The purpose of this guide is to provide examples/types of SCADA and control systems and their typical use in industry. This document then describes the functional areas of those SCADA systems which typically use analogue serial telecommunications technologies, those components which are impacted with the move to ethernet TCP/IP communications; the security risks to consider when migrating to IP-based communications, and practical tips for ensuring the reliability and security of SCADA systems when leveraging ethernet TCP/IP protocols and communications links.

This guidance is designed to impart good practice advice for securing industrial control systems such as process control, industrial automation, distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems. Such systems are used extensively across the nation’s critical national infrastructure. The document provides valuable advice on protecting these systems from electronic attack. It has been produced by the Red Tiger Security firm on behalf of CPNI and peer reviewed by members of the SCADA and Control Systems Information Exchange.

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favouring by CPNI or Red Tiger Security. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. CPNI and Red Tiger Security accept no responsibility for any errors or omissions contained within this document. In particular, CPNI and Red Tiger Security shall not be liable for any loss or damage whatsoever arising from the usage of information contained in this document.
Securing the move to IP-based SCADA/PLC networks

Use of wired circuits for carrying several types of serial communications 19
Figure 8: Legacy SCADA system using fibre (mapped to the ISA 99 model) 19
Use of Wireless RF systems for serial communications 20
Figure 9: Legacy SCADA system using RF (mapped to the ISA 99 model) 20

The move to Internet Protocol 22
Internet Protocol (IP) defined 22
Figure 10: 7-layer and 4-layer OSI models and data flow diagram 22
Common control system components likely to move to IP 23
Most typical migration path from serial to IP 24
Changes required at the front end processor (FEP) 24
Implementing the new ethernet communications path from HMI to RTU 25
Zones, conduits, boundaries and security levels 25
Figure 11: Original concept of zones and conduits (from the first version of ISA99 standard in 2003) 26
Figure 12: Security levels as depicted in the ISA 99 standard 27

SCADA systems which leverage ethernet TCP/IP communications 28
Legacy replacement (e.g. modems replaced) 28
Tunnel serial traffic over IP 28
Tunnelling RS-232 over ethernet IP networks 28
Figure 13: Leveraging TCP/IP networks to transmit RS-232 serial data over IP 29
Definitions for various types of ‘SCADA firewalls or gateways’ 29
Figure 14: Table 1: Comparison of network gateway devices 29
Serial to IP converters (convert leased and dial line modems to cellular broadband service) 31
Figure 15: Cellular communications for SCADA (option 1) 31
Figure 16: Cellular communications for SCADA (option 2) 32
Multi-network design 33
Figure 17: Modernisation in process: legacy and IP devices on the same IP network 34

Future technologies 35

Management of SCADA/PCN IP-based networks 36
Challenges with the transition to IP networks 36
Best practices for managing SCADA/PCN IP-based networks 36
Figure 18: Harvesting security alerts and logs off of SCADA system devices 37
Figure 19: Use of Intrusion Prevention System (IPS) technology for networks directly upstream of SCADA environments 38
Executive summary

Overview

‘Supervisory control and data acquisition’ (SCADA) and control systems were initially designed to monitor and control industrial processes using proprietary protocols, and were typically kept isolated from other computer systems. Since these SCADA systems were never designed with security in mind, and are now being connected with business networks and the internet, they are now more than ever at risk.

With the move to 21st Century networks taking place, many traditional telecommunications providers are moving from a circuit switched to a packet based infrastructure. This allows the convergence of many different network types (e.g. voice, data, video, physical security and control signals) onto a single network and can represent significant cost savings to a business. Many businesses have increased connectivity between the SCADA and corporate network in order to gain improved business and allow more informed decisions to be made, with no consideration for security of the SCADA and corporate systems. With an increased level of risk in the Internet Protocol (IP) world and the increasing interest in the security of control systems, it is important that asset owners understand the various IP-based solutions available in order to make an effective security based risk management decision.

With routable IP-based communications, threats can come from anywhere, and these networks are much more dynamic in nature. New management activities are now required with ethernet TCP/IP SCADA systems that did not exist in legacy serial communications. These activities include keeping networked devices up to the latest firmware, providing network access controls to block unauthorised access, and monitoring the use of these devices.

This best practice guidance document first defines the various components of a SCADA or control system, and then explains how various parts of these SCADA systems have evolved to operate over switched IP networks. This document also covers several aspects to consider when deciding to convert from dedicated serialised telecommunications circuits to IP-based packet switched networks. Managing SCADA systems that operate over IP networks requires much more security oversight, as well as additional security solutions and considerations. After discussing these topics, this document provides a section on future technologies and Next Generation Networks (NGN).
Best practice: design and management of IP-enabled SCADA networks

This document contains several best practice recommendations to consider when converting from serial to IP-based SCADA telecommunications infrastructures. The recommendations have been lifted from various sections of the document and are listed here as a quick reference guide.

Network isolation / segmentation

- Keep the SCADA IP network physically separate and isolated from the Corporate IT Network and other un-trusted networks.

- Where physical separation is not a practical option, logical separation must be applied due to the heightened risk of IP-enabled SCADA systems. It should be noted that logical separation is more complicated to implement effectively, and runs the risk of ineffective configuration over the life of the assets.

- Use quality assurance techniques to ensure that all security requirements identified during the design phase are developed, tested and implemented within the final product. Also consider using the ISA S99 security levels as a model when designing SCADA and control systems based on IP-based protocols. The ISA S99 security standard defines security levels 0 (Instrumentation) all the way up to level 5 (internet-facing systems). Each security level is designed to support specific SCADA components based on functionality requirements and security. For example, FEPs (Front End Processors) are typically placed in level 2, right alongside the HMI or operator console. They log data to a data historian, which resides in the DMZ or level 3.

- IP communications which originate from untrusted networks outside of the SCADA and control system networks should terminate in a DMZ or buffer network; they should not be allowed to make direct connections with components in the SCADA and Control Systems networks.

- Devices on the inside of the SCADA and control systems network should not be able to communicate directly with the internet, nor should they be used with external email.

- Avoid the use of Virtual LAN (VLAN) technology as a method of keeping SCADA IP communications logically separated from Corporate IT communications: VLAN technology was not designed as a security method.

