LOGIIC™

Cyber Security System

Linking the Oil and Gas Industry
to Improve Cyber Security

Brief Product Description

The LOGIIC cyber security system monitors an industrial facility's entire information infrastructure by combining relevant control system data with other security data.

Product First Available

September 11, 2006

Developers

The LOGIIC system was developed through a unique public and private partnership that included experts in homeland security, oil and gas, security research, security technology, and process control technology from the following organizations:

- Government: DHS Science and Technology Directorate
- Oil and gas industry: Chevron, CITGO, BP and Ergon Refining
- Research: Adventium Labs, Sandia, and SRI International
- Security vendors: ArcSight, 3Com, and Symantec
- Process control technology vendors: Honeywell, OMNI Flow Computers, and Telvent

Product Price

The LOGIIC system solution integrates a varying number of security components depending on the deployment architecture. As a rough estimate of total system cost, a base installation at a facility whose information infrastructure consists of three networks (one process control, one demilitarized zone, and one business) would typically require an enterprise security management system (we used ArcSight's), a gateway security appliance/firewall (we used Symantec's), an intrusion detection system for each network (we used Symantec's), and host-based firewalls for each essential control system platform (we used 3Com's embedded firewall). The combined cost of these components for this base system would be approximately $150,000.

Product's Primary Function

The LOGIIC solution addresses the oil and gas industry's concern that their process control system (PCS) networks are not monitored for cyber intrusions as is routinely done on business networks, allowing potential cyber adversaries to compromise essential PCS components undetected. The oil and gas industry and other critical infrastructure operators face new cyber threats and vulnerabilities to their PCSs, which are used to manage refineries, pipelines, and other mission-critical operational facilities. New threats come from adversaries who may want to destabilize energy industry supply capabilities and the national economy. New vulnerabilities have been introduced with the migration to standard information technology (IT) components and networking technologies in the PCS environment, and the integration of business and PCS networks, exposing PCS to the full spectrum of cyber threats resident on the Internet. We developed the LOGIIC solution through a unique public-private partnership jointly funded by the U.S. Department of Homeland Security and industry.

As shown conceptually in Figure 1, the comprehensive monitoring system developed in LOGIIC provides an integrated, multi-component security solution that monitors a PCS for abnormal activity, and then combines and correlates this information with security event data from business networks to provide enterprise-level situational awareness over an operational facility's entire information infrastructure. The LOGIIC monitoring system embodies both a newly developed security architecture as well as the instantiation of this architecture using a suite of vendor-supplied and adapted security products, including host-based embedded firewalls, PCS protocol-aware intrusion detection systems, and an enterprise security management application that provides event aggregation and correlation services.

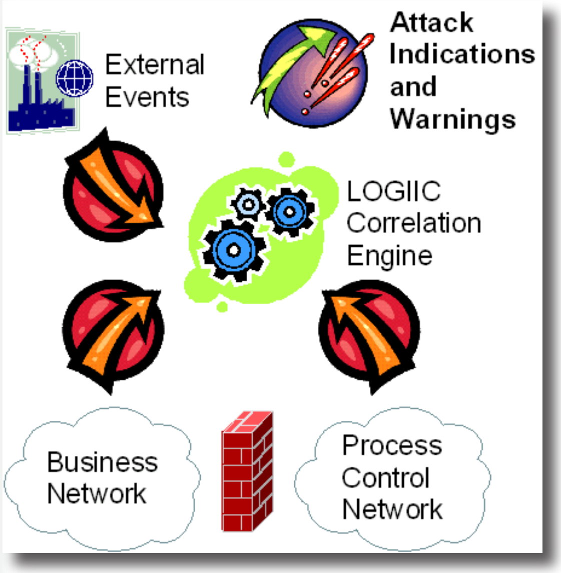

Figure 1: Conceptual View of LOGIIC Monitoring Solution

In developing the LOGIIC solution, our project team overcame a number of technical challenges, including:

- developing an idealized system architecture representing information infrastructures commonly deployed at refineries and pipeline control centers,

- identifying the set of vulnerabilities, or attack scenarios, that could be potentially exploited in this system architecture to provide an adversary with access to critical process control system components,
- understanding the abnormal events that an adversary's exploits can cause in a process control system,
- designing a defense-in-depth placement of security sensor technologies to detect and alarm on suspicious activity,
- adapting an enterprise security management (ESM) application (or correlation engine) to aggregate and correlate sensor events to detect intrusions,
- evaluating the system's performance in a test environment set up to mimic a realistic field environment.

