Juniac,
IATA Director General and CEO

Safety and surveillance

As areas where large numbers of people convene, airports raise a diverse range of safety and security issues. The prevention of unauthorised access and detection of suspicious activities are a key focus for airport operators, particularly in light of recent terrorist attacks.

Video surveillance and video management solutions that give operators an exhaustive overview of the airfield and its perimeters are a powerful frontline defence.

When it comes to security requirements onboard the aircraft, video surveillance and aircraft data management systems are also on the rise. According to a report by Allied Market Research, the commercial aircraft video surveillance systems market, which was valued at $594m in 2016 will reach an impressive $860m by 2023.

Used to record and analyse activity in the cockpit and for cockpit door surveillance, as well as in the passenger cabins or cargo areas, video surveillance systems are used to monitor and act as a deterrent against disruptive or suspicious passengers, but they also provide recorded footage as evidence for prosecution.

Cameras inside the cabin are complemented by environmental camera systems that help capture images of the aircraft's exterior and surrounding environment. Helping to ensure safe operations while in-flight, these camera arrays are also used to help the pilots to perform ground manoeuvres and evade wingtips as well as to assist in gauging the light, climate and other environmental factors.

However, with the forecasted double digit growth in passenger traffic and, therefore, more video surveillance activity comes increased volumes of data. In response to this, scalable IP (Internet Protocol) surveillance systems and new innovations in analytics are helping to raise airline and airport security to new heights. These systems enable digital surveillance streams to travel over the internet, which in turn enables various departments to monitor video feeds from separate PC workstations and even offsite locations. Video analytics are playing an increasingly significant role in airport and airline security with software algorithms being used to detect specific activities and scan for suspicious individuals. For instance, cameras with facial recognition technology work to help authorities identify terrorist threats and marked individuals on government watch lists. Using behavioural recognition technology, cameras can also be programmed to detect incidents such as disruptive passengers, abandoned objects, congestion, reverse movement through checkpoints, and cars spending too much time parked in one spot outside a building. Such solutions are enabling aviation stakeholders to identify, monitor and manage each situation as it evolves.

When it comes to security, airport operators face a variety of challenges, not least due to the complexity of airport operations themselves, the architectural conditions and the multitude of stakeholders.

Caught on camera

Theft, in addition to unruly, disruptive passengers and provocations in the cabin have led to an increasing need for airlines to monitor and record activity in the cabin. Joachim Reuter, Product Manager at KID-Systeme – specialists in the design of aircraft cabin electronics – reveals how the company expanded its portfolio to include video surveillance systems.

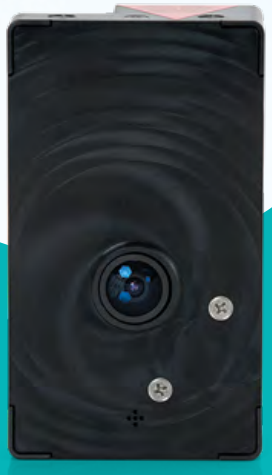
As a result of increased passenger traffic and constantly evolving security risks, challenges within the aviation industry have changed significantly since KID-Systeme launched SKYpower – its in-seat power and cabin power management system – in 1999. But, despite aviation's changing security landscape, passenger comfort and convenience remain integral to KID-Systeme's cabin solutions, which now also include an open software platform and cabin video surveillance services in response to the industry's security needs.

KID-Systeme's move into the video surveillance sector began in 2008 when the company was selected to develop and supply the camera system for use onboard Airbus's A350 aircraft. Exclusive to this particular aircraft model, the integrated solution was not available to be used fleet wide. However, in response to increasing demand from airline customers wanting to deploy the cabin surveillance option on all aircraft types, KID-Systeme developed a standalone video surveillance system for different aircraft types.

The company's initial concepts for a standalone camera concept were unveiled in 2014 with the Universal Video Surveillance System (UVSS) offering a modular and ›››

Cargo camera

Installed in the main and bulk cargo hold, cargo cameras work with motion detection to enhance recording control and provide complete surveillance of cargo operations onboard the aircraft. All recordings are watermarked for usage in further investigations if necessary.



Cabin camera

Cabin video monitoring helps keep passengers safe through any unwanted happenings during the operation of aircraft. It can also be used to provide evidence at a later date if needed.

Personal Data

Data storage and privacy is one of our primary concerns. We are frequently asked: What happens to video recordings and who has access to them?

The material that is stored on the server is coded, without a suitable "key" it remains encrypted and unreadable.

The operator of the system, in this case the airline, is able to decode the data and is responsible for handling it responsibly.

The film recordings are stamped with a watermark, which makes it possible to use them as evidence in court.

> “Airlines face multi-million dollar costs each year in terms of baggage claims and trolley thefts. KID-Systeme’s UVSS can help by combining surveillance and connectivity to help deter, monitor and resolve such incidents.”

scalable video surveillance solution for all types of aircraft.

Product Manager Joachim Reuter and his team of developers were integral to the architecture of this new system and in June 2015 an opportunity arose to partner with an airline customer wanting to trial UVSS across its fleet. Reuter and his team worked closely with the airline to understand their needs and conduct thorough cabin inspections to advise on the number and type of cameras required as well as optimal installation positions.

Just two years later, in November 2017, KID-Systeme’s UVSS made its official debut and since then hasn’t stopped evolving and adapting to the cabin environment and customer needs.

It offers airlines a surveillance system with customisable functionalities that can be tailored to individual expectations and needs. Up to 40 high-definition cameras allow monitoring of all areas in the aircraft. Video streams can be recorded and – in case of passenger misbehaviour or theft – used as evidence. Even in lowlight conditions infrared illumination capability enables the system to operate, while movement detection reduces the amount of storage space required.

UVSS is the only system on the market that combines video surveillance with an air-to-ground connection. Connectivity during flight and on the ground enables airline security to access videos during operation of the flight. The possibility of data analysis and pattern recognition combined with the possibility of immediately sharing incidents and dangerous situations with the ground makes the system unique.

Cockpit door camera

Keeping track of happenings in and around the cockpit during live events in the air, KID-Systeme’s Cockpit Door Surveillance System helps pilots and cabin crews during the flight as well as supporting possible further investigations after an event.

KID-Systeme

Seamlessly innovative and boldly green.

KID-Systeme is a market-leading supplier of electronic cabin systems for passenger and corporate aircraft, based in Germany. With their mindset geared towards innovations in technology, sustainability and customer experience, KID counts the most renowned airlines worldwide as their valued customers. Our product range encompasses customizable in-seat power solutions, cabin and cargo safety features, as well as an open hosting platform for applications and entertainment.

www.kid-systeme.com

KIDSYSTEME

Zooming in on surveillance challenges

Video security equipment manufacturer Dallmeier has more than 35 years of experience in transmission, recording and picture processing technology and is a leading pioneer of CCTV/IP solutions worldwide. Its multifocal sensor camera system, Panomera®, offers video technology surveillance for large airport areas, far surpassing the conventional HD 1080p standard. Dallmeier's Product Marketing Director, Josua Braun, discusses the merits of the system for airports.

What are the challenges for airport security?

