
The intent of the MOSAICS architectural framework is to interoperate with the open Elastic Stack tool Elasticsearch version 7.9.

MOSAICS refers to the MOSAICS Reference Architecture in these technical requirements. These requirements represent a minimum set of technical requirements that may be used to implement operational defense. These technical requirements are not unique to any DoD location.

| Requirement Number | Functional Requirement not Implemented |
|---|---|
| F1.0 | MOSAICS System Identification Requirements |
| F1.1 | System Component Identification and Baselining Requirements |
| F1.1.2 | MOSAICS shall create an inventory of network discoverable physical ICS devices that are part of MOSAICS. |
| F1.1.4 | MOSAICS shall maintain an inventory of network discoverable physical ICS devices that are part of MOSAICS. |
| F1.1.6 | MOSAICS shall create an inventory of network discoverable software components that are part of MOSAICS. |
| F1.1.8 | MOSAICS shall maintain an inventory of network discoverable software components that are part of MOSAICS. |
| F1.2 | System Communication Mapping Requirements |
| F1.2.4 | MOSAICS shall create a map of ICS data flows within MOSAICS. |
| F1.2.5 | MOSAICS shall maintain a map of ICS data flows within MOSAICS. |
| F2.0 | MOSAICS System Protection Requirements |
| F2.1 | Identity and Access Management Requirements |
| F2.1.6 | MOSAICS shall maintain the list of authorized users with remote access to MOSAICS. |
| F2.2 | Authentication Requirements |
| F2.2.1 | MOSAICS shall maintain the access permissions and authorizations that affect facility ICS (examples are sensors, workstations, networks, and field devices) operations. |
| F2.2.3 | MOSAICS shall manage the authorized users for remote access to facility ICS equipment if supported by facility ICS equipment. |
| F2.2.4 | MOSAICS shall manage the authorized users for remote access to MOSAICS. |
| F2.2.5 | MOSAICS shall ensure facility ICS user actions and component (e.g. hardware or software) operations are authenticated (using a determined level of authentication) prior to use. |
| F2.3 | Access Control Requirements |
| F2.3.1 | MOSAICS shall monitor the physical access control systems used for protection of facility ICS. |
| F2.3.2 | MOSAICS shall monitor the physical access control systems used for protection of MOSAICS. |
| F2.3.3 | MOSAICS shall maintain the list of authorized users with remote access to facility ICS equipment. |
| F2.3.6 | MOSAICS shall provide data flow control for MOSAICS. |
| F2.3.7 | MOSAICS shall bind identity credentials to interactions within the facility ICS during operations. |
| F2.3.8 | MOSAICS shall bind identity credentials to interactions within the facility ICS during MOSAICS operations. |
| F2.5 | Information Protection Requirements |
| F2.5.4 | MOSAICS shall maintain a system baseline of relevant MOSAICS components (e.g. hardware or software) within the facility. |
| | MOSAICS shall utilize a configuration control mechanism to update facility ICS inventory. |
| | MOSAICS shall utilize a configuration control mechanism to update MOSAICS inventory. |
| F2.6 | Data Security Requirements |
| F2.6.1 | MOSAICS shall maintain the protective / monitoring systems for facility ICS components to a level of availability determined by the facility owner. |
| F2.6.3 | MOSAICS shall permit local / remote maintenance activity on the facility ICS from credentialed and authorized maintainers. |
| F3.0 | MOSAICS Monitor and Detection Requirements |
| F3.1 | Baseline Comparison Requirements |

| | |
|---|---|
| **F3.1.1** | MOSAICS shall monitor the status of the contributing critical infrastructure nodes (e.g. power, water, IT) that support the facility. |
| **F3.2** | **Monitoring Requirements** |
| **F3.2.6** | MOSAICS shall monitor data flows of MOSAICS components and systems. |
| **F3.2.7** | MOSAICS shall monitor signatures for indication of malware for MOSAICS components. |
| **F3.2.10** | MOSAICS shall detect MOSAICS component behavior that is not consistent with normal operations. |
| **F3.2.12** | MOSAICS shall detect violations of access/usage rules and policies on MOSAICS components. |
| **F4.0** | **MOSAICS Analysis Requirements** |
| **F4.1** | **Anomaly Analysis Requirements** |
| **F4.1.10** | MOSAICS shall analyze the status of MOSAICS components for threats to MOSAICS. |
| **F4.1.12** | MOSAICS shall analyze accesses (remote, local, physical, logical) of MOSAICS components and systems for threats to MOSAICS. |
| **F4.1.14** | MOSAICS shall analyze data flows of MOSAICS components and systems for threats to MOSAICS. |
| **F4.1.16** | MOSAICS shall analyze any physical intrusion attempts of all components identified by MOSAICS to be monitored throughout the facility. |
| **F4.2** | **Event Requirements** |
| **F4.2.4** | MOSAICS shall generate a list of potential impacts on the facility ICS of the detected event. |
| **F4.2.6** | MOSAICS shall provide the capability for a user to enter potential impacts on the facility ICS of a detected event. |
| **F7.0** | **MOSAICS Mitigation Requirements** |
| **F7.1** | **Event / Incident Response Execution Requirements** |
| **F7.1.2** | MOSAICS shall identify COAs to apply to existing problems. |
| **F7.1.9** | MOSAICS shall provide the capability for the user to segment affected system components, if |
| **F7.1.10** | MOSAICS shall be able to segment affected system components, if selected. |
| **F7.1.11** | MOSAICS shall provide the capability for the user to stop selected facility ICS component operations. |
