SPE 112133

Secure Architecture for Process Control

Eyad Alqadi, Cisco Systems Incorporated

This paper was prepared for presentation at the 2008 SPE Intelligent Energy Conference and Exhibition held in Amsterdam, The Netherlands, 25–27 February 2008.

Abstract

The cost of shutting down a refinery, or an oil well, or even a digital pipeline can cost millions of dollars in revenue loss to any oil company, and with today's oil prices at their highest peak, this could be devastating to the economy of countries were oil revenue still represents up to 70% of their total GDP. Now imagine, if this was caused by unauthorized access or breach of security to the production operations- Process Control Systems ?

Process Control Systems have always been an integral and crucial part of any Energy company's critical infrastructure. Over the years, they have evolved from stand-alone islands to interconnected networks that co-exist with corporate IT environments, introducing many security threats. For the past years, these systems were effectively isolated from sources of cyber threats external to their owners and operators. But today, growing demand in the industry driven by new business requirements and new advancement in technology to link both systems together has led to an increase need to secure process control systems in order to minimize their vulnerabilities to cyber threats.

In response, Cisco Systems has developed and innovative solution called "Secure Architecture for Process Control". This solution is designed to address the risks inherent in modern process control systems while providing best of breed security solutions and delivering comprehensive asset protection and secure access to real-time information.

This paper will examine the new security threats facing the most critical infrastructures in the Energy industry and it will address the following topics; What are the new business trends and drivers ? What are the new security threats ? How secure is your system ? Should you be worried ? What solutions are available today ? What new services can be introduced ?

Background:

Most oil & gas (Exploration & Production) companies run separate networks; 1) Enterprise Network that manages the back office traffic and other business applications such as email, ERP, HR,…etc. This is no different from other corporate network in different verticals. 2) Production Networks or Process Control Networks (PCN) which are used primary to monitor, control sensors, and provide communications from oilfields / oil rigs to a control centre over wireless, frame relay, microwave, VSAT, and / or fiber. SCADA (Supervisory Control and Data Acquisition) and DCS (Distributed Control Systems) are the most common methods for implementing Process Control Networks in the oil & gas industries. Historically, they run proprietary hardware and communications protocols. SCADA systems are typically spread over miles of distance and sometimes have their programmed control functions in the central host computer, whereas DCS systems are usually installed within single large facilities with the local processor providing the control logic. In recent years, both SCADA and DCS systems have evolved to include PC's standard operating systems, TCP/IP communications, and internet access.

What are the New Business Drivers and Trends ?

1) There is new shift in the industry towards open standard and open protocols (TCP/IP) in the Process Control Systems (PCS) which led vendors to develop their new products using predominantly Object Linking and Embedding (OLS) and Process Control (OPC) technologies that are MS Windows based. In addition, there is growing demand for Internet & Intranet applications, and new requirements by users to access networks remotely.
2) The evolution toward network connections between corporate IT and process control systems along with advances

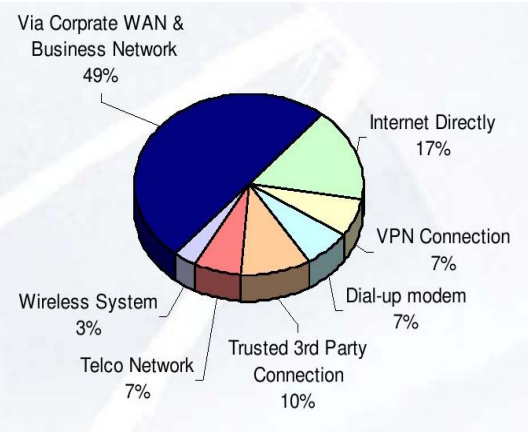
in technology and business practices has exposed previously isolated control systems to Internet attacks. Other new exposures include unsecured network connections such as wireless devices, and control systems network connections to third party (maintenance vendors, outsourced business process connections).