When it comes to security, airport operators face a variety of challenges, not least due to the complexity of airport operations themselves, the architectural conditions and the multitude of stakeholders.

One example is the recurrent violations of the security area. Here, expensive terminal closures occur time and again because no suitable technology is available to enable the emergency services to gain an overview of the situation in a sufficiently short time.

Another example is the optical protection of the apron areas. In the event of a security-relevant incident, the police take over the camera systems, which often results in all other parties involved being "blind", so to speak.

Regardless of the area of application, however, all airport operators must pay attention to the cost-effectiveness of their systems. This requires solutions that are as lean as possible and can be operated efficiently. Internal billing models are also becoming increasingly interesting, for example, when Artificial Intelligence (AI)-based systems allow passengers to be better directed and waiting times to be reduced or shop stops to be optimised.

Airport security officers can use Panomera® to comfortably capture even the largest spatial contexts with significantly fewer screens.

Distance 200 m / 650 ft

Distance 420 m / 1,400 ft

Distance 500 m / 1,600 ft

Distance 750 m / 2,400 ft

Compared to megapixel and PTZ cameras, Panomera® multifocal sensor systems always capture the entire scene in a defined minimum picture quality. This allows operators to perform high-resolution zooms in both live operation and recording.

With passenger traffic on the rise, how do you envisage the future of airport security?

The main focus will be on the smart use of analysis and AI-based assistance systems to meet the challenges posed by the continuing increase in passenger numbers. In addition to this, it is absolutely essential for airport operators to operate the systems for security as economically as possible and avoid a cost explosion. This will come down to deploying "smarter" airport security by using innovative, disruptive technologies such as multifocal sensor technology or AI-based assistance systems.

How can video surveillance assist airports in overcoming these challenges?

Dallmeier's unique, patented "Panomera®" – multifocal sensor camera systems enable the complete monitoring of even the largest spatial contexts with considerably fewer systems than is the case with comparable solutions. The multifocal sensor technology offers the largest images with maximum detail resolution. This technology offers a significantly better overview of the situation in the often complex architectural contexts at the airport and a significantly higher operator efficiency. The special technology also enables several operators to zoom into different areas of the image simultaneously and independently of each other. This revolutionises optical support, for example, when tracking down baggage left alone or securing apron areas.

> "Dallmeier's "Panomera®" multifocal sensor camera systems enable the complete monitoring of even the largest spatial contexts with considerably fewer systems than is the case with comparable solutions."

Airspace protection

With activity in Unmanned Aerial Systems (UAS) – drones, unmanned aircraft or Remotely Piloted Aircraft – booming, counter-drone technology is critical in keeping the skies above us safe and open for business.

According to consulting group PricewaterhouseCoopers (PwC), the drone industry has gained momentum in the past couple of years and is poised to be worth $127 billion by the end of 2020. Subsequently, there has been a sharp increase across the aviation industry to develop systems including artificial intelligence and advanced robotics, to reliably detect, identify and manage drone activity.

An increasing number of close drone encounters are frequently being reported by airline pilots. But it was the suspected drone sightings at Gatwick Airport in 2018, as well as at Heathrow Airport and Newark Airport in 2019, that were the real wake-up call for airports, airlines and aviation authorities. While none of these alleged airport sightings have resulted in fatalities, they did highlight how unprepared the global industry was when it comes to drone protection

In lieu of the Gatwick incident, the UK Government has fast tracked its drone detection standards capabilities and as of March 2019 it is illegal to fly a drone within 5km of an airport. Similarly, the US-based Federal Aviation Administration (FAA) has ordered increased surveillance of drone operations in areas where reports of risky or noncompliant drone operations are high, which includes communities and areas close to airports. It cites that unmanned aircraft sightings have dramatically increased over the past two years with more than 100 sightings reported each month.

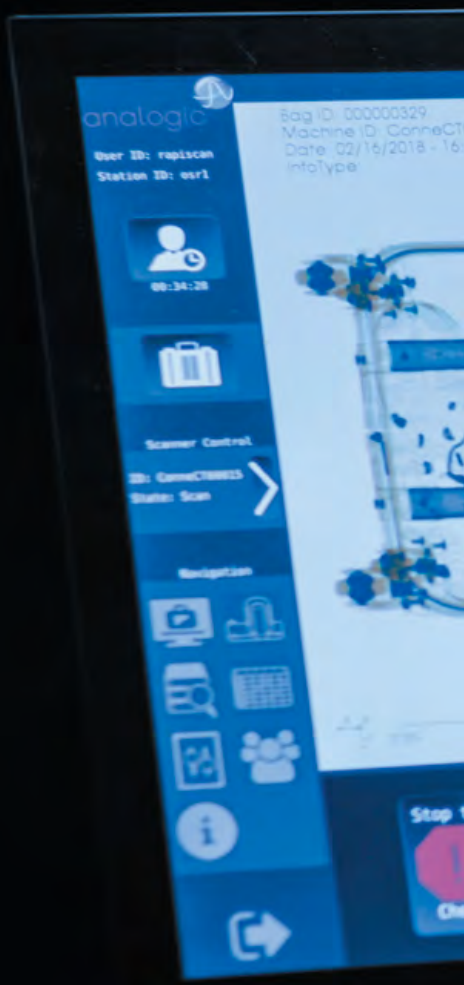
Although questions remain as to whether the enforcement action taken against negligent drone operators is adequate, the real focus for counter-drone technology needs to be based around a data-driven process. Dedrone's Regional Sales Manager for UK and Ireland Amit Samani states that until recently "there was a lack of quantifiable data… the focus now should be on getting airports working with regulators using tangible data and action points – the whole counter-drone strategy has to start with a data driven process."

Modern security requires a multi-layered approach to keep up with the evolution of drone technology, says Amit Samani of Dedrone. Most airports today use radio frequency sensors to detect, track, identify and classify drone activity. In an airport there's obviously lots of active equipment, so on the whole you don't want active systems that could impact other systems on the airfield.

Dedrones' RF Sensors are purpose-built for airspace security and collect hard data on drone activity in the airspace. They can detect where a drone or multiple drones are, classify them and track the user. DroneTracker software then connects sensors, performs machine-learning analysis, and is the central nervous systems for the complete solution. Multiple layers of security can be added by integrating sensors such as radar, infrared or acoustic devices.

The drone industry has gained momentum in the past couple of years and is poised to be worth $127 billion by the end of 2020. Subsequently, there has been a sharp increase across the aviation industry to develop systems including artificial intelligence and advanced robotics, to reliably detect, identify and manage drone activity.

Passenger and baggage screening



The 9/11 terrorist attacks in New York might have been a turning point in aviation's history for the need to increase security during baggage and passenger screening. However, with innovative technologies continually emerging to help improve efficiency at security checks and to avoid the inconvenience of long queues for passengers, the tides are finally turning once again. Using computed tomography (CT) scanning technology for baggage screening can eliminate the need for passengers to remove liquids and laptops from their bags. It's a major step forward in aviation security and is already being embraced by airports around the world through industry suppliers such as Rapiscan and Analogic.