| **F7.1.12** | MOSAICS shall provide information to the user regarding affected facility ICS component operations that may need to be stopped by the user. |
| **F7.1.13** | MOSAICS shall provide the capability for the user to restart selected facility ICS components. |
| **F7.1.14** | MOSAICS shall be able to restart selected facility ICS components. |
| **F7.1.15** | MOSAICS shall provide the capability for the user to switch selected facility ICS components to manual control and assume control. |
| **F7.1.17** | MOSAICS shall monitor facility ICS status after applying the mitigation to determine the mitigation effectiveness. |
| **F8.0** | **MOSAICS Recovery Requirements** |
| **F8.1** | **Recovery Planning Requirements** |
| **F8.1.1** | MOSAICS shall provide the capability for the user to determine what type of end state the facility should achieve based on the recovery procedure. |
| **F8.1.2** | MOSAICS shall provide the capability for the user to determine the recovery timeframe that is feasible based on the resources available and the existing mission priorities. |
| **F8.3** | **Recovery Execution Requirements** |
| **F8.3.8** | MOSAICS shall have the ability to reset the access permissions on identified MOSAICS components. |
| **F8.3.12** | Placeholder to look at automation of software updates. |
| **F8.4** | **Recovery Verification Requirements** |

| | |
|---|---|
| **F8.4.1** | MOSAICS shall provide the capability for the user to test the operation of replaced facility ICS components to ensure normal operations. |
| **F8.4.2** | MOSAICS shall have the ability to test the operation of replaced facility ICS components to ensure normal operations. |
| **F8.4.3** | MOSAICS shall provide the capability for the user to test the operation of replaced MOSAICS components to ensure normal operations. |
| **F8.4.4** | MOSAICS shall have the ability to test the operation of replaced MOSAICS components to ensure normal operation. |
| **F8.4.6** | MOSAICS shall determine recovery effectiveness. |

| Requirement Number | Techcnical Requirements not Implemented | Mapping to Functional Rqmts |
|---|---|---|
| ***T1.0*** | ***MOSAICS System Identification Technical Requirements*** | |
| **T1.1** | **System Component Identification Technical Requirements** | |
| **T1.1.3.17** | MOSAICS shall maintain an inventory of computer components affiliated/integrated with the facility ICS. | F1.1.3 |
| **T1.1.3.18** | MOSAICS shall maintain an inventory of network components affiliated/integrated with the facility ICS. | F1.1.3 |
| **T1.1.9.1** | MOSAICS shall handle conflicts between manually and automated entry of inventory information of ICS physical components. | F1.1.9 |
| **T1.1.9.2** | MOSAICS shall handle conflicts between manually and automated entry of inventory information of ICS software components. | F1.1.9 |
| **T1.3** | **System Component Categorization Technical Requirements** | |
| **T1.3.2.1** | MOSAICS shall allow the operator to set an 'importance/risk' value. | F1.3.2 |
| **T1.3.2.2** | MOSAICS shall provide the capability for the user to define and assign user defined attributes. | F1.3.2 |
| **T1.3.4.1** | MOSAICS shall provide the capability to manually categorize the importance of the networks and devices for prioritizing response. | F1.3.4 |
| **T1.3.4.2** | MOSAICS shall provide the capability to automatically categorize the importance of the networks and devices for prioritizing response. | F1.3.4 |
| **T2.0** | **MOSAICS System Protection Technical Requirements** | |
| **T2.1** | **Identity Management, Authentication and Access Control Technical Requirements** | |
| **T2.1.1.1** | MOSAICS shall have the ability to provide mutual authentication with other systems. | F2.1.1 |
| **T2.1.1.2** | MOSAICS shall be compatible with existing authentication protocols within an | F2.1.1 |
| **T2.1.1.4** | MOSAICS shall check for wireless connections to the monitored network. | F2.1.1 |
| **T2.1.2.1** | MOSAICS shall have the ability to provide mutual authentication with other tools. | F2.1.2 |
| **T2.1.5.1** | MOSAICS shall implement whitelisting as a logical access control. | F2.1.5 |
| **T2.1.5.2** | MOSAICS shall implement blocking as a logical access control. | F2.1.5 |
| **T2.1.7.2** | MOSAICS shall provide the capability to throttle data flow in order to manage/observe malicious behavior. | F2.1.7 |
| **T2.4** | **Data Security Technical Requirements** | |
| **T2.4.1.1** | The MOSAICS orchestration capability shall have the ability to store credentials (Safe Credential Storage). | F2.4.1 |
| **T2.4.1.3** | MOSAICS shall encrypt facility ICS data at rest, where feasible. | F2.4.1 |
| **T2.4.1.4** | MOSAICS shall limit access to facility ICS data at rest to authorized users. | F2.4.1 |
| **T2.4.1.5** | MOSIACS shall identify facility ICS data stored in unauthorized locations. | F2.4.1 |
| **T2.4.1.6** | MOSAICS shall have data integrity safeguards, including provenance tracking, for data at rest. | F2.4.1 |
| **T2.4.3.1** | MOSAICS shall protect confidential information when handling it, in accordance with legal and regulatory requirements. | F2.4.3 |
| **T2.4.3.2** | MOSAICS shall encrypt facility ICS data while in transit, where feasible. | F2.4.3 |
| **T2.4.3.3** | MOSAICS shall limit access to facility ICS data in transit to authorized users. | F2.4.3 |
| **T2.4.3.4** | MOSIACS shall identify facility ICS data flowing in unauthorized channels. | F2.4.3 |
| **T2.4.3.5** | MOSAICS shall have data integrity safeguards, including provenance tracking, for data in transit. | F2.4.3 |

