SAND2016-7847C

Open Threat Assessment Platform (OTAP)

Overview

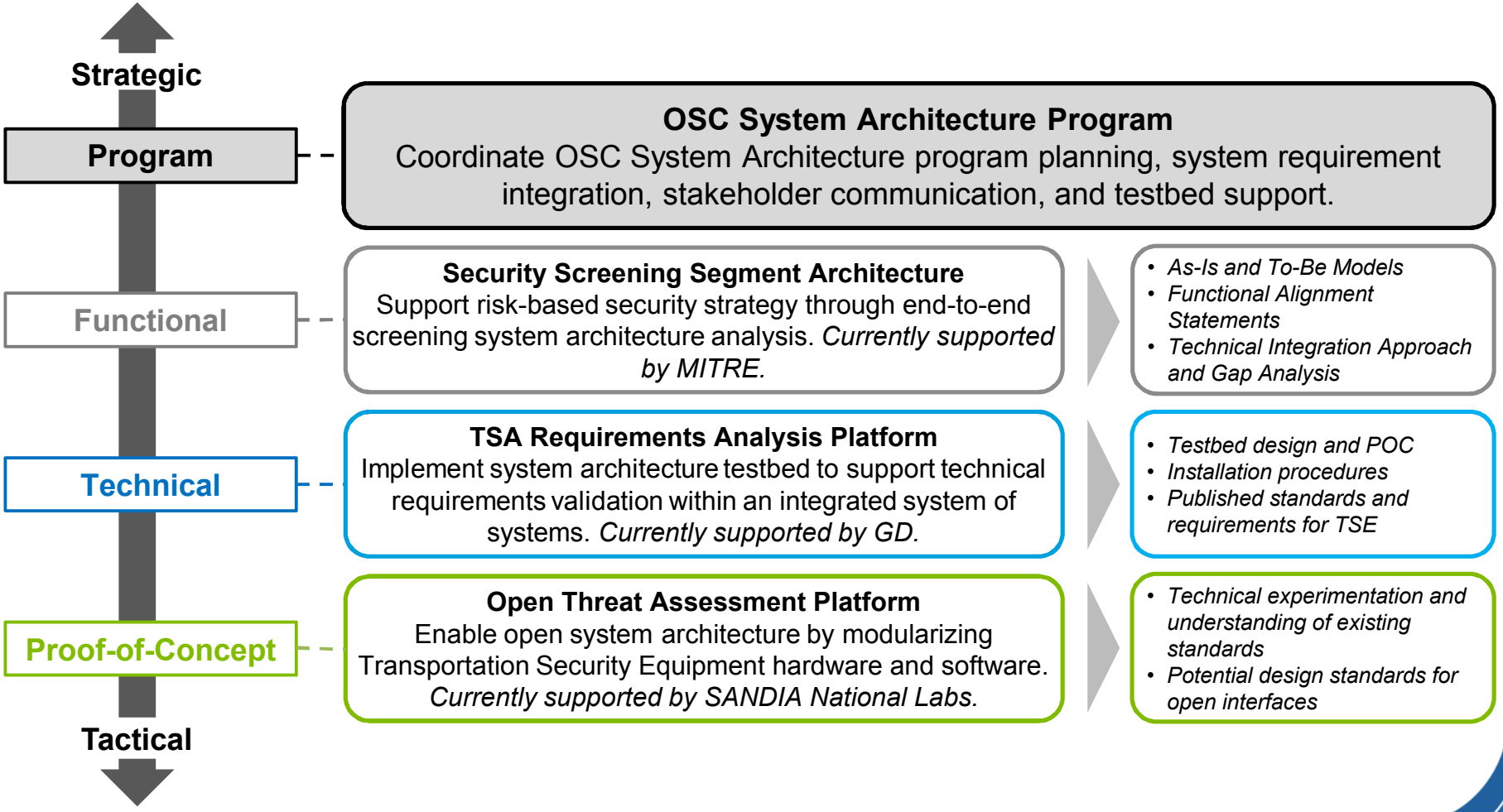
Overview

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

An “open” platform is defined as a technology platform that utilizes a “plug-and-play” or open architecture based on standardization of data formats, interfaces, and protocols that allow for the modularization of a technology platform.

