

SCADA COMMUNICATION PROTOCOLS

By Andrew West, SCADA Communications Architect, Invensys

Data telemetry and telecontrol systems cover a wide spectrum of industries and needs. Some systems are relatively simple and some are complex. Some have modest needs while some have stringent requirements for data integrity and command validation. This paper looks at the use of some of the current standard SCADA communication protocols and their properties.

DIFFERENCE BETWEEN SCADA AND DCS?

A primary differentiator between a DCS (Distributed Control System) and SCADA (Supervisory Control And Data Acquisition) system is the reason that the system exists:

- In general DCS is focussed on the automatic control of a process, usually within a confined area. The DCS is directly connected to the equipment that it controls and is usually designed on the assumption that it is always available.
- A SCADA system is usually supplied to permit the monitoring and control of a geographically dispersed system or process. It relies on communication systems that can be intermittent. Many SCADA systems for high-integrity applications include capabilities for validating data transmissions, verifying and authenticating controls and identifying suspect data. High-integrity SCADA system applications include electric power transmission & distribution and pipeline monitoring & control systems.

DCS often operates with a "state" paradigm: the system relies on the ability to obtain an immediate view of the current state of the system at any time. SCADA systems in many industries (especially electric power) rely on an "event reporting" paradigm where even transitory or "fleeting" changes in the state of the plant are reported.

In view of this, different messaging protocols and formats are used in different industries and applications. In the DCS arena, the "Bus" protocols (Modbus, FieldBus, ProfiBus, etc.) and a slew of proprietary protocols are prevalent. These are suitable for the requirements of DCS Input/Output (I/O). In the SCADA arena, the most commonly used protocols are DNP3, IEC 60870-5-101, Modbus variants and proprietary protocols. Specific applications also have specific protocols designed to meet their needs. Telecontrol and telemetry are areas where system design is required: There is no single solution that is right for every situation.

ELECTRIC POWER HERITAGE

The standardization process in SCADA communication protocols has been driven by the special requirements of electric power SCADA. This process began with the International Electrotechnical Commission in the later half of the 1980's. IEC Technical Committee 57 (Power System Control and i to look at the standardization of communication between substations and control centres. This committee produced a standard, IEC 60870, in many parts, covering the realm of SCADA communications for electric power control. The first part of the standard was published in 1988 and work on the series is still continuing.

The various parts cover...

- Basic concepts
- Environmental characteristics
- General principles of data integrity
- A three-layer stack architecture
- Data link services
- Application functions
- Data formats
- Application objects

LATEST ADDITION TO STANDARD

One part, a "worked example" profile for an Electric Power SCADA protocol, was first published as IEC 60870-5-101 in 1995. The second edition of this standard was published in February 2003. This new edition is almost twice the size of the first edition and the extra content is mainly explanatory material that clarifies the standard. In 2000, IEC 60870-5-104 was published. This standard describes the transport of IEC 60870-5-101 application data over network transports such as TCP/IP. Specific application standards for electrical metering (60870-5-102) and substation protection devices (60870-5-103) have also been produced. The IEC 60870-5-101 and -104 standards are now widely adopted in Europe and some other regions (notably the Middle East) for electric power SCADA.

While the IEC was progressing with the development of the 60870 series, other vendors, particularly those in North America, were well aware of the power industry's requirement for standardized SCADA communication. Many utilities were aware of the IEC's work and were requesting "IEC compliant" SCADA protocols. Several vendors responded to this challenge by taking the early parts of IEC 60870-5 and providing these as an underpinning to their proprietary protocols. DNP3 (then called DNP V3.00) was one such offering developed by

Westronic Inc., an RTU manufacturer based in Calgary, Canada. A significant distinction between DNP3 and its IEC-compliant contemporaries was that Westronic chose to place the protocol specification in the public domain under the control of a "user's group" in 1993.

The DNP Users Group appointed a Technical Committee in 1995 to assume technical responsibility for the extension and enhancement of the protocol. This strategy gained significant market acceptance in North America.

A specification for using DNP3 over LANs and WANs was published in 1998. As of 2001/2002, virtually every substation automation device sold in North America supports DNP3. DNP3 is well supported in the electric power industry in Australia. DNP3 shares the electric power SCADA market with IEC 60870-5-101/-104 in Asia, Africa and South America.

