Open Threat Assessment Platform (OTAP)

ADSA 14

Andrew Cox
May, 2016
acox@sandia.gov

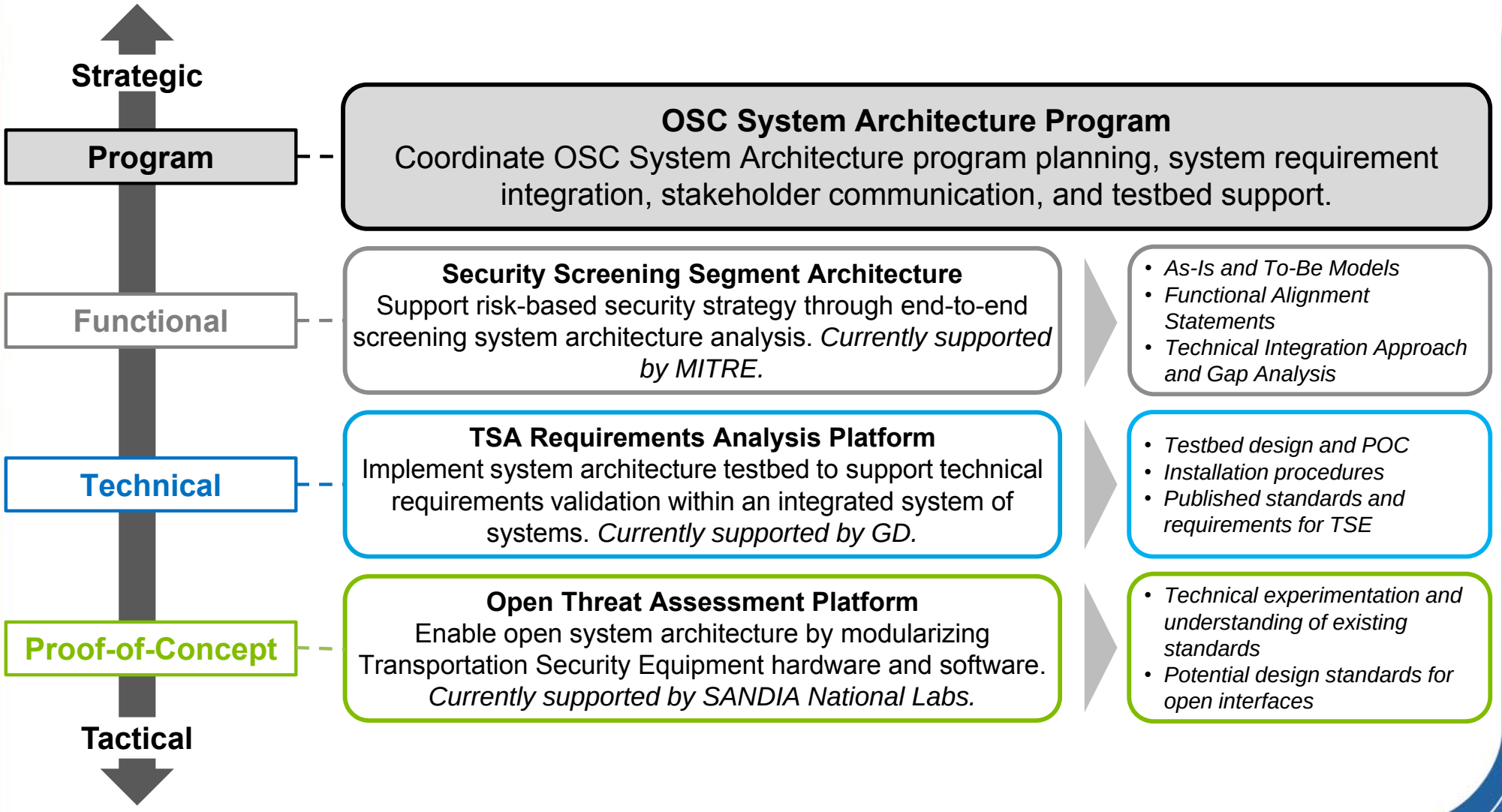
Overview

The ***Open Threat Assessment Platform (OTAP)*** will develop and demonstrate an open architecture baggage screening prototype in partnership with several Transportation Security Equipment (TSE) manufacturers that allows third-party vendors to develop and easily implement detection algorithms and specialized hardware upgrades on field deployable TSE.

An “open” platform is a technology platform that utilizes a “plug-and-play” or open architecture based on standardization of data formats, interfaces, and protocols that allows for the modularization of a technology platform similar to apps on smart phones.

OTAP Part of TSA Systems Architecture Efforts

TSA has initiated a series of complementary investments to design and implement the OSC System Architecture.



