More Situational Awareness for Industrial Control Systems (MOSAICS)

Joint Capability Technology Demonstration (JCTD)

The Joint Capability Technology Demonstration (JCTD) Program addresses joint and combatant command warfighting needs through the execution and demonstration of prototypes within two to four years. The program delivers developmental and operational prototypes to affordably operationalize technologies that enable warfighters to explore novel concepts and to facilitate informed transition to formal acquisition programs.

Problem

- **U.S. critical infrastructure is at risk**

  Extensive dependency on highly vulnerable information technology and industrial control systems equals unacceptable and growing risk

- **The threat is pervasive**

  Virtually any actor with substantial resources can now develop or buy the capability to attack elements of U.S. critical infrastructure with cyber weapons

- **DoD is not postured to stop most dangerous attacks**

  The offensive cyber capabilities of our most capable potential adversaries are likely to far exceed our ability to defend

Defense Science Board 2017

Threat Capability Description

Criminal or state actors who are organized, highly technical, proficient, well-funded professionals working in teams to discover new vulnerabilities and develop exploits. KEY POINT - Finds and exploits unknown vulnerabilities.

Defense Science Board – Cyber Threat Tier IV Adversary

Capability	Description
Target	Highly capable of determining and understanding the technology, people, and processes of the target facility
Access	Demonstrate a capability for limited gap jumping, as well as the ability to effectively traverse the IT/OT boundary
Payload	Demonstrated capability to conduct ICS/SCADA attacks against a variety of targets

Solution: MOSAICS

What is it?

- MOSAICS is a Joint Capability Technology Demonstration funded by the OUSD (R&E) - Emerging Capability and Prototyping
- 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 will it deliver?

- Integrated, operational capability to enable defense of control systems
- ICS baselining tools and programmable logic controller sensors
- Tailored visualizations, analytics, automated cybersecurity orchestration

Anticipated Benefits

- 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 of indicators and mitigations

Stakeholders

OV-1

ICS Protection

Facilities Engineer

Cyber Defender

Industrial Control Systems (ICS)

