KENT STATE UNIVERSITY

10TH NATIONAL AVIATION SYSTEM PLANNING SYMPOSIUM (NASPS)

Plenary Session V. Trending Trends: Incorporating the Latest Best Practices Related to Safety, Security, and Resiliency into System Planning.

Anchorage, AK. Tuesday, 22nd May 2018 – 1000-1115.

Moderator: Dr. I. Richmond Nettey

Associate Dean and Professor, College of Aeronautics and Engineering, 202J Aeronautics and Technology Bldg., Kent State University, Kent OH.

President, University Aviation Association (1997-1998)

Trustee, Aviation Accreditation Board International (2004-2007)

10th NASPS - Plenary Session V – I

- **The combined effect of unprecedented growth in global demand for commercial air travel and the concomitant impact of significant threats to aviation security, have compelled attention to the need for integrating safety, security and resiliency into system planning in a sustainable manner.**

- **This session addresses the latest best practices that are critical to system planning from the multiple perspectives of safety, security and resiliency in the operation and management of large commercial service airports and airport systems.**

- **Sustainability/Resiliency Planning in an Aviation System**
- **Cybersecurity Measures within the System Plan**
- **SMS Integration within System Planning**

KENT STATE UNIVERSITY

10th NASPS - Plenary Session V – II

- **Panel Speakers:**
- **Dominic Nessi, Senior Technology Adviser, Burns Engineering: "Integration of Cybersecurity Measures into Airport System Planning."**

- **Robert Feteanu, Senior Airport Analyst, ARUP: "Latest Trends in Passenger Processing at Security Checkpoints: Confluence of Sustainability, Resiliency, and Cybersecurity."**

- **Jeremy Worrall, Maintenance & Operations Superintendent, Alaska Department of Transportation: "Safety, Security and Resiliency in Airport System Planning: Emerging Trends and Practice in Alaska."**

KENT STATE UNIVERSITY

PRESENTATION – OVERVIEW

- I. INTRODUCTION OF PANELISTS
- II. PANEL PRESENTATIONS
- III. QUESTION AND ANSWER SESSION
- IV. FUTURE CHALLENGES

KENT STATE UNIVERSITY

KENT STATE UNIVERSITY

I. PANEL SPEAKERS

Dominic Nessi

Mr. Dominic Nessi, Senior Consultant

Burns Engineering-AeroTech Partners

- Senior Technology Advisor working with a number of aviation leaders, including the Burns Engineering Group and Barich Associates.

- Founder, AeroTech Partners – an aviation cybersecurity company. Works closely with ACI World and SITA on cybersecurity issues
- Presently engaged in a number of airport technology projects and continues to speak internationally on a variety of topics, especially focusing on cybersecurity.
- Deputy Executive Director and Chief Information Officer, LAWA, 09/2007-02/2016
  - Responsible for all IT functions, including planning, design, implementation and utilization of LAWA's information infrastructure and related voice, data and video communications systems for LAX

KENT STATE UNIVERSITY

Robert Feteanu

Head of Aviation Consulting, ARUP Canada

- P.Eng., Ontario, Canada
- Member of TRB AV050 Committee: Airport Terminal and Ground Access
- B.S. Aerospace Engineering, Polytechnic University Bucharest, Romania
- M.A.Sc. Aerospace Engineering, Ryerson University Toronto, Canada
- Leads the Aviation Consulting for Arup Canada, consisting of Airport Analysis and Simulation, and Airport Planning groups
- Project Manager and Technical Lead (Airport Simulation and/or Planning component) for some of the most prestigious international airport development projects around the world such as New Midfield in Abu Dhabi, Hamad Airport in Doha, New Beijing Airport, Taipei New Terminal 3, New Istanbul, JFK Terminal 5 for JetBlue, Toronto Pearson, etc.

Jeremy Worrall

Mr. Jeremy Worrall, A.A.E., ACE
Maintenance and Operations Superintendent,
Alaska Department of Transportation

- **Airport Operations, South Bend International Airport**
- **Airport Operations, Norman Y. Mineta San Jose International Airport**
- **Airport Safety & Security Officer, Alaska DOT&PF**
- **Regional Aviation Manager, Alaska DOT&PF**
- **2017 Recipient, Aviation Excellence Award, Northwest Chapter of the American Association of Airport Executives (AAAE)**

- **B. S. Aviation Technology – University of Alaska at Anchorage**
- **M.B.A. – Arizona State University**

KENT STATE UNIVERSITY

KENT STATE UNIVERSITY

"Aviation is proof, that given the will, we have the capacity to achieve the impossible."

~ Captain Edward "Eddie" Rickenbacker.

KENT STATE UNIVERSITY

II. PANEL PRESENTATIONS


10th Triennial National
Airport System Planning
Symposium
May 22, 2018
SECURITY
Dominic Nessi, Burns Engineering

How Real is the Cyberthreat to Airports?

Let’s take a look … Around the World in 80 seconds

Ukraine

A major wave of ransomware infections hits media organizations, train stations, **airports**, and government agencies in Russia and Eastern Europe.

Researchers found strong evidence linking the attack to the creators of NotPetya and noted that the malware used leaked NSA-linked exploits to move through networks.

Ukrainian police later reported that the ransomware was a cover for a quiet phishing campaign undertaken by the same actor to gain remote access to financial and other confidential data.

(Center for Strategic a[illegible]Studies [illegible]BE[illegible]17)

Poland

A cyberattack against **Polish flagship carrier LOT** grounded more than 1,400 passengers at **Warsaw's Frederic Chopin Airport** in what an airline spokesman described as the "first attack of its kind".

Hackers used a Distributed Denial of Service (DDoS) attack, a malicious technique commonly used on the Internet to overload an organization's system with multitude of simultaneous communication requests.

Australia

Australian authorities have named a Vietnamese hacker they say was able to break into the IT systems at **Perth International Airport** and steal security information.

The hacker stole a “significant amount” of sensitive security information about Perth International Airport, including building plans, Australian authorities have revealed.

The Perth Airport hacker has been identified as 31-year-old Duc Hoang Hai, who used the credentials of a third-party contractor to access the airport’s systems

Australia - Tasmania

Hobart airport website hacked with 'pro-Islamic militant messages

The website was taken offline three hours after being hacked about 3:00am on Sunday and has not yet returned. Tasmania Police have handed the investigation over to the Australian Federal Police (AFP) as the airport's owners review the website's security.

Saudi Arabia

The hard-drive-wiping “Shamoon” virus used against Saudi Aramco in 2012 was deployed against four Saudi Arabian government agencies.

The attack wiped data on thousands of computers at **Saudi’s General Authority of Civil Aviation**, the Saudi agency that runs **airports**.

Belgium

Belgian investigators have traced a cyberattack targeting Brussels airport hours after the ISIS suicide bombings to a teenager in the United States who had no terror links, prosecutors said today.

FBI agents questioned a 14-year-old boy from Pittsburgh, who admitted trying to hack **Zaventem airport**'s website and computer system in March 2016, they said.

Scotland - England

Last December, a radio transmitter stolen from **Edinburgh Airport** was used to give false commands to pilots. Also last year, a ham radio operator was found to have been issuing false instructions to pilots at **Manchester Airport**. As of yet there have been no successful prosecutions in the U.K. in air traffic hacking cases.

Britain's Civil Aviation Authority has issued a safety alert about a new threat to air passengers: hackers taking over air traffic control transmissions and giving pilots bogus orders.

England

A man in London happened to find intimate and detailed security protocols and maps for London's main airport, **Heathrow,** lying on the ground in broad daylight. The unnamed man noticed a USB stick in bushes on Ilbert Street, in West London, eighteen miles from the airport.

The man handed the USB stick over to the tabloid Sunday Mirror. The Mirror promptly reported that the drive contained 76 folders comprised of around 200 documents, maps, videos, timetables for anti-terrorism patrons, and much more, with information across numerous different systems.

England (continued)

- The exact route the Queen takes when using the airport and security measures used to protect her.
- Files disclosing every type of ID needed – even those used by covert cops – to access restricted areas.
- A timetable of patrols that was used to guard the site against suicide bombers and terror attacks.
- Maps pinpointing CCTV cameras and a network of tunnels and escape shafts linked to the Heathrow Express.
- Routes and safeguards for Cabinet ministers and foreign dignitaries.
- Details of the ultrasound radar system used to scan runways and the perimeter fence.

United Arab Emirates

The **Dubai International Airport** (DXB) had 50 email addresses and associated passwords stolen by a team of hackers from the Portugal Cyber Army and the HighTech Brazil HackTeam.

Viet Nam

Hackers on Friday successfully cyberattacked **Vietnam's two largest airports** and the nation's flag carrier, **Vietnam Airlines**.

The attacks — attributed to a Chinese hacking group known as 1937CN —failed to cause any significant security issues or air traffic control problems.

However, the individuals briefly hijacked flight information screens and sound systems inside Noi Bai (Hanoi) and Tan Son Nhat (Ho Chi Minh City).

Turkey

Istanbul's **Atatürk International Airport** (IST) had password control systems shut down by what is believed to have been a malware attack resulting in departure delays and extended waiting time for passengers.

Italy

The website of **Catania–Fontanarossa Airport** (CTA) in Italy was hacked and shut down for a few hours. A 22-year-old suspect was believed to have illegally accessed and damaged data.

India

The **Airports Authority of India**'s enterprise resource planning system was successfully hacked resulting in the system becoming inoperative, but more importantly resulting in the loss of personal data on employees.

India

The Twitter handle of the **Indira Gandhi International Airport** (IGIA) here was hacked and a "derogatory" message was posted on its page.

"The incident happened at 11 am when a derogatory message was posted. The post was removed within 10 minutes." an airport source said.

Pakistan

Indian Hackers have claimed that they have hacked the websites of **Islamabad, Peshawar, Multan and Karachi Airports**. Indian hackers also injected the sites with a ransomware which restricted them to restore the websites. The hackers demanded Bitcoins in exchange of unlocking the websites.

One of the hackers stated, “We have been closely monitoring attacks coming from Pakistan. They have been engulfed in spreading hatred and abusing India. We have control of many websites and each attack will get a stricter reply from our side.”

Canada

Officials at **Regina's International Airport** say their computers were hacked. People logging onto the airport's website Wednesday were greeted by a picture of a man with a Guy Falkes mask, similar to the one worn by the lead character in 2005's "V For Vendetta" movie.

Underneath was a message taunting web administrators by noting their site wasn't secure. Marketing agency Look Matters oversees the website – yqr.ca – and spokesman Rob Arnold says it appears to have been the work of the Anonymous Group.

United States

Major cyberattack carried out in 2013 by an undisclosed nation-state sought to breach US commercial aviation networks, says Center for Internet Security report.

A sophisticated advanced persistent threat from a sophisticated group of hackers acting on behalf of a nation state used a reputable industry source (ACI-North America) to send phishing emails to airports.

Seventy-five airports were affected and two had systems that were compromised as a result.

Introduction

What is the Connection between the Physical World of the Airport Planner and Cybersecurity?

