Testimony of

Rik Drummond

SGIP Board Member and
Chair of SGIP Testing and Certification Committee

Drummond Group Inc
Fort Worth, Texas

Before the

House Committee on Science, Space, and Technology
Subcommittee on Technology & Innovation
United States House of Representatives

on

"Empowering Consumers and Promoting Innovation through the Smart Grid"

September 8, 2011

Contents

Introduction

Chairman Quayle and Members of the Subcommittee, I am Rik Drummond, CEO of *Drummond Group Inc*, a testing and certification server provider. I am a board member of the NIST sponsored *Smart Grid Interoperability Panel* and the Chairperson of the *Smart Grid Interoperability Panel's Testing and Certification Committee*.

Thank you for the invitation and opportunity to appear before you today to discuss *Drummond Group's* involvement in Smart Grid testing and certification as well as the *Smart Grid Interoperability Panel (SGIP) Testing and Certification Committee's (SGTCC)* endeavors to solve Interoperability issues in Smart Grid products and services. I will focus on our accomplishments, our direction, and some of the key items needed to ensure protection of consumer privacy and the maintenance of cost/benefit for current services, while driving innovation within Smart Grid development.

1. Drummond Group Activities, Testing Challenges

A – Describe Drummond Group activities related to testing and certification of smart grid technologies and modernization of the electric grid

Drummond Group has been heavily involved in the Smart Grid since 2004, when I became the initial Chair of the DoE sponsored *Smart Grid Architectural Council* in 2005-2006. *Smart Grid Architectural Council* was the initial group to start socializing the need for general Interoperability among software and hardware to solve the known and projected problems on the USA Power Grid as we moved to the Smart Grid.

In 2009 *Drummond Group* was selected as the Interoperability Specialist subcontractor to the *Center for Commercialization of Electric Technology* (CCET) on "Discovery Across Texas: Technology Solutions for Wind Integration in ERCOT DE-OE0000194."

Drummond Group continues to work with CCET on this endeavor. We are currently focused on the third party privacy issue for shared information for the purpose of enhancing the consumer experience in the Smart Grid. The focus is on third party providers that help the consumer manage their

electrical power consumptions more effectively and efficiently while ensuring existing privacy rules and regulations are implemented.

I am on my second term as chairman of the NIST sponsored *Smart Grid Interoperability Panel Testing and Certification Committee* (SGTCC). I am also on my second term as a board member of the *Smart Grid Interoperability Panel*. Our focus this year in SGTCC is: 1) Speeding the off-the-shelf productization of standards based interoperable products in the market place, 2) increasing the consistency of interoperability testing and certification services across all products implementing the 100+ technical standards used to integrate the Smart Grid systems, and 3) decreasing the cost to service providers and consumers in implementing and integrating products within their portions of the Smart Grid network.

SGTCC released the initial voluntary interoperability policies and procedures in December 2010, nine months after the kick-off working meeting of the SGIP in March 2010. These voluntary, predominantly ISO9001 based policies and procedures are enshrined in the SGIP's "Interoperability Process Reference Manual" version 1 (IPRM). We are currently working on the release of version 2. This second version will increase clarity, fill in gaps identified by the six initial users of the Manual and streamline the implementation process by the testing and certification community. Version 2's anticipated released date is January 2012 for general use by the Smart Grid culture. While the focus of the IPRM is to enhance interoperability in products based on a single standard, there are interoperability issues the IPRM will not solve. It will not solve those issues of integrating multiple products, based on multiple standards in support of a service provider's workflow or technical or business process. An SGIP workgroup exists to solve these issues which are currently called internally, for lack of a better name, *End-2-End Testing Workgroup*.

End-2-End Testing normally takes place in the pre-production roll-out of Smart Grid infrastructure by the Transmission and Distribution Service Providers (TDSP). Many suppliers of electricity, Transmission and Distribution Service Providers, generally, repeat in a large degree, the end-2-end testing and integration verification that was previously accomplished at other service providers. Of course, there are differences in the configuration of products between service providers, but SGTCC believes that commonalities far out weigh the differences. The focus of our *End-2-End Testing Work Group* is to facilitate the sharing of these test data results and

techniques to speed the implementation of new technologies and services across the Smart Grid. The thinking is: since another Service Provider has already accomplished it, why not leverage their findings to facilitate integration in one's own network area?

B - What are the greatest technical challenges of testing and certifying Smart Grid technologies in the market with few standards in place to support interoperability?

