LOGIIC

Real-Time Data Transfer Project

May 2016

Final Public Report

Document Title	*LOGIIC Real Time Data Transfer 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	06/27/16
Approved (date)	06/27/16
Approver (EC or AF)	EC
Digital Signature for PDF	Michael Marlowe

REVISION HISTORY

Version	*Author*	*Date*
1.0	A. McIntyre (SRI)	5-10-2016

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 (DHS), Science and Technology (S&T) Directorate to review and study cyber security 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 Real Time Data Transfer (RTDT) Project focused on the assessment and analysis of real-time data transferred outside the core IACS environment. RTDT solutions provide data sets that support operational decisions in an efficient manner. The project evaluated solutions available in the market that collect and move data from Layer 2 and 3 to Layers 3.5, 4, and beyond.

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 their cyber security capabilities. Hands-on assessment activities conducted in an IACS environment evaluated the security provided by RTDT solutions. Solutions provided by automation vendors and third-party vendors were included in the project. Solutions were installed, configured, and assessed in an IACS laboratory environment. The technical findings and operational conclusions that were derived during each assessment are aggregated and summarized in this report.

Both automation vendor and third-party RTDT solutions were assessed. Although the data transfer functionality provided by each solution is effectively the same, the solutions varied in size and structure, depending on the vendor's design and integration with other control systems. Assessments included evaluation of the encryption implementation, security of data in transit and at rest in the architecture, security of applications, servers, access control mechanisms, and other security attributes.

The objective of this report is to convey important factors that should be weighed when considering an RTDT solution and to support a dialogue between asset owners and automation vendors. This project identified a number of positive security attributes within the solutions. It also identified areas of technical consideration that could create threat vectors and compromise the integrity of the data in transfer, or allow unauthorized access to the data. These findings are categorized, and recommendations are made within each category. Example findings include:

- **Differences Between Automation Vendor and Third-Party Solutions**
  Differences in design and operability include size of the system, number of components, configurability, and management. Automation vendor systems tend to be larger in scope and hardware. Third-party solutions are generally smaller and focus on transferring the data between existing points in the network.

- **Solution Footprint and Management**
  Larger systems present a broader attack surface and require significantly more configuration and management to ensure each component is secure.

- **The Use of Third-party Components within Automation Vendor Solutions**

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

Vulnerabilities may exist at various levels of integrated third-party components, and commonly arise from the configuration decisions made by the automation vendor. If third-party products are used, security must remain inherent throughout the supply chain by, e.g., ensuring that OPC components are fully patched. Automation vendors must collaborate with the third-party component vendors to ensure that the most secure configurations are deployed and maintained.

- **Networking Components**
  If firewalls and switches are provided within the solution, they must be configured securely, tested, and validated. Testing revealed that some networking components do not operate as fully intended by the vendor. A true DMZ, rather than a single switch, is recommended.

- **Importance of Encryption**
  When a solution includes an encryption mechanism, the implementation of a valid algorithm (such as AES) and key handling and change processes are important in protecting the data in transfer. Details on the algorithm and implementation must be available from the vendor. Independent testing and validation of the encryption mechanism is recommended.

- **Networking and Packet Handling**
  Network levels should be protected by securely configured components, as mentioned above. Packet integrity and packet privacy contribute significantly to the security of the data in transfer. In particular, packet integrity protects against man-in-the-middle (MiTM) attacks.

- **Layered Security**
  Data should be protected in transit and storage, at levels commensurate with its criticality. Most solutions offer granular tag security. Asset owners should define the access restrictions and protections required at each level and ensure that the solution meets those requirements. In addition to protection of the data in transit, data stored (even temporarily) in databases should be protected by encryption or database controls. Integrity of the solution itself should be maintained through application security, removal of default settings, and protection of log files.

- **Using and Maintaining the Solution**
  Good security practices that extend to RTDT solutions include removal of default application passwords and default accounts, disabling unnecessary ports and services, and configuring the solution based upon the principle of least privilege. An established patch management program is necessary to ensure security remains throughout the life-cycle.

The detailed technical findings and operational conclusions derived during this project produced a set of topics that should be evaluated when selecting a RTDT solution. The implementation of new technologies in a critical operational environment requires careful evaluation and planning to ensure protection of core IACS assets, data, and operational stability.

Table of Contents

Table of Figures

DISTRIBUTION

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

ABSTRACT

The LOGIIC program was established to review and study cyber security 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.

The LOGIIC Real Time Data Transfer (RTDT) Project focused on the assessment and analysis of real-time data transferred outside the core IACS environment. RTDT solutions provide data sets that support operational decisions in an efficient manner. The project evaluated different RTDT technologies available in the market that collect and move data from Layer 2 and 3 to Layers 3.5, 4, and beyond.

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 their cyber security capabilities. Hands-on assessment activities conducted in an IACS environment evaluated the security provided in RTDT solutions. Solutions provided by automation vendors and third-party vendors were included in the project. Solutions were installed, configured, and assessed in an IACS laboratory environment. The technical findings and operational conclusions that were derived can assist asset owners in evaluating the security attributes of RTDT solutions prior to implementation.