| | | |
|---|---|---|
| **T2.4.5.1** | MOSAICS shall protect ICS monitoring data from exfiltration. | F2.4.5 |
| **T2.4.5.3** | MOSAICS shall employ network monitoring devices (e.g., firewall, IDS, etc.) to control ICS traffic flow via blocking IPs, blocking domain/urls, and segmenting subnets. | F2.4.5 |
| **T2.4.6.1** | MOSAICS shall employ network monitoring devices (e.g., firewall, IDS, etc.)to control MOSAICS traffic flow via blocking IPs, blocking domain/urls, and segmenting subnets. | F2.4.6 |
| **T2.4.7.1** | MOSAICS shall perform integrity checks on SCADA system components protected by MOSAICS. | F2.4.7 |
| **T2.4.7.2** | MOSAICS shall perform integrity checks on ICS Physical Systems protected by MOSAICS. | F2.4.7 |
| **T2.4.7.3** | MOSAICS shall perform integrity checks on MOSAICS components. | F2.4.7 |
| **T2.7** | **Protective Technology Technical Requirements** | |
| **T2.7.1.1** | MOSAICS shall log security-related actions and operations in the ICS network and | F2.7.1 |
| **T2.7.1.8** | MOSAICS shall attach to a Global Positioning System or Network Time Protocol for log stamps. | F2.7.1 |
| **T2.7.2.1** | MOSAICS shall automatically log alerts on error conditions as they occur. | F2.7.2 |
| **T2.7.2.2** | MOSAICS shall report the status of its own error conditions. | F2.7.2 |
| **T2.7.2.3** | MOSAICS shall automatically provide alerts for logged errors to an operator. | F2.7.2 |
| **T2.7.2.4** | MOSAICS shall automatically log its own failures as they occur. | F2.7.2 |
| **T2.7.2.5** | MOSAICS shall automatically provide alerts for failures to an operator. | F2.7.2 |
| **T2.7.2.6** | MOSAICS shall log all actions that it performs, including provenance (e.g., associated information origin). | F2.7.2 |
| **T2.7.2.7** | MOSAICS shall provide the ability to archive historical log data (i.e., data on alerts, actions taken) for a minimum of 30 days. | F2.7.2 |
| **T2.7.2.8** | MOSAICS shall provide the ability to recover previously archived historical log data. | F2.7.2 |
| **T2.8** | **Operational Availability Requirements** | |
| **T2.8.1.1** | MOSAICS shall function as expected without errors or failures for at least <23.5> hours per day (value to be supplied by enterprise). Operational availability. | F2.8.1 |
| **T2.8.1.2** | MOSAICS shall function as expected without errors or failures at least <9,000> hours before any malfunction (value to be supplied by enterprise). Mean time between | F2.8.1 |
| **T2.8.1.3** | MOSAICS shall apply updates, such as enhancements, bug fixes, and integration module developments to MOSAICS products as they are received from the product vendor. | F2.8.1 |
| **T2.8.1.4** | MOSAICS shall have the ability to install authorized software patches received. | F2.8.1 |
| **T2.8.1.5** | MOSAICS shall provide the ability for the user to specify either automatic or manual application of approved updates for installing software patches to the MOSAICS | F2.8.1 |
| **T3.0** | **MOSAICS Monitor and Detection Technical Requirements** | |
| **T3.1** | **Baseline Comparison Technical Requirements** | |
| **T3.1.2.1** | MOSAICS shall check for BIOS and other Firmware modifications. | F3.1.2 |
| **T3.1.2.3** | MOSAICS intrusion detection capability shall employ scanning to gather and track detailed configuration information about the ICS. | F3.1.2 |
| **T3.1.2.5** | MOSAICS shall detect updates to ICS component inventory in real time. | F3.1.2 |
| **T3.1.2.10** | MOSAICS shall detect new traffic, potentially unauthorized traffic, and device | F3.1.2 |
| **T3.1.2.11** | MOSAICS shall produce a status change event within 30 seconds of the event occurring for passively monitored ICS components. | F3.1.2 |
| **T3.1.2.12** | MOSAICS shall detect changes in registry values. | F3.1.2 |
| **T3.1.2.13** | MOSAICS intrusion detection capability shall track changes in hardware. | F3.1.2 |
| **T3.2** | **Continuous Monitoring Technical Requirements** | |
| **T3.2.1.2** | MOSAICS shall monitor system logs for application failures. | F3.2.1 |

| | | |
|---|---|---|
| **T3.2.1.5** | MOSAICS shall monitor the status of facility ICS components based on state changes or at a facility provided frequency. | F3.2.1 |
| **T3.2.2.1** | MOSAICS shall create error events/reporting for communication failures. | F3.2.2 |
| **T3.2.2.2** | MOSAICS shall create error events/reporting for unacceptable device behavior. | F3.2.2 |
| **T3.2.2.3** | MOSAICS shall monitor MOSAICS health and status. | F3.2.2 |
| **T3.2.3.1** | MOSAICS shall support a method to import log files from HBSS sensors on embedded host equipment for the purpose of monitoring host access. | F3.2.3 |
| **T3.2.3.4** | MOSAICS shall monitor HBSS logs for suspect remote accesses. | F3.2.3 |
| **T3.2.3.8** | MOSAICS shall control local and remote user access to networks and devices. | F3.2.3 |
| **T3.2.3.10** | MOSAICS shall detect unexpected accesses into the ICS components via a wireless access point. | F3.2.3 |
| **T3.2.3.14** | MOSAICS shall detect repeated/continuous logins. | F3.2.3 |
| **T3.2.3.15** | MOSAICS shall detect repeated/continuous logouts. | F3.2.3 |
| **T3.2.5.4** | The MOSAICS solution shall (?passively poll/actively query?) the control systems | F3.2.5 |
| **T3.2.9.1** | MOSAICS shall integrate multiple techniques for detection (Ex. stateful protocol, pattern, signature, etc.). | F3.2.9 |
| **T3.2.9.2** | For each ICS protocol that MOSAICS monitors, MOSAICS shall maintain a table of 'normal' and 'violation' actions. | F3.2.9 |
