# Sempra Energy Utilities

**Terry Mohn**
San Diego Gas and Electric
Sempra Energy
mmohn@SempraUtilities.com

Stakeholder education and higher risk profiles are vital to successful interoperability standards adoption – a white paper regarding GWAC's Interoperability Framework.

Interoperability specified in a public forum, such as standards bodies, is the best way to ensure product evolution, viable competitive markets, innovation and long-term cost controls. Viewed holistically, utility systems that adhere to common standards weather age and abate obsolescence best. Innovation thrives even as assets age due to the fact that parts are interchangeable, even though the entire system remains essentially unchanged. Yet, utility systems are complex; not limited to classic application software, but rather include large and small devices, nodes if you will, at the edge of the network.

As we descend the GWAC framework layers, the effort becomes increasingly more difficult to adhere to standards without accepting tradeoffs in other areas. High level abstraction, particularly while modeling and outlining architecture, is much more conducive to prescriptive interoperability requirements. I posit that as we peer lower into the framework stack, approaching product implementation, the challenges conforming to interoperability standards becomes increasingly more difficult and costly for first movers. This argument does not condone disregard for interoperability, rather it highlights the need for sound analysis of the consequences of delving too deeply into detailed interface specifications.

For example, in California our state building code standards department has declared that beginning 2009, all new HVACs installed must be controlled by programmable communicating thermostats (PCT). These thermostats must register with a load serving entity and respond to demand control and reliability events. As architects, we can immediately visualize the system architecture: application, headend controller, transport, data interchange, radio card, thermostat, and display.

We can quickly list the interface points between various systems and prescribe data and physical standards that must exist to enforce interoperability. One particular challenge rises as we descend deeper into the design of the communication device within the PCT. We certainly can specify the physical connection between the radio card and the PCT chassis. We can also easily specify the data exchange between these components. There will be a point where interoperability boundaries are no longer prescriptive, though, if we consider these devices are asked to operate over many years. The challenge will be to decide when specifications are "complete enough" to satisfy the benefits.

Consider our desire to specify the security model between the controlling system, the central energy management system, and the endpoints (PCTs). It is our desire to use industry standard public key infrastructure with a high level message cryptographic techniques, such as AES-128. Manufacturers understand these requirements and can build the computing and memory components into the radio portion of the PCT. Now, the added complexity is this system must remain in effect for 20 years. How do we deal with the fact that in five years, AES-128 will be broken by a Zigbee communicating Timex watch?

It is a fact that interoperability allows us to change out the aging asset.  Suppose we want to avoid rolling a truck, a customer service call, to all homes and replace all PCTs.  One suggestion to lower the replacement cost is to transmit software changes over the air, basically a firmware upgrade while the system is running.  This is all well and good, but the manufacturer now must consider higher initial production costs to accommodate unknown future software changes.  Therefore, several factors are affected by our desire to retain assets for a longer period of time: memory, MIPS, power factors, etc. How much flexibility must the manufacturer build into the device to accommodate these needs?

If the manufacturer had chosen a non-standard approach, perhaps the security attack vectors would have been smaller, thereby requiring less likelihood of accommodating firmware upgrades.  It appears that in order to accommodate a high degree of flexibility and future innovation, initial device costs are higher.

As stewards of design for a new paradigm, one that embraces flexibility through interoperability, our industry requires us to educate all stakeholders to the fact that there are potentially negative short-term consequences to this vision.  The market leaders, those who provide products first in the market, are likely to incur higher manufacturing costs than those who follow later.

Our responsibility is to assist the market in building these “first mover” products.  This can be achieved in a number of ways, but particularly: 1) support and invest in applied research so that we can uncover the consequences early in product design; and 2) as we issue RFPs, the utility industry is collectively responsible to adhere to the same specifications where possible.  As we independently require certain standards within our requirements documents, we need to ensure we are consistent with a majority of our utility colleagues.

In addition to providing the degrees of interoperability, this group has a duty to continue educating and supporting early adopters.  For a risk-averse industry, this is probably a larger challenge than writing the requirements.