ICS OT IoT Security Factory/Site Acceptance Test (FAT/SAT)

Scope and Statement of Work

Date	Services Performed By:	Services Performed For:
[Date]	[Company Address] [City, ST ZIP Code]	Customer Customer Address

CONSULTANT ICS OT IoT Security FAT/SAT Approach

Through security feature checks, vulnerability scans, pentesting, fuzzing and exploit testing project teams will discover both known and potentially unknown vulnerabilities in ICS OT IoT systems and devices throughout their lifecycle. Factory and Site acceptance testing (FAT/SAT), systems testing and validation, gate reviews etcetera are very critical check points during an ICS OT IoT project, that must occur prior to commissioning and turn over to production operations, when correcting security weaknesses in a component, device or system under consideration, test or scope is the most optimal time to do so.

Many frameworks, standards, guidelines, and practices recommend and, in some cases, require that detailed technical security reviews, testing and equipment level assessments are conducted during the design build, integration and testing phases of new projects. Some examples include but are not limited to:

- **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)

Pulling from requirements and practices, our approach is to review the technology, procedures, processes and people within the identified systems or equipment under consideration within the scope of the factory and or site acceptance test. Some of the areas that will be tested and reviewed can include but are not limited to:

- 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), conduit and network diagrams and piping & instrumentation diagrams (P&ID) properly show how each component interacts with each other. This includes showing 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, DNP, IEC61850), and interfaces are used between and within each component
- Defining security zones
- Checking user interface features for role-based access control, multifactor authentication, privilege and least functionality for human users, APIs, and service accounts
- Running pentesting and vulnerability scanning tools against 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
- Reviewing and testing PLC IEC 61131 logic (e.g., Ladder Logic, Function Block Diagram, Function Chart) against PLC Top 20 secure coding practices
- Reviewing and testing structure text and script-based languages against OWASP Top 10 (e.g., SQL, Python, JSON, Siemens SCL)
- Checking configurations of firewalls, din rail 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 SAT

Overview of CONSULTANT

CONSULTANT is an ICS OT IoT cyber professional team with experience in conducting security test and assessments, including FAT and SAT for ICS OT IoT IIoT and cyber-physical systems.

Scope of Work

The scope of work defines the systems, components, and equipment under consideration for FAT or SAT, as well as tools that may be used, needs for access, and expected deliverables during and post FAT or SAT.

Note: work with customer to call out specific equipment, systems, zones, packages etc. in scope for the FAT or SAT and place them here in this section. Deviations from this equipment list will result in additional pricing for added scope during the FAT or SAT.

Delivery Period

Scheduling of team members to attend the FAT or SAT is negotiated based on team availability and the timing of customer project FAT or SAT phases for the equipment, components, and systems under consideration within the package, zone, and enclave scope.

Note: once the dates and specifics of the actual FAT or SAT are known place the dates, locations etc. here. Deviations from this may require additional charges (e.g., travel logistics changes etc.).

Project Management & Communication

The lead point of contact for the customer during the FAT or SAT event is expected to communicate regularly, at least weekly to support any issues, questions, billing and invoicing, access issues, travel issues etcetera. FAT or SAT team members will be onsite for the FAT or SAT and participate in all daily punch list and hotwash meetings for daily progress reports on scope of equipment already tested, reviewed, initial daily findings and attempted mitigation fixes, punch list updates etcetera.

Methodology and Approach

As defined in scope of work section. Below goes into a bit more details about what a customer should expect in the CONSULTANT's security FAT or SAT approach.

Pre-FAT/SAT event

1. **Customer to secure any required work permits for local host nation if required for duration of FAT or SAT event** - Includes collaboration on tourist visas if required for team members and registration of credentials etcetera with host nation.

2. **Determine and document scope of equipment, zone, system under consideration –** work with customer FAT, SAT technical points of contacts to get a general list of make, models, versions, any logistical issues etcetera to enable the CONSULTANT team to ensure the necessary tools needed for testing certain components is included in the security FAT or SAT kits prior to travel.
3. **Schedule and Book Travel** – work with customer FAT or SAT project manager and payment point of contact to ensure hotels, rentals and flights are booked and paid in advance by the customer for all security FAT or SAT team members that will be participating in the event.
4. **Prep testing tool kit prior to travel** – security FAT or SAT team ensures testing tools including licenses and peripheral devices are prepared, licensed and working prior to travel.

FAT or SAT Event

1. Travel to designated location at least the night before expected reporting to customer FAT or SAT event location
2. Meet with customer FAT or SAT team and owners, installers, programmers' etcetera of systems and equipment under consideration.
3. Attend initial FAT or SAT stand up meetings, kick off team introductions, review logistics, access needs, scope of work, tool set up, team working areas, lunch, local transportation, etcetera
4. Execute testing steps, methodology, tools, procedures and provide updates to FAT or SAT equipment list, punch lists, immediately share quick mitigations to be fixed during FAT or SAT event and capture items on punch list that may go on a roadmap and risk register to be addressed in production post FAT, SAT, or commissioning
5. Provide daily updates in daily punch list review and hotwash meetings
6. Fly back home to do post FAT or SAT final reports of all findings including prioritized unmitigated findings.

Post FAT or SAT

1. Create an overall FAT or SAT findings and mitigations report. Includes all open remaining punch list items and a plan of actions & milestones (POA&M) roadmap of prioritized recommended mitigations for each specific finding
2. Conduct optional follow up post report meeting to discuss any questions, issues and offer any additional services and support for additional FAT or SAT events, mitigation services etcetera
3. Ensure report and POA&M accepted and final invoices are paid.

Deliverables

CONSULTANT will provide the following security FAT or SAT deliverables:

- **Onsite daily updates to equipment list and punch list with active ongoing findings itemized by each component, equipment, system in the FAT or SAT scope**

- **Final FAT or SAT findings and recommended mitigations report including a prioritized POA&M roadmap**
- **Optional summary out briefing slides that summarized key most critical findings and mitigations from the overall report and POA&M**

CONSULTANT Responsibilities

- CONSULTANT shall provide customer with ICS OT IoT security expertise, services and deliverables defined in this SoW
- CONSULTANT shall provide as needed optional coaching of customer staff in areas where onsite travel is not possible within desired timelines due to post COVID19 travel bans and social distancing requirements or local laws and orders between countries and regions.
- CONSULTANT shall provide its own tools and request necessary temporary access account privileges for necessary testing tools
- The security FAT or SAT is limited to selected components, equipment, and systems in scope of this SoW. This includes any directly adjacent components needed to access the FAT or SAT environment.
- Implementation of recommendations to remediate discovered risks is not included in this engagement/SoW. Separate CONSULTANT services can be priced and purchased in separate SoW for advisory and or systems security engineering related services to support remediation efforts.
- Additional modification of tasks or scope will result in the opportunity being considered a separate engagement offering that will require additional scoping, additional costs and/or change order.
- CONSULTANT will provide its own tools as necessary mentioned in this SoW

Customer Responsibilities

- Customer will designate one (1) employee to serve as a primary authoritative point of contact (POC) at the organizational level for the project. The POC will be responsible for enabling CONSULTANT to schedule customer resources for required meetings, travel, logistics, billing, access needs, and other needs deemed necessary to complete the project work as scoped. The POC will participate in status meetings as required and will serve as the first point of escalation for any project-related requests or issues.
- Customer will provide access to all proprietary information, applications, site locations, assets, systems, devices and third parties necessary to complete the Scope of Work.
- Customer and customer resources will execute all data gathering activities in an efficient manner, and data will be promptly submitted to CONSULTANT within the requested timeframe to stay on schedule with the scope, delivery, methodology and approach timelines outlined in this SoW. Any delays incurred in acquiring this information or access

may result in the need for a Change Order and rescheduling of the project, at the discretion of CONSULTANT.

- Customer will provide the necessary staff availability to complete testing and reviews. Customers' inability to provide this staff may affect the completion of tasks and/or deliverables.
- Customer will provide access to any necessary facility, tools, systems, information, devices, accounts, and work areas to complete the project. This includes vendor products and software such as calibration tools, PLC programming tools for equipment in scope etcetera.
- Customer will authorize CONSULTANT to use its own tools, resources, and technologies (e.g., OneDrive, Teams, Nmap, Kali, Wireshark, laptops, scripts, USB etc.) for the duration of the engagement across all components within scope. If it is required for CONSULTANT to only use customer provided laptop, then customer will provide local admin credentials to the laptop and allow CONSULTANT to bring and install all necessary tools and peripherals to complete the security FAT or SAT. This includes access to third party equipment in scope of the FAT or SAT.

Fee Schedule, Terms & Conditions

This engagement will be conducted as a fixed cost in addition to reimbursable travel expenses for flights, uber, rental cars, hotel, meals, baggage fees etcetera. The total value for the Services pursuant to this SoW shall not exceed the cost listed below unless otherwise agreed to by both parties via the project change control procedure, as outlined within. A Project Change Request (PCR) will be issued specifying the amended value.

This figure is based on the Scope of services and deliverables in this SoW. The fixed cost does not include the reimbursable travel expenses. Travel expenses will be submitted as expense invoice after each site visit, and they are payable immediately upon submission from CONSULTANT to customer.

Item Description	Estimated Project Total
CONSULTANT security FAT or SAT services and deliverables	**$**

Note: Average pricing is $X00,000 - $X00,000 per FAT or SAT event depending on scope of equipment and duration of FAT or SAT (e.g., group of packaged systems and components and security stack for 2-3 weeks). 30% of estimate is due upon acceptance of SoW to begin security FAT or SAT event. Remaining balance should be paid in full within 72 hours of receipt of

deliverables. If additional FAT or SAT events are scheduled or requested then full payment of completed FAT or SAT events must be received before scheduling additional FAT or SAT events. All invoicing and payments are processed as ACH and or credit both partial and full lump sum payments accepted and billed via automated electronic invoices from FreshBooks accounting system. **An automatic 5% rate will be added per 10 days late payment upon all submitted invoices. All invoices are due upon submission by CONSULTANT. Late fees apply to separate reimbursable expenses invoices as well.**

Out-of-Pocket Expenses / Invoice Procedures

Covers reimbursable travel and supplies such as baggage fees, airfare, hotel, uber and rental vehicles etcetera.

Assumptions

The following assumptions are observed throughout this engagement:

- CONSULTANT assumes no responsibility of liability for actions of customer staff during engagements either by their own actions or their understanding of recommendations, requests, questions or coaching from CONSULTANT
- A Change Order may be required for any additional equipment or durations beyond the agreed scope in this SoW for the quoted fixed price.
- CONSULTANT assumes that the final deliverable report will be consistent with the items identified in the Deliverables section within this SoW. A Change Order fee will be applied to any additional deliverables that are required and are not included within this SoW.

Project Change Control Procedure

The following process will be followed if a change to this scope of work (SOW) is required:

- A Project Change Request (PCR) will be the vehicle for communicating change. The PCR must describe the change, the rationale for the change, and the effect the change will have on the project SoW.
- The designated Project Manager of the requesting party (CONSULTANT or Customer) will review the proposed change and determine whether to submit the request to the other party.
- Both Project Managers will review the proposed change and approve it for further investigation or reject it. CONSULTANT and Customer will mutually agree upon any charges for such

investigation, if any. If the investigation is authorized, the Customer Project Managers will sign the PCR, which will constitute approval for the investigation charges. CONSULTANT will invoice Customer for any such charges, if any. The investigation will determine the effect that the implementation of the PCR will have on SOW price, schedule and other terms and conditions of the Agreement.

- Upon completion of the investigation, both parties will review the impact of the proposed change and, if mutually agreed, a Change Authorization will be executed.
- A written Change Authorization and/or PCR must be signed by both parties to authorize implementation of the changes investigated. The PCR will cover the fees, pricing, and scope of requested changes.