This report discusses the assessment attributes, findings, and considerations for using RTDT solutions in IACS environments.

Acknowledgements

The project to evaluate RTDT 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 cyber security in the oil and gas industry, and to the IACS community in general. The Automation Federation serves as the LOGIIC host organization and provides a necessary home and legal framework for our efforts.

LOGIIC would like to thank the DHS S&T Directorate for providing leadership, vision and commitment to enhancing cyber security. We would also like to express our appreciation for the vendors who participated in the project and the work of our team of subject matter experts (SMEs) 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 to DHS S&T. 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 program 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. LOGIIC initiatives are applicable to many industries with control systems.

The LOGIIC Real Time Data Transfer (RTDT) Project focused on the assessment and analysis of real-time data transferred outside the core Industrial Automation and Control Systems (IACS) environment. RTDT solutions provide data sets that support operational decisions in an efficient manner. The project evaluated solutions available in the market that collect and move data from Layer 2 and 3 to Layers 3.5, 4, and beyond. Given the shift toward increased interconnectivity and the desire for optimized decision-making, there is a need to quickly move data out of the core IACS area. Based on surveys of the LOGIIC members, expanded use of RTDT solutions is likely to occur over the next two years. An understanding the security aspects and operational requirements of these solutions will assist asset owners in choosing a solution that best fits their risk portfolio.

LOGIIC conducted a series of research surveys and studies to identify product offerings in the marketplace, their applicability to an IACS environment, and their cyber security capabilities. Solutions provided by automation vendors and third-party vendors were included in the project. Hands-on assessment activities conducted in an IACS environment evaluated the security provided in RTDT solutions. Solutions were installed, configured, and assessed in an IACS laboratory environment. The technical findings and operational conclusions that were derived can assist asset owners in evaluating the security attributes of RTDT solutions prior to implementation.

The objective of this report is to convey important factors that should be weighed when considering RTDT solutions in an IACS environment and to 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 RTDT Project was established and defined by the LOGIIC members (Technical Team, Executive Committee, and the DHS sponsor). Automation vendors were engaged and invited to participate in an assessment.

The broad project objective was to evaluate and test RTDT solutions that were presently available in the market. These RTDT solutions collect and move data from Layer 2 and 3 to Layers 3.5, 4, and beyond. RTDT solutions provide data sets that support operational decisions in an efficient manner.

This project helped to provide the foundations for the LOGIIC members to:

- Study, with the main automation suppliers, their recommended architecture for RTDT and possibly introduce these vendors to emerging solutions.
- Understand the current vulnerabilities and risks associated with emerging solutions for RTDT from major suppliers of industrial automation and control systems.
- Prepare recommendations for secure transfer of real time data.
- Assist major suppliers to improve RTDT solutions in the future.
- Prepare for future projects that will help LOGIIC develop best practices to effectively deploy and manage the transfer of data to various endpoints (i.e., a system on the business network, remote system, cloud, or mobile device).

In November 2014, LOGIIC conducted a survey of RTDT technologies available from a selected vendor set[2]. At the same time, LOGIIC conducted a survey of Executive Committee members on their use of and interest in RTDT. The study included four broad areas: data transfer applications, application delivery controllers, transfer to mobile systems, and transfer to the cloud. The surveys produced a large amount of data and assessment opportunities. The project was re-scoped in size to focus solely on data transfer applications. The findings of this assessment will support future proposed projects in areas such as cloud and mobility.

The LOGIIC member survey sought to identify the mechanisms that members had in place, their needs for transfer of data to and from Level 3, and the corporate perspective and risk model for movement of this data in the short and long term. The project was scoped using an understanding the technical considerations that factor into purchasing and implementation decisions made by the member companies.

Key takeaways from the survey:

- Data is moved in and out of the core IACS based upon need, through varying mechanisms.
- Many members use servers and clients to push or pull data, or integrated applications that specialize in data movement.
- When considering RTDT decisions, optimization is the lead motivator. Facilitation of remote connectivity and access at Level 4 from other business units are important considerations.

Use cases that presented interest to the LOGIIC members included RTDT for health and monitoring, trending analysis, decision support and situational awareness, and data sharing with strategic partner systems.

[2] LOGIIC Member Study, 2014.

LOGIIC conducted hands-on testing activities to expand its knowledge in RTDT. An assessment team was assembled that included Subject Matter Experts (SMEs), and a test architecture constructed at a laboratory facility. Building upon previous surveys, test scenarios were selected that reflect core questions posed by the LOGIIC team members. Although test scenarios were defined prior to laboratory exercises, testing afforded flexibility that allowed for pivot attacks and additional investigation into potential threat vectors or vulnerabilities, if applicable.

The assessments conducted during this project sought to answer key technical questions related to the movement of data from Level 2 to Level 4 or beyond. These answers identified the security risks associated with movement of this data, including the following example questions:

- What security controls are required to protect the data in transit?
- What security controls are required at the origination and end points?
- Do server or client capabilities for managing and packaging data introduce risks?
- What security considerations should be evaluated when implementing a data transfer solution?
- What is the life-cycle management of maintaining a secure data transfer solution?

