CPNI
Centre for the Protection of National Infrastructure

CPNI VIEWPOINT

CONFIGURING AND MANAGING REMOTE ACCESS FOR INDUSTRIAL CONTROL SYSTEMS

MARCH 2011

Acknowledgements

This Viewpoint is based upon the *Recommended Practice: Configuring and Managing Remote Access for Industrial Control Systems* 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 Systems play a vital role in critical infrastructure. Today, business demand has led to the rapid deployment of modern networking technologies, which has accelerated the interconnectivity of these once isolated systems. This new connectivity has empowered asset owners to maximise business operations and reduce costs associated with equipment monitoring, upgrading and servicing, whilst creating a new security paradigm for protecting control systems from cyber incident.

This Viewpoint outlines guidance for the development of remote access strategies for industrial control systems. *The Recommended 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

Industrial control systems play a vital role in critical infrastructure. The requirements for their high availability and proper functioning demand that the systems be protected from both intentional and unintentional incidents that can impact their operation. In the past, the risk to these systems was mitigated by ensuring complete separation of operational domains from external networks and access to the control function was limited to authorised users with physical access to a facility. Today, business demand (such as increased and faster online access to real-time data, using less resources) has led to the rapid deployment of modern networking technologies, which has accelerated the interconnectivity of these once isolated systems. This new connectivity has empowered asset owners to maximise business operations and reduce costs associated with equipment monitoring, upgrading and servicing, whilst creating a new security paradigm for protecting control systems from cyber incident.

This Viewpoint outlines guidance for the development of remote access strategies for industrial control systems. The Viewpoint is aimed particularly at senior management and business leaders from organisations within the National Infrastructure.

Our view

Remote access in control systems architecture

With the growing interconnectivity between control systems architectures, corporate architectures, peer sites and other operational entities, organisations have had to abandon the traditional (and sometimes ideal) concept of total domain isolation. Realistically, industrial control systems have always had some aspect of remote access play a part in operations. Vendors have had access to support their systems and the communications infrastructure was traditionally quite extensive so that it supported data control and acquisition from long distances. The mechanisms for data acquisition involves several different types of communications media, many of which were not dedicated to a single utility but were shared among some number of different entities. A number of the security functionality and concepts that Information & Communications Technology (ICT) has used can be leveraged in control system architectures. The challenge is how to apply cyber security good practices to remote access programs such that the solution supports the requirements for business operations.

Remote access security considerations unique to control systems

Culture has always played a part in how cyber security is implemented in control systems environments. When security foundations are based in the complete and total isolation from untrusted domains, the migration toward creating security solutions that account for interoperability can be challenging. Regardless, the basic attributes associated with control systems functionality, attributes that are based on requirements for high availability and data integrity, create opportunities to leverage proven security technologies and adjust for operational requirements.

The perspective of those responsible for creating remote access solutions that allow for direct connectivity into industrial control system operations may not perceive cyber security as a critical concern but rather how the access solution can be managed to maintain critical operations. When trying to address the security component, many direct connections are justified by the perceived obscurity of the system and the risk is mitigated by the assumption that little understanding exists of how the system actually works. As has been repeatedly proven, this approach is not only dangerous but can lead to some significant operational risk (i.e. the lack of awareness that mission-critical systems are directly connected to the internet).

A vast majority of control systems environments are deployed in domains that are considered to be critical infrastructure. Risks to these environments are not limited to the company operating the infrastructure. Remote access to a control system does expose some aspects of the architecture to remote manipulation. Remote access may be an exploitable attack vector that adds extra risk regarding the availability of the control system. The introduction of security for remote access cannot impede or degrade the normal operational processes that are critical for the control system to function normally.

For example, the remote access security implementation will have to consider the necessity for real time operations. Surprisingly, many organisations fail to recognise the realistic impact that security can have on real-time operations and will often discount the possibility of deploying security countermeasures without appropriately analysing the impact performance. Many control systems environments need to operate in real time, with some environments requiring sub-millisecond polling. Any latency that is created due to the deployment of a countermeasure, such as encryption, may negatively affect the overall process and cause unnecessary delays or shutdowns. Additionally, much of the data on a control system can be deemed non-confidential - therefore the lack of encryption within the communication paths between the critical system components can be tolerated if it is risk-managed.

Many control systems environments are geographically dispersed and may even cross international boundaries. The nature of these deployments requires that many field locations are unmanned and the requirements for availability often make the remote access solution address connectivity more than security. This may limit some procedural-based security protections such as allowing only temporary access to the system. Adding security functionally that may slow down the management of the field equipment, such as calling a help desk to enable remote access, may be justification for keeping an ‘always on’ remote connection.