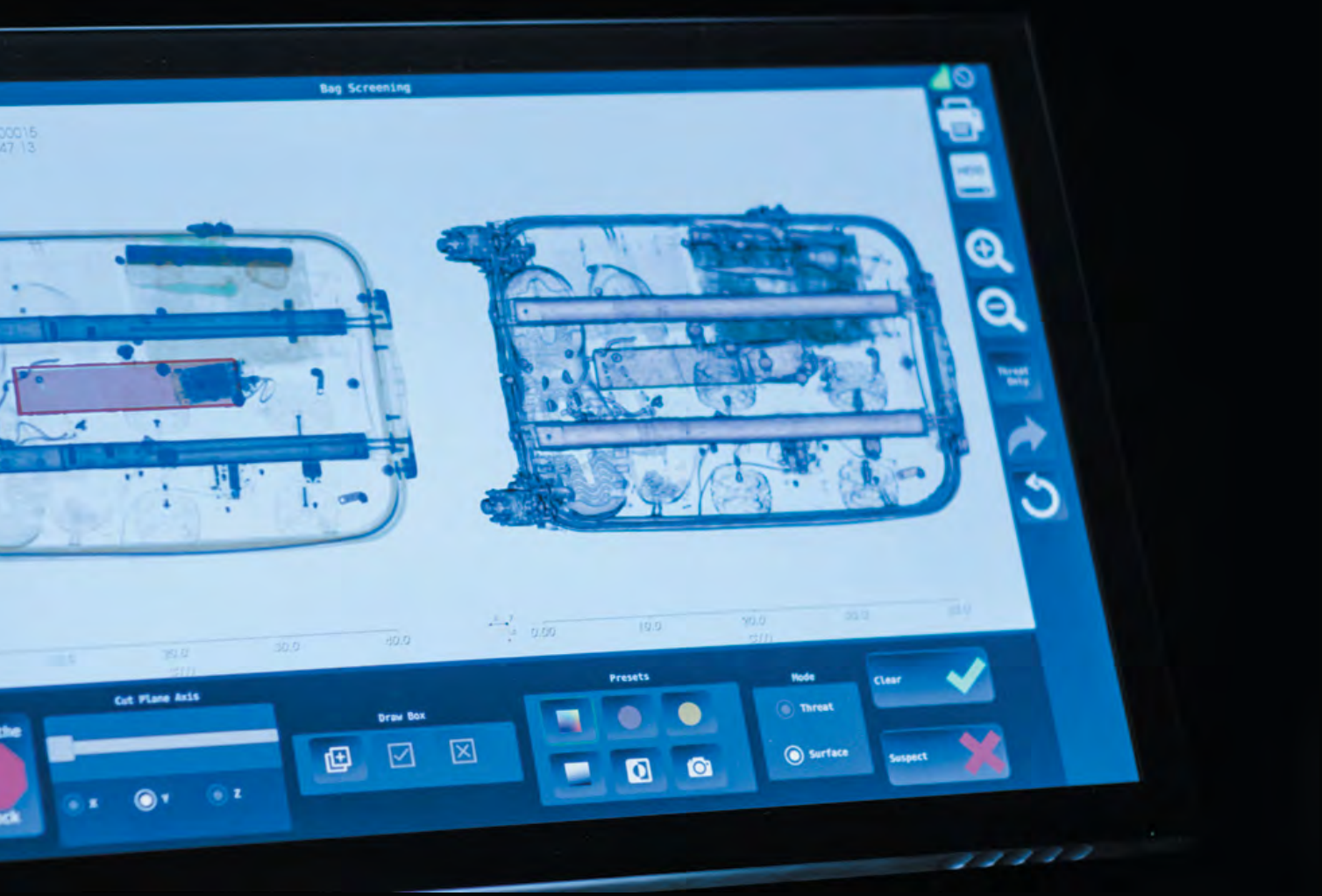
Biometric solutions are also on the rise for baggage handling solutions. Smiths Detection showcased its proof of concept for an integrated biometric checkpoint solution for the first time in September 2019. It enables risk-based screening (RBS) through linking passengers with their trays. RBS will allow for differentiated levels of screening to be applied to individual passengers and their belongings based on criteria such as personal risk profile, flight or destination. What's more, by linking passengers to trays, airlines could monitor passenger flow through security for specific flights or track the number of trays per flight to predict overhead compartment capacity.

The big buzzword when it comes to transforming the passenger journey, biometrics are increasingly being used at various touchpoints throughout the airport including security checkpoints. They are even being explored for use onboard the aircraft. In 2017, Panasonic Avionics Corporation and Tascent entered into a strategic partnership to create unique offerings that use biometrics to personalise the in-flight experience including biometric payment capabilities.

Border control authorities are also heavily investing in biometrically enhanced authentication and security measures. These investments are increasing return on investment and helping stakeholders develop more sophisticated monetisation strategies. These include streamlining identity management and passenger flow, decreasing processing time, automating passenger authentication, improving the overall experience, and developing new interoperable platforms and services.

What's more, IATA is now advancing the use of biometrics further to eliminate the use of paper-based travel. The association is currently working on the development of an integrated identity management solution known as One ID. The idea is to bring together biometrics, electronic boarding passes and travel visas into a single form of digital travel document that virtually eliminates mobile or paper-based alternatives. Ultimately, a passenger's face is all that will be needed to proceed through an airport and onto the plane. Although still in its infancy IATA's One ID solution is being touted as a game changer in enhancing the passenger experience and accommodating booming passenger growth while maintaining stringent security levels.

The challenge with using biometrics to create a more seamless journey is of course around data privacy and protection. While industry experts cite that more and more passengers are accepting the notion that the use of biometrics has a time-saving advantage that outweighs their concerns over an image of their face being captured, there remains a need for governments across borders to standardise regulations and establish common standards.



Superior screening

Rapiscan Systems announced in March 2019 that its 920CT checkpoint screening system had achieved C3 approval from the European Civil Aviation Conference under its Common Evaluation Process for Explosive Detection Systems for Cabin Baggage. The 920CT system follows the ECAC standards and allows passengers to leave liquids and laptops in their carry-on luggage during the screening process at airport checkpoints that use the system. Rapiscan's 920CT is equipped with advanced software and detection algorithms that are designed to be upgradeable. Rapiscan Systems says the 920CT is superior to 2D systems as it provides improved visualisation of potential threats due to its 3D volumetric imaging.

Cyber security

The aviation sector has benefited hugely from the increasing level of connectivity and digitalisation across the value chain, from opportunities for better customer service to more efficient flight services, safe cargo operations and an enhanced overall passenger experience. But how well is the industry equipped to cope with the latest threat posed by increasing digitalisation – that of a cyberattack?

The greatly increased use of technology including big data as well as in-house and outsourced analytics, alongside greater connectivity and the wider reliance on data sharing with stakeholders and users all serve to increase cyberattack vulnerabilities for both airlines and airports.

