Industrial Control Systems Technical Security Assurance Position Paper

Published by:
CREST
Tel: 0845 686-5542
Email: **admin@crest-approved.org**
Web: **http://www.crest-approved.org/**

Principal Author
Andrew Wilson,
Jerakano Limited

Reviewer
Jason Creasey,
Jerakano Limited

Principal reviewer
Ian Glover,
CREST

The UK National Cyber Security Centre contributed to the production of this document, which encapsulates the diverse views of the Industrial Control System community and proposes a model for gaining assurance in ICS environments. The NCSC believes this paper provides a valuable contribution to the current thinking on this challenging topic and we look forward to working with CREST, as well as ICS operators and the cyber-security industry in the UK in order to make the UK the safest place to live and do business online.

Acknowledgements
CREST would like to extend its special thanks to those CREST member organisations and third parties who took part in interviews and participated in the workshops.

DTP notes

For ease of reference, the following DTP devices have been used throughout the procurement Guide.

A Good Tip

A Timely Warning

Quotes are presented in bold, blue italics, like this.

Key findings

The key findings from research into the technical security assurance of Industrial Control System (ICS) environments conducted with subject matter experts and specialist security testing organisations are shown below.

1	In the absence of periodic standards-based technical security testing, ICS environment owners and operators have no objective way of gaining assurance that cyber risk is being adequately managed.
2	ICS environments are rapidly changing (eg. due to process optimisation, Information Technology (IT) / Operational Technology (OT) convergence and technology evolution) and this is leading to a higher degree of exposure and a risk profile that is characteristic of conventional IT environments.
3	Securing ICS environments in many organisations is technically demanding and difficult to undertake (obscure and often obsolete technology, limited resources, high degree of sensitivity).
4	Technical security testing specialists regard inadequate management support (eg. lack of budget, poor resourcing, low risk appetite) as the most important factor affecting the ability to secure ICS environments and undertake technical security testing activities.
5	ICS security standards and guidelines are evolving but currently contain little information to directly help technical security testers. At present there is no definitive standard for technical security testing in ICS environments that is mandated by regulatory bodies.
6	To ensure the approach to testing properly reflects the needs of the organisation, it is important for it to include the risk perspectives of process engineers, safety specialists and those working in IT and cyber security.
7	Multi-disciplinary testing teams should be assembled for ICS technical security testing consisting of members with different testing skills, knowledge and perspectives on risk management (such as resident process engineers, safety specialists and IT staff).
8	Because of the unique technologies, critical processes, and sensitive testing requirements there is a higher demand placed on the skills, knowledge and situational awareness of technical security testers working in ICS environments, as opposed to conventional IT environments.
9	Technical security testing approaches should be intelligence-led, threat-scenario based, draw on well–established technical security testing principles and where possible use red teaming concepts.
10	Promotion of the importance of technical security testing needs to be carried out so that ICS environment owners, process engineers and safety specialists have a better awareness of the importance of technical security testing in the management of cyber risk.

A practical technical security testing process for ICS environments

As part of this project, a practical technical security testing process for ICS environments has been developed and is shown in ***Figure 1*** below.

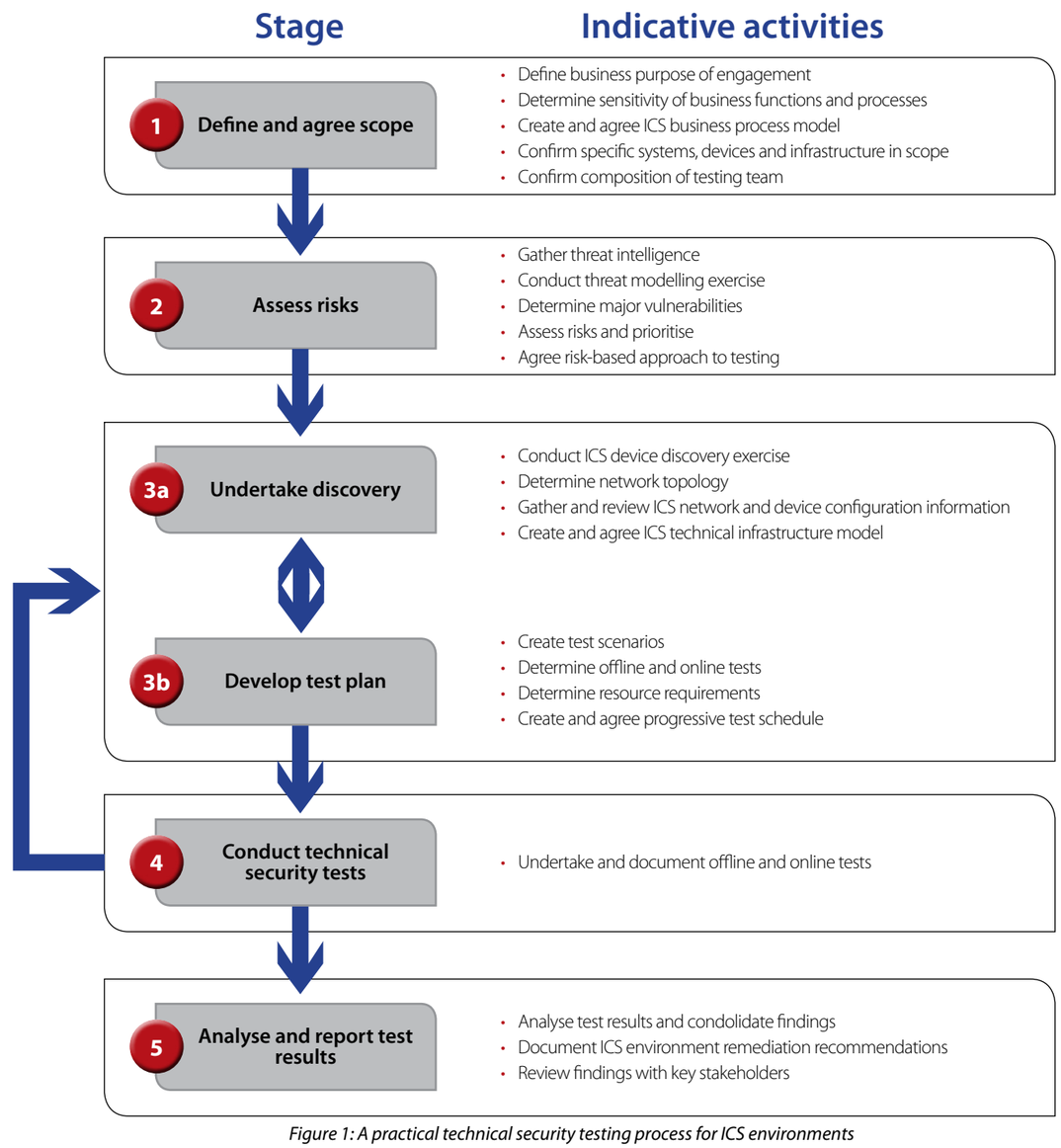


Figure 1: A practical technical security testing process for ICS environments

The ICS technical security testing process is described in more detail in ***Part 4 – Undertaking technical security testing in ICS environments.***

Table of contents

Part 1 – Introduction and overview

About this Position Paper

This Position Paper presents the findings from a CREST project on the Technical Security Assurance of Industrial Control Systems (ICS). This document is based on detailed research and includes insights, commentary and analysis garnered from subject matter experts through:

- Requirements and validation workshops held at CREST member facilities
- Desktop review of published literature on ICS security and ICS security testing
- Structured interviews with subject matter experts on ICS security
- Review of the US Department of Homeland Security (DHS) and the UK Centre for the Protection of National Infrastructure (CPNI) document ***Cyber Security Assessments for Industrial Control Systems***
- Analysis of the input pack on ICS security and ICS technical security assurance that was completed by workshop participants and members of the project review group.