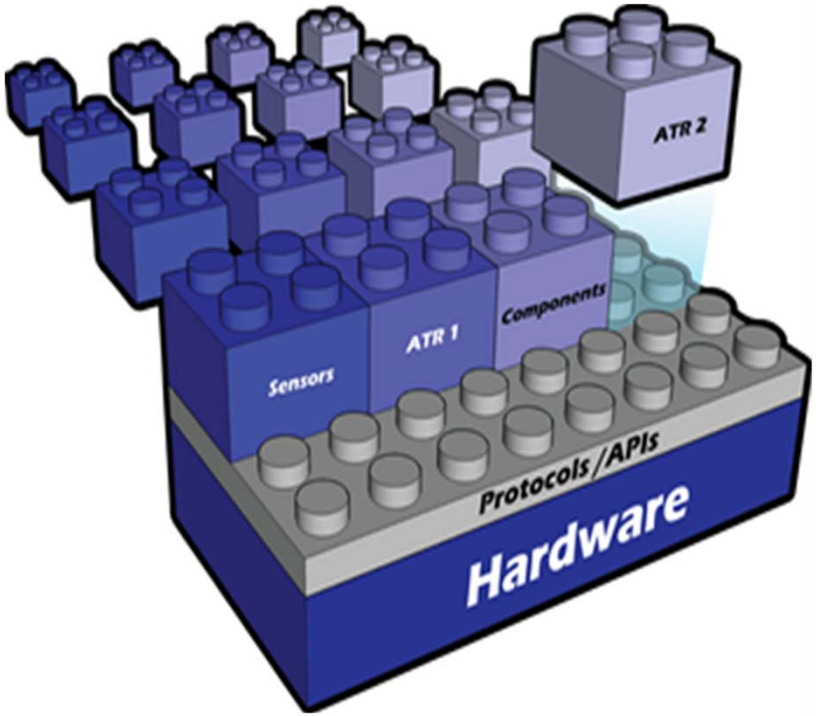
OTAP Software Enables Plug-and-Play

Moving to an Open Systems Architecture (OSA) will lower the technical complexity for upgrading Transportation Security Equipment (TSE) with the goal of upgrades seamlessly integrated into a plug-and-play platform.

Simpler integration allows for more frequent and cost-effective waves of innovation which, in turn allow TSA capabilities to match and then exceed adversary capabilities.

A plug-and-play platform promotes increased specialization in the security technology market.

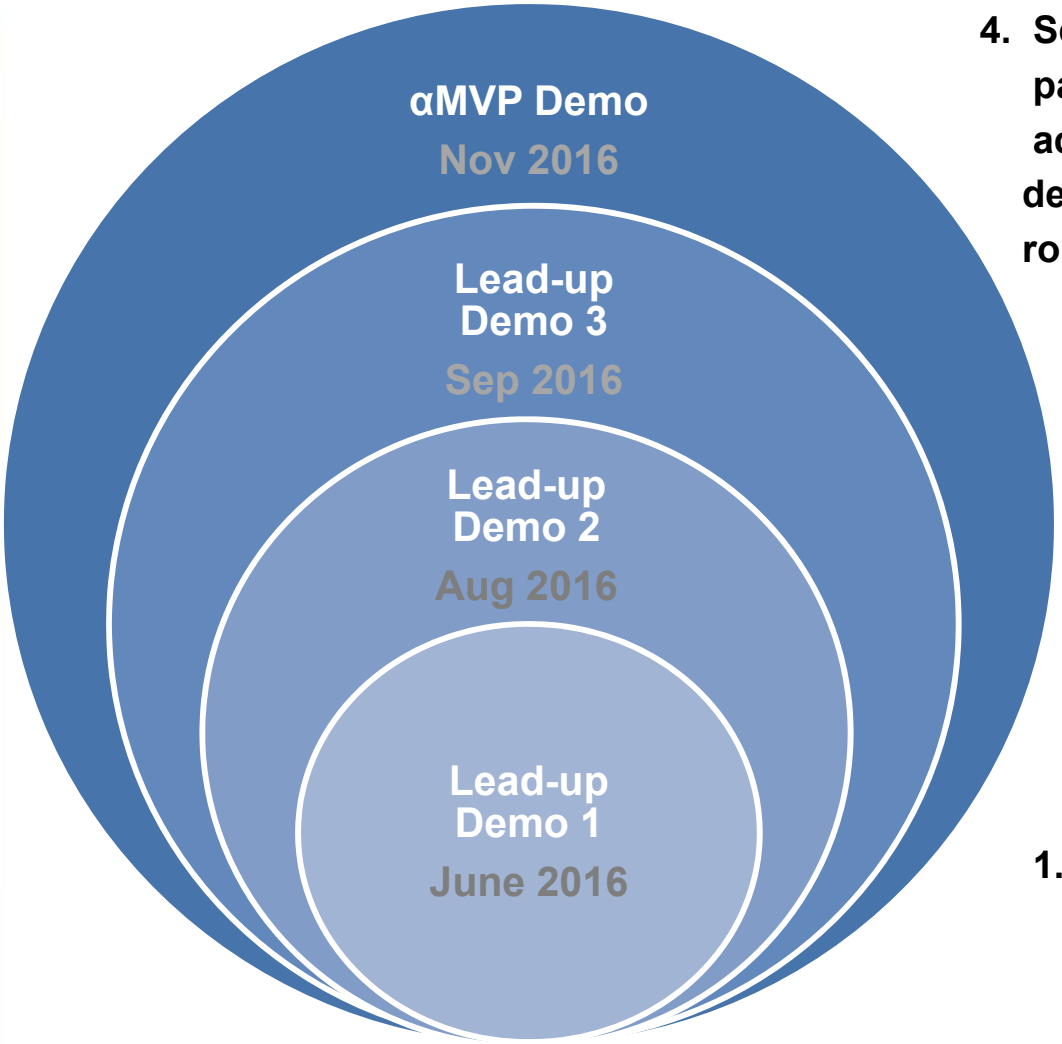
As a result, the quality of capability upgrades may increase as well.