Introduction

Most airport managers believe that cybersecurity is solely the domain of the IT department, but …

Introduction

…Cybersecurity is the responsibility of the airport's entire management team:

- IT department
- Legal counsel
- Public Safety
- Facilities
- Risk Management
- Human Resources, and
- **Airport Planning**

Introduction

Best handled through an airport's information technology governance committee which should have membership of all of the organizations just listed.

What binds these organizations together?

Introduction

Cybersecurity attacks could lead to:

- Unintended release of PII or sensitive information
- Loss of financial information
- Release of confidential emails
- Loss of IT resources
- Unavailable technology tools and resources
- Loss of physical security technology – CCTV & Access Control

Introduction

and result in:

- Public embarrassment for the airport
- Loss of confidence by the traveling public
- Financial loss
- Legal consequences
- Inability to perform critical functions

Introduction

A cyber attack does not necessarily have to be aimed at you

An airport could experience a debilitating attack just because it is attached to the internet

The Stuxnet virus spread to 80 countries after it struck the Iranian subterfuges, including Chevron in the United States

The Goal of Cybersecurity

- Confidentiality
- Availability
- Integrity

The Goal of Cybersecurity

- Confidentiality and Integrity relate specifically to the data itself

- **Confidentiality** is equivalent to privacy
- **Integrity** ensures that the data has not been tampered with and is accurate and comprehensive and complete

The Goal of Cybersecurity

- Confidentiality and Integrity are primarily assured through technology tools, hardware and software

The Goal of Cybersecurity

Availability requires a different approach and has a far more physical component requiring input from the airport planners

Availability focuses on data, but also systems, applications and **infrastructure**

The Goal of Cybersecurity

Availability is dependent on:

- Power – primary and redundant
- Fiber – primary and redundant
- Secure MPOEs
- Dedicated and secure data centers and server rooms
- Well spaced and secure communication closets

The Goal of Cybersecurity

Unlike hardware and software, these physical considerations are not easily acquired if not properly planned for, oftentimes making the airport planner, the CIO or IT Director's best buddy

The highest rated risks for cybersecurity often relate directly to the airport's inability to ensure Availability

Airport Building Systems

Airport building systems, control systems, HVAC, etc. are often the most over-looked IT systems when it comes to cybersecurity

Today's building systems have all of the same components as a typical office application:

- IP addressable
- Contain a database(s)
- Use the Airport's network
- Need external connections

Airport Building Systems

Airport planners and the IT department need to work with the Facilities department to ensure that newly planned and designed systems have the same IT infrastructure protections as the rest of the IT environment

- There is no airgap
- Legacy building systems use outdated protocols
- Can be used as a threat vector to other airport systems

Airport Building Systems

One unnamed US airport experienced an internal threat in its building system

A disgruntled employee turned on the heat every day at noon during the summer

This caused the airport a very difficult situation for 34 days until it was discovered

Airport Building Systems

Why so long to discover?

- The average cyber attack isn’t even discovered for an average of 260 days
- Cyberattacks are fairly easy to hide
- Internal threats are particularly easy to hide because the internal threat often has administrator privileges which could make altering logs easy and are not picked up in external network logs

Direct Impact on Planners

Let’s look to our friends South of the Border

- Ft McMurray airport attacked by Dharma, a form of ransomware
- The hacker demanded ransom in exchange for the decryption key

Direct Impact on Planners

- Hackers entered system through a vulnerability with VPN access
- Once the hacker got into the system through the server infrastructure. They were able to access all files and folders with administrative credentials
- They encrypted all the data which left Ft McMurray unable to access any files & services
- Ft McMurray did not pay the ransom, but …

Direct Impact on Planners

- Employees shut down for a total of 7 business days
- System rebuild and reprogram 6-8 weeks to full restore
- No DATA lost or compromised
- Total insurable Damages + $375,000

How would you function if all of your planning files were lost tomorrow?

Do you now if those files are completely backed up and protected?

The Greatest Threat

The single most devastating attack an airport could sustain would be a combined physical/cyber attack

Has not happened yet … but it is certainly within the realm of possibility

Imagine a coordinated active shooter attack coupled with CCTV, access control, audio paging and other communication medias and public safety systems rendered inoperable

Thank you for your attention

Dom Nessi, Burns Engineering

Trending Trends
Passenger Processing at Security

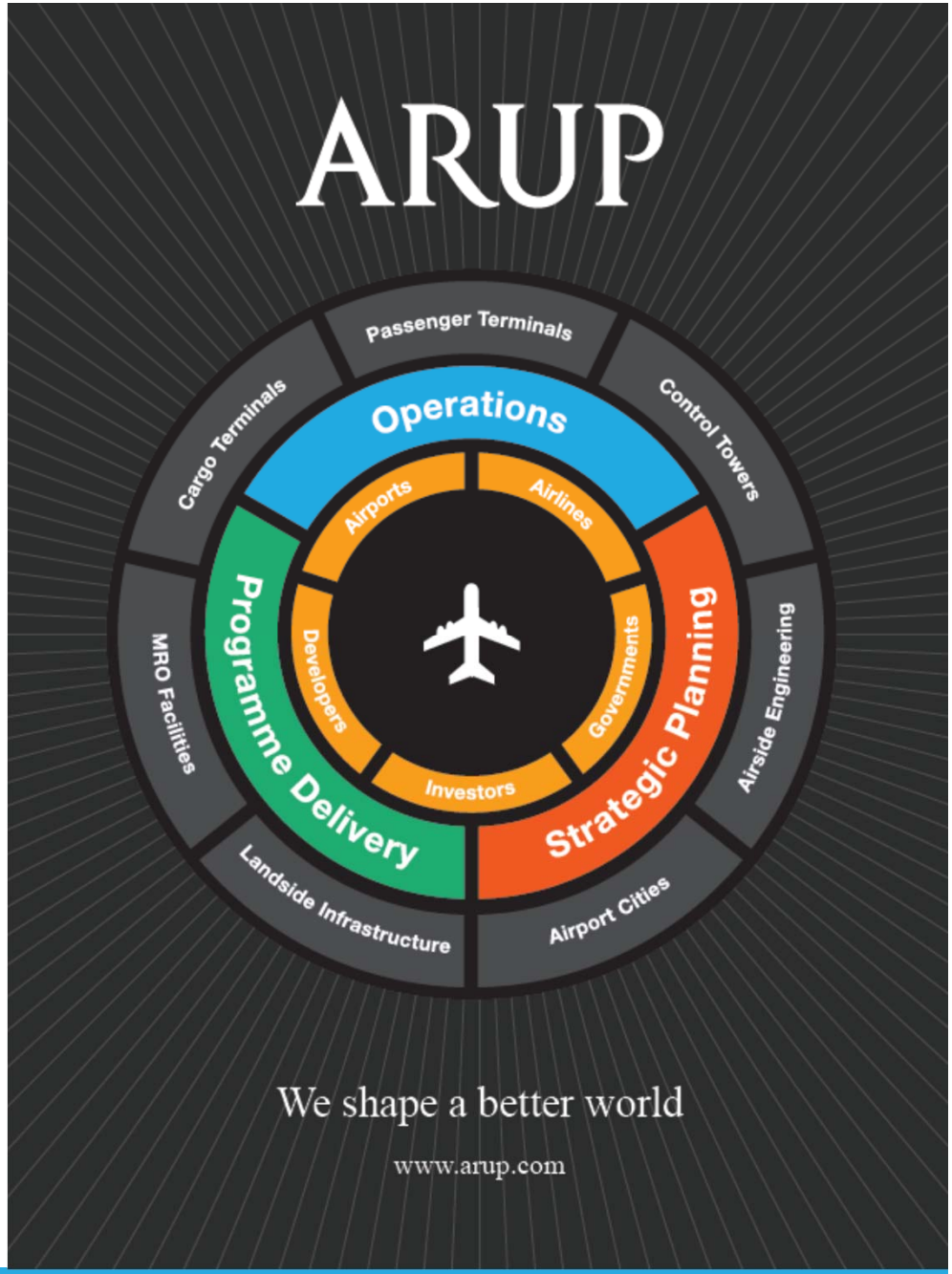
Robert Feteanu

May 22, 2018

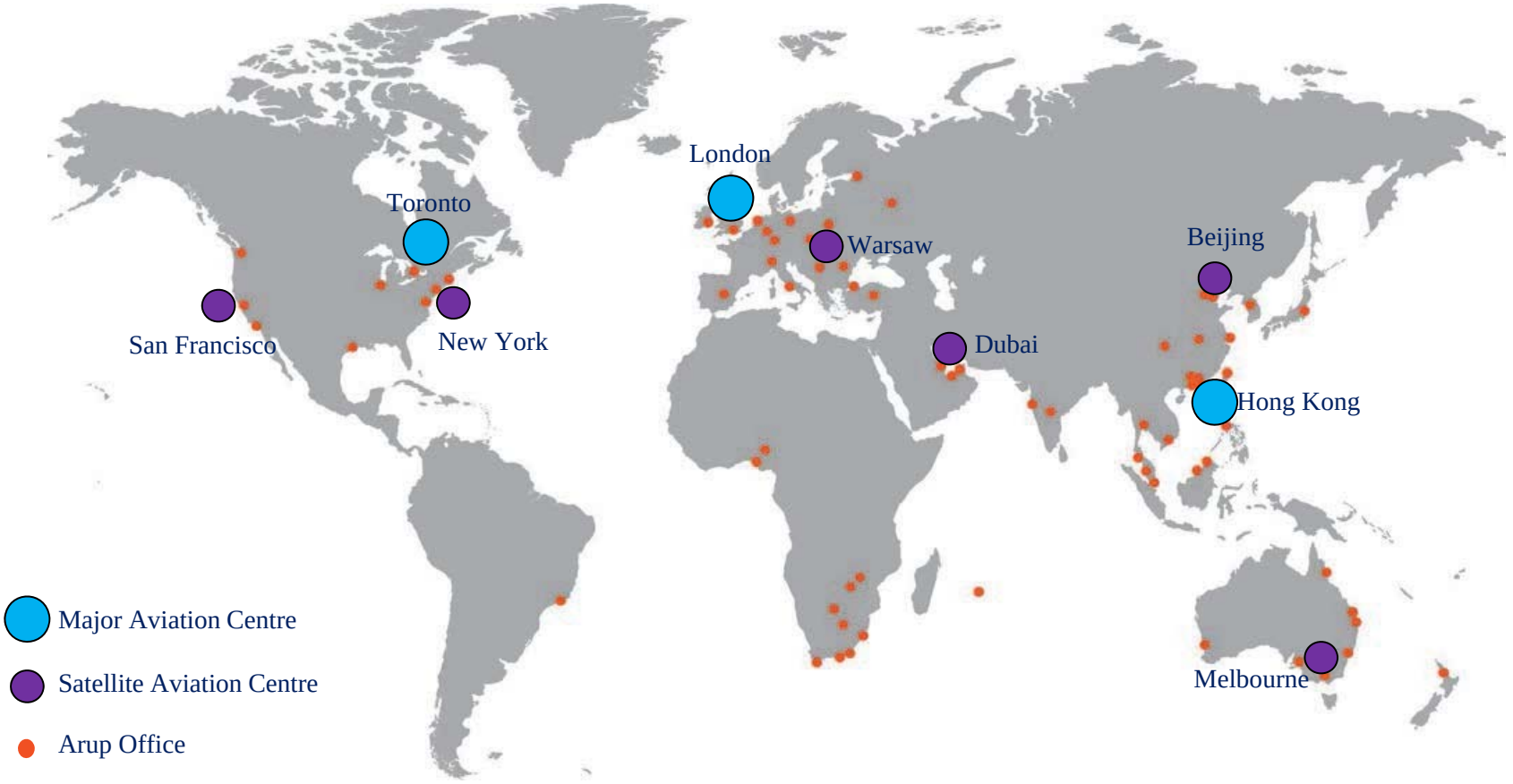
ARUP

Overview

- Current Developments
- Security Processing
  - Passengers
  - Hand Baggage
- Future Trends
- Future Ready Airports



Global Presence



ARUP

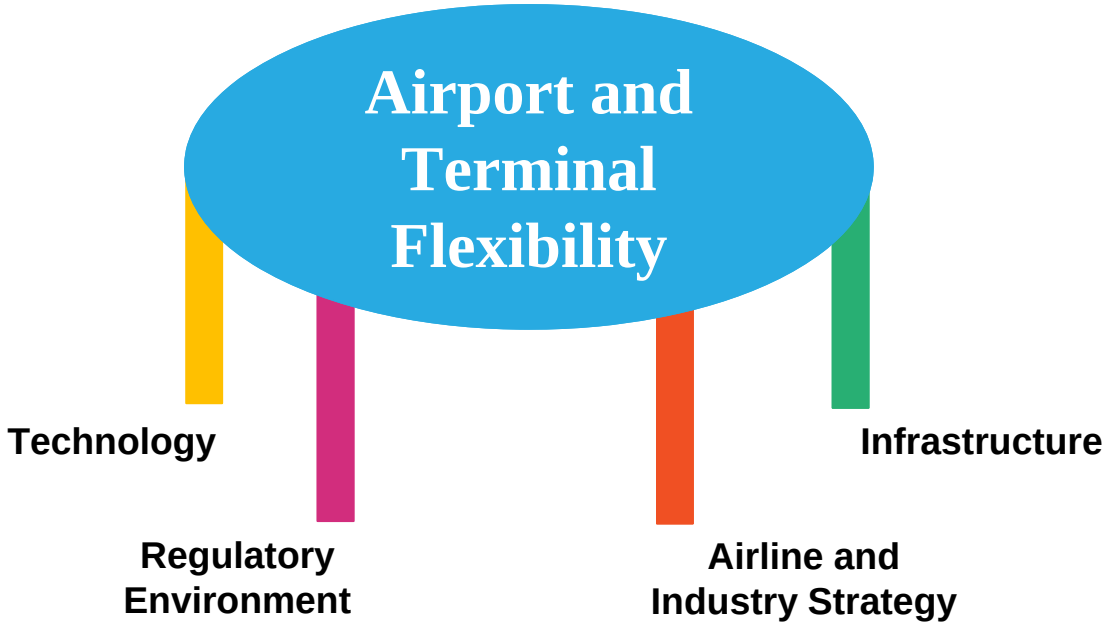
Major Airport Developments

ARUP

Taipei Airport (T3)

ARUP

The Pillars of Flexibility



Passenger Satisfaction = **Passenger Experience** — **Passenger Expectation**

ARUP

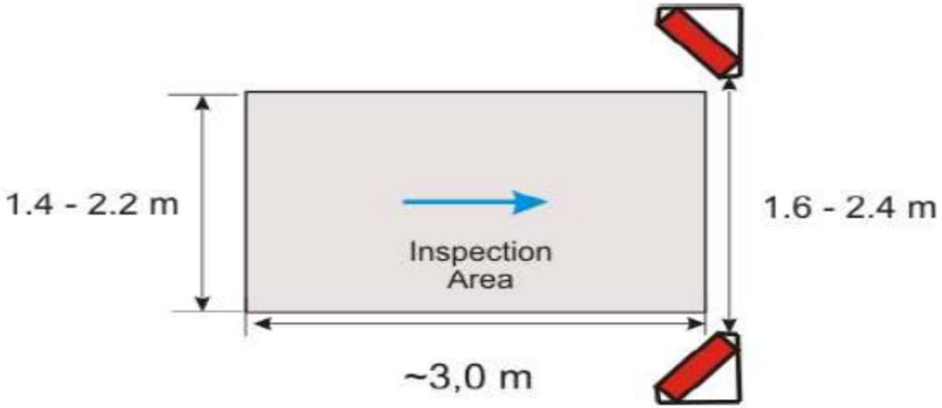
Location of Passenger Screening

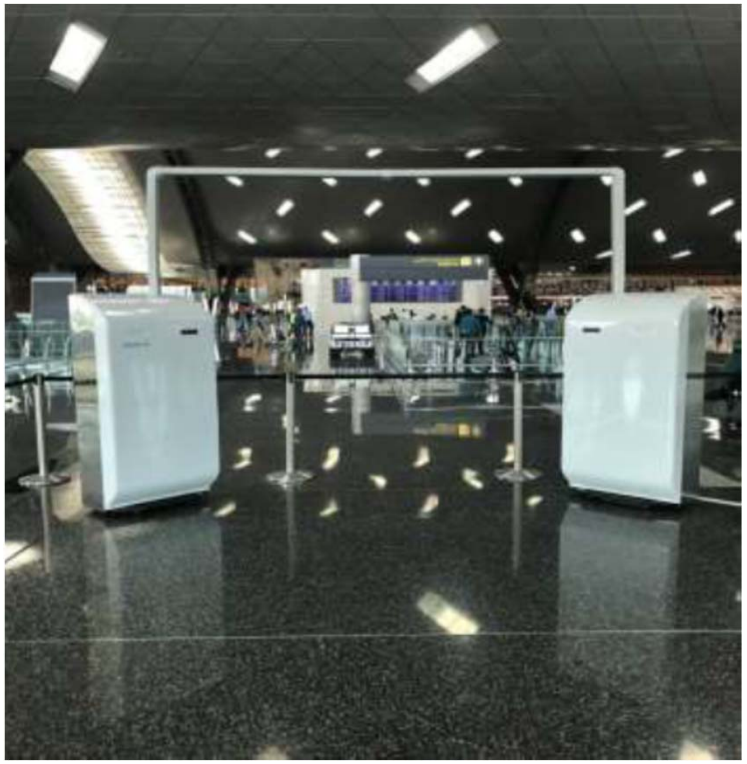
Abu Dhabi – Midfield Terminal Building (MTB)

ARUP

Pre Check-in Screening

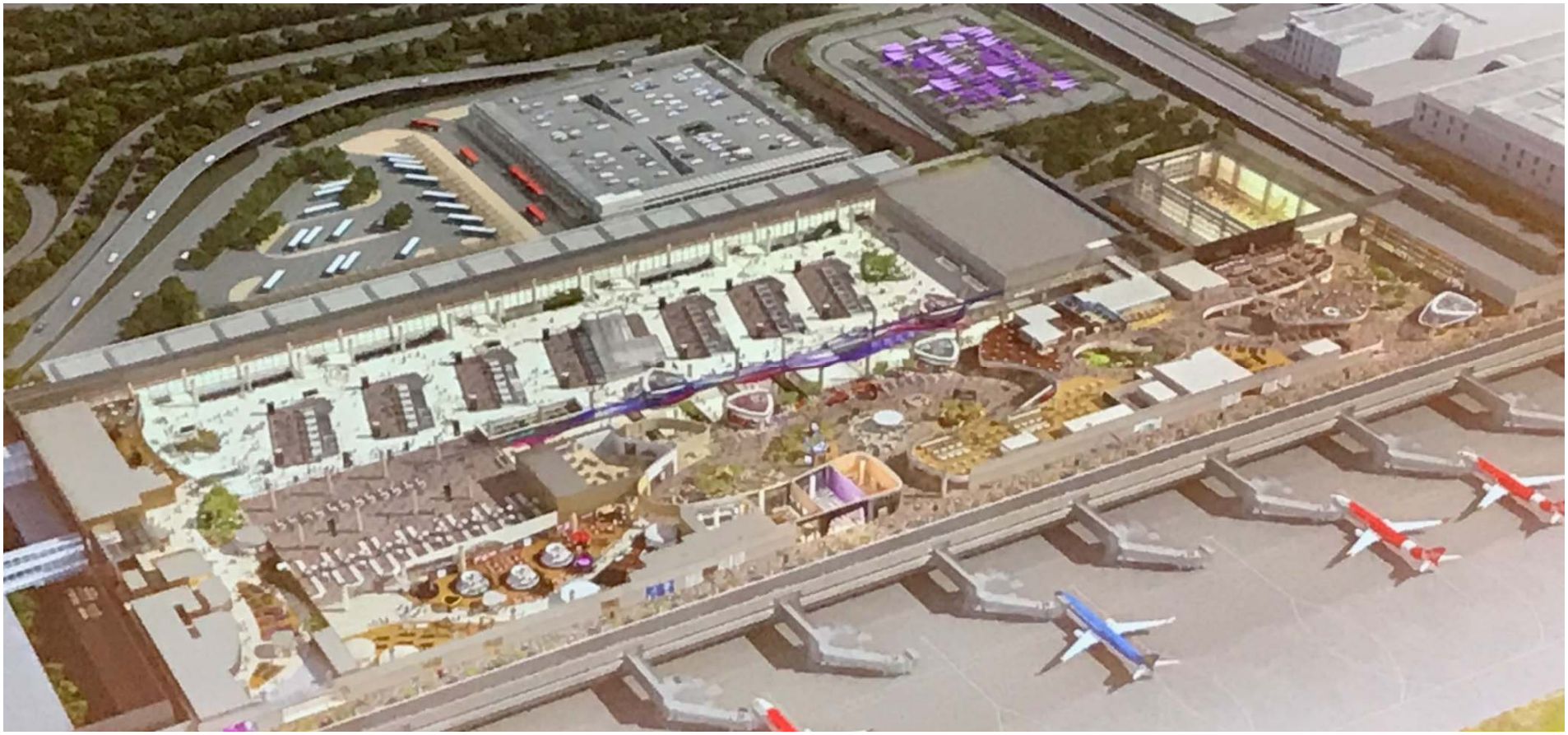
- **Pre Check-in Screening**: Doha Trials
- HSR: walk through technology
- Up to 12,000 people per hour





