Risk Assessment for Coventry Airport, UK

Author: Leen El Mir

Date: 8-12-2024

Contents

1. Introduction

This risk assessment evaluates the cybersecurity of Coventry Airport, located in the UK. The airport has operated for over 12 years and is among the largest UK airports. Coventry Airport accommodates international and domestic flights on its five terminals. The airport relies heavily on Industrial Internet of Things (IIoT) Devices, Smart Transportation and Smart Infrastructure Technologies.

The purpose of the assessment is to audit the airport's security. The report considers and suggests suitable Risk Management Standards and Frameworks to accommodate for the airport's use of IIoT devices. The assessment contains a risk analysis of the IIoT devices. It also suggests risk mitigation strategies and makes key recommendations to safeguard the airport from cyber threats and vulnerabilities.

2. Risk Management Standards and Frameworks

2.1 IEC 62443

2.1.1 Overview

IEC 62443 is an international standard developed to secure industrial automation and control systems (IACS) (IEC, 2021). IACSs include IIoT devices such as lighting and baggage systems, all of which are critical in airports.

The standard is divided into four parts (IEC, 2021).

i. **IEC 62443-1** defines terminologies, concepts and models relevant to the security of IACSs.
ii. **IEC 62443-2** discusses processes for managing IACS security, including creating a robust security program, implementing patch management, and defining security requirements for service providers involved in IACS operations.
iii. **IEC 62443-3** defines system security requirements and assigns security levels to protect critical airport processes, such as air traffic control, based on risk severity.
iv. **IEC 62443-4** focuses on the security of individual hardware and software. This ensures that IIoT devices are secure by design and throughout their lifecycle.

2.1.2 Suitability

IEC 62443 is well-suited for airport operations, especially because of its focus on securing industrial control systems that are critical in the functioning of IIOT devices, such as surveillance systems. The standard provides detailed security guidelines for network architecture as well as operational technology (OT), thus offering effective responses to essential concerns of supply chain security, data integrity, and system availability. IEC 62443 is based on defence in depth; it offers a layered security approach against a wide range of threats. The holistic strategy involves not just technological safeguards but also emphasizes training and competence building of staff operating IACSs. This integration of technical strategy with human-centred approach makes IEC 62443 versatile and a robust framework for making the IIoT systems in airports resilient, which in turn makes them safer and more efficient.

2.1.3 Limitations

Although IEC 62443 is highly relevant, the standard has some notable disadvantages. The implementation of the standard is resource-intensive; it requires a lot of time, expertise and financial investment (Gordon, 2021). Effective execution requires seamless coordination between upgrading technology and human resource development, which, in turn, can easily become a significant challenge to smaller airports or those not having a robust cybersecurity strategy. The implementation of this standard also requires making significant changes to the existing processes in place, which could disrupt operations. On its own, IEC 62443 cannot cater to the needs of an airport environment. It is a generalized standard which does not comprehensively address the unique security requirements of an airport.

2.2 NIST SP 800-53

2.2.1 Overview

NIST SP 800-53, published by the National Institute of Standards and Technology (NIST), is a foundational framework for managing and securing federal information systems (National Institute of Standards and Technology, 2020). It aims to protect sensitive and critical infrastructure by establishing security controls against a diversity of threats. It applies to both physical and cybersecurity domains.

NIST SP 800-53 divides controls into families. Such families include Audit and Accountability, Incident Response and Access Control, with each addressing a specific security/privacy requirement. The framework discusses control baselines for different impact levels (low, medium, or high); this helps organizations select controls based on what risk levels they find appropriate. The framework also details how to tailor controls to meet an organization’s needs, such as adding or modifying controls. It includes privacy controls which address the protection of personally identifiable information (PII) and compliance with privacy laws. Also, the framework’s continuous monitoring ensures that security measures remain effective as time passes.

2.2.2 Suitability

NIST SP 800-53 is highly suitable for airport operations, especially when considering deploying IIOT devices. The framework's security controls protect the devices from cyber vulnerabilities and ensure their integrity. The framework also discusses OT systems' security, which is crucial for maintaining airport infrastructure and business continuity. The flexible security measures it offers allow airport authorities to tailor controls based on the risk profiles they create with their own judgement. Another notable factor is the framework's emphasis on continuous monitoring. This enables airports to protect critical infrastructure against dynamic threats.

2.2.3 Limitations

NIST SP 800-53 is generally applicable in the context of an airport environment. However, it possesses some limitations. The primary issue is that the framework was originally designed with federal information systems in mind. This implies it does not fully address the operational and regulatory issues specific to airports. Another issue is that like IEC 62443, the framework is complex and can be challenging for airports with limited cybersecurity resources and expertise. Additionally, the framework's vast array of controls may be overwhelming for smaller airports that have limited resources. The framework is also limited to information security, so it does not fully address the specific vulnerabilities of operational technology, or the unique risks that originate from IIoT devices.

2.3 CAA CAP 1850

2.3.1 Overview

CAP 1850, or the Cyber Assessment Framework (CAF) for Aviation, aims to assess the cybersecurity of IIoTs in aviation environments. Developed by the Civil Aviation Authority (CAA) for aviation in the UK, it ensures compliance with the UK's Network and Information Systems Regulations (NIS) (CAA, 2019).

