LOGIIC

Safety Instrumented Systems Project

September 28, 2018

Final Public Report

Document Title	*LOGIIC Safety Instrumented Systems Project Public Report*
Version	*Version 1.0*
Primary Author	*A. McIntyre (SRI)*
Distribution Category	*Public – Unlimited Distribution*
Approval Status	*Approved - September 28, 2018*
Reviewed by AF Legal	*Approved - September 28, 2018*
Approved (date)	*Approved - September 28, 2018*
Approver (EC or AF)	*Marty Edwards – September 28, 2018* *Managing Director Automation Federation*
Digital Signature for PDF	Marty Edwards Digitally signed by Marty Edwards Date: 2018.09.28 12:03:59 -06'00'

EXECUTIVE SUMMARY

The Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) 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 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 Project 11, Safety Instrumented Systems (SIS), 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 11 objective was to evaluate SIS solutions currently available in the market and develop conclusions about the security of specific architecture designs. This project builds on LOGIIC Project 2, which also investigated the security of three architecture designs for SIS solutions. LOGIIC Project 2 was conducted nearly a decade ago; since then, significant advancements and changes have been made in both the technology and the recommended best practices for the IACS environment.

LOGIIC conducted a series of research surveys and studies to identify product offerings in the marketplace and identify their cybersecurity capabilities. Hands-on assessment activities conducted in an IACS environment evaluated the security of these solutions.

The scope of this project included an assessment of full SIS solutions including controller, engineering workstations (EWSs), network backbone and supporting components. LOGIIC sought to understand the threat landscape of current SIS offerings and identify the evolving SIS designs that take into account previous research, findings and international standards.

The objective of this report is to convey the findings and conclusions from hands-on assessments that provide asset owners with important considerations in selecting an SIS design, and to support a dialogue between asset owners and automation vendors.

This project identified technical and operational findings in SIS solutions assessed in an IACS laboratory environment. These findings include:

Integrated Architecture
Since Project 2, SIS architectures have shifted towards a more integrated design. Several factors likely contributed to this shift, including the development and adoption of industry SIS design standards and the desire for asset owners to have increased situational awareness.

Reducing the Attack Surface
The SIS solutions tested in Project 11 contained multiple components and redundant networks, making the architectures significant in size and capability. Given the size and number of components, minimizing the attack surface requires that security be considered at the SIS design phase.

Networking
Network structure makes a significant contribution to the overall security of the SIS. Assessment findings in several areas indicated the influence in overall security. These include redundancy, more secure protocols, and domain security.

Firewalls

Firewalls are necessary since they filter malicious network traffic and protect against some denial-of-service (DoS), packet-manipulation and packet-injection attacks. However, firewalls require proper configuration and periodic maintenance.

Intrusion Detection

Most SIS solutions include intrusion detection mechanisms that produce configurable alerts. Intrusion detection capabilities and their configurability vary depending on the solution, but they play an important role in situational awareness of the SIS.

Lock Functionality

The SIS solutions assessed in Project 11 used a software and/or hardware locking mechanism. This restricts certain functionality such as downloading a configuration and making changes to the safety logic. Although these locks provide significant protection against unauthorized changes to the SIS, third party research conducted in late 2017 showed that some of implementations could potentially be bypassed by an attacker with presence on the SIS.

Documented Recommendations

Many SIS vendors maintain a suite of documentation that includes detailed security recommendations. These clearly define best practices and recommended configurations. However, some vendors do not identify, or make recommendations on, the most secure implementation. Assets owners should request that vendors provide these recommendations based on product testing, validation, and past implementation experience.

Since Project 2, SIS solutions have shifted toward integrated designs with the IACS. A number of industry standards were developed in the past decade that provided guidelines for securely integrating SIS and IACS. Comparing the technical findings between Project 2 and Project 11 identified areas of progress and improvement. Asset owner and vendor engagement has led to a clearer understanding of operational goals and greater inherent security in SIS designs. Vendors provide security recommendations and documentation that assist in a more secure implementation, based on the asset owners' needs. Current default configurations provide some security, but many configurable options can be leveraged by asset owners to increase security.