| **T3.2.9.3** | The MOSAICS violations tables shall be configurable by the MOSAICS administrator. | F3.2.9 |
| **T3.2.9.4** | MOSAICS shall classify ICS protocol actions (normal versus violation) based upon protocol functions and record an function violation event when monitoring detected a protocol action classified as a violation. | F3.2.9 |
| **T3.2.9.5** | MOSAICS shall classify ICS protocol actions (normal versus violations) based upon behavioral analysis and record an violation event when monitoring detected an | F3.2.9 |
| **T3.2.9.6** | MOSAICS shall be capable of operating multiple, simultaneous behavioral analytics ( 10 analysis threads). | F3.2.9 |
| **T3.2.9.7** | MOSAICS shall support a programmable interface to its behavioral analysis capabilities (python, others) for the purpose of adding custom analytics. | F3.2.9 |
| **T3.2.9.8** | MOSAICS shall provide the capability to learn normal and abnormal system behavior. | F3.2.9 |
| **T3.2.9.9** | MOSAICS shall provide the capability to integrate anomaly detection analytics beyond those that are signature based. (Ex. machine learning, etc.) | F3.2.9 |
| **T3.2.9.16** | MOSAICS shall detect ICS component malfunctions. | F3.2.9 |
| **T3.2.9.36** | MOSAICS shall monitor for anomalous Kerberos logons. | F3.2.9 |
| **T3.2.11.1** | MOSAICS IDS shall alert on hidden files on the ICS network. | F3.2.11 |
| **T3.2.11.2** | MOSAICS shall alert on file accesses made via removable media. | F3.2.11 |
| **T3.2.11.3** | MOSAICS shall provide the capability to use a whitelist. | F3.2.11 |
| **T3.2.11.4** | MOSAICS shall monitor access events on ICS components, based upon ICS logs provided to MOSAICS by the ICS components, in order to identify usage rules and policy | F3.2.11 |
| **T3.2.11.7** | MOSAICS shall display an alert when violations of access/usage rules and policies on facility ICS components are detected. | F3.2.11 |
| **T3.2.11.8** | MOSAICS shall block actions performed by users not possessing the appropriate access rights/roles. | F3.2.11 |
| **T3.2.11.9** | MOSAICS shall restrict network access to users not possessing the appropriate access rights/roles. | F3.2.11 |
| **T3.2.11.10** | MOSAICS shall detect actions performed by users not possessing the appropriate access rights/roles. | F3.2.11 |

| | | |
|---|---|---|
| **T3.2.11.11** | MOSAICS shall monitor actions performed by users not possessing the appropriate access rights/roles. | F3.2.11 |
| **T3.2.13.2** | MOSAICS shall display an alert when unauthorized use of external devices on the ICS network is detected. | F3.2.13 |
| **T3.2.14.1** | MOSAICS shall generate a system event and ingest this event to the MOSAICS data store. | F3.2.14 |
| **T3.2.14.2** | The MOSAICS solution will share information from detection of threats to mitigation actions taken to resolve. | F3.2.14 |
| **T3.2.14.5** | MOSAICS shall automate detection of events by using system generated alarms. | F3.2.14 |
| **T3.2.14.6** | MOSAICS IDS shall alert on unknown IP addresses. | F3.2.14 |
| **T3.2.14.9** | MOSAICS shall generate alerts for detected repeated/continuous logouts. | F3.2.14 |
| **T3.2.14.23** | MOSAICS shall generate a system event when actions performed by users not possessing the appropriate access rights/role are detected. | F3.2.14 |
| **T3.2.14.30** | MOSAICS shall log account changes and privileged use. | F3.2.14 |
| **T3.2.14.31** | MOSAICS shall check for multiple logins with the same credentials. | F3.2.14 |
| **T3.2.14.32** | MOSAICS shall check for default passwords. | F3.2.14 |
| **T3.2.14.33** | MOSAICS shall provide the ability to perform user account administration. | F3.2.14 |
| **T3.2.14.34** | MOSAICS shall provide the ability to perform platform usage audits. | F3.2.14 |
| **T3.3** | **Security Technical Requirements** | |
| **T3.3.5.1** | MOSAICS shall analyze data flows of MOSAICS components and systems for threats to MOSAICS. | F3.3.5 |
| **T4.0** | **MOSAICS Analysis Technical Requirements** | |
| **T4.1** | **Anomaly Analysis Technical Requirements** | |
| **T4.1.1.3** | MOSAICS shall process sensor data to identify events and save them in the MOSAICS data store. | F4.1.1 |
| **T4.1.1.4** | MOSAICS shall capture the following event types, i.e., up/down status of ICS devices, anomalous ICS traffic, un-authorized ICS control traffic, login connection, running processes, open files, and changes to files or system settings. | F4.1.1 |
| **T4.1.2.1** | MOSAICS shall store all sensor data, host-based and network-based, in the MOSAICS data store for later processing by anomaly detection algorithms. | T4.1.2 |
| **T4.1.3.1** | MOSAICS shall execute anomaly detection algorithms on sensor data, including host sensor and network sensor data. | F4.1.3 |
| **T4.1.3.2** | MOSAICS shall run anomaly detection using time series analysis, pattern analysis and policy based algorithms. | F4.1.3 |
| **T4.1.3.3** | MOSAICS anomaly detection algorithms shall be configurable in the time series generation, the specific patterns being monitored and the specific policies to be | F4.1.3 |
| **T4.1.3.5** | MOSAICS shall provide an API to allow for the addition of new software for anomaly detection algorithms. | F4.1.3 |
| **T4.1.3.21** | MOSAICS shall allow for custom API programming interfaces. | F4.1.3 |
| **T4.1.3.22** | MOSAICS shall automatically measure the characteristics of expected facility ICS activity in order to define normal behaviors. | F4.1.3 |
| **T4.1.4.6** | MOSAICS intrusion detection capability shall perform analytics in real time when forwarded network traffic from a span port on the ICS network. | F4.1.4 |
