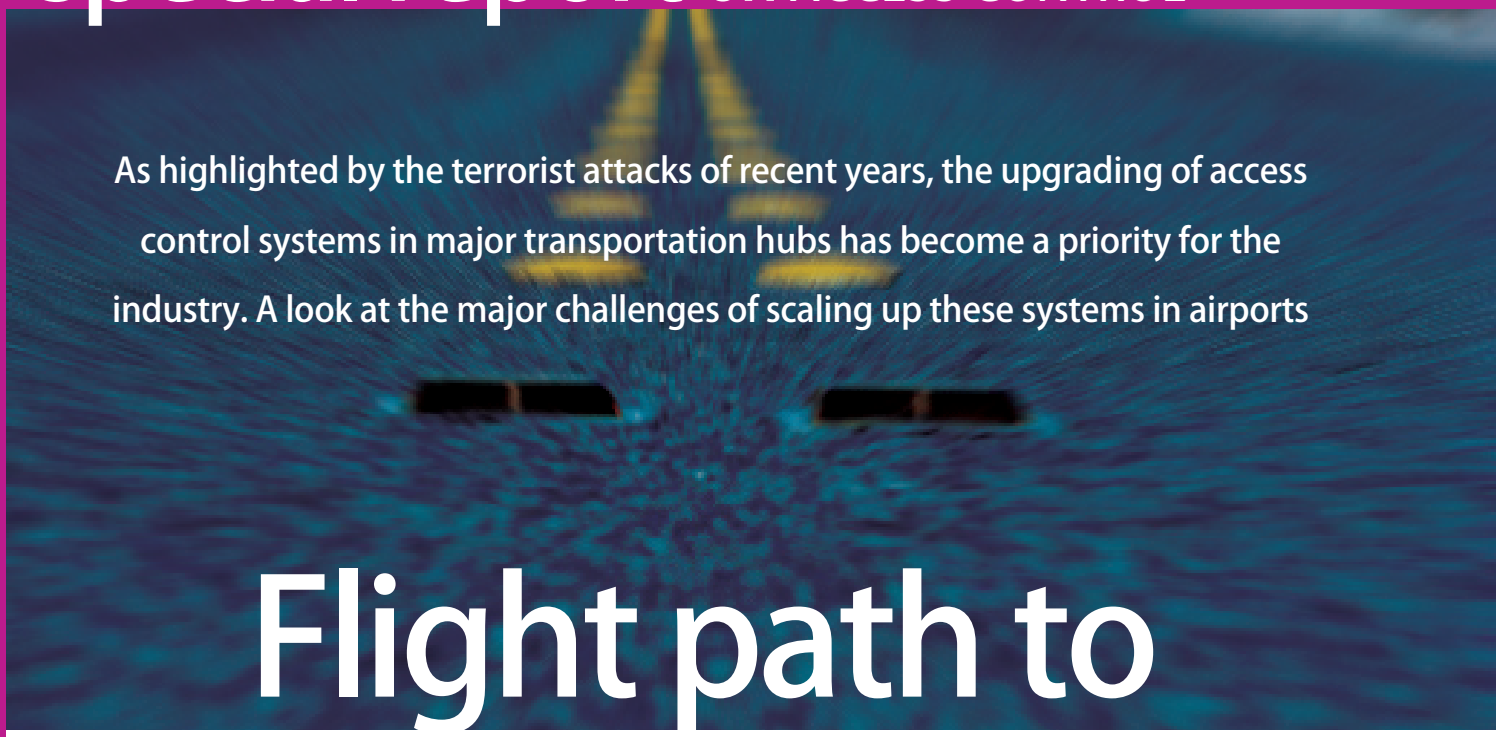


As highlighted by the terrorist attacks of recent years, the upgrading of access control systems in major transportation hubs has become a priority for the industry. A look at the major challenges of scaling up these systems in airports

Flight path to airtight security

by Ayman Ashour, Newton International Management

Transport security has been an important topic for many years. In the years since the terror attacks of September 11, 2001 airport security has received particular attention. The Madrid, London and Bombay events highlighted the vulnerability of transportation security beyond air. While airports and railway stations have not been the only targets of terror attacks, they have certainly been amongst the most widely publicized. Transport applications in general pose a unique set of challenges to the security industry.

Customer-employee ratio

Chief amongst these challenges is the very high ratio of customers to employees, the nature of the transient customer, and the rotating nature of transport employment. Office buildings, courthouses, hospitals and hotels may share some of these characteristics in terms of the ratio of customers, or the public, to employees. Yet it is rare to find as high a ratio as is the case within an airport or a railway station. Moreover, employees such as airline and train crews, retail outlet staff, emergency personnel and contractors move through airports unlike the staff of any office building.

