CYBER SECURITY IMPLICATIONS OF SIS INTEGRATION WITH CONTROL NETWORKS

Abstract

The LOGIIC program was established to review and study cyber security issues and their business implications as they pertain to the oil and gas sector. Recognizing the importance of Safety Instrumented Systems (SIS) in the oil and gas industry, and the rapidly emerging vendor solutions that offer varying degrees of integration with control networks (as opposed to specific isolation), LOGIIC sponsored the security evaluation and study of several SIS architectures. This session will provide a high level overview on common findings and provide recommendations to raise the bar on security especially in lieu of recent events in the news. Examples of areas of focus are in access control, resource management, and communications, and integration with basic process control systems (BPCS). An overview of the approach taken to conduct this study will also be provided.

Author

The LOGIIC Consortium – SIS Working Group; Zachary D. Tudor, SRI International, editor

Keywords

Cyber security, safety systems, process control, architecture, risk

Background

The LOGIIC[1] consortium was established by members of the oil and gas industry in partnership with the Cyber Security 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 impacting 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. Recognizing the importance of safety instrumented systems (SISs) in the oil and gas industry and the rapidly emerging vendor solutions that offer varying degrees of integration of safety functions with control networks (as opposed to isolation from them), LOGIIC sponsored a security evaluation and study of several SIS system architectures. The goals of the project were to determine what, if any, current or emerging cybersecurity issues exist within integrated control and SIS architectures, determine their impact, and develop recommendations to help reduce the cyber risk introduced by integrating SIS

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

solutions. The project sought to identify applicable and relevant security concerns regarding SISs in several areas of interest, such as access control, functional integrity of safety operations, and integration with basic process control systems (BPCSs).

LOGIIC contracted with leading subject matter experts (SMEs) who assisted the LOGIIC team in the development of a functional requirements document (FRD) and the identification of three reference architectures reflecting common strategies for integrating control and safety. LOGIIC then identified leading automation vendors who provide systems representing one or another of the reference architectures, and selected three representative systems for evaluation. The objective was not to conduct a vendor comparison, but rather to assess for each of the representative architectures, to what degree the safety function could be interrupted by an attacker with a foothold on the BPCS. The SMEs conducted tailored evaluations of the vendor systems in the summer and fall of 2010, and findings from evaluations were reported to the participating system vendors and the LOGIIC members. To the extent possible, information or findings that may identify the specific vendors participating or systems evaluated have been withheld from this report.

This paper consolidates key issues, findings, and recommendations regarding SIS integration with control system networks, based on the systems evaluated. It is based on findings as observed during the security assessment of the preconfigured systems provided by the system vendors that volunteered to participate in this study. The findings and recommendations are derived from the activities, observations, and expertise of the assessment team.

The project and its findings and recommendations are intended to inform a broad and varied audience that includes:

- Security, control systems, and SIS product vendor engineers and architects, and control system product integrators who design or implement secure industrial control systems (ICSs) integrated with SISs
- System administrators, engineers, and other information technology (IT) professionals who administer, patch, or secure ICSs integrated with SISs, and security consultants who perform security assessments and penetration testing of ICSs integrated with SISs
- Managers who are responsible for ICSs integrated with SISs and senior managers who are trying to understand implications and consequences as they justify and apply an ICS cybersecurity program to help mitigate impacts on business functionality
- Researchers and analysts studying the unique security needs of ICSs.

General Findings

The system evaluations, which were an aggregation of both automated and manual (tailored) assessment activities, yielded several observations. First and foremost, the technical integrity of the safety function was not impacted during any of our evaluations. However, in each evaluation, observations suggested vulnerabilities that could lead to temporary loss of operational view of the system or cause operator interfaces to experience issues related to integrity and availability. Several of the supporting technologies inherent in the commercial solutions (communication protocols, for

example) also had vulnerabilities that could lead to both compromise and privilege escalation. Each of the systems experienced some issues regarding availability, especially when networks were flooded with attacks and test patterns intended to subject the environment to data saturation. However, the countermeasures that were often implemented, including those related to traffic throttling, generally mitigated attacks successfully.

Although the technical safety integrity of the systems evaluated was not compromised, this was not the case for system availability. **Loss of control, loss of view, and false safety trips could negatively impact business financials (income), the environment, contractual obligations, and corporate reputation.**

For the SIS project, three distinct architectures were selected for evaluation, designated Architectures A, B, and C. In Architecture A, the BPCS and SIS controllers, engineering workstations (EWSs), and human-machine interface (HMI)/operator workstations (OWSs) all reside on a common local area network (LAN). In some cases, the SIS EWS and the BPCS EWS may reside on the same physical workstation, but with role separation. Architecture A is illustrated in Figure 1.

