LOGIIC
Remote Access

June 2015

Final Public Report

Document Title	*LOGIIC Remote Monitoring Project Public Report*
Version	*Version 1.0*
Primary Author	*A. McIntyre (SRI)*
Distribution Category	LOGIIC Approved For Public Distribution
Approval Status	Approved For LOGIIC Use
Reviewed by AF Legal	2015-06-05
Approved (date)	2015-06-05
Approver (EC or AF)	EC
Digital Signature for PDF	Signed by the Managing Director Automation Federation on June 05, 2015

REVISION HISTORY

Version	*Author*	*Date*
1.0	A. McIntyre (SRI)	5-4-2015

EXECUTIVE SUMMARY

The LOGIIC[1] Consortium was established by members of the oil and gas industry in partnership with the Cybersecurity Research and Development Center (CSRDC) of the U.S. Department of Homeland Security, Science and Technology Directorate (DHS S&T) to review and study cybersecurity issues in Industrial Automation and Control Systems (IACS) which impact safety and business performance as they pertain to the oil and gas sector. LOGIIC has sponsored research initiatives that involve the interests of oil and gas sector stakeholders.

The LOGIIC Remote Access Project focused on the use of remote connectivity to systems in the IACS environment for the purposes of monitoring and diagnostics. Vendors use this approach to monitor equipment at asset owner sites. Data collected from this equipment provides insight into system health information and can be useful in troubleshooting and optimization efforts. Although remote access solutions are commonly present in business environments, use of this technology in the IACS environment requires evaluation of risk, planning, and security controls to ensure core assets are protected from attack and unauthorized access is prevented.

LOGIIC conducted a series of research surveys and studies to identify product offerings in the marketplace, their applicability to the Industrial Automation and Control Systems (IACS) environment, and cybersecurity capabilities. Hands-on assessment activities, conducted in an IACS environment, identified the security risks and capabilities of remote access solutions and the impacts associated with their use in an operational setting.

The objective of this report is to convey important factors when considering remote access in an IACS environment and support a dialogue between asset owners and automation vendors. This report presents conclusions on the use of remote access for monitoring of end-devices in an IACS environment. These conclusions are the result of technical assessment and analysis.

[1] LOGIIC - Linking the Oil and Gas Industry to Improve Cybersecurity.

Table of Contents

Revision History 2

Executive Summary 3

Distribution 6

Abstract 7

Acknowledgements 8

1 Introduction 9

2 Project Summary and Background 10

3 Technical Approach 12

Assessment Methodology 12

Assessment Approach 12

Analysis of Findings 13

4 Assessment Findings 14

Recommended Implementations and Vendor Documentation 14

Network Segregation and Layering 14

Network and System Security 15

5 Conclusions 17

Acronyms 18

Table of Figures

Figure 1: Technical Scope 11
Figure 2: Test Vectors 13

DISTRIBUTION

This report is approved by U.S. Department of Homeland Security and the LOGIIC Executive Committee for unlimited public distribution.

ABSTRACT

The LOGIIC Consortium was established to review and study cybersecurity issues as they pertain to the oil and gas sector, and has sponsored research initiatives that involve the interests of oil and gas sector stakeholders. The exponential growth in attempted and successful cyber threats, whether malicious or unintentional, combined with operational demands for increased system reliability and availability motivate the need for a better approach.

Historically, remote access to and from process control networks has been limited, restricted or in some cases explicitly denied as a technical control against inadvertent or unauthorized access to control and automation infrastructure. However, as business demand increases, Industrial Automation and Control System (IACS) suppliers are offering or developing new solutions to support this new opportunity, and it is seen as a growth area for IT in the industrial environment. This evolution fundamentally changes the threat landscape by potentially increasing exposure to emerging cyber threats, which are increasing in both frequency and sophistication.

To date, the robustness and resilience of technologies used by these suppliers to support their remote access solutions have not been assessed or analysed for potential cyber vulnerabilities, and the associated risks are unknown.

In addition to understanding the risks associated with solutions for remote access from vendors, this project assists asset owners in identifying short-term mitigations and vendors in improving remote access solutions in the future. This project allows LOGIIC members and vendors to develop future best practices to effectively deploy and manage remote access.