Article by Drummond: **How the GridWise Interoperability Framework Can Save Time and Money**

Coming to Grips with a Definition

Smart Grid interoperability means different things to different people. Some view it as a low-level technical topic. Others view it as a standard with an obscure name. Both are components of interoperability, but there are many other aspects.

The GridWise Interoperability Framework aids the discussion of those many aspects by breaking the problem into bite-sized pieces. This article is the first in a series that will explore each aspect in more detail. The goal is to clarify interoperability and to determine what needs to be agreed upon so that systems can play together with the least amount of effort and cost.

Wikipedia's definition of interoperability is: "the ability of diverse systems and organizations to work together (inter-operate). It further states that "the IEEE defines interoperability as: the ability of two or more systems or components to exchange information and to use the information that has been exchanged." It is interesting to note that Wikipedia says the term can be used technically or broadly in a way that takes into account "social, political, and organizational factors that impact system to system performance."

Anyone that has observed interoperability efforts in other industries can confirm that social, political and organizational factors have at least as much impact as purely technical issues! Past decades have witnessed interoperability conflicts over things such as Betamax vs. VHS, HD vs. Blu-Ray, systems-oriented architecture (SOA) and (just now beginning) iPhone vs. the Google mobile phone standard. For every battle that shows up in the

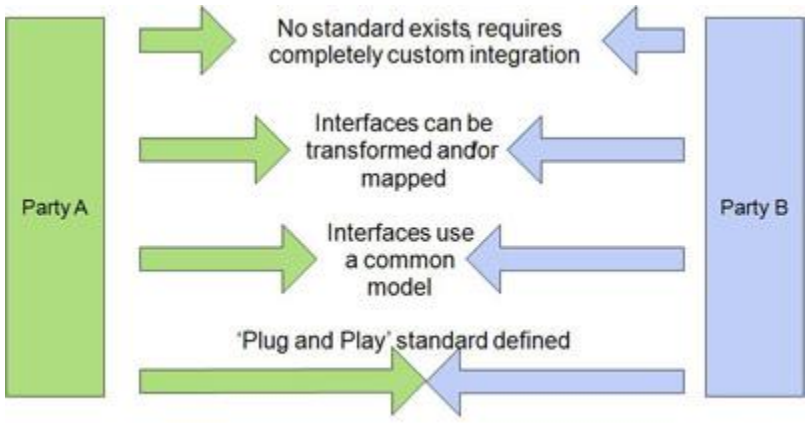
headlines, there are dozens of others known only to insiders, but with similar consequences: delay, confusion, higher costs and higher risks for end users.

The Expanded GridWise Definition

The GridWise Interoperability Framework exists to minimize that kind of pain and delay. It adds to previous definitions of interoperability with the following characteristics:

- An exchange of meaningful, actionable information between two or more systems across organizational boundaries.
- A shared understanding of the exchanged information.
- An agreed expectation for the response to the information exchange.
- A requisite quality of service: reliability, fidelity, and security.

There are many paths to interoperability. They range from expensive, custom integration projects to plug-and-play architectures. Scott Neumann describes this variability as the "distance to integrate." (See drawing.)



As an illustration, the flash drive in your pocket is a plug-and-play device. It conforms to the USB specification as a specific type of USB device, which is recognized by the operating system to have specific properties and behavior. If the flash drive does not conform to these specifications (or if the correct device driver is not installed in the operating system) then plug-and-play becomes plug-and-*pray* or plug-and-*slay* (as in urge to kill).

The Four Levels of Interoperability

Plug-and-play (at the bottom of the drawing) is usually reserved for interfaces in wide-spread, commodity use. Product interchangeability is supported by rigorous specifications and strenuous testing. The high cost of

achieving this level of integration requires a large market to apportion the costs.

The next level (second from bottom) involves systems that use a common information model but with differing technical transports, transaction sequences and data encoding. Integrating such systems requires time and effort – but at least they are talking the same language. System design, software development and testing at the information level are still needed, as they are for the underlying technical transports and data encoding. As the GridWise Interoperability Framework reminds us, interoperability means all layers must work together from technical to informational to organizational.

At the next level up, some interfaces use different information models and the data must be mapped or translated before it can be used. Think about currency and exchange rate. If you know the exchange rate between the US and France then it's easy to map dollars to francs.