Core OTAP Elements

Open Platform Software Library (OPSL)	• A set of open, commonly available, and standardized data interfaces, exchanges, and formats to enable engineering of 3rd party components (e.g., automated threat recognition algorithms or ATRs) for their seamless integration into a TSE.
Passenger Baggage Object Database (PBOD)	• A database of TSE-scanned outputs (e.g., raw radiography data, reconstructed images) of threats; Information on non-threats; and associated metadata to develop ATR capabilities. PBOD is a single data repository (and possible access to other repositories) made available for industry.
ATR Algorithm *Integration*	• A set of software applications that process TSE signal outputs (e.g., both raw radiography data and image data) to provide assisted or automated decision-support information to TSOs.
3rd Party Hardware Component *Integration*	• Integration of 3rd party specialized hardware components (e.g. upgrades to existing TSE that can provide greater security performance).into an open TSE.

Incremental αMVP Demos



4. **Scan bags with both ATRs chosen per simulated passenger risk "score". ATR provide basic non-accurate threat signal (accuracy to be later developed). Full MVP documentation for all OPSL roles.**

3. **2nd ATR linked to OPSL and utilizes AT scan data. Both ATRs utilized even with manual switching. One ATR developed per PBOD collected data for at least 1 explosive type.**

2. **One ATR linked to OPSL and utilizes scan data from AT. ATR developed using any data available.**

1. **OPSL installed on one AT that can perform basic scan functions.**

Current Status of Work Streams

- OPSL
  - Working w/Rapiscan to modify 620DV OS to be able to read proprietary image file (.rcf) to a non-proprietary format (DICOS) by end of May
  - Implemented Stratovan's DICOS Image Converter Tool on 620DV converting open standard .png files to DICOS format
  - On schedule to demo OPSL as part of Lead-up Demo 1
  - Initial ATR API code and documentation complete
- PBOD
  - C4 threat article, bag set and database complete by end of May.
    - ~300 threat images fully labeled with ground truth (100% completed)
    - ~1000 non-threat images (50% complete)
  - Moving on to sheet explosive and other military, commercial and HME explosive types
  - Beginning CT scans of C4 by end of May
  - PBOD process and app complete

Policy Considerations

- OTAP is a prototyping project and does not represent a change to TSA's current technology acquisition policy
- The OTAP experience and lessons-learned will inform policy
- The goal - create new ways to reward innovation and therefore sustain a healthier and more diverse vendor market.

- OTAP's goal of creating an open system architecture is one effort (out of multiple) pursued by TSA to enable ***the broadest possible range of technologies and business models to flourish***.
- ***A wider variety of vendors will more easily, quickly, and reliably be able to create capability upgrades (e.g. detection algorithms)*** across the TSE fleet at lower cost to both vendors and TSA.

Backup Slides

Value Propositions

TSA

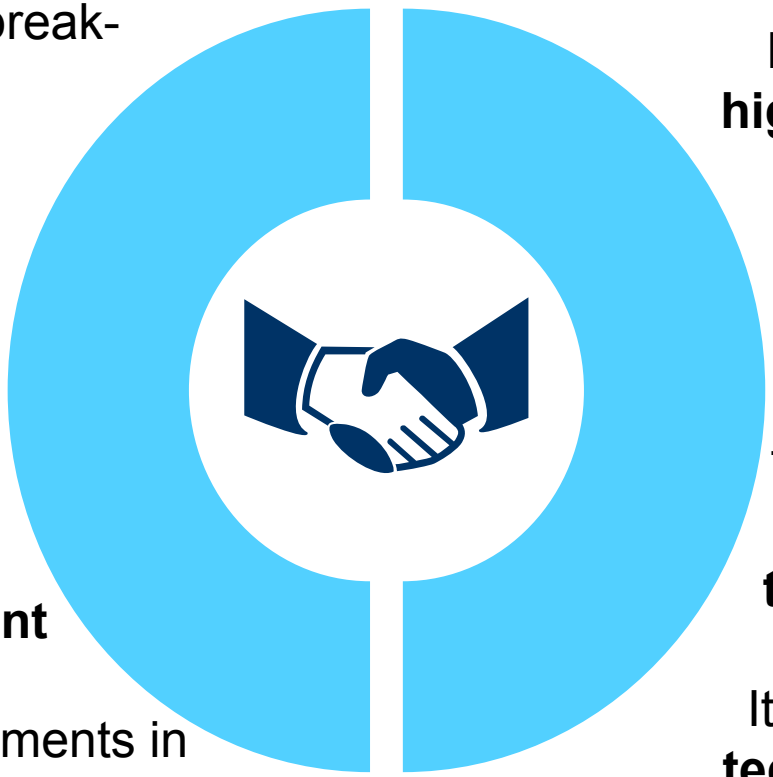
More capability advances, quicker to mature and at lower lifecycle cost

