WHITE PAPER

Partners in Cyber Security

The Advantages of an Integrated Factory Acceptance Test in an ICS Environment

By Jerome Farquharson, Critical Infrastructure and Compliance Practice Manager, and Alexandra Wiesehan, Cyber Security Analyst, Burns & McDonnell

When adding, modifying or upgrading a system, many critical infrastructures conduct a Factory Acceptance Test (FAT). A FAT includes a customized testing procedure for systems and is executed before the final installation at the critical facility. Because it is difficult to predict the correct operation of the safety instrumented system or consequences due to failures in some parts of the safety instrumented system, a FAT provides a valuable check of these safety issues. Similarly, since cyber security can also impact safety of critical systems if a system is compromised, it naturally makes sense to integrate cyber security with the FAT, a concept that brings extreme value and savings to an implementation process.

An Integrated Factory Acceptance Test (IFAT) is a testing activity that brings together selected components of major control system vendors and Industrial Control System (ICS) plant personnel in a single space for validation and testing of a subset of the control system network and security application environment in an ICS environment. Conducting an IFAT provides important advantages and benefits including: time savings, cost savings, improved ability to meet compliance requirements, and increased comfort level with integrated security solutions.

Background

Industrial Control System (ICS) is a general term that encompasses several types of control systems used in industrial production, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCSs), and other smaller control system configurations such as Programmable Logic Controllers (PLCs), which are often found in critical infrastructures such as electricity, water and gas utility systems.

Over the past three decades, several hundred of these protocols have been developed for both serial, Local Area Network (LAN) and Wide Area Network (WAN) based communications in industries including wastewater and electrical generation/distribution. Approximately 10 protocols currently dominate the industrial marketplace and include systems such as MODBUS®, Distributed Network Protocol (DNP3), EtherNET/IP, Process Field Bus (PROFIBUS) and Foundation Fieldbus. The choice of protocol is typically a function of the operating requirements, industry preference, vendor and the design history of the system. For example, in a power utility's SCADA system, a master located in a central facility could use the DNP3 protocol to query and control slave Remote Terminal Units (RTUs) distributed in remote substations. SCADA systems and RTUs have published standards for communication between control centers, acceptance of alarms, issuance of controls, and polling of data objects such as MODBUS® located in Application Layer (Layer 7). These standards, through the last few years, have moved towards a more open standard for SCADA systems versus proprietary protocols, for example, TCP/IP Layer 3 and Layer 4. Other protocols, such as Fieldbus and PROFIBUS, are either analog or point-to-point making them difficult to inherently secure without encapsulation, which is not technically feasible.

SCADA applications are also very delay-sensitive and newer protocols such as Frame Relay, Gigabit Ethernet, and Asynchronous Transfer Mode (ATM) introduce data delay which can cause SCADA protocols to assume errors in the link. The traditional SCADA system was a closed serial network that contained only trusted devices with little or no connection to the outside world. As control networks evolved, the use of TCP/IP and Ethernet became common place and interfacing to business systems became the norm. This connectivity increases the exposure to security risks and as a result, increases vulnerabilities to process and SCADA networks.

IT security has advanced more rapidly in the corporate market due to high security requirements typically mandated for federal and banking environments. For example, the wide use of computers in military and defense installations has long necessitated the application of security rules and regulations. Similar to SCADA systems, the basic premise was network isolation. This concept was basically separating a system logically and applying it to a physical environment. Additionally, system downtime was tied to a percentage of uptime and a tolerance towards how long a system can maintain an outage. Most IT systems were also subject to applications and programming issues that require frequent reboots. But over time, IT systems evolved from single-processor-type systems to faster processors that could run multiple applications at the same time. Industry types all tend to drive security requirements, which were then layered over existing hardware and software applications. Federal regulations and standards, such as NIST, ISO27001 and FISMA, also help drive security on IT based systems. Now the idea of Defense-in-depth is being applied in the design of IT systems and communication networks.

ICSs were very different from IT systems in that they were deterministic systems with very high reliability constraint requirements. They followed the AIC model of Availability, Integrity and Confidentiality; whereas IT systems were CIA – Confidentiality, Integrity and Availability. The key distinction was availability and the importance of it to ICSs versus IT systems. With the inherently isolated design of ICSs, security was believed to be an automatic occurrence; however that was far from the truth. We learned that PLCs and SCADA systems could be comprised. Simply placing a firewall as a logical perimeter defense mechanism, leaving all internal systems with very few or no security controls, only allowed for a greater compromise since a disgruntled employee could sabotage a system from the inside. Along with the frequent misnomers of security, the other challenge for security in ICSs is the slow vendor adoption of security solutions within their applications or hardware solutions. An ICS has multiple interconnected systems and each vendor utilizes its own unique solution which is independent of other vendor's solutions. This approach results in multiple vendors providing multiple solutions to solve the same problem of cyber security. There is no integration of cyber security solutions, which exacerbates the administration of cyber security within an ICS environment.

IFAT Benefits/Advantages

The purpose of an IFAT is to avoid costly redesign and troubleshooting during outage operations. Conducting an IFAT provides an opportunity to verify communications between systems and discover any potential issues prior to installation. Discovery of issues during the IFAT avoids costly outage delays and rework by allowing redesign and troubleshooting to be completed in a more suitable environment, rather than attempting fixes under the pressures of an impending outage completion date. The IFAT, along with subsequent testing during installation, also provides oversight and verification to aid in meeting regulatory requirements for the site.

In addition to the time and cost-saving benefits of an IFAT, the integrated testing allows the customer and the vendors to obtain knowledge and comfort with the integrated security solution. The tests are designed to verify that systems and applications perform as required and do not negatively affect system operations. Upon completion of the IFAT, customers and vendors gain confidence that the integrated solution can be implemented without adverse affects to the vendor systems and will function to meet the customer's needs. Because ICSs are now more integrated with IT systems and have a large percentage of digital systems, the number of vulnerabilities also increases. Therefore, the need for a more consistent cyber security implementation is extremely important. With the proliferation of cyber attacks, it is even more important to include cyber security in the initial design of an ICS, rather than later retrofitting multiple systems, which can be costly with no guarantee of a reduction in cyber vulnerabilities. More than 100 ICS cyber security incidents have been confirmed to date. This number will only increase as ICS environments become more interconnected with IT systems.

Cyber security also affects the vendor and the integrator. If not adequately addressed, these attacks — whether intentional or unintentional — can have impacts ranging from trivial to significant environmental discharges, serious equipment damage, and even deaths. Plant operators are also susceptible to these attacks. With more ICS environments having mandatory regulatory compliance requirements addressing cyber security, significant fines can result from non-compliance with standards such as NERC CIP, CFATS, and others. It can also reduce asset reliability, impacting neighboring plants or other regional entities.

In addition, without an IFAT, issues relating to the operation and maintenance of security controls can be uncovered during installation. These issues are often related to simple configuration changes, or multiple cyber assets not being captured by the vendor security solution. These issues require significant rework by site personnel during difficult outage operations.

Execution of an IFAT is intended to mitigate these issues before anticipated outage dates and allow redesign and troubleshooting to be completed in a more suitable environment. In addition, the IFAT (and subsequent testing during installation) can provide oversight and verification to aid in meeting the compliance requirements in an ICS environment.

An IFAT provides significant advantages and benefits:

a. It will allow plants to better meet compliance requirements with vendor's support implementing a single solution resulting in a cohesive network environment.
b. It saves time from an implementation schedule during an outage because many of the cyber security design are validated in a lab.
c. It increases the confidence level of both the plant and vendor of the proposed solution and provides proof that concepts actually work.
d. ICS personnel are better positioned to accept and support existing vendor security solutions.
e. The proposed vendor's solution can prove both system and network integration with other ICS and IT systems

A successful IFAT requires the attendance of three groups of individuals: the customer, the vendors (including control system vendors and security solution vendors), and a neutral third party. Customer representatives are necessary to provide oversight, decision making and technical knowledge of the

corporate systems. Representatives also gain knowledge and comfort with the integrated solution since the end product will be placed in operation at their site(s). Representatives from each control system vendor and integrated security solution vendor must be present to verify their systems are configured as required and to provide technical insight when troubleshooting the integrated security solution.

Finally, an impartial third party is fundamental in conducting a successful IFAT. To benefit all parties involved, the third party defines and runs the testing activities and serves as the host for all customer and vendor representatives in order to create a neutral, productive environment. The customer, the vendors, and the third-party host collectively ensure the success of the integrated solution and gain knowledge from one another throughout the IFAT process.

Conducting an IFAT

Any IFAT requires planning and preparation in order to be successful. The scope of an IFAT consists of three basic areas:

- Determination of systems and networks
- Testing to ensure the equipment operates correctly to
  - Ensure regulatory compliance
  - Ensure maintainability by customer site personnel
- Reporting IFAT results to vendors

First, with the guidance of the neutral third party, the customer and vendors must determine the integrated network design and the systems required for testing at the IFAT. To provide the most benefit, the actual systems being installed at the customer site should be present at the IFAT for testing. When the actual systems are not available, equivalent systems should be used.

Once the integrated network has been designed and the necessary systems have been identified, a test plan is developed. The IFAT test plan, written by the neutral third party based on customer and vendor requirements, describes the integrated network tests and security application tests to be conducted. This test plan is reviewed with all IFAT participants to ensure understanding and agreement. Upon agreement on a final test plan, detailed test plans are developed, including step-by-step guides and pass/fail criteria for each test. These test plans are followed during actual testing activities.

The neutral third party will conduct testing of the vendor solutions according to the agreed-upon IFAT test plan and utilize IFAT checklists to keep track of test items. During the testing, participation by vendor and customer personnel is highly encouraged to ensure the fairness and accuracy of tests. If during testing a system or application is not performing as required, an IFAT Variation Report form is used to document the issue along with the recommended solution and party responsible for correcting the issue. Every effort is made to keep all parties involved and informed of progress and issues encountered during the testing.

Upon completion of the IFAT testing activities, a final results package is distributed to all parties including the results of all tests, final baseline configurations for all systems and an action item list for unresolved issues. This set of documentation provides the customer and vendors with the necessary tools for a smooth installation of system components.

Conclusion

With the current trend of more intelligent ICSs and increased regulatory compliance, the best practice to achieving ICS and IT integration is by conducting an IFAT. A common problem that occurs in the industry is the unanticipated work associated with implementing security controls which can result in production issues. Performing an IFAT avoids costly redesign and troubleshooting during outage operations saving time and money that leads to an enhanced, sound security solution.

Authors:

Mr. Farquharson is the Leader of Burns & McDonnell's Saint Louis security practice. He leads with a multi-disciplined background of cyber and physical security, information systems and business advisory consulting. Mr. Farquharson is an experienced Security Network Engineer with 23 years IT & Compliance experience that includes experience in Network Design Implementation, Support and Troubleshooting of CISCO Routers, Switches, Firewalls, VPN Devices, Intrusion Detection Systems and network management systems. An innovative, solutions-driven Network Management and Security Specialist with well over 10 years directing the planning, design, deployment and integration of secure high-availability network infrastructure, connectivity and Web services architecture for leading Fortune 500 companies in system and network administration and engineering, hardware evaluation, project management, systems and network security, incident analysis and recovery.

Ms. Wiesehan works on projects involving air pollution regulations and control technologies as well as water treatment system operations. She also provides support work for projects involving utility cyber security with a concentration in compliance and critical infrastructure protection. Her air quality experience includes projects that entail design, construction and start-up phases of major new and retrofit work at coal-burning power plants. Ms. Wiesehan's work also includes contributing to feasibility assessments and cost estimates for air pollution control technologies for the control of SO_2, NO_x, particulate, and mercury emissions. Her water treatment experience includes developing commissioning procedures for water treatment system components and developing startup/operation procedures for water and waste water treatment systems. Ms. Wiesehan's cyber security experience includes contributions to projects involving security assessments as well as policy and procedure development.

For More Information:

Burns & McDonnell recently performed an IFAT in conjunction with FoxGuard Solutions, Inc. (www.foxguardsolutions.com). Larry Alls, Security Engineering Manager at FoxGuard, is presenting "lessons learned" at the ICSJWG Spring 2011 Conference in a session titled: *Integrated Factory Acceptance Test (IFAT) as Security Best Practice*.

Jerome Farquharson – jfarquharson@burnsmcd.com, www.burnsmcd.com/cybersecurity