- If existing corporate IT network infrastructure such as switches, routers and WAN links must be used as a transport method for portions of the SCADA communications, then the SCADA communications should be encrypted and routed through a VPN tunnel through corporate IT or other non-critical networks.

- When building a complete end-to-end IP network, avoid using devices which use layer 3 separation between SCADA and other non-critical networks. Devices claiming layer 3 network isolation use VLAN (Virtual Local Area Network) technology to virtually isolate network traffic. VLAN technology was initially designed as a bandwidth-shaping tool, and was never designed with security in mind. Several free hacking tools allow VLAN-walking capability that allows an attacker or malware to jump across any layer 3 VLAN network. For true network isolation use equipment that can provide isolation at layer 2.
• Do not permit SCADA or control system devices to be dual-homed to two or more networks that are at different security zones or trust levels. For example Plant Data Historians should only be connected to one security zone, such as the DMZ, then a firewall rule or access control rule should be created to specifically allow traffic from the Plant Data Historian to be exchanged with the SCADA or control system over specified ports at specified rates.

• If remote access is allowed into the SCADA or control system over an IP-based network, then a different authentication check should be made to remote users in addition to the authentication process used to log into the corporate IT network. In addition, remote access should not be permanently enabled; it should only be granted upon request from a known and trusted source, with an end time agreed, following which the access should be discontinued.

• A good cyber defence must compliment active blocking devices like firewalls, IPS, and network in-line antivirus appliances with passive detective technologies which can detect, log and alert to what is happening at the network, server and application layers. NIDS (network intrusion detection sensors), HIDS (host intrusion detection sensors), Syslog events, and SNMP traps can all be configured to send their logs and alerts to a centralised SIEM (Security Incident and Event Management) appliance where the logs and alerts can be reviewed and escalated as needed.

Management considerations for SCADA/PCN IP-based networks

• When managing IP-enabled telecommunication devices, network equipment, PLCs, RTUs, protocol gateway converters, and any other embedded devices, disable any unnecessary services and limit the attack footprint by disabling or blocking unnecessary TCP and UDP ports.

• Limit the use of clear text protocols such as telnet, ftp, and http. Instead, force the use of encrypted protocols, where technically feasible.

• Most IP-enabled telecommunication devices such as switches, routers, firewalls, protocol converters, media converters and serial terminal servers support SNMP (Simple Network Management Protocol) for monitoring the health and performance of the devices. Ensure that the latest version of SNMP is enabled, and configure the security and performance based alerts to be collected by a SEM (Security Event Management) system. The default SNMP community strings should also be changed.

• Most IP-enabled telecommunication devices such as switches, routers, firewalls, protocol converters, media converters and serial terminal servers support the logging of security events such as denied attempts. Logging should be enabled in such a way that a log is kept resident on the device and a copy sent out to a Defence syslog server. If an SEM is already present on the network collecting SNMP events, then send the syslog information to the same SEM. Organisations will have to determine the appropriate frequency and scale of operation in reviewing logs generated by IP-enabled devices. Several industry best practices such as ISA 99 suggest that logs be reviewed on at least a monthly basis. Government regulations such as NERC CIP require that logs be reviewed within 30 days, and that the reviewer must sign off that the action was performed. As indicated in the previous point, if SNMP is used, the latest version of the protocol should be used that supports encryption and the default community strings should be changed.
- For SCADA and control system networks that contain critical components, system administrators should also consider deploying in-line network appliances at the choke points that perform Network Intrusion Prevention and Anti-Virus to filter and drop packets that are a known signature match for malicious traffic.

- Firmware for IP-enabled telecommunications equipment and control devices should be kept up to date within the current patch cycle. Due to its real-time nature, patching SCADA system components is problematic, and in many instances not a practical option due to the consequent overhead of retesting the system. Purchasing industrial control equipment that have gone through an industry security certification like the ISA Certification process, helps ensure that the components have gone through rigorous vendor and industry inspection. Some control system vendors will test the latest security patches on their systems first, and release a ‘certified patch’ for their end users. Leveraging industry and vendor certification processes can reduce the periodicity of system patching.

- Control devices such as PLCs, RTUs, Smart Meters, ethernet I/O and IP-enabled instrumentation should be deployed with a password or PIN code that must be required to make changes to the configuration over an ethernet connection. Based on the level of risk, some devices may be configured to only allow configuration changes over a serial console cable.

- Control devices such as PLCs, RTUs, Smart Meters, ethernet I/O and IP-enabled instrumentation have known TCP/IP stack vulnerabilities. Switches, routers, firewalls, or any network devices in front of the control devices should be configured with rate limiting commands to restrict data from flooding the device.

- The alerts and logs from network equipment can be either configured for sending to a SEM (Security Event Management) system and viewed by IT security staff, or be translated to OPC tags and viewed by SCADA and control system operators. Translation software is available to convert SNMP and Syslog data to OPC.

- Whether the network is monitored by IT staff or SCADA operators, responsibility for the care and management of the networks should be clearly defined, and system logs should be reviewed on at least a monthly basis.
**Introduction**

**Terms and definitions**

Throughout this document, the terms ‘SCADA’ and ‘control system’ are used as generic terms to refer to all industrial automation and control systems, distributed control systems (DCS), energy management systems (EMS), and related real-time monitoring and control systems.

The follow list defines some of the acronyms and industry-specific terms used within this report.

- **APT** Advanced Persistent Threat
- **AD** Active Directory
- **CIP** Critical Infrastructure Protection
- **DCS** Distributive Control System
- **DMZ** Demilitarised Zone
- **ESP** Electronic Security Perimeter
- **ISA** International Society of Automation
- **PLC** Programmable Logic Controller
- **RTU** Remote Terminal Unit
- **SCADA** Supervisory Control and Data Acquisition
- **TCP/IP** Transmission Control Protocol (TCP) / Internet Protocol (IP)

**Target audience**

This guide is aimed at anyone involved in the security of process control, SCADA and industrial automation systems including:

- process control, automation, SCADA and telemetry engineers;
- information security specialists;
- physical security specialists;
- government and policy makers;
- business leaders;
- risk managers;
- health and safety officers;
- operations engineers;
- security professionals (either in-house staff or outsourced).