ARUP

Singapore Changi T4

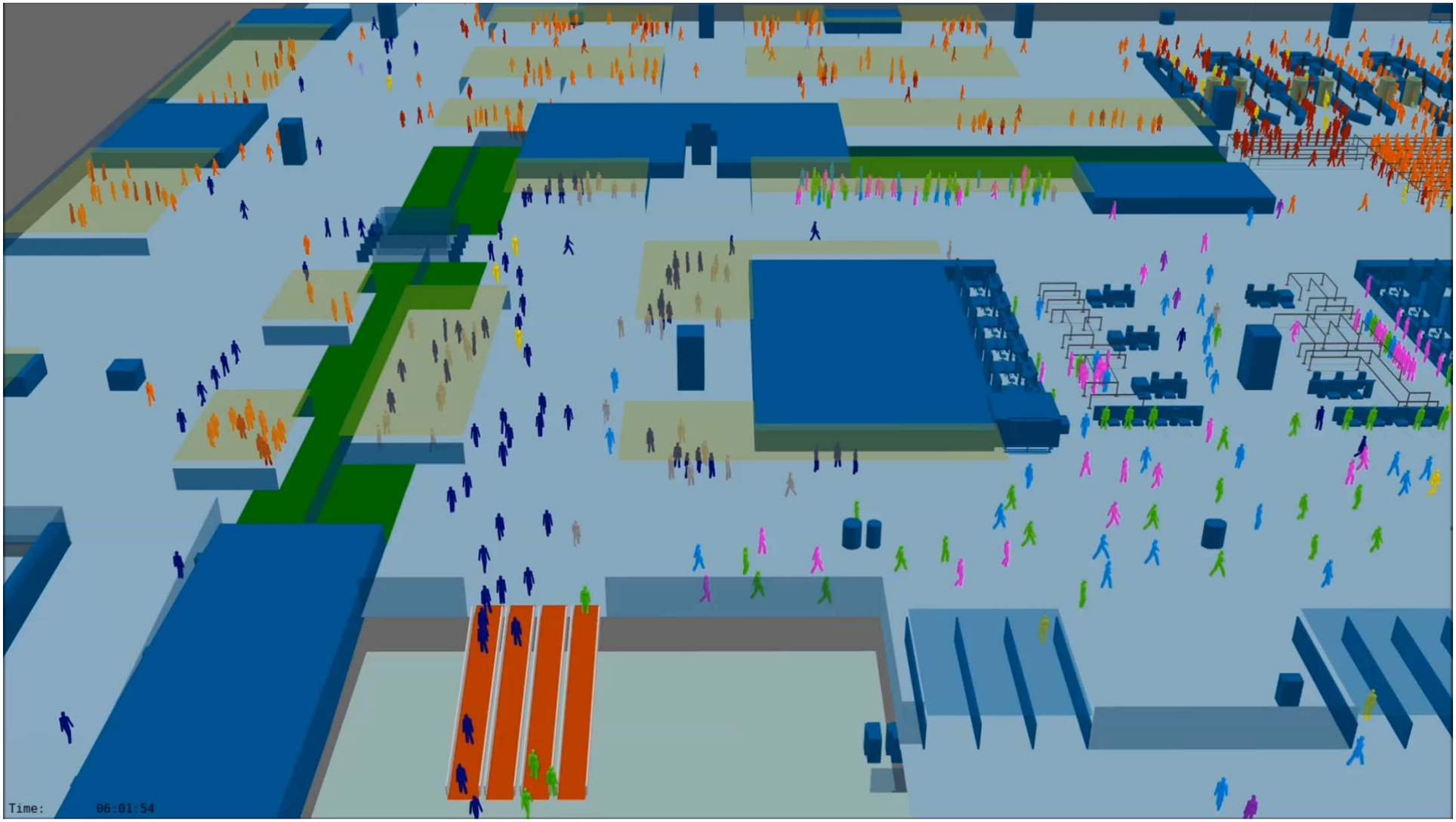


ARUP

Incheon T2 Expansion

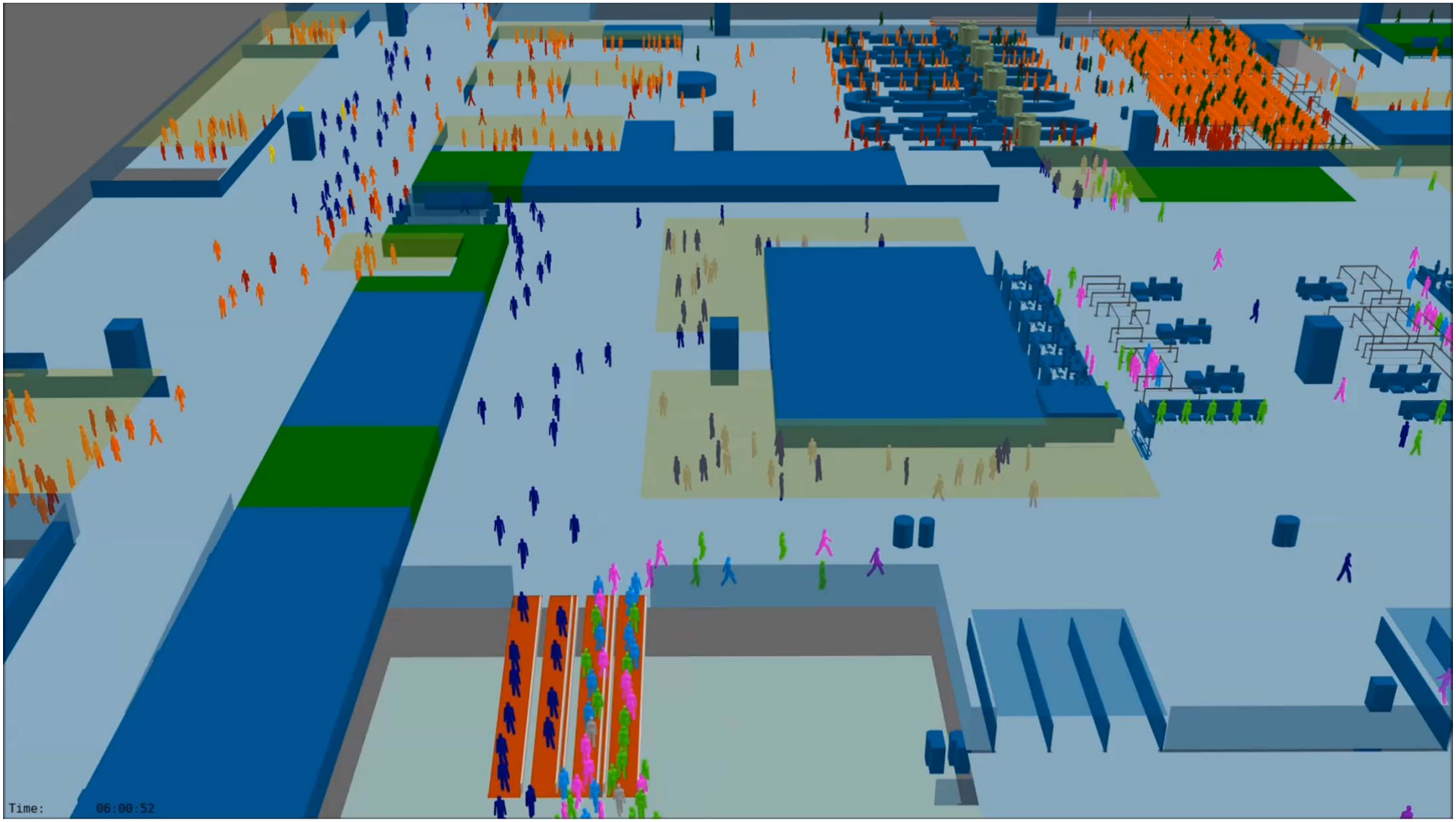
ARUP

Centralized



ARUP

Split



ARUP

Passenger Screening
An Evolving Process

Security Checkpoint

- Two independent processes take place during screening process. They need to be synchronized as much as possible

People

Trays

ARUP

Security Process – Change in Legislation

People

- Walk Through Metal Detector (WMD)
- Body-scanning (AIT) is mandatory
- AIT rate: 150 pax/hour
- **TWO** AIT and **One** WMD is required for two security lanes

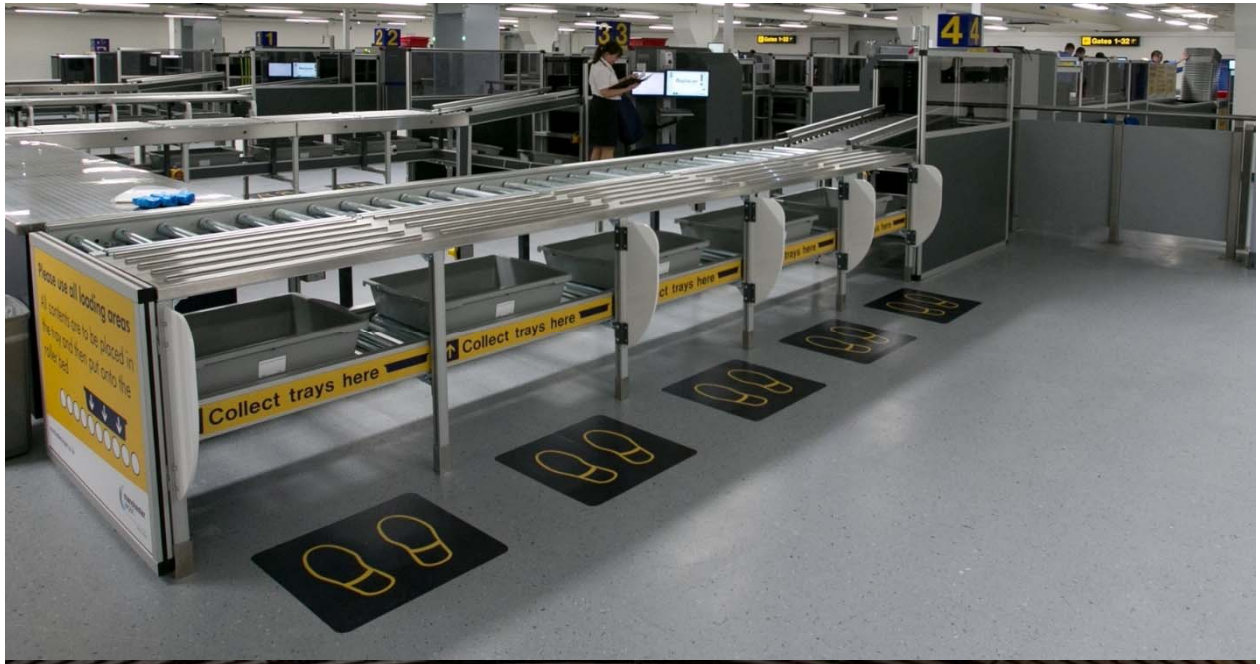
Trays

- ASL lanes with/without matrix screening
- Even longer and wider lanes
- Faster process: 500-700 big trays/hour or 250-350 pax/hour

New Process

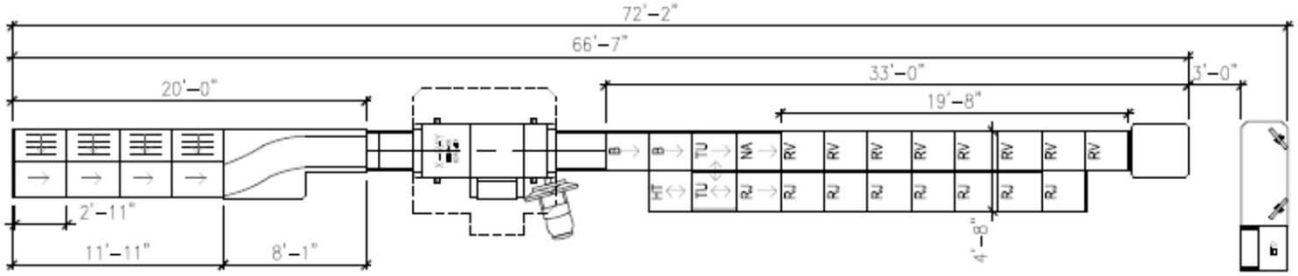
- Parallel divestiture
- Matrix screening
- Remote screening room for officers
- CT technology for 3D imaging