Throughout the Position Paper you will find tips, warnings and quotes provided by a diverse set of contributors, including expert suppliers (such as many CREST members), consumer organisations, government bodies and academia. These bring real-world, practical experience to the Position Paper, allowing you to get a better feel for the types of action that are most likely to apply to your organisation.

Audience

This Position Paper is aimed at organisations in both the private and public sector. Project research has revealed that the main audience for reading this Position Paper is IT managers, information security managers and technical security testing specialists. It should also be of interest to process engineers, safety specialists, business managers, procurement specialists and IT auditors.

Purpose and scope

The purpose of this Position Paper is to set out the main challenges and possible solutions for gaining technical security assurance of Industrial Control Systems. It provides the basis for further work on the development of detailed guidance material that can be used by specialists to help secure ICS environments and in particular those that make up the Critical National Infrastructure.

The main requirements of this project are laid out in Table 1, together with the part(s) of this Position Paper where more detail can be found.

Table 1: Project requirements

Requirement	Detail
Understand the context for the technical security assurance of ICS environments	Part 2
Learn about the challenges that organisations face with in gaining technical security assurance of ICS environments	Part 3
Consider a practical approach to gaining assurance of the technical security of ICS environments	Part 4
Review the next steps that need to be taken to foster the uptake of technical security testing in ICS environments	Part 5

The scope of this Position Paper has been restricted to focus on the main topics related to technical security assurance of ICS environments that have emerged from the project research. It has therefore not included topics that are either very generic or very specific, such as:

- Penetration testing in general, which is covered in separate CREST guides (see www.crest-approved.org)
- Hazard operations and safety culture in ICS environments
- In-depth analysis of infrastructure, devices and protocols in ICS environments
- The specific technical security tests to be used in ICS environments
- The operation of technical security testing tools typically used by commercial technical security testing organisations.

The material in this Position Paper will provide valuable input to many of these topics, any of which could be the subject of a future research project.

Rationale

This Position Paper is based on the findings of a research project - ***conducted by Jerakano Limited on behalf of CREST*** – which looked at the requirements organisations have to undertake technical security assurance of ICS environments.

The increased connectivity of ICS environments and their use of conventional IT infrastructure components and protocols has enlarged the attack surface that can be exploited by ever more sophisticated cyber security attackers, such as state-sponsored attacks, organised cybercrime and extremist groups.

The objectives of the CREST Industrial Control Systems Technical Security Assurance project were to help organisations:

- Make their ICS environments more difficult for cyber security adversaries to attack
- Reduce the frequency and impact of cyber security incidents affecting ICS environments
- Complement existing security guidance and standards aimed at securing ICS
- Meet compliance requirements and corresponding test procedures
- Familiarise themselves with cyber security attacks and the measures that are required to counter these threats.

The work on the project also covered elements of cyber security threat analysis; cyber security intelligence; penetration testing; technical and management assurance techniques; detailed network and infrastructure monitoring; and cyber security incident response.

The project included a detailed review of the DHS / CPNI document ***Cyber Security Assessments of Industrial Control Systems – A Good Practice Guide.***

This Position Paper complements existing CREST reports that have been produced on penetration testing that can be found on **http://www.crest-approved.org**.

Project research

The research on this CREST project included:

- Performing desktop research on many different sources of information
- Conducting telephone interviews with key stakeholders, such as CREST members and clients
- Site meeting with CESG (now National Cyber Security Centre) and CPNI to discuss feedback on the report ***Cyber Security Assessments of Industrial Control Systems – A Good Practice Guide***
- Running two large workshops where experts in technical security testing from more than 30 organisations determined the scope of the project, validated the findings of this Position Paper and provided additional specialist material.

Applicability

Industrial Control Systems, particularly those that form part of the Critical National Infrastructure, are high risk and high business impact and consequently require the highest level of technical testing (***see Figure 2***).

The STAR and Penetration Testing services shown in ***Figure 2*** are supported by comprehensive codes of conduct for both the company and the individual. These codes are used to ensure the quality of the services provided, the integrity of the companies and individuals and adherence to audited policies, processes and procedures. This provides a significant level of protection for any organisation procuring these types of services.

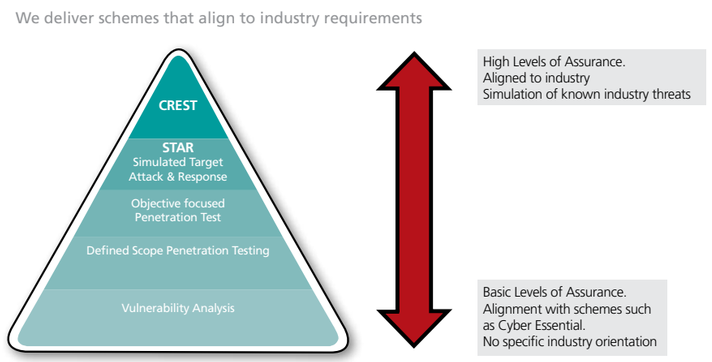


Figure 2: CREST assurance schemes

Part 2 – Setting the scene

The changing nature of ICS environments

Industrial control systems are deeply embedded in many different industry sector organisations and play a vital role in organisations that make up the critical national infrastructure of most countries (eg. energy, water, transportation). Historically the relative isolation and specialised nature of ICS environments has helped to ensure exposure to attack has been relatively low. This has changed in recent times with an increase in the connection of ICS environments into the wider corporate network of many organisations (eg. to support business process efficiencies) and the greater use of more conventional IT technologies (eg. to lower costs associated with support and maintenance).

For the purpose of the project, the definition of an Industrial Control System provided by NIST in SP.800-82r2 Guide to Industrial Control Systems (ICS) Security has been adopted.

A device, or set of devices, that manages, commands, directs or regulates the behaviour of other devices or systems.

Supervisory Control and Data Acquisition (SCADA) refewrs to an industrial computer system that monitors and controls a process.

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 (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures.

Computer-based solid-state devices that control industrial equipment and processes.

As connectivity and access have increased and a better understanding of ICS infrastructure has become more widely known this has led to an increase in the attack surface of ICS environments and an increased likelihood of malicious activity. The consequences of attack could be very damaging, particularly in the case of critical infrastructure, so it is important to ensure ICS environments are protected. Technical security assurance is a vital element of the range of measures required to fully protect ICS environments and will help ensure organisations are able to identify and remediate vulnerabilities that could be exploited. Frequent technical security assurance provides stakeholders, both inside and outside the organisation, with objective fact-based information on what remediation is required, why it is required and how it should be applied.

