ABSTRACT for the 2018 ISA WWAC Symposium

Beyond Modbus

Designing SCADA with Other Open SCADA Protocols

Jacob Brodsky, PE

Jacobs, National Security Solutions
6716 Alexander Bell Drive
Columbia, MD 21046
Email: Jacob.Brodsky@jacobs.com
Phone: 443-285-3514

SUBMISSION TYPE

___ 30 minute presentation

_X_ 6-12 page paper plus 30-minute presentation

___ 3 foot wide x 4 foot high large format poster

KEYWORDS

SCADA, ModbusTCP, ModbusRTU, DNP3, IEC 60870-101/104, OPC-DA, RTU, Event-Oriented, Security

ABSTRACT

SCADA systems tend to grow exponentially. Water Utility experience over the last 30 years shows that, in a manner similar to Moore's Law, the point count from the field doubles approximately every five years. Unfortunately, real time protocols such as Modbus require polling rates at the Nyquist limit or better to report from the field without gaps or lost information. Thus every doubling of the point count causes a doubling of bandwidth costs. Event oriented SCADA protocols do not need to poll this frequently and offer improved time resolution, at the cost of additional complexity in the Alarm and Historian systems.

Advantages of event oriented SCADA include the possibility of recovery from telecommunications outages of up to several hours or more without loss of data. In addition, it may offer lower bandwidth costs (a concern where bandwidth costs are a factor).

Event-oriented protocols can have problems with OPC-DA mapping to what is essentially a real-time interface. Methods of dealing with remotely time-stamped events, where the event and time of arrival are significantly different, will be discussed.

With event oriented systems one can push many calculations to the field RTU. This is enabled because the RTU is required to be aware of the time and sequence of events. For example, totalizers and volumetric calculations can be reported precisely every fifteen minutes with very minimal overhead. These features could be mapped to Modbus, but because they're not standardized, it wouldn't be portable through system upgrades.

Advantages and disadvantages of migration from Modbus will be presented as a summary.

ABOUT THE AUTHOR

Jacob Brodsky, PE: *After 31 years doing everything ICS and SCADA from the Instrumentation to the Historians and servers at the Washington Suburban Sanitary Commission; Ten Years on the DNP3 Technical Committee, Co-Authoring and Co-Editing two editions of a Handbook on SCADA/Control Systems Security by CRC Press, and co-founding the SCADASEC e-mail list; it is possible that Jake might know something about SCADA security and design. Jake is a Professional Engineer of Control Systems, registered in the State of Maryland; and a Senior ICS Security Engineer for the National Security Solutions of Jacobs.*