ITMR

योगः कर्मसु कौशलम्

WHITE PAPER ON

SCADA Protocols and Security

Prepared by **Mohammed Samiuddin**

Contents

Introduction

Automation is the use of various control systems for operating equipment's. Industries focus on automation because it saves labour and requires minimal human intervention. There are various control systems in the industry, including Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), intelligent field devices, smart meters, and smart equipment diagnostic systems. These systems are common across the industrial infrastructure. They control pipelines, water and transportation systems, utilities, refineries, chemical plants, and a wide variety of manufacturing operations. One of the prominent element which needs attention from a security stand point is SCADA.

The development of SCADA system started when the need for IT-security consisted of protecting physical access to the computers of the system. During the last couple of years, the number of connections to SCADA systems and the use of internet-based controls with SCADA have increased rapidly. Process control and SCADA systems are becoming more reliant on standard IT technologies. They have emerged as vital elements of the nations' critical infrastructure. Having understood the essential nature of SCADA, HTC through its research and development initiative has been working on SCADA security over the years.

Control systems communicate through communication protocols and enable management of remote systems. They have been functionally adapted to Transmission Control Protocol/Internet Protocol (TCP/IP) and other Information Technology (IT).

SCADA systems are now being exposed to a variety of threats and vulnerabilities that were earlier not visible since, performance and availability requirements vastly differ for administrative IT systems and SCADA systems. This white paper outlines SCADA protocols and security status.

Scada Protocol and Security

Scada Protocol

SCADA is classified as the technology which enables user to collect data from one or more distant facilities and/or send limited control instructions to those facilities. SCADA protocols evolved out of the need to send and receive data, and control information locally and over distances in deterministic time. Deterministic in this context refers to the ability to predict the time required for a transaction to take place when all relevant factors are known and understood. Hundreds of SCADA protocols like DNP, MODBUS, CAN, etc., exist today. Some of these protocols are capable of supporting more than just telemetry and control functions. Many RTU-type devices are built around embedded systems, comprising processor modules, analogue and digital inputs and outputs, and communication ports such as EIA-232 and 485 interfaces.

SCADA systems are essentially a centralised communication system where the data server polls each remote terminal unit (RTU) to collect data. A remote terminal unit (RTU) that monitors and controls a production well in an oilfield is connected only with a few sensors at the well it resides. The RTU collects sensor data at pre-defined intervals, and only sends data back when being polled by a central data server. Users can accesses data in one of the two ways: directly connecting to the RTU in the field or reading from the data server in the control room. There is no data sharing and forwarding between different RTUs. Usually these RTUs communicate with the data server. Once SCADA data has been collected by the master station, it can be shared with other control centres using IEC 60870-6 and can interface with Energy Management Systems (EMS), Dynamic Monitoring Service (DMS), and Management Information Systems (MIS) applications using common interface model (IEC61970).

Scada Protocol and Security

Distributed Network Protocol (DNP)

Byte oriented protocols such as DNP3 are used for supervisory and control communications in the electrical power grid domain. This was developed to facilitate communications between various types of data acquisition and control equipment. DNP is a layer two protocol that is used for serial or IP communication between control devices. It provides the rules for remotely located computers and master station computers to communicate data and control commands. This protocol is non-proprietary and uses the term outstation to denote remote computers found in the field. The term master is used for the computers in the control centres. It provides multipexing, data fragmentation, error checking, link control, prioritisation, and layer 2 addressing services for user data.

MODBUS / Profibus

In the late 1970s, Modicon Incorporated developed the MODBUS protocol. MODBUS is positioned in layer 7. The MODBUS protocol defines the methods for a PLC to obtain access to another PLC, for a PLC to respond to other devices, and the means for detecting and reporting errors. Modbus is a request/reply protocol and offers services specified by function codes. Modbus communication interface is built around messages.

Profibus (Process Fieldbus) is an open fieldbus serial network standard for use in time-critical control and data acquisition applications. It falls under the European international fieldbus standard, EN 50 170, and defines the functional, electrical, and mechanical characteristics of a serial fieldbus

CAN Protocol

Controller area network (CAN) protocols (ISO Standard 11898-1) were developed for the automotive industry by Robert Bosch GMBH in the mid-1980s for use in serial communications up to 1 Mbps. CAN supports up to 110 nodes on a two-wire, half-duplex network. CAN communications are based on the Ethernet carrier sense multiple access with collision detection (CSMA/CD) method. With CSMA/CD, multiple devices compete to transmit information over a common bus. DeviceNet is an open standard that is used to connect equipment such as motor starters, sensors, valve controls, displays, operator interfaces, and higher level control computers and PLCs. DeviceNet is based on CAN protocols.

Scada Protocol and Security

IEC 61850 Protocol

Utility Communications Architecture (UCA) version 2.0 is a family of communications protocol aimed at meeting the needs of electric utilities. UCA 2.0 is based on the Manufacturing Message Specification (MMS) from ISO Standards ISO 9506-1:2000 and ISO 9506-2:2000. UCA 2.0 is migrated to IEC Standard IEC61850 for substation automation.