OTAP Part of TSA Systems Architecture Efforts

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



Core OTAP Elements

Open Platform Software Library (OPSL)

- A set of open, commonly available, and standardized data interfaces, exchanges, and formats. OPSL will serve an interface to enable engineering of 3rd party components (e.g., threat recognition algorithm) for their seamless into a passenger baggage screening system. An open platform can be described as enabling a plug-and-play system not unlike third-party apps developed for smart-phones.

Passenger Baggage Object Database (PBOD)

- A database of X-ray-scanned outputs (e.g., raw radiography data, reconstructed images) of potential threats identified based on intelligence and analysis; information on non-threats; and any associated metadata that is used to train or build ATR capabilities. The purpose of PBOD is to contain in a single repository (or to make available to other authorized depositories) data that can be used to train algorithms for vetted vendors.

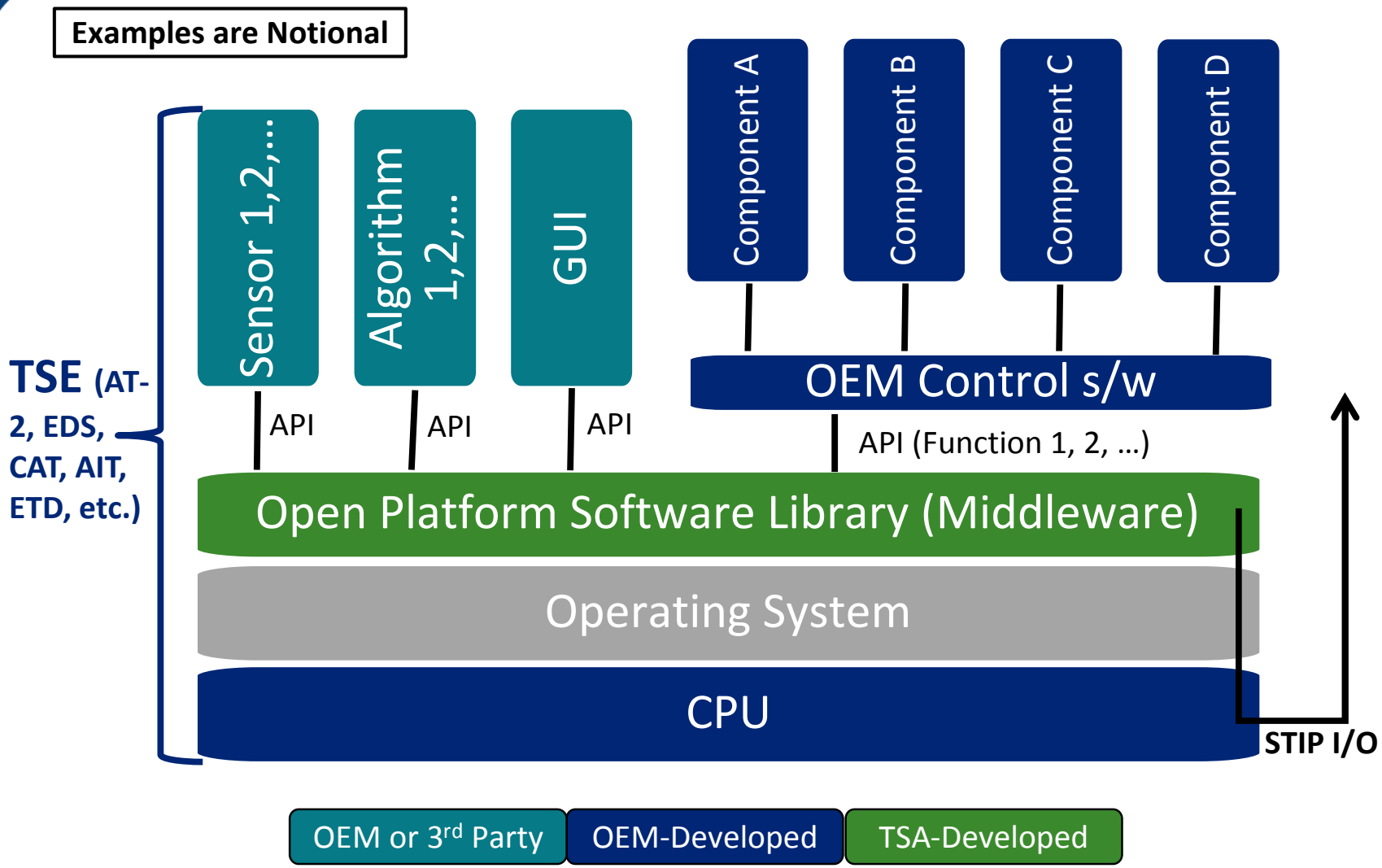
ATR Algorithm *Integration*

- A set of software applications that process the various signal outputs (e.g., both raw radiography data and image data) of the X-ray scanner to provide assisted or automated decision-support information to TSOs.