Architecture A represents the system with the most extensive integration. Although this level of

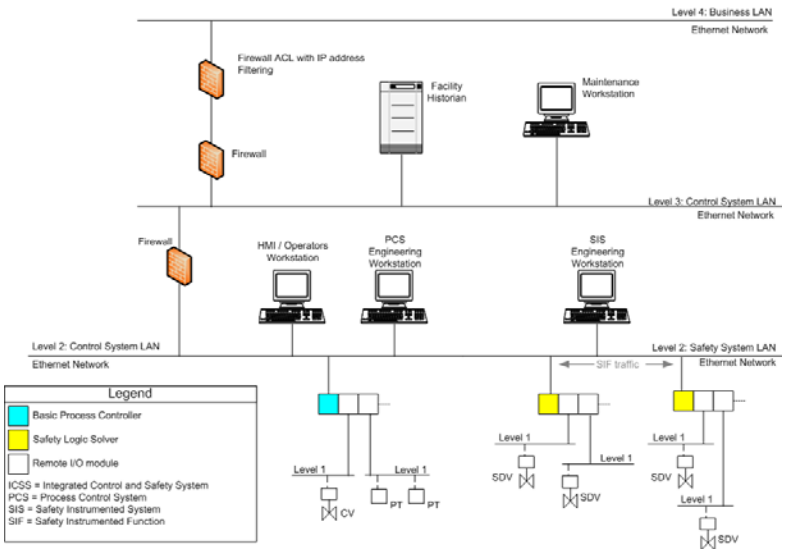
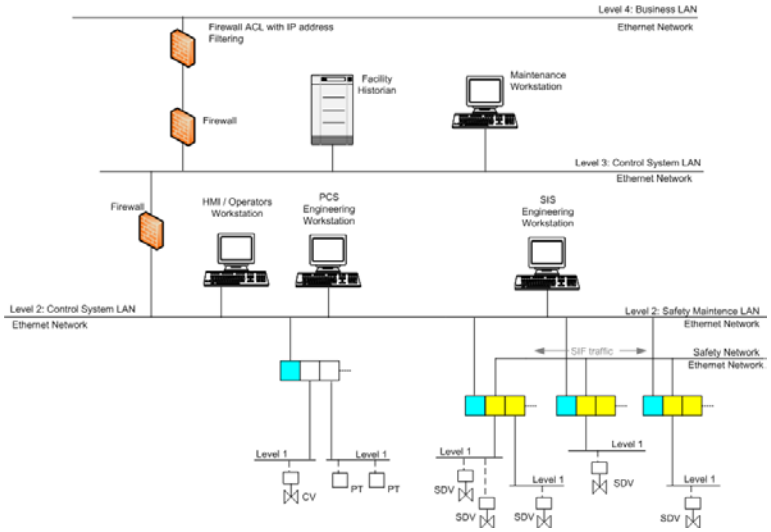


Figure 1 Integrated Control and SIS, Architecture A

integration provides many benefits to the end user, such as simplified wiring, ease of communication configuration, and lower hardware costs, it is also the most vulnerable of the three architectures evaluated.

In an Architecture A-type system, the SIS EWS was susceptible to denial-of-service (DoS) attacks caused by network floods or other malicious network traffic on the control system LAN. Loss of the SIS EWS, as caused by a DoS attack, could result in a dangerous condition if, for example, a value was forced or overridden prior to the loss of service. Without the SIS EWS, it may be impossible to remove the forced or overridden value. In this architecture, the SIS EWS is also susceptible to more sophisticated attacks, such as manipulation of system logs and offline configuration files. Since the SIS

EWS resides on an open LAN with several additional personal computers (PCs), it is also more susceptible to malware in this configuration than in architectures where the SIS EWS resides on a private safety network. The SIS controllers also are exposed to additional threats in this configuration. It was demonstrated in testing that peer-to-peer communications between SIS controllers are



vulnerable to DoS attacks. If safety instrumented functions (SIFs) are configured using peer-to-peer communications, a DoS event can lead to a false trip of the SIF.

Architecture B, shown in Figure 2, 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 provides significant protection of safety-critical communications.

