MOSAICS

More Situational Awareness for Industrial Control Systems (MOSAICS) Joint Capability Technology Demonstration (JCTD) Overview Briefing

October 2021

Bottom Line Up Front (BLUF)

- Our National critical infrastructure is at risk
- Cyber threats to Industrial Control Systems (ICS) are expanding
- First operational cyber security platform supporting Operational Control System Technology

"...MOSAICS addresses the increasing serious threats to the critical infrastructures upon which we depend to accomplish our Defense critical missions. I can't say enough good things about the MOSAICS team. I hold them out as a sterling example of what a JCTD should be. They have assembled a dream team of DoD and industry partners and they are effectively demonstrating the military utility of the integration of sufficiently mature technologies..."

Daniel (Rags) Ragsdale,

(Former Principal Director for Cyber - OUSD R&E)

The work the JCTD team has done is foundational to protecting DOD's critical infrastructure from cyber attack!

MOSAICS Description

What's the MOSAICS JCTD?

MOSAICS is an integration of COTS and GOTS technologies for enhanced situational awareness and defense of industrial control systems associated with task critical assets

What did the JCTD do?

Demonstrated the ability to baseline control system networks & end point devices and semi-autonomously identify, respond to, and recover from asymmetric attacks on critical infrastructure in mission-relevant timeframes

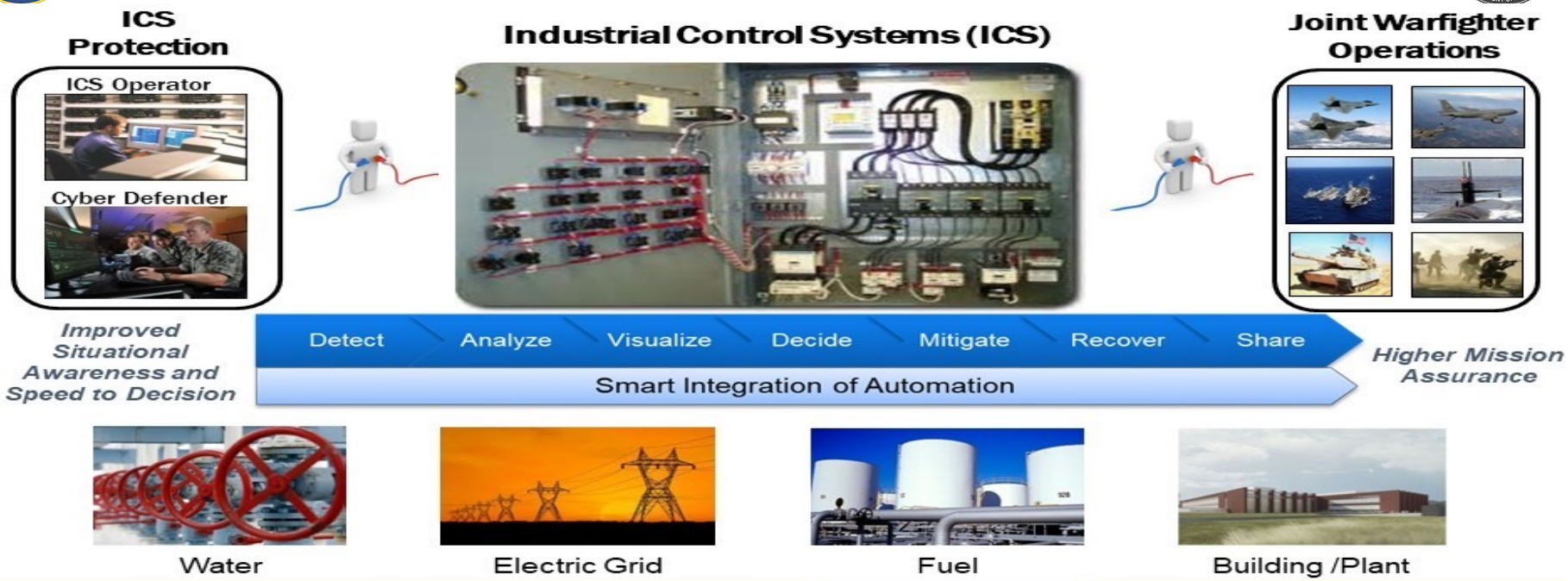
Operational value to the warfighter:

- Enhance understanding of risk to critical infrastructure and supported operational capabilities
- Detect control system threats faster – from months to minutes
- Improve situational awareness driving real-time decision aids to enable cyber defender response
- Disrupt adversary kill-chain in mission-relevant time
- Limit adversary re-use of attacks through enhanced sharing of indicators and mitigations
- Application of referenced open-system architecture across the Services

Example Prototype

Commercial Technology Set Tailored to Site Needs

MOSAICS OV1 FY18 – 21



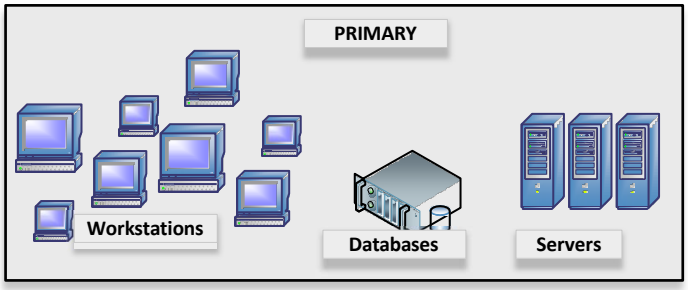
Protect Critical Infrastructure Industrial Control Systems from Non-Kinetic Attacks

Modernization Area / Mission Priority	Deliverable	OSD Funding / Co-Funding & Cost Share	STAKEHOLDERS
CYBER & Autonomy	Operational Prototype, Cyber Infrastructure Defense of Industrial Control Systems (ICS)	25.4% / 74.6%	USINDOPACOM / USNORTHCOM USN, USAF, USMC OSD A&S Energy & CISO NSA & CYBERCOM DOE

Description / Impact: MOSAICS integrates COTS and GOTS technologies for enhanced situational awareness and operational defense of industrial control systems that operate critical DoD infrastructure assets from cyber attack. MOSAICS will transition its operational prototype to Naval Air Station North Island San Diego, CA and to US Naval Facilities Engineering Command (NAVFAC) for transition in FY21.

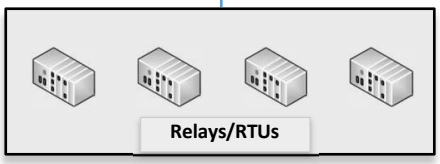
MOSAICS Functional Architecture

Level 2 / 3
Operations Control



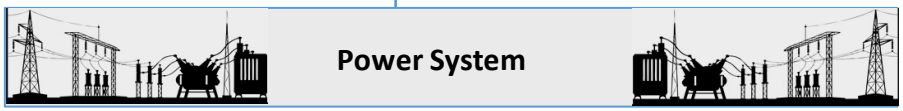
- End-point Detection

Level 1
Intelligent
Devices



- Network Detection
- Serial Detection

Level 0
Physical
Process



- Data Repository
- Security Orchestration
- Baseline Capability
- Visualization
- Data Analytics

MOSAICS Success Stories

- Early focus on COTS solutions with strong focus on functional and technical requirements shared with Industry
- Published CONOPS, Operational, Functional, & Technical Requirements
- Created first ever control system semi-automated baseline capability
- Applied IACD automation for USCYBERCOM ACI TTP execution of ICS operator "in-the-loop" mitigations in near real time
- MOSAICS IATT approved / documentation will support NAVFAC ATO
- Characterized varied operational cybersecurity roles and gaps
- Created MOSAICS framework for reuse applied to all ICS sectors
- DOD CIO Cybersecurity Reference Architecture (CSRA) will incorporate Control Systems as an Appendix D based on the MOSAICS framework
- Despite the pandemic, the MOSAICS team completed a successful MUA within 1 month of original planned date
- Outreach to Industry (3 Industry Days)
  - 4-5 Nov 2020 (Virtual) / 18-19 May 2021 (Virtual) / 18-20 Oct 2021 (National Harbor)

Additional Success Stories
Military Utility Assessment (MUA)