We heavily leveraged the collective resources and expertise of our oil and gas, government, vendor, and research partners to develop this revolutionary situational awareness solution, which combines PCS and other security event data to detect, for the first time, a broad range of cyber intrusions. The LOGIIC solution was created through a unique public-private partnership, which drew upon the complementary skill sets and expertise bases of the partnership's stakeholders:

- Oil and gas asset owners drove the LOGIIC solution development by contributing their business and operational understanding of their facilities and security needs.
- Government worked with the project team to define and manage the LOGIIC partnership model and brought a national perspective on cyber security risks.
- Vendors provided the detailed understanding of the PCS and security components employed in the LOGIIC system.
- Researchers defined plausible threat models and led the design and implementation of the LOGIIC solution.

The synergy generated within the LOGIIC partnership developed a solution that no member of the team believes they could have achieved on their own, and offers hope for future successful public-private partnerships to conquer other homeland security challenges.

Additional background on the system environment and solution follows.

PCS and LOGIIC Test Environment Implementation Background

The LOGIIC system was developed to have broad applicability within the oil and gas as well as other PCS-dependent industries, and its defense-in-depth design was conceived from a very thorough characterization of threats, vulnerabilities, and potential consequences of PCS disruption. Figure 2 shows an idealization of a common information infrastructure existing at many companies using PCSs. Some aspects in this idealization reflect good security practices that are not always found at every company—the use of a demilitarized zone (DMZ) to separate the business network from the control network is one example. Cyber points of entry, or attack vectors, are shown in Figure 2 as "Bad Guy Starting Points" (BGSP). To ensure a comprehensive solution, the LOGIIC design is based upon a detailed examination of threat vectors and vulnerabilities using an adversarial modeling (or "red teaming") methodology to identify critical attack paths and disruption scenarios.