Joint Warfighter Operations

Operational Cyber Defense Capabilities

Detect → Analyze → Visualize → Decide → Mitigate → Recover → Share

Smart Integration of Automation

Mission Assurance

Water

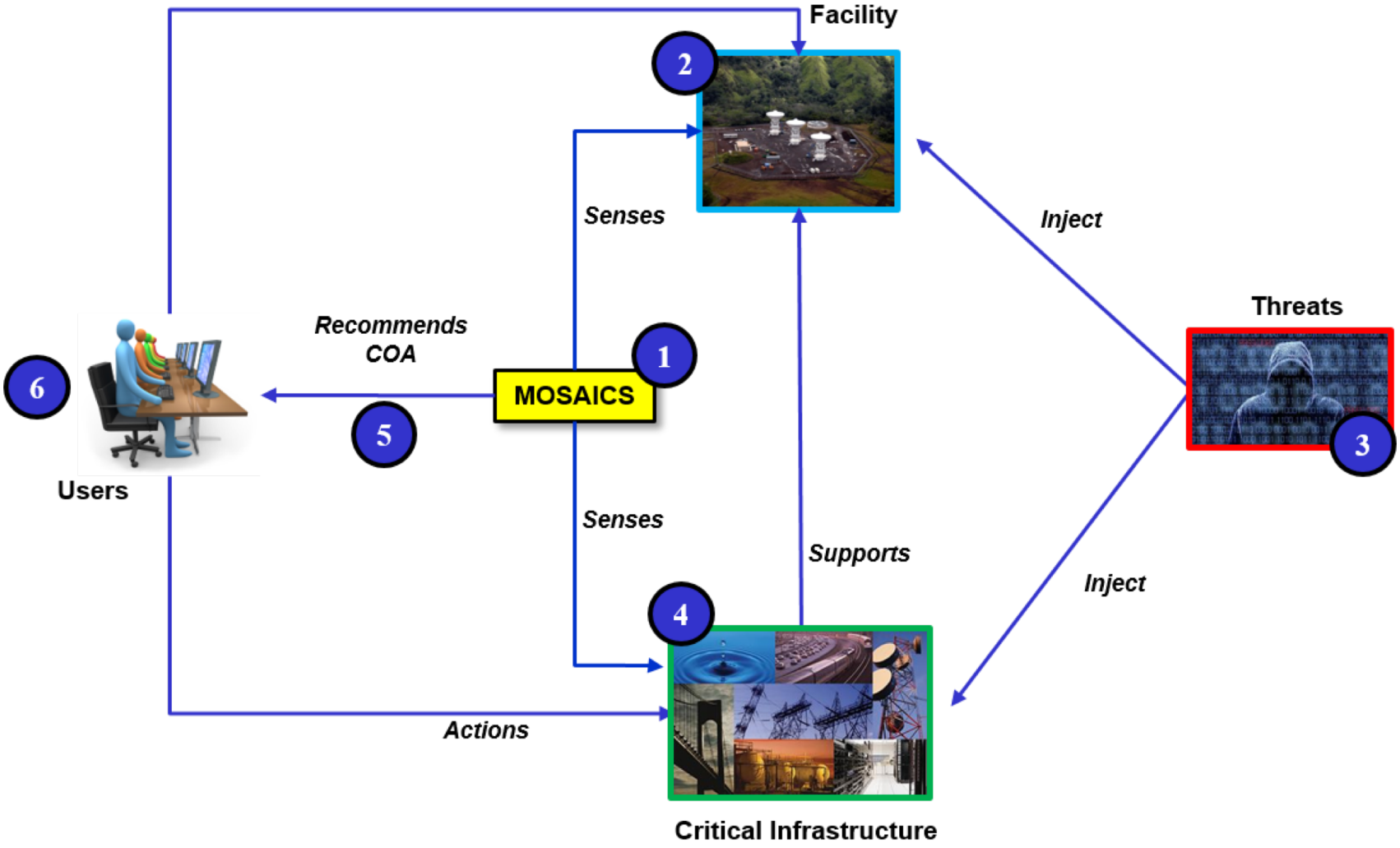
Electric Grid

Fuel

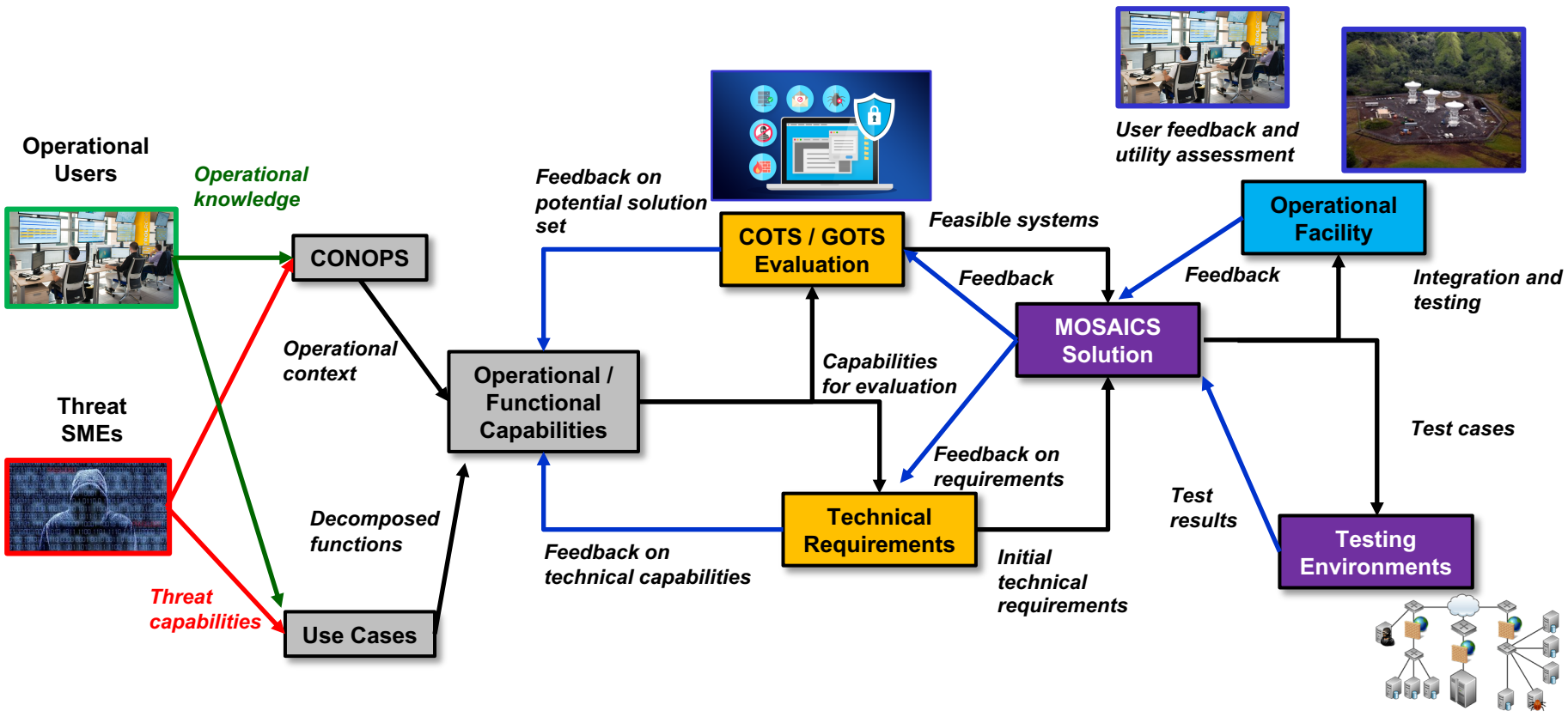
Building /Plant

Protect Critical Infrastructure Control Systems from Cyber Attacks

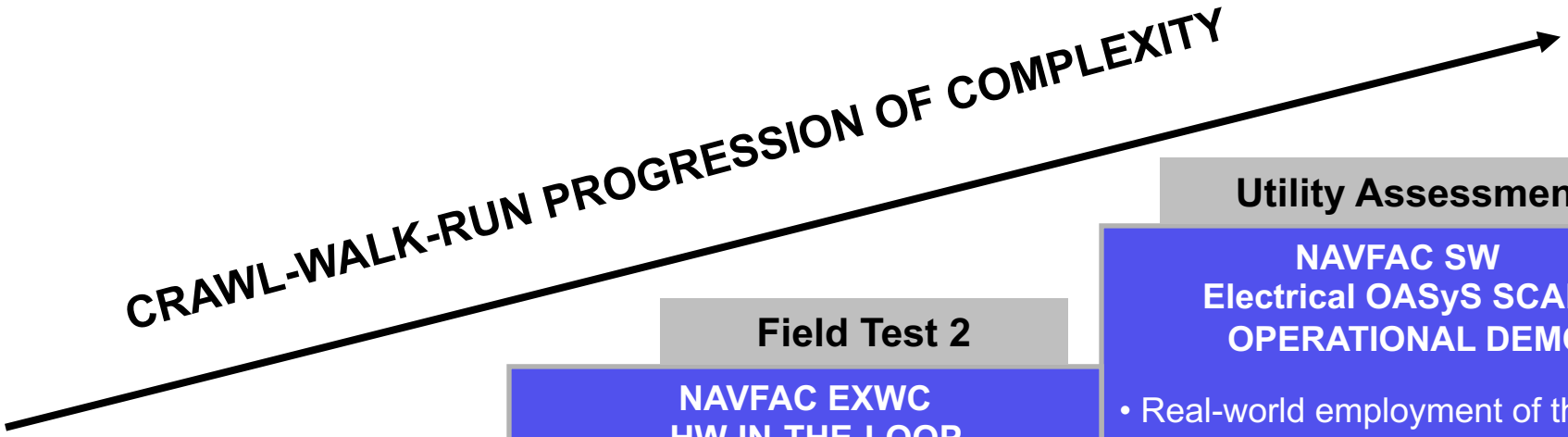
CONOPS


Facility
2
Senses
Inject
Threats
3
Recommends
COA
6
1
MOSAICS
5
Users
Senses
Supports
Inject
4
Actions
Critical Infrastructure

Systems Engineering Approach



Test Concept



Field Test 1

JOINT BASE SAN ANTONIO DEMO

- Combined live network and cyber range test
- Assess most mature capabilities in a realistic environment

Field Test 2

NAVFAC EXWC HW-IN-THE-LOOP

- On state-of-the-art SCADA testbed at Port Hueneme, CA
- Simulated ops environment
- ICW Trident Warrior

Utility Assessment

NAVFAC SW Electrical OASyS SCADA OPERATIONAL DEMO

- Real-world employment of the fielded prototype in San Diego, CA
- Assess in operational environment under mission conditions with operational users
- IAW CONOPS and TTP
- ICW USPACOM exercise