The key aspects of CAP 1850 include indicators of Good Practice (IGPs) which assess the cybersecurity of an aviation setting (CAA, 2019). For example, IGPs could assess access control and incident response. It focuses on addressing vulnerabilities to IIoT devices and operational technologies. CAP 1850 relies on 14 principles, split into 39 Contributing Outcomes. It is designed whereby each Contributing Outcome is ranked to indicate the airport's level of 'cyber hygiene'.

2.3.2 Suitability

CAP 1850 is suitable for applications in an airport setting primarily because it addresses how to manage cybersecurity risks in aviation systems, specifically IIoTs. Although it does not comprehensively discuss all IIoT-related risks, the guideline aligns with NIS Regulations and the CAF. It is designed with aviation stakeholders in mind, so it can be more easily implemented than more comprehensive but technical guidelines. Another factor that makes it easily implemented is that it is designed to be flexible and scalable to each organization's needs. The framework also stresses organizations remaining up to date on cybersecurity threats, which can help mitigate IIoT threats.

2.3.3 Limitations

While CAP 1850 is a useful guideline, it is not exhaustive enough to manage the cyber risks of an airport. Since it is only a guideline, it cannot be used as an indicator of compliance on its own. Additionally, CAP1850 focuses primarily on compliance with frameworks and regulations, such as NIST, rather than addressing IIoT threats in depth. Hence, the guideline lacks the technical depths of other frameworks when discussing threats to IIoT systems.

2.4 ISO/IEC 27001

2.4.1 Overview

ISO/IEC 27001, published by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), is an international standard for managing information security. The standard explains how to implement, maintain, and improve an organization's management system for information security (bsi., n.d.). It focuses on identifying and measuring cyber risk levels associated with confidentiality, integrity, and information availability.

2.4.2 Suitability

ISO 27001 outlines an information security management system (ISMS), whereby it details procedures for managing and operating an organization's security. The standard especially addresses critical infrastructure organizations, such as airports. It is useful for integrating broader risk management and complementing controls on an organizational level. The standard is applicable to all the airport's assets, which includes its usage of IIoT devices (Ewon, 2024). It addresses IIoT devices within the larger framework of IT and physical security rather than regarding IIoT devices on their own.

2.4.3 Limitations

The main limitation of ISO 27001 is that it does not specifically address IIoT controls. Its focus is more angled towards governance and standardizing the procedures, so it does not address the technical issues of IIoT devices. It does not address the unique features of IIoT systems or how they interact with operational technology or industrial control systems in airports. This is a significant limitation because IIoT devices are usually embedded in either of the aforementioned systems.

2.5 Recommended Security Framework(s) and Standard(s)

This risk assessment proposes Coventry airport implements both IEC 62443 and CAP 1850. Given that the airport is large with five terminals, the airport can implement IEC 62443 to address all the large infrastructure used. IEC 62443 would cover securing the large assets such as the industrial control systems and operational technology. It is advantageous because it specifically focuses on IIoT system security. The standard also provides technical details on how to secure the systems and their communications.

The integration of CAA CAP 1850 ensures the airport meets aviation-specific security standards in the UK, which are instigated by the UK CAA. CAP 1850 would ensure the airport properly protects the IT and OT systems that support airport security, air traffic control, and screening. It also ensures meeting security requirements for physical and cyber infrastructure in the airport. Its focus on risk assessments and continuous monitoring ensures the airport's security is constantly monitored in real-time.

By combining the two standards, the airport can achieve global compliance (using IEC 62443) and meet local regulatory compliance (using CAA CAP 1850).

2. Risk Analysis

2.1 Risk Register

Risk Id	Source	Vulnerability	Risk Description	Likelihood	Impact	Severity	Assets Affected	Mitigating Action
HK1	NIST, 2017b	The camera's application does not adequately authenticate users when logging in. [CVE_867❸_❸❺87]	Attackers can gain unauthorized access and access sensitive data such as camera feed.	Likely	Severe	High	Hikvision Surveillance Cameras (DS-2CD2xxx Series)	Regularly update the cameras' firmware. Use strong password on camera's application. Only use cameras when connected to secure networks.
HK2	NIST, 2023	When connected to a network, the cameras have an authentication bypass vulnerability in their Hik-Connect Module. [CVE_8689_0❹787]	Attackers can send specially crafted malicious messages over the network to access the system without credentials. This leads to unauthorized access and data breaches.	Possible	Significant	Medium High	Hikvision Surveillance Cameras (DS-2CD2xxx Series)	Limit use of the Hik-Connect Module and disable it when not in use. Enforce firewalls to limit malicious messaging. Download the security patch released by Hikvision.
HW1	NIST, 2017a	The system's web interface has weak validation mechanisms during authentication. [CVE_867❸_❶709]	Unauthenticated attackers could send special HTTP requests to the web server to bypass authentication. This allows them to gain administrative access and trigger a directory traversal attack.	Likely	Severe	High	Honeywell Building Management Systems (Honeywell XL Web II)	Regularly update to the latest version. Enforce network segmentation to limit access to the devices.
HW2	CISA, 2018	HMIWeb browser, used in Honeywell EBI R500, improperly handles certain inputs. This causes a stack-based buffer overflow in the ActiveX control. The system is prone to code execution if users	Exploiters could remotely execute arbitrary code on the system when a user access a malicious HTML document. If successful, this could lead to a partial loss of availability, integrity, and confidentiality of the system.	Possible	Significant	Medium High	Honeywell Building Management Systems (Honeywell EBI R500)	Enforce the updated patches on HMIWeb. Educate employees on malicious document detection. Implement web content filtering to enforce security.