Analysis of best modular break-points helps define system architecture

Modular TSE interfaces **increase vendor access** to TSA market

Whatever Congress appropriates, TSA gets **more capability per $ spent**

Implements explicit commitments in **OSC Strategy, TSA 5-yr Tech Investment Plan,** & by **OMB/DHS**



Industry

More frequent, predictable and viable business opportunities with TSA

Modularity leads to **steadier high-margin revenue stream**

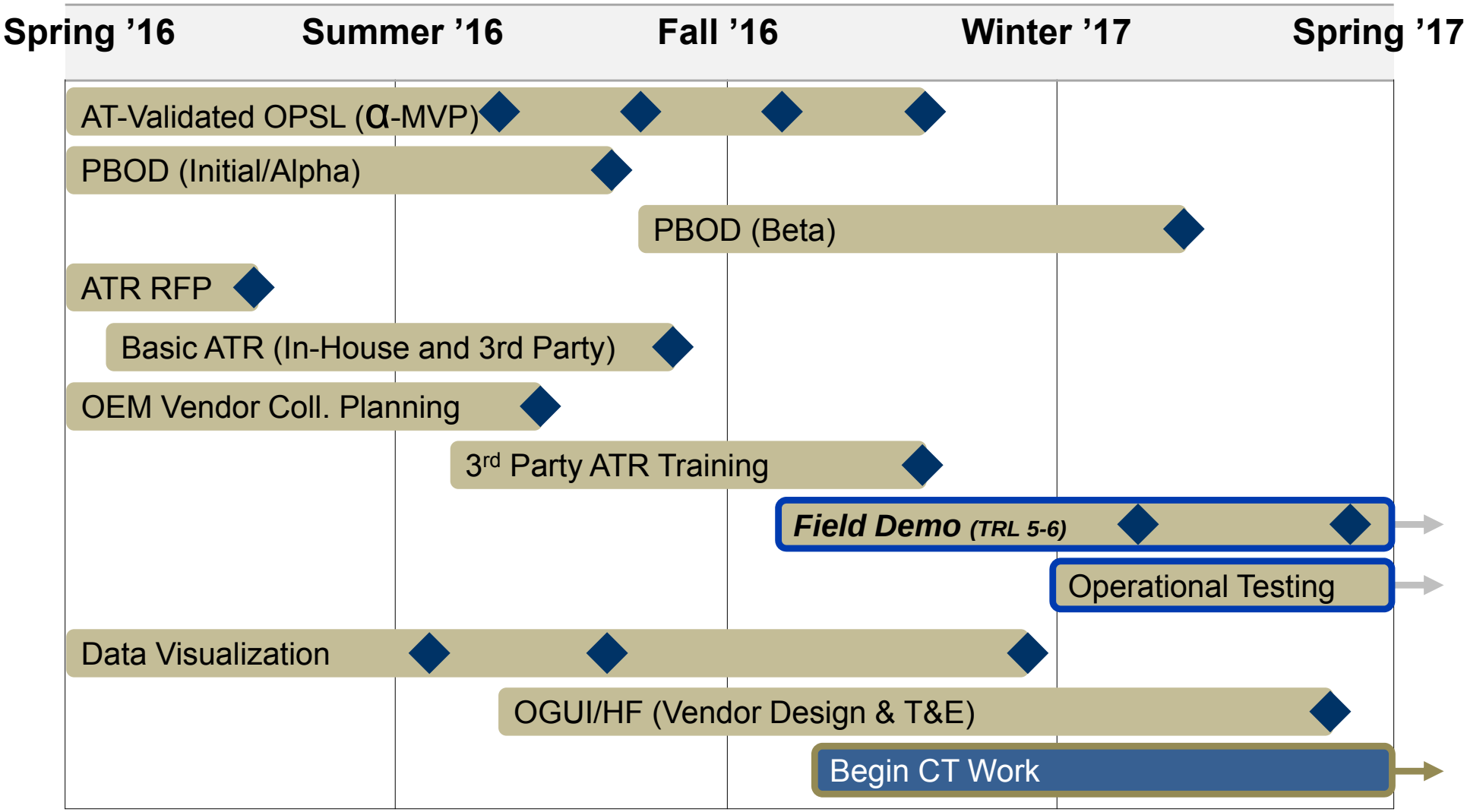
Access to **threat scan dataset** enables better, quicker sys. development

TSA-provided middleware & SDK **reduce barriers to entry** in TSA marketplace

Iterative prototyping **reduces technical risk, time and cost during T&E**

OTAP can create value for TSA and a more-vibrant security vendor industry

OTAP 18 Month Milestone Estimate



RFQ Evaluation Summary

Sandia RFQ #577847, **X-ray Radiography Hardware System**, was issued on November 18, 2015 and closed on December 26, 2015.