This project focused on the analysis of RTDT from the core IACS environment. Figure 1 provides a logical diagram that shows the placement of many RTDT systems and serves as the project's reference architecture.

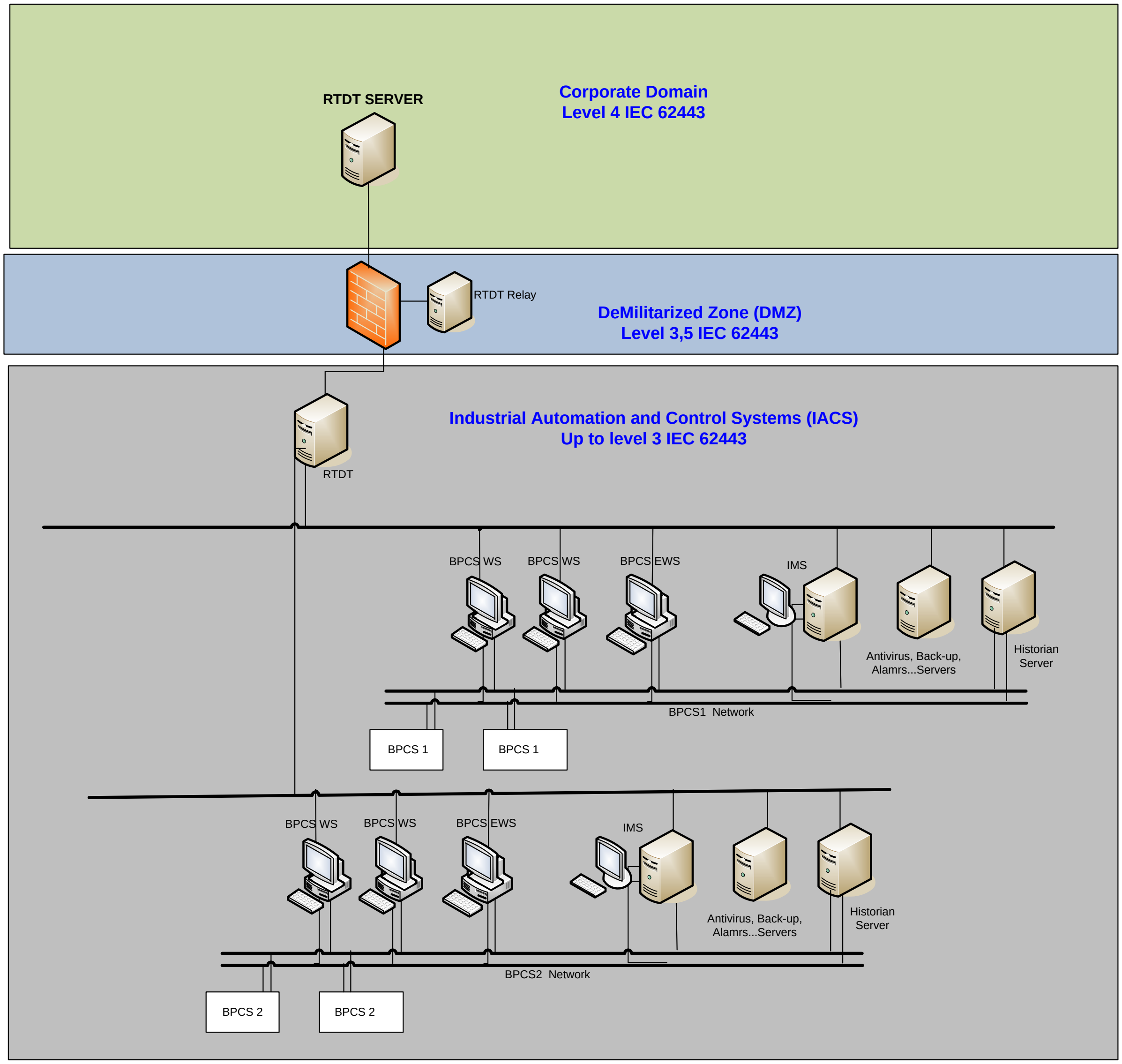


Figure 1: Reference Architecture

The project scope included data collection systems that reside in the core IACS architecture, and servers and clients that reside in the DMZ that manipulate those data sets to provide situational awareness, system health, and trends. The scope also included clients that may exist at Level 4, and receive data for use on the enterprise network.

3 Technical Approach

Technical surveys, market reviews, and engagement with automation vendors contributed to the scoping of the project and individual test scenario. Assessment and analysis followed a standard approach and 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*, to ensure that all testing expresses a plausible threat that is applicable to the oil and gas industry. The assessment scope and individual test scenarios were defined by characterizing risk in terms of threat, vulnerability and consequence.

After selecting an automation vendor and an SME in testing data transfer technologies, a Test Plan was developed that identified test scenarios and rules of engagement. The automation vendor provided network and design diagrams in advance. Test cases were developed with this architecture knowledge, and therefore the assessments were considered “partial knowledge” assessments. While in the laboratory, each participating vendor provided a demonstration and overview of their systems.

