Regardless of whether you are doing a retrofit or new construction of an industrial control system, make cybersecurity part of your acceptance testing. AIT presents a list of some of the security testing and reviews that should occur during FAT and SAT.

Building Cyber-security into ICS Acceptance Testing

Security FAT and SAT as a Service

AIT
Applied Integrated Technologies

Isiah Jones
Cyber Engineer (ICS OT IIoT IoT)
Applied Integrated Technologies
August 2022

Asset owners and operators must build cybersecurity protections into new and upgraded Industrial Control Systems (ICS). This increases process safety and reliability by reducing cybersecurity risk, thereby protecting what is undoubtedly a major business investment. Acceptance testing, both factory (FAT) and site (SAT), are important phases of the project and is the best time to introduce cybersecurity testing into the project.

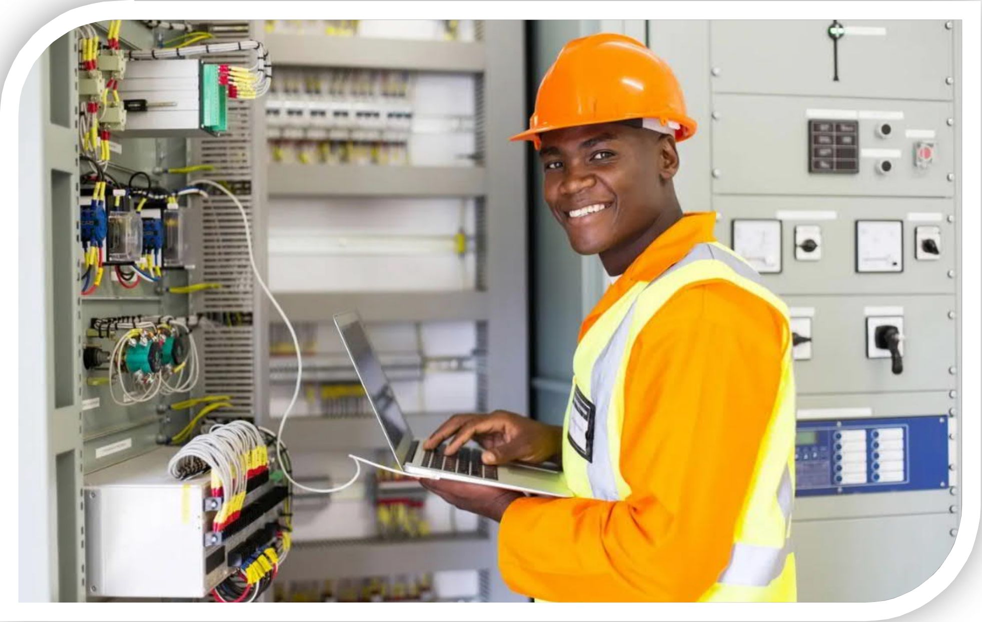
This testing applies to all sorts of ICS including automation systems, operational technology (OT), safety systems, embedded systems, and industrial internet of things (IIoT). Regardless of whether you are doing a retrofit or a new greenfield project there are a lot of cybersecurity reviews and tests to perform. Here is an abbreviated list of some of the security testing and reviews that should occur during FAT and SAT.

- Checking equipment list, bills of materials and design specifications to build, test and document make, model, versions, ports, protocols, and features of assets believed to be acquired per project engineering design and end user requirements. This includes building and checking an accurate asset inventory
- Ensuring process flow diagrams (PFD), network diagrams, and piping & instrumentation diagrams (P&ID) properly show how each component interacts with each other.
- Documenting security zones and conduits. This includes defining the security requirements of each zone and showing the types of conduits (e.g., mechanical, electrical, RF/wireless, ethernet, fiber, serial and fieldbus), ports and protocols (e.g. BACnet MSTP vs BACnet/IP, CIP ENIP vs DeviceNet vs ControlNet, OPC UA vs OPC DA vs OPC-XML-DA), and interfaces used between and within each component.
- Checking user interface features for role-based access control, multifactor authentication, least privilege and least functionality for human users, APIs, and service accounts
- Penetration testing and vulnerability scanning of components including applications, interfaces, network zones and devices
- Checking security features against ISA/IEC 62443 part 4-2 and 3-3 foundational requirements for products
- Ensuring PLC Top 20 secure coding practices are used in the PLC IEC 61131 logic (e.g., Ladder Logic, Function Block Diagram, Function Chart)
- Reviewing and testing structure text and script-based languages against OWASP Top 10 (e.g., SQL, Python, JSON, Siemens SCL)
- Checking configurations of firewalls, routers, switches, applications, operating systems, RTOS, gateways, IO devices, controllers, drives, virtual machines, sensors, programming, and calibration software for security weaknesses and bad or insecure configuration practices
- Updating punch lists with security findings and recommended mitigations then retesting initial implemented mitigations for correctness and updating risk registers with remaining unresolved residual risks that could not be mitigated during FAT and or SAT

Many security practices, frameworks, guidelines, and standards have requirements that require security validation, testing and verification to occur during the factory acceptance test and site acceptance test phases of projects. If you are following one of the standards below, these tests apply to you.

- Risk Management Framework (RMF) Step 4 Assess Security Controls – where initial FAT, SAT, systems validation, and initial mitigations are captured on Plans of Actions and Milestones (POA&M)
- NIST SP 800-160 Systems Security Engineering – Verification and Validation Technical Process phases
- ISA/IEC 62443 part 3-2 – Security Risk Assessment for Systems & ISA84.00.09 Security for Safety Systems – identifying systems and components under consideration and performing detailed technical risk assessment of systems and components under consideration in scope of project phase
- NIST Cybersecurity Framework (NIST CSF) - Risk Assessment (ID.RA) - ID.RA-1: Asset vulnerabilities are identified and documented, Supply Chain Risk Management (ID.SC) - ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations
- NIST SP 800-53rev5 & 82rev2 – CA-2 (Control Assessments), CA-8 (Penetration Testing), RA-3 (Risk Assessment), SR-6 (Supplier Assessments and Reviews), SR-10 (Inspection of Systems or Components)

Unfortunately, many owner/operators, vendors, and integrators lack the ICS cybersecurity trained staff to conduct these ICS cybersecurity focused testing and reviews during fast-moving FATs and SATs. AIT's CMAC team can supplement your staff and ensure these critical tests are conducted properly.



AIT's security engineering professionals have global experiences providing security FAT, SAT, systems validation and verification testing, and review services for commercial and government customers. We can supply our expertise during design, build, integration, verification, and/or validation phases of greenfield and retrofit projects. AIT's ICS OT security engineers are regular contributors and members of ISA/IEC 62443 and ISA84.00.09 standards committee working groups. AIT's staff also maintain current GICSP and CISSP certifications.

AIT's CMAC team offers FAT and SAT as a service. To seek out security FAT and SAT services please contact Isiah.Jones@ait-i.com and Larry.Jaffe@ait-i.com.