This project concludes that, although SIS solutions continue to evolve into integrated designs, security mechanisms have been designed into new solutions with configurable options that can be leveraged by asset owners. Engagement between asset owners and vendors has resulted in robust, capable SIS solutions that employ defense in depth, access control, and situational awareness. When selecting an SIS solution, asset owners should consider the points described in this report when aligning SIS capabilities with the security and operational goals at their organizations.

Table of Contents

Table of Figures

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 broad Project 11 objective was to evaluate SIS solutions currently available in the market and develop conclusions about the security of specific architecture designs. This project builds on LOGIIC Project 2, which investigated the security of three architecture designs for SIS solutions. LOGIIC Project 2 was conducted nearly a decade ago; since then, significant advancements and changes have been made in both the technology and the recommended best practices for the IACS environment.

LOGIIC conducted a series of research surveys and studies to identify product offerings in the marketplace and identify their cybersecurity capabilities. Hands-on assessment activities conducted in an IACS environment evaluated the security of these solutions.

The scope of this project included an assessment of full SIS solutions including controllers, engineering workstations (EWSs), network backbone and supporting components. LOGIIC sought to understand the threat landscape of current SIS offerings and identify the evolving SIS designs that consider previous research, findings and international standards.

The objective of this report is to convey the findings and conclusions from hands-on assessments that provide asset owners with important considerations for selecting an SIS design and to support a dialogue between asset owners and automation vendors.

2 PROJECT SUMMARY AND BACKGROUND

The LOGIIC Project 11, Safety Instrumented Systems (SIS), was established and defined by the LOGIIC members which includes the technical team, executive committee and the Department of Homeland Security (DHS) sponsor. Automation vendors were engaged and invited to participate in an assessment.

The broad Project 11 objective was to evaluate SIS solutions currently available in the market and develop conclusions about the security of specific architecture designs. This project builds on LOGIIC Project 2, which also investigated the security of three architecture designs for SIS solutions. LOGIIC Project 2 was conducted nearly a decade ago; since then, significant advancements and changes have been made in both the technology and the recommended best practices for Basic Process Control System (BPCS) environments.

Based on the findings of LOGIIC Project 2, this project's goal is to re-evaluate cybersecurity vulnerabilities based on the threat scenarios of typical architectures. Like Project 2, Project 11 categorizes SIS architectures into three designs based on interconnectivity. Since Project 2, the market has evolved in ways to support securely integrated SIS and control systems. Techniques to do this are defined by International Electrotechnical Commission (IEC) standards, with which many SIS solutions are compliant. The following information describes the categorized SIS architectures.

Architecture A
In Architecture A, the BPCS and SIS controllers, engineering workstations (EWSs) and human-machine interface (HMI)/operator workstations (OWSs) reside on a common local area network (LAN).

