INDUSTRIAL CONTROL SYSTEMS
Community of Interest

An Introduction to Cyber Security Testing within an Industrial Control System/Operational Technology Environment.

Aims of this guidance

This new guidance is designed to help organisations understand the importance of Cyber Security Testing of Industrial Control Systems (ICS)/Operational Technology (OT) systems and ultimately gain assurance of the cyber security maturity of their environments.

It has been designed to complement the NCSC's General guidance on Adversary simulation/penetration testing and security testing, while focusing on the specific and unique aspects relating to ICS/OT.

Important Note: *While the ICS COI is supported by the NCSC, and NCSC staff are involved in a range of its activities, no formal review of this guidance article has been undertaken by the NCSC. The ICS COI and its members strive to produce relevant ICS/OT specific cyber security guidance to supplement principle based cyber security guidance published by NCSC and have taken care to reference this guidance where applicable. This guidance article will be reviewed every 18 months to ensure that it has not been superseded by guidance published by NCSC, relevance and that any references are still accurate. The ICS COI and its activities are purely voluntary, with guidance articles produced that are deemed needed by UK Operators and their supportive industry partners. The fact that this guidance article has been published by the ICS COI has no relevance to the priority and focus of guidance published by NCSC.*

Who is this guidance for?

If you are responsible for the provisioning, management or performing security testing of ICS/OT assets, this article is designed to provide initial context on the suitability of distinct aspects of security testing for your environment. Which can be considered assurance-based testing and adversary simulation/penetration-based testing methodologies.

Structure of this guidance

This article is one of three, it is designed to be read in isolation but is complementary to the other two articles currently in production: Assurance testing in ICS/OT Environments and Adversary Simulation/Penetration Testing in ICS/OT Environments.

This article is designed to provide initial context on the suitability of distinct aspects of security testing for your environment. Which can are considered assurance-based testing and adversary simulation/penetration-based testing methodologies.

Introduction

Regular testing is vital to improving cybersecurity in critical infrastructure. This article is broken into two sections.

- **Why - Security Testing in ICS/OT:** A high-level overview of the importance of security testing within ICS/OT environments.
- **Applying - Security Testing in ICS/OT:** A short case study of a fictitious company, and how traditional assurance security testing and adversary simulation/penetration security testing was applied.

Why - Security Testing in OT

When it comes to securing ICS/OT environments, three key methodologies are used: traditional assurance, adversary simulation/ penetration and principle-based assurance security testing. All are vital, yet distinct, providing tools in assessing and improving cyber security in these critical infrastructures.

ICS/OT environments play a critical role in energy, utilities, manufacturing, transportation and other industrial sectors, where disruptions can have severe consequences, including safety risks, financial losses, and service outages.

Traditionally these systems were isolated, however they are increasingly being connected to the other networks (*e.g. Internet, cloud, corporate networks, other ICS/OT networks*) to drive

efficiencies, enhance operational controls, and in theory improve the overall security and visibility of any risks or issues. This integration, however, introduces new vulnerabilities and necessitates a re-evaluation of cyber security practices.

Security testing is essential in validating the effectiveness of cyber security measures to protect these systems from cyber threats without compromising their availability, reliability, or safety.

The first step should be to perform a holistic review of the organisation from a cyber security perspective; this is typically carried out using the traditional assurance security testing methodology. It is vital to understand the organisations aims or risk assessments, and their mitigations, otherwise they become isolated. The assurance must be demonstrated to link to the business aims and not just generalised good practice (ideally looking at unwanted consequences and the related threat intelligence that helps detail how these consequences could be realised).

Within the context of ICS/OT, traditional assurance security testing involves the ongoing evaluation of processes, configurations, and policies to ensure systems are secure, reliable, and aligned with industry standards. It's non-intrusive and focuses on assessing the overall cyber security posture without impacting operations.

When an area is identified that needs further testing, to enhance confidence that a security measure is functionally correctly, the second step should be to carry out adversary simulation/penetration security testing designed for ICS/OT environments. It is an active method of testing that attempts to simulate real-world cyberattacks to identify vulnerabilities, testing the system in a controlled way to understand how it would fare against adversaries.