The following high-level steps were followed during the assessment for each device or system of devices:

1. Reconnaissance
2. Information Capture/Data Retrieval Attempts
3. Targeted Attack
4. Denial of Service (DoS)

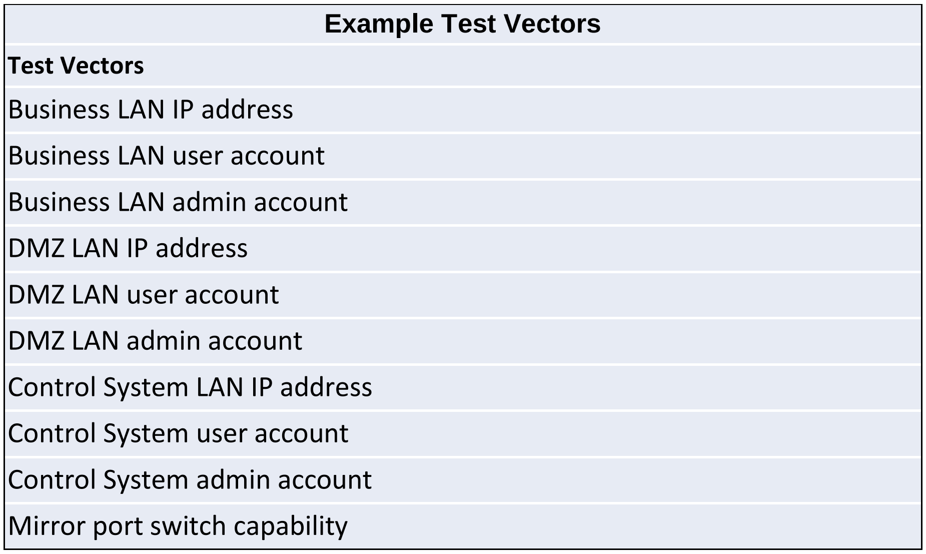
As with the standard LOGIIC assessment approach, attacks were only considered viable if they were traceable and reproducible.

While technical activities, such as reconnaissance and attack, form the basis for most of the assessment findings, observations about interactions with devices, setup, and troubleshooting can provide valuable information for the LOGIIC team. Performance of security features, resilience, and robustness were measured by technical results and by general observations during the assessment.

Assessment Approach

Four RTDT solutions were assessed during this project. Two solutions were offered by automation vendors. The remaining two solutions were considered “third-party” solutions, and were offered by vendors who do not manufacture SCADA or DCS systems. The assessment of each product operated as an independent sub-project. While the assessment approach and test cases were often repeated across the projects, each assessment occured during a separate test phase in the laboratory to ensure confidentiality of specific technical findings.

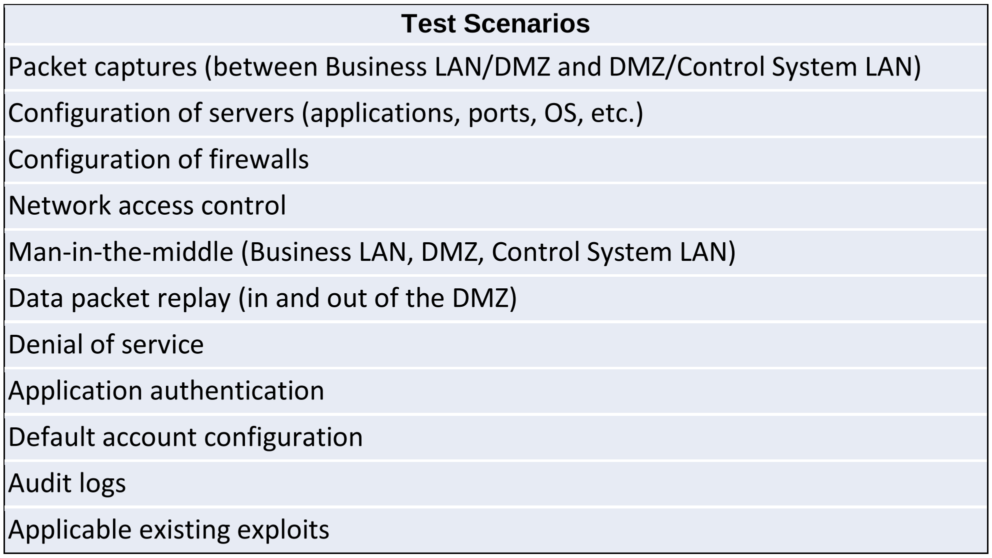
Test vectors were developed by the LOGIIC team, and by the SME, to answer key questions of specific interest to the LOGIIC members. Example test vectors, listed below, were utilized by the SME to develop broader test scenarios and select applicable tools.



