

CREATING SMARTER, SECURE AIRPORTS: THE SHIFT TO INTEGRATED SECURITY



Table of Contents

Abstract	3
Introduction	3
Airport Security Challenges	4
The Need for an Integrated Airport Infrastructure	5
Key Elements of an Integrated Airport Security System	6
Concluding Thoughts	8
About the Author	9
About SIMS	9
Global Infrastructure Service	9
About Wipro IT Services	9

Abstract

While most airports have advanced security measures that entail multiple screening layers, body scanners and explosion detection tools, the actual physical security of the airport has been relegated to the back seat. With constantly evolving regulations and ever-growing incidents of sophisticated security attacks and escalating overheads, airports require advance planning along with the necessary physical infrastructure to drive actionable intelligence. This whitepaper from Wipro addresses the key security challenges that the modern airport faces today along with the need for an integrated IP based security infrastructure. It also walks through the key elements of an connected security system that will enable airports meet the increasing call for safe and efficient airport security.

Introduction

Airport security is a huge challenge with billions of passengers and baggage traversing through hundreds of airports and thousands of flights on a daily basis. According to the 2011 World Airport Traffic Report by ACI (Airport Council International), worldwide airport passenger numbers increased by 5.3% in 2011 to 5.44 billion and global passenger traffic is expected to top 12 billion by 2031.

The booming air travel industry and stringent regulatory requirements necessitates regular overhauls of airport runways and other infrastructure to keep up with current and future demand. Moreover, the continuously growing sophistication of threats are forcing airport to become highly vigilant and are dictating the need for smarter security solutions. These factors are driving investments to the tune of billions of dollars towards the development of identification and screening technologies such as radio frequency identification (RFID) technology, biometrics and prototype screening devices among others.

For instance, the Christmas Day bombing attempt of 2009 and the air cargo bombing attempt of 2010 have prompted the Department of Homeland Security to make critical investments to the tune of hundreds of million dollars in explosives detection systems, passenger screening technologies, and air cargo security for airports across the United States. In fact according to Global Industry Analysts, Inc., the worldwide airport security equipment market is expected to reach USD 288.7 billion by 2015. However, these investments are largely skewed towards internal screening measures while the actual physical security of the airport has been relegated to the back seat. The key question now is - **are airports doing enough to safeguard the actual physical airport infrastructure?**

The following sections discuss the various challenges associated with airport security and the need for an integrated physical security infrastructure for a truly effective security solution.

Airport Security Challenges

Airports pose a labyrinth of unique security challenges due to the sheer scale, volume and cost of infrastructure and people involved. Further, with restricted and sensitive areas within and around airport terminals, it is imperative for the authorities to constantly monitor and record all movements. However, there are significant challenges that span a gamut of factors such as:

Protecting airport infrastructure

Utilizing the right detection technologies and equipment for passenger, baggage and cargo screening

Ensuring secure passenger authentication and identification

Ensuring operational security with in-flight security as well as safe and efficient air traffic management

As discussed in the previous section, airports have largely focused their efforts on screening and detecting breaches inside the airport main premises. The harsh fact is that most airport grounds are

protected by a basic layer of a perimeter intrusion detection system along with obsolete barriers such as analogue cameras, high walls and barbed wire fences. Moreover, considering the fact that there are huge and complex networks of disparate technologies dotting the airport landscape, airports typically face a huge challenge of interoperability of these legacy systems. In many cases, these systems are supplied by different vendors and function in silos, thereby providing a fragmented security picture, leading to slow decision making and inefficiencies – both of which can have serious consequences with millions of lives at stake.

These challenges coupled with the pressure from new airline alliances, low cost operators, and the increasing incidences of airport privatization and acquisition are resulting in a far more competitive environment. Operational efficiency has never been as important as it is today with the focus on driving a more advantageous cost base without compromising growth, quality, safety and security across a wide range of issues and potential threats. This requires increased automation and integration of airport systems to enable a clear, consistent and timely view of the entire airport operation.

More than 1,300 perimeter security incursions have been reported at US airports since 9/11, yet 87% of the nation's airports have not been through a perimeter security assessment.