In the Architecture B-type system, vulnerabilities relate to the location of the SIS EWS. Connecting the SIS EWS to the control system LAN makes this architecture susceptible to the same attacks as Architecture A (e.g., DoS attacks, manipulation of system logs and offline configuration files, and malware). To a lesser extent, the SIS controllers also remain vulnerable in this architecture since they connect to the control system LAN through a network interface. The resiliency of the SIS controllers is highly dependent on the quality of the SIS network interface implementation.

Architecture C, shown in Figure 3, has the fewest inherent vulnerabilities. It is typical of systems that provide an interface between the control system and the SIS but are not tightly integrated, an arrangement most commonly found in legacy and safety-critical systems. In many cases, systems of

Figure 2 Integrated Control and SIS, Architecture B

Architecture C involve the integration of a control system and a SIS from different suppliers.

A major point of vulnerability in the Architecture C-type system is the interface between the control system and the SIS. These links are implemented by using various communication interfaces ranging from nonroutable serial protocols to proprietary TCP/IP-based protocols to open protocols such as Modbus TCP and OPC. The flexibility required of the SIS network interface to support these various protocols creates an opportunity for some potentially significant system vulnerabilities.

The overall theme of the findings suggests that there are significant opportunities for both the vendors and the asset owners to evaluate and improve the security functionality of the safety systems during development and prior to deployment. The effort and costs of measures required to counter many of the observed vulnerabilities would not be significant, and a cooperative partnership between the vendor and asset owner communities would result in successful remediation.

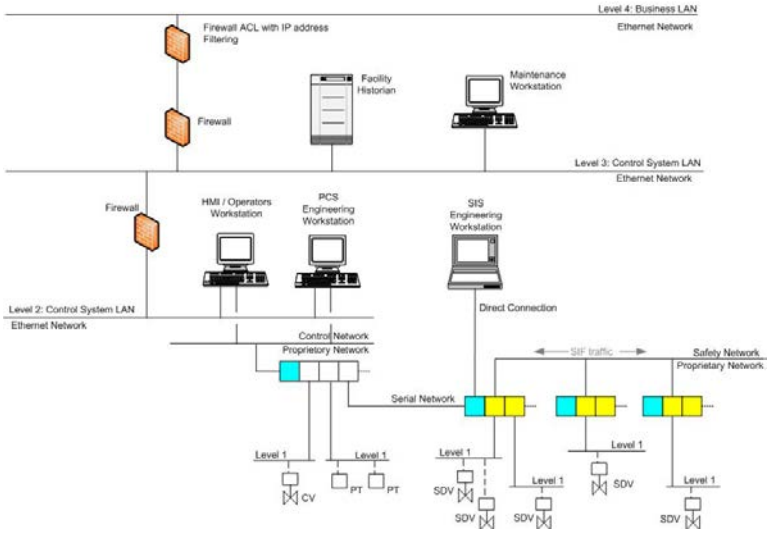


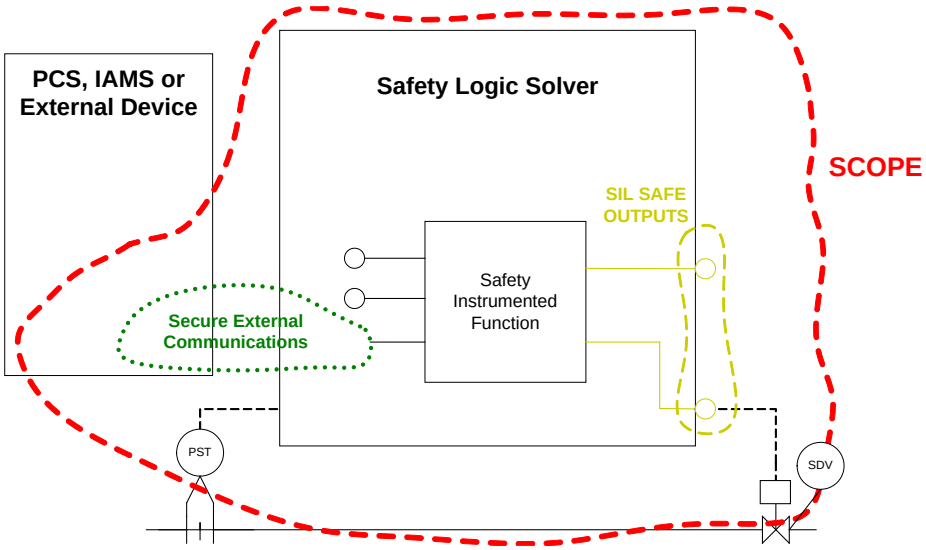
Figure 3 Integrated Control and SIS, Architecture C

Project Scope

The project scope was limited to SIS environments and components that are typically found within the oil and gas industry. To the extent possible, the scope was extended to include larger systems of basic process control elements that complement SISs as related to performing control and safety operations, and to allow the findings to be extrapolated (where applicable) to other industrial control system environments used in other sectors.