To fully understand risks associated with implementing remote access capabilities, assessments were performed in multiple test beds that represented IACS environments. This report describes the Remote Access Project and presents assessment findings, analysis, and conclusions drawn from this activity.

ACKNOWLEDGEMENTS

The project to evaluate remote access technologies was developed and guided by the members of the international LOGIIC forum, who devote their time and expertise to conduct projects that will lead to improvements to cybersecurity in the oil and gas industry, and to the IACS community in general. LOGIIC would like to thank the U.S. Department of Homeland Security (DHS), Science and Technology (S&T) Directorate, for providing leadership, vision and commitment to enhancing cybersecurity.

The Automation Federation serves as the LOGIIC host organization and provides a needed home and legal framework for our efforts. We would also like to express our appreciation for the work of all participants, including our team of subject matter experts who refined the evaluation strategy, performed the system evaluations, and developed the project reports.

Since the inception of LOGIIC, the scientific research organization SRI International has provided coordination, project management, and subject matter expertise. The work performed on this project by SRI International and its subcontractors was funded under contract by the DHS S&T Directorate. The content is solely the product and responsibility of the LOGIIC program and does not necessarily represent the official views of DHS.

1 Introduction

The LOGIIC Remote Access Project focused on the use of remote connectivity to systems in the IACS environment for the purposes of monitoring and diagnostics. Vendors use this approach to monitor equipment at asset owner sites. Data collected from this equipment provides insight into system health information and can be useful in troubleshooting and optimization efforts. Although remote access solutions are commonly present in business environments, use of this technology in the IACS environment requires evaluation of risk, planning, and security controls to ensure that core assets are protected from attack and unauthorized access is prevented.

LOGIIC conducted a series of research surveys and studies to identify product offerings in the marketplace, their applicability to Industrial Automation and Control Systems (IACS) environment, and cybersecurity capabilities. Hands-on assessment activities, conducted in an IACS environment, identified the security risks and capabilities of remote access solutions and the impacts associated with their use in an operational setting.

This report presents conclusions on the use of remote access for monitoring of end-devices in an IACS environment. These conclusions are a result of technical assessment and analysis. The objective of this report is to convey important factors when considering remote access in an IACS environment and support a dialogue between asset owners and automation vendors.

The intended audience for this report is the IACS technical and security communities, and automation and security vendors.

2 Project Summary and Background

The LOGIIC Remote Access Project was established and defined by the LOGIIC members (Technical Team, Executive Committee, and the Department of Homeland Security (DHS) sponsor). Automation vendors were engaged and invited to participate in an assessment. The Project Specification states the following Problem Statement:

> Historically, remote access to and from process control networks has been limited, restricted or in some cases explicitly denied as a technical control against inadvertent or unauthorized access to control and automation infrastructure. However, as business demand increases, Industrial Automation and Control System (IACS) suppliers today are offering, or are developing, new solutions to support this new opportunity and it is seen as a growth area for IT in the industrial environment. This evolution fundamentally changes the threat landscape potentially increasing exposure to emerging cyber threats, which are increasing in both frequency and sophistication.
>
> To date, the robustness and resilience of technologies used by these suppliers to support their remote access solutions have not been assessed or analysed for potential cyber vulnerabilities and the associated risks are unknown.

The primary project objective was to evaluate and test current remote access scenarios to fully understand the security risks and create a model to successfully and securely implement remote access capabilities in an IACS environment.

In August 2013, LOGIIC conducted a survey of remote access solutions available from automation and component vendors. At the same time, LOGIIC conducted a survey of Executive Committee members on their use of remote access and related decision factors in implementation.

The LOGIIC member survey results indicated that remote access is already in use among the members, but all have placed limitations on its use and considered some level of security in the implementation. All members were considering expansion of their remote access capability; therefore, project findings were particularly relevant to implementation decisions ahead. LOGIIC members view the expansion of remote access with caution and choose highly specific implementations that restrict access or require some level of standardization. The members indicated a desire to understand vendors' offerings, methods for securing them, and the impact of remote access on broader security exposure. Members seek confidence and clarity in the remote access design and its security impacts when making implementation decisions.

