Open Architecture for Airport Security Systems

Problem:
• Aviation security has increased in complexity
• With many sources of information and new ways to handle and act on this data there is a need for a different approach to exploit this data and enable new solutions. However, today there are limitations on availability of near real-time data and available interfaces to create cross-vendor solutions

Solution:
• Open Architecture is a solution to prevent data lock-in, vendor lock-in and costly integration
• Open Architecture makes data available, enables interoperability

Results:
• Open Architecture provides more efficient and flexible means of adapting and responding to emerging threats and technological advances - an accelerated response
• Open Architecture provides improved operational, business and procurement efficiencies
• Open Architecture provides foundations for data and outputs to become more easily accessible
• Open Architecture provides all airport operators a framework around which they can build their security implementations
Initiated by Heathrow and Avinor late 2019, a joint industry group, managed by ACI, had by July 2020 published the first version of Open Architecture for Airport Security Systems.

Open Architecture definition endorsed by regulators and major airport operators across Europe, North America, Asia Pacific and the Middle East.

Co-signed by TSA Administrator, CEO Heathrow and Director General ACI EUROPE.

Open Architecture will mature as experience and knowledge develop.

Status of Open Architecture today

Our new Open Architecture agreement with international partners @ACI_Europe and @HeathrowAirport sets out broad guidelines for how airport security lane equipment will share data to better enhance our international security posture.

6:25 PM · Jul 30, 2020

See David P. Pekoske's other Tweets
Progress and achievements

We have worked hard to promote Open Architecture for Airport Security Systems and have presented at:

- ACI World’s 28th ACRIS meeting, International Airport Review’s Online Summit 2020, IATA’s Innovation in Security - Workstream #2
- Autonomous Security Systems Virtual Workshop

Heathrow is now the Chair of ACI EUROPE’s Open Architecture Working Group - currently 3 workstreams - standards and specifications will be written

The manufacturers are starting to see the value in Open Architecture and the benefits not just for their customers but for their businesses.

The ACRIS data model is being enhanced to support aspects of Open Architecture - collaborative work between HAL, Schiphol and Dubai.

Investigation into the applicability of OPSL, VTK and DICOS has been conducted.

Conversations with numerous 3rd parties across industry, academia and governmental have been started.
Supporting slides…
Open Architecture is an approach facilitating:

- Standardisation, interoperability and data sharing in order to cover existing and future airport requirements
- Adding, replacing and updating modules without unreasonable difficulties (commercial barriers, proprietary protocols etc)
- New solutions independent of vendor or location

Open Architecture will set standards in the following areas:

- **Security Equipment** - the devices or hardware
- **Algorithms** - enhanced detection for more than explosives
- **Data Sharing** - images, interfaces, communication and ownership
- **Equipment Control and Monitoring**
- **User Administration**
- **Cybersecurity** - 18 guidelines
- **Accountability**

**What is Open Architecture for Airport Security Systems?**
Integration versus Interoperability

Integrated Systems
- Co-ordinated into a functioning, unified whole
- Any software can be integrated - but at cost
- Changes to components are often difficult to maintain
- Interoperability is NOT guaranteed

Interoperable Systems
- Provide or receive services from other systems
- Connect multiple components from multiple vendors without changing existing components
- Agnostic to changes
- Interoperability guaranteed

A key requirement is understanding the benefits of an Interoperable approach, rather than an Integration approach.
A clear objective for the industry is to move away from proprietary end-to-end systems integration, and instead favour interoperability across interfaces and system boundaries.
Scope

Open Architecture for Airport Security Equipment covers 7 topics:

1. **Security Equipment** - the devices or hardware
2. **Algorithms** - enhanced detection for more than explosives
3. **Data Sharing** - images, interfaces, communication and ownership
4. **Equipment Control and Monitoring** - performance and equipment data, SCADA, IIoT and predictive maintenance
5. **User Administration** - integration with enterprise identity management capabilities, consider opportunities for single sign-on
6. **Cybersecurity** - foundation upon which OA sits, fundamental to data sharing, user administration and effective use of algorithms and assuring integrity
7. **Accountability** - ensure changes due to OA do not invalidate certifications and warranties and to clearly articulate the airport/regulator is not accountable for changes to the algorithms, hardware and software
Open Architecture will:

- Support collection of data in standardised formats and communication mechanisms - support business need for targeted near real-time information
- Support integration of new security equipment with new back-office applications
  - The points above provide data and information to enable previously unavailable key insights
- Integrate with an ID management platform for increased security and access control e.g. card based, biometrics or conventional login
- Support interchanging of detection algorithms and operational compatibility with OEM equipment
- Adherence to cybersecurity guidelines, increased monitoring and event reporting

Roughly 80% of software costs occur after initial deployment - airports will save money by making support and enhancements easier
Open Architecture will:

- Simplify CIP solutions. We can have one CIP system for all the security platforms.
- Enable TIP library to be standardised
- Ensure equipment from different vendors is interoperable.
- Support multiple algorithms and algorithm swapping
  - Explosives detection algorithms from the vendor and algorithms for forbidden items (firearms, sharps, illegal wildlife) and dangerous goods (lithium batteries) from 3rd party vendors.
- Improve training and support management of certifications.
- Enable more cost-effective processing and better optimisation of staff resources.
- Allow introduction of one file per individual containing all screening results - means there must be a method to identify the passenger, or boarding card ID in the security control.
Open Architecture will:

- Enable reduced stock of spare parts - fewer life-limited components
- Optimise equipment downtime - reduce corrective maintenance and increase the efficiency of planned maintenance
- Reduce training costs due to commonality
- Support collection of data in standardised formats and communication mechanisms - enables effective Condition Based Monitoring and ultimately Predictive Maintenance - faults based on consistent data rather than human interpretation

Benefits – Maintenance and Monitoring
Awareness:
Airports must explore the benefits of Open Architecture - work with vendors to ensure interoperability

Competence:
Airports and vendors must gain knowledge of Open Architecture

Tenders:
Airports add Open Architecture requirements when purchasing new systems

Vendor communication:
Airports need to be aware of vendor compliance with (or lack of) Open Architecture

What is the status of the vendors on Open Architecture?
None have a complete solution. Look at their roadmap and talk to them about your business needs and how the concepts of Open Architecture will produce benefits.
Further information

Download the Open Architecture documentation:


Thank you and goodbye!

Comments appreciated:

Richard Dempers (Lead Designer, Security Transformation) - Heathrow

Eugene Kramer (Head of Cybersecurity, Aviation Security & Borders) - Heathrow

Contact ACI EUROPE for further details