Simulators Common Architecture and Requirements (SCARS)

16 Apr 2025

Lt Col Virmil Delgadillo, Materiel Leader, Operational Training Infrastructure

Mr. Michael Baker, Chief Engineer, SCARS

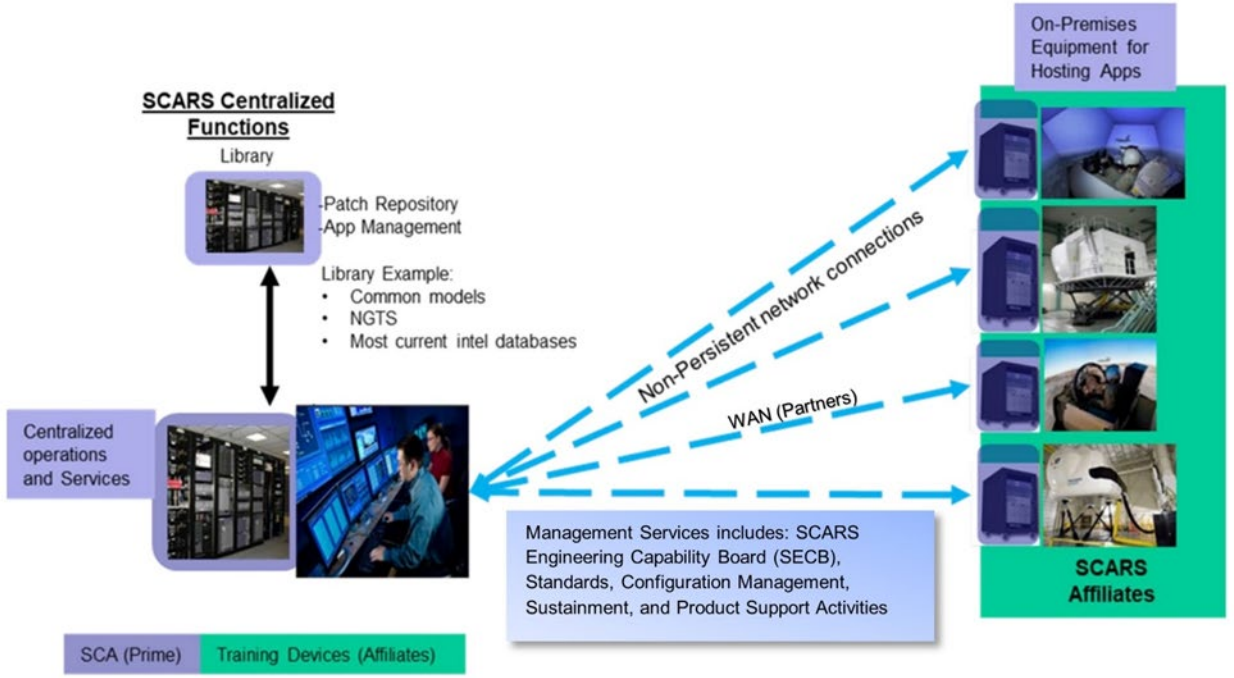
Agenda

- Overview
- Background
- Simulator Common Architecture Requirements and Standards (SCARS) Key Components
- Three Phased Approach
- SCARS Standards
- What Industry Can Do for SCARS

Overview

DELIVERING THE SKILL TO KILL

- Program Sponsor: HAF/A3T
- Supported MAJCOMs: ACC, AFGSC, AFRC, AFSOC, AMC, PACAF, USAFE
- Purpose: SCARS is a sustainment initiative to incrementally establish a Modular Open Systems Approach (MOSA) for Air Force simulators that leverages applications, supports efficient and rapid updates to capabilities, evolves with cybersecurity threats and controls, and minimizes life cycle costs.
- Acquisition pathway: Sustainment Initiative
- Prime vendor: CAE USA
- Contract attributes: IDIQ
  - 5-yr base ordering period (2020-2025) + 5 1-yr options (2025-2030)