In addition to understanding the risks associated with solutions for remote access from vendors, this project assists LOGIIC members with preparation of short-term remediation activities. The findings will also assist suppliers in improving remote access solutions in the future, and allow both LOGIIC members and vendors to develop future best practices to effectively deploy and manage remote access.

LOGIIC members have defined the project scope to include the remote access machine/application and the network protocols used to connect to the company network. The project excludes vendor networks and their processes and controls; member corporate networks (including access solutions) and their processes and controls; and control systems (See Figure 1).

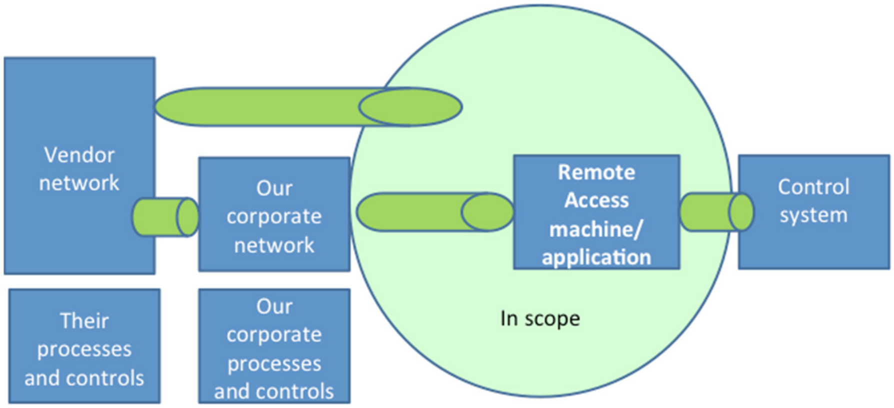

Vendor network
Our corporate network
Remote Access machine/ application
Control system
Their processes and controls
Our corporate processes and controls
In scope

Figure 1: Technical Scope

To meet the project objectives, a vendor selection process was established, candidates were evaluated, and selections were made based on established criteria. All selected vendors offered solutions that provided component-level access for remote monitoring and diagnostics. These solutions included systems that typically reside at asset owner sites and facilitate vendor access to the data collected within the IACS environment. Vendor systems that are used to access this data typically reside at vendors' corporate facilities.

Expanding knowledge in remote access required LOGIIC to conduct hands-on testing activities. A selection process chose multiple vendor technologies for evaluation by a selected Subject Matter Expert (SME). Building upon previous surveys, test scenarios were selected that reflect core questions posed by the LOGIIC team members. Test scenarios were crafted to produce results that answer technical questions relating to implementation, design, specific use cases, and provide input to primary conclusions regarding the use of remote access in IACS environments. Several vendor solutions were selected and multiple assessments were conducted from July to September 2014.

3 TECHNICAL APPROACH

Technical surveys, market reviews, and engagement with automation vendors contributed to the scoping of the project and individual test scenarios. Assessment and analysis followed a standard approach that used previously tested assessment methodologies. The details of the approach are outlined in this section.

Assessment Methodology

LOGIIC consistently bases all assessments on the foundational risk equation, where Risk = Threat x Vulnerability x Consequence. This ensures that all testing expresses a plausible threat that is applicable to the oil and gas industry. Definition of the assessment scope and individual test scenarios is accomplished by characterization of risk in terms of threat, vulnerability and consequence.

After an automation vendor and SMEs were selected, Test Plans were developed that identified test scenarios and rules of engagement. Each vendor provided design diagrams and background information on each tested solution. Therefore, the assessment was considered a “partial knowledge” assessment, with the vendor providing some information and device details in advance.

Each assessment considered insider and outsider threats. Physical access to the systems, and to various connection points, were provided to the SME for the attacker system. All testing occurred during the assessment period; no onsite pre-work was done. For example, no functional setup testing occurred; rather, a configuration review using documentation was performed by the SME in advance of the onsite assessment.

Upon completion of configuration review, specific test scenarios were crafted to evaluate core areas of the remote access solution, data transit security, and individual system targets. These scenarios were conducted during the onsite assessment. Findings were captured in the form of raw data, exploit attempt outcomes, and observations.

