SRI International

Cyber Security Implications of SIS Integration with Control Networks:

The LOGIIC SIS Project

SRI: Zach Tudor

Date: 2011-10-26

© 2011 SRI International – SRI Proprietary Information

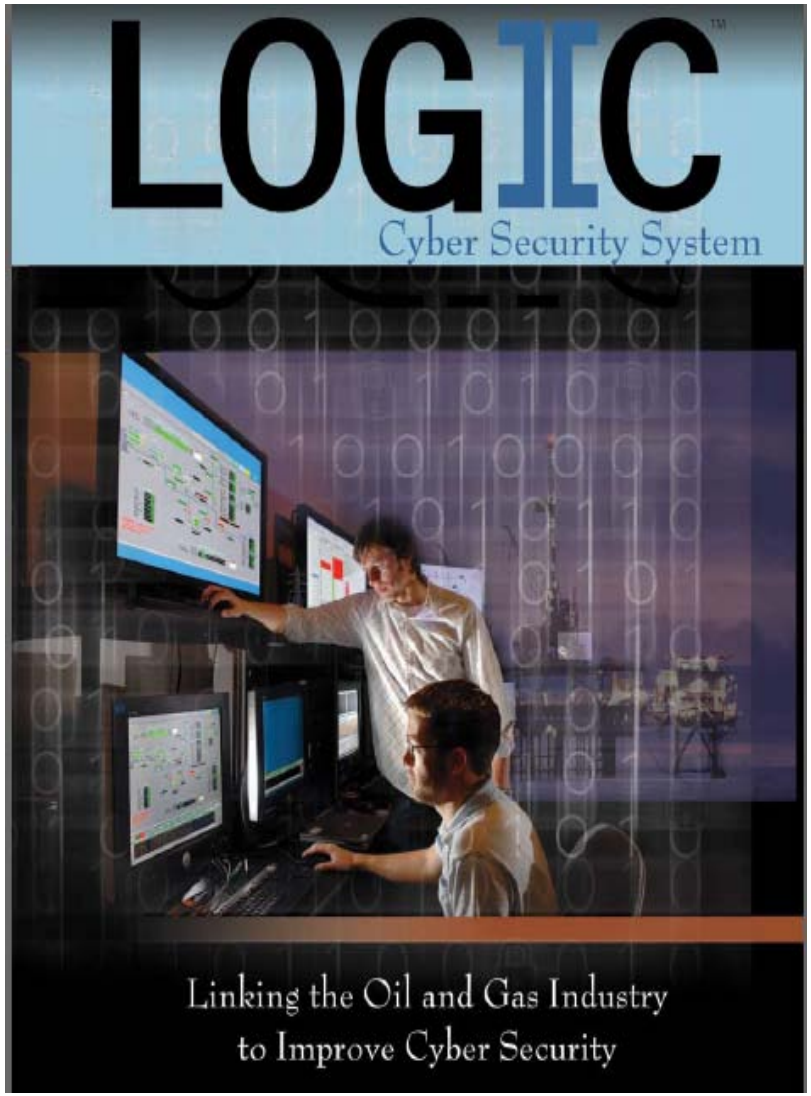
Presenter

- **Zach Tudor** is a Program Director in the Computer Science Laboratory at SRI International. He is a management and technical resource for operational and research and development cyber security programs including the DHS Cyber Security Research and Development Center (CSRDC). For CSRDC he provides technical support, subject matter expertise, and project management for projects including, Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) consortium, and the Industrial Control System Joint Working Group (ICSJWG) R&D working group. Prior to his work at SRI, he led a team of cyber security engineers and analysts directly supporting the Control Systems Security Program (CSSP) at DHS.

© 2011 SRI International – SRI Proprietary Information

Presentation Outline

- About LOGIIC
- SIS Project Background and Goals
- Project Scope and Methodology
- Reference Architectures
- Findings and Recommendations
- Next Steps



© 2011 SRI International – SRI Proprietary Information

The LOGIIC Model of Government & Industry Partnership

- Linking the
- Oil and
- Gas
- Industry to
- Improve
- Cyber Security

- LOGIIC is an ongoing collaboration of oil and natural gas companies and the U.S. Department of Homeland Security, Science and Technology Directorate.
- LOGIIC facilitates cooperative research, development, testing, and evaluation procedures to improve cybersecurity in petroleum industry digital control systems.
- LOGIIC undertakes collaborative research and development projects to improve the level of cybersecurity
- LOGIIC promotes the interests of the sector while maintaining impartiality, the independence of the participants, and vendor neutrality

© 2011 SRI International – SRI Proprietary Information

LOGIIC Broke New Ground in Consortium Governance for Collaborative R&D

- The Automation Federation (AF) serves as the LOGIIC host organization
  - Members approved a participation agreement with AF
  - Each project is covered by a Project Addendum to this agreement
- Member companies contribute financially and technically, provide personnel who meet regularly to define projects of common interest, and provide staff to serve on the LOGIIC Executive Committee.
- Current members of LOGIIC include BP, Chevron, Shell, Total, and other large oil and gas companies that operate significant global energy infrastructure.
- The U.S. Department of Homeland Security, Science and Technology Directorate has contracted with the scientific research organization SRI International to provide scientific and technical guidance as well as project management for LOGIIC.