		access a malicious HTML document. [ICSA_79_6❶9_68A]						
TA1	ICAO and THALES, 2018	Unsupervised devices operating TopSky or insufficient USB port security may expose the device to vulnerabilities.	Attackers may insert an infected USB into the Online ATC system. This could lead to malware execution and data distortion.	Unlikely	Significant	Medium	Thales Air Traffic Control Systems (TopSky ATC)	Disable USB ports on systems critical to running the ATC system. Conduct weekly malware scans. Enforce strict access control to allow only authorized personnel access to the devices.
TA2	ICAO and THALES, 2018	The system uses ADS-B radio signals to transmit information about an aircraft's position.	Attackers may spoof the radio signals. This could cause distortions in aircraft position information and lead to airplane collisions.	Possible	Significant	Medium High	Thales Air Traffic Control Systems (TopSky ATC – EuroCat-C)	Use anomaly detection systems in order to validate signals and detect unusual patterns. Implement rigorous encryption and authentication procedures.
TA3	ICAO and THALES, 2018	VPNs that are not configured correctly or Remote Desktop Protocols with weak authentication are possible entry points into the ATC's LAN.	Remote attackers could access the ATC's LAN. This allows attackers to delay information being relayed to traffic controllers or it can allow them to manipulate sensitive data.	Possible	Severe	Medium High	Thales Air Traffic Control Systems (TopSky ATC – Euro Cat-C)	Enforce firewalls to protect from attackers. Use updated intrusion detection systems. Heavily encrypt communications.
TA4	ICAO and THALES, 2018	Since EuroCat-C is an older version of TopSky, its authentication mechanisms are not as modernized.	Unauthorized attackers may exploit the outdated mechanisms to access critical sections of data.	Possible	Significant	Medium High	Thales Air Traffic Control Systems (EuroCat-C)	Implement multi-factor authentication to minimize the possibility of unauthorized access. Implement rigorous password policies to limit access to authorized personnel.

TA5	Murdock, 2016	IFEC systems connected to the airplane's Wi-Fi are potential entry points for hackers.	Attackers may use this entry point to control passengers' in-flight displays.	Possible	Significant	Medium High	Thales In-Flight Entertainment (IFE) System (TopSeries)	Keep the IFEC system software updated to ensure all the latest security patches are installed. Isolate the IFEC system from other critical network systems to minimize an attack's severity.
TA6	THALES, 2023	Poor segregation in the networks between IFEC and critical control systems in the aircraft.	Attackers may hack the networks gaps, compromising control system.	Possible	Severe	Medium High	Thales In-Flight Entertainment (IFE) System (TopSeries)	Implement firewalls between the critical control systems and the IFEC. Use strong encryption protocols for any data that is transmitted between the control systems and IFEC.
GA1	Mitre, 2021 NIST, 2021b	The detectors have stack-based buffer overflow vulnerabilities in UDP checksum handling. [CVE-2021-21901 and CVE-2021-21903]	Attackers could trigger this vulnerability of buffer overflows by sending special packets. These could cause remote code execution and remote detector control.	Likely	Severe	High	Garret PD 6500i metal detectors	Ensure firmware is regularly updated to the latest version. Implement an intrusion detection system to detect abnormal packets being sent. Analyse the detectors' logs occasionally to detect any unusual activity.
GA2	NIST, 2021c	The iC Module contains a directory traversal flaw that could potentially allow for file overwriting. The vulnerability is found in the CMA CLI 'setenv' command. [CVE-2021-21904]	Attackers can gain access to sensitive files. They could modify, delete, or overwrite these files. They could also execute random commands on the system.	Likely	Moderate	Medium	Garrett PD 6500i and Garret Multi-zone metal detectors	Regularly update the detectors' firmware. Implement least privileges principle to restrict access. Restrict network access to system.
GA3	CloudDefense, 2021a CloudDefense, 2021b	Two stack-based buffer overflow flaws are present on the system. They can be caused by uploading a malicious file on	Attackers can trigger the overflow in the CMA readfile of the iC Module. By doing so, they can execute arbitrary code on the system.	Possible	Significant	Medium High	Garrett PD 6500i and Garret Multi-zone metal detectors	Regularly update firmware to patch any vulnerabilities.