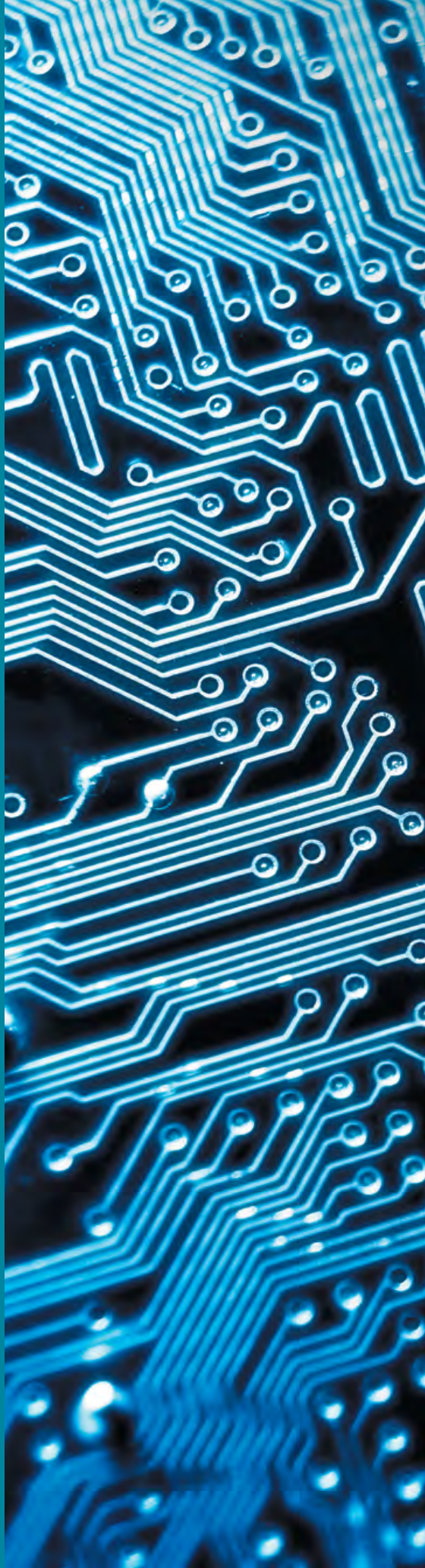
Cyber threats range from low-skilled individuals who use scripts or programs developed by others to attack computer systems, networks and disfigure websites, through to highly skilled and motivated nation states. But regardless of their level of expertise, a successful attack on an airport or airline could paralyse its operations.

The European Aviation Safety Agency (EASA) says there are 1,000 cyberattacks on aviation systems each month. Multiple systems across civilian aviation and cargo operations are open to hacking and malware attacks. Reservation systems, flight traffic management, access control management, passport control, cloud-based airline data storage and cargo handling systems are all under threat. Meanwhile, onboard an aircraft there's multiple IT systems also at risk. From flight control systems and fuel gauges to maintenance computers, in-flight connectivity solutions, GPS-based navigation systems and critical crew services that rely on satellite communications, the potential points of IT and cyber vulnerability continue to evolve. Add to this the millions of passengers now accessing the internet and using their own phones and devices when travelling by air. Combined, this has created a vast aeronautical, satellite-based communications ecosystem, integrated with terrestrial networks, where the number of places a cyber threat might gain access and wreak havoc have increased almost beyond measure.

Cyber security is a complex, critical challenge that stakeholders across the industry are still getting to grips with. But the pressure is on to actively reduce this risk. According to The Aviation Cyber Security Market – Growth, Trends and Forecast, this sector is expected to register a Compound Annual Growth Rate (CAGR) of around 11% over a five-year period to 2024.

The industry is certainly taking note. Organisations such as the Civil Air Navigation Services Organisation (CANSO) have developed a Cyber Security and Risk Assessment Guide, while IATA has developed an industry-wide Aviation Cyber Security Strategy. Meanwhile PA Consulting, which collaborated with four major airports to understand the common vulnerabilities to cyberattacks and outline the best practice for cyber security urges airports to take a holistic approach – one that builds cyber security into airports by design.

As with all factors that have the potential to disrupt the industry, the ever-evolving threat of a cyberattack requires an integrated risk management approach combined with threat intelligence and real-time information sharing.



Cyber threats range from low-skilled individuals who use scripts or programs developed by others to attack computer systems, networks and disfigure websites, through to highly skilled and motivated nation states. But regardless of their level of expertise, a successful attack on an airport or airline could paralyse its operations.

The IFEC Cyber Threat Landscape

The IFEC system is often perceived to be an isolated system with little risk to itself or other onboard systems. Argus experts explain why the truth is slightly more complicated and what can be done to mitigate associated risks.

RISK TO IFEC

Being an after-market system allows in-flight entertainment and connectivity (IFEC) to be comprised of commercial off-the-shelf (COTS) components, unlike the rest of the aircraft which has to conform to many rules and regulations. While using COTS components makes the IFEC price-competitive, it also introduces some inherent risks.

The most serious risk is **providing adequate patch management**. COTS means the manufacturer is not responsible for the entire production chain but rather integrates third-party components. When vulnerabilities are discovered – whether by white-hat researchers who can easily obtain the same components, or by black-hat hackers – the original tier-n manufacturer needs to issue a patch, and propagate it up the supply chain to all customers. The IFEC manufacturer's hands are tied here.

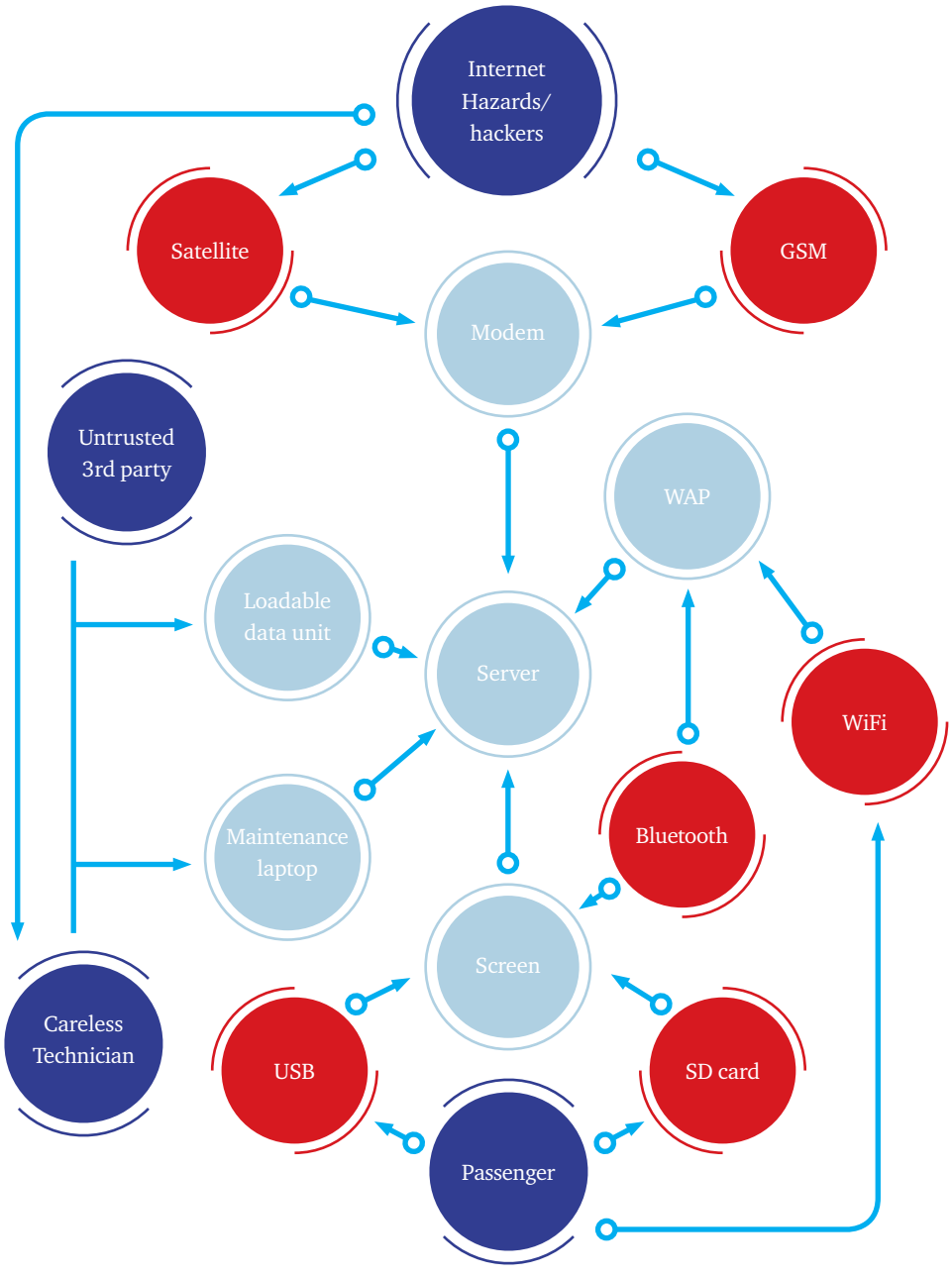
Second are problems originating in **insecure implementation**. Even with good SDLC practices (uncommon as they are,) mistakes still make it to the implementation stage. An insecure admin panel was detected in more than one IFEC implementation, potentially enabling an attacker to make modifications to the system. Not only that, but having third-party components means that while the IFEC manufacturer might have performed Threat Analysis and Risk Assessment (TARA) on their system, problems originating in third-party components might be unaccounted for.