COTS BEST OF BREED TECHNOLOGIES & GOTS GAP FILLERS

RIGOROUS ASSESSMENT WITH REPRESENTATIVE ENVIRONMENTS AND THREATS

Operational Requirements

- Protect task critical assets from disruptive cyber attacks
- Enhance intrusion detection
- Automate *Advanced Cyber Industrial Control Systems TTP*
- Provide robust analytics and decision support
- Deliver actionable situational awareness and enterprise info sharing

Functional Requirements

Identify | Protect | Detect | Analyze | Visualize | Decide | Mitigate | Recover | Share

F1.0 Identify System Components	F2.0 Protect from Threats	F3.0 Monitor / Detect threats	F4.0 Analyze detected events	F5.0 Visualize status	F6.0 Decide on COA	F7.0 Perform mitigation actions	F8.0 Perform recovery actions	F9.0 Share data
F1.1.1 Inventory physical devices	F2.1.1 Protect data at-rest	F3.1 Monitor facility status	F4.1 Profile networks and systems	F5.1 Collect system status	F6.1 Generate available COA	F7.1 Select mitigation technique	F8.1 Determine desired end state for recovery	F9.1 Select data to share
F1.1.2 Inventory software components	F2.1.2 Protect data in-transit	F3.2 Monitor critical infrastructure status	F4.2 Compare against normal behaviors	F5.2.1 Display top-level view of facility capability	F6.2 Determine automated COAs	F7.2 Select equipment / node to apply mitigation	F8.2 Determine recovery timeframe	F9.2 Collect data
F1.1.3 Map communication and data flows	F2.2 Manage facility ICS assets	F.3.3.1 Detect changes from baseline configuration	F4.3.1 Perform system analysis	F5.2.2 Display affected network elements	F6.3 Display COA to user	F7.3.1 Protect / harden	F8.3 Consider list of recovery COA	F9.3 Receive data from external sources
F1.2 Categorize system components based on criticality and vulnerability	F2.3 Establish operational availability goals for ICS data capacity	F.3.3.2 Monitor system components	F4.3.2 Perform malware analysis	F5.2.3 Display affected devices	F6.4 Consider facility priorities	F7.3.2 Diversify	F8.4 Select recovery COA	F9.4 Store data
F1.3.1 Manage credential access	F2.4 Protect against ICS data leaks	F.3.3.3 Detect malware	F4.3.3 Perform network analysis	F5.4 Display identity of event	F6.5 Consider threat severity	F7.3.3 Segment	F8.5 Preserve data for forensic analysis	F9.5 Set access permissions
F1.3.2 Manage physical access	F2.5 Protect communications and control networks	F.3.3.4 Detect anomalous behavior	F4.4 Categorize event	F5.5.1 Display functional impact	F6.6 Consider CI availability	F7.3.4 Stop	F8.5.1 Restart	F9.6 Verify identify / access from requester
F1.3.3 Manage remote access	F2.6 Perform integrity checks for software, hardware, firmware information integrity	F.3.3.5 Detect rule/policy violations	F4.5 Perform event correlation	F5.5.2 Display information impact	F6.7 Consider mission priorities	F7.3.5 Restart	F8.5.2 Reinitialize	F9.7 Enable / deny access to data
F1.3.4 Manage access and authorization	F2.7.1 Develop a system baseline	F3.4.1 Monitor state of physical barriers	F4.6 Record events	F5.6 Receive operator acknowledgement		F7.3.6 Switch to manual control	F8.5.3 Reset permissions / access	F9.8 Send data
F1.3.5 Manage network integrity	F2.7.2 Maintain system baseline					F7.4 Observe system reaction to mitigation actions	F8.5.4 Replace	
F1.4 Utilize identity credentials in facility operations	F2.7.3 Implement a configuration control process to update system inventory						F8.5.5 Reconnect	
F1.5 Authenticate components	F2.8 Test recovery and protection systems and plans						F8.5.6 Test operation of system component	
	F2.9 Maintain ICS protection / monitoring systems						F8.7 Observe recovery progress	
	F2.10 Perform routine maintenance on ICS components (local or remote)							
	F2.11 Maintain audit logs for ICS protection / monitoring systems							
	F2.12 Protect against cyber threats							

Identify System Components

Inventory key system devices and components to support the facility's mission and categorize based on criticality and results of vulnerability assessment and identify internal external data flows and connections.