- Very long screening lanes, close to 21 meters
- Increased throughput rates
- Better utilization for officers
- 3D technology will reduce number of trays per passenger: liquids, laptops etc. can remain in bags

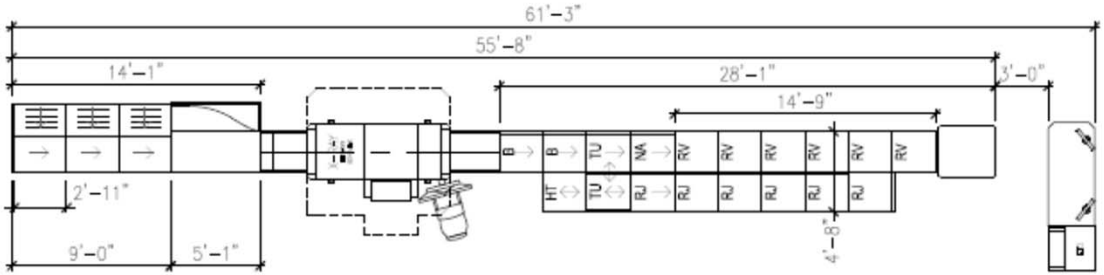


ARUP

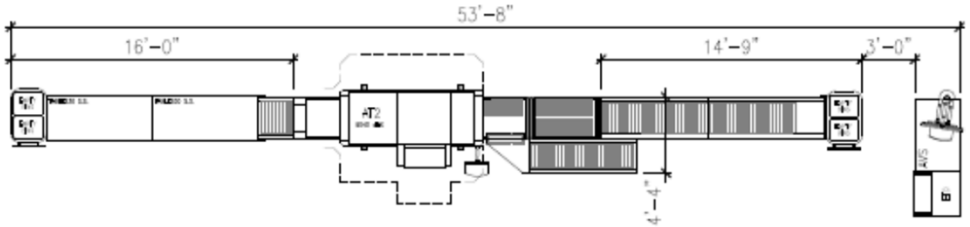
ASL Lanes



MACDONALD HUMFREY AUTOMATED LANE OPTIMUM CONFIGURATION



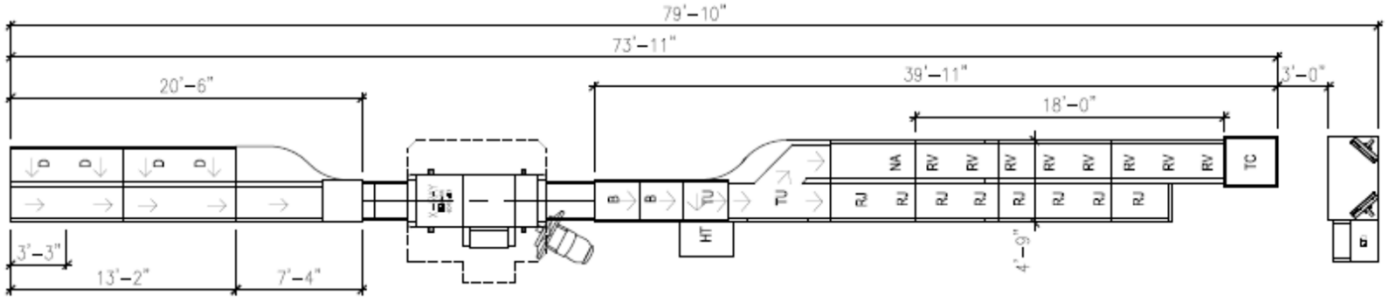
MACDONALD HUMFREY AUTOMATED LANE STANDARD CONFIGURATION



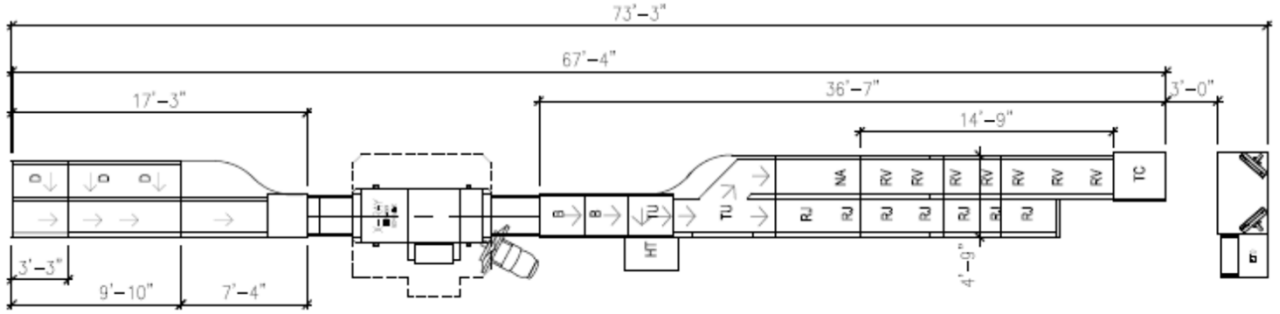
STANDARD AT LANE