If such translations are not available, then you are at the top-most level and it's time to pull out the checkbook. The old adage applies: "Anything is possible with software, given enough time and money." There is a thriving systems integration market for providing custom (and costly) interoperability solutions. Money can either be spent each time an end-user attempts to integrate or on a one-time interoperability/conformance test at the product level. It typically costs much less to do a one-time interoperability/ conformance test at the product level.

Now that we understand the definition of interoperability and the distance to integrate, we can start implementing specifics for the Smart Grid.

2. SGIP – Represents Testing and Certification Vendors

A - Describe the process of testing for conformance and Interop.

Article by Drummond: **Six Steps to Achieve Interoperable Networks, Systems, and Devices in the Smart Grid on any Standard**

Conformance is not Interoperability

The program must clearly convey the different meanings between conformance of an implementation to a standard, and interoperability between two or more implementations of the standard. Confusion regarding this aspect is currently a major hindrance to the success of conformance and interoperability programs. This misunderstanding of the differences between conformance and interoperability in the marketplace, testing, and at times, the program authors themselves, results in confusion as to what is meant by successfully passing the testing program. Conformance means that an implementation adheres to the dictates of the standard.
(I will not discuss profiling of standards at this time)

While one might think that all programs that completely adhere to a standard (conformant) would be interoperable, in practice they often are not. Interoperability means that implementations adhere to the dictates of the standard and intercommunicate appropriately with other implementations that adhere to that same standard. (I will forgo the discussion of gateway standards at this time.) Interoperability adds one more requirement over and above conformance.

The problem is that many testing programs test only for conformance and then unceremoniously presume and declare it interoperable. Stakeholders in the marketplace believe they are receiving interoperable implementations because they have been told so, but they are getting only conformant products. Conformant implementations may not be interoperable among themselves. This is especially the case in more complex software and hardware systems. This leads to the first aspect discussed above in which "certified" implementations now require debugging when they are installed by the end-user, thus damaging the credibility of the test program. And they slow ongoing Smart Grid implementation. Once the compromising of the testing program's credibility starts, it can take a few of years to correct the

perception by the marketplace of end-users. This is why the test program must be thought of as a stakeholder in the process early on.

B - What is the importance of testing and certification in the implementation of standards of Smart Grid devices, systems, and processes?

Interoperability Verified not presumed

The program must verify, not just assume, interoperability among the various product implementations of a standard. There are many different types of standards. Some are device oriented. Some are business-to-business. Some are written from the ground-up, detailing all the software and firmware with dependencies on other standards to achieve their purpose. Other standards are focused on communication protocols, while others are focused on the semantic meaning of the data. Only testing the conformance of any of these standards may achieve different levels of 'near' or 'actual' interoperability. Depending on a number of factors, including the standard, the testing regime, the software/firmware under test, and others, conformance testing may produce interoperable implementations. Such a result is good in that no additional testing steps are required to achieve interoperability. However, there remains a problem. It is rarely known that a conformance test has produced interoperable product implementations unless verification is performed with an additional test step to prove that the implementations are indeed interoperable. There are only two points in the timeline as a standard evolves from formation to product implementation where implementations can be verified as actually interoperable:

1. The product implementations may verify interoperability in concert with conformance testing; or
2. When the end-user is attempting to deploy the product implementation in the field.

The first case represents the testing program and the stamp of approval of 'certified' by the program and demonstrates that products are both conformant and interoperable. In the second case, the conformant and presumed interoperable implementations are released to the marketplace where the end-user is expected to validate interoperability and correct any shortcomings in the testing program. It is well known from studies over the past 20 years that errors found in software products after field deployment

may cost as much as 40 times the amount to correct than if those errors are found before the implementation is released to the marketplace. This additional cost does not include the original cost, frustrations and loss of good will by the end-users.

Not verifying that conformant implementations are interoperable when they are given a 'certified' grade in a conformance and interoperability testing program often cause the program to become irrelevant as we have seen in other industries. When this happens, interoperability often stalls for that standard in the industry -- sometimes for years.

Summary

Success of a conformance and interoperability program is about methodologies, market positioning and securing success for all the stakeholders. The program must be focused on supporting the implementations in the field for not only the product lifecycle, but also the lifecycle of the standard. The program must clearly identify what it is offering to the all the stakeholders as it identifies certified implementations. Are the products verified conformant or are the products verified conformant *and* interoperable? The program designers must anticipate its growth and demise as conformance and interoperability become institutionalized in the implementations over their lifetimes. All of these issues should be anticipated for a successful testing program irrespective of the standard. Not doing so may greatly reduce the introduction of conformant and interoperable implementations of the standard into the industry -- stalling interoperability.