Six companies will receive awards to the RFQ.

EDS / CT Systems

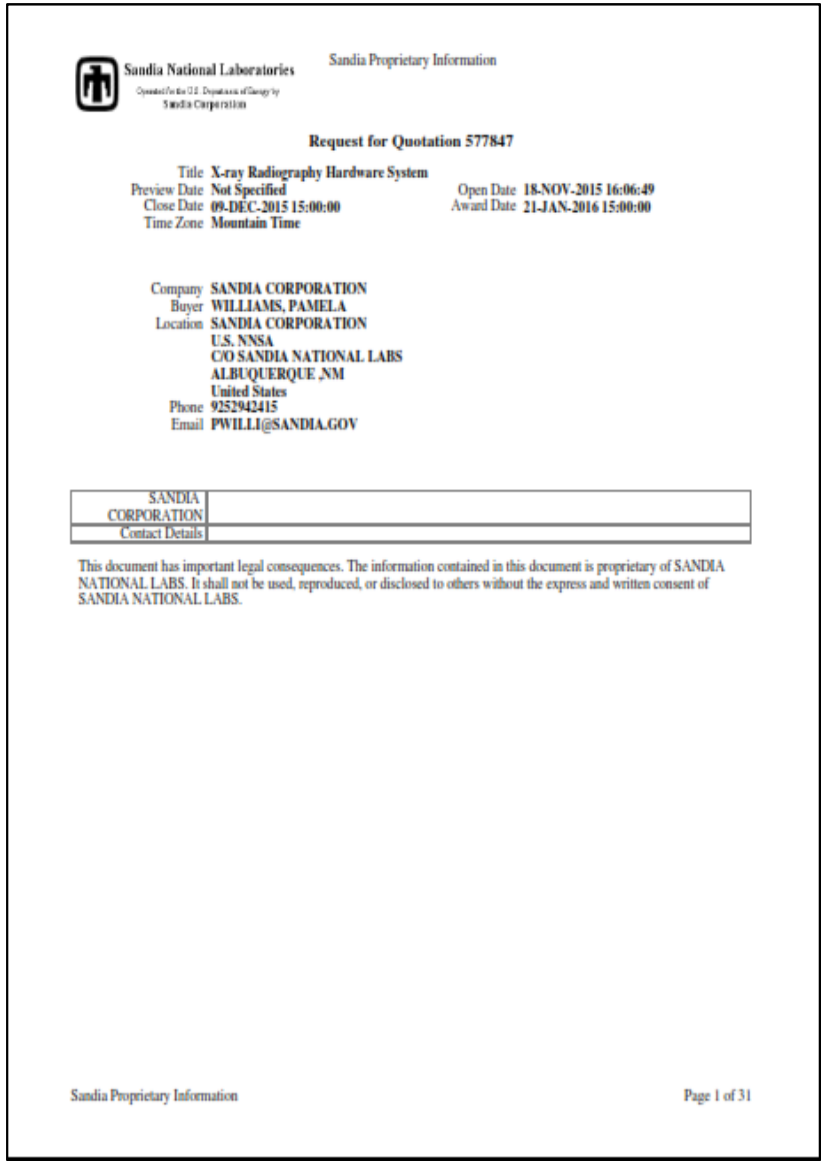
- IDSS (Checkpoint CT)
- 2 Additional (Awards in process)

AT Systems

- Rapiscan
- ScanTech
- 1 Additional (Award in process)

Additional awards to OEMs expected in **April 2016**

Two upcoming RFQs for software and hardware *components*



Sandia National Laboratories

Sandia Proprietary Information

Request for Quotation 577847

Title **X-ray Radiography Hardware System**
Preview Date **Not Specified**
Close Date **09-DEC-2015 15:00:00**
Time Zone **Mountain Time**
Open Date **18-NOV-2015 16:06:49**
Award Date **21-JAN-2016 15:00:00**

Company **SANDIA CORPORATION**
Buyer **WILLIAMS, PAMELA**
Location **SANDIA CORPORATION**
U.S. NNSA
C/O SANDIA NATIONAL LABS
ALBUQUERQUE ,NM
United States
Phone **9252942415**
Email **PWILLI@SANDIA.GOV**