ARUP

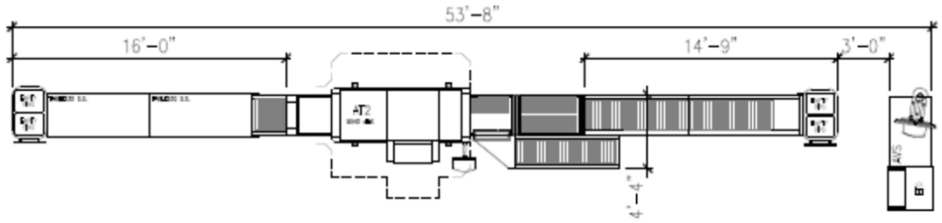
ASL Lanes



RAPISCAN SYSTEMS AUTOMATED LANE OPTIMUM CONFIGURATION



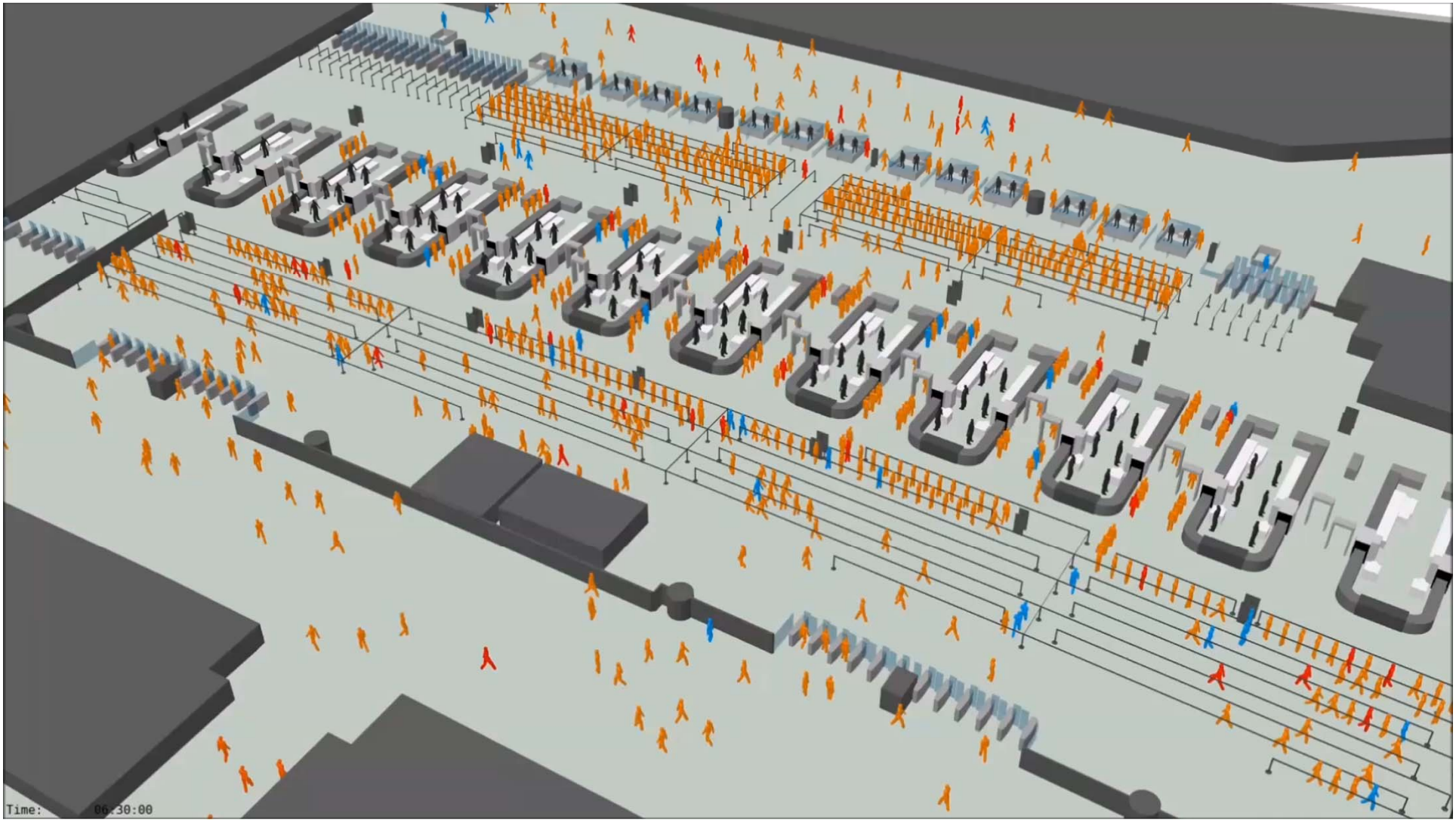
RAPISCAN SYSTEMS AUTOMATED LANE STANDARD CONFIGURATION



STANDARD AT LANE

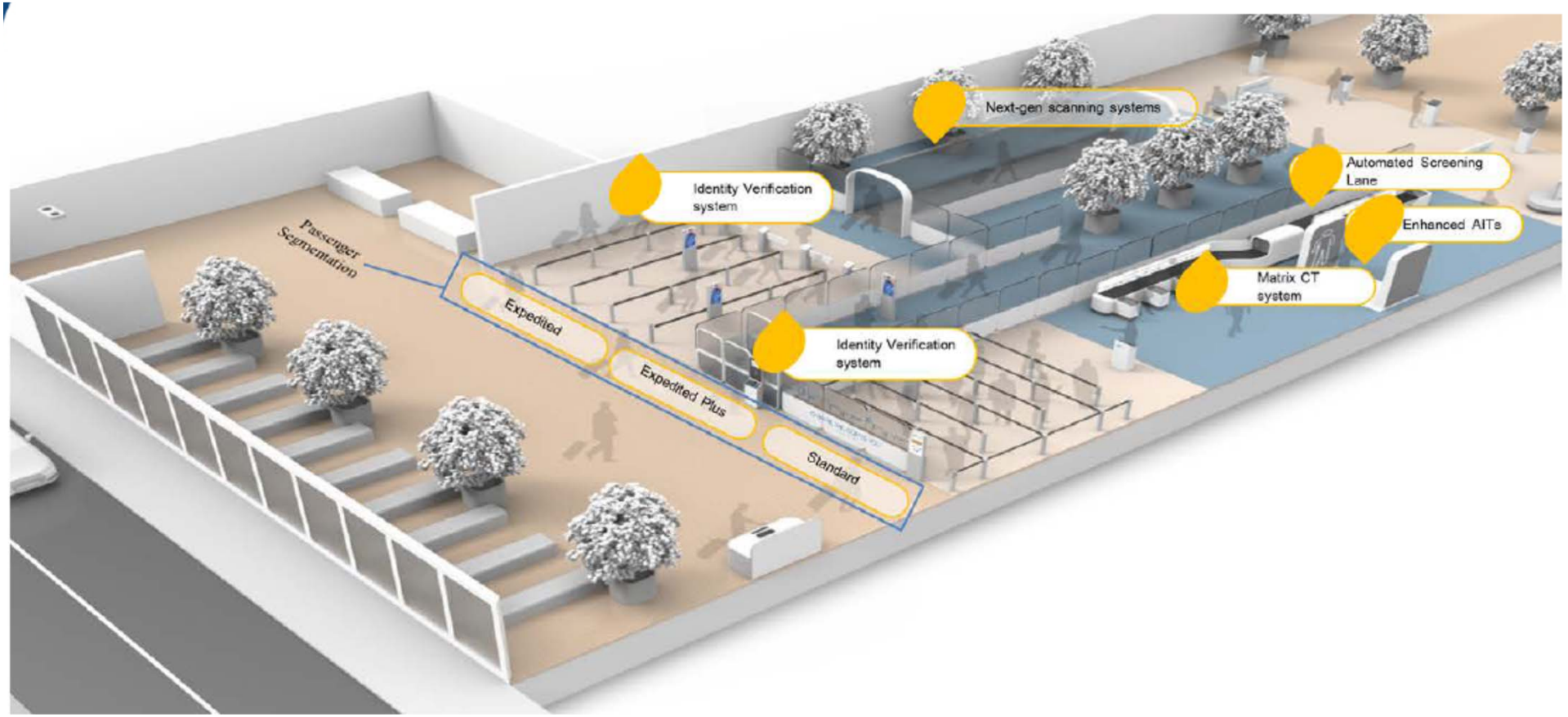
ARUP

Future Ready Airport?



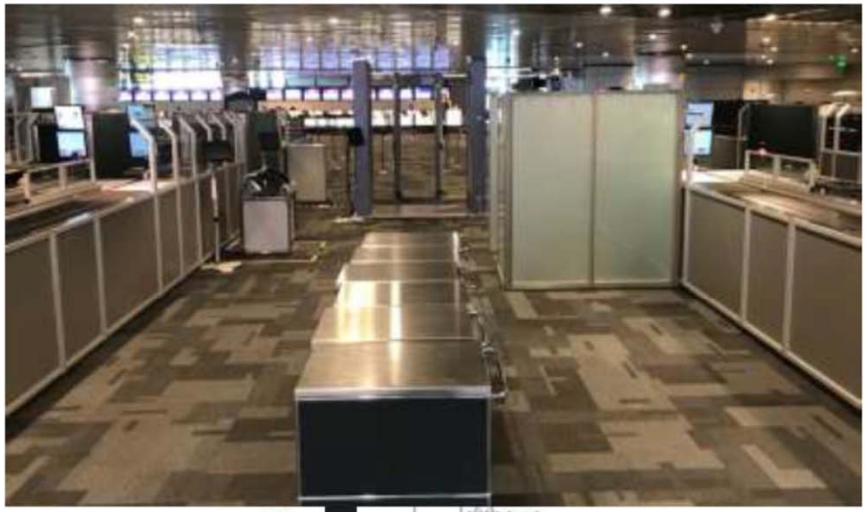
ARUP

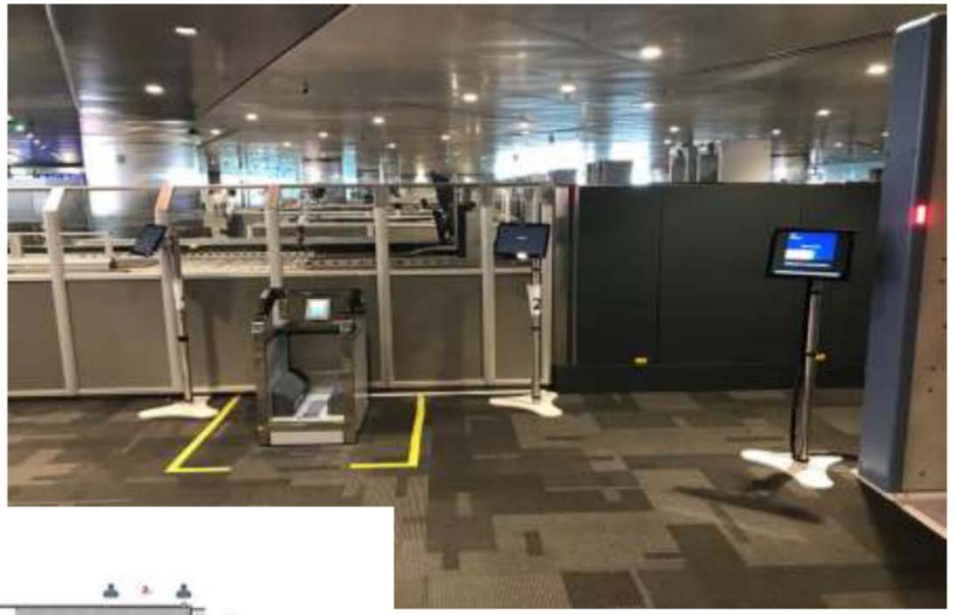
TSA Vision



ARUP

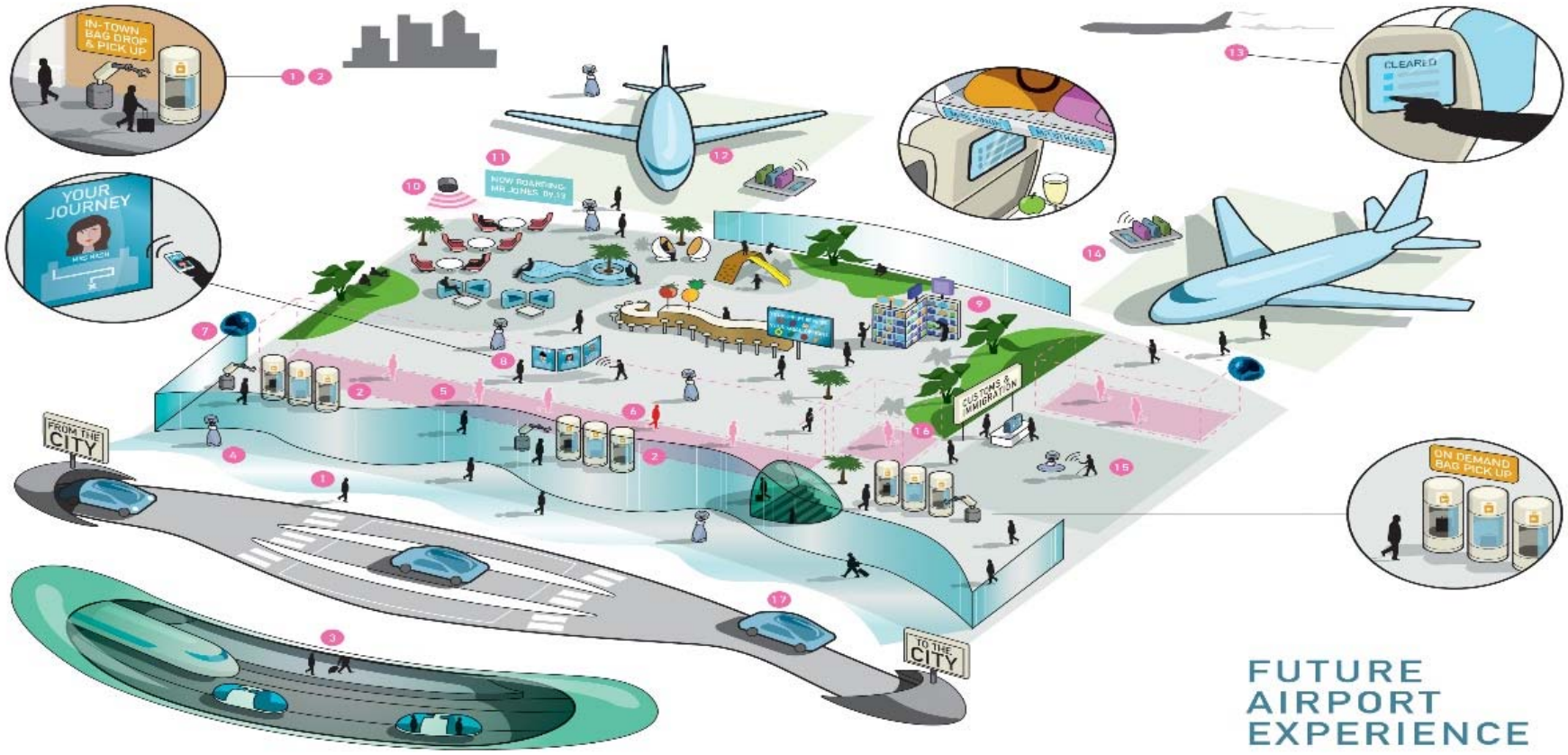
Doha Trial





ARUP

Future of Air Travel



ARUP

Thank You!