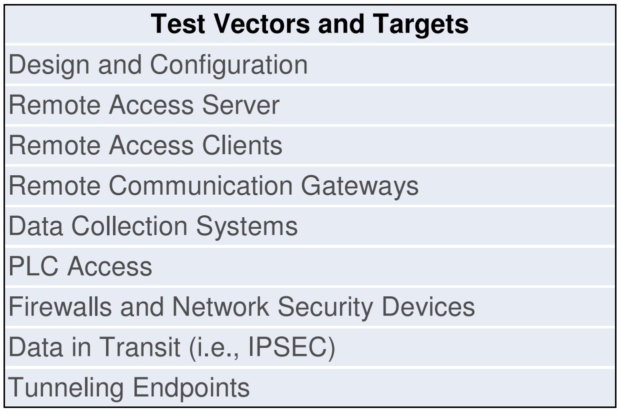
As with the standard LOGIIC assessment approach, attacks were only considered viable if they were traceable and reproducible. While technical activities such as reconnaissance and attack form the basis for most of the assessment findings, observations about interactions with devices also provide valuable information for the LOGIIC team.

Assessment Approach

The vendor architectures under test were similar in design and representative of typical component-level remote access systems. Therefore, a standard approach was used for every assessment. The approach included the following high-level actions:

1) **Configuration Review**
   The SME reviewed the network and system documentation provided by the vendor in advance of the onsite assessment.
2) **Onsite Execution of Test Scenarios**
   Test scenarios were created to test the targeted areas identified in Figure 3.
3) **Onsite Observations**
   During the testing, observations on usability, potential threat vectors, or implementation concerns were documented.
4) **Analysis and Conclusions**
   Findings and observations were collected and analyzed, and broader conclusions were formed.

Test vectors were developed by the LOGIIC team, and by the SME, to answer key questions of specific interest to the LOGIIC members. These test vectors, listed below, were utilized by the SME to develop broader test scenarios and select applicable tools.



Test Vectors and Targets
Design and Configuration
Remote Access Server
Remote Access Clients
Remote Communication Gateways
Data Collection Systems
PLC Access
Firewalls and Network Security Devices
Data in Transit (i.e., IPSEC)
Tunneling Endpoints

Figure 2: Test Vectors

The SME conducted the test scenarios using their attack methods, payloads, and equipment. Standard assessment tools were used during the assessment. All test scenarios were based on plausible threats, and completed by conducting reconnaissance and performing targeted attacks. Attacks included customization and payloads developed by the SME. One or more attacks were used in each test scenario. These attacks included network, operating system, application, and denial-of-service (DoS) attacks.

Analysis of Findings

The technical conclusions conveyed in the following sections of this report are based on several inputs from the assessment: namely, the SME findings. SME findings included raw data captured from the test scenarios. The SME also ranked the severity of the findings from each test scenario. Raw data collected during the assessments was combined with observed findings and configuration review results for analysis. This analysis resulted in the broad conclusions conveyed in this report.

4 ASSESSMENT FINDINGS

The assessment produced numerous technical and operational findings. The similarity between the solutions under test helped to facilitate broader conclusions and considerations that asset owners should evaluate prior to implementation.

Recommended Implementations and Vendor Documentation

Many vendors offering remote access solutions provide a recommended architecture. Asset owners should consider using the vendor-recommended architecture as baseline or assess the risks of alternative architectures. Assessment findings indicate that the security of the solution can greatly be affected based upon the location of systems. For example, placement of servers and clients inside respective DMZs and behind firewalls, or application filters, can significantly change the security of a solution. Customized, unique implementations may not offer the same level of protection.

If a vendor does not yet offer a recommended, secure architecture, asset owners should encourage vendors to do so. This increases the confidence of asset owners during purchasing and implementation decisions. Some vendors used an informal implementation and design model that should be formalized and documented as part of the vendor's recommendations. Use of a recommended architecture often means including the security controls built into the design in the most effective way. For example, the most secure recommendations included placement of the clients and server in DMZs instead of the business network or core IACS network.