Background – USAF OTI Problem Statement

DELIVERING THE SKILL TO KILL

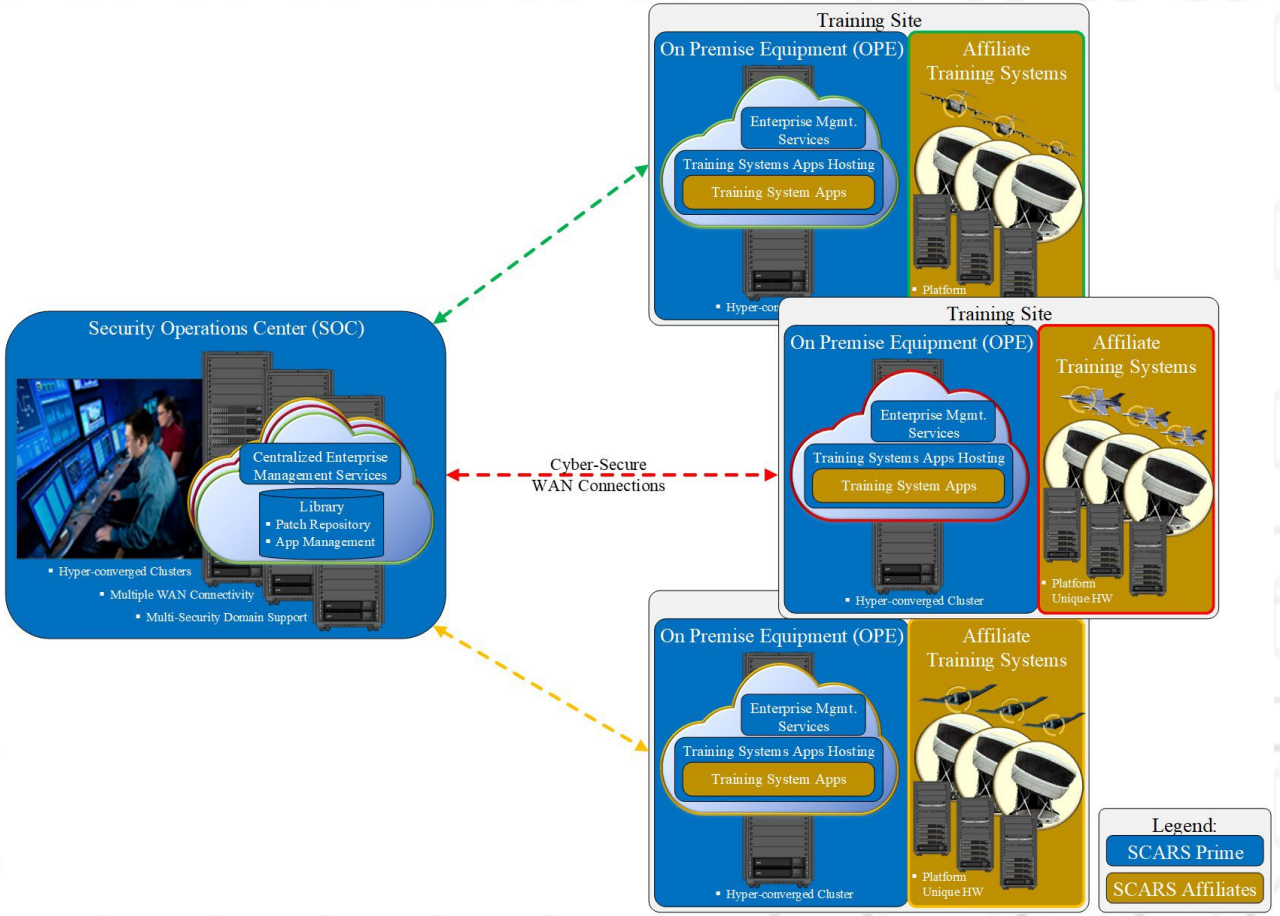
- Large base of training devices with disparate configurations – very limited reuse
  - Over 2400 training devices (50+ platforms) supporting 9 MAJCOMs
  - Uniqueness of devices requires costly unique development, production and support
- Cyber threats are continuous, evolving, & increasing in frequency and severity
  - AF Training Systems must comply with DoD Risk Management Framework (RMF)
  - Implementing RMF is costly to sustain (scans) and implement changes (patches)
- Demand on training systems is increasing – higher fidelity and greater interoperability
  - Training effectiveness is limited by the lack of standards and common architectures within the training device

New Approaches are Necessary to Efficiently Move Forward and Support the Warfighter