The IEC 61850 protocol is a new standard devised by working group 10 of the IEC Technical Committee 57 which has significantly alleviated the high complexity, time consuming, and interoperability issues in substation automation. IEC 61850 is a virtual protocol which consists of abstract models of data and services.

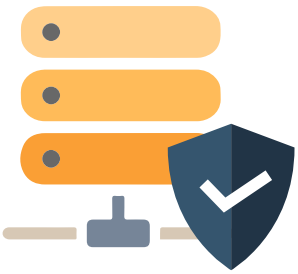
Communication services in IEC 61850 are abstract and model driven. These services are defined by the Abstract Communication Service Interface (ACSI) and are organised in two groups of communication services. The substation information exchanged between IEDs is referred as Pieces of Information for Communication (PICOM), while the path established for transmission of PICOMs is referred as an association.

As IEC 61850 data and services are abstract and cannot themselves provide a concrete interaction between IEDs, they are mapped to concrete communication protocols. These mapping are carried out by the Specific Communication Service Mapping (SCSM).

Current Trends

Today's SCADA systems are often vertically integrated, largely proprietary systems. Interoperability of systems is often limited. While closed protocols and systems might maximise the short-term benefit of systems providers, they limit the ability of the field to grow and constrain innovation by new players. There is an increasing and important trend towards open SCADA protocols, allowing third party tools to manipulate the data.

Automotive manufacturers are exploring in-vehicle automation and between-vehicle safety systems. Safe sharing between vehicles is necessary in such systems to provide cross-vehicle warnings of breaking and collision prevention. If data is readily available in a standard format, third parties could propose energy optimisations and utilities could better understand power usage and potentials to time-shift load.



Scada Protocol and Security

Security Issues

While the prioritisation in traditional information security is CIA (Confidently, Integrity, and Availability) the prioritisation for SCADA systems is AIC (Availability, Integrity, Confidently). Understanding the network architecture of SCADA systems is critical to effectively evaluate their security status. Industrial automation and control represent the traditional use of SCADA systems, and on the surface seem to represent a clear case where data must be protected to preserve competitive advantage. Some typical attacks that might be mounted against SCADA systems which employ standard hardware and software are:

- Malicious code such as viruses, Trojan horses and worms
- Unauthorised modification and manipulation of critical data
- Unauthorised disclosure of data
- Details of service
- Unauthorised access to audit logs and modification of audit logs

Some of the possible SCADA attack targets that would be affected are: oil production which includes those controlling port energy, communications, water, bridges, dams, and pipelines.

Conclusion

Common protocols for data exchange are essential to make wide access to SCADA data possible. Several points in a SCADA system provide opportunities for open access. Different trade-offs arise at each level, from very simple analogue interfaces at the lowest levels to wide area network protocols at higher levels.

SCADA systems are exposed to the same cyberspace threats as any business system because, they share the common vulnerabilities with the traditional IT systems. As such, it is beneficial to formulate and enforce security standards to strengthen the cyber security of SCADA networks.

With the advent of the terrorist threat to the nations' critical infrastructures, SCADA systems no longer have low-visibility, as anonymous entities work silently to control / tamper industrial and commercial operations.

About the Author

Mohammed Samiuddin spearheads the branding aspects & managing client relationships of ITMR. His passion includes speaking on cyber security threats, data security practices and new technological areas.

Reference

John Heidemann and Wei Ye— Towards Full-disclosure: Broadening Access to SCADA Data to Improve Safety, Reliability, and Security

Ronald.L Krutz., Securing SCADA systems, Wiley, 2006

About ITMR

Institute of Technology, Management and Research (ITMR), a division of Mamta Trust, is a premier institute that provides world class professional training programs for the corporates and academic sector. ITMR's motto 'yogah karmasu kausalam' means 'Yoga is excellence in action' and is the foundation of its vision to evolve into a "CENTRE OF EMINENCE" to offer cutting edge vocational skills and mold professionals to become business and technical domain experts. ITMR's professional and corporate training programs include several cutting edge to help working professionals acquire domain expertise and meet the current and emerging challenges in the IT world.

Our flagship training program on Cyber security has PDCIL is a top of the class cyber security program in the country training top officials in the Police departments, Indian and International Banks, Military, Legal fraternity, Fortune 100 Global companies and Blue Chip India IT companies.

ITMR also offers research programs on Cyber Security (network security monitoring and access products), in association with Secure IQ, a leading provider of network security software products with headquarters in Fairfax, Virginia, USA and operations and development in Chennai, India.

Institute of Technology Management & Research

(Division of Mamta Trust)

2/850, Mugaliwakkam Road, Mugaliwakkam, Chennai - 600 125, Tamil Nadu, INDIA.
Admin Office: HTC Towers, No.41, GST Road, Guindy, Chennai – 600 032,
Tamil Nadu, INDIA. Phone: +91 44 4345 3500 / +91 44 4345 3349
Contact for More Information: training@htcitmr.ac.in