Unlike traditional adversary simulation/penetration testing for Information Technology (IT) environments, which often focuses on identifying and exploiting vulnerabilities with network scans and automated tooling, ICS/OT adversary simulation/penetration testing is designed to provide confidence that security controls and processes work as intended while ensuring operational continuity.

Finally, a principle-based assurance testing approach should be taken simultaneously in parallel with both previous approaches. This involves not just looking at a snapshot in time, but looking at, for example, the full ecosystem, product life cycle, product manufacture's security maturity level. and the business aims. So that a full understanding of the risks associated with any identified issues can be understood.

In summary, the purpose of different security testing methodologies in ICS/OT environments, is that the stakes are higher due to the potential for system downtime or safety risks, both of which are two key pillars of an ICS/OT environment. The minimisation of these risks must come first, and all steps must be taken at all steps to prevent risks, unless they are accepted, in writing, by the authorised business persons. This will result in a very low risk appetite for all parties involved with security testing for ICS/OT environments.

The purpose of security testing within ICS/OT environment is to:

- Verify the effectiveness of security controls in preventing, detecting, and responding to cyber threats, (ensuring that security controls do not have an impact on safety).
- Ensure alignment with regulatory requirements and frameworks such as NIS Regulations, IEC 62443, and CAF.
- Assess resilience against cyber threats by mapping potential attack paths and validating defence mechanisms.
- Minimise operational risk, to acceptable levels, by adopting non-intrusive and controlled testing methodologies that do not disrupt industrial processes.
- Support continuous improvement by identifying areas for enhancement in security policies, procedures, operational instructions, resilience and incident response capabilities.

This article will explore the role of traditional assurance security testing and adversary simulation/penetration security testing within these environments, how they differ, and how to apply them effectively to protect essential entities and critical national infrastructure. Adversary simulation/penetration security testing is typically a deeper dive into individual elements such as network segmentation implementation. Whereas traditional assurance security testing is more likely to detect issues around governance, procedures and policies in how the network segmentation is managed and provide an initial wider (the bigger picture) holistic perspective of the security landscape for an organisation.

The Role of Traditional Assurance Security Testing in ICS/OT Environments

The key purpose of traditional assurance security testing for ICS/OT is to provide confidence in the cyber security and resilience of ICS/OT environments. ICS/OT systems often involve legacy equipment that runs continuously and plays critical roles in areas like energy, gas, and water. Shutting these systems down for testing is often not an option, and even minor disruptions can have significant consequences for both operational safety and public services. Therefore, any security testing should have the scope of what it covers clearly defined, agreed and authorised beforehand. The opportunity that a maintenance period provides should not be underplayed, as it allows a range of security testing to be undertaken at a reduced risk to the operational environment.

To address these challenges, traditional assurance security testing uses non-invasive methodology. The methods focus on assessing cyber security without interacting directly with live ICS/OT systems, reducing the risk of unintended disruptions.

- **Architectural & Configuration Reviews** - Evaluating network segmentation, access controls, and system configurations to identify security gaps. Reviewing the configuration of ICS/OT systems to ensure they align with established security frameworks like IEC 62443 and NIST SP 800-82.
- Threat Modelling & Attack Path Mapping - Identifying possible attack paths an adversary could use to move from IT to ICS/OT systems.

- **Log & Anomaly Analysis** - Reviewing system security logs and security telemetry to detect signs of compromise.
- **Process Reviews** - Evaluating human factors, such as how operators interact with ICS/OT systems, to identify gaps in access control (Privilege Access Management), incident response procedures and patch management.
- Network Monitoring - Observing ICS/OT network traffic in real time to detect anomalies, unauthorized access attempts, or misconfigurations without directly interfering with system functionality. This has the benefit of also acting as a light touch network segmentation review. This also has the ability to help identify unapproved devices communicating on the network.
- **Simulated Vulnerability Scanning** - Instead of scanning live systems, ICS/OT Assurance relies on simulated environments (like testbeds or digital twins) to identify potential vulnerabilities in a safe manner.
- Vulnerability Assessments - Assessing known weaknesses in ICS/OT assets without actively exploiting them.
- **Incident Response Testing:** Simulating cyber incidents to assess the effectiveness of response and recovery plans.

By providing non-intrusive evaluations, assurance testing builds a baseline understanding of a system's security without causing operational disruptions.