| **T4.1.5.2** | MOSAICS shall perform integrity checks on facility ICS components. | F4.1.5 |
| **T4.1.5.3** | MOSAICS shall perform diagnostic procedures on facility ICS components. | F4.1.5 |
| **T4.1.5.16** | MOSAICS shall support methods to analyze sources of potential threat, including distributed and centralized methods (Ex. aggregation of IDS and system level unauthorized changes, etc.). | F4.1.5 |

| | | |
|---|---|---|
| **T4.1.5.17** | MOSAICS shall provide the capability to model and characterize threats in the sources of input that can be used (Ex. syslog, etc.). | F4.1.5 |
| **T4.1.13.1** | MOSAICS shall analyze data flows of facility ICS components and systems for threats to the facility ICS or critical infrastructure. | F4.1.13 |
| **T4.1.17.1** | MOSAICS shall display analyses correlations. | F4.1.17 |
| **T4.2** | **Event Technical Requirements** | |
| **T4.2.1.2** | MOSAICS shall categorize events as an incident (e.g. root level / user level intrusion, denial of service, or malicious logic), a reportable event (e.g. unsuccessful activity attempt, non-compliance activity, reconnaissance, investigating, or explained anomaly), or non-reportable event and update the event meta-data in the MOSAICS | F4.2.1 |
| **T4.2.1.3** | MOSAICS shall distinguish between threats, vulnerabilities, faults, errors and failures. | F4.2.1 |
| **T4.2.2.2** | MOSAICS shall provide the capability for root cause of decision support analytics for those of questionable or unhealthy state. | F4.2.2 |
| **T4.2.2.4** | MOSAICS shall perform log analysis. | F4.2.2 |
| **T4.2.3.1** | MOSAICS shall provide centralized analysis summary and detailed logs of anomalous activity on the system networks and devices. | F4.2.3 |
| **T4.2.3.5** | MOSAICS shall maintain an index of all incidents and reportable events in the MOSAICS data store for further investigative purposes. | F4.2.3 |
| **T4.2.3.7** | MOSIACS shall collect all cyber, physical sensor, and component status data of the ICS and MOSAICS components for forensic analysis at a later time. | F4.2.3 |
| **T4.2.5.1** | MOSAICS shall support a variety of alerting mechanisms, including visual alert on a dashboard, email alerts, and logging alerts in the MOSAICS data store. | F4.2.5 |
| **T5.0** | **MOSAICS Visualization Technical Requirements** | |
| **T5.1** | **Detected Event Visualization Technical Requirements** | |
| **T5.1.2.5** | MOSAICS displays shall integrate with existing operational visualization systems at the identified site. | F5.1.2 |
| **T5.1.2.8** | MOSAICS shall provide the capability to display the decision logic which provided the determination and application of ACI TTP alert classification. | F5.1.2 |
| **T5.1.2.9** | MOSAICS shall provide the capability to display any thresholds which trigger an alert or cause an event to be brought to the user's attention. | F5.1.2 |
| **T5.1.2.10** | MOSAICS shall provide the capability to display workflows associated with alerts and | F5.1.2 |
| **T5.1.2.16** | MOSAICS shall display system health information for network assets. | F5.1.2 |
| **T5.1.4.3** | MOSAICS shall display an alert for repeated/continuous logins. | F5.1.4 |
| **T5.1.4.4** | MOSAICS shall display an alert for detected repeated/continuous logouts. | F5.1.4 |
| **T5.1.4.10** | MOSAICS shall display an alert for detected rapid logons/logoffs. | F5.1.4 |
| **T5.1.4.15** | MOSAICS shall generate an alert when ICS component malfunctions are detected. | F5.1.4 |
| **T5.1.4.19** | MOSAICS shall generate an alert when rapid logon/logoffs are detected. | F5.1.4 |
| **T5.2** | **Facility Status and Impact Visualization Technical Requirements** | |
| **T5.2.1.1** | MOSAICS shall provide the capability to aggregate status information by facility. | F5.2.1 |
| **T5.2.2.5** | MOSAICS shall provide the capability to display the responsible party and contact information of devices monitored by MOSAICS. | F5.2.2 |
| **T5.2.2.7** | MOSAICS shall provide the capability to display processes running on devices monitored by MOSAICS. | F5.2.2 |
| **T5.2.2.11** | MOSAICS shall provide the capability to display network connections to adjacent facilities. | F5.2.2 |
| **T5.2.2.12** | MOSAICS shall provide administrator access to workflow performance data. | F5.2.2 |

| | | |
|---|---|---|
| **T5.2.2.16** | MOSAICS shall have the ability to display workflow performance data to a MOSAICS administrator. | F5.2.2 |
| **T5.2.3.1** | MOSAICS shall provide the capability for color coded alarms. | F5.2.3 |
| **T5.2.6.1** | MOSAICS shall provide text-based alerts. | F5.2.6 |
| **T5.2.6.2** | MOSAICS shall display the context of cyber threat impacts to the mission criticality of facility ICS components that may be impacted. | F5.2.6 |
| **T5.3** | **Alert Management Technical Requirements** | |
| **T5.3.1.5** | MOSAICS shall provide the capability to display mitigations or workflows nested within a given workflow. | F5.3.1 |
| **T5.3.2.1** | MOSAICS shall create an alarm when an alert is not acknowledged. | F5.3.2 |
| **T5.3.3.2** | MOSAICS displays shall be configurable by the user (colors of alarms, blinking alarms, audible alarms). | F5.3.3 |
| **T5.3.3.3** | MOSAICS shall minimize, to the extent possible, nuisance alarms. | F5.3.3 |
| **T5.3.3.4** | MOSAICS shall provide the capability to set alarm thresholds. | F5.3.3 |
| **T5.3.3.5** | MOSAICS shall provide the capability to define alarms. | F5.3.3 |
| **T5.3.3.6** | MOSAICS shall provide the capability to send alarms via email and text message to pre-defined list of recipients. | F5.3.3 |
