Communicating the Semantics of Resources in Networked Control Systems

Jim Butler (jimbutler @ cimetrics.com)

Cimetrics Inc., Boston, MA

Keywords: Smart Grid, information model, semantic interoperability, control systems, network protocol design.

Abstract

Several organizations are developing information models for the Smart Grid that are intended to improve semantic interoperability between devices, systems and applications that need to exchange information. Future systems should have the capability to describe the semantics of their network-visible resources in an interoperable way using those information models. This paper introduces several methods that devices and systems could use to describe the semantics of their network-visible resources, with an emphasis on methods that could be applied to existing networked control systems.

1. INTRODUCTION

The term "Smart Grid" refers to a future electrical grid which makes use of information technology to operate in a way that is smarter than the electrical grid that was developed throughout the 20th century. The Smart Grid in North America will rely upon a greatly increased flow of information within and between the multitude of systems that control the generation, transmission, distribution, storage, and consumption of electricity.

Realization of the potential benefits of the Smart Grid will require interoperability, which the GridWise Architecture Council (GWAC) has defined as follows: "The capability of two or more networks, systems, devices, applications, or components to exchange information between them and to use the information so exchanged." [1]

There are various aspects to achieving interoperability within an electric power grid, as described in the GWAC's "GridWise Interoperability Context-Setting Framework" [1]. The framework defines a number of interoperability categories (e.g. syntactic interoperability) and cross-cutting issues (e.g. discovery and configuration) which have proven to be valuable in discussions among participants in Smart Grid related technical activities in the U.S.

Of particular relevance to this paper is semantic interoperability, which requires that communicating parties share an understanding of the meaning of the data being communicated. One tool for achieving semantic interoperability is for the communicating parties to share one or more information models. Formal information models are typically defined using a modeling language such as UML. Prominent among the information models used in the electric power industry is the Common Information Model (CIM), which is defined in certain IEC standards. ASHRAE and NEMA are jointly developing the Facility Smart Grid Information Model (FSGIM) with the intention of making it into a standard [3].

Achieving semantic interoperability is often one of the major challenges when existing systems are integrated in the "real world". In this author's experience, it is often difficult (and expensive) to determine what the underlying information model is. It would be great if systems could do more to help us to understand what their data means.

This paper examines various methods that control systems could use to communicate the semantics of their network-visible resources in an interoperable way. Potential consumers of that information include system integration tools and applications that analyze system performance.

Although emerging standards offer the promise of improving how future systems interoperate, it is essential that we think about how can enhance our existing systems and network protocols, because they are likely to be with us for a long time.

2. NETWORK PROTOCOLS FOR CONTROL SYSTEMS

Networks are often used within distributed systems in order to enable control and monitoring applications. Substation automation and the control of HVAC equipment within facilities are two such applications that are relevant to the Smart Grid.

Many network protocols designed for control applications have been developed. These protocols are typically designed to achieve syntactic interoperability, network interoperability, and basic connectivity (as defined in [1]). Some protocols contain mechanisms that are intended facilitate semantic interoperability; however, the burden of ensuring semantic interoperability ultimately falls on the engineers and technicians that design and configure systems.

Before we consider the general problem of enhancing existing systems to better support semantic interoperability, let's look at two popular open protocols that are widely used in control systems within commercial and industrial facilities.

2.1. Modbus

The Modbus protocol [4], which was originally designed in the late 1970's by Modicon for industrial control applications, is an example of a network protocol that was not designed to facilitate semantic interoperability. Modbus's data model contains tables of network-addressable registers (16-bit values), discrete inputs (1-bit read-only values) and coils (1-bit writable values) that can be read and, in some cases modified, by Modbus client devices. Engineers have made use of Modbus registers in some creative ways, such as combining two adjacent registers to form 32-bit floating-point numbers.

Manufacturers of application-specific devices that support Modbus typically publish a document containing a "register map" that details how the Modbus registers are used to provide network-accessible functionality in a particular device. For example, the manufacturer's documentation for a popular power meter states that the measured line frequency can be calculated by multiplying 0.01 by the 16-bit integer value read from register 4013.

In general, Modbus devices do not describe their own data in any meaningful way. This is not to say that it is impossible to accomplish using Modbus, but in the absence of accurate documentation, it is almost impossible to determine how to interact with Modbus devices.

2.2. BACnet

BACnet [2] is a protocol designed for building automation applications that was first approved as an ASHRAE standard in 1995. It is primarily used within HVAC control systems designed for large commercial and industrial facilities, but many manufacturers of lighting control systems have added support for BACnet to their product lines in order to facilitate integration.

BACnet uses objects as containers of network-visible data. A BACnet object contains a set of properties, each of which contains some data that can be read and, in some cases, modified by other devices using standard network services. A number of standard object types have been defined; some object types are used to represent physical I/O devices, and others are designed to facilitate trending, scheduling, and alarming. One example is the Analog Input object type, which is typically used to represent an analog sensor.

BACnet objects can make their semantics visible to a certain extent. Table 1 shows an example of an Analog Input object (with some properties omitted) that represents an air temperature sensor that would typically be placed in a room; note that the object includes the engineering units and an English-language description of what the object represents.