The project was designed specifically to focus on using known and common vulnerability testing and detection techniques for common ICS and IT vulnerabilities, and was extended to include additional test cases specific to industrial automation and SIS. Findings and observations were defined in the appropriate context of existing safety certifications. Figure 4 provides a graphical overview of the scope of the project. By limiting the analysis specifically to safety operations, significant complexity was avoided. By maintaining a focus on safety operations, the study included specific analysis of the impact of exploiting these vulnerabilities on the safety system, as opposed to peripheral analysis of the supporting technology that might be present in the solution architecture. The scope was developed specifically to determine plausible exploitable vulnerabilities that could impact safety operations, with supporting elements to include the impact on operator command and control.

Figure 4: SIS Project Scope



Project Methodology

The LOGIIC SIS project's approach to the comparison of different SIS integration architectures was to select commercially available vendor systems that were representative of the reference architectures defined in the FRD. The evaluation schedule, MOU, and monitor configurations were customized and reviewed with the vendors and SME teams. A template evaluation plan (EP) was tailored for each evaluation to reflect differences in the systems being evaluated approved by the vendor and the LOGIIC team. The tailoring of the EPs allowed for the flexibility required to develop and perform a robust set of applicable tests for each vendor system, and the use of a template ensured adherence to a baseline that provided a comparable set of qualitative results.

From the initially developed FRD, comprehensive evaluation frameworks were developed. These frameworks could then be augmented to accommodate the uniqueness of each type of architecture under evaluation, and could be reconstituted as evaluation plans. The inputs to these EPs were proven threat models, as derived from experience and expertise of the subject matter experts involved in the assessment, combined with concise safety requirements specifications. The threat model included threats to be extrapolated for each vendor environment, using targets of evaluation for the assessment.

Since the focus of the project was the integrity of integrated safety and control systems, a series of safety requirements specifications were reviewed, and from that set of specifications a definitive list of test requirements was developed. For each test architecture, the list of safety requirements was assigned a level of criticality. Safety system assumptions then were made, and a comprehensive set of project-specific integrated functional requirements (IFRs) was developed.

Evaluation Plan Approach

The evaluation plan for each architecture evaluated in the project was derived from the framework created for the project. The elements of evaluation consisted of structured automated testing activities and unstructured systematic testing. Both approaches to testing the SIS systems were found to be advantageous in that they allowed for the flexibility required to meet the nuances and uniqueness of each system under evaluation. Like traditional assessment processes, the structured automated testing provided a landscape for the subject matter experts to create more specific and unstructured systematic test activities. This collaborative approach facilitated the discovery of specific vulnerabilities by using techniques and procedures attributed to an adversary that were most likely to fit the threat profile being used.

It is important to recognize that during the testing, ongoing parallel SIF verification was performed to ensure that any impact on the safety function would be identified. Subject matter experts ensured that the safety functions of the systems under evaluation were configured in compliance with all relevant vendor documentation and that the evaluation plans were not in conflict with the IEC 61508 requirements. Moreover, subject matter experts also ensured that the safety integrity level (SIL) certificate was not jeopardized. During the evaluation process, hardware and software safety monitors were deployed and assessed to determine the impact on the safety system during the vulnerability testing. (Note: To facilitate testing, in some cases systems in the BPCSs were not fully hardened or configured to exact recommendations.)

Test Methodologies

Testing included a variety of approaches that combined automated and tailored security assessment tactics. Testing elements were selected on the basis of plausibility and applicability and were tailored to meet the assessment goals, tuned to align with plausible threat scenarios. Using this approach ensured wide coverage of plausible attacks from a variety of points of presence in the target architecture.