Alaska Department of Transportation & Public Facilities

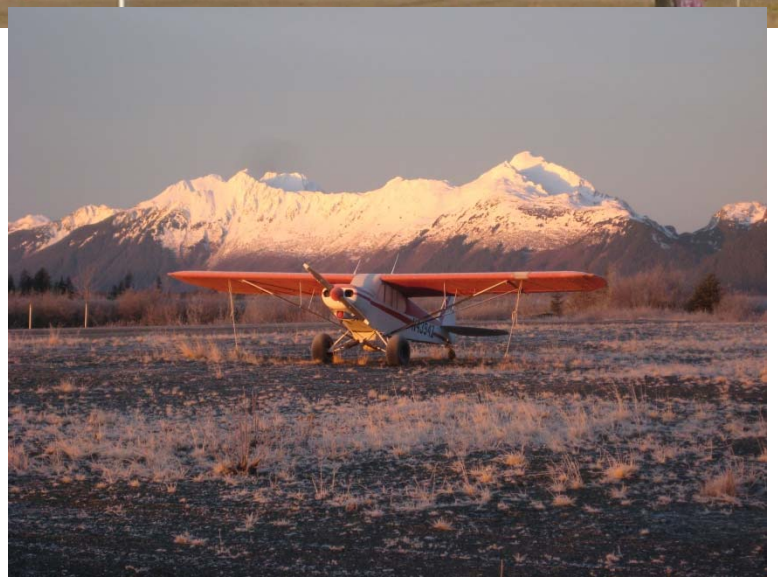
Identity Management System

Jeremy Worrall, A.A.E., ACE

May 22, 2018

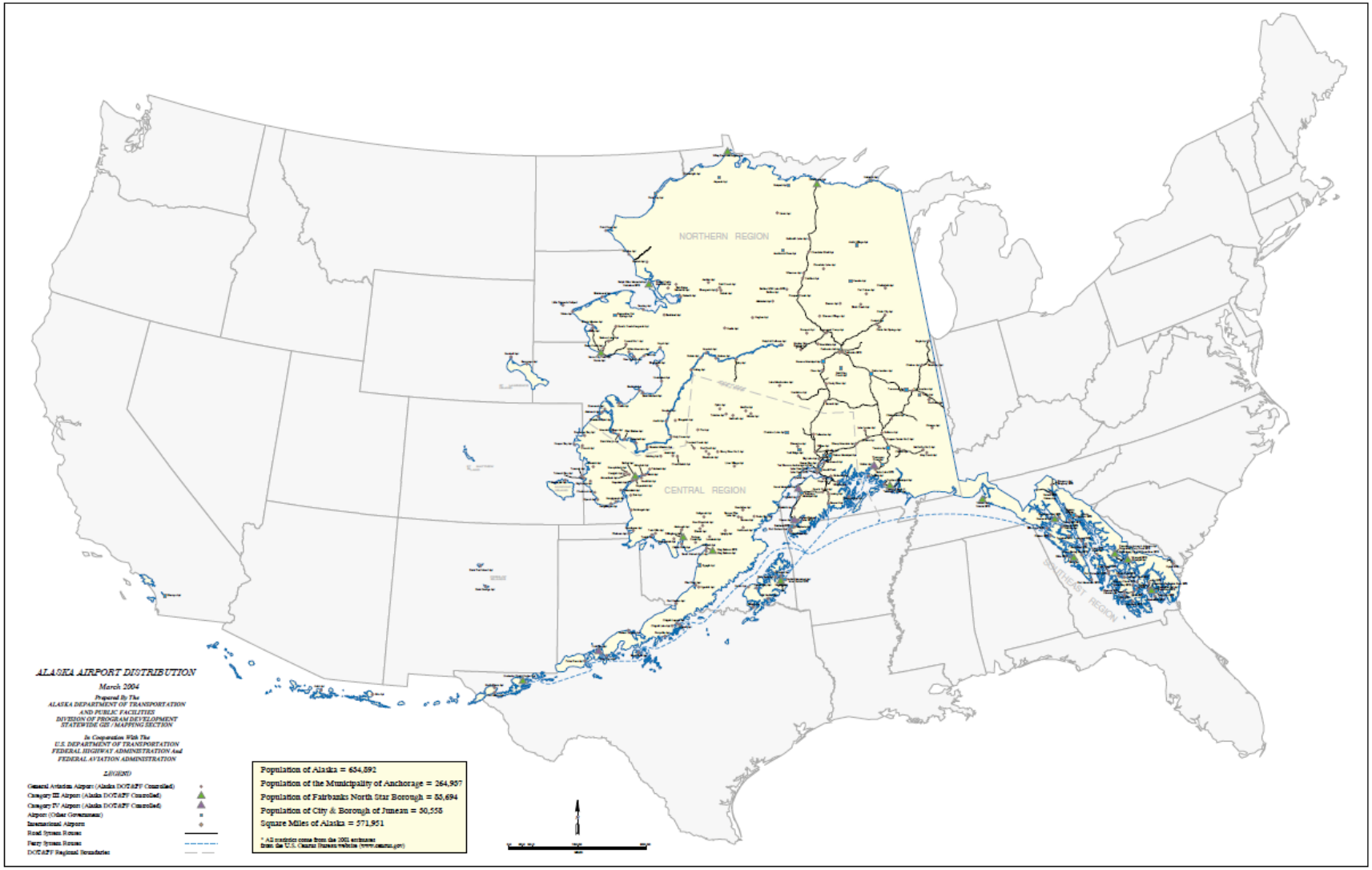
Keep Alaska Moving through service and infrastructure

AVIATION!