		the device and forcing it to call ‘readfile’. [CVE-2021-21905 and CVE-2021-21906]						Restrict the upload of files to authorized personnel. Use checksum verification or digital signatures to ensure file integrity.
GA4	NIST, 2021a	The CMA run_server in the iC Module is exposed to an authentication bypass. Remote attackers can cause a race condition during authentication. [CVE-2021-21902]	Remote attackers can exploit an authenticated user’s session by sending network requests during authentication. This can grant attackers access to the system, leading to data leakage or control of the device. Hijackers can also execute commands while posing as the hijacked user.	Possible	Severe	High	Garrett PD 6500i and Garret Multi-zone metal detectors	Enforce multi-factor authentication to minimize hijacking. Regularly monitor access logs for any suspicious behaviour. Set specified session timeouts for user sessions.
GR1	Security, 2020	Garmin G1000 uses flyGarmin to manage its database and receive information about its software updates.	FlyGarmin could become unavailable due to a ransomware attack on Garmin’s cloud services. This would cause a delay in Garmin G1000 receiving updates on software and database, halting a pilot’s access to navigation data.	Possible	Significant	Medium High	Garmin G1000 Integrated Flight Deck – flyGarmin service	Regularly perform backups of G1000’s databases to avoid constantly relying on real-time downloads from flyGarmin.
AX1	CVEdetails, 2018a Axis Communications, 2018	The firmware’s HTTP server mishandles the processing of some received requests. [CVE-2018-10660]	Attackers could send HTTP requests specially crafted to exploit the HTTP server’s vulnerability, allowing for shell command injection. This could lead to a Denial of Service (DoS) attack or to crashing the camera’s operations, making it non-responsive.	Possible	Significant	Medium High	Axis Communications Network Cameras (Axis Q6032-E) – (Axis M3005-V)	Routinely conduct vulnerability scans of the Axis cameras. Upgrade devices models to the latest firmware. Limit exposure of devices directly to the Internet (port-forwarding). Apply IP filtering to whitelist authorized clients.
AX2	CVEdetails, 2018b	The firmware has inadequate authentication mechanisms. [CVE-2018-10661]	Attackers could send specially crafted HTTP requests to bypass the login process. Attackers can	Possible	Significant	Medium High	Axis Communications Network Cameras (Axis Q6032-E) – (Axis M3005-V)	Deploy a web application firewall (WAF) for devices

	Axis Communications, 2018		then have complete remote access of the camera.					running vulnerable HTTP servers. Routinely conduct vulnerability scans of the Axis cameras. Limit exposure of devices directly to the Internet (port-forwarding). Apply IP filtering to whitelist authorized clients.
AX3	CVEdetails, 2018c Axis Communications, 2018 Kovacs, 2018	The firmware's interface is misconfigured and mishandles some HTTP requests. [CVE-2018-10662]	Attackers can send specially crafted HTTP requests, allowing them to execute root-privileged commands. Attackers could bypass authentication, cause a DDoS attack, and/or freeze the camera's video.	Possible	Significant	Medium High	Axis Communications Network Cameras (Axis Q6032-E) – (Axis M3005-V)	Routinely conduct vulnerability scans of the Axis cameras. Limit exposure of devices directly to the Internet (port-forwarding). Apply IP filtering to whitelist authorized clients.
AX4	Axis, 2017	The AXIS Q6032-E Network Camera reached its end-of-life and end-of-support on 28-02-2017; firmware updates and security patches for known bugs are no longer provided for this camera model.	The unsupported AXIS OS leaves the device susceptible to all known bugs and new vulnerabilities.	Possible	Moderate	Medium	Axis Communications Network Cameras (Axis Q6032-E)	Replace the Axis Cameras Q6032-E with the newer and supported model, AXIS Q6074-E.
ZX1		ZXP card printers are at risk of being physically tampered with when not stored in secure, restricted-access areas.	Unauthorized personnel could print fraudulent cards, modify the printer's internal settings or steal sensitive data from previously conducted print jobs.	Possible	Significant	Medium High	Zebra ZXP Series 9 Card Printers	Install alarms and physical locks to limit access to the printing room. Regularly audit printing logs to detect any suspicious behaviour.
FR1	VOIP Networks, 2017	Attackers could phreak the Voice over Internet Protocol (VoIP) services provided by the VCS. This can be due to outdated protocols or weak communication encryption in	Remote attackers could gain access to sensitive call data.	Possible	Significant	Medium High	Frequentis VCS (Voice Communication System) 3020X	Ensure end-to-end encryption using TLS. Install an intrusion prevention system (IPS) and a VoIP firewall.