Example Test Vectors
Test Vectors
Business LAN IP address
Business LAN user account
Business LAN admin account
DMZ LAN IP address
DMZ LAN user account
DMZ LAN admin account
Control System LAN IP address
Control System user account
Control System admin account
Mirror port switch capability

Figure 2: Test Vectors

Test Scenarios were defined that represented potential attacks against all elements of the RTDT solution. These include areas that may be attacked by insider and outsider threats. Figure 3 represents the general test scenario categories. In some test scenarios, multiple test cases were designed to ensure completeness of testing.



Test Scenarios
Packet captures (between Business LAN/DMZ and DMZ/Control System LAN)
Configuration of servers (applications, ports, OS, etc.)
Configuration of firewalls
Network access control
Man-in-the-middle (Business LAN, DMZ, Control System LAN)
Data packet replay (in and out of the DMZ)
Denial of service
Application authentication
Default account configuration
Audit logs
Applicable existing exploits

Figure 3: Test Scenarios

The SME conducted the test scenarios using their attack methods, payloads, and equipment. Each assessment included vendor setup and a pre-work phase conducted by the SME. The pre-work phase included connection of test equipment, network validation, reconnaissance, and traffic capture. During the pre-work and testing phases, the SME utilized publicly available tools and SME-developed customized scripts.

Test Tools
Kali Linux™ distribution for penetration testing[3]
Wireshark®[4]
Nmap
Nessus®[5]
Ettercap
Arp spoofing tools
Computer forensic tools
Custom attack scripts
Existing exploits
Reverse engineering tools

Figure 4: Test Tools

White cell[6] activities during the assessment were performed by the LOGIIC Technical Lead. All test techniques, steps, results, and observations were noted during the assessment.

Analysis of Findings

The technical conclusions described in the following sections of this report are based on a series of inputs and data sources, including:

- Background research conducted under the project,
- Product documentation, technical briefings, and design details from the automation vendor,
- Assessment test scenario results,
- Background information on each threat vector provided by the SME,
- Observations during the assessment, and
- Functional and usability testing.

In addition to technical test findings, operational observations also contribute to overall project conclusions. This includes usability, ease of setup, maintenance requirements, and skillsets required to maintain and use the system. These findings assist LOGIIC members in determining a return on investment should they choose to implement this technology in an operational setting.

[3] Kali Linux ™ is a trademark of Offensive Security.

[4] Wireshark is a registered trademark of the Wireshark Foundation.

[5] Nessus is a registered trademark of Tenable Network Security.

[6] A white cell is an independent person who collects findings and records events during the assessment. White cell activities are not typically performed by a red teamer or a vendor.

4 Assessment Findings

The assessment produced numerous technical and operational findings. This section presents technical and operational findings and key discussion points. Approximately 35 to 55 individual test cases were conducted during each assessment. Findings from each test case were reviewed and ranked by consequence-based severity and likelihood. These technical findings were merged with operational conclusions, and observations were categorized into broader areas. Each area is relevant when considering the selection and implementation of an RTDT solution.

Positive Security Attributes

Throughout the assessments, specific attributes of the solutions were identified that added to the inherent security of the solution. These include:

- Correct implementation of encryption when included in the solution,
- Use of packet integrity and packet privacy,
- Up-to-date patching,
- Disabling unnecessary ports and services,
- Protection of data at points of rest during the overall transfer through database security or access control,
- Protection of application log files with access controls and ensuring contents can support an adversary’s attempt to gather detailed information on the application, certificates, or key exchange,
- Removal of default settings, and
- Careful configuration of network devices at all levels.

As will be discussed in the following sections, configuration of these attributes within an RTDT solution is necessary to achieve protection at all levels of the network.

Automation Vendor and Third-Party Solutions

The assessments included solutions offered by automation vendors who offer full control systems alongside RTDT solutions, and third-party vendors who specialize in the RTDT area and do not sell full control systems. The solutions tested incorporate a variety of OPC UA, DA, and DCOM protocol standards. The inclusion of different types of vendors was intended to provide a spectrum of product capabilities for testing. Technical findings within these two categories of vendors generated operational conclusions that may help asset owners choose the solution that best fits their risk portfolio and desired level of engagement with the solution.

The automation vendor solutions under test were designed primarily to interface with a particular control system offered by the vendor. However, these solutions were also able to interface with other control systems and third-party tools. Still, this approach to design resulted in solutions with a larger footprint, more components, and at times more configurability. The automation vendor solutions typically included significantly more hardware and networking components. Due to the larger footprint and numerous components, an asset owner may feel they have received the entire package from the automation vendor, including service and maintenance, with assurance that it will work in the environment with their existing control system.

The third-party solutions tested were created to perform a single objective: to integrate with the control system, or systems, by moving data securely from an origination to a destination point. The solutions under test were significantly smaller and consisted only of software. The solutions were designed to be installed on the hardware of the asset owner's choosing. Though network security recommendations may be provided to the asset owner, no networking hardware is included in the solution. As a result, the asset owner may need to configure security on their own networking components.

We will see in the following sections how these differences affect the security of the solution, which must be matched with the asset owner's desired level of engagement throughout the life-cycle.