Focusing on threats and vulnerabilities that would impact the safety system (and supporting information resources), the team created specific portfolios of test suites that include the following categories of attacks on communication robustness:

- ARP specific attacks (Grammar, Host Reply Storm, Cache Request Storms, Saturation, etc.)
- Ethernet specific attacks (Broadcast Storm, Fuzzer, Grammar, Multicast Storm, Unicast Storm, etc.)
- ICMP and IGMP specific attacks (Fuzzer, ICMP Storm, Type/Code Cross Product, V3 corruption)
- IP specific attacks (Invalid IP Options, Multicast Storm, Unicast Storm, Broadcast Storm, Fragmented Storm, Fuzzer, Grammar–Field Fuzzer, Grammar–Fragmentation, IP Grammar–Options Fields, IP, LLDP Grammar, LLDP Saturation, LLDP Storm, Ping of Death, etc.)
- TCP/UDP specific attacks (Fuzzer, Grammar, Scan Robustness, TCP/IP Grammar, TELNET DEFENSICS, UDP Broadcast Storm, UDP DEFENSICS, UDP Data Grammar, UDP Fuzzer, UDP Grammar, UDP Multicast Storm, UDP Scan Robustness, UDP Unicast Storm, etc.)

In addition to these tests, and to provide for a more comprehensive assessment, advanced vulnerability enumeration and scanning was performed. This was combined with tailored scripts to address the uniqueness of the target of evaluation, and the combination proved very effective in (a) confirming vulnerabilities uncovered by automated scanning and (b) providing a foundation to create and execute system-specific exploits. These combined elements included modified network sniffing, traffic replay, data injection, signal interrupt messaging, bit-flipping and integrity impact tests, payload injection attacks, resource starvation, cryptographic analysis, password cracking, privilege escalation, directory traversal, forced error manipulation, and other derivative tests to assess the security posture of the devices. It was through this test vector, combined with automated testing activities, that many of the more severe vulnerabilities were uncovered.

Findings and Recommendations

This section discusses findings in a general way and provides applicable mitigation strategies that could be of interest to asset owners and vendors alike.

The assessment effort showed that there are both vulnerabilities that are common across the technologies tested and vulnerabilities that are unique to certain architectures. Many of these observations were provided by automated testing designed to observe system impacts under network duress, complemented by tailored manual testing and confirmation of the observed vulnerabilities. Mitigation strategies for many of these vulnerabilities relate to the deployment of defense-in-depth strategies, proactive assurances against protocol-specific weaknesses, and traditional IT measures that can be ported into the safety domain. The vulnerabilities tend to be associated with basic networking protocols, and recommended countermeasures will also include networking security best practices.

All the architectures were observed to be impacted under certain types of testing that addressed communications availability. These vulnerabilities did not result in the failure of the safety system but rather introduced possible denial of service or denial of control from an operator perspective that could require system shutdown. These included aggressive storm traffic, malformed packet storming, unicast storms, and other traffic-related vulnerabilities that could be mitigated by using many of the same countermeasures recommended for architecture-specific vulnerabilities.

Architecture A

Architecture A is the most tightly integrated of the three reference architectures evaluated. Although this level of integration provides many benefits to the end user, such as simplified wiring, ease of communication configuration, and lower hardware costs, it is also the most vulnerable of the three architectures evaluated.

The SIS engineering workstation is susceptible to DoS attacks caused by network floods or other malicious network traffic on the control system LAN. Loss of the SIS EWS could result in a dangerous condition if, for example, a value was forced or overridden prior to the loss of service. Without the SIS EWS, it may be impossible to remove the forced or overridden value. In this architecture, the SIS EWS

is also susceptible to more sophisticated attacks, such as manipulation of system logs and offline configuration files. Finally, since the SIS EWS resides on an open LAN with several additional PCs, it is also more susceptible to malware in this configuration than in other architectures where the SIS EWS resides on a private safety network. The SIS controllers also are exposed to additional threats in this configuration. It was demonstrated in testing that peer-to-peer communications between SIS controllers are vulnerable to DoS attacks. If SIFs are configured using peer-to-peer communications, a DoS event can lead to a false trip of the SIF.

Vendors should offer a fixed-configuration ICS firewall (i.e., brand-labeled or vendor supported with preconfigured rules) to make it easier for end users to implement the recommended modifications shown in Figure 5. Firewalls typically allow traffic through certain ports to certain hosts, and less typically perform rate limiting, traffic shaping, etc. This recommendation complements the above-noted suggestion that vendors update their technology to handle higher rates of traffic properly.