> ***Because ICS is widespread and the dependency is very high, the prospect of a successful, universal attack propagating is particularly alarming to those responsible for critical infrastructure***

ICS incidents are real

Incidents in ICS environments are real and there is now a strong body of evidence that critical infrastructure is a target not only of adversarial nation states but also of determined and skilled criminal attackers. Many will have heard of the major ICS incidents that have made the press in recent years such as the Ukranian power plant hack. the Stuxnet attack on the Iranian Nuclear facilities and the German steel mill incident and also possibly the emergence of ICS-focused malware such as Havex and Dragonfly. Unfortunately the media storm that has surrounded these isolated indicators has in some respects been misleading as it has detracted from an overall picture that is far bleaker. In reality many organisations with ICS environments are unclear what level of threat they face or whether they have already been breached. In 2015 SANS surveyed 314 respondents on security in their ICS environments. The results of this survey revealed that:

- 32 % indicated their control system environments or networks had been infiltrated or infected at some point
- 34% believe their systems had been breached more than twice in the past 12 months
- 15% reported needing more than a month to detect a breach
- 44% were unable to identify the source of the infiltration.

Furthermore when asked about the source of attacks respondents indicated that:

- 42% saw external actors as the top 1 threat vector
- 19% saw integration of IT and OT as the top threat vector
- 11% saw insider threats as the top 1 threat vector.

From these findings it is clear that ICS environments have never been more exposed to external attackers and they are using new points of ingress introduced through increased use of conventional IT to carry out attacks.

Interviews with subject matter experts has revealed that major incidents affecting ICS environments often go unreported. While this may be for sensible commercial and / or national security reasons it does make it difficult to provide an accurate view of the level of risk faced by organisations - particularly those that are part of the Critical National Infrastructure. Improved reporting and the more widespread sharing of incident data within organisations and across the supply chain would help to address this shortcoming.

While aspects of ICS environments are unique it is increasingly the case that, with the adoption of conventional IT technology, ICS technical architecture is becoming less obscure and easier to understand and manage.

Research conducted by the project into the challenge of securing ICS environments revealed respondents **Very High** level of agreement with the:

- Disappearance of the air gap as a viable control
- Difficulty in obtaining suitable log data for attack analysis and forensics.

There was a **High** level of agreement with the:

- Reluctance of ICS environment owners and process engineers to allow IT and security people access to ICS environments for security testing purposes
- Use of home-brew testing approaches typically assembled from well known sources (eg. NIST SP.800-82r2)
- Lack of accurate information on the devices in ICS environments
- Need for vendors to do more to secure their products in ICS environments.

> ***The devices market is dominated by a small number of vendors. Vendors in the ICS field do not enjoy a great reputation for security***

Subject matter experts that were interviewed for the project have pointed to the current lack of adequate ICS-related technical security architecture reference models available in the public domain. They confirmed that practitioners would benefit from having access to a greater variety of industry-specific types to help compare and improve their own measures.

Key issues in ICS security

Project research helped to identify 9 main factors that could affect the ability to secure ICS environments (***see Figure 3***).

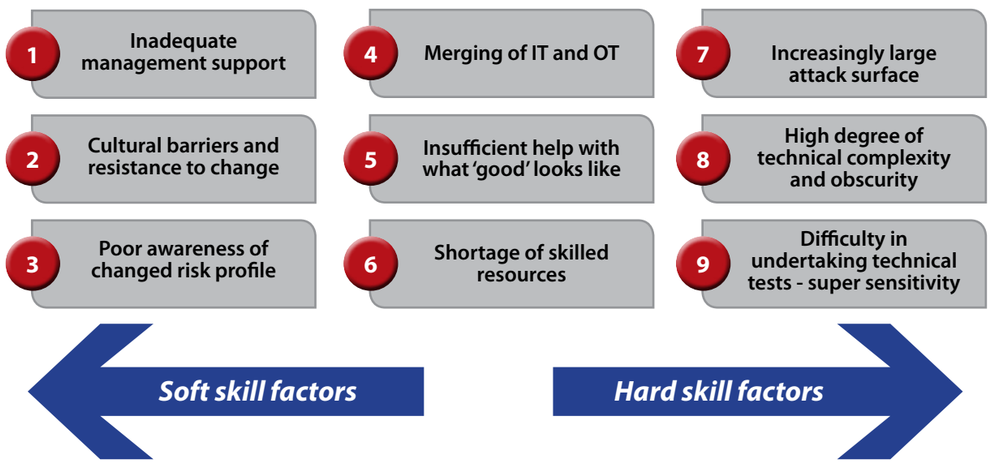


Figure 3: Factors that make ICS security difficult

Each of these factors alone makes achieving an acceptable level of security in ICS environments difficult. Collectively they create a formidable set of challenges that need to be addressed in order to manage risk. For technical security testers understanding this background in an ICS environment is important as most of these factors are both fundamental in nature and highly interrelated.

Research helped to identify the relative importance of these factors. There was a **Very High** level of agreement that **Inadequate management support** is a key factor. All other factors recorded a **High** level of agreement from participants apart from **High degree of technical complexity and obscurity** and **Insufficient help with what 'good' looks like** which recorded a Medium level of agreement.

In general soft skill factors are regarded as being more important than hard skill factors in the extent to which they affect the ability to secure ICS environments. It should be noted that this may reflect the advanced skill-set, experience and technical confidence of participants who were predominantly drawn from a technical security testing background.

Difficulties in conducting technical security tests

Because of the high sensitivity of many ICS environments, extreme caution must typically be exercised in conducting technical security tests. It is important to carefully consider the type and nature of technical security testing that can be undertaken and test analysts should make use of a broad range of methods and alternative approaches as part of their testing methodology. In contrast with conventional IT environments, ICS environments typically place a higher value on 'availability' than 'integrity' or 'confidentiality'. This requires a different approach to technical security testing. Conventional technical security tests that are invasive in nature or place a burden on the network may inadvertently cause damaging loss of service events and should be avoided. For example, where a 'ping sweep' might be used in a conventional IT environment to help identify hosts and nodes it might be more appropriate in an ICS environment to examine router configuration files or even to trace the physical wires for confirmation of connections.

Testers need to understand the technologies that are unique to ICS environments, the processes that could be affected by testing and the types of tests that can be used most effectively. This places a higher demand on the skills, knowledge and situational awareness of the tester. It calls for specialist individuals that are supported by a well-founded methodology.

> ***Every ICS is unique. Every ICS is different. You have to learn what's going on in your one***

In response to research probing the use of technical security testing in ICS environments, respondents indicated their **Very High** level of agreement with the:

- Need to proceed with a high degree of caution during technical security testing of ICS environments
- Requirement for the use of qualified testers and the use of testing techniques that are different from the conventional
- Lack of an authoritative approach for testing the security in ICS environments
- Need for more widespread training and education in ICS security and technical security testing of ICS environments
- Requirement to provide technical assurance of ICS environments.

There was a **High** level of agreement with the:

- Requirement for technical security testers to have a good knowledge of process environments and the unique protocols and devices in ICS environments.

Standards and guidance

There are many standards and guidance related documents available to help organisations in the management of security in ICS environments. The work of the International Society of Automation (ISA) has been particularly important in this area and has provided the basis for the development of the International Electrotechnical Commission (IEC) IEC 62443 set of standards on ICS security that have been published or are due to be published over the coming years. Industry sector specific guidelines have also been produced to help address the particular concerns of specific industries (eg. chemical, power generation, water). Within the UK the Centre for the Protection of National Infrastructure (CPNI) has created a range of documents that cover the broad spectrum of key issues that need to be addressed to secure ICS environments (eg. Security for Industrial Control Systems - A Good Practice Guide).

> ***There is a need to encourage people to conduct technical security tests more regularly to a specific standard***

Note: A detailed review of the main ICS security standards and guidance documents that are currently available has been conducted as part of the project and can be found in the document ***CREST ICS Technical Security Assurance – Research documents***, which is available upon request from CREST.

ICS security standards and guidelines

An extensive number of ICS security standards and guidelines were analysed as part of the project research and some of these are summarised below.

IEC 62443: Industrial communication networks - Network and system security

A newly emergent international standard for securing ICS environments based on ISA99. The primary goal of the IEC 62443 series is to provide a flexible framework that facilitates addressing current and future vulnerabilities in Industrial Automation and Control Systems and applying necessary mitigations in a systematic, defensible manner. The full set of documents that make up this standard are still under development and will not be completed for a number of years. At present there is no direct coverage of technical security testing but a number of documents in the series may be relevant to the development of a technical security testing approach.

ISA99: Industrial Automation and Control Systems Security

A series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Controls Systems (IACS). These documents form the basis of IEC 62443 and their purpose is to improve the confidentiality, integrity, and availability of components or systems used for manufacturing or control and provide criteria for procuring and implementing secure control systems.

NIST SP.800-82r2 Guide to Industrial Control Systems (ICS) Security

A comprehensive document that is well structured and threat / vulnerability / controls oriented. The document provides a notional overview of ICS, reviews typical system topologies and architectures, identifies known threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

CPNI Security for Industrial Control Systems – A Good Practice Guide

A framework of documents that address the core issues in securing ICS environments. This framework is primarily intended for those who are directly responsible for securing ICS, whether they are looking to establish a new programme or complement one that already exists. It will assist ICS professionals in improving their knowledge of security as well providing IT professionals with insight into ICS environments. Senior leaders in an organisation are informed about the rationale for establishing an ICS security capability and the activities required to secure ICS environments.

Cyber Security Assessments for Industrial Control Systems

The purpose of this guide from the US Department of Homeland Security and the UK Centre for the Protection of National Infrastructure is to 'educate asset owners on the general process of a cyber security test and provide insight on specific testing methods so owners learn to prescribe a custom assessment that will maximise the output of their testing budget'.

As an educative document it largely achieves this goal but it does not contain sufficient detail in the process or any measurement or assessment criteria that would enable practitioners to clearly determine the make-up of an effective cyber security assessment in an ICS environment.

The guide is useful for those individuals who are new to ICS security and want to understand more about cyber security testing in these environments. Despite being aimed at 'asset owners' (an undefined term in the document) it is most likely to appeal to process engineers who have the time and inclination to read a relatively long document and want to understand the broad sweep of issues associated with testing ICS security.

Parts of this document (eg. an improved version of the process) could be incorporated into either 1) a framework for ICS technical security testing, 2) a procurement guide for ICS technical security testing services, and 3) to help create awareness raising and training material.

While guidance, standards and good practice on ICS security in general have been available to practitioners for many years these sources of information have included very little on how to undertake technical security testing of ICS environments.

The need for ICS risk assurance

Business leaders require assurance that risk in ICS environments that could affect the operation of critical business processes is being managed effectively. Systematic and rigorous technical security testing helps clarify the security status of ICS environments and plays a key role in the identification, assessment and remediation of cyber risk – a key part of the risks that can affect organisations. By reporting cyber risk, business leaders have a 'clear line of sight' to risks that require remediation and ensure they are able to meet the obligation that comes with high office.

> ***Executives do not necessarily understand the problem. People on the ground get it but there seems to be something lost in translation***

When undertaking any testing in ICS environments it is important to be aware of the different stakeholders that could be involved and the different drivers and motivations that they have that could affect the assessment. ICS environment owners, process engineers, safety specialists and security practitioners will typically have different perspectives of the risk related to an ICS environment and consequently will have different expectations about the types of test that should be conducted and the nature of the assurance they require. This is particularly the case in the absence of any recognised standard for undertaking technical security testing or a regulatory directive on technical security testing.

Guidance on how to align and integrate the perspectives of different stakeholders on assessing and managing risk in ICS environments can be found in the document NIST SP.800-82(r2).

Technical security testing is a key element of **ICS Risk Assurance** but it is only one aspect and proper consideration needs to be given to the other constituent elements that are required in an overall framework (***see Figure 4***).

ICS Risk Assurance

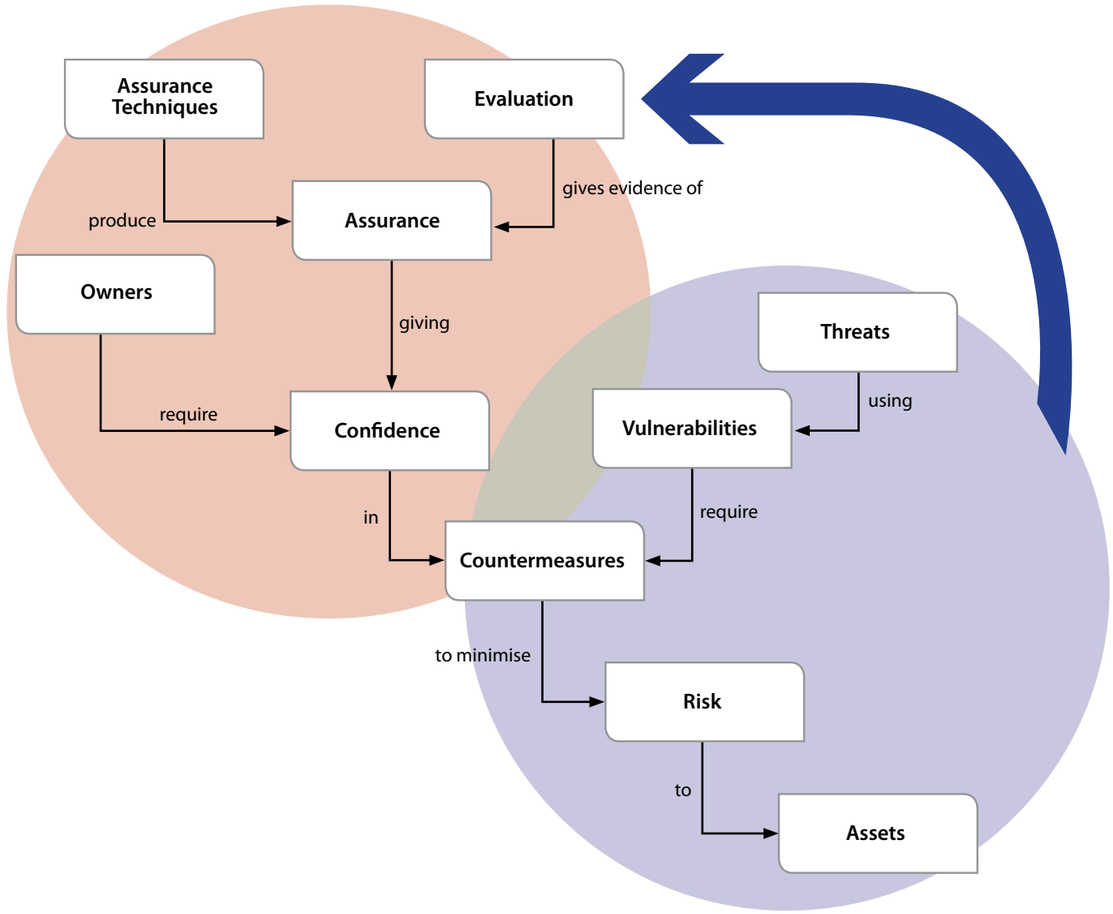


Figure 4: The elements required to provide ICS risk assurance

For ICS environment owners to have confidence in the countermeasures that are in place to manage risk, it is necessary to have effective **Assurance Techniques** and a programme of Evaluation. The process of assessing countermeasures can be achieved with a clear understanding of the **Threats** and **Vulnerabilities** that apply to the ICS environment and the **Risk** that needs to be mitigated. Where **Assurance Techniques** are not clear or inadequate or where there is no systematic programme of **Evaluation** the **ICS Risk Assurance** process will be less valuable. The same holds true where the scope of an ICS environment (ie. **Assets**) is unclear or poorly defined or where **Threats** are not fully analysed. All elements are necessary and essential to provide **Technical Security Assurance** to management; where any element is missing this will lead to weakness in the approach.