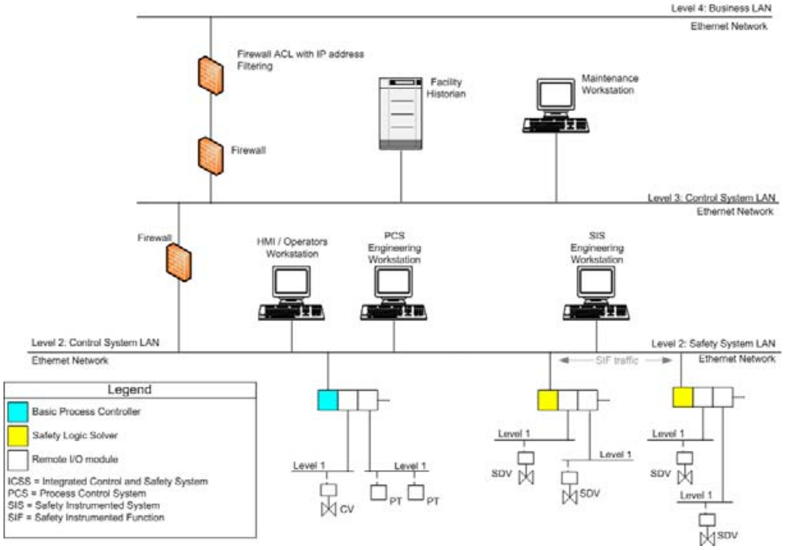

Level 4: Business LAN
Ethernet Network
Firewall ACL with IP address Filtering
Facility Historian
Maintenance Workstation
Firewall
Level 3: Control System LAN
Ethernet Network
Firewall
HMI / Operators Workstation
PCS Engineering Workstation
SIS Engineering Workstation
Level 2: Control System LAN
Ethernet Network
Level 2: Safety System LAN
Ethernet Network
SIF traffic
Legend
Basic Process Controller
Safety Logic Solver
Remote I/O module
ICSS = Integrated Control and Safety System
PCS = Process Control System
SIS = Safety Instrumented System
SIF = Safety Instrumented Function
Level 1
Level 1
CV
PT
PT
Level 1
SDV
Level 1
SDV
Level 1
SDV
Level 1
SDV

Figure 1: Integrated PBCS and SIS, Architecture A

Architecture B

Architecture B is similar to Architecture A, except that it provides an isolated safety-critical network for peer-to-peer communications between SIS controllers. This architectural modification is intended to provide significant protection of safety-critical communications.

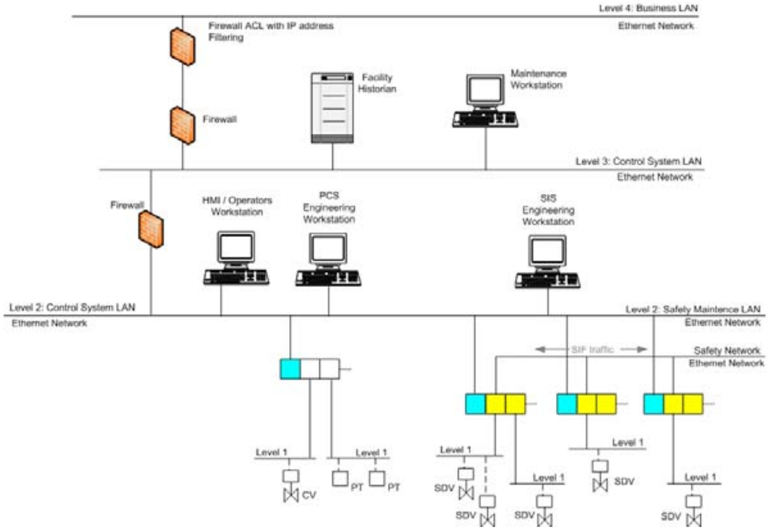


Figure 2: Partially Integrated BPCS and SIS, Architecture B

Architecture C

Architecture C is different from Architectures A and B. Architecture C consists of independent BPCS and SIS. In this design, the SIS is both logically and physically isolated from the BPCS. SIS and BPCS are connected through a direct point-to-point communication connection. This point-to-point connection does not travel over the same network interface that is used for other communications (for example, to the SIS EWSs). These types of point-to-point communications may use either serial or Ethernet connections depending on the specific protocol in use.