- US Rep. Bill Keating (MA-10)/GAO

The Need for an Integrated Airport Infrastructure

Let us consider a scenario where an alert related to a breach at a remote area away from the airport hub is triggered. The efforts of the airport authorities to track down this breach are typically stonewalled due to several reasons which make the process of finding the intruder much harder. Some of the key reasons are -

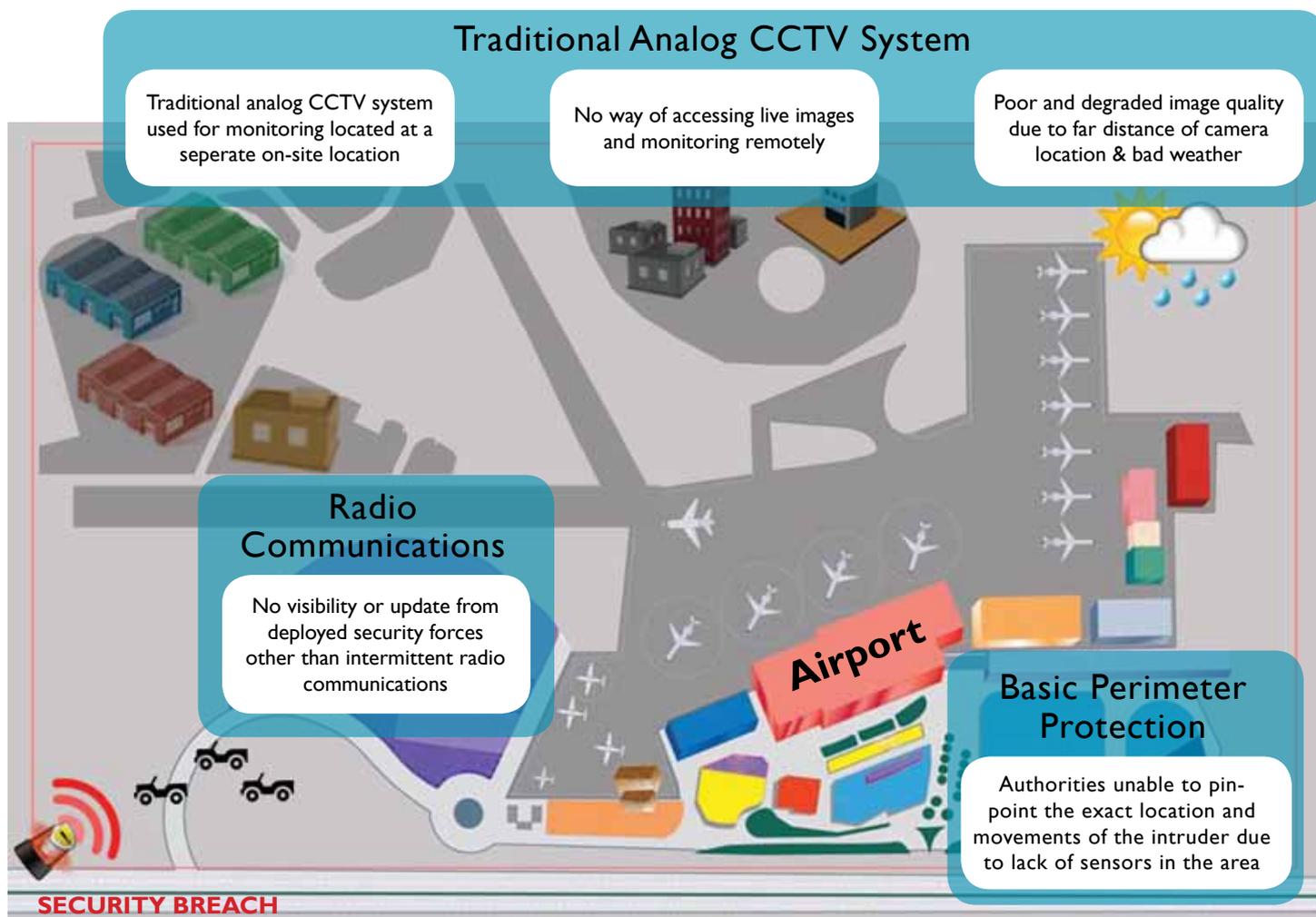


Figure 1: Assessing Security at the Airport Premise

Assume there has been a significant lapse of time between the breach alert and the ensuing response. *What if the team cannot find the intruder quickly? What if the intruder is a terrorist? Shouldn't there be a better way of triggering off the alarm earlier and enabling real-time tracking along with a coordinated effort with multiple teams for an effective security incident resolution?*

As the above example emphasizes - the traditional physical security protection tools are no longer enough to protect an airport even if its internal screening processes are highly advanced. A major airport in South Asia for instance spent billions of dollars on a new, modern terminal and to upgrade operations. As one of the largest

infrastructure investments in recent times, this airport boasts a swanky premise with cutting-edge facilities, high-speed metro link connectivity and is expected to handle 100 million passengers by 2030. Considering the sheer size and scope of this airport, it would almost be impossible to envisage the disastrous consequences and potential losses that a perimeter security breach could entail.