Part 3 – Technical security assurance of ICS environments

Important elements in technical security testing

Structured interviews conducted with subject matter experts and technical security testing specialists helped to identify a number of important elements that need to be addressed as part of an effective ICS technical security testing approach (***see Figure 5***).

All of these elements are important and have significant implications for how technical security testing in ICS environments is conducted (eg. the use of a standard assurance approach, support and guidance on how to undertake technical security testing, specialist skills in technical security testing). It is therefore important to ensure that any approach to technical security testing of ICS environments adequately addresses the underlying issues related to these elements.

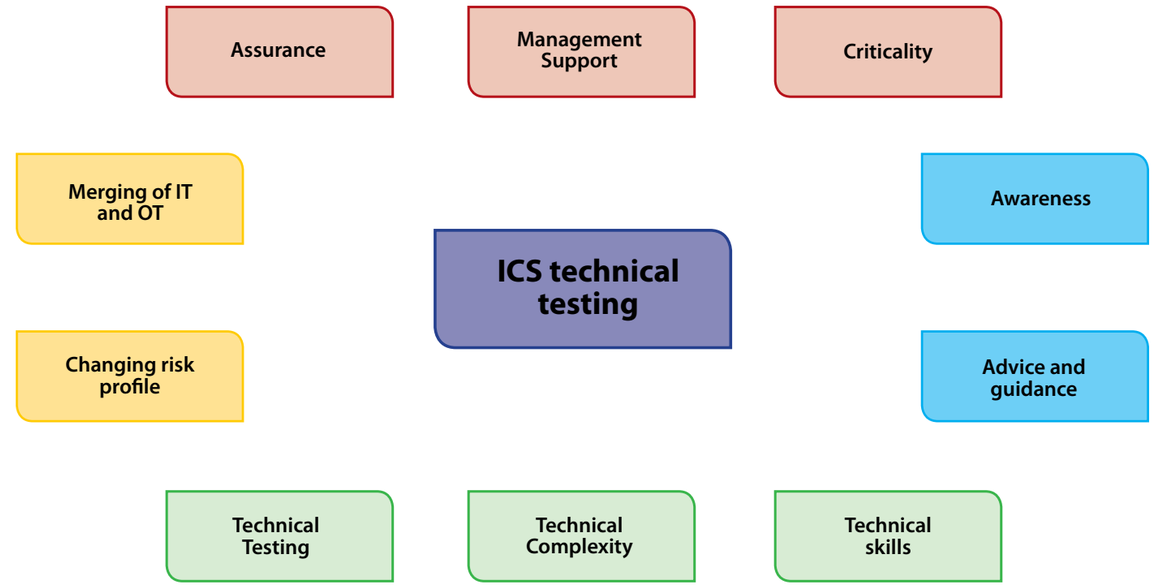


Figure 5: Important elements in technical security testing of ICS environments

These themes are grouped by:

- **Business assurance** – Assurance; Management support; Criticality
- **Education, training and knowledge sharing** – Awareness; Advice and guidance; Threat status
- **Technical capability** – Technical security testing; Technical complexity; Technical skills
- **Infrastructural environment** – Merging of IT and OT; Changing risk profile

Business assurance

ICS environment owners require assurance that there is adequate protection in place to manage the risk of cyber security incidents however there is often reservation about approving tests that could possibly be disruptive. In order to achieve this:

- Technical security assurance activities should be business-led and signed off upon successful completion (ie. there is a clear line of sight to corporate risk management activities)
- Technical security assurance activity must be aligned with the risk appetite and risk attitude of the organisation; it should reflect the criticality of processes, systems and information of the ICS environment
- Reliable, effective and transparent technical security assurance processes and procedures must be in place (eg. documented test plans)
- Management support is required to approve and support technical security testing.

Education, training and knowledge sharing

Key stakeholders such as ICS environment owners, process engineers, safety specialists, IT staff, and cyber security specialists require a good understanding of the unique challenges associated with securing ICS environments. It is also important that they are aware of the strengths and weaknesses of technical security testing in ICS environments. To achieve this there needs to be:

- Education and awareness programmes in place to help key stakeholders understand the importance of securing ICS environments and the use and benefit of technical security testing
- Access to industry advice and guidance for technical security testers and other security practitioners to help improve and refine their approach to technical security testing (eg. through a definitive guide to conducting technical security testing in ICS environments) and situational awareness
- Effective sharing of up-to-date information on threats and vulnerabilities (e.g, such as that provided by CERTUK for incident information) both inside organisations and along supply chains.

Research on the project showed that in response to questions about the knowledge testers require to conduct technical security testing in ICS environments, respondents indicated that there was a **Very High** level of agreement with the need for **Technical knowledge** and a **High** level of agreement with the need for **Domain knowledge** and **Process knowledge**.

> ***Best practice in ICS technical security testing needs to be shared more effectively***

Technical capability

Modern ICS environments typically include a combination of information technology (IT) and operational technology (OT). While well-established methods, tools and techniques exist to assess technical security in IT environments this is not the case in OT environments where legacy technology, obscure protocols, a heightened degree of sensitivity and a widespread reluctance to test has hampered the development of good practice and held back the emergence of effective 'play books'. It makes it more likely that periodic 'errors' will occur in testing as the best ways of working and the best tools are not shared and refined.

An effective technical security testing approach must address the technical capability challenges that concern the:

- Technical security testing tools that should be used and the technical security testing techniques that should be applied in ICS environments (eg. intelligence-led testing)
- Technical complexity of ICS environments and the need to understand the infrastructure and entities that make up the ICS architecture
- Technical skills of testers and the organisations for whom they work.

In response to questions about the types of tools and techniques used in ICS technical security testing, respondents rated the use of Architectural review, Configuration review, Port scanners and Packet sniffers as **Very High**. In terms of methods used in technical security testing of ICS environments Laboratory assessment, Component testing, Staff interviews and Risk assessment were rated as **High**.

ICS-CERT Cyber Security Evaluation Tool

The Cyber Security Evaluation Tool (CSET) from the US ICS-CERT is a no-cost, voluntary technical assessment which provides a snapshot of an organization's cybersecurity posture. It helps ICS environment owners and operators assess cybersecurity strengths and weaknesses within their control system environments and can also be used to assess traditional IT infrastructure.

The CSET exists as a downloadable application (free of charge), which can be installed locally on a standalone workstation or laptop. Once installed, the tool guides an ICS environment owner through a step-by-step process to assess their environment, based upon a series of questions derived from industry recognized standards, guidelines, and best practices (eg. NERC CIP-002 through CIP-009 Rev 4).