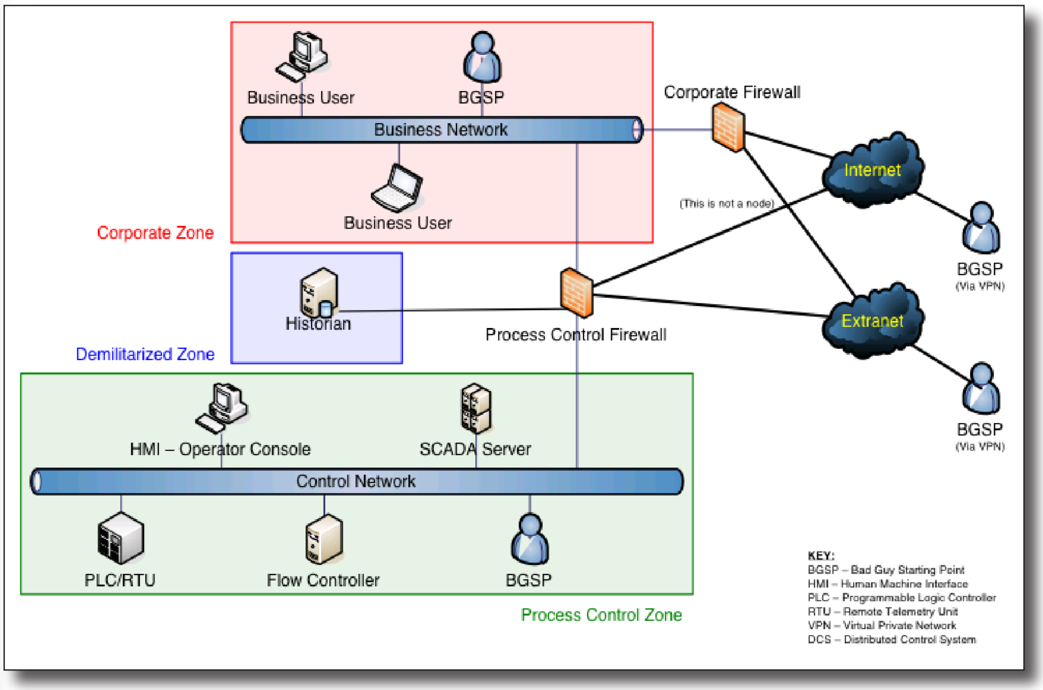

Figure 2: Idealized System Architecture

The LOGIIC solution was implemented and evaluated in the test environment shown in Figure 3, which was designed to closely mimic field conditions. The test environment includes both a supervisory control and data acquisition (SCADA) application typically used to manage pipelines as well as a distributed control system (DCS) application used to run refineries. These applications reside on process control networks (PCNs) with other PCS-specific equipment.

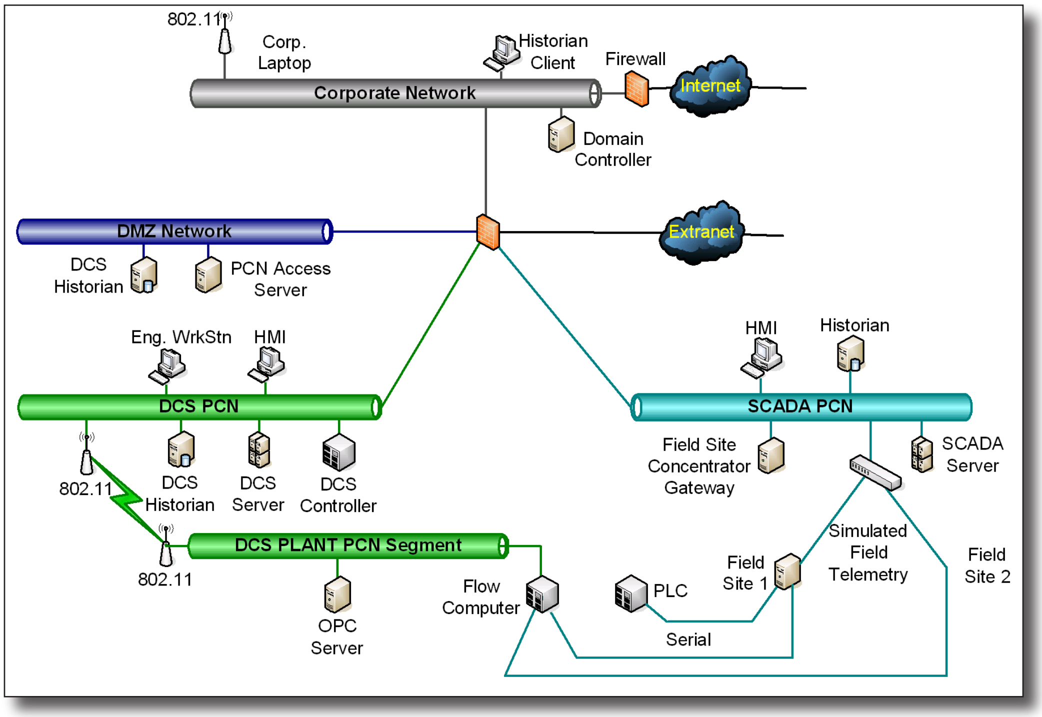

Figure 3: Test Bed Environment

How the LOGIIC Monitoring System Works

The LOGIIC system provides facility-level awareness of threats to process operations by sensing and correlating low-level events to produce prioritized security warnings. The LOGIIC design considers a full range of event sources that might be indicators of an attack or process disruption. These events range from human intelligence to security alarms to abnormal system state, which either on their own or in combination with other events might indicate a cyber or physical intrusion. The LOGIIC system is extensible to include many of these events, such as physical security alarms, but focused in its initial instantiation on events generated by standard IT defenses and control-system-specific sources. The standard IT defenses selected as event sources include:

- network segment firewalls (in reporting, not blocking modes),
- host firewalls (again, in reporting, not blocking modes),
- network intrusion detection systems (IDS),
- network devices (wired and wireless routers).

Three sources specific to control systems are included:

- PCS-protocol aware IDSs on the PCNs,
- alarms from the DCS and SCADA,
- alarms from flow computers.