3) Skill shortage and lack of enough field expertise are forcing the industry to look for new ways to provide remote management for unmanned operations and oilfields/oil rigs. New remote management and services could yield to increases in operation agility, production, and oil recovery as well as provide heath and safety protection for personal.
4) Increase of new security threats and systems vulnerability from unauthorized users accessing both networks has led governments to create new policies, measures, and regulations to protect these assets.
5) There are key differences between Corporate IT systems and Process Control Systems. Control Systems operators strive for availability, reliability, and safety while IT security staff stress confidentiality, integrity, and availability. In addition, cultural difference between corporate IT staff and Process Control Networks staff could be a major obstacle where both groups have always operated independently.
6) Process Control Networks historically operated in isolated environments in which network security was viewed as unnecessary and these networks lacked security features and practices common to corporate IT systems. On the other hand, today both networks are being linked together to improve monitoring, management, and quick decision making.
7) Process Control Systems have lower technology refresh rates than Corporate IT systems and their life cycle can reach up to 30 years. In contrast, new emerging Process Control Systems are using TCP/IP interfaces used by Corporate IT systems.

How Secure is Your System ? Should You be Worried ?

Today, there is growing demand coupled with new trends in the industry to link both networks for the following reasons;

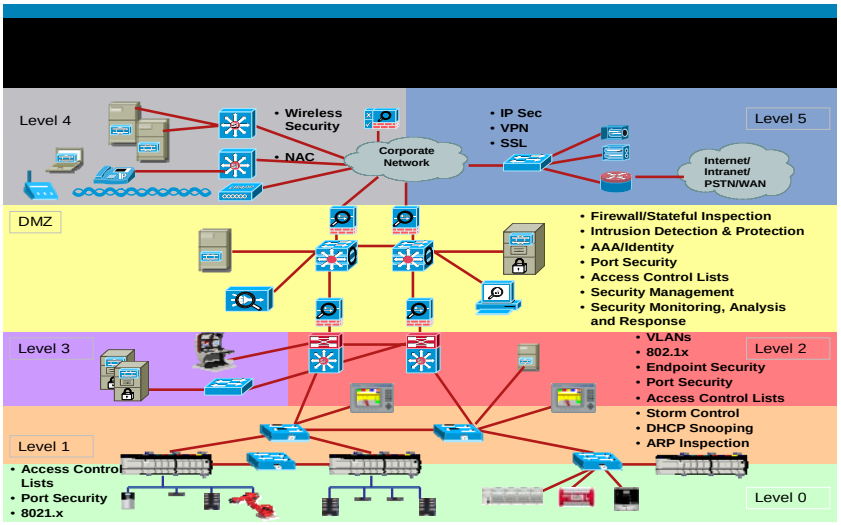
1) Increase of cyber threats against process control systems.
2) Increased demand to link operation and corporate networks under one common secure platform.
3) Process control vendors offering Ethernet and/or IP enabled systems/devises.
4) Requirements for remote access, real-time, visibility, and post incident analysis.
5) Ability to capture forensic information to help troubleshooting and improve real-time decision making.
6) Optimize enterprise-wide operational performance and efficiency from disparate systems, joint ventures, or acquired companies into single secure common used format.
7) Deployment of new services and applications (Wireless, Voice, Video, etc.).
8) Demand for high level secure system due to terrorism threats.



Source: Eric Byres, BCIT

What is Secure Architecture for Process Control ?

Cisco's Secure Architecture for Process Control provides tighter integration and a secure platform linking both business and production operations under one common security policy. This approach delivers greater asset protection while enhancing productivity and collaboration across the entire value chain.



What are the Key Benefits of the Solution ?

Secure Arachitecture for Process Control allows energy companies ensure their Process Control (PC) infrastrcutre is properly secured, by leveraging best practices and industry leading solutions from Cisco's self-defending network architecture – allowing the companies to safely extend access to the PC networks (whether to drive collaboration by sharing operational information or to bring additional expertise to facilitate troubleshooting), add further value-added capabilities, drive business process improvements and ensure regulatory compliance.

By taking a comprehensive approach, and managing policies in a consistent manner across both the enterprise network and the PC networks, energy companies can achieve the highest level of availability and reliability, identify and contain threats, and maximize uptime. Additional benefits for implementing Cisco's Secure Architecture for Process Control;

1) Provide secure link between corporate IT systems and the process control networks.
2) Provides timely and appropriate response to threats and incidents.
3) Regulatory security policy compliance.
4) Reduce operating and management expenses.
5) Adhere to corporate IT security policy.
6) Support new and advanced services and technologies
7) Ensures best practice security for process control network
8) Protects data and physical assets, using network as the platform
9) Increases access and connectivity to critical data
10) Allows secure remote access by vendors, maintenance staff
11) Enables trading based on real-time inventory levels
12) Supports improved Health, Safety & Environment procedures