| **T5.3.3.8** | MOSAICS shall track alerts assigned to users until they are resolved. | F5.3.3 |
| **T6.0** | **MOSAICS Decision Technical Requirements** | |
| **T6.1** | **Event / Incident Response Analysis Technical Requirements** | |
| **T6.1.1.1** | The MOSAICS orchestration capability shall have the ability to execute workflows triggered in real time (i.e., real-time processing). | F6.1.1 |
| **T6.1.1.2** | The MOSAICS orchestration capability shall provide the ability to schedule workflows. | F6.1.1 |
| **T6.1.1.3** | The MOSAICS orchestration capability shall provide the ability to set thresholds for actions to occur (e.g., define a default timeout for receiving responses). | F6.1.1 |
| **T6.1.1.4** | The MOSAICS orchestration capability shall have the ability to execute multiple workflows concurrently (i.e., batch processing). | F6.1.1 |
| **T6.1.1.5** | The MOSAICS orchestration capability shall have the ability to execute multiple, nested workflows, which are part of one large workflow. | F6.1.1 |
| **T6.1.1.6** | The MOSAICS orchestration capability shall have the ability to execute multiple, interconnected workflows, which are part of one large workflow. | F6.1.1 |
| **T6.1.1.7** | The MOSAICS orchestration capability shall have the ability to execute individual workflows initiated from the same trigger event independent from any other orchestration tool within the same enterprise. | F6.1.1 |
| **T6.1.1.8** | The MOSAICS orchestration capability shall have the ability to execute the same workflow from more than one indicator. | F6.1.1 |
| **T6.1.1.9** | The MOSAICS orchestration capability shall provide the ability to include conditional logic in workflows. | F6.1.1 |
| **T6.1.1.10** | The MOSAICS orchestration capability shall provide the ability to reverse the automated actions of a previous workflow (Rollback). | F6.1.1 |
| **T6.1.1.11** | The MOSAICS orchestration capability shall continually be aware of the state of any workflow (Workflow State Awareness). | F6.1.1 |
| **T6.1.1.12** | The MOSAICS orchestration capability shall continually be aware of the sequence of tasks of any workflow (Workflow Sequence Awareness). | F6.1.1 |
| **T6.1.1.13** | The MOSAICS orchestration capability shall provide the ability to catalog workflows. | F6.1.1 |
| **T6.1.1.14** | The MOSAICS orchestration capability shall provide the ability to control workflow versioning. | F6.1.1 |

| | | |
|---|---|---|
| **T6.1.1.15** | The MOSAICS orchestration capability shall provide the ability to archive previous workflows for a minimum of one year. | F6.1.1 |
| **T6.1.1.16** | The MOSAICS orchestration capability shall provide the ability to recover archived workflows. | F6.1.1 |
| **T6.1.1.17** | MOSAICS shall provide the ability for users to define system operating parameters that are defined in their enterprise policies and procedures. | F6.1.1 |
| **T6.1.1.18** | MOSAICS shall provide the ability for users to edit their previously entered system operating parameters that are defined in their enterprise policies and procedures. | F6.1.1 |
| **T6.1.1.19** | MOSAICS shall keep track of the association between system operating parameters vs. the workflows. | F6.1.1 |
| **T6.1.1.20** | The MOSAICS orchestration capability shall adhere to the mutual principle of least privilege in relation to any process interfaces. | F6.1.1 |
| **T6.1.1.21** | The MOSAICS orchestration capability shall adhere to the mutual principle of least privilege in relation to any user interfaces. | F6.1.1 |
| **T6.1.1.22** | The MOSAICS orchestration capability shall adhere to the mutual principle of least privilege in relation to any tool interfaces. | F6.1.1 |
| **T6.1.1.23** | The MOSAICS system will capture and maintain audit logging of all human decisions and automated actions performed on the MOSAICS system; (for TBD period of time). | F6.1.1 |
| **T6.1.1.28** | MOSAICS shall recommend manual and automated courses of action to improve security hardening and resiliently responding and recovering to malicious events. | F6.1.1 |
| **T6.1.1.29** | MOSAICS shall recommend COA that allows for integrated response of the cyber defender and system engineer, considers the time scale and distinguishes role response (Ex. integrates automated/manual cyber defender actions vs field engineer procedures, etc.). | F6.1.1 |
| **T6.1.1.45** | MOSAICS shall provide the capability for the user to schedule back ups of MOSAICS workflows. | F6.1.1 |
| **T6.1.1.46** | MOSAICS shall provide the capability to perform back ups of MOSAICS workflows. | F6.1.1 |
| **T6.1.1.47** | MOSAICS shall provide the capability for the user to schedule back ups of MOSAICS work flow data. | F6.1.1 |
| **T6.1.1.48** | MOSAICS shall provide the capability to perform back ups of MOSAICS work flow data. | F6.1.1 |
| **T6.1.1.49** | MOSAICS shall have the ability to back up the MOSAICS orchestration service | F6.1.1 |
| **T6.1.1.50** | MOSAICS shall provide the capability for the user to schedule back ups of the MOSAICS orchestration service configuration. | F6.1.1 |
| **T6.1.1.51** | MOSAICS shall have the ability to failover operations to a backup orchestration tool in the event of a failure or during maintenance downtime. | F6.1.1 |
| **T6.1.1.52** | MOSAICS shall have the ability to capture its performance data. | F6.1.1 |
| **T6.1.2.1** | MOSAICS orchestration capability shall automate current business or technical processes as described by the ACI TTP. | F6.1.2 |
| **T6.1.2.3** | MOSAICS shall determine a range of COAs to address the threat. | F6.1.2 |