Key tasks:

- Inventory physical devices
- Inventory software components
- Map communication flows
- Map data flows
- Categorize system components based on criticality and vulnerability
- Establish priorities

Protect from Threats

Identify | **Protect** | Detect | Analyze | Visualize | Decide | Mitigate | Recover | Share

Implement controls to limit access to physical and logical assets to authorized users, processes and devices and protect data-in-transit and data-at-rest

Key tasks:

- Manage identities and credentials
- Protect data at rest and in transition
- Manage facility ICS assets
- Protect against ICS data leaks
- Protect communications and control networks
- Perform integrity checks for software, hardware, firmware information integrity
- Maintain ICS protection systems
- Maintain audit logs for ICS protection/ monitoring systems
- Protect against cyber threats

Monitor / Detect Threats

Monitor system components for indications of an adversarial presence such as malicious activity and anomalies including evidence of malicious code and unauthorized personnel, connections, devices and software and monitor system components for unauthorized changes from baseline configurations

Key tasks:

- Monitor critical infrastructure status
- Detect chances from baseline configuration
- Monitor system components
- Detect malware
- Detect anomalous behavior
- Detect rule / policy violations
- Generate events

Analyze Detected Events

Examine anomalous or malicious activity to determine if there is a threat to the system and evaluated the severity and type of detected threat

Key tasks:

- Profile networks and systems
- Compare against normal behavior
- Perform system analysis
- Perform malware analysis
- Perform network analysis
- Categorize events
- Perform event correlation
- Record events

Visualize Status

Identify | Protect | Detect | Analyze | **Visualize** | Decide | Mitigate | Recover | Share

Provide visibility of the operational state of the system and of malicious and anomalous activity to the system operator and create logs and reports of malicious and anomalous activity

Key tasks:

- Collect system status
- Display top-level view of facility capability
- Display affected network elements
- Display affected devices
- Display identity of event
- Display functional impact
- Display information impact
- Receive operator acknowledgement

Decide on COA

Evaluate events and determine manual and automated courses of action that minimize risk while considering the mission impact of the various COAs

Key tasks:

- Generate available COAs
- Determine automated COAs
- Display COAs to user
- Consider facility priorities
- Consider threat severity
- Consider CI availability
- Consider mission priorities

Perform Mitigation Actions

Identify | Protect | Detect | Analyze | Visualize | Decide | **Mitigate** | Recover | Share

Execute the courses of actions needed to eliminate or minimize any deleterious effects resulting from malicious activity, anomalies and threats

Key tasks:

- Select mitigation technique
- Select equipment / node to apply mitigation
- Protect / Diversify / Segment / Stop / Restart / Switch to manual control
- Observe system reaction to mitigation actions

Perform Recovery Actions

Identify | Protect | Detect | Analyze | Visualize | Decide | Mitigate | **Recover** | Share

Perform the activities needed to restore the system to a fully mission-capable state

Key tasks:

- Determine desired end state for recovery
- Determine recovery timeframe
- Consider list of recovery COAs
- Select recovery COAs
- Preserve data for forensic analysis
- Restart / Reinitialize / Reset access / Replace / Reconnect
- Test operation of system component
- Observe recover progress

