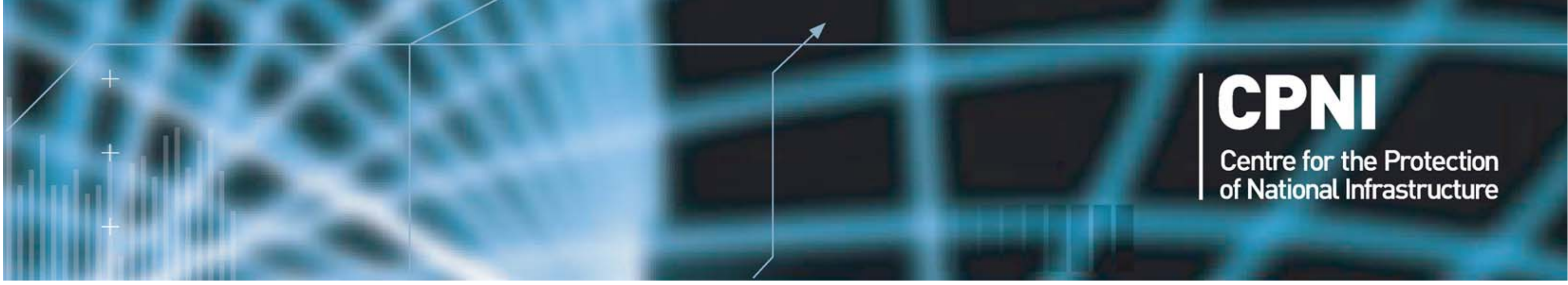

CPNI
Centre for the Protection
of National Infrastructure

CPNI VIEWPOINT

CYBER SECURITY ASSESSMENTS OF INDUSTRIAL CONTROL SYSTEMS

MARCH 2011

Acknowledgements

This Viewpoint is based upon the *Cyber Security Assessments of Industrial Control Systems – Good Practice Guide* prepared jointly by CPNI and the Department of Homeland Security. The findings presented here have been subjected to an extensive peer review process involving technical advisers from CPNI, our information exchange groups and wider industry.

Purpose of this Viewpoint

Industrial control system owners and operators may use a cyber security assessment to find out whether their system is vulnerable to a cyber attack. The assessment identifies and seeks to mitigate vulnerabilities that would allow an attacker to disrupt or take control of the system.

This Viewpoint provides an overview of how to plan and execute a cyber security assessment, and outlines the assessment methods available. The *Good Practice Guide* is available on the CPNI website.

Disclaimer:

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Purpose and aim of this document

Cyber security has become a vital part of conducting business in today's world. Industrial Control Systems (ICS) were originally built as stand-alone systems that were not interconnected and had little in the way of security protections. The internet and internet protocol networks have changed the design of many ICS such that the control network is now often a protected extension of the corporate network. This means that these ICSs are potentially reachable from the internet by malicious and skilled adversaries.

One tool that an ICS asset owner may utilise to assess the risk to the ICS is to procure and facilitate a cyber security assessment. The ICS cyber security assessment identifies and seeks to mitigate vulnerabilities that would allow an attacker to disrupt of take control of the system.

This Viewpoint document provides an overview of how to execute an ICS cyber security assessment to assist those responsible for procuring or facilitating a cyber assessment of an ICS. In addition, a number of alternate vulnerability testing methods are also outlined. The Viewpoint is aimed particularly at senior management and business leaders from organisations within the National Infrastructure.

Our view

What is a cyber security assessment of an ICS?

ICS owners and operators may employ a cyber security assessment to find out whether their system is vulnerable to a cyber attack. This effort can take many forms including a laboratory, production or modelling assessment.

Many considerations have to be taken into account because of significant differences between an ICS cyber security assessment and the tests that would be performed in a standard corporate environment. For example, several tools employed in such a test could have a serious impact on the ICS itself. Various ICSs will malfunction or halt completely when security tools, such as scanners, are run on the network.

It is imperative that ICS owners and assessment teams understand the potential impact to the ICS from the testing operations. Any activities that may put the production system at risk should be performed on an offline system so that failures in the ICS will not impact the business or safety of an installation.

Why cyber security assessments are important?

Cyber security has become a vital part of conducting business in today's world. ICSs were originally built as stand-alone systems that were not interconnected and had little in the way of security protections. The internet and ubiquitous internet protocol networks have changed the design of many ICS such that the control network is now often a protected extension of the corporate network. This means that these delicate ICSs are potentially reachable from the internet by malicious and skilled adversaries. In addition, new vulnerabilities often are discovered in the current operating systems and third-party software that make up today's ICSs. The implications of these vulnerabilities to the ICS domain may not be obvious, but could be exposed by a cyber security assessment.

Planning a cyber security assessment

- Rank ICS components and functionality by potential consequences due to loss of required functionality, data integrity or access control (worst-case consequence analysis).

- Consider the goals and focus of the testing and the amount of information to be provided to the assessment team. (In most cases, it is preferable to assume a worst-case scenario and to provide the testers with as much information as they require, assuming that any determined attacker would already have acquired this. Likewise, ICS owners should be wary of wasting effort on internet to corporate networks tests.)

- Secure the ICS applications, hosts and networks as much as possible, noting security holes that cannot be fully mitigated due to ICS operational requirements. (Eliminating the 'low-hanging fruit' and identifying the most important security goals and obstacles can foster a more valuable security assessment because the assessment team will be forced to search deeper for vulnerabilities. In addition, ICS system and network administrators will also be better prepared to discuss the most important security goals and obstacles, unique to their ICS installation and operational requirements, when creating the test plan).

- Choose and appoint the cyber security assessment team, including determining the rules of engagement and execution of a non-disclosure agreement.
- Create the test plan, remembering not to set too detailed parameters and to allow the assessment team to use their initiative so as to maximise the number of vulnerabilities that can be discovered.
- Determine, in conjunction with the assessment team, the most appropriate assessment methodology for the security test (see Assessment methodologies section below).
- Obtain vendor involvement, so as to remediate ICS product vulnerabilities if necessary.

Reporting

- The asset owner should define the desired level of reporting during the planning stages of the assessment.
- Reporting requirements should be solution-oriented and tailored to the unique ICS.
- Documentation of potential consequences due to successful exploitation of vulnerabilities should be specific to the environment, which may include the vulnerable ICS application, hosts and networks. ICS administrators can then determine the criticality of unauthorised access or DoS to the affected component.
- During the assessment, ICS administrators and managers should discuss each finding with the assessment team, and utilise their expertise to implement as many mitigation techniques as possible. This can reduce the need for validation testing of mitigations for assessment findings.
- Recommendations should address system requirements and ICS administrators responsible for implementing them should have the opportunity to make sure they understand how.
- The assessment team can also help the ICS owner work with the ICS vendor to remediate vulnerabilities in the ICS products and define ICS product security requirements for future procurements.

Assessment Target

When performing an ICS assessment, one of the first decisions that must be made is the target of the assessment. The choice is any combination of the following categories of targets:

- ICS products (lab assessment);
- ICS network (production assessment);
- ICS perimeter (penetration test).

A lab assessment focuses on the ICS software; a production system assessment focuses on the ICS network and host security without putting it at risk. A penetration assessment tests the ability to reach the ICS. All three assessment methods are required to perform a thorough assessment of the ICS's security risks. Budget is the primary limiting factor. An ICS owner should first assess his ability to remediate the source of identified vulnerabilities. A vulnerability assessment is of little value if the identified vulnerabilities are not remediated. In general ICS owners have the most control over their own networks. A network, or production, assessment should be top priority in this case. A penetration test may be the next priority for the same reason. A lab assessment is important for assessing the security posture of the ICS products.

Assessment Methodologies

The actual testing performed on an ICS can take many forms:

Laboratory assessment

A laboratory assessment is one in which the ICS is offline from the production system. This replicate system should be as functionally as close to the production system as possible so that the testing mimics the production conditions. Many asset owners have development or test facilities which may be largely pre-configured to the ICS under consideration. A laboratory assessment is most effective when the goal is to search for vulnerabilities within the processes and protocols that implement the ICS. This may not be of much value if the owner cannot mitigate the identified vulnerabilities.

Production system

A cyber security assessment of a production ICS is performed at the asset owner’s location while the ICS is in production. This means that every ICS feature normally used will be present and active for the test. Onsite cyber security assessments of an ICS play an important part in the overall security of an installation. As long as the asset owner and assessment team understand the implications of this test, they can focus on what will provide value without impacting the process. The test will definitively answer the question of what an attacker could do at this site. This type of assessment can be employed as a follow-up to a laboratory assessment or when no other way is available to test this ICS.

End-to-end penetration assessment

An end-to-end penetration assessment is one in which the goal of the effort is to gain an understanding of how far an attacker could reach. However, the information required to complete this analysis can be obtained piecemeal. For example, if the assessment team demonstrates an exploit that allows them to compromise a DMZ server (victim X) from an attacker box (attacker A) on the corporate LAN and they have shown an exploit for another DMZ server (victim Y), it is reasonable to infer (provided firewall rules are not preventing such) that attacker A could gain remote control of victim Y. It is typical for the test plan to assume that the attacker has already gained a network presence on a corporate host. Therefore, the ICS cyber assessment team can focus on those items that are unique to the ICS domain. An end-to-end assessment is effective when the goal is to understand if an attacker could reach the control network.

Component testing

Component testing is testing pieces of an ICS separately from the rest of the system. These tests usually work with the target component isolated (disconnected) from the rest of the ICS. An example of a component test is a PLC, RTU, HMI application or database that plays a significant role in the ICS. Component testing can be a valuable task if enough information is available. The biggest hindrance for this type of test is that the assessment team will not see how other components communicate with the target. Therefore much of the component's functions (potential attack vectors) will be dormant during the test.

Technical documentation review

A technical documentation review examines an ICS by looking over documents such as system inventory, architecture diagrams, process diagrams, procedures and process documents. A technical document review can be an effective tool if the goals for the task are to prepare for a cyber security assessment or to improve the process. However, this effort will not be able to identify vulnerabilities in the hardware and software that make up the ICS. Instead of a formal task, an assessment team may perform 'need-based' document reviews as they go about a test. For example, they may review architecture diagrams prior to beginning an assessment and reference other documents when they encounter pieces of the ICS they want to explore further.

Functionality & configuration review

This assessment team should examine the ICS by validating the functionality and checking the configuration of the system. This effort will help the assessment team understand the ICS's unique requirements and characteristics. This activity could identify areas where the process could be optimised. This is the only way to assess and secure the production system components and network.

Staff interviews

The team could formally interview the ICS staff. The goal of these interviews would be to gain further understanding and insight into the processes and procedures of the ICS. Interviewing key staff should be part of a production assessment and the documentation and configuration review processes.

Risk assessment

Risk analysis is used to determine whether an asset is protected and to what level. A cyber security risk assessment is a mathematical way to estimate the likelihood that a system can be attacked using cyber means. Risk assessments are often associated with metrics, models and graphs. This method requires less time and resources than a penetration test. The results of a risk assessment may or may not be a good indicator of the security of the system. For example, a risk assessment may determine that many cyber attacks are not viable due to the presence of a firewall or network security appliance. This determination could be a placebo if the protection device is misconfigured or does not have adequate signatures. Therefore, risk assessments are appropriate for certain situations but should never replace manual testing if the goal is to assess a system for vulnerabilities.