Electronic Access Control Systems (EAC) have been deployed in many airports to facilitate the movement of employees. The figure overleaf shows multiple levels or zones of security for a typical airport. It is interesting to note that access points to the highest security areas are typically unmanned (e.g. going to the airside from baggage handling or gate areas). It is also interesting to see that most employees

use the same manned areas as passengers to gain access to the gate and shopping areas. The logic is that most employees, once screened alongside passengers, can use the electronic access control system to go where they are authorized to go, when they are allowed to.

Going beyond basic access control systems

Almost two full years prior to the terror attacks of 9/11 the US government's own audit of access control in several major airports (Audit of Airport Access Control, USA Federal Aviation Administration, Report No. AV-2000-017 of November 18, 1999) revealed serious problems. It was shocking to read comments such as "we successfully penetrated secure area on 117 (68%) of 173 attempts from the non-sterile and sterile areas of the Airport" and "...Once we penetrated secure areas we boarded aircraft operated by 35 different air carriers 117 times..." Further reading of this audit would suggest that the various systems simply failed to achieve their objective of controlling access.

Transport security applications require much more than fulfillment of basic access control functions

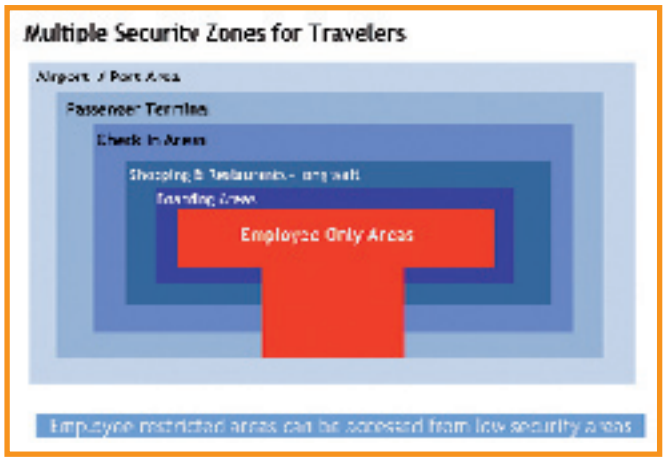
After well over two decades of experience with EAC, it is fair to conclude that the vast majority of systems available in the market do a more than adequate and reliable job of the basic access control functions; namely interfacing with the identification and/or authentication devices,

authorizing the unlocking of doors or gates based on programmed instructions, and reporting as well as archiving various events. Yet transport security applications, for the reasons discussed, above require a great deal more than mere fulfillment of the basic functions of access control.

Airport security zones: strangely, access points to the highest security areas are typically unmanned

Three main EAC challenges

Three primary challenges are imposed on most airports' EAC. The first is integration with CCTV video systems. It is crucial for EAC to function as a seamless and whole security system. As an example, video can generate alerts or even shutdowns in the case of "piggybacking", where a second person follows an authorized person through an access controlled door. Piggybacking was cited as an important reason for failures in the FAA audit report referenced above. Second, EAC is used as the primary security detections system, with the reliability of the alarm functions ensuring door and lock status critical. The integrity of data communication security on the various networks is clearly critical. It is surprising that many access control systems continue to fail to offer basic tamper resistance to door condition monitoring circuits and hardly any form of encryption. The third challenge is seamless integration between the EAC and the identity management systems. Given the high level of staff rotation, crew from different airports, retail & food outlets, contractors, janitorial, maintenance, emergency personnel and so on, a seamless interface is paramount between the EAC and the various identity management databases which confirm cardholder identity and, most importantly, the privileges that the cardholder is entitled to at that specific point of time at that location.



The importance of EAC standards

EAC systems have operated in a relatively standards-free world. While the integrity of wiring of fire alarm systems, for example, is subject to rigorous and detailed standards and approvals in most countries, there is no equivalent for access control. It is the buyer's responsibility to confirm the suitability of their chosen EAC for security applications. Similarly the CCTV interface can range from a truly seamless one that allows full operation of the entire security system from a single screen, to fairly simplistic and often ineffective interfaces. This has also been the case for integration between the EAC and identity management systems until recently. However, this is now changing and - so far mainly in the USA. US HSPD 12 (Homeland Security Presidential Directive12) and FIPS 201 (Federal Information Processing Standard 201) and a number of related working groups have initiated very detailed, indeed arguably overly detailed, standards for security of many aspects of identification systems, management of privileges and associated updates and interfaces to EAC. This is a significant step for any security system but of critical importance in the transportation industry where masses of employees and customers flow.