SANDIA CORPORATION	
Contact Details	

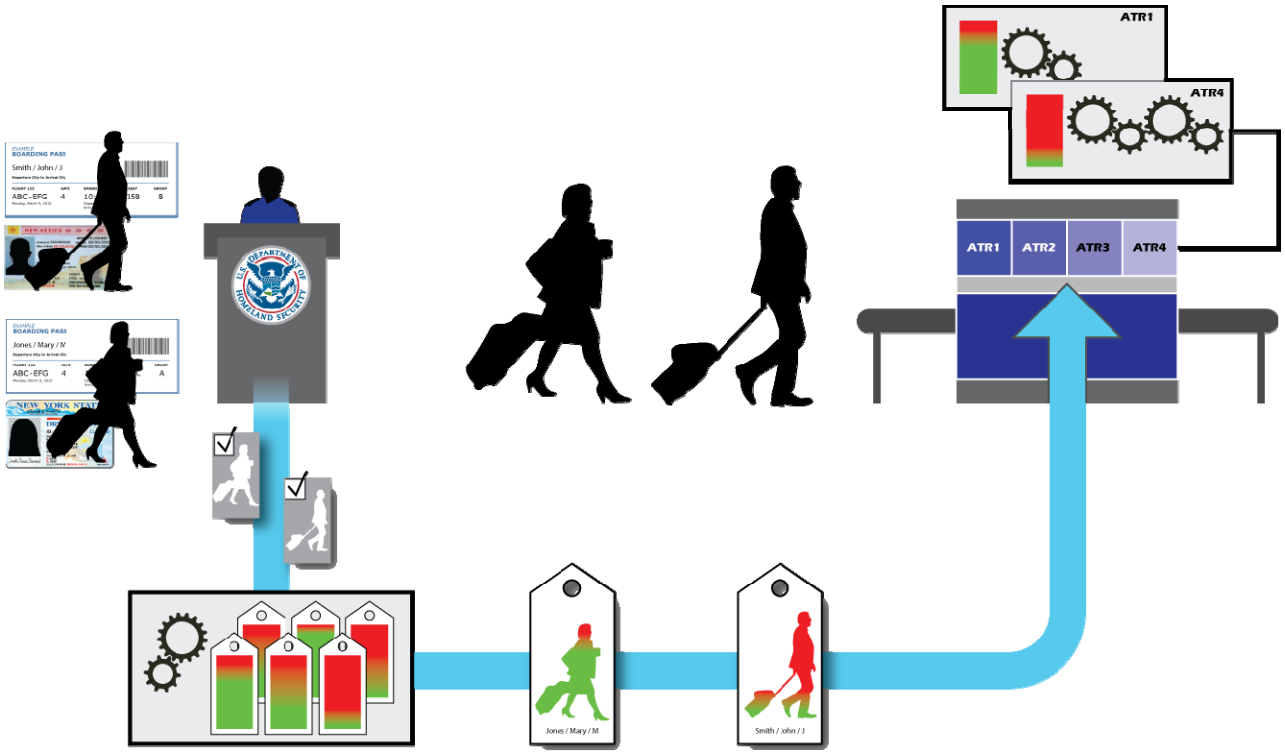
This document has important legal consequences. The information contained in this document is proprietary of SANDIA NATIONAL LABS. It shall not be used, reproduced, or disclosed to others without the express and written consent of SANDIA NATIONAL LABS.

Sandia Proprietary Information

Page 1 of 31

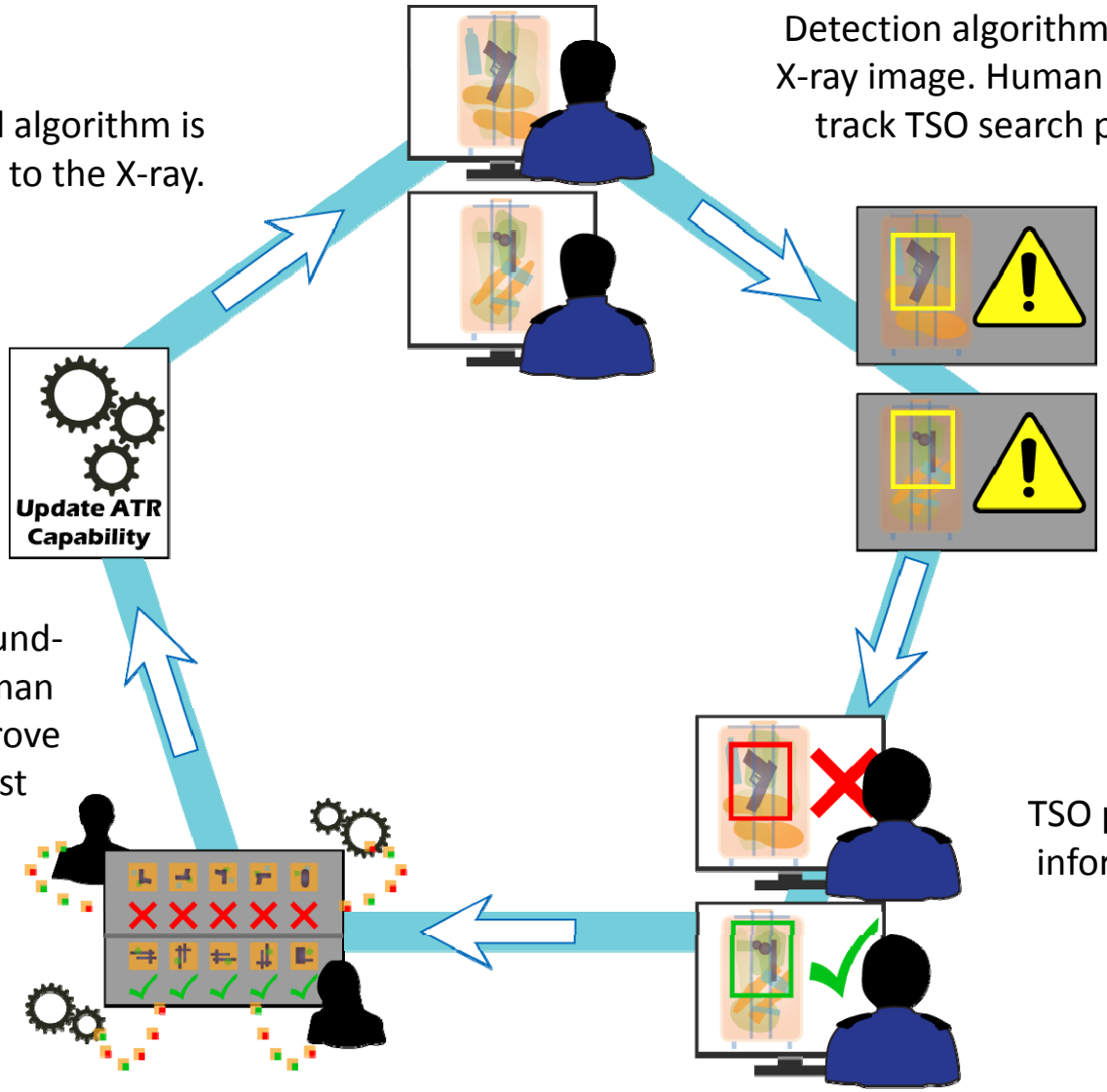
Open Systems Architecture ➔ Modularity ➔ CONOPs Flexibility