*Note: the role of cyber security can be outsourced to a 3rd party through the use of MSSP (Managed Security Service Program), however the responsibility and accountability for security can never be outsourced; it must be owned by a senior designated manager.*
Types of SCADA and control systems

Before describing what elements of a SCADA or control system are impacted by the move from serial to IP-switched communications circuits, we should first provide an overview of the various types of SCADA and control systems, and their use in industry. This section defines the most common types of SCADA and control systems.

Automated systems

- Automation is embedding logic in a controller to allow a process to run efficiently without constant human intervention.
- An automated system contains at least one controller, but may also include a local touch screen or terminal for the system operators to interact with the controller.
- An automation system is typically the lowest level building block for higher level SCADA, DCS, and process control systems and can either exist as an isolated disconnected system, or be networked with other systems.

Supervisory control and data acquisition (SCADA)

- SCADA systems extend the capabilities of an automated system so that it can be monitored or controlled from a remote location.
- Only master servers at the centralised control room can send commands to distributed controllers installed out in the field or read and write data from them.
- SCADA software can automate the flow of data to other business applications.
- SCADA systems are typically used when automated processes are not in one geographical location. Examples in industry include oil and gas pipelines; electric power transmission and distribution; water and waste water operations; gas utility service; onshore and offshore oil and gas production; wind power farms, and any other application whereby the monitoring points are scattered geographically across a large region.
Distributed Control System (DCS)

- With DCS systems, the monitoring and control functions are embedded into all major components of the control system, instead of only in the master servers.

- All distributed controllers, engineering workstations, operator consoles, and field inputs/outputs (I/O) are networked together so that all system components are on one platform without the hierarchy found in SCADA Systems.

- DCS systems can also automate the flow of data to other business applications.

- They are typically used when all automated processes are in one geographical location. Examples in industry include large petrochemical facilities, refineries, chemical manufacturing plants, food and beverage manufacturing, and other heavy industrial plants where all the industrial control systems are physically located in the same geographical area.

- DCS systems are often integrated with MES (Manufacturing Execution Systems) to extend the functionality and tracking capabilities of the facility.
Manufacturing Execution Systems (MES)

- Extends the functionality of a SCADA or DCS system for batch management and may include one or more of the following functions:
  - managing work orders, receipt of goods, shipping, quality control, maintenance, scheduling or other related tasks;
  - link enterprise accounting systems like SAP to plant floor industrial control systems;
  - automate the management of batches or recipes;
  - track and control raw material and finished goods inventory;
  - track Key Performance Indicators (KPI);
  - make intelligent decisions to influence production and cost management;
  - manage resources, including inventory and personnel.

Energy Management System (EMS)

- EMS systems are a type of SCADA system used specifically for electricity transmission monitoring and control.
- These systems comprise:
  - centralised servers at the primary and backup control centres;
  - distributed monitoring and control elements at remote substations;
  - disconnect and reconnect switchgear at substations and on top of electrical poles near power transformers;
  - EMS systems also typically include demand scheduling/load balancing systems, OMS (Outage Management Systems), GIS Mapping Systems, and NMS (Network Management Systems).

- Also used in Electricity Transmission & Distribution systems to monitor and control distribution of power to large industrial users and neighbourhoods.
- During the last five years there has been a movement in North America to integrate EMS systems with AMR (Automated Meter Reading) systems.

Automatic Meter Reading (AMR)

- Refers to the ability to automatically collect data from electricity, gas and/or water meters through several different communications networks, including RF wireless, power line carrier, telephone, and other ways.
- The main business driver for deploying or implementing AMR systems is to automate monthly customer billing, and reduce labour costs involved with involved with traditional meter reading.
- AMR systems typically involve meters fitted with communication modules, collection systems (including handheld computers, drive-by systems and fixed network coordinator nodes), as well as supporting software to manage collection of the data.
Automatic Metering Infrastructure (AMI)

- Generally refers to systems that are capable of automatically collecting detailed energy usage data more frequently than the traditional meter reading that happened once a month.
- Collection of data on a more frequent basis enables utilities to support time-based pricing programs for their customers, as well as to achieve other benefits relating to energy delivery and customer empowerment through informed energy usage choices.
- In North America, many believe that AMR and AMI systems are building blocks of the future ‘Smart Grid.’

Building Automation Systems (Building Management Systems)

- Implemented to control the lighting, heating, cooling, and security of a building.
- Building Automation Systems, or also known as Building Management Systems, are another example of a distributed control system. The control system is a computerised, intelligent network of electronic devices, designed to monitor and control the mechanical and lighting systems in a building.
- The core objective of these systems is to keep the building climate within a specified range, provide lighting based on an occupancy schedule or room sensors, monitor system performance and alert engineering or building administrative staff to failure of system utilities.
- These systems can greatly reduce building energy consumption and maintenance costs when compared to a non-controlled building. A building controlled by a BAS is often referred to as an intelligent building system, or a ‘Smart’ Building.

Industrial control systems (ICS)

- The term ICS has evolved into a general term that applies to all types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and smaller control systems that use programmable logic controllers (PLC) or PC-based control.

NOTE: The SCADA and control systems industry has now standardised the term ICS. The United States’ Department of Homeland Security formulated the ICSJWG (ICS Joint Working Group) specifically to address cyber security issues related to SCADA and control systems. The ICS-CERT organisation has been set up within US-CERT specifically to address SCADA and control system security vulnerabilities and provide incident response guidance.
Figure 3: Example of a building automation or building management system
SCADA and control system components

Overview of a typical SCADA system

Although there are differences in the functionality of the various types of industrial control systems described in the previous section of this paper, they all share common system components.

All SCADA systems require sensors, instrumentation or other metering devices to acquire information about the physical process. The sensors, instrumentation and metering devices are connected to field control devices such as PLCs (Process Logic Controllers) or RTUs (Remote Terminal Units). These control devices take real-world physical input signals (voltages and currents) from the sensors and instrumentation, convert the signals to digital data and make decisions based on programmed logic or commands from the system operators to turn other equipment on or off or change system control parameters.