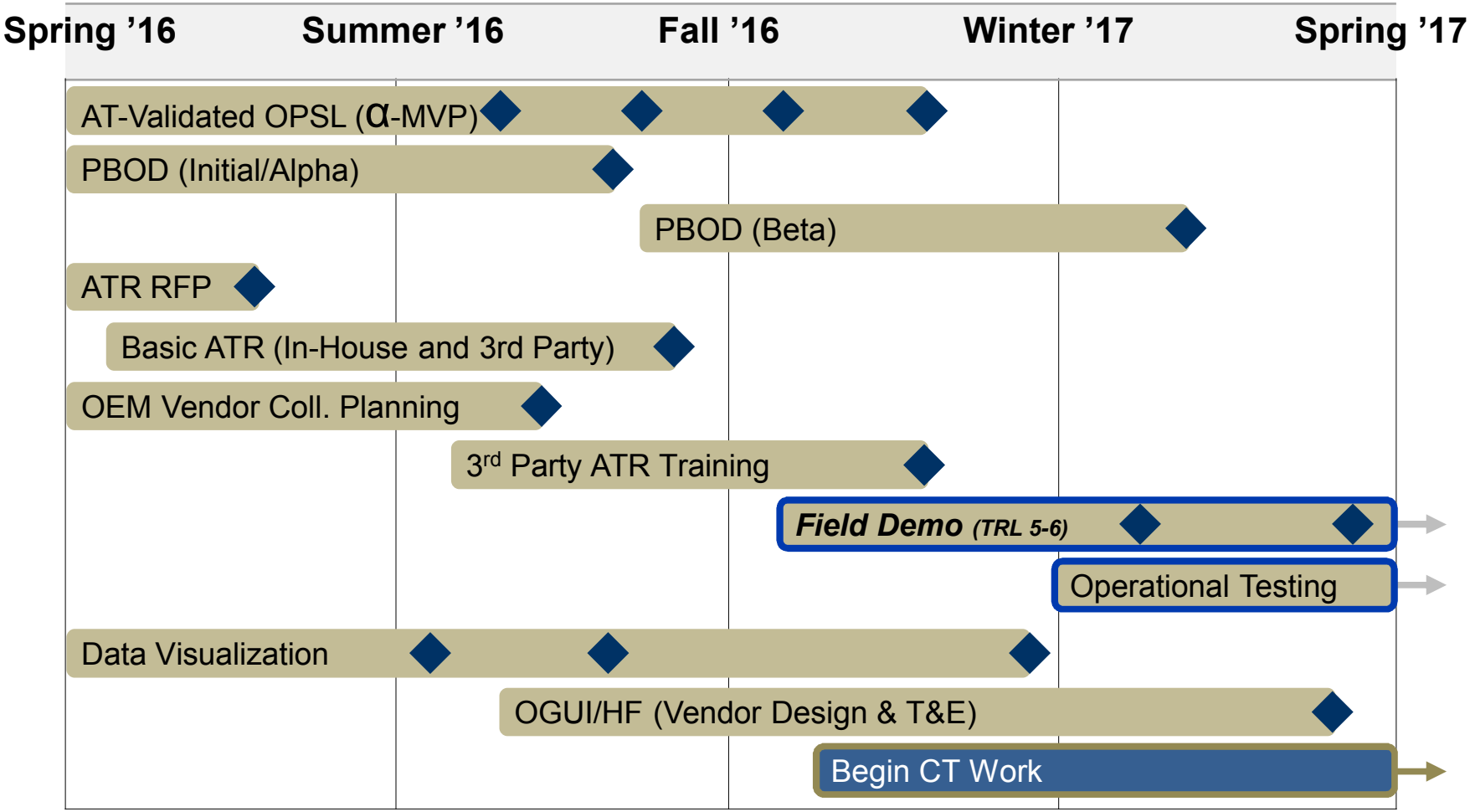
3rd Party Hardware Component *Integration*

- Integration of 3rd party specialized hardware component on an OTAP-enabled system. 3rd party hardware components could be potential upgrades to existing screening equipment that may provide greater security performance.