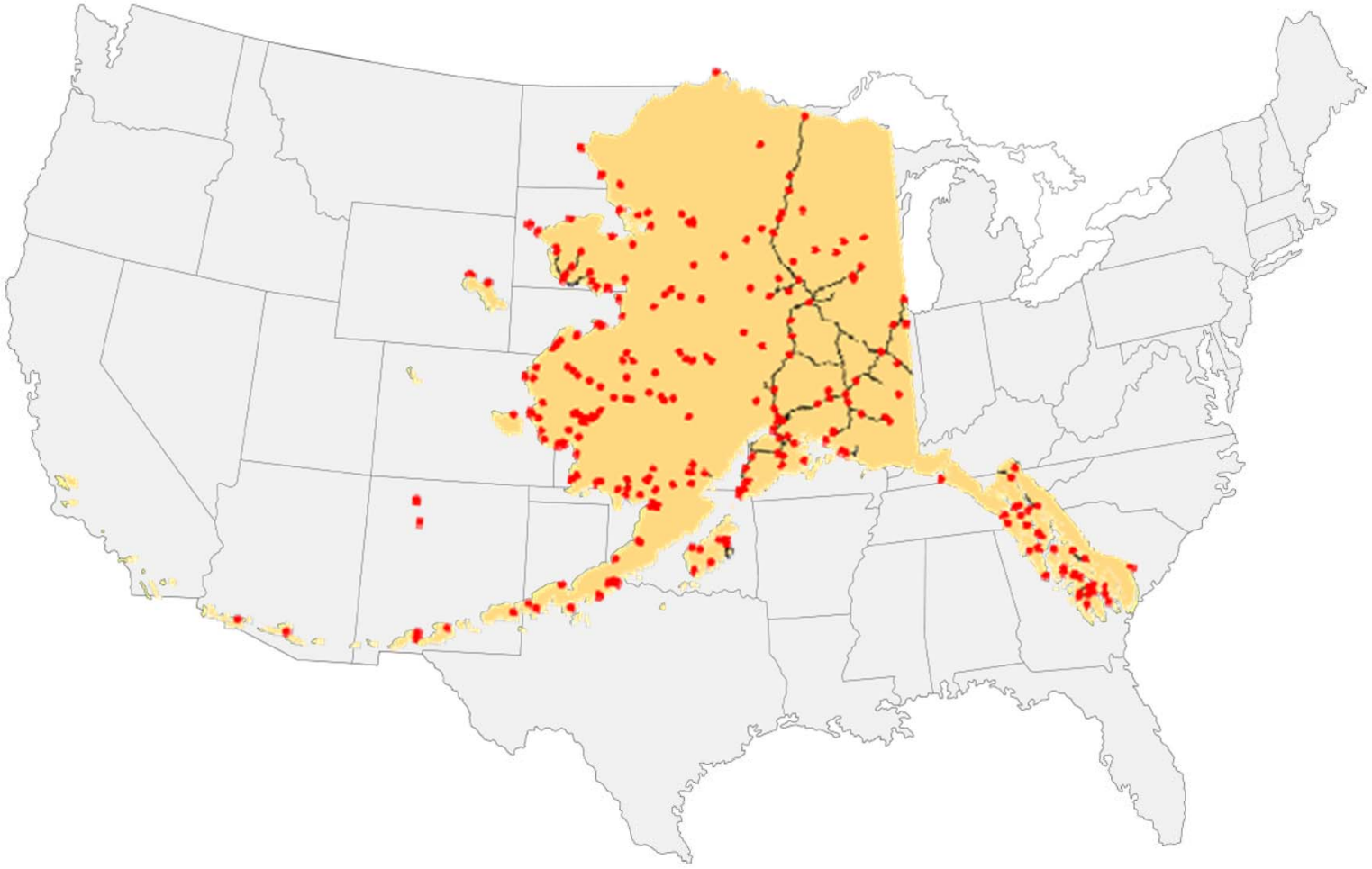
Alaska, the 49th State

Alaska to Scale

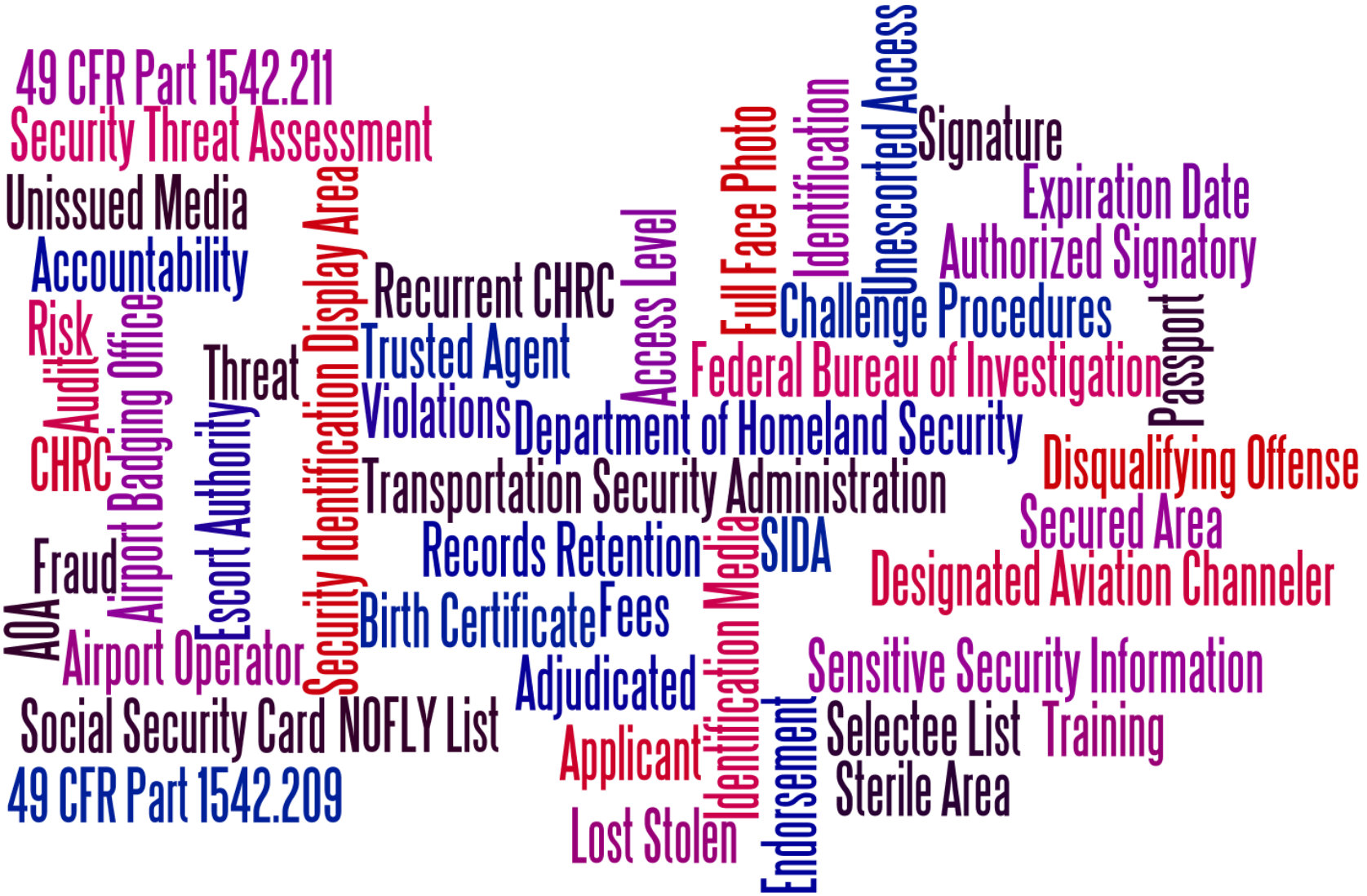


Alaska's Highway System

Alaska's Airports



Airport ID Badging



Airport ID Badging

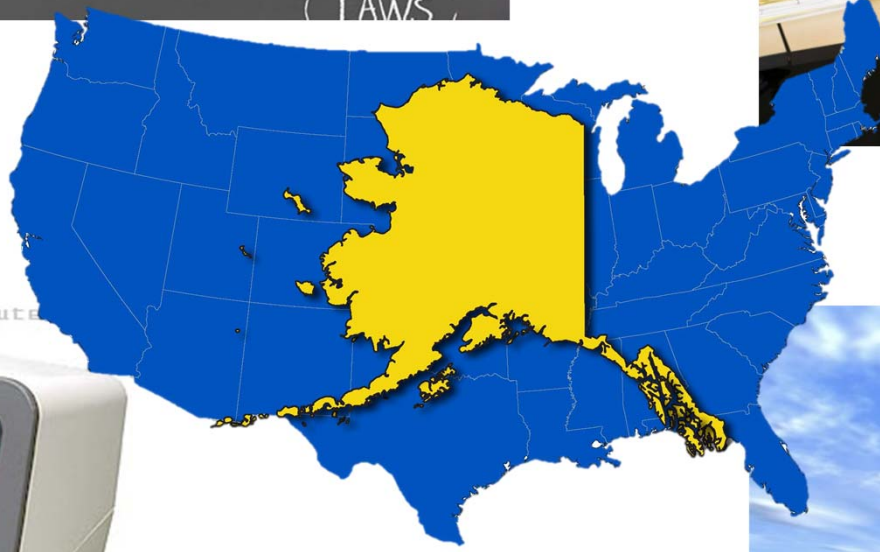
More stringent requirements since 9/11

- Fingerprint based criminal history records checks (CHRC)
- Airport Security Coordinator

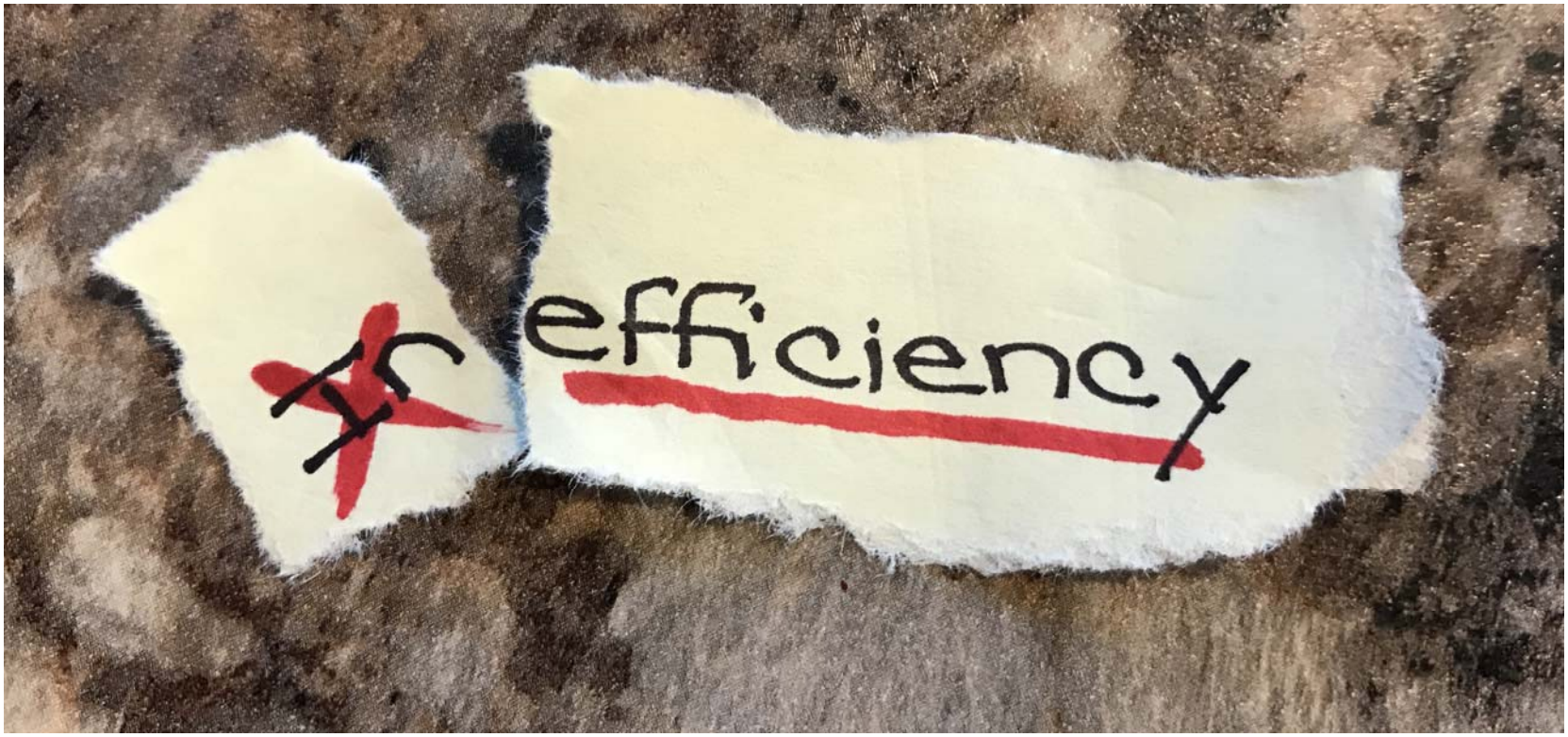
TSA Changes in the Last 10 Years

- Security Threat Assessment
- Trusted Agent
- Recurrent CHRC
- Authorized Signatory
- Enhanced Audits
- Increased Training

State of Alaska

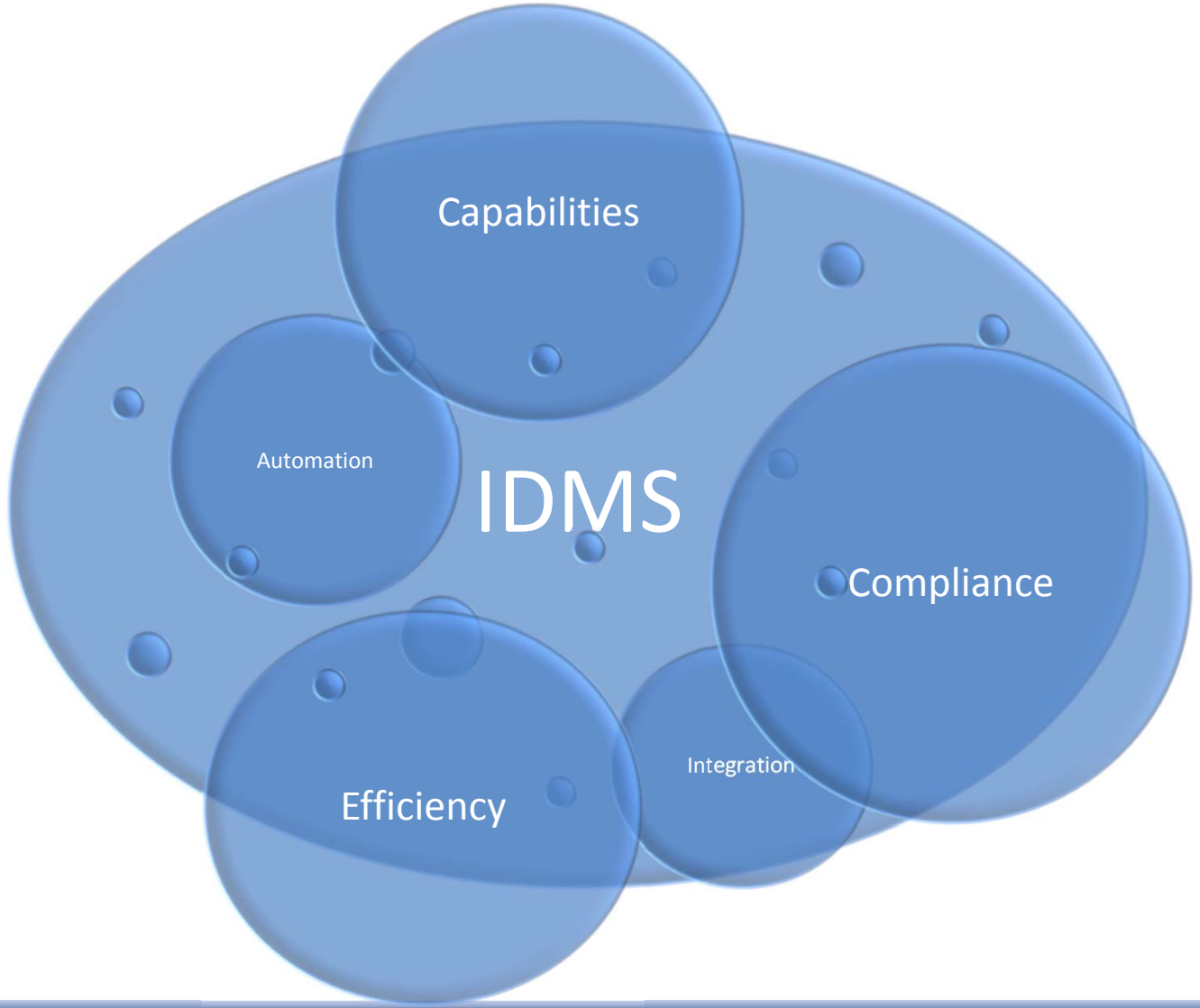


Shortcomings



Replacement

IDMS Project Goals



Possibilities

New Process Walkthrough

Current Status

- FAI Go-Live May 21
- 15 Rural airports
- ANC

Next Phases

- “One Badge”
- Interoperable Physical Access Control Systems (PACS)
- Shared Training

Jeremy Worrall, A.A.E., ACE
Airport Operations Superintendent
DOT&PF Statewide Aviation
(907) 451-5230
jeremy.worrall@alaska.gov