AUSTRALIAN LEAD

While IEC 60870-5-101 is specifically an electric power-oriented protocol (with specific objects for things such as Transformer Tap Positions, etc), DNP3 is a more generic SCADA protocol. As such it has found acceptance in a wider set of industries, including oil & gas pipeline control systems and water & wastewater systems. Australia leads the world in adoption of DNP3 for water and wastewater SCADA. In an unusual departure from the European norm, IEC 60870-5-101 is used in the UK for electrical transmission SCADA, but DNP3 is often used for distribution SCADA because of its capability to make efficient use of multi-drop radio communication networks.

All the other SCADA protocols are now relegated to "also ran" status in the electric power SCADA protocol race. The September 2002 Newton-Evans report on the electric power market reported that DNP3 was the most used protocol within substations in North America (52% of utilities), followed by Modbus Plus (31%). Between the substation and the control centre, DNP3 serial is in use at 32% of utilities; DNP3 over LAN/WAN (TCP/IP or UDP/IP) is in use at 19%. The next highest groupings are "other TCP/IP" at 9% and Modbus Plus at 6%. The majority of existing systems use one of the many legacy proprietary protocols. DNP3 on serial and LAN/WAN transports remains the most specified protocol in North American Electric Power for new and upgrade installations.

ANALYSIS OF THESE PROTOCOLS

Both DNP3 and IEC 60870-5-101 serve similar functions. They both:

- Reliably and efficiently transfer field data (including information about transitory events) to the master station
 - Allow commands to be issued to the field with a very high degree of control security (verification and rejection of errors) by using the high-integrity select-before-operate command strategy
 - Suit medium bandwidth communication channels (e.g. 9600-baud serial connections)
 - Include good data link frame integrity checking
 - Support application layer data object identification
 - Include data validity checking flags
 - Support the transmission of digital (on/off) and analog data (in integer or floating-point formats), counters and digital and analog control commands or setpoints
 - Support transfer of files, setting of clocks, etc.
- IEC 60870-5-101 also supports some electric power specific objects related to transformers and substation protection devices.

The protocols support the transfer of "report-by-exception" (RBE) where only changes in field data are reported. RBE improves the efficiency with which data can be transferred under "normal" conditions. The protocols are also capable of transmitting data with millisecond-resolution timestamps, allowing accurate identification of the sequence of actions in the field. These event-reporting capabilities are useful for accurate analysis of power system events. They are also useful in other industries (such as pipeline or water monitoring systems) where relatively

infrequent scanning can be used to recover an audit trail of field activity.

DNP3 supports an "unsolicited reporting" mode where a field device can report events without being polled by the master. Unsolicited reporting can be very useful for a large electrical distribution network where (for example) pole-top reclosers can report activity on a shared radio bearer without being polled. IEC 60870-5-101 also supports an "unsolicited" reporting mode, but only with a dedicated point-to-point communication channel-unlike the DNP3 model that can support unsolicited reporting on multi-drop communications channels.

SPECIFICATIONS

As evidenced by the newly-released edition of IEC 60870-5-101, work is still going on to improve these protocols. The DNP3 Technical Committee has published a series of Technical Bulletins since 1995 that contain clarifications and extensions to the protocol. The DNP3 protocol specification is presently being updated to incorporate this material. The new specifications are due for publication in 2003/2004.

Standardized conformance testing has boosted the end-user's confidence that devices from different vendors will work together. The DNP3 Technical Committee first published a conformance test for outstation devices in 1998. It is presently developing test procedures for master stations. The IEC working group is currently preparing test procedures for IEC 60870-5-101 and -104.

Other development work continues in SCADA protocol standards today. Current

work items on both committees' lists include:

- Improved security (especially validation of authorization of control commands)
- Configuration definition (machine readable/automatic configuration) to simplify system integration

WHAT'S NEXT?

The IEC 60870-5-101/-104 and DNP3 protocols were purpose-designed for their SCADA roles. They probably have a service life of another 15 to 20 years. It is not yet clear what will replace them. The IEC 61850 substation automation protocol might take over their role. Much could depend on a revolution or evolution in communications bandwidth and processing power. The trend for expansion of SCADA applications to collect field data for corporate IT systems will have an impact on system requirements. The future seems to promise greater integration and data sharing between devices with less manual configuration effort.

CONCLUSION

There definitely are standards for SCADA communications. Some of the protocol standards that are commonly used in electric power SCADA have been discussed here. Electric power SCADA usually imposes more stringent requirements than other industries; thus some of the issues mentioned above may not be applicable everywhere. Adhering to standards generally results in more flexibility, vendor-independence, cost savings and a degree of "future-proofing". As always, it is up to the end user to decide how important they are in any particular application.