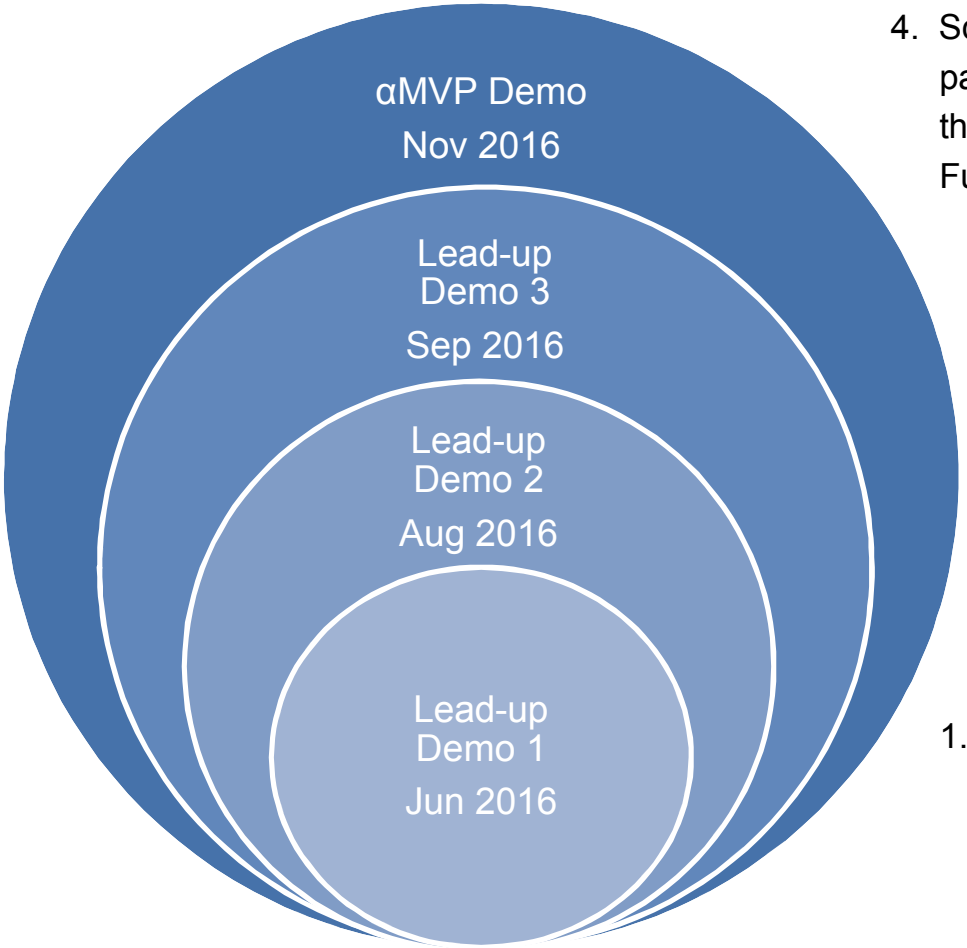
OTAP Software Enables Plug-and-Play



OTAP 18 Month Milestone Estimate



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.

Policy Considerations

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

- ❑ OTAP's goal of creating an open architecture is one effort 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.

Incentivizing Innovation

- While the technology that enables OTAP to be an open architecture will be non-proprietary or freely shared, **Original Equipment Manufacturers (OEMs) and *3rd party applications (hardware or software) could be proprietary or non-proprietary to ensure market rewards for innovation for different technology business models.***

- An open architecture will allow 3rd party vendors to easily develop and implement capability upgrades because they can utilize a stable, well-designed interface implemented on screening technology.