Third is the **long production and update cycles** in the aviation industry. Design choices that are deemed secure at the time of the product's design can quickly turn into security risks by the product's release, as the threat landscape evolves. And unlike in the IT industry (and even in the automotive industry), quick, remote over-the-air software updates are still unacceptable – even if the first problem of patch management was mitigated, there'd still be a problem delivering the patch.

Fourth is the **constant friction with passengers**. Malicious passengers can compromise their own system and proceed from there. They don't need to leave the IFEC domain to wreak havoc – it's enough to pop a message on other passengers' screens to instil fear.

> “ IFEC systems are comprised of commercial off-the-shelf (COTS) components, unlike the rest of the airplane which has to conform to many rules and regulations. While using COTS components makes the IFEC price-competitive, it also introduces inherent risks. ”

Typical attack surface of a model IFEC system



RISK TO OTHER SYSTEMS

If an attacker manages to escape the IFEC, they could perform lateral movement and attack other components onboard the plane. **Crew Terminal** and **CMS** infection could be leveraged into a Denial-of-Service attack on cabin functions such as lights, PA system, and air-conditioning – a risk resulting in annoyance and costly compensations. If the **cockpit** is using the same Internet connection, then the **Electronic Flight Bag** (EFB) is also at risk of being manipulated or compromised.

What’s more, there are scarcely any backup books in the cockpit anymore.

HOW TO MITIGATE

As in other domains, a layered security plan is required:

- Secure design and layout for **prevention**, such as SDLC and domain separation;
- Event monitoring, recording, and transmission for **detection** and **Incident Response**.

Solutions should be **vulnerability-agnostic** as vulnerabilities are bound to keep being found and reported.

In the past few years we have been witnessing the automotive industry acknowledging the risks for similar technology and taking a very proactive approach to mitigating the threats. We think it’s time for the IFEC industry to do the same.

The article was written by Rubi Arbel, VP Aviation, and Inbar Raz, Senior security architect, at Argus Cyber Security, an aviation and automotive cyber security company.

Future-proofing cabin cyber security

The aviation industry has benefited immensely from innovations in connectivity within the cabin. But with these advances in technology comes the constantly evolving threat of a cyberattack. Miltope explores how dynamically improving system intelligence might be the solution for future-proofing the cabin instead of thicker firewalls.

Wireless cabin networks have become an integral part of an aircraft's infrastructure. Their utilisation is growing exponentially as a result of the rise in handheld devices and demand for onboard connectivity for both passengers and crew. The Internet of Things (IoT) is also increasingly finding its way into the aircraft, which means more touchpoints between external devices and the network.

However, with these rapid advances in connectivity we are also seeing cyber threats evolve with similar speed and creativity.

So, how can we protect against these threats?

Traditional responses address "known threats" via static and passive tools such as firewalls or authentications that were developed to rectify previous attacks. However, constantly evolving cyber threats require a more proactive and dynamic approach enabling cyber security to evolve at pace with the threats.

Several regulatory bodies have recognised the need to tackle cyber security differently and are translating these into directives. For example, the EU with its Network and Information Security (NIS) directive has determined such requirements become law.

For the aircraft cabin this means two kinds of controls: continuous Security Monitoring and Anomaly Detection for the usage behaviour displayed on the network.

Miltope has incorporated software technologies to build a cyber-secured wireless cabin network. The two key components for this cyber protection are:

a) Machine learning driven by Artificial Intelligence that operates the monitoring and anomaly detection process. For the latter, the system identifies the normal utilisation and derives "abnormal" behaviour. For an airline this means that the system on each aircraft – whether its connected to the internet or not – establishes what is "normal" for a network and recognises abnormal utilisation. Naturally, the usage patterns will differ between, for example, a daytime business-oriented three-hour flight within Europe and a nine-hour overnight holiday flight from Florida. The system understands that and differentiates accordingly.
When the aircraft is online (in-flight or on the ground), the airline system can collate and compare the various "normalities" between fleets, routes and flights to build an even bigger database of network behaviour patterns.

b) The identified "abnormal" behaviour then results in rectifying actions, triggered by the Location, Position and Tracking feature of the CHT (Cognitive Hotspot Technology) software that is part of the Miltope solution. CHT is a set of algorithms that also maximises the resources of the WiFi network such as access points, different radios, available channels and varying power levels in order to maximise the wireless network capacity while keeping the number of access points to a minimum.

What is the beauty of this solution in comparison to old-school cyber security?

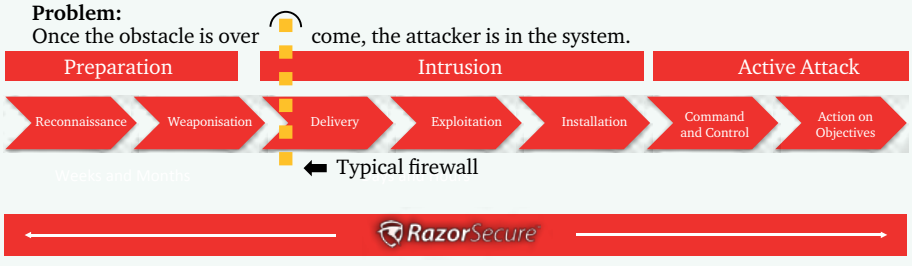
While firewalls and authentications gradually became lesser obstacles for intelligently evolving cyber threats, the new approach allows for the system to become smarter with each iteration, thus resulting in future-proof protection. What's more, because this is a software-based solution there is no need to update the underlying hardware platform in order to get a more secure cabin network.