		the VoIP services of the Frequentis VCS 3020X.						
FR2	VOIP Networks, 2017	Insufficient bandwidth management could allow attackers to overload the VoIP network of the VCS by consuming all the available bandwidth. This constitutes a Denial of Service (DoS) attack.	Attackers could trigger the DoS attack by spamming redundant SIP call-signalling messages. Communications between air traffic towers and pilots would be limited or even halted.	Possible	Significant	Medium High	Frequentis VCS 3020X	Implement SIP firewalls. Ensure the bandwidth reserves can adequately handle message spamming. Ensure load balancing by distributing network traffic to prevent a single point of failure.
TH7	THALES, 2021	The TopSeries Avant offers an e-commerce feature on its display screens. Passengers input their banking details to make purchases on the device.	Insufficient encryption may allow attackers to intercept or access these details. This could lead to data leaks, financial fraud.	Possible	Significant	Medium High	Thales IFE System TopSeries Avant - Passenger data (personal information, credit card data) - IFE database	Enforce network segmentation in order to isolate the IFE system from other operational systems. Ensure the device's stored data is encrypted with AES-256.
TH8	THALES, 2021	The Avant system offers a mobile phone-based touchless control feature; it allows passengers to control the IFE system using their mobile phones. Authentication mechanisms are used to pair the devices.	Attackers could exploit weak authentication mechanisms of the feature. They could gain unauthorized access to the system whereby they inject malicious commands or access passengers' sensitive data.	Possible	Significant	Medium High	Thales IFE System TopSeries Avant - Passenger devices - Network infrastructure	Monitor the network traffic by deploying an intrusion detection system. Establish session limits and log out users to prevent persistent access.

Table 1. Risk Register of Key Technical Risks at Coventry Airport.

2.2 Critical Risks

The most critical risks are summarized in this section. They were selected based on the CVSS v3 severity metric (NIST, 2022). Specifically, the selection was based on the highest impact scores, previously documented cases, and analogous impacts on similar devices.

2.2.1 Garret PD 6500i/MZ Metal Detectors (CVE-2021-21902)

This vulnerability leads to the authentication bypass of Garret PD 6500i and Multi-zone metal detectors. The vulnerability exists in the CMA run_server_6877 function of the devices, which handles the authentication requests (aqua vulnerability database, 2021). Attackers can connect to the network at properly timed instances to hijack a user's active session, bypassing authentication.

According to the CVSS score, this vulnerability is critical because it can be exploited remotely over a network, increasing the likelihood of attacks occurring (aqua vulnerability database, 2021). The attack is complex, since it relies on triggering a race condition to hijack the session. However, it requires no special privileges or user interactions, making the vulnerability easily exploitable.

The severity of this risk is high since the confidentiality, integrity, and availability of data are highly compromised (aqua vulnerability database, 2021). Attackers would have complete access of user's credentials, sensitive information and possibly personal data of travellers. With this attack, the attackers could also manipulate the metal detector's settings, allowing items that would normally be prohibited to pass the detector. Attackers may also render the device inoperable or unavailable for usage.

2.2.2 Hikvision DS-2D2xxx Series Surveillance Cameras (CVE-2017-7921)

This risk describes an improper authentication issue in the Hikvision DS-2D2xxx Series Surveillance Cameras. The camera's application inadequately authenticates users, allowing attackers to escalate their privileges and gain privileged access to sensitive information.

According to the CVSS metric, the vulnerability can be remotely exploited (NIST, 2017b). It is categorized as having low attack complexity, indicating it requires no special conditions or skills. It also requires no special privileges or user interactions, making the attack easily conducted.

The impact of this risk is critical (NIST, 2017b). Attackers could manipulate such an attack to exploit devices besides the airport's cameras. It also results in a total loss of confidentiality, integrity and availability of data. This implies that attackers could access sensitive video feeds, modify recorded data, or even render the cameras inoperable.

2.2.3 Axis Q6032-E – Axis M3005-V (CVE-2018-10660)

This vulnerability is present in the Axis IP cameras, Axis Q6032-E and M3005-V. It allows attackers to bypass authorization and conduct shell command injections. The specifics of this vulnerability are explained in Section 2.3.3.

The severity of this risk is critical, with a CVSS score of C:H, I:H, and A:H (NIST, 2018). This indicates strong impacts on confidentiality, integrity, and availability of data. For example, it could lead to illegal access to private surveillance footage. It could also result in severe data breaches that expose vital information about passenger movements and airport operations. Even less experienced attackers could take advantage of this vulnerability due to its low attack complexity (AC:L) and lack of requisite privileges (PR:N). Additionally, there is a greater chance of operational disruption because hacked video systems may make it more difficult to monitor in real time.

2.3 Critical Vulnerabilities

This section summarizes the key vulnerabilities critical to the airport's operations. They were selected based on the CVSS v3 severity metric (NIST, 2022). Specifically, the selection was based on the highest exploitability scores, previously documented cases, and analogous vulnerabilities of similar devices.

2.3.1 Hikvision DS-2CD2xxx Cameras (CVE-2023-48121)

This vulnerability exists in the Hik-Connect Module of the Hikvision Surveillance Cameras (Model: DS-2CD2xxx Series). The Hik-Connect Module is the application designed to monitor the camera's video stream. The vulnerability is due to the application inadequately validating a user's credentials when they log on. Precisely, the vulnerability is in an SDK developed by EZVIZ, integrated into the Hik-Connect module to facilitate cloud-related services (use IP, 2023). Remote attacks can access the system by sending specially crafted messages to the impacted devices.

The CVSS score indicates this vulnerability is critical because it can be easily exploited. Its attack complexity is low, indicating the attack requires no special circumstances or advanced software to be executed (HIKVISION, 2023). The attack can be exploited remotely over a network, making it accessible to attackers from any location and increasing the likelihood of attacks. It also requires no user privileges or interactions, indicating that any non-user can easily carry out this attack.