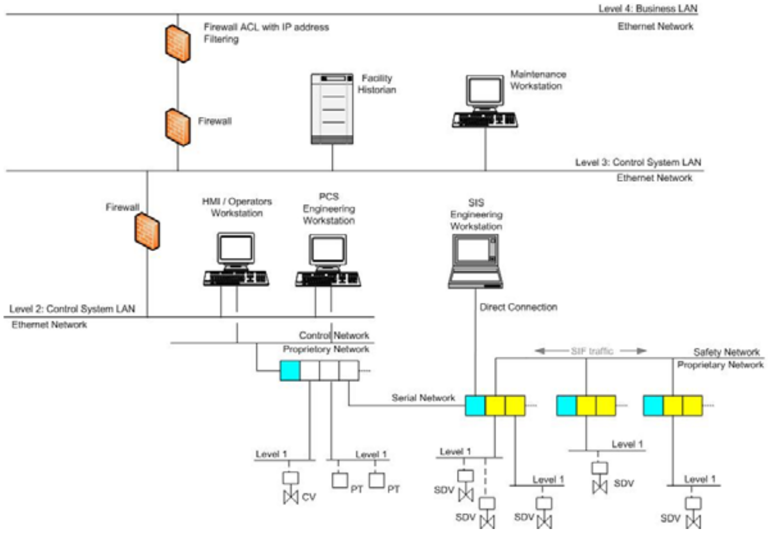


Figure 3: Not Integrated BPCS and SIS, Architecture C

For each typical architecture, the scope of this project included the system inventory (including subsystems, network devices, and software); cybersecurity risk assessment; security of operations (including the network segregation and/or integration); logical and physical protection; maintenance policies and tools; backup, restore, and disaster recovery plans; and host protection and patch management.

A survey of LOGIIC members' use of SIS was conducted in July 2016. Findings indicate that:

- SIS is clearly a valuable part of operations, with security concerns relating to integrity, availability and risks relating to access, denial of service and connectivity.
- Some upstream and downstream segments within the same organization use different SIS architectures. There is not an apparent trend, however, for all upstream or downstream segments in different organizations to use the same model.
- Project 2 provided some guidance to the members. Since then, standards have been fully integrated into vendor designs and technology has evolved.
- All members are considering upgrading SIS solutions in the near future.
- Members wanted Project 11 to identify risks in the new technologies, how the architectures are being applied across solutions, and technology roadmaps.

The Project answers key questions regarding whether a cybersecurity threat can:

- Impact the safety instrumented function (SIF).
- Impact the performance of the SIS.
- Impact the by-pass mode.
- Impact the instrumentation management functions.
- Compromise engineering and operation function of the SIS.
- Provoke spurious SIF trips.
- Compromise the BPCS function used for the operation and engineering of the SIS.

The Project identifies and tests the impact of any vulnerability discovered on one sub-system or device of the SIS or the BPCS, and helps to provide the foundations for the LOGIIC members to:

- Study the architectures of automation suppliers (BPCS and SIS) and package vendors who integrate SIFs in their integrated or non-integrated solution.
- Study the vendor-standard interconnectivity between the BPCS and the SIS (e.g., directly from SIS CPU, through non-routable communications).
- Study the communication between several SISs (e.g., dedicated SIS peer-to-peer or not).
- Understand, from the proposed BPCS-SIS architecture, the threats that can exploit vulnerabilities with the relevant associated risks.
- State and propose recommendations for selecting and implementing a typical BPCS-SIS architecture.
- Assist major automation suppliers and package vendors to improve the security of their BPCS-SIS solution in the future.

3 Technical Approach

Technical surveys, market reviews and engagements with automation vendors contributed to defining the project scope and individual test scenarios. Assessment and analysis followed a standard approach and used previously tested assessment methodologies. This section outlines the details of the approach.

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 a subject matter expert (SME) in testing SIS technologies, the team developed a test plan that identified test scenarios and rules of engagement. The automation vendor provided network and design diagrams in advance. Because test cases were developed with this architecture knowledge, the assessments were considered partial-knowledge assessments. While in the laboratory, the participating vendors provided a demonstration and overview of their systems.