"When the aircraft is online (in-flight or on the ground), the airline system can collate and compare the various "normalities" between fleets, routes and flights to build an even bigger database of network behaviour patterns."

Typical Cyber Attack process (Lockheed-Martin model)

Old cyber security: Passive, static protection occurring at one point in the process

Problem:
Once the obstacle is over come, the attacker is in the system.



New cyber security: Active, dynamic protection throughout the whole process.

Solution: Continuous monitoring of system utilisation to detect abnormalities as indication of attack.

nMAP2 with RazorSecure

- RazorSecure learns "normal" system behaviour
- The system then identifies "abnormal" behaviour
- This can identify attacks across the entire kill chain

Machine Learning (AI)

Future oriented, not driven by past experiences

Detects attacks also when not online.

Training

Underpinning the industry's ability to maintain safe, efficient operations is of course a global network of qualified and competent personnel. However, a global skills shortage is a multi-faceted problem, which is now high on the industry's agenda. By 2036 some 620,000 pilots will be needed across the global network and no less than 80% of these aviators will be new pilots, not yet flying today.

It's a similar story playing out across the industry with respect to future engineers, cabin crew, maintenance personnel, air traffic controllers and other skilled technicians. The predicted growth in the number of aircraft and the current record order backlogs of major manufacturers such as Airbus and Boeing demonstrate that finding, developing and retaining a skilled workforce is a major challenge. There is, however, visible evidence for partnerships, collaborations and concerted action across the STEM (science, technology, engineering and maths) education landscape to deliver the demand for a skilled workforce across the industry and around the globe.

From departments including fire safety and air traffic management (ATM) to cabin crew, pilots, compliance monitoring, legal, cargo and fuelling, training is a vital cog in aviation's wheel. Continued investment to ensure adequate training is not just available, but also accessible and affordable for existing personnel and their successors is essential. Aviation leaders are urged to embrace the need to find a sustainable solution to appointing appropriate human resources to support the industry's growth while maintaining stringent safety and security protocols. This can only happen with the collaboration of manufacturers, training schools, airlines and other related institutions.

As a UN specialised agency dedicated to achieving the sustainable growth of the global aviation industry, the International Civil Aviation Organization (ICAO) offers its Global Aviation Training (GAT) Office as the focal point for all ICAO training related activities. It asserts that sustainable, safe and secure global aviation development relies on the availability of qualified and competent employees, supervisors and managers to plan, co-ordinate, manage, operate, maintain and oversee all complex operations in various airports, airspaces and aircraft.

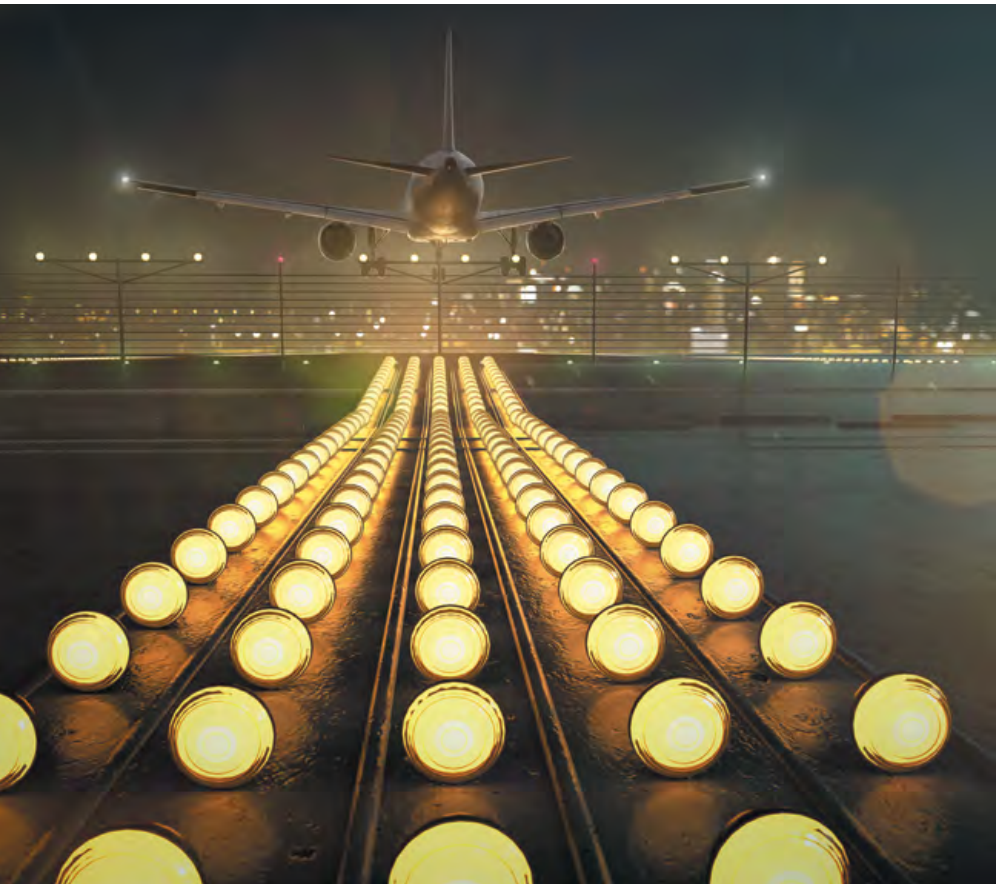
"To facilitate the development and delivery of ICAO training, GAT established a network of training organisations under the TRAINAIR PLUS Programme (TPP)," Diego Martinez, Chief of GAT, told INFOCUS Safety & Security. "As of March 2020, over 100 organisations from 80 ICAO Member States have joined the TPP and embarked on the development and delivery of ICAO competency-based training packages. In 2019, more than 5,000 trainees globally have benefited from ICAO classroom and online training," he continues.

Explaining that the ICAO catalogue comprises more than 250 training packages in nine key areas, Martinez says, "These can be delivered in a classroom format, in the premises of aviation organisations worldwide, or in online and blended formats. In 2020, new courses regarding State Safety Programme, Unmanned Aviation, Facilitation, Civil Aviation Master Planning or Aviation Medicine are being made available to the aviation community. Additionally, workshops to support States in their aviation training and capacity-building roadmaps will be delivered."

Martinez also urges aviation organisations to invest in training their next generation of aviation professionals, as well as refresh the competencies of their current generation of professionals. "Due to the advent of new technologies, as well as attrition impacts, it is key to plan ahead. Identifying key competencies which will be required to operate today and tomorrow's aviation jobs is an example of a critical activity which all organisations should undertake as a priority," he concludes.