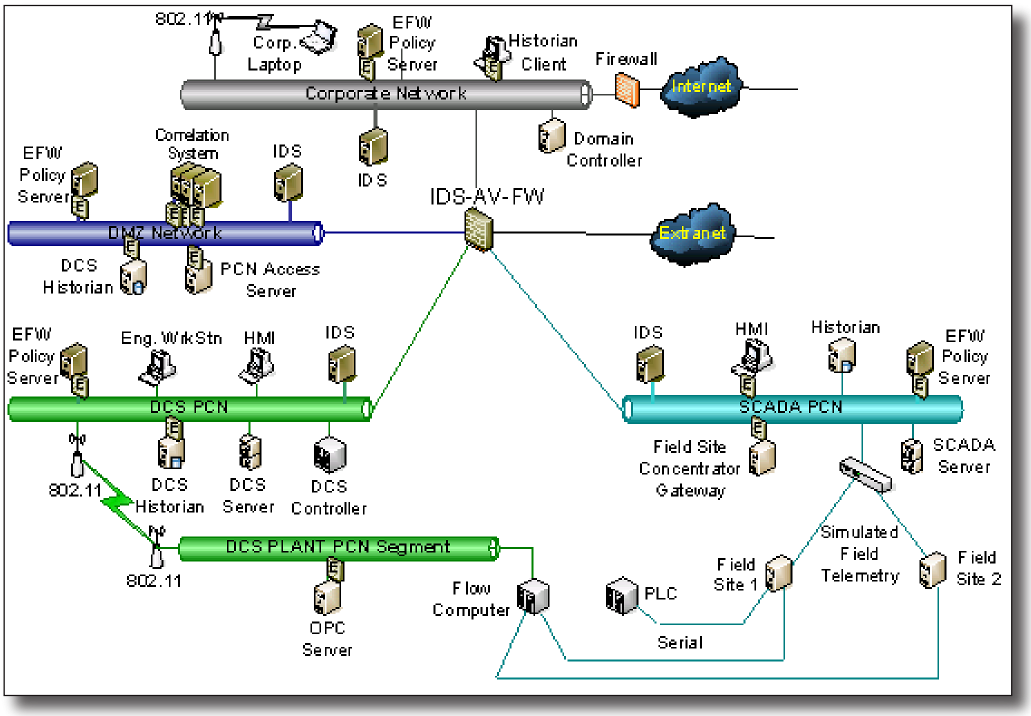

Figure 4: Final LOGIIC System Configuration with Security Sensors

The LOGIIC monitoring system, using a defense-in-depth philosophy, defends the control system in-depth across the full breadth of attacker paths. We selected a suite of sensors to implement this defense-in-depth strategy. These sensors are triggered by abnormal activity to produce security events that are aggregated and correlated by an ESM application. The LOGIIC monitoring system is shown in Figure 4 superimposed over the test bed environment architecture shown in Figure 3. The component sensors and their integration with an ESM is described briefly below.

Sensor Integration: An ESM integrates events from the various sensors, filters out the noise, and identifies patterns indicative of hostile activity. Event correlation rules developed within the ESM identify relationships between distinct security alerts and infer their significance. A key innovation in the LOGIIC monitoring system is the relating of security events in the IT network with events occurring in the PCN, allowing PCS operators to identify and counter threats to their facilities that would have previously gone unnoticed until potentially catastrophic process disruptions occurred.

We chose ArcSight as the ESM for this system because of its strong event correlation capabilities. ArcSight provides data collectors (or "connectors") for a large number of traditional security products, enterprise applications, and databases. We developed new custom connectors to integrate the PCN field devices included in the LOGIIC monitoring system. The following nine sensors compose the system:

1. OMNI SE v1.24 from OMNI Flow Computers—As part of LOGIIC's design strategy to include PCS data, the flow computers on the pipeline network are monitored for security-related events such as unsuccessful logins.
2. SNS 7120 from Symantec—This security appliance performs as an intrusion detection system (IDS) and can monitor both standard protocols like TCP, as well as proprietary protocols that are relevant to SCADA systems like Modbus.
3. SGS 5620 (v3) from Symantec—This multi-function appliance performs as a network firewall and gateway for the LOGIIC monitoring system.
4. PIX v6.3.3 Firewall from Cisco—This is an industry standard firewall product.
5. EFW from 3COM—This NIC-based firewall product fills a critical niche in the LOGIIC design between detecting malicious activity on the host using application-specific detectors or the host operating system itself, and detecting malicious traffic only passing between different network segments using the network IDS. In contrast, the EFW detects unauthorized network traffic between individual hosts, even hosts within the same network segment. It often provides multiple points of detection for improved correlation.
6. DCS from Honeywell—This distributed control system on the refining network is monitored for security-related events.
7. SCADA from Telvent—This SCADA system on the pipeline network is also monitored for security-related events.
8. Microsoft Windows Events—Microsoft Windows events are monitored because many PCS applications now run on this operating system.
9. Aironet 1200 from Cisco—In recognition of the proliferation of wireless networks in facilities, security events from this wireless access point are monitored.

Correlation Rule Development: We developed event correlation rules in the ArcSight ESM to fuse events from the sensors listed above. A unique feature of the LOGIIC monitoring system is its correlation of both standard IT and new PCS event data to provide situational awareness across an organization's PCN and business networks. We developed three sets of correlation rules to enable this awareness:

1. Rules that uniquely identify steps or vectors of the critical attack scenarios, such as traversal from one network segment to another.
2. Rules that enforce common PCN policies. Since the PCN is typically quite static compared to business networks, violations that can be alerted upon include rogue systems, configuration changes, and port scans.

3. Rules that implement a data dictionary for process-control-specific security events, mapping proprietary logged PCS events to standardized security events.

Monitoring Performance: We evaluated the LOGIIC monitoring system by executing a number of different cyber attacks that triggered various sensors and correlation rules. The system successfully detected attacks targeting PCS applications and the PCN networks—an industry first—and then successfully correlated this information with other security event data to provide prioritized, high-level alerts of these cyber intrusions—another industry first. Performance was notable in two areas:

- Detection of attacks on PCS. Relevant events were generated by IT types of sensors placed to detect events on the PCN, and events extracted from the control system applications. The correlation rules used events from both sources to create the attack pictures. The IT types of sensors provided events generated by their standard IT signature set, as well as events generated by a Modbus signature set to detect PCS-specific attacks. The control system applications were also able to provide unique control system alarm events for correlation.

- Reduction in workload for a hypothetical security analyst looking for attacks. This resulted from the filtering and reduction of the number of events the analyst would need to examine to understand the attacks. One of the attack scenarios used created over 7,000,000 low-level events from the system sensors, which were reduced to about 1,000 correlated events and then further prioritized to only 130 high-priority alerts.

Competitors

The only other product we are aware of that offers some of the functionality of the LOGIIC system is one recently introduced by Tenable, which provides a correlation framework for heterogeneous alarms in a PCN. The Tenable solution does not provide the enterprise-level view of the LOGIIC system (LOGIIC detects, correlates, and visualizes an attack as it penetrates various network perimeters), nor does it appear to incorporate and correlate process anomalies with intrusion detection.

Competitive Matrix

Most oil and gas companies today are using a limited number of point security solutions to increase their security posture. These include antivirus protections on hosts and external network gateways, intrusion detection or protection systems on corporate networks, and firewalls or other network partitioning between control and business networks. Unfortunately each of these solutions on its own only provides a partial picture and leaves companies exposed to cyber threat. Few of these solutions detect control-system-specific security events. The LOGIIC solution implements IT-type intrusion detection on control systems networks and uses events from the control system itself to detect attacks. The LOGIIC system demonstrates how all security-related events can be logged and analyzed in a central location and the true threat level accurately determined by correlating all security feeds with the relative asset value as well as attacker history. In this way a prioritized list of threats can be monitored through a "single pane of glass." A comparison of the LOGIIC system's capabilities to traditional IT security technologies is shown in Table 1.