Vendors should ensure that a separate network interface reserved on the safety controller is connected to a limited number of safety operator stations or EWSs. When the safety controller is connected to the larger BPCS network, invalid or malicious network traffic may result in a loss of communications. Having a separate, dedicated communications connection to the controller will allow communications and functional changes to be made even if the other communications interface is down. Vendors

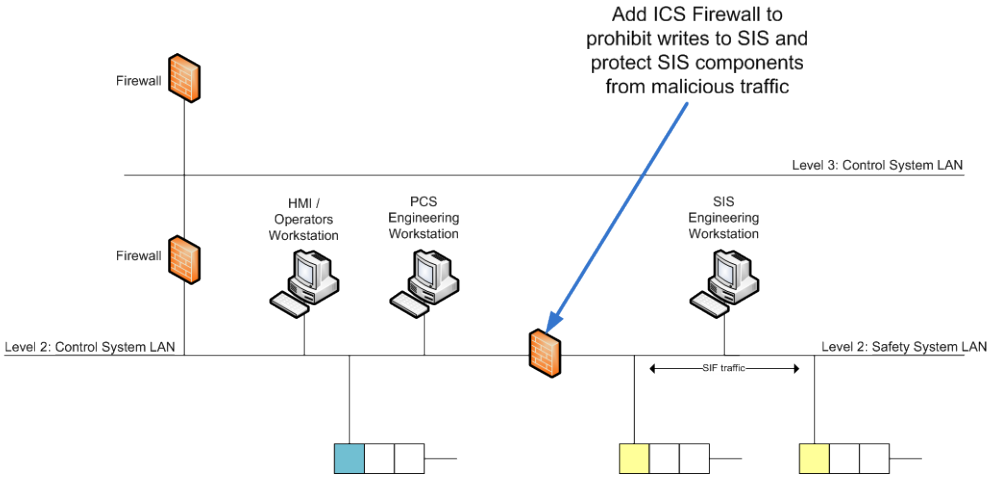


Figure 5: Recommended Modifications to Architecture A

should include the ability to limit which actions can be performed on the controllers running safety functions, depending on the network connection used to request the action. For example, if the controller running the safety function is connected to a secondary safety controller, BPCS network, and SIS network, then each network connection could have different restrictions. The BPCS network could be restricted to read-only actions, the SIS network could have only read and write access, and the secondary safety controller could have full safety failover functionality enabled (for example).

End users and system integrators can lessen the inherent vulnerability of this architecture, as shown in Figure 6, by inserting a properly configured (appropriately backed up or redundant) ICS firewall between the DCS and SIS components. As noted above, firewalls can allow traffic through certain ports to certain hosts and provide perimeter-like countermeasures to critical devices. Firewalls will

provide network isolation and protection for the SIS components while still allowing appropriate communications between the SIS and the DCS. Since this architecture is highly integrated, an effective solution would include the deployment of firewalls in front of all SIS components to limit access from the BPCS hosts. The firewall should, if possible, be configured to deny all writes from the DCS into the SIS. Rules should be configured to allow real-time data from the SIS controllers to the HMI/operator workstation. Of course, for this configuration to be effective the BPCS EWS and the SIS EWS must be deployed on separate workstations.

Architecture B

A point of vulnerability in Architecture B is the location of the SIS engineering workstation. Connecting the SIS EWS onto the control system LAN makes this architecture susceptible to the same attacks as Architecture A (e.g., DoS attacks, manipulation of system logs and offline configuration files, and malware). To a lesser extent, the SIS controllers also remain vulnerable in this architecture since they connect to the control system LAN through a network interface. The resiliency of the SIS controllers is highly dependent on the quality of the SIS network interface implementation.

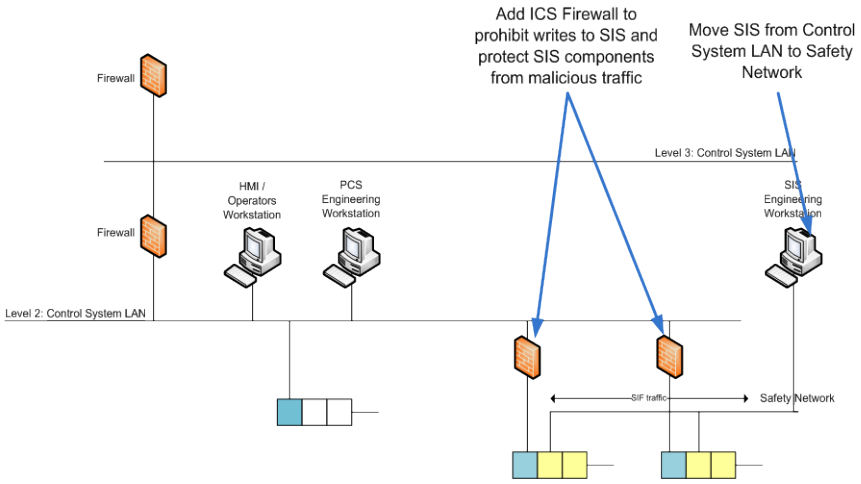


Figure 6: Recommended Modifications to Architecture B

We recommend that integrated control system and SIS suppliers develop a system security manual or guidebook that provides a third-party validated security assessment of the common variations of their system architectures. Such an assessment should incorporate an integrated threat analysis that communicates to the end user the threats that are addressed by the system and those that must be mitigated by the end user, as well as potential residual risks.