Photo: Skyborne Airline Academy

The International Civil Aviation Organization's (ICAO's) Global Aviation Training (GAT) Office is the focal point for all ICAO training related activities. It asserts that sustainable, safe and secure global aviation development relies on the availability of qualified and competent employees, supervisors and managers.



Safety & Security – a partnership you can rely on

For as long as aircraft have been flying, the prevention of loss of life has always been the ultimate goal. However, as all incidents are a series of events or threats coming together, safety management is about mitigating or removing threats throughout the organisation's operation to reduce events that can cause losses.

The European Aviation Safety Agency's (EASA's) emerging safety regulations for service providers within the whole aviation system confirm the importance of developing effective management systems into the culture of operations. In parallel, the importance of culture aligned with effective aviation security management systems (SeMS) is gaining momentum, with the International Civil Aviation Organization (ICAO) placing culture as the key focus for 2020. A key focus for the Civil Aviation Authority (CAA) is also the introduction of a SeMS approach into aviation security, clearly applying safety performance-based regulatory learning into security.

SAFETY FIRST

At Baines Simmons, part of the Air Partner group, we view this safety objective as the intentional outcome of an effective management system.

People are at the heart of driving effective safety and security systems. Determining the vision of what a good system looks and feels like is key along with a clear appreciation of current performance indicators, aligned to desired metrics and a clear route to success based upon priorities determined by risks and vulnerabilities.

INVESTING IN THE PRIORITIES

We have amassed a wealth of knowledge and expertise in supporting our clients to build a management system unique to them that addresses compliance and safety risk management hand in hand through our SMARRT MAP™.

Investing in analysis provides you with the confidence and capability to develop robust foundations that are compliant with

regulatory intent and fully integrated with your operational requirements. Furthermore, it guards against inefficiencies and wasted investment.

We have worked with the world's largest aviation organisations to develop and power up their management systems utilsing our suite of diagnostic, advisory and training services that are recognised as world leading.

> "Investing in analysis provides you with the confidence and capability to develop robust foundations that are compliant with regulatory intent and fully integrated with your operational requirements."

BETTER TOGETHER

Excitingly, we are now able to draw upon the expertise of Redline Assured Security, who joined the Air Partner family in December. Together we are proud to offer combined and unique capability as Air Partner's Safety & Security Division.

Redline is a recognised expert in aviation security training, quality assurance, compliance management and is the UK's only ICAO endorsed Aviation Security Training Centre. It works with organisations to embed security management policy, process and systems to ensure compliance with ICAO, EU and national standards. It has invested significantly in the development of software tools, in particular its digital SeMS. This cloud-hosted management system combining aviation security and software development expertise, enables users to track key performance metrics in near real time across multiple sites.

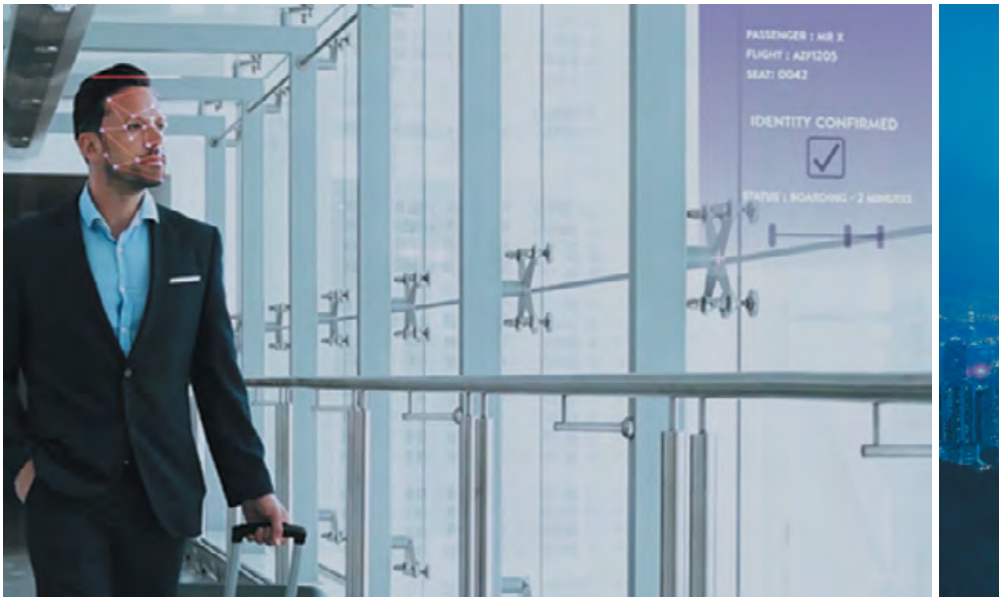
WORKING IN PARTNERSHIP

This collation of data from multiple safety and security streams brings clarity and focus to pre-determined metrics, enabling timely management review and intervention to significantly reduce unnecessary and potentially costly exposure to risks and vulnerabilities.

To learn more about how our new and unique Safety & Security division can support you to create a tailored, cost effective, culturally embedded, safety and security management system, please email safesec@airpartner.com or call +44 (0) 1276 859 519

Innovation in aviation security

ACI World explains why the growing demand for air services and the continual development of new technologies amply illustrate why the aviation industry needs to develop systems and process that can anticipate and meet tomorrow's facilitation and security challenges.



The air transport system is always under pressure to deal with a wide range of security threats, from explosives to drones, to chemical and cyber security attacks. Growth also puts pressure on airport facilitation by adding to congestion. New security measures are often added, but few are ever removed or reconsidered.

These challenges also present an opportunity to think about security differently, in a more holistic manner. From the time the person starts their journey to the time the aircraft departs, they should feel equally secure. At ACI, we seek to defend all parts of the airport from attacks, including public or landside areas.

For this reason, innovation in aviation security is a priority for ACI and its member airports in all regions. We are finding inspiration in all parts of society – from artificial intelligence, biometrics and automation to smart regulation principles and data management.

SMARTER SECURITY SCREENING

ACI's Smart Security programme identifies improvements that can be made to the screening process through a combination of existing and emerging technologies. The programme explores how passenger screening could be designed by providing airports with solutions which help maintain security while increasing operational efficiency and passenger satisfaction.

Ultimately, Smart Security looks beyond mid-term solutions and focuses on risk-based security concepts, innovative processes, and advanced screening technologies that will help achieve a truly seamless passenger journey through airports. ACI will soon release its "Vision 2040" for Smart Security which will transform the traditional checkpoint by exploring concepts such as off-airport screening, stand-off detection and seamless walk-through security processes.

