General DataComm
The Best Connections in the Business

GDC Implementations for Securing Distributed Control System (DCS) and Supervisory Control and Data Acquisition (SCADA) Networks

Introduction

Since September 11, 2001 United States agencies involved with national security have become increasingly concerned about the vulnerability of the North American power grid, water supply, refining, nuclear facilities and railroads to electronic intrusions or "cyber attacks". Several studies have been conducted and have identified changing socio-economic conditions that increase the probability of such computer-based attacks. Increased domestic and international terrorism, industry related issues affecting the utilities job market, the shift to more open standards for interconnection of DCS and SCADA networks and a growing population of computer-literate people with widely available hacker tools are factors that contribute greatly to the likelihood of such threats.

In this paper, we will identify and discuss threat origins and how technologies available today from GDC can mitigate these threats and be part of a comprehensive network design and security policy to ensure safe and secure communications between components of DCS and SCADA networks.

What is a DCS or SCADA network?

DCS are used to control large, complex processes such as power plants, refineries, and chemical plants typically, but not always, at a single site. A DCS is comprised of a supervisory layer of control and one or more distributed controllers contained within the same processing plant. The supervisory controller runs on a central server and communicates with subordinate controllers via some form of peer-to-peer network. The supervisor sends set points to and requests data from the distributed controllers. The distributed controllers control their process actuators (switches, valves, flow controllers, etc) based on requests from the supervisor. These controllers typically use a local field bus to communicate with the actuators and sensors eliminating the need for point-to-point wiring to each device. Many times, the distributed controllers in a DCS have the capability to be accessed via a modem allowing remote diagnostics and servicing by vendors and plant engineers.

A SCADA network typically consists for a Central Monitoring System (CMS), contained at a central plant for example and one or more Remote Stations. The CMS houses the Control Server and the communications access via a peer-to-peer network. The CMS collects and logs information gathered at the Remote Stations and generates necessary actions based on the gathered data. A Remote Station consists of either a Remote Terminal Unit (RTU) or a Programmable Logic Controller (PLC) which controls actuators and monitors sensors. Remote Stations typically have the capability to be interfaced by field operators via laptops or other handheld devices to perform diagnostics and repair operations. The communications network is the medium for transmitting information between Remote Stations and the CMS. These facilities can be telco lines, cable, or RF.

Fieldbus - Ethernet

It is important to understand that DCS and SCADA based industries are undergoing a change in how these networks are implemented. Controller networks typically were based on proprietary serial cabling and/or fieldbus architectures (Fieldbus, Modbus, Profibus) which have upper data limits of about 2Mbps, node limitations, and distance limitations which all varied from technology to technology. This would all need to pass through a gateway to get to the internal IT network — a very cumbersome approach. The development of Ethernet-capable controllers and PLCs and the need for integration of other requirements (security devices, bar code scanners, smart cards, etc) are helping to drive the industry towards more open and ubiquitous architectures. This shift is also made apparent by the fact that many vendors are encapsulating the bus protocols into TCP/IP: Modbus/TCP (Modbus protocol over TCP/IP, EtherNet/IP (ControlNet/DeviceNet over TCP/IP), Fieldbus High-Speed Ethernet and ProfiNet (Profibus over Ethenet). Ethernet is quickly becoming a larger part of DCS and SCADA network implementations, in some cases replacing or augmenting the older bus-type architectures.

Threats

As demonstrated daily, any TCP/IP based network is subject to intrusion. These intrusions come from numerous sources including:

Threats from within:

-- Company staff, technician, operators.
-- Security breaches may not be intentional, BUT….
-- Emailed viruses

Threats from the outside:

-- 3rd party support services
-- Communications lines
-- Vandalism/terrorism

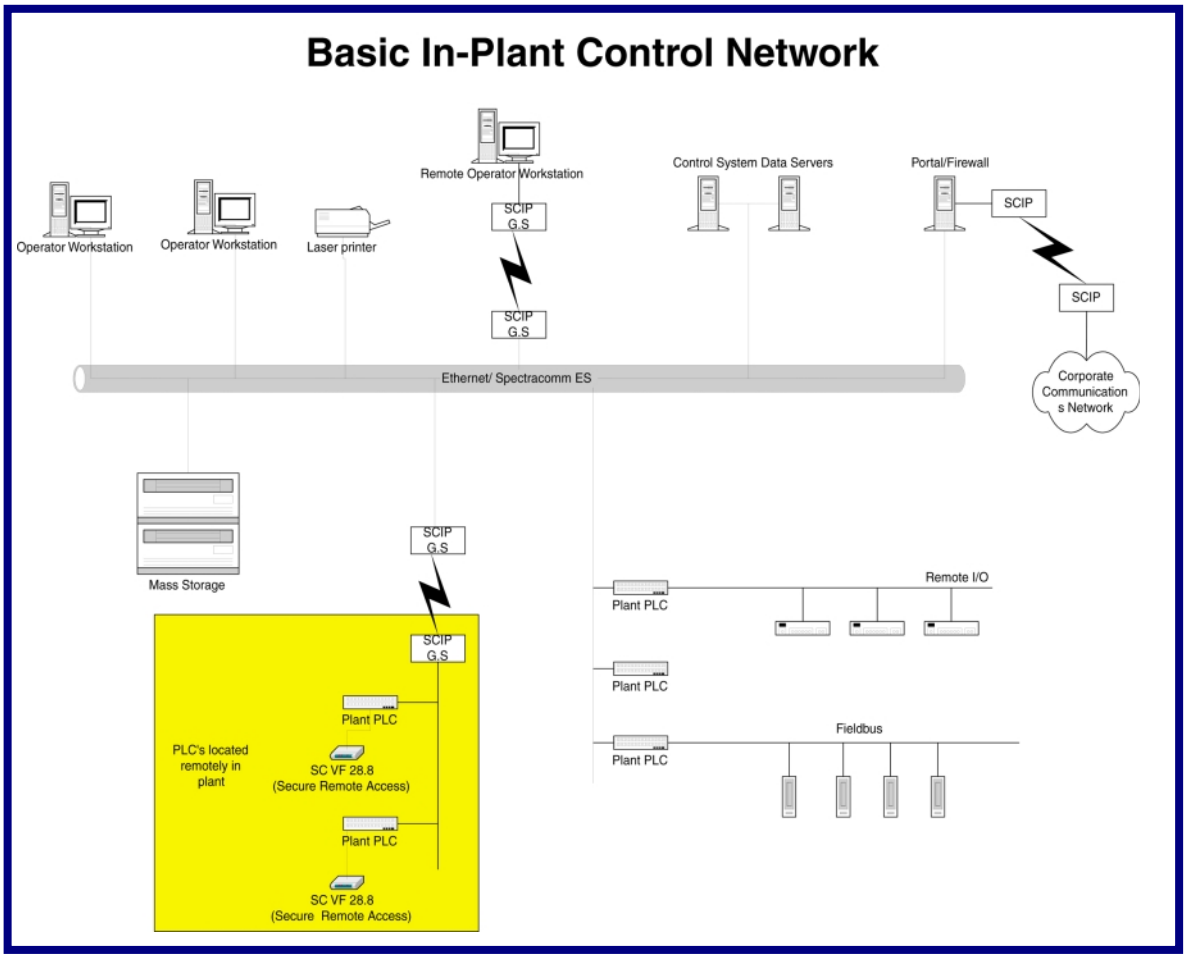
Security measures should not be taken lightly. Remember, if your network is easy for your IT Department to manage, it is most likely easy for an outside party to infiltrate.

How can GDC address security issues with DCS and SCADA networks?

GDC products should be part of a comprehensive secure network implementation. Other elements that should be addressed are policies and enforcement, virus detection and prevention, firewalls, and Intrusion Detection Systems (IDS). GDC's line of secure modems and IP access products can be the first line of defense at the most basic levels of your network – OSI Layers 1 and 2.

As stated earlier, most legacy DCS/SCADA networks have modem access to some controllers (and potentially elsewhere) for remote maintenance and troubleshooting. GDC's family of V.34 modems with Steadfast® Security and additionally RADIUS authentication can make these connections "hack-proof". GDC's Steadfast® Security, which is a proprietary, handshake-based exchange requires a GDC modem at both ends. If the handshake password exchange is not completed properly, the call is dropped before ever being connected to the network. With a common length password of 6-8 alphanumeric, it would be statistically impossible for any hacker to gain access, assuming they have a GDC modem Additionally, adding RADIUS authentication security where applicable would further enhance the security.

With the migration / augmentation of the DCS and SCADA peer-to-peer networks to 10 / 100 Ethernet, GDC's line of IP access products, SpectraComm IP (SCIP) and SpectraComm Ethernet switch (SCES) can provide first-line intrusion prevention. All of the SpectraComm IP and Ethernet switch units implement GDC IronGate Security features. These features, including port-based shutdown and MAC address filtering, can limit access only to authorized devices and personnel as designated by the MAC Address tables configured in the unit by the network administrator. It should be noted that a SCIP unit in LAN Extension (LAN-X) mode can not only filter MAC addresses on the LAN, but can also filter on the WAN port as well to ensure that unauthorized access does not occur from the circuit (Telco facilities). Additionally, the SCIP and SCES implement industry-standard TACACS+ compatible clients for centralized authentication.