Solution Footprint and Management

Both of the third-party solutions that were tested followed a similar methodology which provides the asset owner with the solution and allows either the vendor or the asset owner to perform the installation and configuration.   Configuration instructions and security recommendations are provided by the vendor. If the asset owner uses a defense-in-depth methodology within their operations, they would need to ensure that sufficient layers of security are in place around the third-party solution. This includes firewall configuration, monitoring, etc. No remote management or connectivity options existed in the third-party solutions. Patch management consists of vendors alerting the asset owners that patches are available. Obtaining and installing the patches is the responsibility of the asset owner. If an asset owner prefers to control the supporting network infrastructure, as well as the RTDT solution, a third-party solution may be an attractive option.

Because the third-party solutions have a limited number of installation points and no additional hardware, the system footprint is small. This reduced footprint also reduces the attack surface, a benefit which was evidenced throughout the test scenarios. The assessment team concluded that the absence of unnecessarily complex structures reduces possible threat vectors and adds to the inherent security of the RTDT solution. Maintaining this security does require sufficient protections from the surrounding architecture, which is managed by the asset owner.

The automation vendor solutions tested were significantly larger in size, and included servers and networking hardware. This larger footprint, which is discussed in the remaining technical findings, offered a broader attack surface. Implementation, ongoing maintenance, and patch management is offered by the vendor, and could be included as part of a broader maintenance agreement between the vendor and asset owner. Because asset owners value automation vendor accreditation, and ensured operability with an existing control system is attractive, these solutions may be an easier — but not necessarily more secure — choice for the asset owner.

The Use of Third-party Components in Automation Vendor Solutions

In solutions provided by the automation vendors, use of third-party components within the RTDT solution is not uncommon. Vulnerabilities may exist at various levels of third-party solutions, and commonly arise from configuration and implementation issues. If third-party products are used, security must remain inherent throughout the supply chain, design and implementation. This was evidenced during the assessments, when vulnerabilities were discovered that existed in unpatched third-party OPC components. If these components are included in a solution, they must be configured and maintained to recommendations made by the third-party vendor, at a minimum. Asset owners must be assured that each component in the solution they are purchasing is secure, with no default accounts or passwords, and patches are current to the implementation date. The importance of patching also raises the question of long term maintenance. In a fielded solution, the asset owner and the automation vendor need to clearly identify who is responsible for third-party patch maintenance.

Networking Components

Many automation vendor solutions include networking hardware. Some provide recommendations for firewall configuration. As with the inclusion of third-party components, an asset owner must be assured that networking devices provided by the automation vendor, such as firewalls and switches, are configured securely. The assessments revealed that these components did not always provide the required security, or perform in a manner that the automation vendor anticipated. This evidence underscores the finding that if an asset owner chooses to implement an RTDT solution with many components, they must be assured that all components have been tested and are secure. It is also recommended that network devices provided by the vendors be monitored by the asset owner with network management tools. Management and patch maintenance of all components in the solution must be clearly established with the automation vendor at the beginning of the life-cycle.

Importance of Encryption

When an RTDT solution includes an encryption mechanism, implementation of that encryption becomes a critical element to successfully securing the solution. Some of the more significant findings identified in this project surround the encryption offered by each solution. This is true of both automation vendor solutions and third-party solutions. All solutions assessed offered some type of encryption in the data transit. In addition to ensuring that all data paths are encrypted to a level satisfactory to the asset owner, the implementation details must also be identified. These include:

- **Algorithm Selected**
  The encryption algorithm should be commensurate with industry best practices, such as AES. Vendors should clearly identify the algorithm in use, such as AES. Asset owners should not assume that advertised “encryption” means that an acceptable algorithm has been implemented. Assessments indicated that in several cases, vendors did not correctly implement a valid encryption algorithm, which created potential vulnerabilities. Asset owners may choose to do independent validation of the encryption algorithm during design reviews and pre-implementation testing to ensure sufficient protections exist against MiTM attacks.

- **Implementation Details**
  Encryption is not inherently secure unless implemented correctly. Key generation, handling, and storage are details that should be provided to the asset owner. Hard-coded keys or confusion on how to change a key could create security risks.

- **Understanding When and Where Data is Encrypted**
  In addition to ensuring that data paths are encrypted, asset owners should ensure the encryption of passwords used for authentication to various servers within the solution. If desired, an asset owner may also wish to encrypt data at rest in storage locations within the solution (an observation noted later in this report).

- **Identifying the Path Forward**
  Because these solutions may be fielded for a significant length of time, asset owners should discuss the path forward for upgrading to new encryption options when appropriate.

Networking and Packet Handling

While firewalls and smart switches can provide significant benefit in protecting the RTDT solution, vulnerabilities that must be mitigated, patched, and maintained may exist on these devices. Network design and flow of traffic must be considered prior to implementation. Firewalls and switches do not necessarily protect against MiTM attacks. ARP spoofing may also be possible, depending on the implementation. Even though network equipment, including firewalls and switches, may be provided by the vendor, they may not operate as anticipated. These devices must be verified and tested prior to full fielding.