The assessments for each device or system of devices used the following high-level steps:

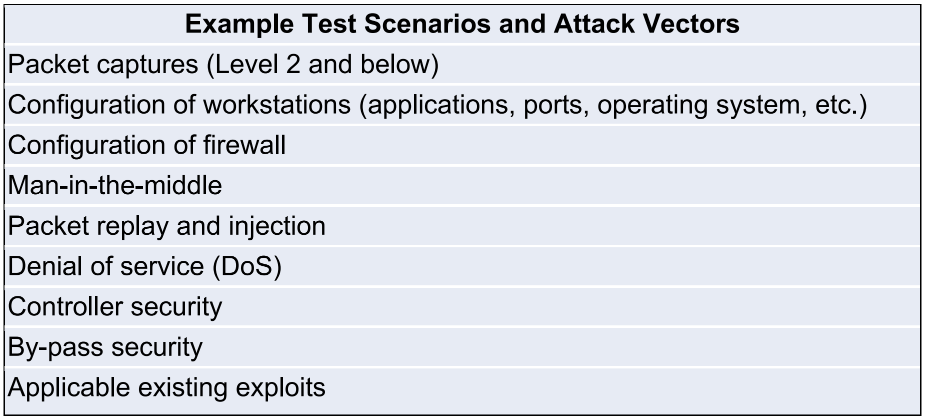
1. Reconnaissance
2. Information capture and/or data retrieval attempts
3. Targeted attack
4. Denial of service (DoS)

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, formed the basis for most of the assessment findings, observations about interactions with devices, setup and troubleshooting provided 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

Multiple SIS solutions provided by automation vendors were assessed during this project. The LOGIIC team and SME developed test vectors and test scenarios to answer key questions of specific interest to the LOGIIC members. Example test vectors were used by the SME to develop broader test scenarios and select applicable tools (Figure 4).



Example Test Scenarios and Attack Vectors
Packet captures (Level 2 and below)
Configuration of workstations (applications, ports, operating system, etc.)
Configuration of firewall
Man-in-the-middle
Packet replay and injection
Denial of service (DoS)
Controller security
By-pass security
Applicable existing exploits

Figure 4: Test Scenarios and Attack Vectors

The SME conducted the test scenarios using defined 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 used publicly available tools and SME-developed customized scripts.

For each architecture under test, the SME used various connection points and accounts (provided by the vendor) to represent various levels of insider and outsider threat. Insider connections included physical access to the safety network, Level-2 IP addresses and user and administrator accounts. Outsider threat was represented by testing from other logically separated networks or a representative system on the control system network.

Test Tools
Wireshark (Network traffic monitor)
Nessus (Vulnerability scanner)
Nmap (Network and port mapping)
Kali Linux (Linux distribution for penetration testing)
Custom Test Scripts

Figure 5: Test Tools

White cell[1] 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
- Functional and usability testing

In addition to technical test findings, operational observations also contributed to overall project conclusions. These observations included usability, ease of setup, maintenance requirements and skillsets required to maintain and use the system. These findings assisted LOGIIC members in determining a return on investment based on how they implement newer versions of this technology in an operational setting.

[1] 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 team member 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 130 individual test cases were conducted during each assessment, depending on the test architecture. 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.

Integrated Architecture

Since Project 2, SIS architectures have shifted toward a more integrated design. Key factors that likely contributed to this shift include (1) the development and adoption of industry SIS design standards and (2) the desire for asset owners to have increased situational awareness. Vendor feedback indicates that asset owners seek the ability to see alerts and status from points outside the SIS network. It is assumed, based on vendor roadmaps and feedback, that increased integration is expected in future products.

Increased integration, as pointed out in Project 2, requires added security measures. Implementation of these measures in the design is likely the most effective approach. These measures, however, must be maintained throughout the SIS life-cycle to ensure that the architecture remains secure.

Lastly, feedback from LOGIIC members indicate that SIS solutions are expected to be rated SIL3 or higher to be considered for an implementation with core operational assets.

Reducing the Attack Surface

The SIS solutions tested in Project 11 contained multiple components and redundant networks, making the architectures significant in size and capability. Given the size and number of components, minimizing the attack surface requires the consideration of security at the design phase. Reducing the attack surface requires the mitigation of operating system, application, and network vulnerabilities in the design. This includes disabling unnecessary ports, services, and accounts; removing default passwords; and enforcing access controls using the principle of least privilege. Minimizing the attack surface in the design phase ensures that the system is more secure at the time of implementation.

Maintaining security is critical. Patching and updating components of the SIS is necessary to mitigate risks, but it is also a complex task. Many systems are not easily accessible, which requires a well-planned, well-executed patch effort.

While the solutions tested in Project 11 mitigated many risks during the product design phase, technical findings and vendor feedback indicate that this is not a simple task. Vulnerabilities within the operating system or third-party components may not have available patches. Likewise, new vulnerabilities may emerge throughout the life-cycle that require patches or updates to mitigate.

Networking

As expected, the network structure makes a significant contribution to the overall security of the SIS. Assessment findings in several areas indicated the network's influence in overall security, including:

- **Redundancy** – The solutions tested in Project 11 included redundant safety networks with automatic failover capabilities. If configured correctly, redundancy provides significant protection from denial and disruption of service.

- **Protocols** – Some SIS vendors use proprietary protocols in currently available products. These protocols include packet structures that require significant effort to reverse engineer. Packet features such as timestamps, cyclic redundancy checks (CRCs) and sequence numbers add to the robustness of the protocol. These features complicate the successful manipulation and re-injection of a packet, even when network access is gained. The complexity of recreating a legitimate network packet likely makes this threat vector unattractive to the adversary.

  Protocols that use peer-to-peer communication create a complicated attack surface requiring multiple devices to be compromised for an attack to be successful. Many vendors have included encryption in their protocol roadmaps for future development, which will improve security.
- **Domains** – Consideration of security within domains is important to maintaining the principle of least privilege, a reduced attack surface, and role-based access control. Domain considerations include the security of the domain controller and the user and service accounts within the domain. Many currently available SIS solutions include some level of domain security, and it is important to maintain that level of security throughout the system's life-cycle; therefore, the domain should be included in patch and maintenance plans.

Firewalls

Throughout the testing, it was determined that the firewalls are necessary since they filter malicious network traffic and protect against some DoS, packet-manipulation, and packet-injection attacks. However, firewalls require proper configuration and periodic maintenance. Firewall rules should be configured to be as restrictive as possible. Regular firewall maintenance and updates must be performed to ensure secure operation. The placement of the firewalls within the architecture, along with many other SIS components, can make maintenance and patching a complicated process. Finally, firewalls do not protect against all attacks; they provide one layer of protection and should be used in conjunction with other protections.

Intrusion Detection

The SIS solutions assessed in Project 11 included an intrusion-detection mechanism that produced alerts based on certain actions made by the assessment teams. Intrusion detection capabilities and their configurability vary depending on the solution; however, they play an important role in situational awareness of the SIS. The configuration of alerts and network monitoring capabilities should be fully leveraged by asset owners. The intrusion-detection capabilities performed well in all products assessed in Project 11.

Lock Functionality

The SIS solutions assessed in Project 11 used a software and/or hardware locking mechanism that restricts functionality such as downloading a configuration and making changes to the safety logic. Although these locks provide significant protection against unauthorized changes to the SIS, third party research conducted in late 2017 showed that some of implementations could potentially be bypassed by an attacker with presence on the SIS. Many aspects of the locks, such as duration and automatic re-lock, are configurable. Asset owners should enforce their protection and access goals by configuring the locks accordingly. Although vendor defaults may be sufficient, it is worth additional review and configuration by the asset owner.

Documented Recommendations

Many SIS vendors maintain a suite of documentation that includes detailed security recommendations that clearly define best practices and recommended configurations. During Project 11 testing, these documents helped identify ways to reduce the attack surface and described the available layered protections and security mechanisms inherent to the system. It is recommended that asset owners use this documentation and work closely with the vendor to maximize all security capabilities within the system and match risk mitigations with their own organization's risk portfolio. When evaluating an SIS solution, or at the onset of an implementation or upgrade, asset owners should request detailed documentation from the vendor. If the documentation is limited, the vendor should be required to provide detailed guidance on the most secure implementation. If this does not exist, asset owners may wish to conduct their own independent testing and define the most secure implementation.

5 CONCLUSIONS

SIS solutions serve a critical role in overall operations. These large systems can be highly configurable and offer built-in redundancy and protective mechanisms. Like many early technologies within the operational environment, security was best achieved through airgaps or separation from other assets. In the past decade, these operational technologies, including SIS, have shifted towards a more integrated design driven mainly by the required movement of real-time data for situational awareness. While optimization and maintenance make integrated technologies and networks attractive and cost effective, integration requires significant security measures that are designed into the system and maintained throughout its life-cycle.

Several broad conclusions can be made about the security necessary in an SIS solution. Many security mechanisms are present in SIS solutions, and many are highly configurable by the asset owner. When selecting an SIS, asset owners should consider these points:

- Integrated SIS design can be accomplished securely with appropriate controls. A design should be reviewed for access controls, network separation, the principle of least privilege, and inherent security capabilities. Vendor technology that is compliant with industry standards can be a good starting point. Asset owners can confirm compliance with IEC standards through vendor engagement. Compliance is generally advertised in SIS marketing materials.
- Reducing the attack surface requires layered security throughout the operating system, application, and network. Good security practices, such as disabling unnecessary ports, services, and accounts and removing default passwords, can greatly reduce potential vulnerabilities.
- Maintenance and management of all components within the SIS through patching, updates, and periodic assessment is necessary to ensure security is maintained. The reduced network accessibility to the SIS can make these processes difficult, but they are required to ensure a reduced attack surface.
- Network security plays an important role in the overall security and stability of the SIS. Network security should include packet security through CRCs, timestamps, and/or sequence numbers. Protocol security can be achieved through proprietary protocols and/or encryption to create a complex environment unattractive to an adversary. Network redundancy, present in most SIS solutions, helps prevent disruption and denial of service. Firewalls and domain security also contribute to the layered approach to security.
- Configurable intrusion-detection capabilities provide situational awareness and alerting on the safety network.
- Hardware and software locks on the safety controllers can provide additional protection against unauthorized changes to safety logic.
- Vendor security recommendations are included in documentation suites and provide valuable information on configurable security options.

Technical findings that were identified in LOGIIC Project 2, conducted nearly a decade ago, remain relevant and can be useful in understanding ongoing risks and evolving SIS technologies. Several conclusions from Project 2 include:

- Increased integration introduces greater risk
- Default configurations are not necessarily secure
- Defense in depth reduces risk
- Clear guidance on secure implementation is needed from the vendor
- Ongoing research in security of SIS solutions is required
- Traditional Information Technology (IT) security best practices need to be evaluated with respect to their applicability in the safety domain
- Engagement between the vendor and asset owners is necessary

Greater integration definitely increases risk, particularly if security is not considered within the design of the SIS. Since Project 2, several industry standards have been developed to assist in securing an integrated design. Asset owners have demanded increased access to data, but also require a consistent level of security. As a result, vendors have developed integrated solutions with more inherent security and consideration for industry recommendations. The evolution of technology in the IACS environment indicates that integration for the purposes of speed, efficiency and awareness will continue. Feedback from participating vendors indicates that SIS solutions will continue to leverage an integrated approach in the future.

Comparing the technical findings between Project 2 and Project 11 identified areas of progress and the need for further improvements. For example, asset owner and vendor engagement has led to a clearer understanding of operational goals and the need for greater inherent security in SIS designs. Vendors are providing security recommendations and documentation that assist in achieving a more secure implementation, based on asset owners' needs. Current default configurations provide some security, but many configurable options exist that can be leveraged by asset owners to increase security.

Defense in depth and layered security were included in the solutions tested in Project 11, although this should continue to be identified as an ongoing recommendation to ensure risk mitigation and attack surface reduction. Traditional IT security measures, such as securing accounts and domains and removing default passwords, have a defined role in securing aspects of an SIS, but the criticality of a system requires advanced security measures and methods to prevent downtime or disruption.

An operational safety network requires consideration of security beyond standard IT implementations. Redundancies, protocols and packet security are present in current SIS solutions, but should evolve as technology changes to ensure that security needs continue to be met.

This project concludes that, although SIS solutions continue to evolve into integrated designs, security mechanisms have been designed into new solutions, with many configurable options that can be leveraged by asset owners. Engagement between asset owners and vendors have resulted in robust, capable SIS solutions that use defense in depth, access control, and situational awareness. When selecting an SIS solution, asset owners should consider the points described in this report to align SIS capabilities with the security and operational goals at their organizations.

The following summary of recommendations that were identified during the project are provided with a primary owner shown in parenthesis:

- Check ports and close those that are not needed. (asset owner)
- Consider using modern versions of protocols that prevent the passing of data in clear-text. (asset owner)
- Ensure that a security information and event management (SIEM) system is used to monitor logs in real-time. (asset owner)
- Verify that all versions of firmware result in full recovery after DoS attacks are removed. Although DoS attacks were possible, the SIF was not affected. (vendor)
- Remove unnecessary applications and services that may present vulnerabilities. If needed, work with the OS provider to mitigate risks associated with automatically installed software that cannot be deleted. (vendor)
- Review and verify that all default passwords are changed. No default passwords were identified during testing. (asset owner)
- Apply patches in a timely manner to ensure the appropriate management of vulnerabilities. (asset owner)
- Evaluate the security options available with the system, select the option that is most secure and configure the system to achieve maximum security. (asset owner)

Since LOGIIC completed Project 2 over 10 years ago, vendors have made the following cybersecurity improvements:

- SIS solutions are designed to provide comprehensive cybersecurity capabilities (e.g., enhanced cybersecurity capabilities of controllers), and new capabilities have addressed cybersecurity enhancements requested by asset owners
- Added new access control authentication mechanisms (e.g., Smart Card for the EWS)
- Provided new and enhanced network solutions (e.g., new switches, better placement of firewalls, improved firewall capabilities and logic, etc.)
- Added and/or improved hardware and software locks to protect credentials, devices, etc.
- Certification of components (e.g., Achilles)
- Separated some functions (e.g., domain controllers) to simplify maintenance, which facilitates the timely application of patches
- Provided integration and support for SIEM solutions with SIS solutions
- Increased support for antivirus applications and introduced support for application whitelisting
- Increased focus on cybersecurity and managing risks associated with end-of-life components

APPENDIX

Acronyms

Term/Acronym	Definition
BPCS	Basic process control system
CRC	Cyclic redundancy check
CSRDC	Cybersecurity Research and Development Center
DHS S&T	Department of Homeland Security, Science & Technology Directorate
DoS	Denial of service
EWS	Engineering workstation
HMI	Human machine interface
IACS	Industrial automation and control system
IEC	International Electrotechnical Commission
IT	Information Technology
LAN	Local area network
LOGIIC	Linking the Oil and Gas Industry to Improve Cybersecurity
OWS	Operator workstation
SIEM	Security information and event management
SIF	Safety instrumented function
SIS	Safety instrumented system
SME	Subject matter expert

Acknowledgements

The project to evaluate SIS 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 in the IACS community in general. The Automation Federation serves as the LOGIIC host organization and provides the governance and legal framework for our efforts.

LOGIIC would like to thank the DHS S&T Directorate for providing leadership, vision, and commitment to enhancing cybersecurity. We would also like to express our appreciation to the vendors who participated in the project and the work of our team of 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 the DHS Science and Technology Directorate. The content is solely the product and responsibility of the LOGIIC program and does not necessarily represent the official views of DHS.

Distribution

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