Risks & Mitigations

- Risks
  - Ensuring OPSL software can work across different OEM platforms without impacting speed.
  - Ensuring implementations on OEM platforms are easy and consistent.
  - Cyber security concerns

- Mitigations
  - Frequent, iterative field testing to validate requirements and surface hidden assumptions
  - Building cyber security into architecture up-front

Backup Slides

Value Propositions

TSA

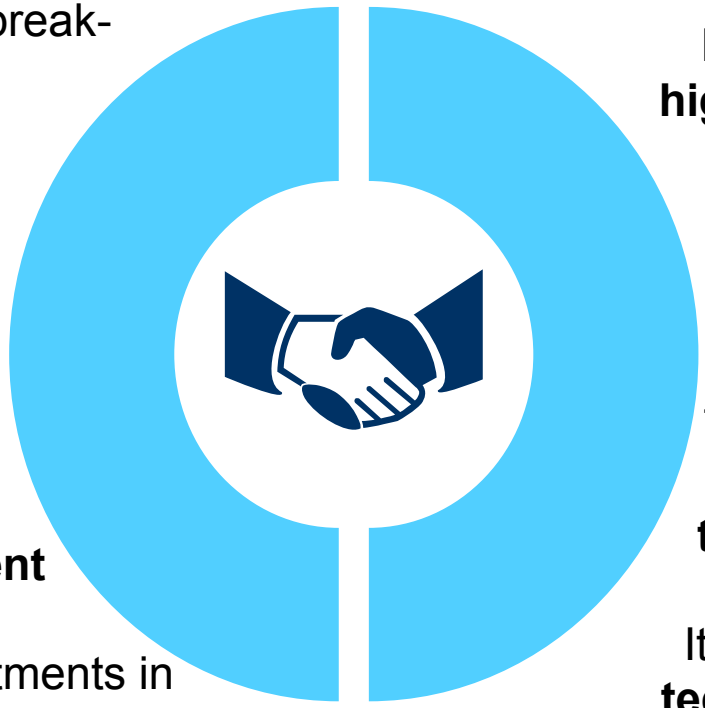
More capability advances, quicker to mature and at lower lifecycle cost

Analysis of best modular break-points helps define system architecture

Modular TSE interfaces **increases 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 **reduces 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

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

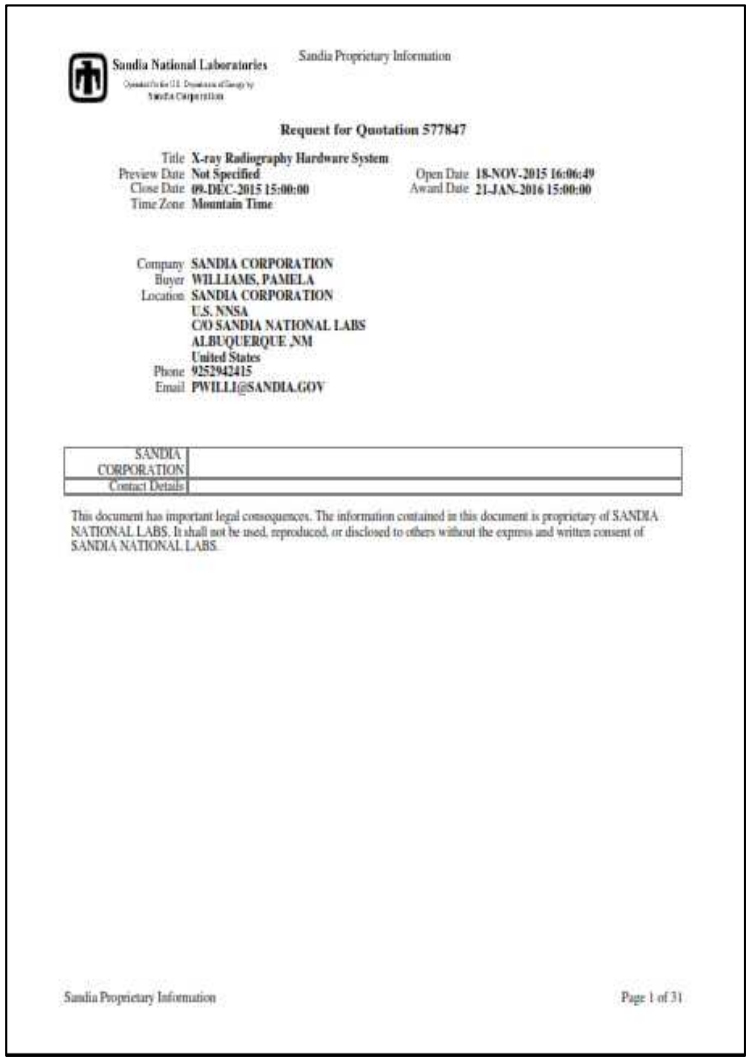
- 3 Companies (Awards in process)

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

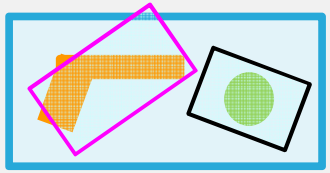
Prototype Concept

Develop API to a non-proprietary X-ray to decouple the hardware sensor and detection algorithm.