The control devices are connected over hardwired or wireless communications back to control room environments where the HMI (human machine interface) software systems are used by system operators to interact with the control devices, change system parameters or send commands to the plant equipment.

Figure 4: Major components for a typical SCADA system
Components of a SCADA system that historically used serial communication channels

Although the operator consoles, SCADA servers and control room system components all use ethernet TCP/IP communications, the communications to field devices, controllers, meters, and smart instrumentation still use serial communications.

The ISA (International Society of Automation) published a two-part standard on cyber security called the S99 standard which defines specific security levels (levels 0–5) for control system and corporate IT components based on their function in the system.

![Sample Legacy SCADA/DCS Architecture](image)

*Figure 5: Legacy SCADA system components (mapped to the ISA 99 model)*
In legacy systems, the operations systems were not typically connected to the business LAN, and the field controllers and plant equipment located at level 1 and level 0 used serial circuit communications as shown in the diagram above.

Since levels 3 and above in SCADA and control systems are typically already leveraging ethernet TCP/IP networking to connect the SCADA computer workstations and servers to other networks, we can focus on the lower levels of the system which involve acquiring data from controllers and field devices.

This next section will review various architectures of legacy SCADA systems and examine how modems, wired copper and fibre circuits, and wireless RF systems were used to provide analogue serial communications between the field equipment such as RTUs and PLCs and the central control room computer systems.
Legacy SCADA systems use various methods of serial communications

Primer on serial communications

SCADA communications over a serial or analogue channel typically use serial cables with DB9 connections on each end. The diagram and pin-out table below shows the typical use of each signal line in a RS-232 data link:

![Pin-out diagram for serial communications](image)

Serial communications require each device on the same channel to use the same settings so that the master device can communicate with each slave device on the channel. The following communications settings are used to define how a serial channel functions:

- Communications channel and IRQ
- Baud rate (typically: 300, 1200, 2400, 4800, 9600, 19,200)
- Number of bits (8 or 7)
- Parity (none, even or odd)
- Number of stop bits (typically 1)
- Example: 9600, 8, N, 1
- Flow control and error-checking (CRC, none, Xon/Xoff)
  
  **NOTE:** Flow control is rarely used in SCADA communications

All devices on a RS-232, RS-422, or RS-485 must be configured with the same serial communications settings. The following sections provide examples of serial analogue systems over various wired, fibre, or wireless media.
Use of modems for serial communications

For systems which are scattered over a large geographical area, POTS (plain old telephone service) modem lines were a common method for SCADA systems to leverage phone lines provided by telephone carriers to connect the centralised control room equipment to the components out in the field.

Slow limited bandwidth and latency issues are the leading drivers for migrating away from serial communications over modems, cellular infrastructure, or ISDN networks. For remote locations like offshore oil and gas platforms, the only option is satellite communications, and the timing and latency issues are greater for satellite. The following sections provide examples of how serial communications can be sent over wired, fibre and RF media.
Use of wired (copper or fibre) circuits for carrying several types of serial communications

For SCADA, Energy Management Systems and Distributed Control Systems contained within a regional area that can be covered with copper or fibre circuits, the controllers, RTUs and other field equipment are typically connected over TDM (Time Division Multiplexed) circuits.

These circuits can break out either large bandwidth circuits like T1 and DS3, specialised proprietary trunks for CCTV, or smaller individual RS-232 circuits for polling PLCs and RTUs. The underlying technology is still based on serial analogue channels, whereby attackers have to gain access to the physical channel to subvert the system. Modernisation brings additional risk, since switched IP networks can be routed into from foreign external networks if security is not applied correctly.

Figure 8: Legacy SCADA system using fibre (mapped to the ISA 99 model)
Use of wireless RF systems for serial communications

In many cases, due to geographical constraints, POTS lines were not already in place to allow for the use of modems in these legacy systems, and it was very cost prohibitive to lay copper or fibre circuits to all the scattered field devices. This was particularly the case in industries such as oil and gas production, water and waste water treatment, pipeline management and others where the nature of the distribution of these systems required another solution.

Large wireless RF systems were designed and deployed to provide communications coverage from the devices in the field to the control room computer systems.

Figure 9: Legacy SCADA system using RF (mapped to the ISA 99 model)
These wireless systems were developed with either licensed radios that used known fixed transmit and receive frequencies, or with spread spectrum radios that used frequency hopping techniques to avoid having to use fixed RF frequencies. Both the licensed and non-licensed wireless RF systems were initially only designed to transport serial communications.

In legacy wireless RF systems the master radio can connect directly to slave radios to poll the field devices for data, or in some cases, might have to connect through a repeater site to get the signal down to the slave devices if line of sight is not permitted. Repeater sites are typically used due to geographical constraints such as large hills, mountains, or buildings that might be in the way blocking the signal from the master radio.

Serial protocols only allow for one master to communicate to one slave at a time, and while the slave is responding to the master, it is consuming a serial channel that cannot be used for any other purpose. Technicians could not remotely troubleshoot or program the field devices using serial communications, so all modifications and device management had to be performed out in the field.
The move to Internet Protocol

Internet Protocol (IP) defined

Internet Protocol is responsible for addressing hosts and routing data packets from a source host to the destination host across one or more IP networks. The IP includes specific addresses to identify hosts and provide a logical location service. Each packet is tagged with a header that contains the meta-data for the purpose of delivery. This process of tagging data with IP information is also called encapsulation.

The 7-layer OSI model and the 4-layer internet model are two methods of describing TCP/IP communications. The 7-layer OSI model is used to define networking protocols and the 4-Layer model defines TCP/IP communications.

Data move from the application layer on the client side down through the layers to the physical layer where it is transported to the host. From here the data move up through the layers again to be presented on the host side.

Figure 10: 7-layer and 4-layer OSI models and data flow diagram
Securing the move to IP-based SCADA/PLC networks

Routing TCP/IP protocols built on IP communications allow the data to be separated from the transport method, thus opening up many ways to route data from the source to final destination. Instead of requiring a dedicated end-to-end link (as with serial channels), packetised communications based on IP communications can be routed over multiple methods such as wireless RF, microwave, satellite, fibre, DSL or even cellular broadband. This provides more options for those deploying or integrating SCADA systems.

