A Case for Object Based Security Protocol Standards

David Green, DAQ Electronics, Inc.
ANSI Perimeter Security Summit May 17,2005

DAQ Electronics was founded in 1975 by 5 engineers with experience in the Supervisory Control and Data Acquisition (SCADA) field. SCADA deals with the monitoring and control of sensors and devices over a geographically dispersed area. Typically, different types of utilities, i.e. Water, Gas. Oil, Communications, and Electric will use a SCADA system to remotely monitor and control the various locations of their systems.

The majority of DAQ's business came from selling Remote Terminal Units (RTUs), the devices that physically control and monitor the remote locations, to the Electric Utilities.

The experience that SCADA brings to DAQ's security products are related to dealing with difficult communications infrastructures and providing complete user configurability of the system. It is not uncommon for a SCADA system to support hundreds of stations over 1200 baud telephone circuits. Also, electric utilities have clear and exacting requirements of their needs. If an open breaker needs to be presented on the screen as flashing green with pink polka-dots that is what you must to provide them. As a result, every facet of the user interface in DAQ's system is configurable for look and feel. Finally, Electric Utility SCADA has many intelligent devices that must be brought into the system via various communications interfaces and protocols. All of DAQ's products inherently support this type of functionality.

As DAQ explored avenues for growth, it determined that Physical Security systems, remotely monitoring and controlling a geographically dispersed set of Security sensors and information, presented an interesting parallel to the SCADA market. In the early 1990's, DAQ created Security hardware and software for integrated Intrusion Detection, Access Control, and CCTV systems. The product had so many advantages from its SCADA background that the first system ever sold was to the Pentagon.

It is interesting watching the technology of the Security Market evolve and seeing how it parallels obstacles and solutions in the Electric Utility SCADA market, that have led to the creation of beneficial communications standards. In a typical substation, an RTU will have to monitor physically connected inputs, such as Switches, Voltages and Currents, and communicate with other intelligent devices in the station, such as Meters and Relays, that also provide SCADA data. Add in to the mix that some of the data needs to be treated as real time, while other data may be more historical or analytical in nature.

The retrieval, organization, and distribution of the data is not simple. Many of the intelligent substation devices use unique legacy protocols for the sharing of data, and much of the data needs to be sent to different places. Additionally, almost all of the information uses discrete point numbers, with no linkage to the actual device with which it is associated.

Voltage 1 might come from Breaker number 1 while Voltage 2 may come from Breaker number 5. What this means, is that in order for a system operator to see the information in an intelligible way, significant configuration time must be spent matching the discrete I/O points with the devices with which they are associated.

To deal with these complexities, the industry began to create standards. The first standards simply created common protocols and languages for moving discrete data between devices. These protocols have been in effect for a number of years, and have saved utilities great time and money on integration, as well as allowing them more choices for equipment, as many devices are now plug and play. However, these protocols have done nothing to help with the significant configuration aspects of linking individual points back to a specific device.

The next step is that the industry is devising standards to create data object definitions. These definitions allow a device, for example a Circuit Breaker, to be defined as to exactly what types of data it contains (i.e. 3 Voltage, 3 Current, 1 Power, 1 Open/Closed, etc.). With this scheme, data can now be moved as a grouping (i.e. data for Circuit Breaker number 1), eliminating the need for configuration and linking at each end.

The parallel in the trends of the Security market and particularly in Perimeter security are interesting. A perimeter security environment deals with many different types of sensors and data. This can include conventional motion, infrared and fence protection contact closure sensors, intelligent communications based Chemical, Biological, Nuclear, and Explosive detection sensors, and visible and millimeter wave camera and radar streams.

Let's take the challenges associated with a theoretical example, and look how it would be handled today, versus how forward reaching communications standards would be a benefit.

Assume a large perimeter fence extending for several miles. The fence has camera coverage and sensors to detect and assess incidents, including explosive detection and radar in 200 foot increments. Additionally there is a flood light that can illuminate when an event occurs. The cameras operate on their own private coaxial system, and each control panel handles the I/O for 3 sections of fence.

For starters, each device that supports serial or IP communications must have a protocol "driver" written in the Control Panel so that the data can be understood. In our example, the control panel will communicate with the radar and explosive detection sensors, each using a different serial protocol. If more devices are added, more protocols may be required, that may result in additional development charges to the end-user. With a standard protocol, all devices on the system become plug_and_play. Any control panel can communicate with any intelligent sensor, and even with any Security front end.

The next level of complexity is the presentation of the information to the Security guard. When an event occurs, the operator needs to be presented with the appropriate information on the screen, including the alarm, the correct aerial view or graphic, and a

live video feed of the appropriate camera. This is a flexibility present in all credible security systems, but integrators know that it takes a significant amount of keyboard time to make this happen.

The complexity arises from the way that the data is organized and transmitted to the front end. The protocols used today in most systems use discrete point numbering schemes with messages equating to "SENSOR 1 IS ON, SENSOR 2 IS OFF", with no information at all about where sensor 1 and sensor 2 come from. The integrator must know this and enter the data appropriately at the front end.

An alternative approach is to devise protocols that allow for the definition and creation of data "objects". In our example, an object might be a 200 foot section of fence. A Fence Section Object contains a Radar, an explosive detector, a camera, and a flood light. Now a protocol message can take the form of "THE DATA FOR FENCE SECTION 1 IS……." All the master station has had to be told is the definition of what a Fence Section Object is, that there are 6 of them, and what they are named. The discrete I/O points are no longer important.

It is difficult to convey all of the benefits of protocol standards, particularly those that are object based, in such a short amount of space. However, it should be evident that time and money can be saved for everyone as movement towards such a platform is made.