SCARS Key Components

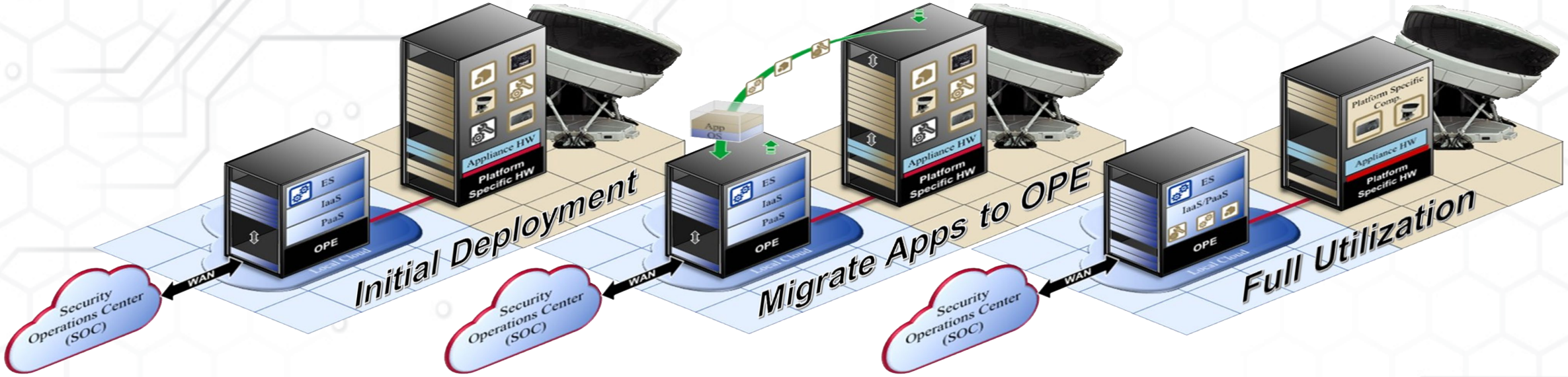
DELIVERING THE SKILL TO KILL

- Security Operations Center
  - Remote management of OPE and SCARS WAN
  - Dashboard for central management and enterprise view
  - SCARS Help Desk
- On-Premise Equipment (OPE)
  - Local cloud for hosting simulation applications
  - Scalable
  - Common security controls
  - Works with any WAN
- Wide Area Network (WAN)
  - Utilizing existing partner networks, if available
  - SCARS WAN currently in proof-of-concept phase
- Training Systems with approved ATOs
  - No ATO, no SCARS
- SCARS Standards
  - Key to establishing common architecture



Three Phased Approach

DELIVERING THE SKILL TO KILL



PHASE 1: EFFICIENT CYBERSECURITY

- Provide centralized cyber-maintenance for vulnerability scans, patches, anti-virus, & enterprise-wide RMF controls
- Common Cyber Tools
- Centralized Scanning/Patching of trainer devices

WARFIGHTER BENEFIT: *Significantly reduced trainings system down time for maintenance and faster ATOs*

PHASE 2: COMMON ARCHITECTURE

- Majority of functionality for training systems moved to a common infrastructure
- New technologies support a complete migration to cloud/virtual computing
- Common modeling and interfaces
- Virtualize software that is not hardware dependent

WARFIGHTER BENEFIT: *Reliability improved, minimized maintenance, and reduced cost of functional improvements*

PHASE 3: STANDARD APPLICATIONS

- Training systems embrace common applications
- Common infrastructure for application hosting
- Only software that can't be virtualized is trainer specific
- Extensive Common Models

WARFIGHTER BENEFIT: *Application re-use across platforms and consistent performance enhances "fair fight"*