A successful attack would notably compromise the confidentiality of user data; this may lead to sensitive data leakage (HIKVISION, 2023). However, the data's integrity will not be severely impacted; while some data may be modified, the data will largely remain intact. This implies that attackers may modify some footage or metadata, but the surveillance data will remain generally intact. Additionally, the attack would not impact the availability of the system's operations.

2.3.2 Honeywell XL Web II (CVE-2017-5143)

This vulnerability describes an authentication bypass in the Honeywell XL Web II device. Specifically, the vulnerability lies in the system's web interface that weakly validates user credentials.

This vulnerability is critical because it can be exploited remotely, which allows attackers to exploit the device from anywhere within the network (NIST, 2017a). Also, the attack can be executed easily since it is categorized with low attack complexity, so individuals with low technical skills can also execute this attack. It requires no user privileges or interactions, making it more accessible to individuals.

In an airport, such an attack could grant attackers access to sensitive information such as airport operational data or user credentials. It would also allow attackers to control operations such as lighting, heating, ventilation, and air conditioning, all of which the building management system controls.

2.3.3 Axis Q6032-E – M3005-V (CVE-2018-10660)

This vulnerability exists in multiple Axis IP Cameras, including the models Axis Q6032-E and M3005-V. It is a remote code execution flaw (RCE), whereby attackers can execute random commands on the camera. The attack occurs by sending specially crafted HTTP requests to the camera's web system; this allows attackers to bypass authorization and execute shell command injections.

This vulnerability is noteworthy because its exploitability score is high (score: 3.9) (NIST, 2018). The attack can be conducted remotely over the network. It also requires no specialized conditions or skills, so individuals with low technical skills can execute it. With no user privileges or interactions required, this attack is likely to occur.

As previously detailed, the impacts of this attack can be detrimental to the confidentiality, integrity and availability of data. Therefore, the implementation of the outlined mitigation strategies is critical (Table 1).

3. Recommendations

3.1 General Recommendations

Recommen-dation Id	Recommendation Description	Affected Assets	Recommendation Impact	Source
RC1	Periodically run security training for both staff and administrators to increase their awareness of the risks associated with IIoT devices and the importance of following security best practices.	Awareness of Employees – Possibility of insider threats	Ensuring all employees are well-educated on potential cyber-risks decreases the probability of successful attacks and insider threats.	ISO 27001:2022 Annex A Control 6.3 (hicomply, 2022)
RC2	Regularly perform security audits on all IIoT devices, tracking the access and configuration changes. Implement an intrusion detection system to facilitate the auditing process.	Detection and/or prevention of potential attacks on IIoT devices	Auditing will allow the real-time and prompt response to malicious activity.	IoT Security Foundation (IoT Security Foundation, 2021)
RC3	Develop and implement a comprehensive incident response plan to attacks targeting IIoT devices and systems.	Response to Security breaches	This reduces or prevents the impact of security breaches by ensuring that threats are promptly and systematically managed.	NIST SP 800-61 (Cichonski et al., 2012)
RC4	Regularly update the software, including the latest security patches, of all IIoT devices and systems used.	Exploitation of Known Vulnerabilities and/or outdated software	This mitigates the possibility of known vulnerabilities being exploited.	NIST SP 800-61 (Cichonski et al., 2012)
RC5	Enforce physical security measures to secure locations storing IIoT devices. Examples include installing alarms, physical locks and security guards at high-risk locations.	Physical Security of IIoT Devices	This protects IIoT devices from hijacking and/or unauthorized access.	IoT Security Foundation (IoT Security Foundation, 2021)
RC6	Apply device authentication protocols to ensure only authorized IIoT devices connect to the airport's network. Use secure boot processes, digital certificates, cryptographic keys, integrity checking, and strong authentication protocols.	Unauthorized Device Access	This reduces the risk of unauthorized devices connecting to the network and being used as entry points for cyberattack.	IoT Security Foundation (IoT Security Foundation, 2021)

Table 2. Recommended Mitigation Strategies for Coventry Airport.

3.2 Key Recommendations

3.2.1 RC1 – Train Employees

It is recommended that employees and administrators are periodically exposed to comprehensive training tailored to the specific risks of IIoT devices in airport environments. Specifically, the training can focus on devices' vulnerabilities, operations, and how they could be exploited by attackers. The practice could also discuss how to safely use a device and how an employee can securely manage their credentials. To mitigate insider threats, training should also educate employees on how to detect and report suspicious activity. Employees can be regularly tested to ensure the information they learned during training is retained.

RC1, outlined in Table 2, is significant because it mitigates the likelihood of human-caused errors or insider threats. Training employees well on what to detect can help them detect issues more promptly, decreasing the impact of these risks and addressing them firsthand. The training program will also ensure employees are compliant with industry standards such as General Data Protection Regulation (GDPR) and ISO/IEC 27001. This ensures the airport is safeguarding the employed IIoT devices and adhering to legal industrial requirements.