Other details for consideration include the service path and protocols. Service path names should be fully quoted to mitigate service path vulnerabilities, which generally appear on network audits. In addition, some standard protocols use Windows NTLM, which must be configured for added authentication or packet integrity.

In all solutions assessed, the use of packet integrity or packet privacy provided protection against MiTM attacks and data alteration. As additions to encryption, packet integrity and maintaining security of and monitoring network components provide key aspects of securing the overall RTDT solution.

Lastly, to ensure optimum security, a true DMZ (as defined by industry guidelines) should be implemented in the architecture. Some solutions can be used with a single switch, rather than a full DMZ, which does not provide the most security.

Layered Security

RTDT solutions require layered protections. In addition to testing the protection of data in transit, these areas were also evaluated during the assessments:

- **Storage**
  Most RTDT solutions offer data storage capabilities at points within the overall solution. These can exist at multiple levels within the architecture. Storage is commonly accomplished through a SQL database. In the solutions assessed with storage available, data was not encrypted. SQL databases were often configured with access controls and the principle of least privilege. Encrypting stored data may be important to an asset owner, depending on the level where data is stored and the length of time it is stored.

- **Log Files**
  Components within the RTDT solution often generate log files with system information. Review of these logs files was included in each assessment. Files were inspected for content and to determine if file protections aligned accordingly. In many cases, log files included information about certificate exchange, and debugging and application information. These files typically have the required access controls, such as read-only restrictions.

- **Default Settings**
  Like all solutions in the IACS environment, good security practices involve review and change of any default settings that may be vulnerable. This includes default accounts and passwords, permission levels, and application settings. The principle of least privilege should be consistently applied throughout the RTDT solution. Any unnecessary ports and services should also be disabled.

- **Tag Security**
  Many RTDT solutions offer configurable tag security, which allows the asset owner to control access to data at a granular level. This level of configurability can provide asset owners with the ability to change settings as they deem necessary. However, the default security settings on the tags (which can be set to minimal protections) should be thoroughly reviewed, and configured accordingly. Though configurable tag security provides useful options for asset owners, it is an element that must be reviewed and maintained to ensure it provides the needed protections.

Using, Managing, and Maintaining the Solution

During the assessment, information was collected from the vendor and observations were made that help to form conclusions about the operation and maintenance of security features. The installation process was observed during all assessments. No significant obstacles arose for any of the solutions under test. For the most part, installation of hardware and software proceeded as expected. The only area of troubleshooting during installation for both automation vendor or third-party solutions was the integration with networking hardware. This is common in any technical solution that relies on proper and specific communication pathways. Still, this troubleshooting did not add significant time to the installation processes. Depending on the footprint of the system being installed, installation times ranged from 45 minutes to 10 hours. Installation time included hardware and software setup, system and security configuration, and network troubleshooting.

Configuration and management of each solution under test was provided through a series of user interfaces. User permissions, tag security, and defining ports, and other details can be configured by the user. Most vendors provide security recommendations to change default settings and restrict access. As access levels and information flow may change, an asset owner would need to interface with the system to change the security accordingly. While this may not involve significant human resources or training, a user would need to understand the details of the system and networking.

Patches are handled differently based on vendor patch and update programs. Automation vendors may include patches for the RTDT components as part of their larger control system patch programs. The third-party vendors that participated in this project alert their customers when patches become available. Asset owners would then need to obtain and implement the patches on their systems.

A common asset owner concern is the level of effort and skillset required to manage and maintain the system. Like nearly all other technologies assessed under the LOGIIC projects, RTDT solutions require some level of ongoing engagement with the system after installation and configuration. Technical findings identified during the assessments indicate the importance of patching the systems, particularly those systems with many components. The desired level of engagement during installation, configuration, and ongoing management, may be a factor in selecting an RTDT solution.

5 Conclusions

Increasing interconnectivity and the need for advanced situational awareness requires accessibility to data generated within the lower levels of the core IACS environment. Transferring this data requires movement to other levels within the organization or to strategic partner systems. In all cases, data is made accessible to those who are outside the core IACS environment, but have a need to know. To achieve this, the data must be handled, transferred, and stored with protections in place.

Automation vendor and third-party solutions were assessed, and although data transfer functionality is effectively the same, the solutions varied in size and structure, depending on the vendor's design and integration with other control systems. Automation vendor solutions typically included hardware, software, and networking components that were offered in one solution package. Third-party vendors typically provided software-only solutions, which are meant to be installed on hardware provided by the asset owner on a network with existing firewalls in place.

Automation vendor solutions offered a larger footprint, with more components that require security and management. However, these solutions are often installed by the automation vendor, accredited, and included in broader patch management plans. Third-party solutions provided a smaller footprint and therefore a smaller attack surface. Requirements to configure and maintain the security of the system and networking components would likely be the responsibility of the asset owner. Asset owners should review the size of the system, configuration, and management requirements and choose a solution that aligns with their risk portfolio and desired level of engagement with the solution.

Technical findings identified during all assessments can be summarized as follows:

- Solutions with larger footprints and more components provide an increased attack surface. Mitigating these risks require careful configuration, patching, and ongoing maintenance.