Because many control systems environments have the requirement to operate in real time, the demand to quickly connect to a system when necessary is crucial. Often, operators may feel impeded by the multiple steps required for remote access and will either want to remove some security features that slow down their connection process or create workarounds to expedite connectivity. A good example of this includes an organisation maintaining the use of the default administrative credentials involved in remote access, or the creation of passwords that are not complex and are not forced to change on a regular basis. As stated before, when operators are working under duress and system survivability is paramount, many users will want to (or be required to) connect to a remote system as quickly as possible and do not want to have to worry about connecting with a complex password or one that they have not used for many years. These practices, in addition to those that involve using the same password for every field device, greatly reduce the chances of a remote access capability being secure. The need for remote access to be as quick as possible can justify not adhering to added robust security protections.

Finally, from a pure technology perspective, many control system devices or implementations may not have the capability to effectively use even basic security features such as authentication or authorisation. With control systems having a larger than average life cycle, some upward of 20 years, the incorporation of effective remote access security countermeasures is just simply not plausible. Even though the asset owner may make repeated requests to the vendor, the cost associated with implementing the effective remote access solution is larger than the purchasing of a new system itself. This situation does not favour the operator but rather the vendor, leaving the operator little choice in creating aftermarket solutions. Secure remote access can be accomplished, but asset owners can expect to require the full support of the vendor to help secure existing remote access capabilities.

Shaping remote access strategy

Because securing remote access is an integral part of any defence-in-depth strategy, the foundation of creating usable guidance as it pertains to control systems environments must include both users and the technology to be accessed remotely. To generalise control system architectures is difficult and to develop a recommended practice for securing remote access that is applicable to all architectures is impossible. It may help organisations to shape their remote access strategy by determining who requires access to certain resources as well as understanding attack vectors that can be created unintentionally.

Understanding both users and roles can have a significant impact on how the remote access strategy evolves. In most control systems operations, the roles that would require remote access to control assets may include, but are not limited to:

- System operators and engineers for local systems
- System operators and engineers for remote systems
- Vendors
- System integrators
- System support specialists and maintenance engineers
- Field technicians
- Business partners
- Reporting or regulatory entities
- Customers
- Supply chain representatives
- Managed service providers

The roles of the users that would require remote access to mission-critical operations can be extensive and the assignment of specific access depending on those roles can be complicated at best.

Remote access concerns

Asset owners required to provide remote access will have a number of options available, including tunnelling; providing direct access to applications, access portals; and remote desktop access. Considering the availability and integrity demands usually required of control systems, asset owners must be rigorous in ensuring that the remote access solutions are balanced appropriately with business requirements.

When considering the options available for provisioning remote access, organisations should be cautious so that no unintentional entry points are created when during implementation. Regardless of the solution, several common elements are pervasive across all remote access technologies:

- Remote access allows users to store critical information locally on their computer or device.
- Remote access solutions are not restricted to using single modes of authentication. The risk associated with information disclosure or compromise can sometimes demand several modes of authentication combined with several different modes of server access.
- Cryptography has and will continue to be part of the remote access solution, but cryptographic communications may impact the timeliness of communications expected and the processing capacity of control system elements within some critical operational environments.
- All remote access solutions depend on the physical security of the devices and authentication elements (e.g. passwords, tokens) initiating the remote connection.

Applying good practice

Most operational environments have limited choices for the technology that can be used for remote connectivity. When combined with the recognition of the critical assets needing to be accessed, the task of defining guidelines can be straightforward. Guidelines that are immediately appropriate to control systems environments include:

- Undertake a formal threat and risk assessment;
- Eliminate all direct connections to critical operational assets;
- Secure modem access beyond default means;
- Use DMZs to segregate business and control architectures;
- Establish user-specific authentication servers;
- Create a security assurance policy for all remote access;
- Use only full tunnelling cryptographic technology;
- Use a password policy specific to remote access elements;
- Wherever possible, use multifactor authentication;
- Use role-based authorisation levels;
- Use dedicated hardware and software to support the remote access solution.

Managing remote access

Security management of the remote access solution should follow defence-in-depth techniques with multiple layers of defence and should incorporate best-of-breed elements from standards. Although not an exhaustive list, the following are examples of layered defence techniques in relation to remote access:

- Intrusion prevention solutions should be deployed on both the business ICT DMZ and the control system DMZ, leveraging operation-specific signatures and triggers defined by the remote access solution parameters;
- Provisioning of identities, authorisation and authentication should be a separate team that adheres to strict change management policies and procedures;
- VLAN or physical segmentation within and between the business ICT networks and control system networks, connected only through a robust firewall configured according to the principle of least privilege;
- Centralised log management and 24/7 monitoring of security events and logs for proactive incident response and more accurate forensics;
- Regular reviews and assessments of technologies deployed and policy and procedure enforcement;
- Patch management strategies for all ICT devices which make up the secure remote access solution, including remote clients, untrusted servers and access gateways and terminal services;
- The use of anti-spyware, anti-malware and anti-virus services which are frequently updated on a scheduled basis.

Conclusion

In conclusion, no single secure remote access solution is applicable to all possible architectures and no single remote access solution can provide adequate security without a defence-in-depth approach. However, by exercising caution and generating and implementing concise requirements based on good analysis, secure remote access solutions can be deployed and maintained.