Table 1 - Example BACnet Analog Input object

Property	Value
Object ID	Analog Input, instance 3
Object Name	ZoneTemp
Description	Measured zone temperature
Present Value	73.0
Units	Degrees F
Min. Present Value	32.0
Max. Present Value	122.0
Reliability	No fault detected

The presence of the metadata properties in BACnet objects has been a contributing factor in BACnet's success, but there are currently no standards on how to use those properties. Some building owners have developed their own best practices for how BACnet objects are to be configured within their systems, but the quality and utility of the metadata in existing BACnet systems varies considerably.

3. MECHANISMS FOR COMMUNICATING SEMANTICS

The standard information models being developed for the Smart Grid are intended to improve semantic interoperability. These models provide a useful abstraction, but it is also necessary to consider how these abstractions will be implemented in control systems.

In particular, how can the semantics of network-visible resources be communicated to applications or devices that wish to use those resources? Can we establish clear relationships between the abstract definitions contained in information models and network-visible resources? How should we handle existing systems and network protocols?

It is unlikely that there will be a single solution that will work well in every situation. With that in mind, let's look at several possible mechanisms that can potentially be applied to existing control systems.

3.1. Structured Documents

Perhaps the most straightforward way to communicate semantics of network resources would be to describe the resources in a structured document with a well-defined format. Such a document could contain items that map onto a standard information model, with instructions on how to access the required data from a particular system. Ideally these documents would be automatically generated by system configuration tools or perhaps by the networked devices themselves.

This general mechanism could potentially be used with systems that have little self-descriptive capability, such as Modbus-based systems, although the structured documents might have to be communicated using a protocol other than the one being used for communication within the control system.

3.2. In-band Mechanisms

Some network protocols can be extended so that semantics of network-accessible resources can be communicated within the protocol itself. Here are some of the possible mechanisms that could be considered.

3.2.1. New Object Types

For network protocols that are under active maintenance, it may be possible to develop new object types that directly map onto data structures defined in an information model of interest.

For example, the FSGIM is expected to define four major components which are constructed using abstract classes. A protocol like BACnet could be extended to include one or more new object types that are specifically designed to represent the functionality of certain FSGIM classes that cannot be easily modeled using existing standard object types [3]. Note that a one-to-one mapping between abstract classes and object types might not always be practical or desirable.

One disadvantage of this mechanism is that the software running in existing systems would have to be upgraded in order to take advantage of the new object types.

3.2.2. Semantic Tagging

Semantic tagging is being widely discussed as a method to improve the functionality of the World-Wide Web.

In its simplest form, semantic tagging involves the selection of one or more attributes (tags) that describe some data; for example, a photograph of a cat sitting in a chair (or a reference to such a photo) could be tagged with "cat", "chair" and "photograph". However, it is often necessary to qualify semantic tags in order to reduce ambiguity; for example, "Australia" could refer to a nation or to a recently released big-budget movie.

The idea of semantic tagging seems be most practical in situations in which it is possible to define a standard vocabulary for a limited domain of knowledge; fortunately there are many Smart Grid related applications that satisfy this criterion. The idea of defining standard sets of semantic tags that are directly derived from Smart Grid information models might be worth exploring.

In some protocols, semantic tags could be directly "attached" to network-visible resources. For example, in BACnet, semantic tags associated with a particular object could be placed in a designated property within that object.

3.2.3. Directories

Directory services allow applications to locate network-accessible resources. In some protocols, these services permit resources of a certain type to be enumerated and descriptive tags to be associated with each resource.

4. CLOSING THOUGHTS

The cost and difficulty of integrating systems is one barrier to achieving a smarter grid. Projects aimed at improving semantic interoperability through the development of standard information models will directly affect the design of new protocols and interfaces, but we must also consider how these information models can be applied to existing systems and network protocols.

References

[1] GridWise Architecture Council, "GridWise Interoperability Context-Setting Framework, v. 1.1," 2008.

[2] “BACnet: A Data Communication Protocol for Building Automation and Control Networks," *ANSI/ASHRAE Standard 135-2010*.

[3] Bushby, Steven T., “Information Model Standard for Integrating Facilities with Smart Grid”, *ASHRAE Journal*, November 2011, pp. B18-B22.

[4] “MODBUS Application Protocol Specification V1.1b,” Modbus-IDA, 2006.

Biography

Jim Butler is CTO of Cimetrics Inc., a company that focuses on improving the performance of commercial and industrial buildings through remote, ongoing monitoring and data analysis. Cimetrics is also a leading provider of BACnet communication products to the building controls industry.

Jim has been actively involved in the design and implementation of communication protocols for distributed control and monitoring systems. Jim has contributed to the development of the BACnet standard since 1994, and he currently leads the BACnet committee's IT working group. Jim served as the first manager of the BACnet Testing Laboratories, which coordinates the conformance testing of products that implement the BACnet standard. He is a currently a member of ASHRAE SPC 201P (Facility Smart Grid Information Model).