3.2.2 RC2 – Continuous Monitoring and Intrusion Detection

Regular auditing of all IIoT devices in Coventry airport is another suggestion. This guarantees that they are operating lawfully and in accordance with industry security regulations. Every device needs to undergo a thorough inspection, which includes evaluating its configurations and access controls. Automated technologies could help spot suspect activity on the devices, which need to be monitored continuously. An intrusion detection system (IDS) can be implemented into the airport environment to supplement the auditing. It could help manage the network traffic, check for vulnerabilities, and highlight login attempts that were brute-forced. For instance, the airport might track IIoT devices using a centralized logging system.

Since RC2 (table) improves airport security, its influence is substantial. In particular, the auditing technique may be useful in identifying long-term system vulnerabilities, such as the absence of security patches. However, the IDS has the ability to instantly identify and notify users of unusual activity. When combined, the two methods provide a layered security strategy, with auditing handling long-term, in-depth checks and IDS handling short-term, continuous monitoring to identify threats.

3.2.3 RC3 – Devise Incidence Response Plan

To address threats to IIoT devices effectively, Coventry Airport must devise and implement a strong and comprehensive incident response plan (IRP). This plan should include systematic procedures on how to identify, mitigate, resolve, and recover from a cyberthreat. To ensure the plan is effective, distinct roles and communication protocols would be assigned to teams of varying security clearances. For maximum capability, the IRP could draw inspiration from existing frameworks such as NIST Cybersecurity Framework or the IEC 27035 Information Security Incident Management standard. To ensure the plan is catered to the aviation environment, the Aviation Cybersecurity Framework (ACSF) can also inspire the IRP.

Having an extensive IRP can significantly impact the airport's risk management process (NetDiligence, 2024). It ensures that when threats occur, they are promptly and systematically handled, mitigating their impact. The IRP would not only protect critical IIoT systems but also minimize financial losses, such as paying for recovery plans and regulatory fines. The IRP would also ensure compliance with the industry's security regulations and ensure incidents are managed in an organized manner (subrosa, n.d.).

4. REFERENCES

aqua vulnerability database (2021). *CVE-2021-21902 | Vulnerability Database | Aqua Security*. [online] Aqua Vulnerability Database. Available at: https://avd.aquasec.com/nvd/2021/cve-2021-21902/ [Accessed 8 Dec. 2024].

Axis (2017). *AXIS Q6032-E PTZ Network Camera - Product support | Axis Communications*. [online] Axis.com. Available at: https://www.axis.com/products/axis-q6032-e/support.

Axis Communications (2018). *Security Advisory*. [online] Available at: https://www.axis.com/dam/public/c7/d1/31/security-advisory-acv-128401-en-US-111563.pdf.

bsi. (n.d.). *ISO/IEC 27001 Information Security Management System (ISMS) for the aerospace industry*. [online] *bsi*. Available at: https://www.bsigroup.com/globalassets/localfiles/en-gb/aerospace/resources/iso-iec-27001-for-aerospace-web-guide-en-gb-1219.pdf [Accessed 8 Dec. 2024].

CAA (2019). *Cyber Assessment Framework (CAF) for Aviation Guidance - CAP1850*. [online] *CAA*. Available at: https://www.caa.co.uk/publication/download/17540 [Accessed 8 Dec. 2024].

Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, [online] 2(2). doi:https://doi.org/10.6028/nist.sp.800-61r2.

CISA (2018). *Honeywell EBI, SymmetrE, and ComfortPoint Open Manager Station (Update A) | CISA*. [online] Cybersecurity and Infrastructure Security Agency CISA. Available at: https://www.cisa.gov/news-events/ics-advisories/icsa-13-053-02a [Accessed 8 Dec. 2024].

CloudDefense.AI (2021a). *CVE-2021-21905: Stack-Based Buffer Overflow in Garrett Metal Detectors iC Module CMA Version 5.0*. [online] Clouddefense.ai. Available at: https://www.clouddefense.ai/cve/2021/CVE-2021-21905 [Accessed 8 Dec. 2024].

CloudDefense.AI (2021b). *CVE-2021-21906: Garrett Metal Detectors Buffer Overflow Vulnerability*. [online] Clouddefense.ai. Available at: https://www.clouddefense.ai/cve/2021/CVE-2021-21906 [Accessed 8 Dec. 2024].

CVEdetails (2018a). *CVE-2018-10660 : An issue was discovered in multiple models of Axis IP Cameras. There is Shell Co*. [online] Cvedetails.com. Available at: https://www.cvedetails.com/cve/CVE-2018-10660/ [Accessed 8 Dec. 2024].

CVEdetails (2018b). *CVE-2018-10661 : An issue was discovered in multiple models of Axis IP Cameras. There is a bypass*. [online] Cvedetails.com. Available at: https://www.cvedetails.com/cve/CVE-2018-10661/ [Accessed 8 Dec. 2024].

CVEdetails (2018c). *CVE-2018-10662 : An issue was discovered in multiple models of Axis IP Cameras. There is an Expos*. [online] Cvedetails.com. Available at: https://www.cvedetails.com/cve/CVE-2018-10662/ [Accessed 8 Dec. 2024].