Assurance testing is complementary to simulated adversary/penetration testing in that is provides areas of focus that needs deeper review. Assurance testing can play a large part into defining the scope of what simulated adversary/penetration testing needs to be conducted.

The Role of Adversary Simulation/Penetration Security Testing in OT Environments

The key purpose of adversary simulation/penetration security testing is to provide an understanding of the effectiveness of controls against real-world attacks. Adversary simulation/penetration security testing is also complementary to traditional assurance security testing; it helps to validate the findings of identified weaknesses.

Given the sensitivity of ICS/OT systems, adversary simulation/penetration security testing should be planned and controlled to avoid unintended consequences. Adversary simulation/penetration security testing must be approached carefully given the complexities and risks involved. According to the NCSC, adversary simulation/penetration testing is a method for gaining assurance by attempting to breach a system's security using the same tools and techniques as an adversary might. They recommend thinking of adversary simulation/penetration security testing as similar to a financial audit.

The traditional assurance security testing and processes should catch any indicators of bad practices; they should highlight where additionally processes / controls are required to mitigate

risks. Adversary simulation/penetration security testing can be used to corroborate that current, updated, or new processes are effective in reducing risk as intended.

Adversary simulation/penetration security testing in ICS/OT environments should follow these principles:

- **Controlled and Phased Approach**: Testing should be conducted in controlled phases, targeting high-risk areas identified by traditional assurance security testing, such as remote access points or critical network boundaries. This ensures the test is focused and minimizes disruption (ideally with scheduled plant maintenance periods being utilised).
- **Testing in Simulated Environments**: Instead of testing live ICS/OT systems, adversary simulation/penetration security testing where feasible should be conducted in simulated environments (e.g., testbeds or digital twins) that mirror the production network. This allows testers to simulate attacks without affecting critical operations.
- **Collaboration with Vendors**: ICS/OT environments often rely on third-party vendors for system maintenance. It's important to work closely with these vendors to ensure that testing does not void warranties or disrupt ongoing maintenance contracts.
- **Third-Party Expertise**: The NCSC recommends using qualified and experienced third-party testers for penetration testing. In the UK, organizations in government sectors use testers certified under the CHECK scheme, while non-government sectors should seek testers qualified through schemes like CREST or The Cyber Scheme. In the future should seek testers that are UK Cyber Security Council (UKCSC) accredited ICS/OT specialists (*currently being developed*)

To address these challenges, adversary simulation/penetration security testing uses more invasive techniques some examples are provided below, such as:

1. **Configuration Review:** This is typically an in-depth review of the active configurations across a sample test of firewalls, routers, Remote Terminal Units (RTUs) or Virtual Private Networks (VPNs).
2. **Build Review:** Using a representative device, it would be actively tested to validate if the device has been configured in a secure and hardened manner. This can be engineering workstations, laptops, servers or kiosk-based devices.
3. **Network Segmentation Review**: Starting with a network architecture, firewall and routing rules configuration review. Followed by a set of tests created and agreed upon with key stakeholders, to validate findings and check for undocumented routable paths. This should be carried out in a development environment.
4. **Cyber Adversary Simulations:** Emulating attacker techniques to assess how well security defences detect and respond to threats.
5. **Cyber Adversary simulation Team exercises**: Collaborating with defensive teams to test detection and response capabilities.
6. **Testbed & Digital Twin Testing:** Using isolated environments that replicate ICS/OT systems for safe, controlled penetration testing and security validation.

By performing routine testing, adversary simulation/penetration security testing can act as one of the pieces required for good regular security processes. However, adversary simulation/penetration testing is not a substitute for all regular security processes. It only provides a snapshot of the security posture on the day of testing. Therefore, it should be complemented by assurance testing, as well as routine security monitoring and functional testing.

Applying – Security Testing in ICS/OT

The following section explores applying Security Testing to the fictional organisation Admin Corp.

Meet Admin Corp

Admin Corp is a fictional organisation that produces Adminox, a highly volatile, refined form of administrative paperwork that is essential to every organisation in the country. It is created from volatile raw products using a continuous chemical process.

As an essential service, Admin Corp must comply with the EU NIS Directive. This means that Admin Corp's network, information systems and technology needed for the production of Adminox must be protected from cyber-attack.