DIGITAL TRANSFORMATION

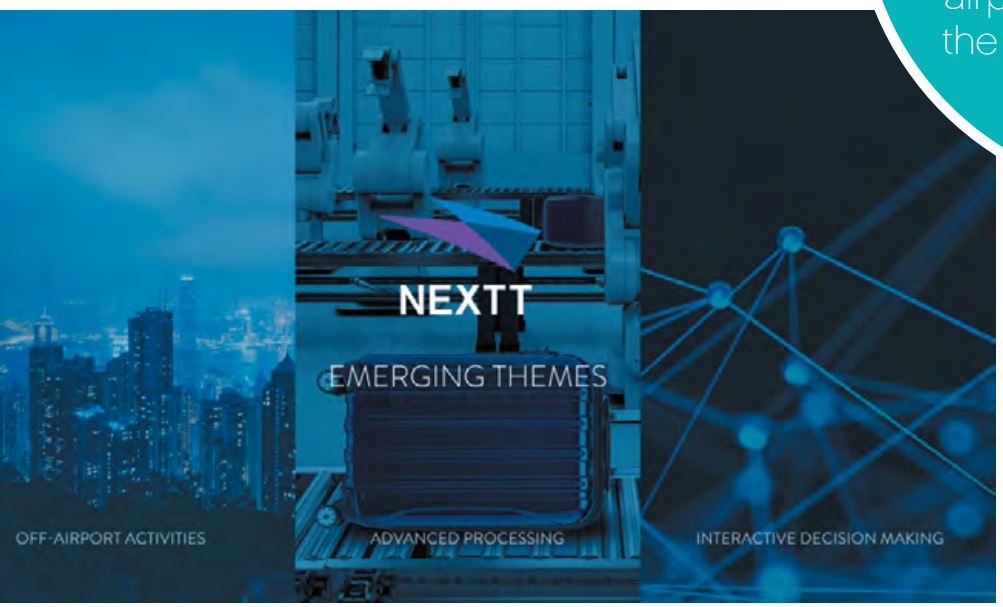
Many elements of facilitation are critical for the future growth of the industry. For airports, security, efficiency, and customer experience are the three key components that need to be addressed in order to drive change. Digital transformation can play an important role in ensuring that all three elements continue to grow while remaining balanced.

The rapid emergence of new technologies can lead to a new way of looking at airport capacity and security challenges. Digital transformation is not only about technology but also about business transformation in a digital world. It is both the implementation of new technologies as well as the integration of existing technologies, processes and services to deliver a better experience to all stakeholders.

Availability of real-time data and the digital transformation of processes and operations will enable airports to tackle capacity challenges, help maintain security while increasing operational efficiency and passenger satisfaction.

However, digitalisation and the use of data introduces an additional security risk, especially concerning cyber security. This will be a key consideration as more processes are digitised, internet of things technologies are deployed and systems are linked. ACI is working with the International Civil Aviation Organization (ICAO) on an action plan for

“ The NEXTT programme looks at the transformation of the complete ground journey for all the elements that currently move through the airport – the passenger, the baggage cargo and the aircraft. ”



aviation cyber security, as well as providing guidance to airports in best practices, training and a tool to help airports assess their cyber security readiness.

TRANSFORMING THE JOURNEY

New Experience Travel Technologies (NEXTT), a joint ACI and IATA initiative, examines the elements that will likely transform the complete end-to-end journey over the next 20 years. The NEXTT programme looks at the transformation of the complete ground journey for all the elements that currently move through the airport – the passenger, the baggage cargo and the aircraft.

It considers how advanced processing technology such as tracking and identification, robotics and automation, can improve safety, security and the customer experience. It also looks at how data can be better used through predictive modelling and artificial intelligence for real time decision making and improved efficiency.

Each of these concepts is considered for cargo, baggage, passengers and aircraft operations.

For baggage, the aim is for convenient and hassle-free luggage handling and tracking with a greater choice of service and offerings. For passengers, it’s about creating a seamless, secure and efficient walking pace journey that is highly personalised throughout. Meanwhile, for cargo, we’re considering more efficient operations and modern technologies to support easier, faster and smarter movement of cargo. And for ground operations, we’re exploring new processes and technologies for aircraft turnaround, including the delivery of services and supplies to the aircraft, apron and taxiway management.

PROMOTING AIRPORT EXCELLENCE

Through programmes such as NEXTT and Smart Security, ACI is helping shape the future of transport and of aviation security. Having a clear vision helps airports advocate with a single voice for regulatory changes, for instance with ICAO, which sets the global Standards and Recommended Practices for security and facilitation.

ACI also provides direct assistance to its member airports, helping them build and maintain strong security and facilitation. The APEX in Security programme, in particular, delivers extensive peer reviews of airports by other airports and provides a unique opportunity for onsite collaboration, exchange of information and improvement.

ACI’s Global Training, the world’s leading provider of airport management and operations education, offers executive leadership, professional accreditation, subject-matter competency and personalised in-house training courses as well as a wide range of web-based coursework, including the management of airport security, cyber security and Smart Security.

Finally, ACI helps its members by producing handbooks and best practices on issues which matter to them. In the realm of Security, ACI has recently released handbooks on landside security, cyber security, autonomous vehicles and addressing insider threats. Due to be issued imminently is a new handbook that covers the whole spectrum of airport security to help airports manage security effectively.

This article was contributed by ACI World’s Nina Brooks, Director of Security, Facilitation and IT; and Nathalie Herbelles, Head of Security and Facilitation.

Aviation Safety and Security Events Calendar

FAA-EASA International Aviation Safety Conference
- 23 – 25 June 2020
- Washington DC, USA
- A joint venture between the Federal Aviation Administration and the European Safety Aviation Agency which aims to advance aviation safety through global leadership, shared commitment, and harmonized safety standards, policy and procedures.

ICAO Global Aviation Security Symposium
- 1 – 3 September 2020
- Montréal, Canada
- Comprises an interactive exhibition, a series of aviation security-related workshops, and panel discussions on current security issues and initiatives.

ACI Public Safety and Security Fall Conference
- 5 – 8 October 2020
- Washington DC, USA
- Continues the conversation on the latest safety and security developments affecting US and Canadian airports.

Airport IT & Security Conference
- 19 – 21 October 2020
- Munich, Germany
- The premier gathering for airport IT and security professionals bringing together 400 senior-level decision makers from 100 global airports.

Aviation Cyber Security Summit
- 2 – 3 November 2020
- London, UK
- Addresses key cyber security issues including how best to respond to evolving cyber threats and the importance of effective risk management throughout the aviation supply chain.

International Aviation Safety & Security Conference
- 25 – 26 November 2020
- Prague, Czech Republic
- Connects professionals from airports, airlines, government institutions and universities, giving them the opportunity to discuss new technologies, possible threats and share best practices.

ACI Airport Exchange - Airport Security Summit Conference
- 1 – 3 December 2020
- Amsterdam, Netherlands
- Brings together senior airport security experts, agencies and senior administrators to address important security issues facing the aviation industry.

Multifocal sensor technology

PANOMERA®

Increased Security. Faster Processes. With Fewer Cameras.

Applications for:

- **Runway, Apron, Taxiway**
- **Security Area, Check-in, Parking**

Dallmeier

Learn more:
dallmeier.com/solutions/airport

MADE IN GERMANY

Rapiscan systems
An OSI Systems Company

TOTAL SECURITY TRAINING

Our fully accredited and specialised training department have various training programs across different areas such as Threat Recognition Training, Aviation Security educational programs, Dangerous Goods training - and courses tailored to support Ground Handling operations in Airports.

We offer numerous security related training and education certifications, to provide companies and students with current and relevant security information on international legislation - a strategic approach to address today's security challenges.

INTERESTED?

email us at:
securitytraining@rapiscansystems.com

RAPISCAN LEARNING ACADEMY

One Company, Total Security.