Ewon (2024). *ISO 27001: a benchmark standard for IIoT*. [online] Hms-networks.com. Available at: https://www.hms-networks.com/industrial-iot-blog/blogpost/hms-blog/2024/07/11/iso-27001-a-benchmark-standard-for-iiot [Accessed 8 Dec. 2024].

Gordon, J. (2021). *The Essential Guide to the IEC 62443 industrial cybersecurity standards*. [online] Industrial Cyber. Available at: https://industrialcyber.co/features/the-essential-guide-to-the-iec-62443-industrial-cybersecurity-standards/.

hicomply (2022). *ISO 27001 Annex A Control 6.3 Guide (2022)* | *Hicomply*. [online] Hicomply.com. Available at: https://www.hicomply.com/hub/iso-27001-annex-a-6-3-information-security-awareness-education-training [Accessed 8 Dec. 2024].

HIKVISION (2023). *Security Vulnerability in Some Hikvision Products*. [online] Hikvision. Available at: https://www.hikvision.com/hk/support/cybersecurity/security-advisory/security-vulnerability-in-some-hikvision-products/ [Accessed 8 Dec. 2024].

ICAO and THALES (2018). *Cyber-Security for Air Traffic Management ICAO*. [online] Available at: https://www.icao.int/NACC/Documents/Meetings/2018/CSEC/P05-CybersecurityPresentation-THALES.pdf.

IEC (2021). *Understanding IEC 62443*. [online] www.iec.ch. Available at: https://www.iec.ch/blog/understanding-iec-62443.

IoT Security Foundation (2021). *IoTSF IoT Security Assurance Framework Release 3.0 Nov 2021 IoTSF product security assurance IoT SF WG1 [Date]*. [online] Available at: https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf.

Kovacs, E. (2018). *Critical Flaws Expose 400 Axis Cameras to Remote Attacks*. [online] SecurityWeek. Available at: https://www.securityweek.com/critical-flaws-expose-400-axis-cameras-remote-attacks/ [Accessed 8 Dec. 2024].

Mitre (2021). *CVE - CVE-2021-21901*. [online] Mitre.org. Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21901 [Accessed 8 Dec. 2024].

Murdock, J. (2016). *Can hackers really hijack a plane using the in-flight entertainment system?* [online] International Business Times UK. Available at: https://www.ibtimes.co.uk/can-hackers-really-hijack-plane-using-flight-entertainment-system-1597418 [Accessed 8 Dec. 2024].

National Institute of Standards and Technology (2020). Security and Privacy Controls for Information Systems and Organizations. *Security and Privacy Controlsfor Information Systems and Organizations*, [online] 5(5). doi:https://doi.org/10.6028/nist.sp.800-53r5.

NetDiligence (2024). *Know the Benefits of an Incident Response Plan | NetDiligence*. [online] NetDiligence. Available at: https://netdiligence.com/blog/2024/10/incident-response-plan-for-cyber-attack/.

NIST (2017a). *NVD - CVE-2017-5143*. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln/detail/CVE-2017-5143.

NIST (2017b). *NVD - cve-2017-7921*. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln/detail/cve-2017-7921.

NIST (2018). *NVD - cve-2018-10660*. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln/detail/cve-2018-10660.

NIST (2021a). *NVD - CVE-2021-21902*. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-21902 [Accessed 8 Dec. 2024].

NIST (2021b). *NVD - CVE-2021-21903*. [online] nvd.nist.gov. Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-21903.

NIST (2021c). *NVD - CVE-2021-21904*. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-21904.

NIST (2022). *NVD - Vulnerability Metrics*. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln-metrics/cvss.

NIST (2023). *NVD - CVE-2023-48121*. [online] Nist.gov. Available at: https://nvd.nist.gov/vuln/detail/CVE-2023-48121.

Security, M. (2020). *An Overview of the 2020 Garmin Ransomware Attack*. [online] www.mitnicksecurity.com. Available at: https://www.mitnicksecurity.com/blog/2020-garmin-ransomware-attack.

subrosa (n.d.). *5 Benefits of an Incident Response Plan | SubRosa*. [online] www.subrosacyber.com. Available at: https://subrosacyber.com/en/blog/5-benefits-of-an-incident-response-plan.

THALES (2021). *Thales elevates the inflight entertainment experience with AVANT Up*. [online] Thales Group. Available at: https://www.thalesgroup.com/en/group/press_release/thales-elevates-inflight-entertainment-experience [Accessed 8 Dec. 2024].

THALES (2023). *Thales product security advisories*. [online] Thales Group. Available at: https://www.thalesgroup.com/en/global/group/psirt/thales-product-security-advisories [Accessed 8 Dec. 2024].

use IP (2023). *Please Read: - Hik-Connect Module Vulnerability Patch (CVE-2023-48121)*. [online] IP CCTV Forum for IP Video, network cameras & CCTV software. Available at: https://www.use-ip.co.uk/forum/threads/hik-connect-module-vulnerability-patch-cve-2023-48121.10677/.

VOIP Networks (2017). *The Top VoIP Security Risks and How You Can Protect Your Business*. [online] VOIP. Available at: https://voipnetworks.com/2017/08/20/voip-security-risks/.