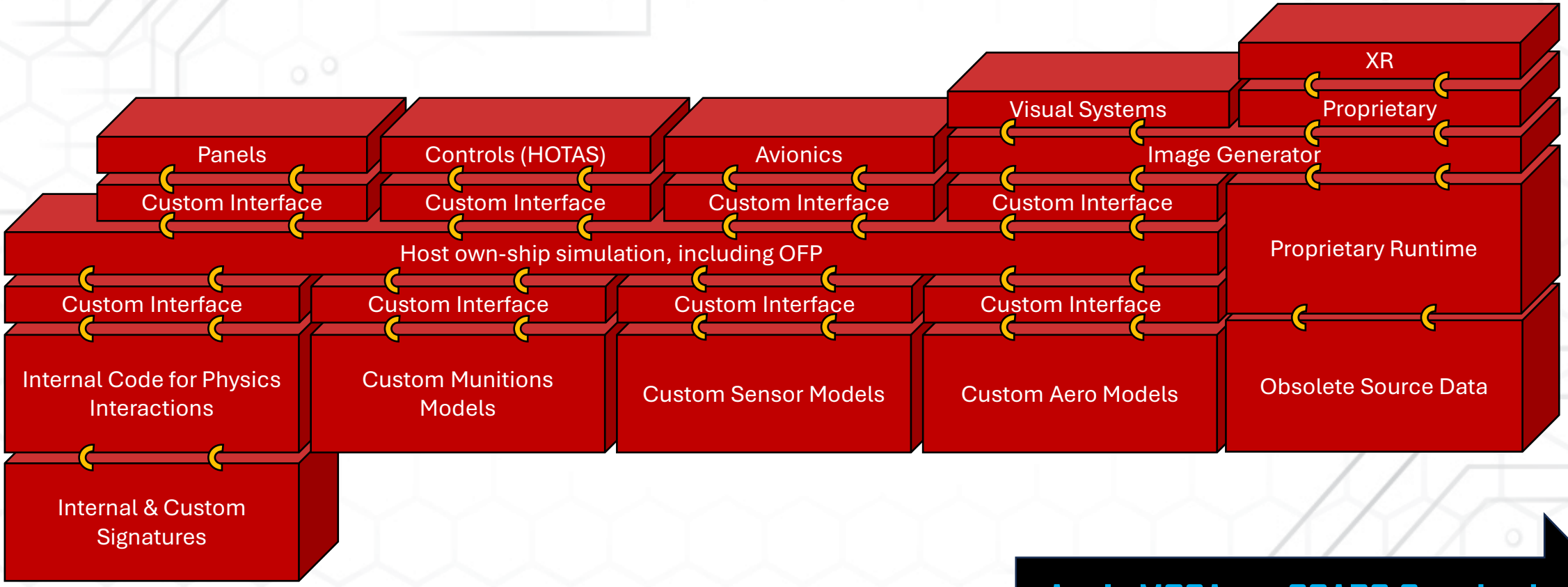
SCARS Standards

DELIVERING THE SKILL TO KILL

- SCARS develops standards for training simulator architecture focused on internal interfaces and architectures
- Standards informed by Requirements and Objectives, and governed through SCARS Engineering Capabilities Board
- Standards published annually – SCARS provides funds to training system programs for standards implementation
- Once implemented and verified through testing, training system is connected to SOC