| **T6.1.2.4** | MOSAICS shall generate suggested COAs based on integrity check results. | F6.1.2 |
| **T6.1.2.6** | MOSAICS shall utilize facility priorities and status information when determining a COA. | F6.1.2 |
| **T6.1.2.7** | MOSAICS shall utilize existing threat and severity to the facility information when determining a COA. | F6.1.2 |
| **T6.1.2.8** | MOSAICS shall utilize available CI resources information when determining a COA. | F6.1.2 |
| **T6.1.3.2** | MOSAICS shall display COAs to the user, upon request. | F6.1.3 |
| **T6.1.4.1** | The MOSAICS orchestration capability shall provide a user interface for creating workflows (Workflow Creation). | F6.1.4 |

| | | |
|---|---|---|
| **T6.1.4.2** | The MOSAICS orchestration capability shall provide a user interface for editing existing workflows (Workflow Editing). | F6.1.4 |
| **T6.1.4.3** | The MOSAICS orchestration capability shall provide a user interface for creating playbooks (Playbook Creation). | F6.1.4 |
| **T6.1.4.4** | The MOSAICS orchestration capability shall provide a user interface for editing existing playbooks (Playbook Editing). | F6.1.4 |
| **T6.1.4.5** | The MOSAICS orchestration capability shall provide a user interface for creating Courses Of Action (COAs) (COA Creation). | F6.1.4 |
| **T6.1.4.6** | The MOSAICS orchestration capability shall provide a user interface for editing existing COAs (COA Editing). | F6.1.4 |
| **T6.1.4.7** | The MOSAICS orchestration capability shall provide a command line or debug interface. | F6.1.4 |
| **T6.1.4.10** | MOSAICS shall provide the capability for users to dictate human in the loop decision | F6.1.4 |
| **T6.1.4.11** | Upon a human in the loop decision, MOSAICS shall automate appropriate human in the loop selected responses. | F6.1.4 |
| **T6.1.4.12** | MOSAICS shall provide the capability for the user to determine a COA utilizing existing threat and severity to the facility information. | F6.1.4 |
| **T6.1.4.15** | MOSIACS shall provide the capability for the user to determine a COA utilizing available CI resources information. | F6.1.4 |
| **T6.1.4.16** | MOSAICS shall provide the capability for a user to determine a COA utilizing existing mission priorities. | F6.1.4 |
| **T7.0** | **MOSAICS Mitigation Technical Requirements** | |
| **T7.1** | **Event / Incident Response Execution Technical Requirements** | |
| **T7.1.1.1** | MOSAICS shall utilize security sensor data and decision support analytics to develop Courses of Action (COA) options for the user. | F7.1.1 |
| **T7.1.1.3** | MOSIACS shall provide the capability to modify COA based upon changing systems circumstances and impact. | F7.1.1 |
| **T7.1.1.5** | MOSAICS shall provide the operators with options for mitigation and allow the user to select their preferred technique. | F7.1.1 |
| **T7.1.3.3** | MOSAICS shall provide to the user software configuration parameters and health of ICS components to enable a mitigative response. | F7.1.3 |
| **T7.1.3.4** | MOSAICS shall provide to the user the specific aspects of the ICS components that are affected and to which the mitigation applies. | F7.1.3 |
| **T7.1.3.5** | MOSAICS shall provide the capability for the user to switch selected facility ICS components assume control. | F7.1.3 |
| **T7.1.3.6** | MOSAICS shall provide the capability for the user to segment affected system components, if selected. | F7.1.3 |
| **T7.1.3.7** | MOSAICS shall provide the capability to perform system segmentation for components. | F7.1.3 |
| **T7.1.3.8** | MOSAICS shall provide the capability for the user to stop selected facility ICS component operations. | F7.1.3 |
| **T7.1.3.9** | MOSAICS shall provide information to the user regarding affected facility ICS component operations that may need to be stopped by the user. | F7.1.3 |
| **T7.1.3.10** | MOSAICS shall provide the capability for the user to directly or indirectly recognize operations and associated components that need to be reset or stopped as the result of a cyber attack or in protection from an attack. | F7.1.3 |
| **T7.1.3.11** | MOSIACS shall provide the capability to the user to apply mitigation techniques to the ICS and MOSAICS components dynamically and confirm effectiveness. | F7.1.3 |
| **T7.1.4.2** | MOSAICS orchestration capability shall command the IDS to block applications. | F7.1.4 |
| **T7.1.4.3** | MOSAICS shall block unknown programs. | F7.1.4 |

| | | |
|---|---|---|
| **T7.1.4.6** | MOSIACS shall have the ability to modify the network segment architecture in response to cyber attack. | F7.1.4 |
| **T7.1.4.7** | MOSAICS shall be able to segment affected system components, if selected. | F7.1.4 |
| **T7.1.4.8** | MOSAICS orchestration capability shall update whitelists. | F7.1.4 |
| **T7.1.5.1** | MOSAICS shall provide the capability for the user to update the ICS component configuration information. | F7.1.5 |
| **T7.1.5.2** | MOSAICS shall provide the capability for the user to modify the protection level of selected facility ICS components to align with mission criticality. | F7.1.5 |
| **T7.1.5.3** | MOSAICS shall provide relevant physical process and security decision support information that allows the user to effectively evaluate the protection options versus benefit and impacts. | F7.1.5 |
| **T7.1.6.1** | MOSAICS shall provide the capability for the user to select a graded response based upon mission criticality that will increase the protection level on selected ICS | F7.1.6 |