Also, since routable communications based on IP technology are not one-for-one master-slave communications as in serial channels. Multiple communication masters and slave devices can communicate at the same time over the same or diverse channels, providing greater redundancy should any one link go down. For instance, if IP communications are used, an RTU can be polled by a satellite uplink and by a cellular broadband connection at the same time. Another benefit of IP communications is that while the master servers and other applications are polling field data, technicians can log into the field equipment over the same IP network without interrupting the system. This makes system administration much easier.

Common control system components likely to move to IP

Operator consoles, master SCADA servers, front end data acquisition servers and back-end historian database systems were designed and developed to be on an IP-based communications network. These components are typically software running on a modern operating system like Windows, UNIX or Linux, on either server or workstation grade hardware. Computer servers and workstations have been connected to IP networks for several decades, so even with legacy systems the computer equipment will most likely be connected to an ethernet network already. The move to IP for computer servers and workstations has already taken place. The last components to move are the embedded devices, including field controllers, meters, instrumentation, and the telecommunications systems linking the control room computing systems with embedded devices in the field.

Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and even Smart Instrumentation began to ship with ethernet communications in the late 1990s. Now nearly every control system vendor offers their equipment with ethernet TCP/IP communications capability.

When the field devices were originally deployed over serial analogue circuits, they were isolated from the cyber threats which faced computer systems, since viruses, worms, and hacking exploits were only effective on devices that supported routable TCP/IP networks. With serial communications, an attacker would have to gain physical access to somewhere along the analogue circuit, clamp onto the channel and then either capture and interpret the serial protocol or inject serial data into the circuit. With the move to IP communications, the risk to cyber threats is much greater since packets can be routed into field devices from other external networks, and the attackers no longer require physical access to the analogue circuits.

Requests from the user community for more open and inter-operable systems have accelerated the SCADA and ICS industry’s move into the TCP/IP world. The race to convert these serial devices to TCP/IP-enabled devices did not provide the vendors with adequate research and development time to design their own secure TCP/IP stacks and IP protocols. Instead, most SCADA and ICS vendors quickly acquired TCP/IP stacks and drivers from other third parties and integrated them into their hardware. At the same time, vendors also needed an ethernet TCP/IP protocol for the computer systems in the control room to communicate with the hardware. A number of vendors decided to simply encapsulate their serial analogue protocols with TCP/IP headers or wrappers, and re-use the same underlying protocols - which do not support authentication or encryption and which transmit data in clear text.

This led to the situation in which the control systems industry finds itself today.
Securing the move to IP-based SCADA/PLC networks

Devices which are directly connected to physical equipment and are responsible for controlling and monitoring the safe operations of real-world processes are the devices which are most vulnerable.

Field devices such as PLCs, RTUs, Smart Instrumentation, Smart Meters and other embedded devices are the most critical element of the SCADA system, since they control the operation of physical equipment such as valves, pumps, drives, boilers, heaters, generators, switching re-closures, compressors, conveyor belts, etc.

Instead of making the system more closed and protected, the move to IP communications opened up devices in the field to other networks and systems by connecting them with TCP/IP communications and open clear-text protocols. These embedded devices do not have the ability to support the security features that most computing systems require, such as Antivirus, Authentication, Encryption, and End Point Security, and many do not support network monitoring and logging either.

So while the industry waits for security features to be added to embedded devices, the best way to secure IP-based SCADA systems is to restrict access to them by implementing secure architectures which prevent access to the SCADA systems from Corporate IT and other third party IP networks.

**Most typical migration path from serial to IP (from the field device perspective)**

When considering migration from a serial system that uses analogue communications to an ethernet networked environment, it is not as simple as configuring the PLC, RTU, or field equipment to accept communications from IP networks. Changes will most likely need to be made at the Front End Processor (FEP) server to switch the SCADA driver from a serial protocol to an ethernet protocol. The telecommunications media and hardware may need to be upgraded or replaced, and finally changes will need to be made out at the field controller hardware as well.

**Changes required at the Front End Processor (FEP)**

If the legacy system is using a serial analogue SCADA driver to poll the data from PLCs, RTUs, or other field equipment over serial circuits, the HMI or operator interface driver is probably a serial protocol driver, and will need to be replaced with an ethernet protocol driver. For instance, if the SCADA system is using a ModbusRTU driver to poll serial data from Modicon PLCs or Modbus-enabled RTUs, this serial driver will need to be uninstalled and replaced with the ModbusTCP driver so the system can poll the Modbus data over a TCP/IP network.

All the system tags which were configured with the ModbusRTU driver will most likely have to be reconfigured and pointed to the new ModbusTCP driver. This is how the HMI or operator interface software knows how to collect data from the field devices, and it will have to be configured to make use of the new ethernet network. Migrating from an analogue serial SCADA driver to an ethernet protocol is not a trivial task; a lot of preparation is necessary to ensure that the system has the least amount of downtime as possible while it is being upgraded to the ethernet protocol driver. In most successful upgrade projects, the new ethernet network communication paths are built in parallel with the analogue circuits so that the system can move over to the TCP/IP communications quickly and seamlessly once all other system changes have been made and tested first.
Implementing the new ethernet communications path from HMI to RTU

Changing the SCADA driver from a serial driver to a TCP/IP protocol is fairly straightforward and has the least amount of operation risk associated with the move to IP communications. The new TCP/IP SCADA drivers can route from the HMI (operator console) to the field devices using TCP/IP communications, and this can be achieved in numerous ways, using many different technologies and techniques.

If an existing TCP/IP network is already in place, such as a corporate WAN link, then the SCADA protocol should not be allowed to mix with the same corporate IT traffic. An IPSEC encryption tunnel could be configured so the SCADA traffic can tunnel through the existing network. The SCADA traffic would be kept secure and isolated from the corporate IT traffic, however this means that the SCADA communications must rely upon the availability of the corporate IT network, and are therefore subject to interruptions due to events on the corporate IT network.

If an existing computer network is not available, then a new communications path will need to be designed and implemented using either wired communications (copper, DSL, fibre, etc.) or wireless communications (point-to-point RF, point-to-multipoint RF, microwave RF, spread-spectrum unlicensed RF, licensed RF, satellite, cellular, etc.). The most secure method is to implement completely separate TCP/IP network communications which are only used by the SCADA system.