C - What challenges has the SGIP faced in working together to develop a framework to ensure interoperability of Smart Grid products?

The first versions of the IPRM went into place in January 2011 for SGIP members. The framework covered 4 broad area:

1. *Enhancing Testing Lab process quality and repeatability.*
   These processes are based on ISO 9001 requirements and are elucidated in the ISO 17025:2005 guide. Currently only a portion of the test labs used in the Smart Grid use these guides as the basis for

their internal testing processes. Many others do not. Quality of the test results from labs is currently spotty. Interoperability is a 100% endeavor. Test Lab producing quality a 99% causes problems. Getting everyone in the Smart Grid to understand the need for consistent quality output for tested products has been problematic. The main inhibitor to solving this problem is the added cost for the implementation of ISO 17025 for product vendors to test products. I personally estimate a cost increase of 25 to 40% over pre ISO 17025 testing.

2. *Requirements for Certifying Test Lab results by a trusted third party*. These certification processes are currently being modified to fit ISO 9001. They will be elucidated in the forth coming ISO 17065 guide. Currently, the working guide is ISO 65. Currently, many product vendors question the need for the additional cost associated with paying for a third party to certify test lab results produce interoperable products.

3. *Guidance on testing of cyber security mechanisms within a software product.*
   Security testing of cyber security mechanisms and interoperability testing are normally at odds philosophically. Security attempts to restrict available functionality depending on authorization while interoperability attempts to remove restrictions so that information flows between entities appropriately. Conducting cyber security testing distinct from interoperability testing does and will cause problems. Tightening cyber security may make the product non-interoperable. And the converse, ensuring interoperability may inadvertently break cyber security mechanism. Conducting a single test of products, covering both cyber security mechanisms and interoperability requirement will allow these clashes to be resolved during the test. Thus a product or products will be released from the test lab that meets both the cyber security and the interoperability requirements at an anticipated lower cost.

4. *Guidance on how to achieve interoperability in testing*.
   Currently may test labs do not test for interoperability. They only test for conformance of a product to a standard and assume that conformance includes interoperability. A conformant product may not be completely interoperable with other conformant products. The

introduction of conformant products in the market place which are only assumed to be interoperable moves the burden of getting products to intercommunicate to the persons installing the products in the field. They may have to fix non-interoperability problems that should have been fixed before the products were released to the market place. This greatly slows the introduction of new capabilities and products installed in the Smart Grid. Many test labs and service providers do not understand that conformance does not ensure interoperability within a set of products.

3. Federal Government Role

What do you believe are the most important actions for the Federal Government to take to ensure the protection of consumer interest, including cost and privacy while driving innovation within the smart grid development?

Since the United States is a federation of states, with attributed states rights, unlike just about any other country, what the Federal Government may do versus what would be helpful to do are not always the same. States differ in their regulations as to privacy of consumer data, security, allowable charges to the consumer and et cetera.

1. Ensure Cyber Security on the smart grid is a top down approach. Piece meal implementation across the Smart Grid will make the verification of security problematic for the USA power Grid.

2. Ensure the population in the USA understands the cost/ benefits of the Smart Grid implementation. Increased Consumer cost for power is going to be problematic. Cost is going up significantly because of new EPA regulations on coal-fired plants and less significantly because of the implementations of smart grid technologies. I predict the consumers, especially those within one of the largest voting blocks, baby boomers on a fixed income, will react negatively to even minor cost increases caused by various regulations and technical enhancements to the power grid.

3. Ensure the implementation of the logic or verbatim use by the Federal Government of the *Interoperability Process Reference Manual* (IPRM v2) by including it within new versions of the FIPS. This would mean approximately 25% of the GDP would be required to increase software and hardware product quality, consistency, reproducibility and interoperability within the IT markets, thus partially, yet significantly, funding the efforts of Test Labs, Certification Bodies and product vendors to implement quality and consistency for Interoperability across all sectors of the economy including Smart Grid. Health and Human Services is implementing the Test Lab and Certification body quality requirements as part of the EHR Meaningful Use requirements for Medicaid and Medicare providers. While these currently do not focus on Interoperability as such they are implementing the quality framework to support Interoperable products within the market place. I would use the FIPS to prime the pump not new regulations on the private sector. The uncertain regulatory environment is slowing growth of the private sector.