Beyond modularizing equipment, an open architecture that utilizes OTAP, STIP, and other communication standards, can also support different CONOPs and screening workflows such as Risk Based Screening (RBS) since communication between sensors will be standardized. Such flexibility would even be possible in the same physical configuration.



Greater flexibility at the CONOPs level can allow for improved efficiencies at a system-of-systems level. The TRAP project can allow for experimentation and validation of potential new CONOPs

Continuous ATR Improvement



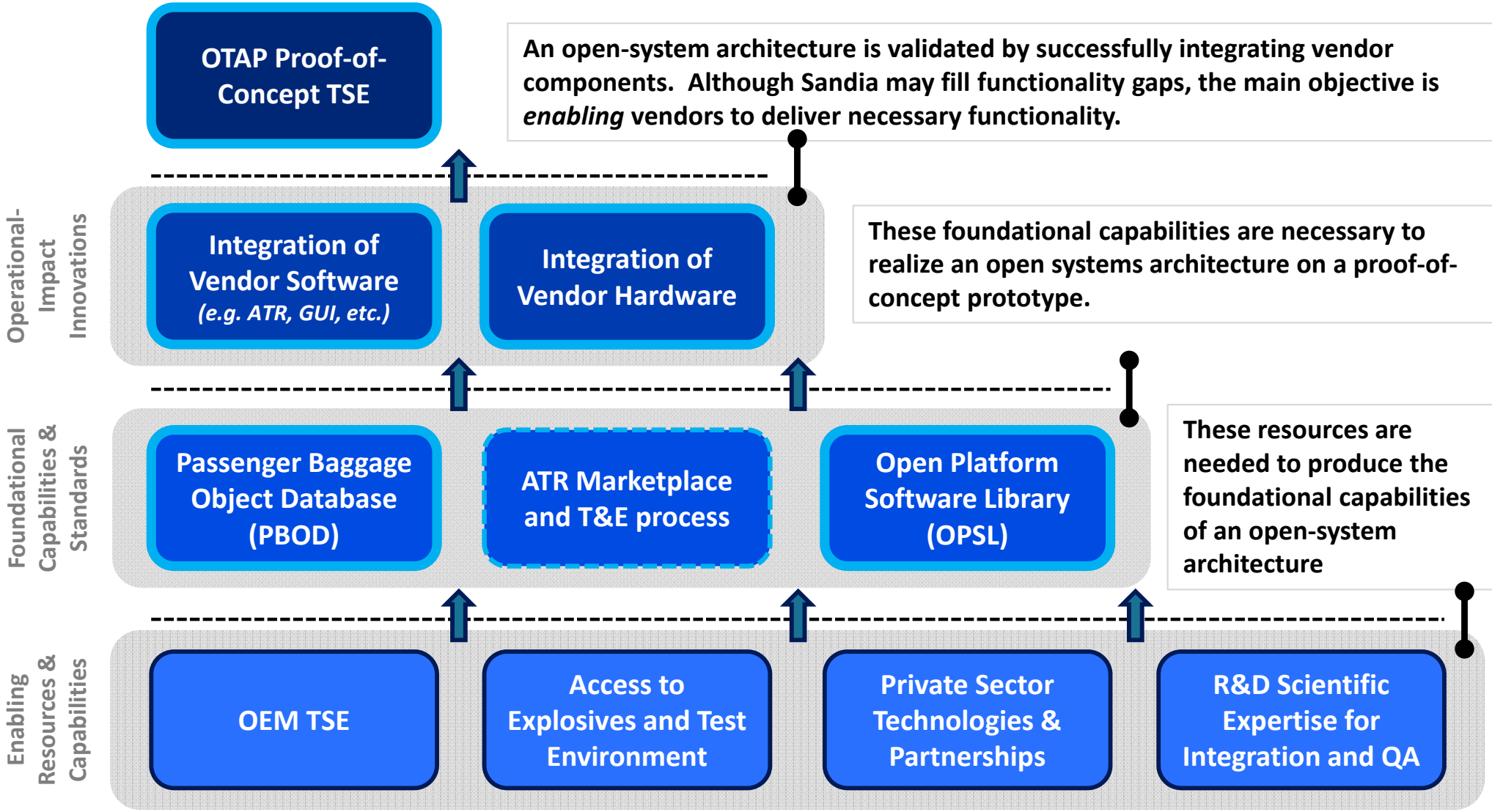
Improved algorithm is deployed to the X-ray.