Before Implementation of SCARS Standards

DELIVERING THE SKILL TO KILL

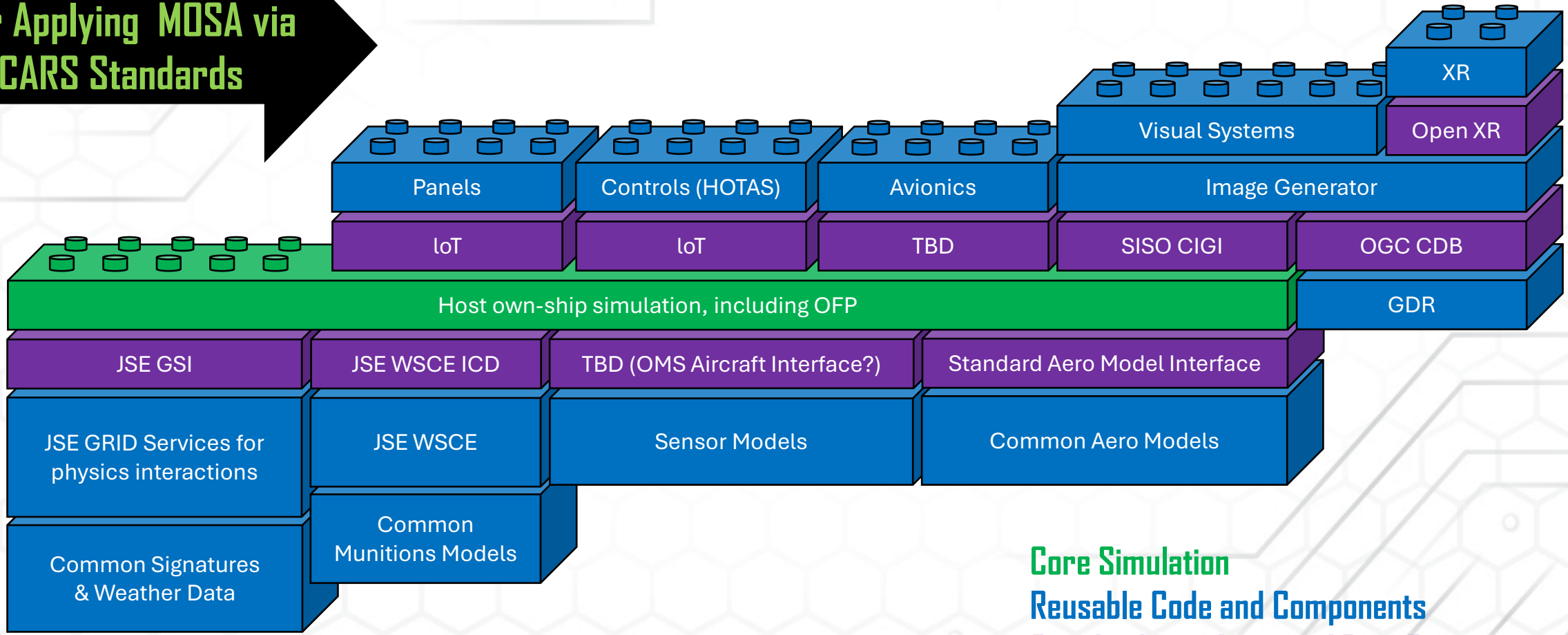


Apply MOSA via SCARS Standards

With SCARS Standards

DELIVERING THE SKILL TO KILL

After Applying MOSA via SCARS Standards



Core Simulation

Reusable Code and Components

Standard Interfaces and Data Formats

Examples of Industry Standards Embraced by SCARS

DELIVERING THE SKILL TO KILL

- Open Geospatial Consortium (OGC) Common Database (CDB)
  - Mandated as interchange format with various minimum specifications
- Simulation Interoperability Standards Organization (SISO) Common Image Generator Interface (CIGI) SISO-STD-013
  - Mandated as interface between simulations and image generators
- Internet of Things (IoT)
  - Mandated for interfaces between simulations and aircrew control systems
- ARINC-610C
  - Mandates specific common simulator functions when using aircraft parts in simulators
- Object Management Group (OMG) System Modeling Language (SysML)
  - Mandated for Model Based Systems Engineering

SCARS Standards

DELIVERING THE SKILL TO KILL

- Basic On-premise Equipment Integration Standard
  - ICD for Integrating training systems with SCARS OPE
- Common Security Controls Standard
  - ICD for training systems to benefit from SCARS-provided cybersecurity controls
- Certification Process Standard
  - Process to test training systems for compliance with SCARS standards
- Application Certification Standard
  - Processed to certify and field training system software with SCARS OPE
- Data Standard
  - ICD of standard data formats for training systems
  - Includes MBSE Modeling Guide and Geospatial Data Specification
- DevSecOps Standard
  - Process for using SCARS-provided DevSecOps pipelines for training system software sustainment
- Architecture Standard
  - ICD for MOSA-compliant modular subsystems and interfaces for training systems

SCARS Standards, cont.

DELIVERING THE SKILL TO KILL

- Some standards are available to the public, and others are limited distribution.
- Standards are required for integration with SCARS infrastructure.
- Standards are applied to USAF training systems which are tested for compliance with applicable verification criteria.
- The USAF is not providing a service to certify products as compliant with SCARS Standards.
- To request standards, send email to
  - aflcmc.wns.scarsstandards@us.af.mil
- To share information with the Innovation Cell, send email to
  - aflcmc.wns.sims_innovate@us.af.mil

What Industry Can Do for SCARS

- Apply modular architectures for hardware and software
- Apply standard interfaces for hardware and software
- Support standard data formats
- Avoid proprietary interfaces
- Recommend industry or defacto or emerging standards/trends to Government
- Share innovative products, solutions, technologies, and ideas with the Innovation Cell
- Apply Internet of Things (IoT) for control systems
- Apply software containers where appropriate
- Licensing methods that do not require connection to Internet or hardware keys/dongles
- OEM product support must include patches/updates in response to identification of cybersecurity vulnerabilities
- Innovate!


ADVANCED TRAINING CAPABILITIES DIVISION
DELIVERING THE SKILL TO KILL