	LOGIIC	AntiVirus	Intrusion Detection/ Protection Systems	Firewall/Network Partitioning
Control Network	Strong	Weak	Moderate	Moderate
Control System	Strong	Weak	Weak	Weak
Perimeter Threat	Strong	Strong	Strong	Strong
Zero Day Attacks	Strong	Weak	Weak	Moderate
Early Warning	Strong	Strong	Strong	Moderate
Insider Threat	Strong	Weak	Weak	Weak
Enterprise-wide, Correlated Alerts	Strong	Weak	Weak	Weak
Response Capabilities	Strong	Strong	Moderate	Weak
Network Protection	Strong	Weak	Strong	Strong
Desktop Protection	Moderate	Strong	Weak	Moderate
Server Protection	Moderate	Strong	Strong, if installed on the server	Moderate

Table 1: Comparison of monitoring capabilities

Improvement Over Competition

The LOGIIC monitoring system extends beyond the very latest commercial enterprise detection and correlation technologies by adapting these technologies to monitor PCS applications and networks—an industry first—and then combining and correlating this information with other security event data to alert facility operators to previously undetectable cyber intrusions and other abnormal activity—another industry first.

To the best of our knowledge, there are no comparable solutions available on the market today: the LOGIIC monitoring system transcends currently available security monitoring technologies by incorporating both PCS and business network events, providing infrastructure operators with a dramatic advancement in situational awareness of their information infrastructure.

Principal Applications

The principal application of this product is to monitor the information infrastructure of oil and gas facilities for cyber intrusions.

Other Applications

Although the partnership team developed this solution specifically for the system architectures and equipment generally found in the oil and gas industry at their refineries and pipelines, the solution is also applicable to other critical infrastructures, such as the electric power industry, which share similar control system threats and vulnerabilities.

Summary

The LOGIIC monitoring system addresses a pressing, unmet homeland security need, allowing industry for the first time to comprehensively monitor their mission-critical, process-intensive facilities like refineries for cyber intrusions, which if undetected, could otherwise result in process disruptions with serious safety, environmental, and economic impacts.

Moreover, with over 85 percent of the nation's critical infrastructure owned by the private sector, the industry-driven partnership model used in LOGIIC establishes a template for how government, asset owners, vendors, and the research community can work together to protect our critical infrastructure.

More Information

More information about the LOGIIC system is provided in the technical report, *Correlating Intrusion Events in Process Control and Business Networks in the Oil and Gas Industry,* which can be requested from:

Ben Cook
Sandia National Laboratories
Phone (505) 844-3795
Email bkcook@sandia.gov

Contact information for the various companies involved in the LOGIIC project can be found on the project website: **www.logiic.org**

For more information about the LOGIIC partnership program, please contact:

Douglas Maughan, Program Manager
U.S. Department of Homeland Security, Science and Technology Directorate
Phone (202) 254-6145
Email douglas.maughan@dhs.gov

or

Ulf Lindqvist
SRI International
Phone (650) 859-2351
Email ulf.lindqvist@sri.com

Glossary/Acronyms

DCS—distributed control system: DCS is a collection of computerized equipment used to monitor and control industrial processes like refineries.

DMZ—demilitarized zone: A DMZ is a computer network used to provide security isolation between two or more other networks.

ESM—enterprise security management: ESM applications are used to collect and analyze security data from heterogeneous devices.

IDS—intrusion detection systems: IDS are used to monitor computer networks for cyber intrusions.

IT—information technology

LOGIIC—Linking the Oil and Gas Industry to Improve Cyber Security

Modbus—Modbus is a serial communications protocol widely used to communicate with PCS field devices; it can also be used to refer to the newer version of this protocol that rides over TCP.

NIC—network interface controller: a NIC, or network card, is the interface that connects a computer to a network.

PCN—process control network: PCN refers to the computer network of a PCS.

PCS—process control system: PCS is used as an umbrella term to refer to DCS, SCADA, and other types of industrial automation systems.

SCADA—supervisory control and data acquisition: SCADA is a collection of computerized equipment used to monitor and control large-scale industrial facilities like pipelines.

TCP—transmission control protocol: TCP is the standard communication protocol used on the Internet and most other modern networks.

Notes

www.logiic.org

Sandia National Laboratories' participation in LOGIIC was funded by the U.S. Department of Homeland Security's Science and Technology Directorate under Program Manager Douglas Maughan. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
SAND2007-2101P. Designed by Creative Arts (505) 844-6416. SP•110231•04/07

Sandia
National
Laboratories

NNSA
National Nuclear Security Administration