In addition to design recommendations, guidelines on patching and maintenance can be extremely helpful in maintaining a level of security. During the assessments, the SME discovered varying vendor approaches to documentation, from minimal to comprehensive. The comprehensive documentation included clearly defined roles, responsibilities, and maintenance procedures.

Security takeaways from the assessment include:

- Ensure that recommended controls be implemented.
- Follow a vendor implementation model, if available.
- Follow vendor maintenance and usage documentation, if available.

Network Segregation and Layering

Access, application, and OS security controls are required as part of an inherent security model. However, the assessments indicated that in a remote monitoring architecture, network security—primarily, network segregation and layering—is extremely important in a secure implementation. This approach isolates critical components within the design and assigns protections accordingly. Layering also helps to protect against outsider and insider threats. A defense-in-depth approach works well in a remote access solution by protecting each component of the system. These layers should be formed around end devices under monitoring, data collection points, servers, and clients. End devices are therefore protected behind several layers of security. This approach protects end devices that may not be robust or capable of device-level protection, and may be susceptible to vulnerabilities or DoS attacks. An attacker would need to compromise several protective mechanisms to reach the end device.

Protection against unauthorized access to remote monitoring servers is important. Vendors employ various mechanisms to protect the server, but basic segregation through the use of firewalls is common and can be effective. Proper network isolation includes port lockdown. Only the minimum number of ports necessary for operation should be accessible. Identification of minimum requirements should be determined prior to implementation, and a plan should be developed that maintains that level of protection throughout the life-cycle. Traffic that crosses network segments should be unidirectional whenever possible. However, communication to a system is commonly initiated from another location; therefore, bidirectional communication traffic is often necessary. This concept may counter an asset owner's existing policies for restricting inbound traffic into a DMZ or the core IACS network. Again, this data flow should be addressed prior to implementation, and sufficient protective mechanisms should be defined.

Other controls, such as the use of VPN, can assist in layering protections, even across network segments at the asset owner's site. A secure VPN implementation and security of the VPN end-points can add to overall security of the solution. Complementary protections can include restrictions, based on IP address, on incoming traffic from the vendor's site. Other restrictions can require the use of IPSEC or other minimum protection levels. These controls are also discussed in the following section.

Network and System Security

A remote monitoring and access solution is only as secure as the individual systems, components, or network backbone that comprise that solution. System and network configuration details should be defined prior to implementation, discussed with the vendor, and established with maximum protections in place. The assessments resulted in the following considerations:

- The system must be protected from insider and outsider threats.
- Access control and strong system and application passwords are necessary.
- Maintaining patches and updates is necessary for continued protection against new vulnerabilities.

Protection against insider and outsider threats is interdependent upon access control and layered security. To protect against unauthorized privilege escalation, role-based access control measures should be in place that control read and write access based on least privilege. Both system and application accounts should be locked down and maintained to least privilege. Any stored passwords should be obfuscated.

Systems should also be locked down. Unnecessary and potentially vulnerable services such as Telnet and FTP, and risky services such as VNC, should be disabled. If a vulnerable service, such as FTP, is required by the vendor, then strong passwords and other layered security such as VPN and secure protocols should be implemented. Limited services and ports are needed on most remote access solutions, which allows disabling of residual services and open ports that create attractive attack vectors. Likewise, the use of standard applications or services that have well-known exploits can produce a larger attack surface that must be secured and maintained. For example, DCOM, SQL, and common webservers present attractive, often exploitable, targets. Common operating systems and applications must be patched and maintained to ensure protections are in place. Vendor accredited patches and updates, and OS patches, must be kept current, with a patching process established early in the life-cycle.

Firewall configuration can assist in reducing the attack surface of a remote monitoring solution. Firewall restrictions should include limiting traffic to SSH, HTTPS, and RDP, or the minimum necessary. Traffic flow and control, such as limiting traffic to read-only requests, should be considered at the beginning of the life-cycle

DoS and password leak attack are attractive attack vectors in a remote access solution. Firewalls may not prevent all DoS attacks. Application-level filtering should be used with firewalls when possible. In one assessment, a firewall blocked network storms, SYN floods, and DoS attacks based on network saturation.