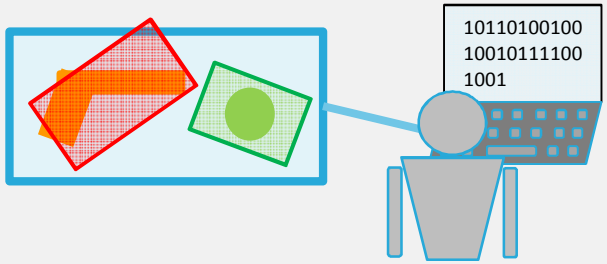
API

- Get_image()
- Get_data()
- Move_belt()
- Stop_belt()
- Annotate_image()
- …

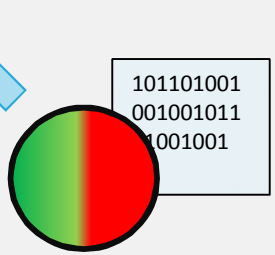
Detection algorithms annotate the X-ray image. Human factors metrics track TSO search performance.



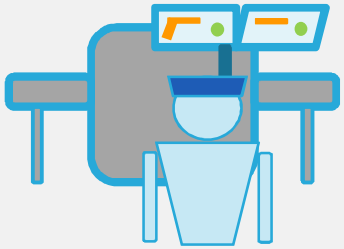
TSO provides ground-truth information to the image.



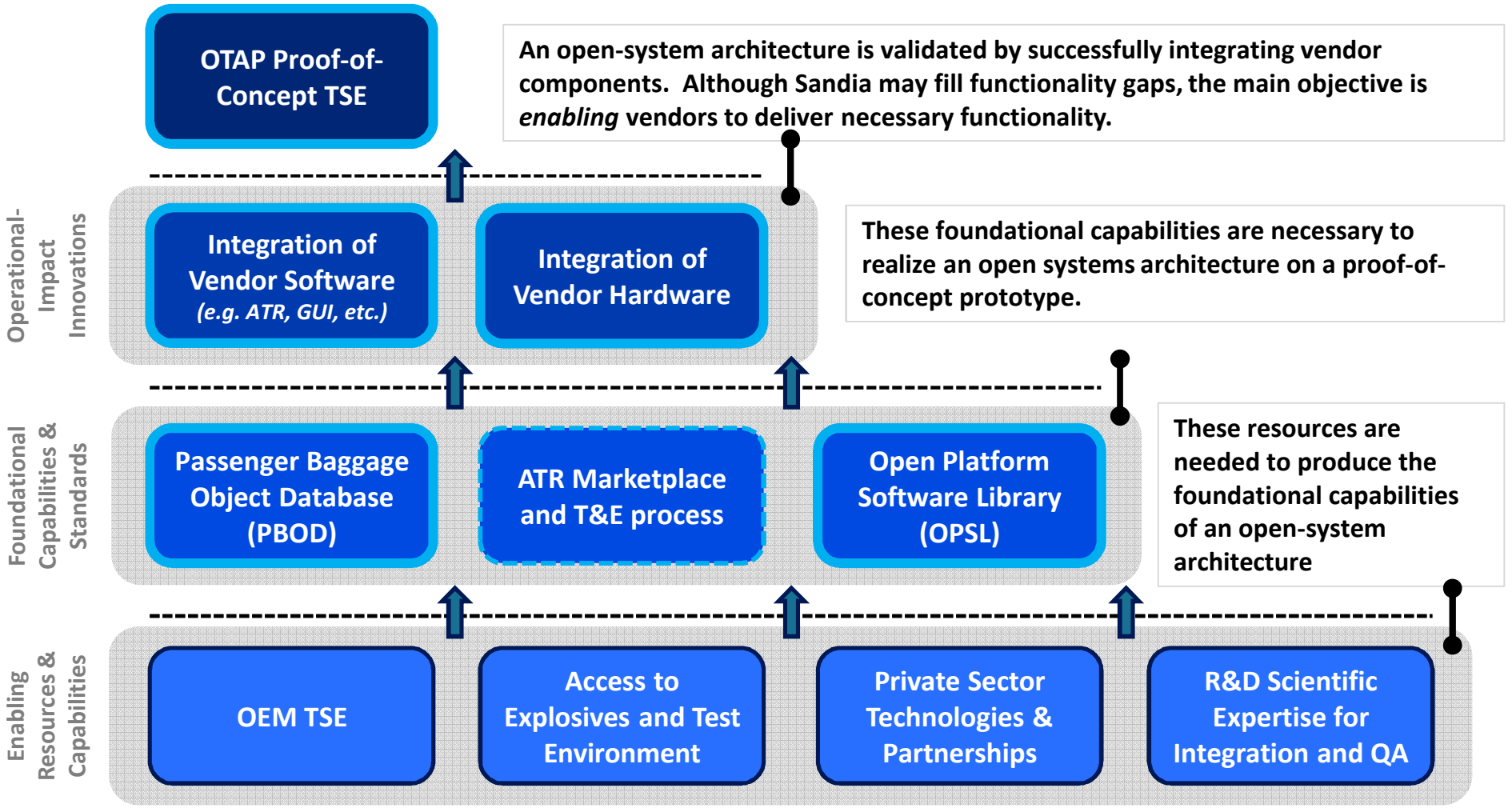
Developers use the ground-truth data sets and human factors research to improve the threat-detect assist algorithms.