Once the questions are answered, CSET provides a graphical representation, identifying areas of strength and weakness, as well as a prioritised listing of options for increasing the organisation's overall cybersecurity defence-in-depth.

Infrastructural environment

As IT and OT increasingly converge in ICS environments this creates new challenges not only for solution architects, designers and implementation teams but also for technical security testers. For example the use of network scanners in OT environments is problematic and can be disruptive or even cause devices to fail. Network security products designed to work within IT environments have not been prepared to work within an OT world that operates within more exacting communication parameters.

> ***Technical security testing in the enterprise IT space is well understood but there is little advice in the ICS world and many environments are not assured***

The increased connectivity of IT and OT has also altered the risk profile of ICS environments. The gradual growth in remote connectivity and connection to the corporate network has served to increase the attack surface. Previously isolated OT environments that would have been difficult to attack are now exposed to the same level of malicious activity that affects conventional IT environments. This potentially broadens the scope of any technical security testing that is required and necessitates the need for greater situational awareness and more use of threat modelling and intelligence-led testing (**see Part 4 - Undertaking technical security testing in ICS environments**).

The infrastructural environment challenges in developing an effective ICS technical security testing approach concern the:

- Convergence of IT and OT in ICS environments and what this means for technical security assessment
- Changing risk profile of ICS environments and how this affects the tests that should be conducted, the frequency of testing and the visibility of reporting.

Part 4 – Undertaking technical security testing in ICS environments

A practical technical security testing approach

Project research identified a variety of possible approaches to conducting technical security testing. Feedback from subject matter experts confirmed that the overall context for all technical security testing should be provided by ICS environment owners (eg. all technical security testing should be business-led) and that the approach should be standards based (***see Figure 6***)

Business-led
Responding to the business drivers, governance requirements and assurance needs of the organisation

Combined testing teams

- Process engineers
- Safety specialists
- IT experts
- Technical testers

Qualified technical security testers

- Experienced
- Knowledgeable
- Professional

Proven tools and methods

- Offline testing
- Online testing
- Red teaming

1 Define and agree scope
- Define business purpose of engagement
- Determine sensitivity of business functions and processes
- Create and agree ICS business process model
- Confirm specific systems, devices and infrastructure in scope
- Confirm composition of testing team

2 Assess risks
- Gather threat intelligence
- Conduct threat modelling exercise
- Determine major vulnerabilities
- Assess risks and prioritise
- Agree risk-based approach to testing

3a Undertake discovery
- Conduct ICS device discovery exercise
- Determine network topology
- Gather and review ICS network and device configuration information
- Create and agree ICS technical infrastructure model

3b Develop test plan
- Create test scenarios
- Determine offline and online tests
- Determine resource requirements
- Create and agree progressive test schedule

4 Conduct technical security tests
- Undertake and document offline and online tests

5 Analyse and report test results
- Analyse test results and condolidate findings
- Document ICS environment remediation recommendations
- Review findings with key stakeholders

Business process sensitivity

- Strategic context
- Process context
- Systems context

Focused threat intelligence

- Industry specific
- Company specific
- Technology specific

Integrated risk assessment

- Process risk
- Safety risk
- Security risk

Standards-based testing process
A consistent approach to ICS technical testing that is transparent, free to use and supported by industry

Figure 6: A practical technical security testing approach for ICS environments

ICS Technical Security Assurance Position Paper

The overall process is generic in nature and similar to many well-established technical security testing approaches. It should be sufficiently flexible to be easily adapted as required to meet the unique requirements of each different testing scenario. It is also important for the process to be straightforward and easy to follow for all stakeholders. This will help in demystifying the activity of technical security testing and aid effective communication about the engagement. The six key steps of the process and their main objective are:

Step	Main objective
1 Define and agree scope	To agree a clear business-based scope for the technical security tests aligned to the strategic, process and system requirements of the organisation.
2 Assess risks	To explore the main threats and vulnerabilities of the ICS environment and determine the key risks and likely risk scenarios to be tested.
3a Undertake discovery	To determine the specific devices that make up the infrastructure, systems and services in the ICS environment.
3b Develop test plan	To create a schedule of carefully constructed offline and online tests that are designed to assess the key risks of the ICS environment.
4 Conduct technical security tests	To conduct a combination of offline and online tests that help to assess the ICS environment in a progressive check-test-check manner.
5 Analyse and report test results	To document and report test results that are aligned to the business objectives and scope agreed with the ICS environment owner.

While the overall process is generic in nature each step includes activities that are unique to technical security testing in ICS environments. This ensures the specific testing requirements of ICS environments are met and includes activities such as:

- Attuning technical security testing to the sensitivity of business functions and processes that relate to the ICS environment (eg. by understanding the potentially adverse consequences of carrying out technical security testing and the capability of the incident response capability that may be required)
- Employing up-to-date threat intelligence to help inform the technical security testing approach that is used
- Developing the most appropriate mix of offline and online tests that are safety and process conscious (eg. by using a check-test-check method).

There are also six defining characteristics that set this approach apart from conventional technical security testing, which are:

- Business process sensitivity
- Focused threat intelligence
- Integrated risk assessment
- Proven tools and methods
- Qualified technical security testers
- Combined testing teams.
- These characteristics of technical security testing in ICS environments are described below.

Business process sensitivity

ICS environments are part of business processes that typically need to operate effectively and without interruption to ensure the success of the enterprise. They are therefore directly linked with business objectives that must be met and consequently should be visible at the highest levels within the organisation. Potentially adverse events should appear on the risk register and there should be a clear line of sight between risk identified on the ground and the achievement of business objectives. It is important to be able to make this connection for all stakeholders and ensure there is a good understanding of the strategic, process and systems context as risk identified in ICS environments will have relevance at all three levels in the organisation.

> ***Technical security testing of ICS environments should not take place in a business vacuum***

Focused threat intelligence

Threat assessment of the ICS environment should be conducted to ensure there is a good understanding of the threats that apply to the specific technologies in use. Threat intelligence, particulalrly that which is relevant to the target company and the industry sector, should be used to help inform judgements about the level of threat in the ICS environment.

Threat intelligence

Threat intelligence, also known as cyber threat intelligence (CTI), is organised, analysed and refined information about potential or current attacks that threaten an organisation.

One of the primary purposes of threat intelligence is to help organisations understand the type, nature, severity, source and origin (eg. nation-state, criminal gang, cyber activitst) of threats that are either directly or indirectly targeted at their environment.

In the case of ICS environments threat intelligence that is most relevant to the organisation will come from a wide variety of sources including the dark web, inside industry sources, open source monitoring, government sources and hacking forums.

In a military, business or security context, intelligence is information that provides an organisation with decision support and possibly a strategic advantage. Threat intelligence is a component of security intelligence and includes both the information relevant to protecting an organisation from external and inside threats as well as the processes, policies and tools designed to gather and analyse that information.

Integrated risk assessment

To ensure the approach to testing properly reflects the needs of the organisation, it is important for it to include the risk perspectives of process engineers, safety specialists and those working in IT and cyber security. Safety specialists and process engineers in particular often have a deep understanding of the causes and consequences of risks in ICS environments and can bring a unique perspective to assessing risk. This is recognised in the NIST document NIST SP800-82 (r2) which provides guidance on how to align and integrate the perspectives of different stakeholders.

By making sure all key stakeholders are part of the risk assessment process it is possible not only to improve the nature of any technical security testing that is conducted but also to help promote its benefits and allay any fears about the possible damaging consequences of poorly executed tests.

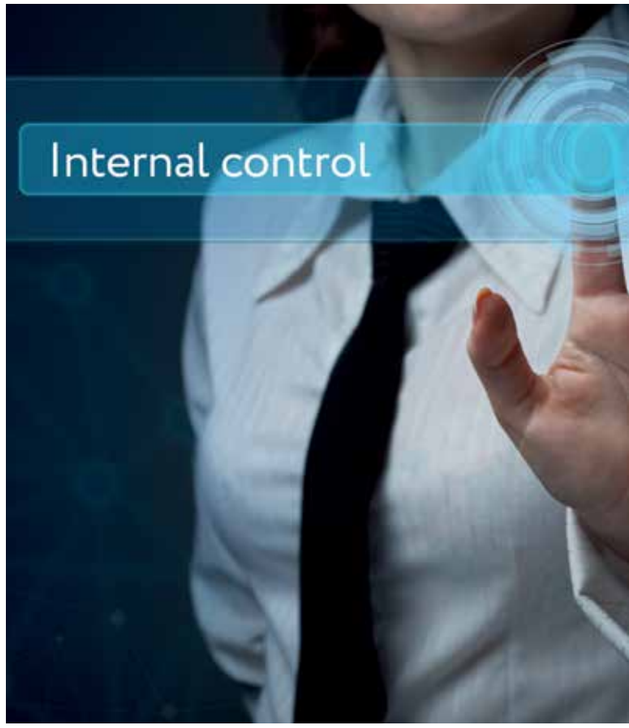
The introduction and use of a common risk management approach such as ISO 31000 would also have the effect of combining different perspectives and would help introduce a common language for discussing terms such as 'threat', 'vulnerability' and 'impact'.

Proven tools and methods

While as a general rule online technical security testing in ICS environments should be used with caution there are a variety of measures that can be taken to ensure services are aligned with the needs of the client and the risk of disruption is minimised. These include:

- Using business-based test scenarios
- Exploiting the domain knowledge of in-house process engineers and safety specialists
- Employing a progressive check-test-check approach that is safety conscious
- Commencing with manual tests before moving to automated tests
- Exploiting wherever possible offline, pre-production, development or test bench environments to simulate live environments

Research on the project indicates that the typical tools and techniques for conducting technical security testing in ICS environments should be used.



In response to questions about the importance of methods used in technical security testing respondents indicated their **High** rating for:

- Laboratory assessment
- Component testing
- Technical documentation review
- Functionality and configuration review
- Staff interviews
- Risk assessment.

Research on the project has shown that Red Teaming is regarded by technical security testers working in ICS environments as a particularly valuable testing technique. The objective of Red Teaming is to break the mould of conventional thinking about the threats and vulnerablities in an environment. Conventional thinking shaped by organisational, cultural and situational factors serves to constrain decision making and can led to a poor anticipation of what actions adversasries could take and how they could attack an organsiation. We are all at risk of conventional thinking when it comes to identifying threats and vulnerabilities. Having a third party skilled in Red Teaming can help to shift our thinking, improve our risk analysis and help determine more effective mitigations.

As technical security assessment becomes established within an organisation, consideration should be given to using tests to help measure the relative maturity of the capability. This depends to a considerable degree on having a recognised maturity model in place to help determine when the criteria associated with a particular level of maturity have been met. The results of all tests should be linked to business objectives and ICS environment owners should have visibility of test outcomes and any remediation actions.

> ***There is nothing magic about ICS pen testing, but it does need to be approached with caution***

Qualified technical security testers

A key requirement is that the technical security testing partner must have a deep understanding of ICS technologies and the role they play in the business processes that they enable. Above all else the testing organisation must be able to work as a partner as technical security testing in ICS environments ideally requires a multi-disciplinary approach and should consist of a team drawn from both the host organisation and the testing organisation.

Previous research suggests that the reasons why an ICS environment operator would partner with a technical security testing organisation are because they can:

- Provide more experienced, dedicated technical staff who understand how to carry out penetration tests effectively, using a structured process and plan
- Perform and independent assessment of their security arrangements
- Carry out a full range of testing (eg. black box, grey box, white box; internal or external infrastructure or web applications; source code review; and social engineering)
- Conduct short-term engagements, eliminating the need to employ you own specialised (and often expensive) technical staff.

To ensure that a chosen technical security testing partner will meet your requirements it can be helpful to define a set of supplier criteria, most of which your chosen supplier should be able to meet – or exceed. These criteria are:

- Solid reputation, history and ethics
- High quality, value-for-money services
- Research and development capability in ICS environments
- Highly competent, technical security testers
- Security and risk management
- Strong professional accreditation and complaint process.

CREST Members – and the technical security testers that they employ – are required to adhere to a rigorous code of conduct for both the individual testers and the organisations for whom they work; backed up by an independent investigation scheme should conflicts arise. Detail of the code are available from CREST at: **http://www.crest-approved.org/about-crest/what-we-do/code-of-conduct/index.html**

Combined testing teams

Technical security testing teams should be made up from a combination of skilled staff from both the testing organisation and key internal stakeholders. Given the sensitive and demanding nature of technical security testing in ICS environments it is important to be able to stop, take stock and re-align testing whenever unknown, high-risk or unforeseen circumstances arise. In these circumstaces the testing organisation must be able to work as a partner rather than in isolation. Ideally a multi-disciplinary approach should be taken with a team of domain, process and knowledge experts drawn from both the host organisation and the testing organisation.

Part 5 – The way forward

Improve foundational elements of ICS technical security testing

There are many different elements of technical testing in ICS environments that need to be addressed to ensure it can be undertaken effectively within organisations (eg. ***see Part 4 – Undertaking technical security testing in ICS environments***). At present there are a number of these elements that are not only poorly undertaken but also foundational in nature. These elements require urgent attention to prevent holding back the more widespread use of technical security testing by ICS owners and operators (***see Table 2***).

Table 2: Foundational aspects of ICS technical security testing

Foundational element	High-level description
A - Technical testing guidance	The lack of a definitive standard that describes how to conduct technical security testing in ICS environments has led organisations to develop their own in-house approaches that are often piecemeal, largely unproven, poorly maintained and do not enjoy the confidence of senior management or other key stakeholders.
B - Practitioner support	Inadequate peer group support for practitioners on how to conduct technical security testing in ICS environments is preventing the virtuous upward spiral of improvement that comes from the dissemination and development of good practice.
C - Security maturity	The relative immaturity of security practice in many ICS environments makes the uptake of technical security testing less likely as more fundamental aspects of security are seen as a higher priority. Organisations who apply recognised good practice in information security management are more likely to benefit from technical security testing than those that are in poor shape.
D - Stakeholder education	Lack of understanding by key stakeholders such as process engineers, safety specialists and IT support staff of the value and importance of technical security testing is likely to hold back the introduction and wider use of technical security testing.
E - Management support	There is often inadequate financial and organisational support from ICS environment owners for undertaking technical security testing. Management support is required to provide the organisational context for risk management.

These are impediments to the use of technical security testing and must be tackled to encourage more widespread and effective technical testing. A regular and systematic programme of technical security testing is essential to help ICS environment owners and operators gain assurances that risks are being managed.

CBEST – setting the standard for technical security testing

CBEST, from the Bank of England, is a common framework that delivers a controlled, bespoke, intelligence-led penetration test against financial institutions' critical systems. Critical systems are those which are essential to the well-being of the institution and the UK financial system as a whole. These tests mimic the tactics, techniques and procedures of threat actors who are perceived by Government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions.

Under CBEST the traditional penetration test is augmented by further validation of the knowledge of the penetration tester. The quality of threat information is substantially increased by the inclusion of specific and targeted threat information from specialist suppliers. This information will allow the penetration tester to simulate more closely real life attacks from competent adversaries. In addition, the cyber security maturity assessment provides KPIs that will help to benchmark the ability of the organisation to detect and respond to such attacks.

CBEST sets the highest standard for technical security testing in financial institutions. It is intended that the approach developed in CBEST is used to help develop similar approaches for other parts of the critical national infrastructure.

Each foundational element that needs to be improved can be addressed through undertaking a range of possible actions. Some of these actions can be undertaken within the ICS operator organisation itself while other actions may require an industry-wide solution and therefore will probably require the assistance of industry associations or regulatory support (***see Table 4***).

Table 4: Improving foundational elements of ICS technical security testing

Foundational element	Examples	Possible actions
A - Technical testing guidance	• Widely recognised technical security testing standard for organisations and individuals to follow • Standards-based implementation advice including reference models, architectural patterns and 'how to' guides • Accreditation service for organisations providing technical security services • Availability of experienced, knowledgeable, professional technical security testing organisation and individuals	A standard, or similar document, for undertaking technical security testing in ICS environments should be developed for use in all relevant industry sectors. The standard that is developed should be supported by implementation advice to assist practitioners. Testing organisations and individuals should be required to meet minimum standards in the technical testing of ICS environments.
B - Practitioner support	• Training and education geared towards the specific needs of technical security testers working in ICS environments • Technical testing advice groups that can provide help in the specific tests, techniques and safety conscious practices should be used in ICS environments • Up-to-date threat intelligence that is relevant to the industry, organisation and technology that is in use in the ICS	ICS environments require the highest possible standards for technical testing and training and education for individuals should be aligned and assessed against those standards by a recognised and experienced body such as CREST. Regulatory bodies, particularly those in utilities, should be encouraged to take a more active role in helping foster the development of practitioners with the requisite skills.
C - Security maturity	• Accurate recording of the scale, scope and inventory of the ICS infrastructure • Defined security architecture with layered defences, established procedures and practices and effective managerial, technical and procedural controls • Dedicated security function with trained and experienced security practitioners • Established programme of security review and improvement	Organisations should consider reviewing their current status of ICS security against established guidelines such as those from NIST and ISA. ICS security assessment services can also be obtained from CREST Members (see **www.crest-approved.org**).
D - Stakeholder education and awareness	• Education of process engineers and safety specialists in the fundamentals of ICS cyber security • Formation of multi-disciplinary teams for undertaking selected ICS security related activities • Awareness raising on the requirements and process for conducting technical security testing in ICS environments • Regular notification of the risk status of the ICS environment including the changing threat intelligence profile	Organisations should establish an educational programme to help ICS operators understand the role and function of ICS security. Multi-disciplinary teams should be established for all ICS security activities that require risk to be assessed. Periodic awareness raising initiatives should be undertaken to remind ICS operators of the importance of ICS security and its changing risk status (typically in response to the increasing threat of external attack).
E - Management support	• Establishing the business context for risk management in ICS environments • Creating the governance oversight for effective safety conscious technical security testing • Allocating adequate resources and budget to support technical security testing internally and by third parties • Establishing a clear line of sight of risks occurring on the ground and how they affect enterprise risk management.	ICS owners should ensure that the enterprise risk management framework and architecture extends to include the ICS environment. This will lead to improved reporting of risk through the enterprise risk register, regular review of ICS risk status and the allocation of budget and resource proportionate to the level of risk and risk appetite of the organisation.

At present many organisations are not able to demonstrate that these elements are solidly in place and therefore are poorly positioned to undertake effective technical security testing. Given the pace of change in ICS environments this is unsurprising and ICS environment operators require more support across the board and also in the form of guidance, promotion and awareness raising before they are able to fully address these foundational elements.

Increase promotion and awareness

Until relatively recently technical security in ICS environments was considered an obscure field that did not attract or require much attention. In recent years this has changed with the realisation on the part of governments, legislators, industry bodies, the media and the general public that cyber incidents in ICS environments can have potentially very serious consequences. As a result there has been considerable effort put into the development of standards and guidance on how to secure ICS environments – particularly those that make up part of a nation state's critical national infrastructure. This work has included very little on technical security testing and assurance and consequently there is still a poor understanding of its value and importance. In fact if there is any common message about technical security testing that has made its way into the collective thinking of ICS environment owners and operators it is that it can be dangerous and should be conducted with extreme caution.

Promotion of the importance of technical security testing needs to be carried out so that:

- ICS environment owners have a better awareness of the importance of technical security testing in helping to manage cyber risk (eg. it should not be seen as a super high-risk activity that should be avoided at all costs)
- ICS environment stakeholders such as process engineers and safety specialists have a better understanding of technical security testing and how it can be conducted in a carefully controlled manner in support of their objectives (eg. to ensure service continuity)
- Practitioners can understand how technical security testing will support them in their efforts to secure ICS environments.

The availability of extensive information on ICS security while welcome is largely aimed at security practitioners and is mostly passive in nature (eg. online documentation). In the absence of specific legislation in the UK to mandate minimum levels of security in ICS environments (eg. through a compliance regime) more active awareness raising should be conducted focusing initially on those organisations working in the critical national infrastructure and then expanding to include others such as those within the digital supply chain.

Conclusions and recommendations

This Position Paper sets out the business background and security challenges that ICS owners face in managing the risks to their ICS environments. There is a pressing need to improve security in ICS environments and technical security testing has a significant role to play in ensuring this is achieved. ICS environment owners require assurances that risk is being identified, assessed and evaluated. Above all else they need to know that there are appropriate measures in place to manage risk.

ICS environments are more sensitive than conventional IT environments and technical security testing that could potentially be damaging should be planned and undertaken with a high degree of caution. The 'deterministic' nature of the devices in ICS environments requires a different approach but not one that is so impoverished that it provides little value or assurance about the strength of measures to resist attack.

> ***"ICS owners are caught in a cleft stick – they want assurances that cyber risk is being managed but they are fearful of the potentially damaging consequences of poorly executed tests"***

Research on the project has helped to identify the high-level characteristics of a practical technical security testing approach and organisations should consider how this could add value to how they approach technical testing at present.

This Position Paper has identified a variety of actions that can be taken to help improve the uptake and use of technical security testing in ICS environments but of fundamental importance is the need to develop a standard for conducting technical security testing and the certification of organisations capable of providing technical testing services against this standard. Work should be commenced to develop this standard to help provide assurance that cyber risks are being managed in ICS environments.

CREST balanced scorecard

The quadrants in this diagram outline the four main areas that deliver the benefits of the CREST vision.

CREST is a not-for-profit organisation that represents the technical information security industry, particularly penetration testing, cyber security incident response and security architecture services.

CREST offers public and private sector organisations a level of assurance that the technical security advisors they appoint are competent, qualified and professional with current knowledge. It also ensures that the companies they engage with have the appropriate processes and controls in place to protect sensitive client-based information.

For further information contact CREST at
http://www.crest-approved.org