With attacks becoming more and more sophisticated, there is a strong need for an intelligent and integrated airport security infrastructure. Airport security solutions are typically a multilayered surveillance approach with a combination of 'smart' fences and sensors in conjunction

with IP CCTV cameras for intelligent surveillance, analytics and access control along with rapid response teams. However, each of these solutions if purchased separately can be a huge administrative burden on the airport's IT staff. These disparate systems will require its own set of dedicated services, maintenance and training. **By integrating these separate security systems under a single console, airport authorities can realize significant advantages of an considerably more powerful security solution at far lower costs.**

At the core of this system integration is a cohesive and unified control center that seamlessly assimilates information from multiple systems to provide a single point of view of all operations. With an integrated control center solution, airport authorities benefit from situational awareness and can quickly assess and proactively respond to an intrusion before it escalates to a serious security incident.

5 Key Benefits of an Integrated Security System

1. Reduced incident vulnerability and increased incidence responsiveness
2. Holistic approach to control by multiple uses of component devices
3. Ease of installation of multiple systems on a single interface
4. Flexibility and ability to easily integrate new security components
5. Operational and maintenance costs

Key Elements of an Integrated Airport Security System

A truly integrated airport security system typically encompasses three main elements – Monitoring, Tracking & Detection and Mobility solutions. These aspects are linked together by the fourth element - a Command and Control Center to mitigate risk across the airport environment by providing actionable intelligence and enabling speedy security incident resolution.



Figure 2: Integrated Airport Security System

Monitoring Solutions

Video Surveillance and Analytics

There has been a growing shift to IP based CCTV cameras that provide significant advantages such as scalability, remote monitoring over internet and easy sorting of digital video files. These IP-based solutions also support intelligent video analytics that augment the video surveillance systems with real-time detection and alerts for defined events.

Access Control

An airport environment requires a comprehensive solution ensuring security across multiple levels that can be seamlessly integrated with third party applications like fire, video, BMS and other such applications. These include usages of smart cards, biometric readers, visitor management systems and so on.

Tracking & Detection Systems

Taut Wires

Taut wires are embedded with electromechanical sensors and can be erected as stand-alone fencing, attached to conventional chain-link fencing, or mounted on existing walls, gates, roofing, etc. These sensor switches are sensitive and tamper proof and a major advantage of this system is that it does not require power supply.

Electro-optical bars

These are steel barriers with an integrated alarm system and serve as an intrusion detection grid in common passage ways like water pipes, windows, canals, etc. This grid is fully functional in a wide range of weather conditions and even functions smoothly when submerged under water for years. Any attempt to cut or remove a part of the grid, or the grid itself, is immediately detected by the opto-mechanical mechanism.

Buried cables

These cables consist of sensors (transmitter and receiver) and are buried inside the perimeter. An invisible EM detection field forms around the cable, which detects the presence of intruders within the field with an accuracy of + 1 meter.

Radar system with cameras

This system enables seamless monitoring and round-the-clock

observation of sensitive locations or observation of potential trouble spots. This high resolution radar can accurately detect personnel and vehicles up to 1400 meters in virtually any weather or lighting condition to provide 24/7 security.

Fire and Safety

Fire and safety tools are a key feature of airport security and offer a range of detectors from optical to multi-sensor detectors.

Mobility Solutions

Vehicle Mounted Camera

The vehicle is equipped with basic CCTV equipment, communication equipment, and video display systems along with seating capacity for operators. The Mobile Video Van is maintained in a complete state of readiness and is capable of capturing and streaming real-time video feeds of an incident.

Vehicle PC

This is installed in a vehicle to automatically provides alerts to patrolling teams in real time and allows the command and control room to know its exact location using secure communication lines and GPS.

Guards with PDAs

PDAs provide live videos and alerts from the control room to the field force using a built-in Wi-Fi communication card and Wi-Fi cloud.

GPS based Vehicle Tracking Solution

This solution enables airports to track the location of its assets – moving or stationary - in real time and respond to any requirement with precision.