If field components such as PLCs and RTUs are legacy devices with serial communications ports only, then TCP/IP-to-RS232 converters must be installed in front of the PLC or RTU port so the converter can encapsulate the serial data into TCP/IP frames and allow the SCADA legacy serial communications to travel over a TCP/IP network. There is no method of securing the serial port on the PLC or RTU, and there is no method to locally restrict the IP networks which can communicate to the serial port through the converter. The only way to restrict IP access to the serial port is by restricting the TCP/IP traffic upstream of the TCP/IP converter. This can be done with switch/router Access Control Lists (ACLs) or with firewall rules that specify which IP devices can communicate with the converter box over specified TCP or UDP ports.

Zones, conduits, boundaries and security levels

In early 2004, a small team of volunteers within ISA (the International Society of Automation) began working on a control systems security standard which was initially titled ISA SP99, where the SP stands for Standard Proposed. In early 2009 the ISA SP99 standard was ratified and approved by the international body and became an official standard entitled ISA S99 - Security for Industrial Automation and Control Systems. The ISA S99 standard was the first industrial control systems security standard that defined the concepts of zones, conduits, boundaries and security levels.
The ISA standard document S99-00-01 defines a security zone as:

‘…A logical grouping of physical, informational and application assets sharing common security requirements. This concept applies to the electronic environment where some systems are included in the security zone and all others are outside the zone. There can also be zones within zones, or sub-zones, which provide layered security, giving defence-in-depth and addressing multiple levels of security requirements. Defence-in-depth can also be accomplished by assigning different properties to security zones.’

The diagram below, provided by the ISA S99 standard, depicts typical Enterprise, Plant and Control zones, with firewalls providing boundaries between zones creating conduits for data flow.

Each zone has a border which is the boundary between systems included on the inside of the zone, and those that would be outside of the zone. Assets which are outside the security zone are by definition at a lesser or different security level.

Security levels can be defined for each functional area of the system, and the ISA S99 model uses level 5 for the most untrusted public security level for internet-facing systems, and reserves level 0 for the most trusted part of the control systems where the instrumentation is directly connected to the physical equipment.

The next diagram places the various functional components of typical SCADA and DCS systems into a logical diagram in the appropriate security levels.
Securing the move to IP-based SCADA/PLC networks

Figure 12: Security levels as depicted in the ISA S99 standard

The architecture proposed by the ISA S99 standard provides the SCADA and control systems industry with a model for segmenting networks at levels 2 and above to ensure that SCADA and control systems are isolated from the Enterprise IT networks through a DMZ (demilitarised zone).

As the lower levels 0 and 1 typically contain instrumentation, meters, PLCs, RTUs and other field embedded devices move to IP communications, additional considerations for security must be taken into consideration.

The next section discusses typical scenarios in which legacy serial communications methods are being replaced by TCP/IP communications.
SCADA systems which leverage ethernet TCP/IP communications

This section provides various methods whereby legacy serial communications are converted to leverage ethernet TCP/IP communications links

- **Legacy replacement (e.g. modems replaced)**

  Modems (modulator-demodulator) are devices which encode digital data by modulating an analogue carrier signal. In most cases this is to enable transmission over POTS (Plain Old Telephone Service). SCADA applications and other serial data networks use serial protocols such as DNP3, IEC 60870-5-101/103/104, Modbus RTU, Modbus ASCII, CDC, S/NET, CONITEL, and ABB that are typically transported via modems such as Bell 202 or V.XX type modems over leased or dial tone telephone lines for communications between the central site and remote facilities. In SCADA systems that used serial communications, a separate leased or dial tone telephone line had to be supplied for each modem link to connect the centralised control room computing systems to remote devices in the field.

  Escalating costs from leased and dial line service providers along with limited leased line availability create access problems for SCADA utility and services users. Recurring monthly costs, together with the limitations of legacy modem equipment may limit the expansion and capability of the services which can be supported over these slow analogue lines.

  Such cost and operational constraints have motivated utility SCADA operators to move to newer telecommunication technologies such as Internet Protocol (IP) based data and wireless networks. These are now widely available and offer expanded services and lower recurring costs, provide alternative remote site access and comply with new regulatory standards such as the NERC CIP requirements in North America.

- **Tunnel serial traffic over IP (slowly migrate as hardware permits)**

  **Tunnelling RS-232 over ethernet IP networks**

  With diverse hardware platforms out in the field, rarely can a SCADA system completely migrate from legacy serial communications to ethernet TCP/IP protocols all at the same time. Typically the legacy and modern hardware are run in parallel mode as the system slowly migrates away from the serial protocols.

  In this scenario, technicians would typically install an RS-232 to IP converter at the Master SCADA servers and also out at the remote sites where older legacy hardware does not support a native ethernet port. The serial protocol is essentially tunnelled through the IP network, and the converter out at the field site removes the IP header, footer, and encapsulation information, then passes the original RS-232 serial protocol to the DB9 serial port so that any connected serial hardware would receive the serial protocol as expected.
Securing the move to IP-based SCADA/PLC networks

Figure 13: Leveraging TCP/IP networks to transmit RS-232 serial data over IP

IP-enabled communications to the new upgraded hardware that supports IP communications can be implemented in parallel so that both the legacy serial and new ethernet IP devices can co-exist in the same system.

Definitions for various types of SCADA firewall or gateways

The sample network diagram above shows the introduction of a device entitled the ‘SCADA Firewall’. This device will also be shown in the remaining examples. The purpose of the device is to provide a security gateway or access control point for network traffic desiring to enter, leave or move between networks carrying critical real-time SCADA traffic.