- Solutions that employ third-party components, such as OPC clients, firewalls, and databases, require security at all layers. An asset owner must be assured that components in the supply chain are configured appropriately, patched, and implemented according to the original vendor's security recommendations. Like encryption, the OPC implementation is critical to ensuring secure data movement.

- In all solutions assessed in this project, encryption was necessary in an RTDT solution to protect data in transit. Correct implementation of the encryption ensures this protection, and includes a viable algorithm, as well as careful key generation, handling, and storage. An asset owner must feel confident in the encryption implementation and may wish to seek independent testing prior to choosing a solution. Asset owners should not assume without validation that simply because encryption is advertised, it has been implemented correctly.

- The security of networking components, such as firewalls and smart switches, is critical to the security of the overall solution. Whether provided by the vendor or the asset owner, these components should be configured and managed to maintain the needed levels of security.

- An inherently secure solution requires that all layers and components be secure. Asset owners should ensure that user settings, tag security, application security, and handling of data at rest meet their security requirements.

- Management of the RTDT solution through patching and updates is necessary to maintain security. An asset owner should evaluate these requirements and identify a path forward with the vendor to evolve to meet changing security needs.

Positive security attributes within an RTDT solution are typically the result of a defense-in-depth approach within the vendor's design. This includes the correct implementation of encryption, use of packet integrity and privacy, disabling unnecessary ports and services, patching, and providing the asset owner with security recommendations.

Reviewing the initial project questions, the following brief conclusions were made:

- **What security controls are required to protect the data in transit?**
  Secure implementation of protocols, encryption, and network security are required. These should be inherent in the design of the system and in maintenance plans.

- **What security controls are required at the origination and end points?**
  Layered system and application security, including IP subnetwork security and segmentation, careful configuration, access controls, and maintained patches are required. If third-party components are included in the design, these components must be implemented securely and maintained with the overall solution. If data at rest is stored in a database, access controls and sufficient protections must be included. These may include granular permissions and ensuring that databases are patched and maintained.

- **Do server or client capabilities for managing and packaging data introduce risks?**
  Application security and patching is important, along with reviewing access controls and tag security for any changes needed to meet changing security requirements. Asset owners may also want to seek the ability to encrypt data in storage at certain points in the solution.

- **What security considerations should be evaluated when implementing a data transfer solution?**
  Encryption, configurability, security of the supply chain, maintenance and other items as listed in the Technical Findings section, should all be considered when evaluating an RTDT solution. An asset owner should review these details with the vendor and may choose to perform a design review or independent testing prior to selection.

- **What is the life-cycle management of maintaining a secure data transfer solution?**
  As stated throughout the report, the asset owner should make sure to patch and change access controls and tag security to meet evolving needs. An established patch maintenance plan with the vendor can assist in forecasting resource needs throughout the life-cycle.

The detailed technical findings and operational conclusions derived during this project produced a set of topics that should be evaluated when selecting a RTDT solution. As is commonly determined in LOGIIC projects, the implementation of new technologies in a critical operational environment requires careful evaluation and planning to ensure protection of core IACS assets, data, and operational stability. In this project, the focus was on security of the data moving outside of Levels 2 and 3. Unlike many other technologies assessed by LOGIIC, RTDT can be entirely disabled in the architecture without impacting core control system operability, although inefficiencies may occur.

Studies performed by LOGIIC as part of this project indicate asset owners' desire to optimize data flow and decision making through data accessibility. This requires an RTDT solution that maintains the level of security desired by the asset owner, but establishes a level of interconnectivity to support operational decisions. These studies indicate that use of RTDT solutions will likely continue to expand. Asset owners should work closely with vendors to establish a detailed understanding of the RTDT solution’s structure and design. Numerous technical details should be considered, including implementation of encryption, use of third-party components, and defense-in-depth attributes. In addition to technical details, operational considerations such as installation, configuration, patching, and life-cycle maintenance should be evaluated. It is possible to securely transfer data outside the core IACS environment if all components and facets of the RTDT solution have been secured and a plan is established to maintain the needed level of security throughout the life-cycle.

ACRONYMS

Term/Acronym	
AES	Advanced Encryption Standard
BPCS	Business Planning and Control System
CSRDC	Cybersecurity Research and Development Center
DCOM	Distributed Component Object Model
DCS	Distributed Control System
DHS S&T	Department of Homeland Security Science & Technology Directorate
DMZ	Demilitarized Zone
DoS	Denial of Service
IACS	Industrial Automation and Control System
IEC	International Electrotechnical Commission
IP	Internet Protocol
LAN	Local Area Network
LOGIIC	Linking the Oil and Gas Industry to Improve Cybersecurity
MiTM	Man-in-the-Middle
OPC	Open Platform Communications
OPC DA	Open Platform Communications Data Access
OPC UA	Open Platform Communications Unified Architecture
OS	Operating System
RTDB	Real Time Database
RTDT	Real Time Data Transfer
SCADA	Supervisory Control and Data Acquisition
SME	Subject Matter Expert
SQL	Structured Query Language