Furthermore, we recommend that suppliers of systems with architectures similar to Architecture B offer a fixed-configuration ICS firewall (i.e., brand-labeled with preconfigured rules) to make it easier for end users to implement the recommended modifications shown in Figure 6.

Although Architecture B provides improved separation of control and safety communications when compared with Architecture A, it is still recommended to protect the SIS controllers from the control system LAN. Therefore, we suggest installing ICS firewalls between the control system LAN and the

SIS controllers per the supplier's recommendations.

To protect the SIS EWS from DoS attacks and unauthorized access, one option is to move the SIS EWS from the control system LAN to a direct connection on the safety network. In this case, extra attention should be given to patch management and anti-virus updates.

Architecture C

The major vulnerability in Architecture C is the interface between the control system and the SIS. These links are implemented by using various communication interfaces ranging from nonroutable serial protocols to proprietary TCP/IP-based protocols to open protocols such as Modbus TCP and OPC. The flexibility required of the SIS network interface to support these various protocols creates an opportunity for some potentially significant system vulnerabilities. We recommend that standalone SIS suppliers develop a system security manual or guidebook that provides a third-party validated security assessment of common methods of interfacing their SIS to various control systems.

Furthermore, we recommend that suppliers of standalone SISs offer a fixed-configuration ICS firewall (i.e., brand-labeled with preconfigured rules) to make it easier for end users to implement the recommended modifications shown in Figure 7.

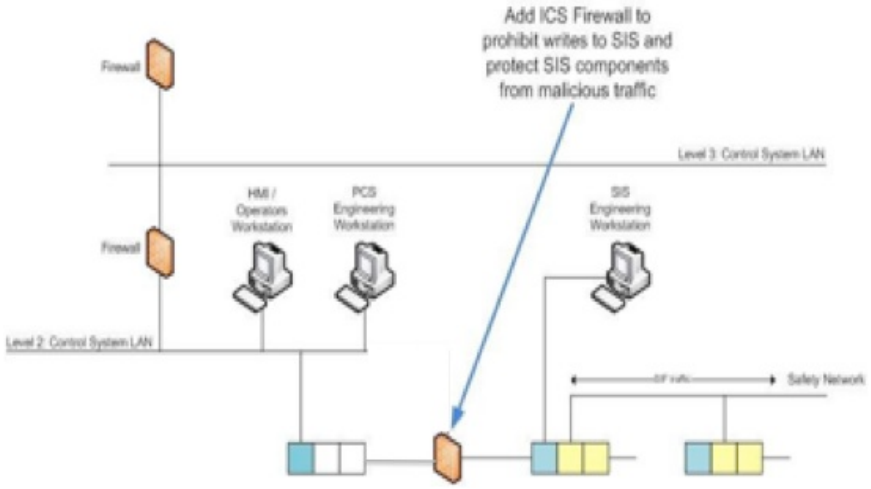


Figure 7: Recommended Modifications to Architecture C

The need to protect communication between the control system and the SIS, as well as the method of protection, depends on the type of communication interface deployed. Nonroutable serial protocols, such as Modbus, require little protection as long as the physical environment is secure (e.g., closed technical rooms, closed cabinets, USB ports disabled). However, TCP/IP communications, such as Modbus TCP and OPC, require additional protection. In these cases, we suggest installing ICS firewalls between the control system LAN and the SIS controllers that are able to provide deep-packet inspection of the industrial protocols used in the application.

Conclusions

The LOGIIC SIS project identified a set of vulnerabilities associated with standard types of contemporary safety systems. Fortunately, these vulnerabilities can be managed or avoided with updated architectures and compensating controls. The project demonstrated that contemporary safety systems have a significant amount of resiliency inherent in them. The project did, however, expose some vulnerabilities that could impact the availability of the mechanisms for operator interaction, as well as several notable vulnerabilities related to versions of hardware and software being used in standard deployments. Loss of control, loss of view, and false safety trips could negatively impact business financials (income), the environment, contractual obligations, and corporate reputation. Through our evaluation and analysis, this report has been able to identify effective countermeasure strategies to empower both vendors and asset owners in their cyber risk reduction efforts.