- With respect to the JCTD, all 235 operational, functional and technical requirements were successfully tested and independently verified during either DT or OT
- NAVFAC Operators trained to use the MOSAICS platform very rapidly
- Overall the MUA went well and the MOSAICS platform performed exceptionally with a few minor issues that were discovered in the real world operational environment and are being remediated
- During the MUA, we baselined over 3000 nodes in the field and were able to track activity and monitor each node simultaneously while targeting a simulated control station within the Industrial Control System network
- We conducted 22 attacks against the target during the MUA and while monitoring the entire network, MOSAICS successfully identified 20 of the attacks for a 90.5% success rate with less than 5% false positives
- Unaware to the JCTD, a contractor installing new components on the electrical system during the MUA also alerted MOSAICS as if it were an attack

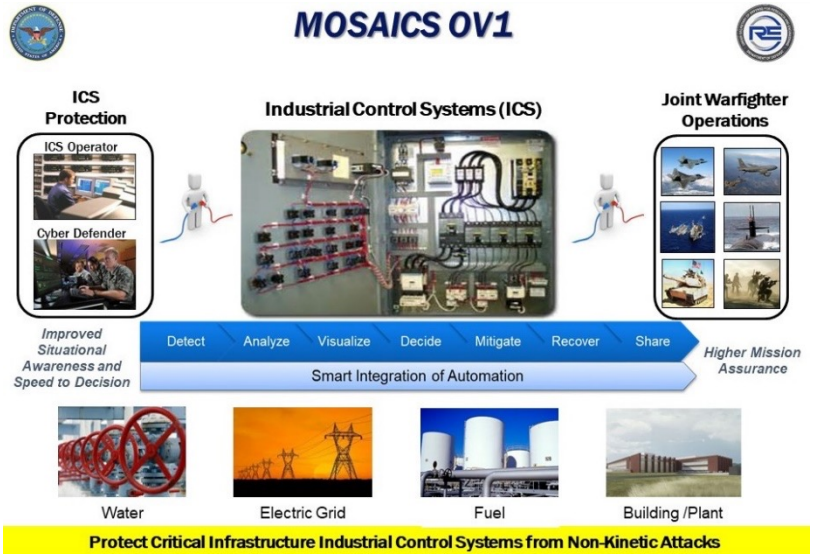
Conclusion

- Addresses risk to US critical infrastructure and force projection
- Detects and mitigates cyber attacks in mission relevant time
- Demonstrates a cyber defense framework for DOD, OGAs, and private sector critical infrastructure
- Transition Success…
  - Leave Behind Capability to NAVFAC SW facility San Diego, CA and Navy Test Bed (EXWC)
  - US Navy fielding at additional locations
  - Transition Open System Standards / Framework to Industry and Joint Services
- Working to garner funding to “Productize” and enhance JCTD capability and buy down risk – MOSAICS 2.0 Next Phase

The Nation needs this capability!

BACK-UP

More Situational Awareness for Industrial Control Systems (MOSAICS) [FY18-21]



Technology Description:

- MOSAICS is a framework integrating of COTS and GOTS technologies for enhanced situational awareness and operational defense of industrial control systems associated with critical assets from cyber attack.

Deliverables:

- Detailed Military Utility Assessment (MUA) Test Plan
- Military Utility Assessment Test and Final Report
- MOSAICS Framework and Integrated Software
- **Semi-automated Baselining tool**
- Operational, Functional, & Technical Requirements to support contracting and system acquisition
- Training and system documentation

Operational Value:

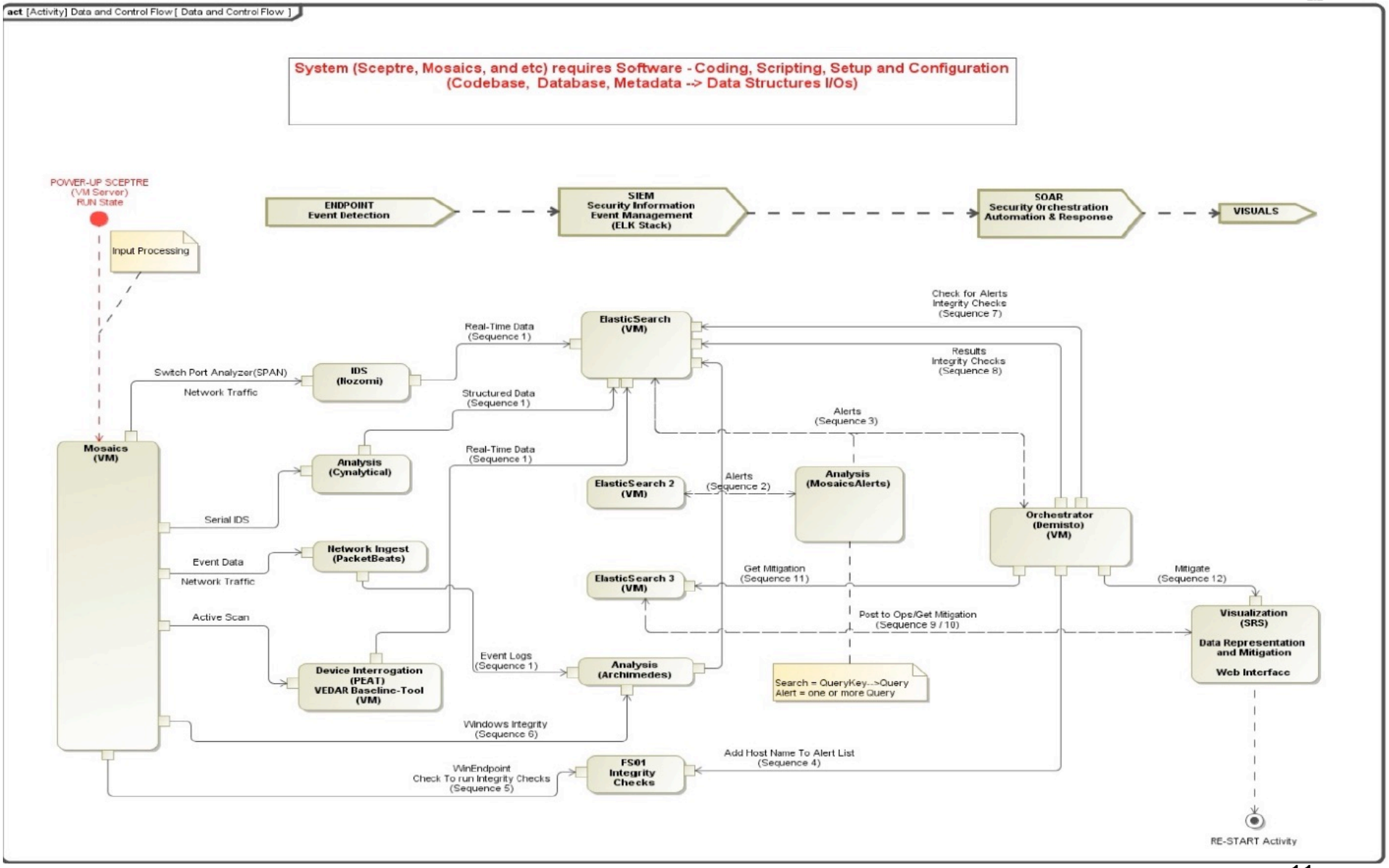
- Enhance understanding of risk to critical infrastructure and supported operational capabilities
- Detect control system threats faster – from months to minutes
- Improve situational awareness driving real-time decisions aids to enable cyber defender response
- Disrupt adversary kill-chain in mission-relevant time
- Limit adversary re-use of attacks through enhanced sharing
- Application of open-system architecture across Services

Transition:

- MOSAICS will transition to US Naval Facilities Engineering Command (NAVFAC) for sustainment in FY21 Program Objective Memorandum (POM).

Participants:
COCOM Sponsors: USINDOPACOM, USNORTHCOM
Technical Managers: Salvatore “Rich” Scalco - NIWC LANT and Dr. William “Waugs” Waugaman – Sandia Nat’l Labs
Operational Managers: Ross Roley - USINDOPACOM and William “Bill” Beary - USNORTHCOM
Transition Manager: Man Nguyen - NAVFAC EXWC
Oversight Executive: Gear Liddy - OSD

MOSAICS Functional Diagram



MOSAICS DATA FLOW