© 2011 SRI International – SRI Proprietary Information

LOGIIC Model Adds Major Value to the Oil & Gas Industry

- Industry gains access to Government-funded experts and labs they would otherwise not have easy access to.
- Participant commitment is key. This kind of partnership is not a spectator sport – the first LOGIIC project was a success because time and resources were invested and people were committed to doing great work.
- The LOGIIC Correlation Project resulted in a real and validated solution, not just a paper product.
  - Chevron Pipeline deployed the solution with some of these benefits:
    - Monitor events in real-time instead of weekly
    - Reduce investigation time for events by at least 85%
    - Provide forensic evidence
  - Many vendors are now developing their products; some are already available in the market.

© 2011 SRI International – SRI Proprietary Information

LOGIIC Project SIS (Background)
Security of Safety Instrumented Systems

- SIS objective: bring a process plant to a safe state when an excursion outside pre-established operating parameters occurs
- SIS increasingly integrate with process control systems
  - Traditional physical separation between control and safeguarding has been reduced through integration of certain systems components of control systems and safeguarding systems
- Research Question: Is the technical integrity of our production facilities jeopardized because of Cybersecurity issues under SIS/BPCS integration? Challenges include:
  - Prevent false trips of SIS caused by corrupted SIS configuration or false signals to SIS
  - Ensure SIS activates when required
  - Prevent operator loss of view

© 2011 SRI International – SRI Proprietary Information

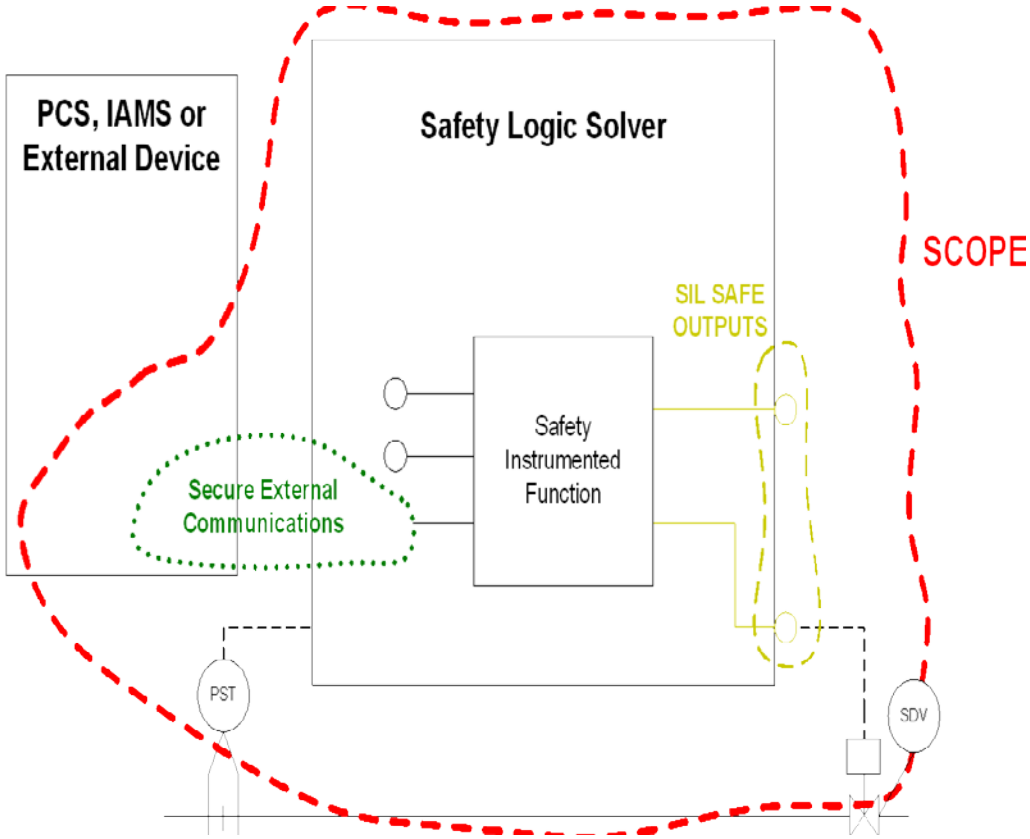
LOGIIC Project SIS Goals and Deliverables

- 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.
- LOGIIC SIS will result in
  - Security improvements
  - Characterization of residual risk
  - Architectural recommendations
  - Confidence in the architectural integrity of SIS
- Status
  - Evaluations completed summer-autumn 2010
  - LOGIIC-proprietary, vendor-specific report prepared for each evaluation
  - Final summary report provides architectural recommendations for BPCS/SIS integration
  - Outreach to standards bodies and the sector is underway.

© 2011 SRI International – SRI Proprietary Information

SIS Project Scope

- The project scope was limited to SIS environments and components that are typically found within the oil and gas industry.
- The BPCS was assumed to have been compromised, and was the entry point for the evaluations.



© 2011 SRI International – SRI Proprietary Information

Project Methodology

- Develop a functional requirements document (FRD) and the identify three reference architectures reflecting common strategies for integrating control and safety.
- Contract with leading subject matter experts (SMEs) who assisted the LOGIIC team in refining the FRD, developing the evaluation methodology and conducted the evaluations.
  - SME companies were LoftyPerch, Wurldtech, Exida, Kenexis
- Selected three representative systems from leading automation vendors who provided systems representing one of the reference architectures for evaluation.

© 2011 SRI International – SRI Proprietary Information

Project Methodology (cont)

- Select commercially available vendor systems that were representative of the reference architectures defined in the FRD.
- 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 evaluation schedule, MOU, and monitor configurations were customized for each evaluation and reviewed with the vendors and SME teams.

© 2011 SRI International – SRI Proprietary Information

Evaluation Methodology

- Testing included a variety of approaches that combined automated and tailored security assessment tactics.
- Focus was on threats and vulnerabilities that would impact the safety system
- 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
  - TCP/UDP specific attacks

© 2011 SRI International – SRI Proprietary Information

Evaluation Methodology (cont)

- Advanced vulnerability enumeration and scanning was performed with tailored scripts to address the uniqueness of the target of evaluation.
- Proved very effective in (a) confirming vulnerabilities uncovered by automated scanning and (b) providing a foundation to create and execute system-specific exploits.
- Methods 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, . . .

© 2011 SRI International – SRI Proprietary Information

Reference Architectures

- Architecture A represents the highest level of integration between the BPCS and SIS
  - The BPCS and SIS controllers, engineering workstations (EWSs), and human-machine interface (HMI)/operator workstations (OWSs) all reside on a common LAN.
- Architecture B type systems have a “moderate” level of integration between the BPCS and SIS
  - Similar to Architecture A except that it provides an isolated safety-critical network for peer-to-peer communications between SIS controllers.
- Architecture C represents systems that have traditional isolation between the BPCS and SIS
  - Typical of systems that provide an interface between the control system and the SIS but are not tightly integrated.

© 2011 SRI International – SRI Proprietary Information

Reference Architecture A

Architecture A is typical of systems that offer a high level of integration between the basic process control system (BPCS) and the safety instrumented system (SIS). In this architecture, the BPCS and SIS controllers, engineering workstations (EWSs), and HMI/operator workstations (OWSs) all reside on a common local area network (LAN).

Characteristics of Architecture A:

- In some cases, the SIS EWS on the process control network (PCN) and the BPCS EWS may reside on the same physical workstation, but with role separation.
- Engineering tools may be integrated into the BPCS database / HMI so that configuration of the logic solver populates the BPCS database / HMI automatically.

© 2011 SRI International – SRI Proprietary Information

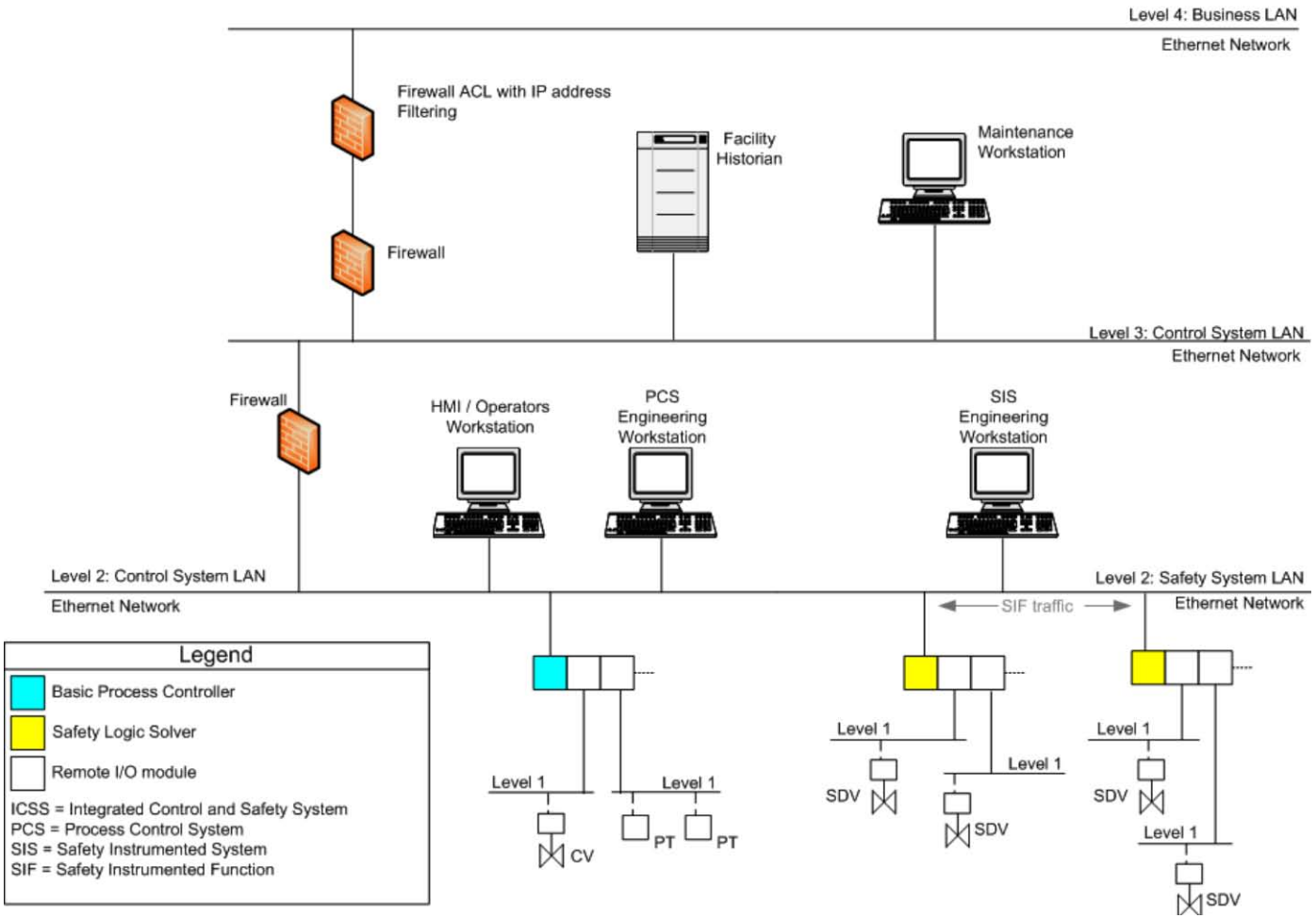
Reference Architecture A (cont.)

Characteristics of Architecture A:

- Interface to BPCS HMI is via direct peer connection on the PCN, but may be proprietary protocol or open protocol (Modbus TCP).
- Field devices are using analog/discrete signals for safety instrumented functions (SIFs), but are starting to use digital bus technologies for diagnostics and configuration where the digital signal is superimposed onto the analog signal. These smart field devices are in turn connected to instrument asset management systems (servers on the PCN). Partial stroke test (PST) for final shutdown elements may be initiated from BPCS and record data on PST results.

© 2011 SRI International – SRI Proprietary Information

Architecture A



Integrated Control and SIS, Architecture A

© 2011 SRI International – SRI Proprietary Information

Reference Architecture B

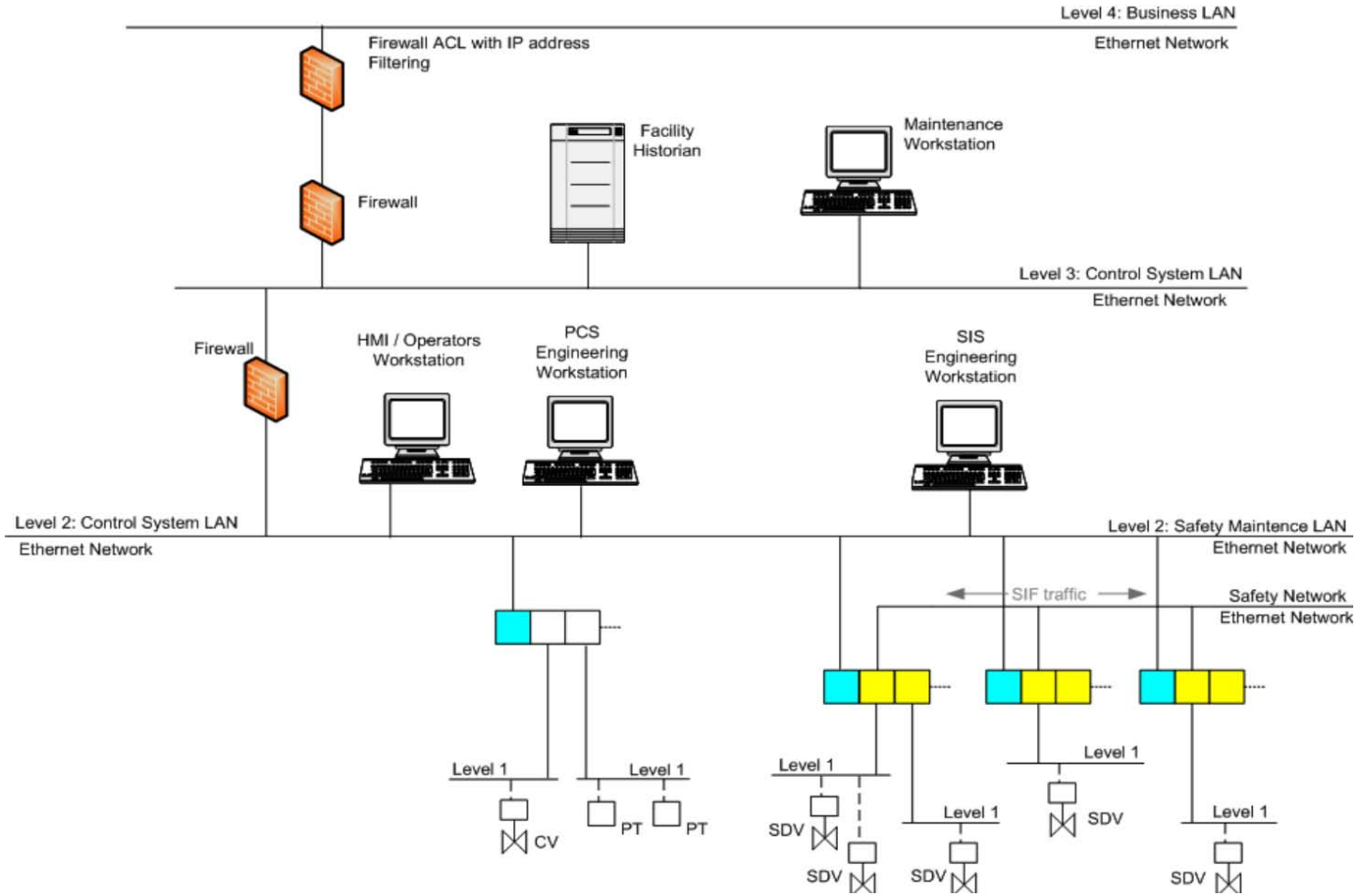
Architecture B is similar to Architecture A, except that it provides an isolated safety-critical network for peer-to-peer communications between SIS controllers. This architectural modification provides significant protection of safety-critical communications.

Characteristics of Architecture B:

- Engineering tools may be accessible on the PCN tied to a proprietary protocol.
- Interface to BPCS HMI is via gateway accessible to the PCN, such as terminal server or OPC server on PCN, or direct connected such as Modbus TCP interface.
- Field devices use primarily analog and discrete signals.

© 2011 SRI International – SRI Proprietary Information

Architecture B



Integrated Control and SIS, Architecture B

© 2011 SRI International – SRI Proprietary Information

Reference Architecture C

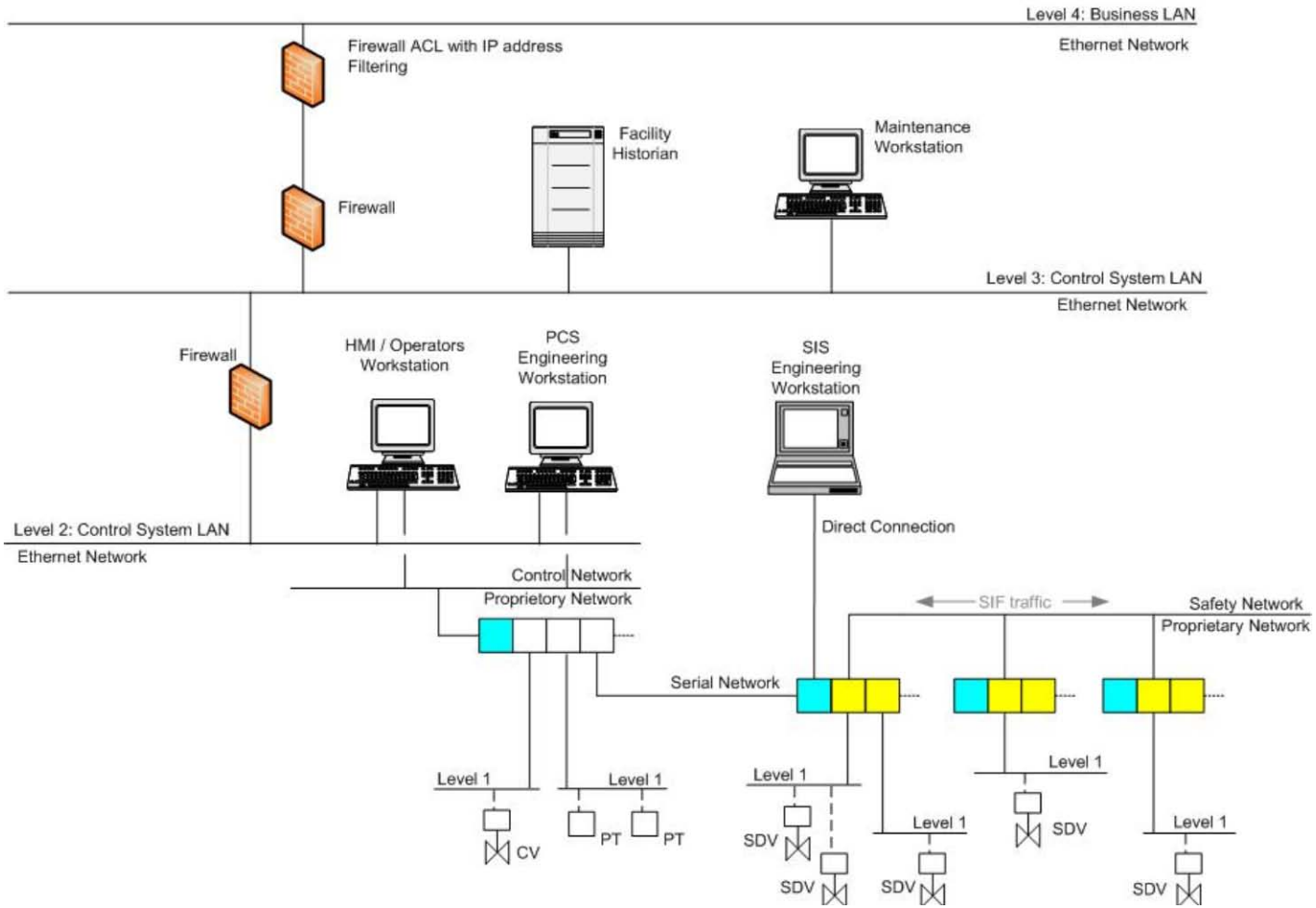
Architecture C is typical of systems that provide an interface between the control system and the SIS but are not tightly integrated. In fact, systems of Architecture C often involve the integration of a control system and a SIS from different suppliers.

Characteristics of Architecture C:

- Engineering tools are directly connected to serial or other communications port on the SIS.
- Interface to BPCS HMI is via proprietary gateway or nonroutable serial connection to the PCN.
- Field devices use primarily analog and discrete signals.

© 2011 SRI International – SRI Proprietary Information

Architecture C



Integrated Control and SIS, Architecture C

© 2011 SRI International – SRI Proprietary Information

Findings and Recommendations

- **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 that could have important business consequences.
- General Findings
  - Greater Integration May Introduce Greater Risk
  - Default Configurations Are Not Secure
  - Defense in Depth Reduces Risk
  - Clear Guidance is Needed
- Architecture Specific Findings
- Specific Architectural Recommendations

© 2011 SRI International – SRI Proprietary Information

General Finding:
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.
- Current vendor strategies still appear to indicate that 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 insight into the vulnerabilities of the underlying operating systems and support technologies used to facilitate integration.

© 2011 SRI International – SRI Proprietary Information

General Finding:
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..
- 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.

© 2011 SRI International – SRI Proprietary Information

General Finding: 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.

© 2011 SRI International – SRI Proprietary Information

General Finding: Clear Guidance is Needed

- Integrated control system and SIS suppliers should develop a system security manual or guidebook that provides a third-party validated security assessment of the common variations of their system architectures.
- The 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.

© 2011 SRI International – SRI Proprietary Information

Architecture Findings

- Architecture A
- Architecture B
- Architecture C

- The integrity of the safety function was never compromised

© 2011 SRI International – SRI Proprietary Information

Architecture A Findings

- The SIS EWS is susceptible to DoS attacks caused by network floods or other malicious network traffic on the control system LAN.
- 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 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.
- Testing showed 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.

© 2011 SRI International – SRI Proprietary Information

Architecture B Findings

- 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.

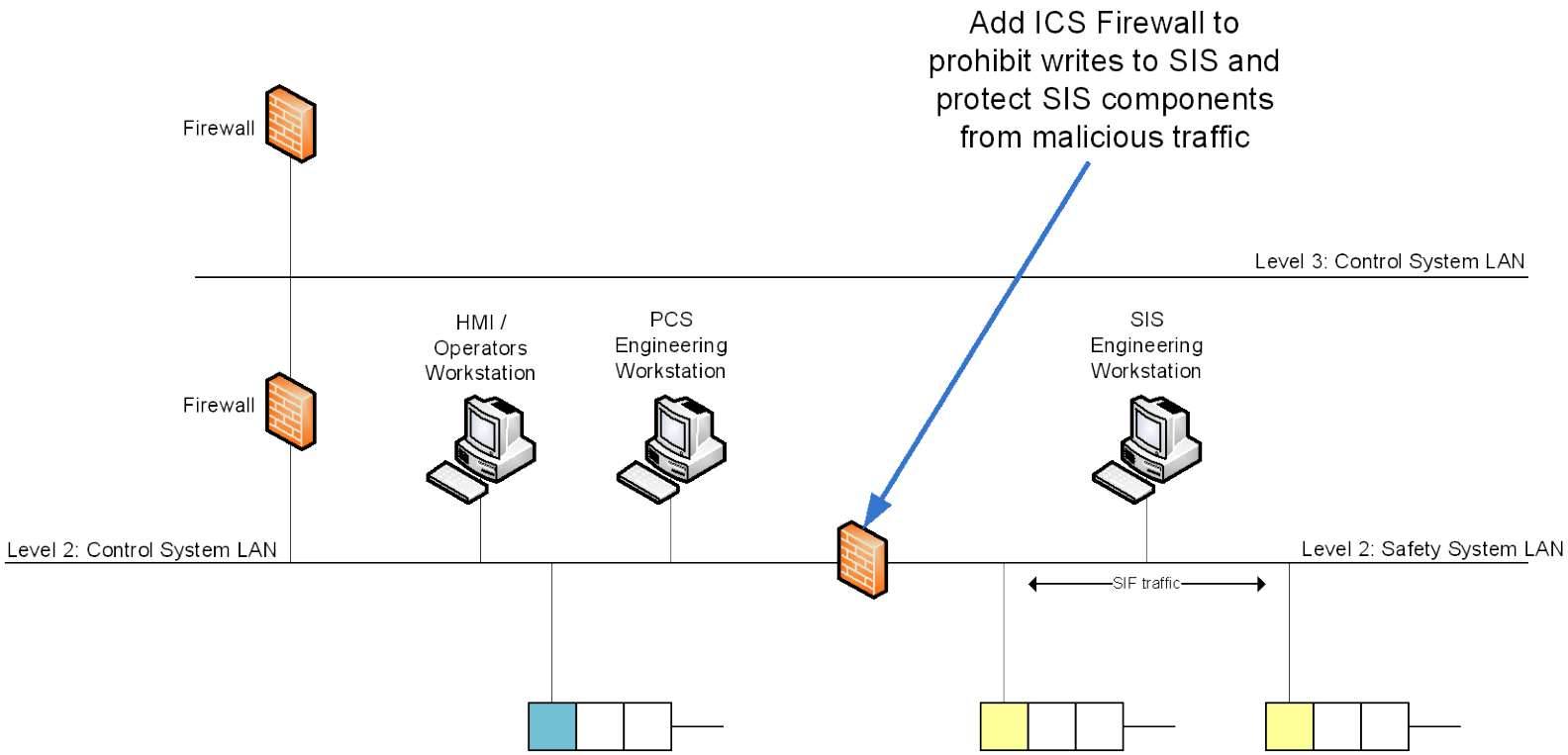
© 2011 SRI International – SRI Proprietary Information

Architecture C Findings

- The most inherently secure architecture
- 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.

© 2011 SRI International – SRI Proprietary Information

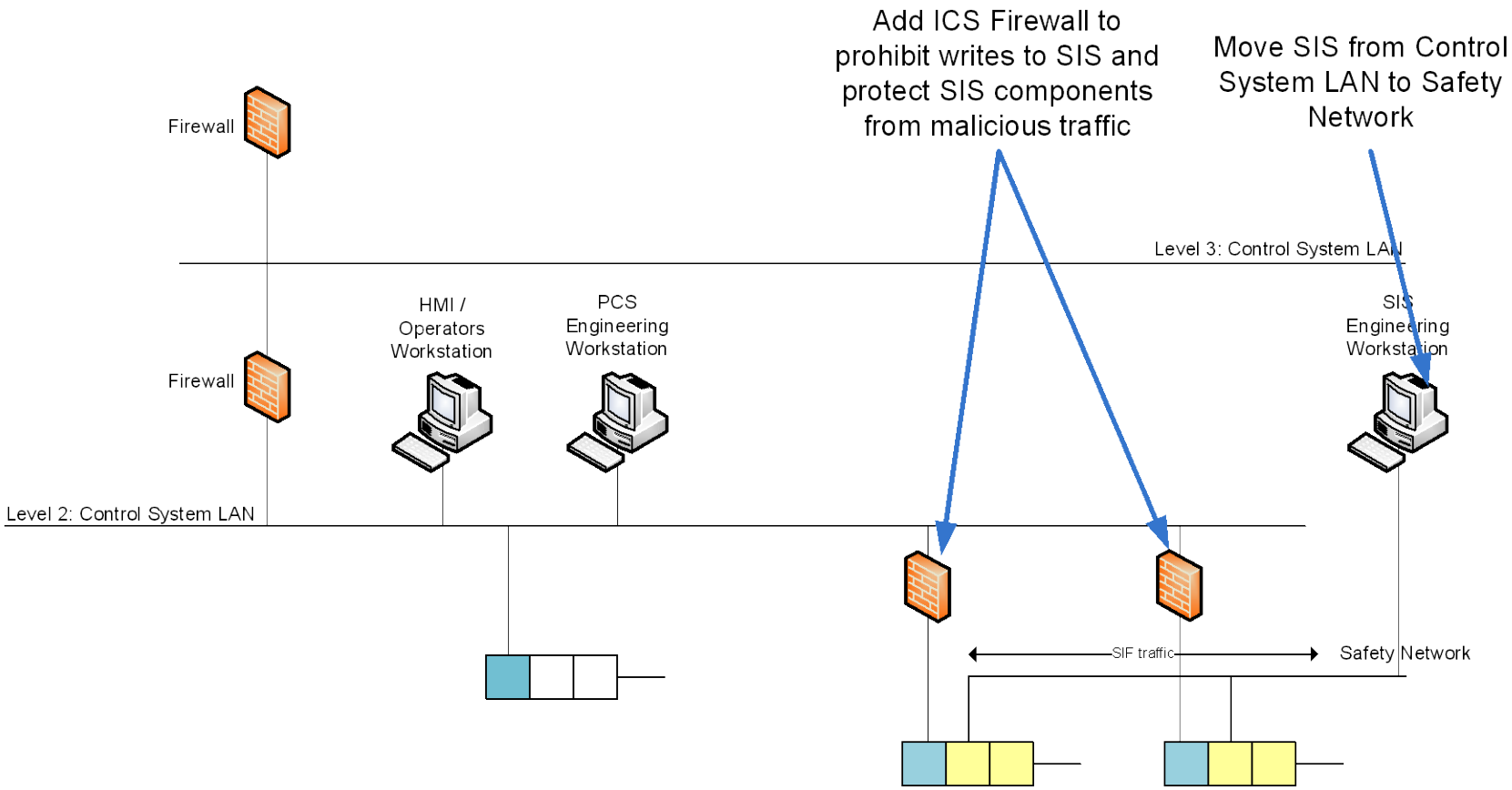
Architecture A Recommendation



Recommended Modifications to Reference Architecture A

© 2011 SRI International – SRI Proprietary Information

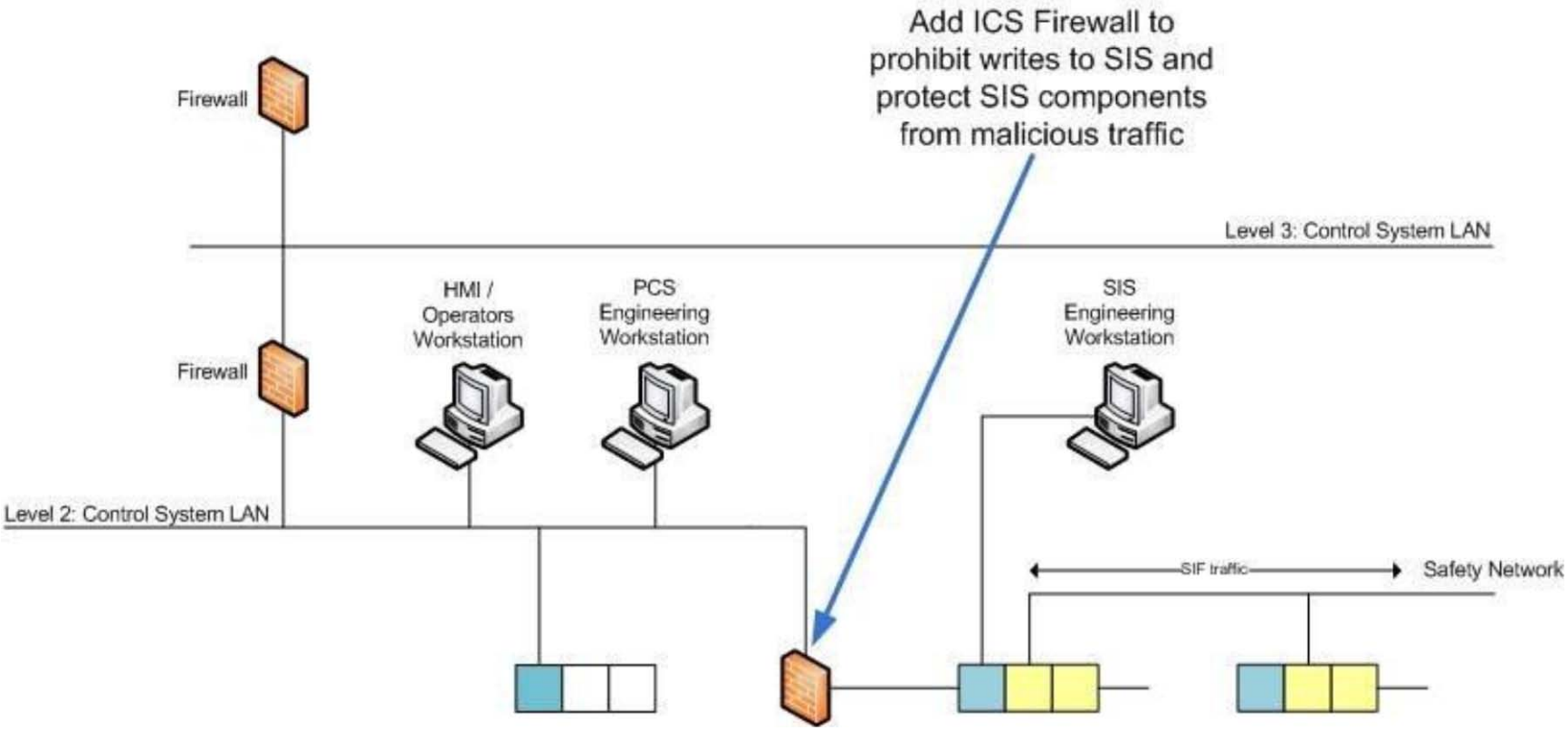
Architecture B Recommendation



Recommended Modifications to Reference Architecture B

© 2011 SRI International – SRI Proprietary Information

Architecture C Recommendation



Recommended Modification to Reference Architecture C

© 2011 SRI International – SRI Proprietary Information

Conclusions and Next Steps

- Lessons learned applied to the next rounds of LOGIIC project selections and performance
- Continue the dialog with vendors to mitigate general and specific findings
- Work with standards bodies to apply the processes and findings of the SIS project
  - ISA 99 timeline for SIS product inclusion in WG7 approved by LOGIIC EC
- Continue outreach
  - Automation Week 2011
  - ICSJWG
  - API Cybersecurity Workshop

© 2011 SRI International – SRI Proprietary Information