Greater Integration May Introduce Greater Risk

Many of the vulnerabilities discovered were attributed to the integration of system elements that were originally designed to operate in isolation. The evolving landscape of asset owner business requirements demands richer integration, and the vendor community is responding to meet those integration needs. Current vendor strategies still appear to indicate that total isolation is preferable, but when integration is required, the vendors do provide recommended best practices to deploy these systems in a secure manner. These vendor recommendations should be followed to the greatest extent possible. The assessment project provided significant insight into the vulnerabilities of the underlying operating systems and support technologies used to facilitate integration. It should be noted, however, that many of the vulnerabilities could not be exploited in a situation where the safety communications element is completely isolated and the adversary does not have specific and direct access to the command-and-control channels.

Default Configurations Are Not Secure

The testing conducted showed that vulnerabilities exist in areas of default configuration, authentication and authorization, unnecessary default services, unencrypted communications, and factors related to denial of service. Although all the systems evaluated demonstrated some vulnerability in their architectural elements, no system was compromised to the point that the SIS was in jeopardy and the safety function failed completely. However, other vulnerabilities identified in this report resulted in compromise of system availability, compromise of the integrity of operational view, and attack vectors that could facilitate an adversary's escalating privilege within critical equipment. In several cases, inherent system vulnerabilities were observed that have been known in the public domain for some time, and the recognition of these existing vulnerabilities showcases the need for vendors to perform more aggressive predeployment testing and more rigorous security lifecycle development.

Defense in Depth Reduces Risk

Implementations of defense-in-depth strategies used in the different architectures showed that minimal modifications to the control and safety system architectures could greatly increase the work effort of an adversary, thus theoretically reducing the cybersecurity risk to the system.

Examples include having the option of employing a discrete input of a foreign key switch to prevent unauthorized configuration changes, and using encryption, strong multifactor authentication, and authorization mechanisms to control access to configuration files.

Clear Guidance is Needed

We highly recommend that integrated control system and SIS suppliers develop a system security manual or guidebook that provides a third-party validated security assessment of the common variations of their system architectures. Such an assessment should incorporate an integrated threat analysis that communicates to the end user the threats that are addressed by the system and those that must be mitigated by the end user, as well as potential residual risks. The system security manual or guidebook provided by the vendor should note the threats and risks that may be encountered when using each configuration option.

Both the vendor and asset owner communities share the responsibility of advancing cybersecurity for the safety systems that are so important to industrial automation environments. Asset owners have a demonstrated interest in cybersecurity and, perhaps more importantly, the vendor community, represented by those vendors participating in the project, has the capability to develop secure systems. The focal points of the observed vulnerabilities are related to the isolation of the safety management systems and the ways that integration across architecture domains can introduce previously unseen vulnerabilities. The project showed that there is a requirement for ongoing research in the areas of cybersecurity for SISs, since today's more highly integrated systems require much more aggressive and comprehensive testing than was needed for the traditional deployment strategies of using complete and total isolation of the safety and control networks. Since future systems are clearly aligning with practices demanding integration across network enclaves, the project has demonstrated that contemporary IT cybersecurity best practices need to be evaluated with respect to their applicability in the safety domain.

The project also illustrated that safety systems in many cases can be quite fragile, and that aggressive and comprehensive cybersecurity testing demonstrates the impact on system availability when exposed to heavy duress. (In contrast to BPCSs, similar tests and traffic volumes might have little or no effect on a typical business IT system.) Notwithstanding that the majority of deployed systems may never be exposed to the magnitude of traffic and data streams our evaluations used to determine vulnerabilities, the analysis can clearly be leveraged by both the vendor and asset owner communities to investigate future requirements for ensuring that integrated safety systems are more resilient than they are currently. Practices associated with security lifecycle testing, vulnerability bench testing, and the development of tailored security test suites will be highly effective in advancing the development and deployment of more secure and resilient integrated safety instrumented systems.

Asset owners and operators are encouraged, whenever possible, to interact with vendors to enhance an overall understanding of the security of their system architectures. The recommendations in this report have been developed to help improve the cybersecurity of safety and control systems, and to support any follow-on activities that involve working with vendors to (a) explore activities that can improve the cybersecurity of the systems or (b) obtain vendor perspectives on the security best practices developed for the deployment of their safety systems in a production environment.