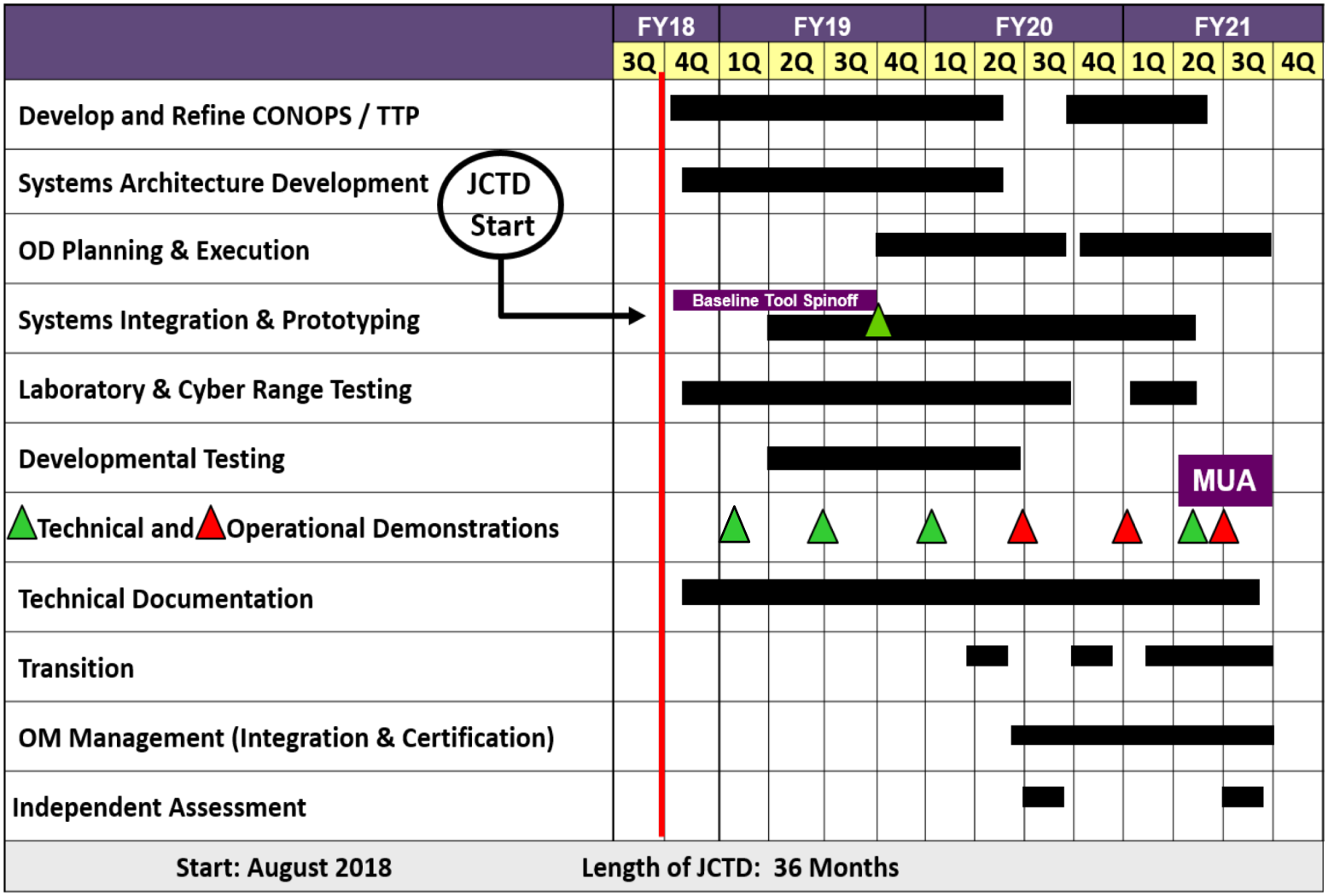
Share Data

Collect the lessons learned, incident data, and evidence in order to coordinate with other organizations to strengthen the ability to effectively respond to cyber threats

Key tasks:

- Select data to share
- Receive data from external sources
- Receive request for sharing
- Collect data
- Store data
- Set access permissions
- Enable / deny access to data
- Send data

Schedule


FY18
FY19
FY20
FY21
3Q 4Q 1Q 2Q 3Q 4Q 1Q 2Q 3Q 4Q 1Q 2Q 3Q 4Q
Develop and Refine CONOPS / TTP
Systems Architecture Development
JCTD Start
OD Planning & Execution
Systems Integration & Prototyping
Baseline Tool Spinoff
Laboratory & Cyber Range Testing
Developmental Testing
MUA
Technical and Operational Demonstrations
Technical Documentation
Transition
OM Management (Integration & Certification)
Independent Assessment
Start: August 2018
Length of JCTD: 36 Months

Transition

Anticipated Deliverables

Phase 1

- CONOPS
- ICS network baselining tool

Phase 2

- ACI TTP automation
- ICS sensors

Phase 3

- Field prototype
- Military Utility Assessment
- Industry Day
- Training plans
- Transition plan
- Unified Facilities Criteria updates
- Final reports