| **T7.1.16.1** | MOSAICS shall provide the user the capability to monitor the effectiveness of each mitigation step on the basis of ICS and process operational status of affected components and process systems. | F71.16 |
| **T7.2** | **Implement ACI TTP Technical Requirements** | |
| **T7.2.1.1** | MOSAICS shall implement (or automate) appropriate ACI TTPs to mitigate cyber threats. | F7.2.1 |
| **T7.2.1.2** | MOSAICS shall implement (or automate appropriate ACI TTPs to identify cyber threats. | F7.2.1 |
| **T7.2.1.3** | MOSAICS shall implement (or automate) appropriate ACI TTPs to recover from cyber threats. | F7.2.1 |
| **T8.0** | **MOSAICS Recovery Technical Requirements** | |
| **T8.1** | **Recovery Planning Technical Requirements** | |
| **T8.1.5.1** | MOSAICS shall provide to the user the capability directly or indirectly to start any stopped components and restart associated operations. | F8.1.5 |
| **T8.1.5.2** | MOSIACS shall allow the user to directly or indirectly-restart a selected facility ICS component after the mitigation has been completed. | F8.1.5 |
| **T8.1.5.3** | MOSAICS shall provide the capability for the user to restart selected system facility ICS components. | F8.1.5 |
| **T8.1.5.4** | MOSAICs shall provide the capability for users to reinitialize selected facility ICS system components. | F8.1.5 |
| **T8.1.5.5** | MOSAICS shall provide the capability for the user to reset the access permissions on identified facility ICS components. | F8.1.5 |
| **T8.1.5.6** | MOSAICS shall provide an indication to the user when physical (e.g. hardware) facility ICS components require replacement. | F8.1.5 |
| **T8.1.5.7** | MOSAICS shall provide the capability for the user to reconnect selected facility ICS components. | F8.1.5 |
| **T8.1.5.8** | MOSAICS shall provide the capability for the user to reconnect selected MOSAICS components. | F8.1.5 |
| **T8.1.6.1** | MOSAICS shall have the ability to recover from system failure. | F8.1.6 |
| **T8.1.6.2** | MOSAICS shall have the ability to recover from system corruption. | F8.1.6 |
| **T8.1.6.3** | MOSAICS shall have the ability to reinitialize selected MOSAICS components. | F8.1.6 |
| **T8.1.6.4** | MOSAICS shall have the ability to reset the access permissions on identified facility ICS components. | F8.1.6 |
| **T8.1.6.5** | MOSAICS shall provide an indication to the user when non-physical (e.g. software) facility ICS components require replacement. | F8.1.6 |
| **T8.1.6.6** | MOSAICS shall provide an indication to the user when physical (e.g. hardware) MOSAICS components require replacement. | F8.1.6 |

| | | |
|---|---|---|
| **T8.1.6.7** | MOSAICS shall provide an indication to the user when MOSAICS software components require replacement. | F8.1.6 |
| **T8.1.6.8** | MOSAICS shall have the ability to reconnect selected facility ICS components. | F8.1.6 |
| **T8.1.6.9** | MOSAICS shall have the ability to reconnect selected MOSAICS components. | F8.1.6 |
| **T8.1.6.10** | MOSAICS shall have the ability to restart selected system MOSAICS components. | F8.1.6 |
| **T8.2** | **Recovery Forensic Technical Requirements** | |
| **T8.2.1.1** | MOSAICS shall provide the capability to export system component data for forensic | F8.2.1 |
| **T8.2.1.2** | MOSAICS shall archive selected system component data for nn days. | F8.2.1 |
| **T8.3** | **Recovery Execution Technical Requirements** | |
| **T8.3.12.1** | MOSAICS shall provide the capability for the user to schedule back ups of MOSAICS interface module data. | F8.3 |
| **T8.3.12.2** | MOSAICS shall provide the capability to back up MOSAICS interface module data. | F8.3 |
| **T9.0** | **MOSAICS Information Sharing Technical Requirements** | |
| **T9.1** | **Event / Incident Communication Technical Requirements** | |
| **T9.1.1.1** | MOSAICS shall provide a user interface to display cyber data. | F9.1.1 |
| **T9.1.1.2** | MOSAICS shall allow the cyber operator to select cyber data to share. | F9.1.1 |
| **T9.1.1.3** | MOSAICS shall provide a user interface to display ICS data. | F9.1.1 |
| **T9.1.1.4** | MOSAICS shall allow the cyber operator to select relevant ICS data to share. | F9.1.1 |
| **T9.1.1.5** | MOSAICS shall be able to share operator selected data in an automated fashion. | F9.1.1 |
| **T9.1.2.1** | MOSAICS shall be able to share data to multiple external stakeholders simultaneously. | F9.1.2 |
| **T9.1.2.2** | MOSAICS shall mutually authenticate organizations with which it shares data. | F9.1.2 |
| **T9.1.2.3** | MOSAICS shall provide the ability to share event data in a standard machine-to-machine messaging format. | F9.1.2 |
| **T9.1.2.5** | MOSAICS shall support indicator sharing. | F9.1.2 |
| **T9.2** | **Threat Information Communication Technical Requirements** | |
| **T9.2.1.1** | MOSAICS shall be able to receive threat data from multiple external stakeholders simultaneously. | F9.2.1 |
| **T9.2.1.2** | MOSAICS shall mutually authenticate organizations from which it receives threat data. | F9.2.1 |
| **T9.2.1.4** | MOSAICS shall receive threat data utilizing the Structured Threat Information Expression (STIX) version 2.0 format. | F9.2.1 |
| **T9.2.1.5** | MOSAICS shall have the ability to store threat data received from external sources for a minimum of 30 days. | F9.2.1 |
| **T9.2.1.6** | MOSAICS shall provide the ability to process external threat data to determine applicability to the local ICS system. | F9.2.1 |
| **T9.2.2.1** | MOSAICS shall provide context for facility ICS impact in threat information data. | F9.2.2 |
| **T9.2.2.2** | MOSAICS shall provide context for mission criticality in threat information data. | F9.2.2 |