However, application-level attacks and malformed packets were successful at a vulnerable end device, even with a firewall. Mitigation for end-device vulnerabilities, implementing a firewall, and layering network and system protections should each be design considerations discussed between the asset owner and the vendor prior to implementation as elements in a comprehensive approach to protection. Asset owners may find it beneficial to thoroughly discuss application-level protections and firmware and hardware vulnerability testing with vendors prior to implementation decisions.

Where possible, VPN and two-factor authentication should be implemented. Proper encryption should occur at VPN endpoints, including physical security of those endpoints at vendor sites. Protocols should be restricted to those that offer security such as IPSEC.

In some tested solutions, authentication mechanisms included the use of pre-shared keys. Risks, such as vulnerability to a brute-force attack, exist with the delivery and sharing method of the key. These risks should be considered and weighed against the benefits of use.

Lastly, if RDP is used, publication of an entire remote desktop instead of just a remote application may provide a broader attack surface.   These details can be identified during design and testing. Similarly to system and network access, application availability should be maintained using the principle of least privilege.

5 Conclusions

Optimization, efficiency, and situational awareness are drivers for increased use of remote access. Remote monitoring and diagnostics of vendor devices inside the IACS environment allows vendors to quickly determine the health of a system, collect information, and troubleshoot a problem. Use of this technology in the IACS environment requires careful design and implementation to ensure access is focused on authorized systems and core IACS assets are protected.

The remote access solutions assessed in this project were similar in design and used primarily to monitor end devices in the IACS environment. Though assessment findings showed similarities and differences, several important aspects of remote access solutions were identified. Asset owners should consider these aspects when evaluating the use of remote access for monitoring by a vendor.

The role of vendor documentation during planning, design, implementation, and maintenance is important. The assessments concluded that vendors presently have varying levels of documentation, and asset owners place significant emphasis on a vendor's recommended architecture. Documentation that provides a recommended, secure architecture with implementation guidance can increase asset owner confidence.

Given the criticality of maintaining patches and updates, a long-term patch management process should be defined with the vendor. This process should ensure that critical patches are maintained on all components of the remote access solution, and a clear path for delivery and installation of patches is determined. Remote access can often employ software with common vulnerabilities. Long term patch management and updating processes should be defined with the vendor. As with any implemented technology solution, a lack of patching can create significant risks.

During design and implementation, best practices indicate that remote access solutions should use layered security and a segregation of the solution from other parts of the network. Layered security places multiple controls between critical assets and a potential adversary, whether an insider or outsider. This is particularly important when end-devices have limited capability for inherent security, such as inabilities to patch or use malware detection, or the need to use a vulnerable service.

System and network security practices should occur at both the asset owner and vendor site, and should be defined prior to implementation. Good system and network security practices are necessary in any IACS implementation. In remote access, it is even more critical to review all unnecessary services and ports, and maintain patches and updates to reduce the overall attack surface.

From this project, it can be concluded that remote access solutions provide value to the asset owner and increase efficiency in understanding system health and situational awareness. Remote access solutions in the IACS environment are becoming more common as interconnectivity and the desire for optimization increase. All benefits of using remote access should be balanced with the risks inherent to the technology. The design and implementation of remote access solutions in the IACS environment requires consideration of network and system configuration, maintenance, and access control. Defense-in-depth approaches should be employed under the principle of least privilege. Collaboration between asset owners and vendors can ensure that both technical configurations and maintenance plans are established at the beginning of the life-cycle.

ACRONYMS

Term/Acronym	
CSRDC	Cybersecurity Research and Development Center
DCOM	Distributed Common Object Mode
DHS S&T	Department of Homeland Security Science & Technology Directorate
DMZ	Demilitarized Zone
DoS	Denial of Service
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL (Secure Sockets Layer)
IACS	Industrial Automation and Control System
IPSEC	Internet Protocol Security
LOGIIC	Linking the Oil and Gas Industry to Improve Cybersecurity
OS	Operating System
RDP	Remote Desktop Protocol
SME	Subject Matter Expert
SQL	Structured Query Language
SYN	Synchronize
VNC	Virtual Network Computing
VPN	Virtual Private Networking