Detection algorithms annotate the X-ray image. Human factors metrics track TSO search performance.

Developers use the ground-truth data sets and human factors research to improve the threat-detect assist algorithms.

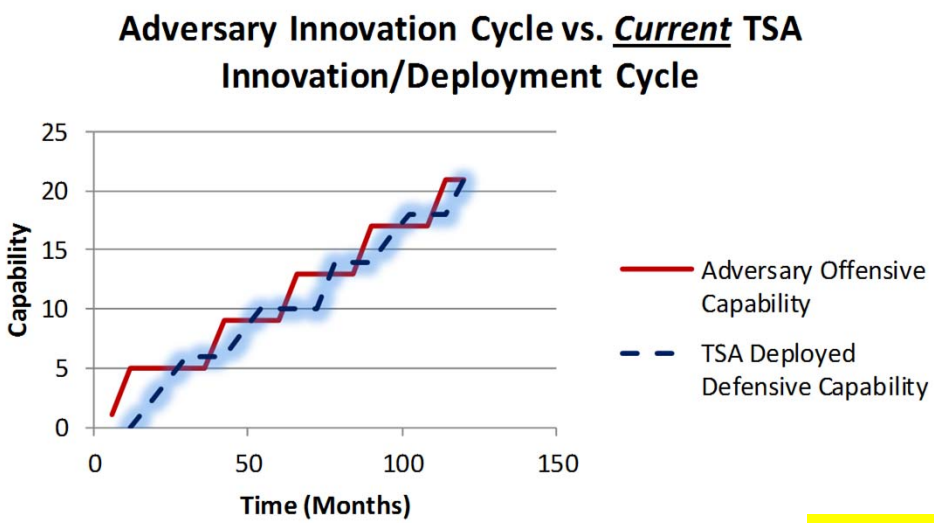
TSO provides ground-truth information to the image.

OTAP Foundational Elements



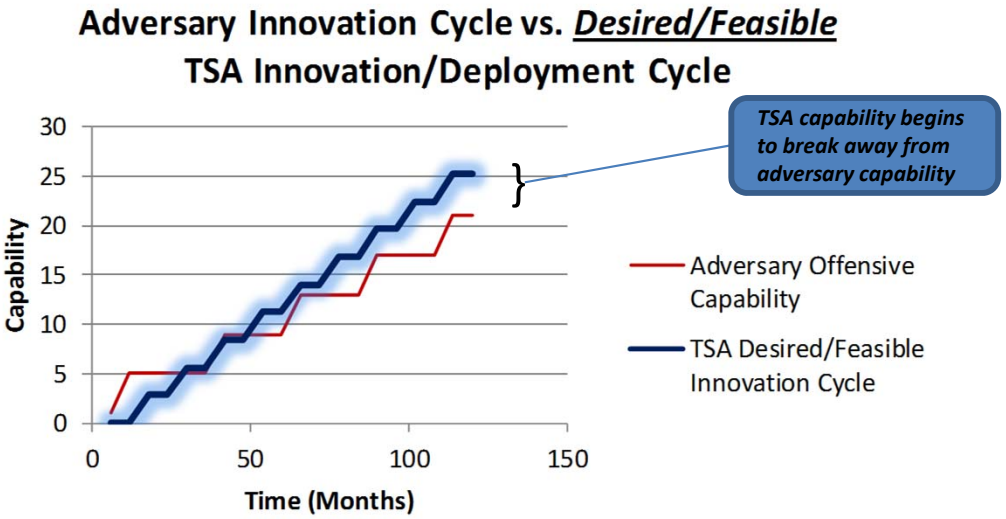
OTAP Goal: Build an open-system architecture that can a) successfully incorporate vendor capabilities, b) withstand the rigors of live operations, c) have a sustainable business model

Speeding the Innovation Cycle



Current proprietary, fully integrated technology architectures result in the need to purchase systems that evolve only as fast as the slowest innovating component in the system ➔ TSA capabilities are just keeping lockstep with adversary capabilities.

Notional Data



An open architecture that fully decouples software from hardware allows innovation to occur at the speed of software *(and available training data)* ➔ More rapid innovation cycles can allow TSA capabilities to gain ground and then exceed adversary capabilities…perhaps at lower cost.