Depending on the level of risk, this gateway device could take on the form of several classes or types of network devices. The table on the next page illustrates several types of typical network gateways which can be used to secure SCADA networks, the ease of deployment, the level of security the device provides, and finally some overall comments on the scenarios when best to use each type of gateway.
### Table 1: Comparison of network gateway devices

<table>
<thead>
<tr>
<th>Device type</th>
<th>Security capability</th>
<th>Ease of deployment / capability</th>
<th>Security assurance</th>
<th>Overall comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch / router</strong></td>
<td>Layer 3 device using VLANs and ACLs (Access Control Lists) to filter traffic based on source/destination IP address and/or source/destination port. Cannot maintain state or perform deep packet inspection of the traffic payload.</td>
<td>EASY: existing network infrastructure devices that have already deployed may have layer 3 separation capability built in, which can eliminate the need to implement new devices. Existing telecom team may be able to maintain the enhanced secure configuration.</td>
<td>Low</td>
<td>Only use in very low-risk environments as ACLs and VLANs can be compromised.</td>
</tr>
<tr>
<td><strong>Firewalls</strong></td>
<td>Purpose-built embedded network appliances which can maintain state as well as performing the same ACLs and VLAN separation as layer 3 switches and routers. Some switching components can be upgraded to have firewall feature set added to the switch.</td>
<td>MEDIUM: new firewall devices most likely needed; new IP networks may need to be created. Specific rules will have to be created for each type of network traffic that must traverse various network interfaces.</td>
<td>Medium</td>
<td>Firewalls are the first level of security appliance that can maintain state for each session. They provide true network isolation and specific rules must be made for each network path.</td>
</tr>
<tr>
<td><strong>UTM Unified Threat Management</strong></td>
<td>UTM devices can perform all of the security features of the switch/router and firewall, plus they can also perform deep packet inspection. They can block traffic when the payload of the network packets are a match on a known virus or exploit signature.</td>
<td>HARD: UTM devices require a greater level of detail during configuration. All the same switching, routing and firewall features must be programmed, and in addition, specific actions can be taken when malicious payloads are detected.</td>
<td>High</td>
<td>If upgrading from a layer 3 device, the UTM is the best choice since it provides the highest level of protection without jumping into the next class of application-aware firewalls. The packet inspection capability can be set to detect and not to block to start.</td>
</tr>
<tr>
<td><strong>SCADA Application-aware industrial firewall</strong></td>
<td>SCADA Application-aware firewalls, also known as Layer 7 firewalls, are programmed to be able to parse the network traffic down to the protocol layer, and can either DENY or ACCEPT traffic based on the SCADA command, such as READ or WRITE data blocks from specific PLC registers.</td>
<td>HARD: to properly deploy Application-aware firewalls the programmer must have intimate knowledge of the process or HMI application. Rules must be made to either block or allow traffic based on the SCADA operator command and the specific area of PLC memory.</td>
<td>High</td>
<td>This class of firewall can lock the SCADA system down to the memory address to only allow network traffic that is required to operate the plant or facility. This class of firewall can prevent a Stuxnet-like attack by blocking data writes to specific PLC memory addresses.</td>
</tr>
<tr>
<td><strong>Data diode</strong></td>
<td>Uses optics to physically ensure that data can only be transferred in one direction.</td>
<td>HARDEST: since data can only transfer in one direction, some protocols that require a connection handshake will need to be tested. The way data is written may need to be altered from a built in API to an SFTP or PUSH type of data transfer.</td>
<td>Highest</td>
<td>Data diodes only allow data to be transferred in one direction. In very high risk scenarios such as nuclear plants and hazardous chemical plants, data diodes can ensure that network traffic cannot pass down to the controllers.</td>
</tr>
</tbody>
</table>

*Figure 14: Table 1: Comparison of network gateway devices*
• **Serial to IP converters** *(convert leased and dial line modems to cellular broadband service)*

With rising costs of lease and dial line service, utility operators are looking for options to replace modems in the field without having to replace any of the hardware, software, or protocol drivers. Cellular broadband services have dropped in price, and several industrial vendors offer a cellular broadband modem that communicates on all major carrier technologies, while still providing a resident RS-232 port for legacy systems. Earlier in this document, the issue of latency was raised with cellular and satellite communications. When considering migration of leased line or modem communications to cellular or satellite options, testing must be done to ensure that the communication performance can still support the real-time requirements of the SCADA system.

---

**Figure 15: Cellular communications for SCADA (option 1)**
Usually, two installation options are found when using cellular broadband modems for SCADA communications. In the first option, the cellular carrier provides static public addresses for each device and uses the internet as the backhaul for connectivity to the field devices.

For some applications where the system is in monitor-mode and can only read from the devices in the field, using this option whereby the carrier assigns ‘public’ static IP addresses to the end points provides greater benefits than the risk.

With the rise in large installation projects involving data acquisition and smart metering, and with the advent of MPLS (Multiprotocol Label Switching), several major international cellular carriers began offering ‘private’ IP networks that leverage cellular broadband as the last mile to the end devices.

**Figure 16: Cellular communications for SCADA (option 2)**
The entry and exit points of an MPLS network are called label edge routers (LER), which, respectively, push an MPLS label onto an incoming packet and pop it off the outgoing packet. The major carriers can drop a wired router anywhere onto the network that acts as the wired MPLS node and configure the remote cellular nodes to operate in the same ‘private’ network.

While the second option is more secure and uses private IP address spaces, VPN (virtual private networks) can be established over MPLS, and there exists two methods for building MPLS VPNs. A layer 3 MPLS VPN, or L3VPN, combines enhanced BGP signalling, MPLS traffic isolation and router support for VRFs (Virtual Routing/Forwarding) to create an IP-based VPN. Compared to other types of VPN such as IPSec VPN or ATM, MPLS L3VPN is more cost efficient and can provide more service options.

However, the carriers do not guarantee the privacy of traffic sent over the MPLS network, and a lot of trust must be placed in the operator of the MPLS equipment to keep the data secure and private along the way. If privacy is a concern, other encryption methods such as end-to-end IPSec tunnels should be considered to encrypt the data at injection points before entering the MPLS backbone.

Another consideration is service level agreements (SLAs). When using telecommunications infrastructure from cellular or 3rd party service companies, SCADA asset owners should be aware that the performance of the system is no longer under their control. Backup communication paths should be implemented to avoid a single point of failure; i.e. the system should be capable of suffering interruptions from the communications provider.