Command and Control Center

This integrated solution enables an airport to increase situational awareness throughout its infrastructure by creating a unified and interactive intelligence picture, drawing data from all sensors, showing the location of the patrols and adding other relevant information such as video from different sources. This combined picture is constantly updated and can be sent by the Control Center to all patrols, thereby serving as a uniform basis for operational planning and allocation of tasks.

Concluding Thoughts

Airports worldwide are viewed as potential targets for terrorism and other forms of crime due to the sheer scale of infrastructure and the number of people concentrated in a particular location. It is a typical misconception in an average person's mind that the threat lies inside the terminal and the periphery where security officials must be ready for any eventuality. However, the security of facilities, infrastructure and strategic assets at airports and in the immediate vicinity is an integral part of a total airport security model and equally critical in ensuring the safety of millions of travelers.

Amid ever changing regulations and with new threats continuing to emerge, airports require advance planning along with the necessary infrastructure to drive actionable intelligence. In the light of these developments, there has been a marked shift towards IP based integrated and networked platforms. These platforms help airports reduce overall IT requirements and the need for training. It also empowers authorities with a single control console that allows them to perform their tasks far efficiently and thus foresee and protect their facilities from potential threats.

About the Author

Chockalingam Chidambaram

Chockalingam currently heads the IBMS and PSS practice of System Integration Services at GIS – Wipro Infotech. He has a comprehensive Sales and Marketing experience for over 2 decades across varied sectors in India, SAARC and Middle East.. He has been a known face in the Surveillance industry with working experience in Industry Majors like Bosch & Honeywell. He has been associated in quite a few landmark projects. As a part of his current role, he carries the charter of establishing and developing the IBMS & PSS practice for India, Middle East and Africa for Wipro Infotech.

About SIMS

Wipro's System Integration and Maintenance Services (SIMS) is a part of Global Infrastructure Services of Wipro. We provide end to end technology services including consulting, system integration and project management with a 3D model of Design, Deploy and Dedicate 24X7 Support. With our vendor neutral approach and best of breed technologies, We ensure all IT worries of the clients are left to us while they concentrate on their business goals.

Our certified processes and over 15 years of service experience are reflected in the success we have achieved in executing projects. Strategic alliances with leading technology players further enable us to deliver cost-effective integration services that are steady, scalable, smart, and innovative and result oriented for your business. Being a pure-play system Integrator, we deliver the best of breed solutions to customers with our vendor agnostic approach.

Global Infrastructure Services

Wipro's Global Infrastructure Services (GIS) is a pioneer in the Infrastructure Management services space with revenues of 2Bn USD. This division contributes to over 30% of IT revenues of Wipro Ltd, with a headcount of over 26,000+ technical specialists. Our strong domain capabilities and specialized offerings help businesses across the globe transform their vision to results. Backed by our strong network of iGCCs (Integrated Global Command Centers) and 10 owned datacenters spread across US, Europe and India, GIS is enabled to provide cost variabilization, accelerated growth and continuous innovation for global businesses. Few of our industry specific service offerings include Wireless Place, Shoptalk™, Bank-in-a-Box while our traditional offerings include data center management, cloud, managed network, managed security, end user computing and business advisory services

About Wipro IT Services

Wipro IT Services a part of Wipro Limited (NYSE:WIT) is a leading Information Technology, Consulting and Outsourcing company, that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of “Business through Technology” – helping clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, a practitioner's approach to delivering innovation and an organization wide commitment to sustainability, Wipro IT business has 135,000 employees and clients across 54 countries.

For more information, please visit or contact www.wipro.com us at info@wipro.com

Disclaimer: The material in this document is provided “as is” without warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. The material are subject to change without notice and do not represent a commitment on the part of Wipro. In no event shall Wipro be held liable for technical or editorial errors or omissions contained in the material, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the material. The materials may contain trademarks, services marks and logos that are the property of third parties. All other product or service names are the property of their respective owners.



DO BUSINESS BETTER

WWW.WIPRO.COM

NYSE:WIT | OVER 130,000 EMPLOYEES 54 COUNTRIES | CONSULTING | SYSTEM INTEGRATION | OUTSOURCING

WIPRO INFOTECH, DODDAKENNELI, SARJAPUR ROAD, BANGALORE - 560 035, INDIA TEL : +91 (80) 2844 0011, FAX : +91 (80) 2844 0256, email : reachus@wipro.com

©Copyright 2013. Wipro Limited. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without express written permission from Wipro Limited. Specifications subject to change without notice. All other trademarks mentioned herein are the property of their respective owners. Specifications subject to change without notice.