Transition Paths

DOD

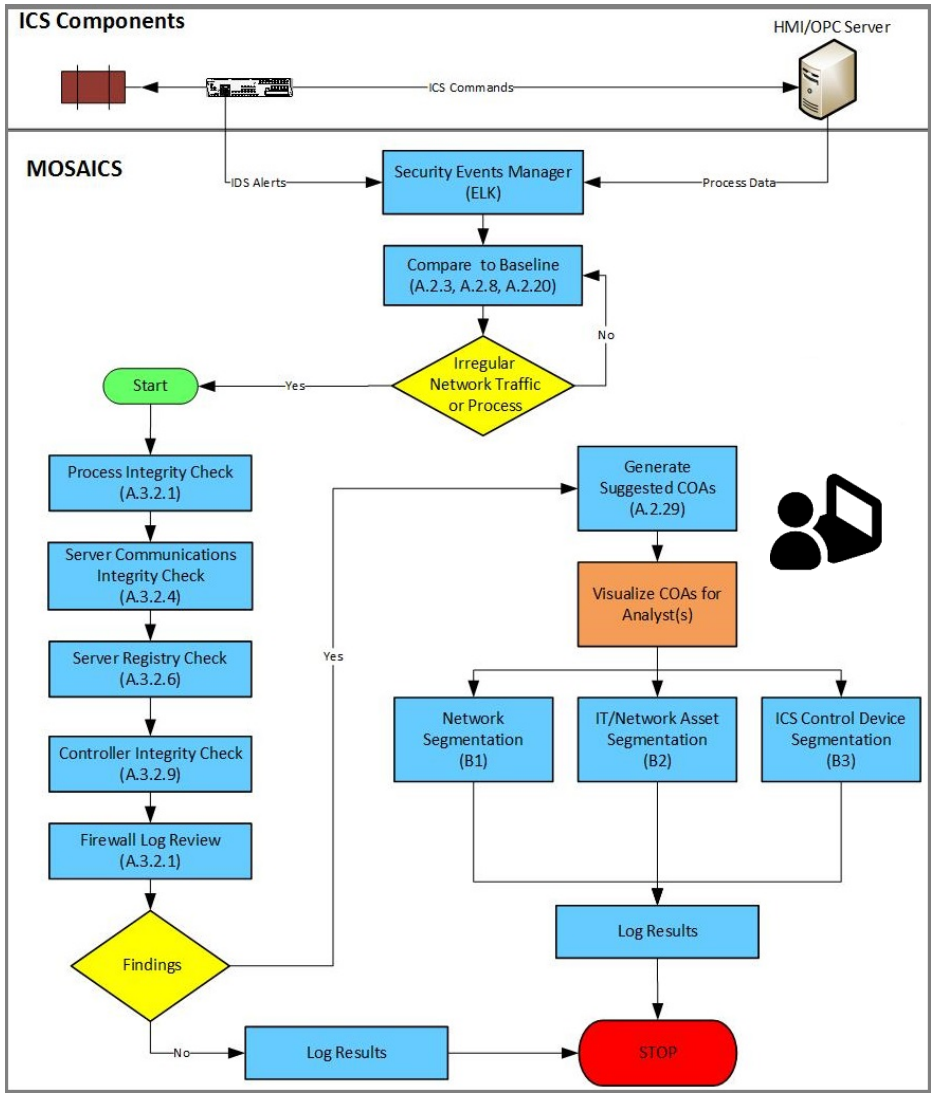
- Air Force – AFCEC
- Army – IMCOM
- Marine Corps – MARFORCYBER
- Navy – NAVFAC
- USCYBERCOM
- Defense Technical Information Center

Commercial partners

Federal sector and utilities

Standards and regulatory organizations

Automation Proof of Concept



- NSA-sponsored
- Apply IACD to ICS/SCADA
- Demonstrate capability early in program
- Prove ability to automate sections of the ACI TTP
- Capture lessons learned for application to MOSAICS

What We Need From Industry

- **Vendors**
  - Link with MOSAICS' systems engineering team
  - Identify capabilities that might address requirements
  - Provide insight into those capabilities
- **Providers**
  - Provide inputs on best practices in the field
  - Share MOSAICS progress and results
    - Lessons learned
    - Automated playbooks
    - Reference architecture

Points of Contact

- **Technical Managers**
  - Rich Scalco, DOD Technical Manager
    SPAWAR Systems Center – Atlantic
    salvatore.Scalco@navy.mil
  - Dr. Bill Waugaman, DOE Labs Technical Manager
    Sandia National Laboratories
    wwaugam@sandia.gov
- **Systems Engineering Team**
  - Dr. Craig Rieger, COTS Integration Lead
    Idaho National Laboratory
    craig.rieger@inl.gov