Admin Corp are regulated for safety by the UK Health and Safety Executive. Therefore, they must take steps to ensure the continued safety of the Adminox production process.

Admin Corps approach to security testing of its ICS/OT environment

For Admin Corp, the stakes are incredibly high—downtime or security breaches could lead to widespread outages, safety risks, and regulatory penalties. Here's how they might apply traditional assurance security testing and adversary simulation/penetration security testing:

Step 1: Traditional Assurance Security Testing

Admin Corp starts by deploying traditional assurance security testing to assess the configuration and security posture of their ICS/OT environment. This includes:

- **Configuration Audits** are conducted to verify compliance with frameworks like IEC62443. This includes ensuring that access controls are properly configured and that system patches are up to date.
- **Network Monitoring** tools are deployed to observe the flow of data between systems, ensuring that no unauthorized communication is occurring.

- **Process Reviews** involve evaluating incident response procedures, identifying gaps in staff training, and ensuring that recovery plans are well-documented.

Step 2: Adversary Simulation/Penetration Security Testing

Once Admin Corp has conducted traditional assurance security testing and built a baseline of security, they move on to a targeted adversary simulation/penetration security testing. This includes:

- **Simulated Environment Testing**: Admin Corp would provide or create a test-bed environment that mirrors its production systems. Penetration testers simulate attacks on this environment, looking for vulnerabilities in remote access points or communication protocols.
- **High-Risk Targeting**: Adversary simulation/penetration testing focuses on high-risk areas identified during the traditional assurance security testing phase, such as network boundaries between corporate IT and ICS/OT networks.
- **Vendor Coordination**: Before testing vendor-supplied systems, Admin Corp coordinates with third-party vendors to ensure that the testing doesn't void warranties or disrupt ongoing maintenance.

Step 3: Continuous Monitoring and Improvement

After the tests, Admin Corp uses the results to improve their internal vulnerability management processes. This includes patching vulnerabilities found during adversary simulation/security testing, via updates, configuration changes or virtual patching. Alongside updating incident response plans were required. Admin Corp also adopts a cyclical approach, conducting regular traditional assurance security testing and adversary simulation/penetration security testing in controlled environments to maintain a secure and resilient ICS/OT infrastructure.

Summary

While both traditional assurance security testing and adversary simulation/penetration security testing play critical roles in securing ICS/OT environments, they serve different purposes. Traditional assurance security testing provides non-intrusive evaluation, ensuring compliance and operational continuity, Adversary simulation/penetration security testing provides simulated real-world attacks to validate the robustness of security controls.

For a company like Admin Corp, a combination of traditional assurance security testing and carefully planned adversary simulation/penetration security testing helps maintain security without jeopardising critical operations, ensuring that both daily functionality and long-term resilience are prioritised.

CAF Indicators of Good Practice Summary

This article discusses measures that contribute to the following CAF Indicators of Good Practice (IGP):

- A2.b Assurance - You have gained confidence in the effectiveness of the security of your technology, people, and processes relevant to essential function(s).
- B4.b Secure Configuration - You securely configure the network and information systems that support the operation of essential function(s).
- B4.d. Vulnerability Management - You manage known vulnerabilities in your network and information systems to prevent adverse impact on the essential function(s).

Statement of Support

This guidance has been produced with support from members of the Industrial Control System Community of Interest (ICS-COI) for publication via the Research Institute for Trustworthy Inter-connected Cyber-Physical Systems (RITICS). This guidance is not intended to replace formal NCSC guidance where already available, and care has been taken to reference such existing guidance where applicable.

This document is provided on an information basis only, and whilst ICS-COI members have exercised reasonable care in compiling the guidance, they provide no warranty as to its accuracy, completeness, or suitability for any particular purpose.

To the fullest extent permitted by law, neither the ICS-COI or its members accept any liability for any loss, damage, cost, or expense arising directly or indirectly from the use of and / or reliance on, this document. Users of this guidance are advised to exercise their own judgement and consider taking independent professional advice.

Any reference to commercial products, services, or entities by name or otherwise, does not constitute or imply endorsement, recommendation or preference by the ICS-COI. The views and opinions expressed in this document shall not be used for advertising or product endorsement purposes.

Document Details

This document is version 1.0 and was published on 23/09/2025. It will be reviewed every 18 months.