Improved algorithm is deployed to the X-ray.

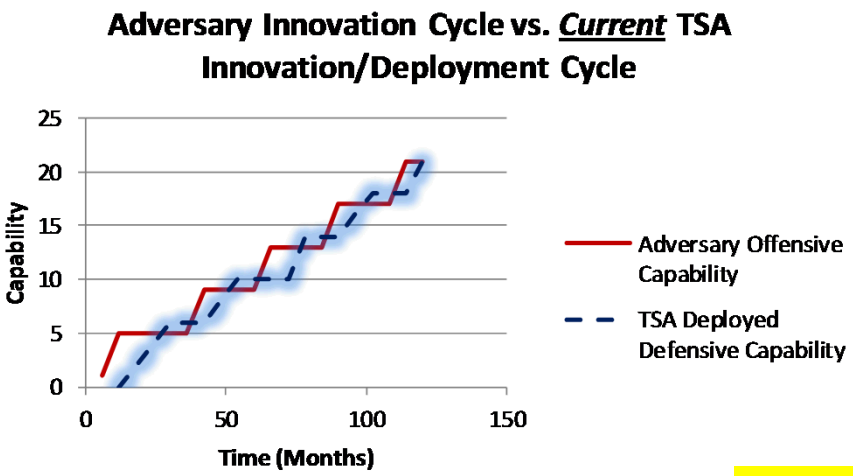


OTAP Foundational Elements



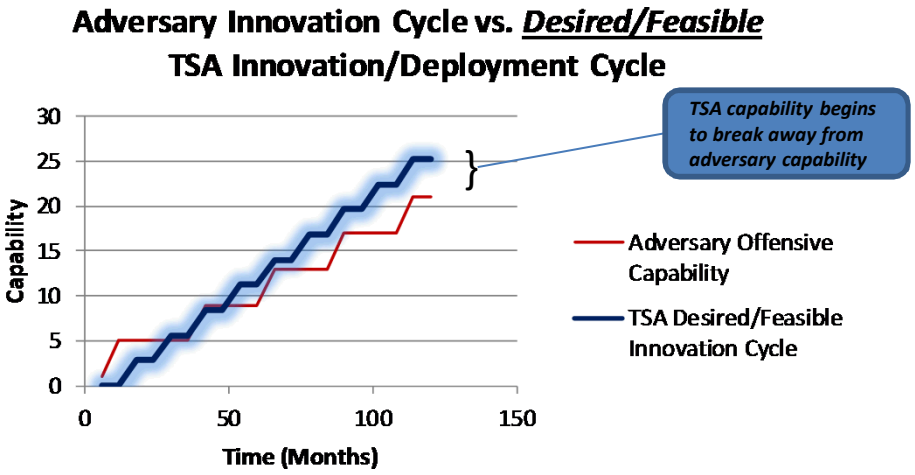
OTAP Goal: Build an open-system architecture that can a) successfully incorporate vendor capabilities, b) withstand the rigors of live operations, c) have a sustainable business model

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 is 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.