- **Multi-network design** (supports both legacy and IP technology in one network)

IP conversion has spurred the growth of multi-network multiplexors that support multiple network transport interfaces on the same hardware platform. These class of devices typically also support 2 to 6 RS-232 communication ports in addition to ethernet IP interfaces. This allows for the best combination of backward compatibility with legacy serial devices with the ability to connect to the site over multiple network configurations. For instance, at one site the cellular broadband may have a strong signal, so a cellular broadband interface is used on the carrier side of the multiplexor. At the next site, there may already have an existing PSTN or Frame Relay network present, so those interface options would be used. There can be a diverse set of telecommunications options that exist throughout the system, and since the multiplexor devices support both IP and serial protocols, the system can be upgraded over time. Depending on the level of risk, various encryption standards can be implemented over the telecommunication links.
Figure 17: Modernisation in process: legacy and IP devices on the same IP network
Future technologies

Next Generation Networks (NGN) is a broad term used to describe key architectural evolutions in telecommunication networks. The overall concept behind NGN is that one network transports all information and services (i.e. voice, data, video, etc.) by encapsulating these into packets. NGNs are commonly built using the Internet Protocol, and therefore many people describe these NGN systems as ‘all-IP’ networks.

The key difference with Next Generation Networks is a more defined separation between the transport (connectivity) portion of the network and the services which run on top of that transport layer. This means that whenever a carrier wants to add on a new service such as voice-over-IP, Video-over-IP, broadband internet or even cable TV, the new service can be commissioned at the central locations, and new hardware deployed to the consumer, but the network transport or core functioning components of the network do not have to be changed. When considering the use of NGN technology with SCADA and control systems, network isolation and redundancy must be considered.

In terms of isolation, some MPLS and NGN technologies support layer 2 separation. Layer 2 is to be preferred over layer 3 separation because the carrier typically manages layer 3, and the system users must put their faith in the carrier. This concern is valid for existing technology today but may change in the future. Where significant risk is involved, consider using the telecommunications carrier as only the transport layer, and inject encryption before traffic enters the MPLS or NGN system, then decrypt it again on the other side after it comes out of the cloud.

The other consideration is that these Next Generation Networks are carrying non-critical data over the same physical infrastructure as the critical SCADA and control systems network protocols, which means that any failure of the infrastructure due to high network traffic, congestion, or security concerns on the other non-critical functions can impact the reliability and availability of the SCADA and control systems protocols. While this concern is valid for the existing technology today, keep in mind that this particular risk may change in the future.

For higher risk applications, multiple redundant network transport methods should be considered, and in some cases building a private network just for SCADA and control systems communications may be required.
Management of SCADA/PCN IP-based networks

Challenges with the transition to IP networks

Compared with serial channels, IP-based networks can be much more challenging to manage. Since serial channels were designed and implemented with a one-to-one relationship, there was no need to monitor those networks. The technology itself also limited the number of connections. Only those serial nodes with physical access to the same serial channel could communicate on the network, and the protocols did not support routing. It was essentially a closed system.

With routable IP-based communications, threats can come from anywhere, and these networks are much more dynamic in nature. New management activities are now required with ethernet TCP/IP SCADA Systems that did not exist in legacy serial communications. These activities include keeping networked devices up to the latest firmware, providing network access controls to block unauthorised access, and monitoring the use of these devices.

Assigning clear ownership responsibility for the management of SCADA/PCN IP-based networks within an organisation is another challenge. In many cases, the SCADA group uses and operates the network, but other outside groups such as IT, telecommunications or network engineering is responsible for maintaining the network.

Best practices for managing SCADA/PCN IP-based networks

- When managing IP-enabled telecommunication devices, network equipment, PLCs, RTUs, protocol gateway converters, and any other embedded devices, disable any unnecessary services and limit the attack footprint by disabling or blocking unnecessary TCP and UDP ports.
- Limit the use of clear text protocols such as telnet, ftp, and http. Instead, force the use of encrypted protocols, where technically feasible.
- Most IP-enabled telecommunication devices such as switches, routers, firewalls, protocol converters, media converters, and serial terminal servers support SNMP (Simple Network Management Protocol) for monitoring the health and performance of the devices. Ensure that the latest version of SNMP is enabled, and configure the security and performance based alerts to be collected by a SEM (Security Event Management) system.
- Most IP-enabled telecommunication devices such as switches, routers, firewalls, protocol converters, media converters, and serial terminal servers support logging of security events such as denied attempts. Logging should be enabled in such a way that logs are kept resident on the device and a copy sent out to a centralised syslog server. If a SEM is already present on the network collecting SNMP events, then send the syslog information to the same SEM. If the corporate IT group has procedures in place to monitor and review syslog information then consider forwarding the syslog data to the corporate IT syslog server.
Securing the move to IP-based SCADA/PLC networks

In the network diagrams and examples shown in this section, the security levels shown align with the ISA S99 SCADA security architecture model.

Figure 18: Harvesting security alerts and logs off of SCADA system devices
For SCADA and control system networks containing critical components, system administrators should also consider deploying in-line network appliances at choke points performing Network Intrusion Prevention and Anti-Virus, to filter and drop packets which are a known signature match for malicious traffic.

Figure 19: Use of intrusion prevention system (IPS) technology for networks directly upstream of SCADA environments
• Firmware for IP-enabled telecommunications equipment and control devices should be kept up to date within the current patch cycle.

• Control devices such as PLCs, RTUs, Smart Meters, ethernet I/O, and IP-enabled instrumentation should be deployed with a password or PIN code that must be required to make changes to the configuration over an ethernet connection. Based on the level of risk, some devices may be configured to only allow configuration changes over a serial console cable.

• Control devices such as PLCs, RTUs, Smart Meters, ethernet I/O, and IP-enabled instrumentation have known TCP/IP stack vulnerabilities. Switches, routers, firewalls, or any network devices in front of the control devices should be configured with rate limiting commands to restrict data from flooding the device.

• The alerts and logs from network equipment can be either configured to be sent to a SEM (Security Event Management) system and viewed by IT Security staff, or can be translated to OPC tags and viewed by SCADA and Control System operators. Translation software is available to convert SNMP and Syslog data to OPC.

• Whether the network is monitored by IT staff or SCADA operators, responsibility for the care and management of the networks should be clearly defined, and system logs should be reviewed on at least a monthly basis.