JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

More Situational Awareness for Industrial Control Systems (MOSAICS) Requirements

Carol Vermilye
MOSAICS Requirements Manager

Topics

1. MOSAICS Requirements Overview
2. MOSAICS Operational Requirements
3. MOSAICS Functional Requirements
4. MOSAICS Technical Requirements
5. Requirements Gaps
6. Questions

MOSAICS Requirements Overview

1. Large body of requirements
   a) Initial set of 206 Functional Requirements developed Summer 2018
   b) Began development of Technical Requirements Spring 2019 – as of Fall 2020 have written on the order of 600 Technical Requirements
   c) Operational Requirements developed Summer 2019

2. Requirements available in MS Excel on DTIC and RDP21

MOSAICS Operational Requirements

1. 23 Operational Requirements allocated MOSAICS JCTD
2. Focus on high-level operational needs to successfully operate MOSAICS
3. Address MOSAICS capabilities
   a) Identify
   b) Protect
   c) Monitor/Detect
   d) Analyze
   e) Visualize
   f) Decide
   g) Mitigate
   h) Recover
   i) Information Sharing

MOSAICS Functional Requirements

1. 104 Functional Requirements allocated to MOSAICS JCTD
2. Focus on providing additional detail regarding functional needs for MOSAICS capabilities

MOSAICS Technical Requirements

1. 334 Requirements allocated to MOSAICS JCTD (Spirals 0 – 5)
2. Focus on level of detail needed to allow development teams to implement MOSAICS

Requirements Gaps (1/2)

1. Functional Requirements
   a) 51 Functional Requirements (of the original body of 206 functional requirements) were not implemented in the JCTD as they were deemed to be out of scope
   b) Exemplar types of functions not implemented in JCTD include:
      i. MOSAICS component identification and baselining
      ii. Management of access permissions and authorized users
      iii. Monitoring of MOSAICS anomalies
      iv. Additional mitigation responses
      v. MOSAICS recovery

Requirements Gaps (2/2)

1. Technical Requirements
   a) 267 Technical Requirements (of the original body of requirements of ~600 technical requirements) were not allocated for implementation in Spirals 0 – 5
   b) Mapped to Functional Requirements not implemented in JCTD
   c) Provide additional detail to implement capabilities such as:
      i. Additional system protection
      ii. Visualization
      iii. Event/incident response
      iv. Information sharing

Technical Requirements Gaps Additional Development Needed

1. Protect
   a) Data and Protective Security, Operational Availability
2. Monitor/Detect
   a) Baseline Comparison, Continuous Monitoring
3. Analyze
   a) Anomaly Analysis, Event Related
4. Visualize
   a) Detected Events, Facility Status and Impact, Alert Management
5. Decide
   a) Event/Incidence Response Analysis
6. Mitigate
   a) Event/Incidence Response Execution
7. Recover
   a) Recovery Planning
8. Information Sharing
   a) Event/Incident Communication, Threat Information Communication

Requirements Gaps Examples

1. Baselining
   a) Check for BIOS and other firmware modifications
   b) Real time detection of updates to ICS component inventories
   c) Detection of new traffic, potentially unauthorized traffic, and device conversations
2. Visualization
   a) Display of information related to detected events
   b) Display of facility status and impact
   c) Additional alert management functionality
      i. User configurable displays (colors, audible or blinking alarms)
      ii. Define alarms
      iii. Send alarms via email and text message to pre-defined list of recipients

Requirements Spreadsheet Excerpt

MOSAICS

JOHNS HOPKINS APPLIED PHYSICS LABORATORY

Requirement Number	Requirement	Mapping
O1.1	Inventory IT and OT system devices and system components in the targeted environment.	Identify
F1.1.1	MOSAICS shall enable creation of an inventory of network discoverable and non-discoverable physical control system (CS) components that are part of the facility's CS or are controlled / monitored by the facility's CS.	O1.1
T1.1.1.1	The MOSAICS mapping of the SCADA system shall, at a minimum, include the host names and IP addresses of the components comprising the SCADA (i.e., Data Historian, Engineering Workstation, Human Machine Interface (HMI), the OPC server).	F1.1.1
T1.1.1.5	MOSAICS shall be capable of automated, active collection of IP addresses for the SCADA mapping, where applicable.	F1.1.1
T1.1.1.6	MOSAICS shall be capable of automated, passive collection of MAC addresses for the SCADA mapping, where applicable.	F1.1.1
T1.1.1.8	MOSAICS shall be capable of manual collection (ingestion and processing) of configuration data from Engineering Workstations, HMIs, Data Historians, firewalls, routers, switches, DHCP servers where applicable, for the SCADA mapping.	F1.1.1
O5.1	Provide alert management.	Visualize
F5.3.1	MOSAICS shall provide the capability for the user to acknowledge alerts.	O5.1
T5.3.1.1	MOSAICS shall provide the capability for the user to acknowledge displayed alerts.	F5.3.1
T5.3.1.2	MOSAICS shall provide the capability to display alerts in aggregation and individually.	F5.3.1
T5.3.1.4	MOSAICS shall provide the capability to display mitigations or workflows that have been triggered to run automatically.	F5.3.1
F5.3.3	MOSAICS shall provide the capability to assign alerts.	O5.1
T5.3.3.1	MOSAICS shall prioritize alarms to display.	F5.3.3
T5.3.3.7	MOSAICS displayed alarms shall be filterable.	F5.3.3

Requirements available in MS Excel on DTIC and RDP21

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Questions?

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY