



Setting the Standard for Automation™

Cyber Security Implications of SIS Integration with Control Networks

The LOGIC SIS Project

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits



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.





Presentation Outline

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



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



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.



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.



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



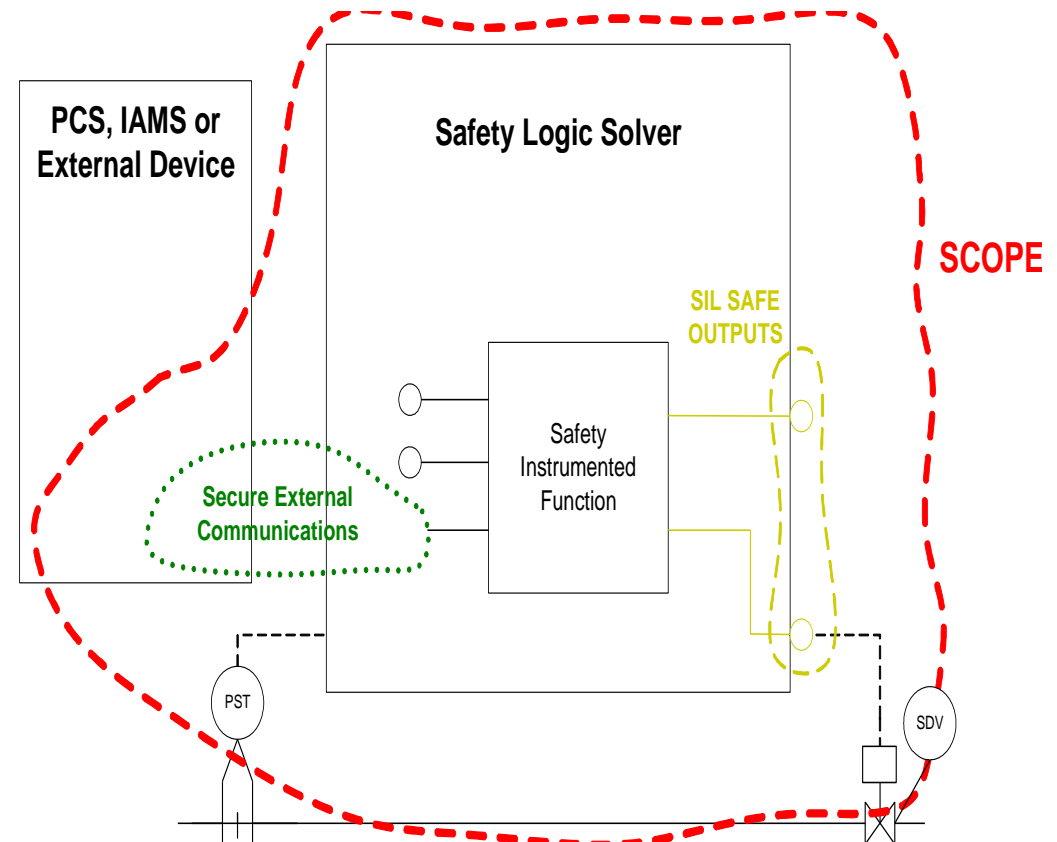
LOGIIC Project SIS

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.

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.





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.
- Selected three representative systems from leading automation vendors who provided systems representing one of the reference architectures for evaluation.



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.



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



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, . . .



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.



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.



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.