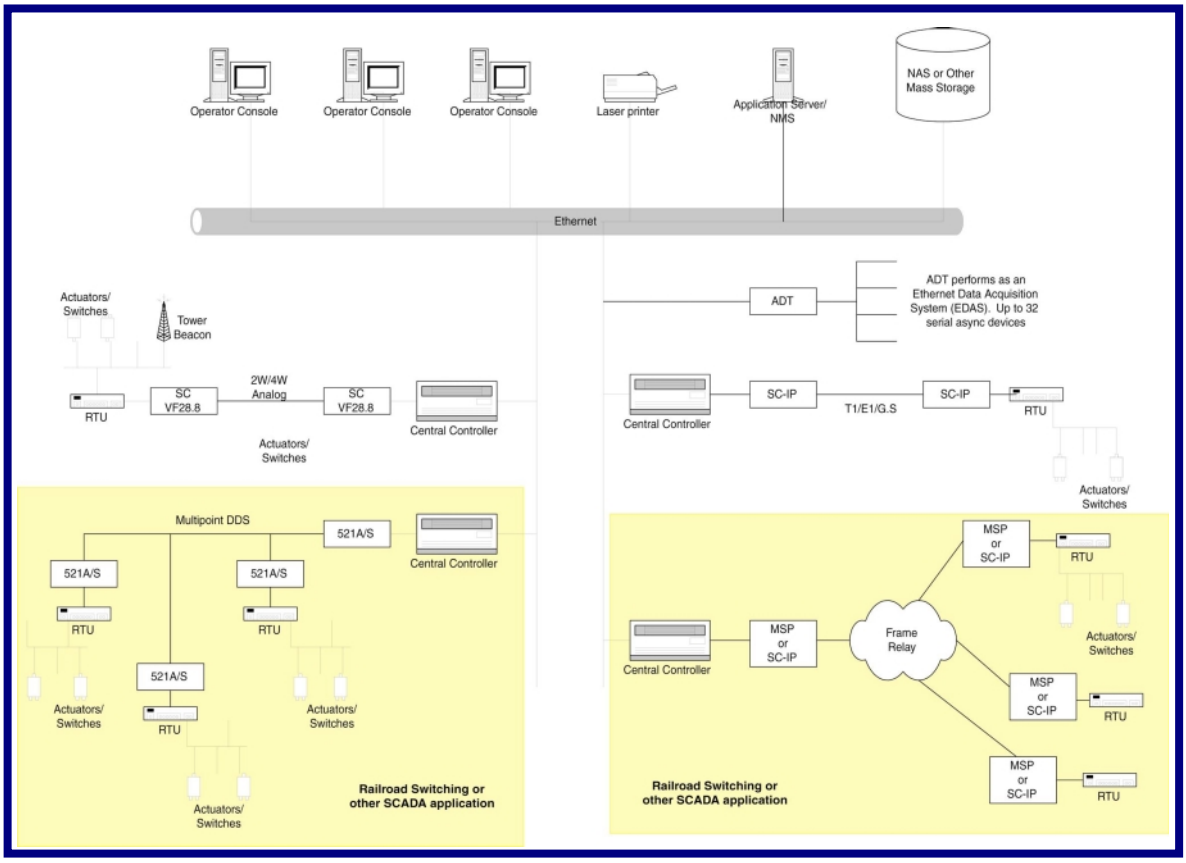


In large-scale processing facilities, the SCIP T1 (1.544 Mbps up to 5000 feet without repeaters) or SCIP G.S (4 Mbps up to 7000 feet on 1 pair or up to 12,000 feet on 2 pair) in LAN Extension (LAN-X) mode, can extend the reach between the Central and Distributed Controller well beyond the 100 meter reach of Ethernet alone. Implementing the MAC-based filtering and / or TACACS+ in these situations allows maintenance personnel to attach to the network at the SCIP as determined by the network administrator.

In SCADA RTU applications, the SCIP T1 in LAN-X mode and SCES offer a compelling and secure solution where one might typically install a router with its associated costs. Implementing the MAC-based filtering and / or TACACS+ allows only authorized maintenance personnel to access the network via the SCIP / SCES as determined by the network administrator. Additionally, the Contact Sense feature on the SCIP could be implemented to alert network monitoring personnel of such things as door opening, high water, high heat, etc. at the Remote Station if so desired.

SCIP and SCES have been independently tested and certified to stringent NEBS Level 3+ requirements for Telcos and additional testing have proven them to be consistent with the classification as temperature “hardened” (-40 °C to +70 ° C) for deployment in extreme environments.

Typical SCADA Application



Conclusion

As has been shown, GDC offers a compelling and competitive solution for first-line defense and intrusion prevention. The combination of Steadfast® Security for dial connections and GDC IronGate Security for Ethernet connectivity, address the most basic levels of secure networking for DCS and SCADA applications as part of a comprehensive security policy.

General DataComm
The Best Connections in the Business

General DataComm, Inc. WORLD HEADQUARTERS: Naugatuck, Connecticut, USA 06770 Tel.1-203-729-0271