BEFORE THE PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA

Order Instituting Rulemaking on the Commission's Own Motion to Improve Distribution Level Interconnection Rules and Regulations for Certain Classes of Electric Generators and Electric Storage Resources.	))))))	Rulemaking 11-09-011 (Filed September 22, 2011)

COMMENTS OF SAN DIEGO GAS & ELECTRIC COMPANY (U 902-E) ON SMART INVERTER WORKING GROUP – PHASE 2 COMMUNICATIONS PROTOCOLS

Jonathan J. Newlander
Attorney for
SAN DIEGO GAS & ELECTRIC COMPANY
101 Ash Street, HQ12
San Diego, CA 92101
Phone: 619-699-5047
Fax: 619-699-5027
E-mail: jnewlander@semprautilities.com

November 10, 2014

BEFORE THE PUBLIC UTILITIES COMMISSION OF THE STATE OF CALIFORNIA

Order Instituting Rulemaking on the Commission's Own Motion to Improve Distribution Level Interconnection Rules and Regulations for Certain Classes of Electric Generators and Electric Storage Resources.	))))))	Rulemaking 11-09-011 (Filed September 22, 2011)

COMMENTS OF SAN DIEGO GAS & ELECTRIC COMPANY (U 902-E) ON SMART INVERTER WORKING GROUP – PHASE 2 COMMUNICATIONS PROTOCOLS

San Diego Gas & Electric Company ("SDG&E") submits comments, herein, pursuant to a request for comments on the Smart Inverter Working Group – Phase 2 Communications Protocols agenda for a workshop which occurred on October 27, 2014. The smart inverter effort is contained within the California Public Utility Commission's ("CPUC's") Rulemaking ("R.") 11-09-011. Pursuant to an email from Energy Division Staff dated November 6, 2014, these comments will be served to the service list for the applicable rulemaking but will not be filed. SDG&Es comments focus on the document entitled *Recommendations for Utility Communications with Distributed Energy Resources (DER) Systems with Smart Inverters – Smart Inverter Working Group Phase 2 Recommendations – Draft Version 2*, updated October 22, 2014 ("Phase 2 Draft").

I. COMMUNICATION PROTOCOL COMMENTS

SDG&E appreciates the opportunity to provide comments on the Phase 2 Draft created as part of the Smart Inverter Working Group ("SIWG"). SDG&E looks forward to continued involvement in the SIWG and expects the document to evolve as parties continue to participate in the reoccurring calls between stakeholders. At this time SDG&E would like to make preliminary recommendations on how the document could be improved.

As a general rule, SDG&E suggests additional clarity such as defining the terms used. For example, "data 'profiles'" should be specific in defining what qualifies as a "profile." This might be the complete specification at all levels of the stack. Similarly, there should not be ambiguity in the specification of data models or service definitions.

Below SDG&E comments on certain specific recommendations set forth in the identified sections of the Phase 2 Draft and which should be discussed by the SIWG:

- Section 3: In addition to "Transport level protocols," the on-the wire formatting and encoding scheme should be specified.
- Section 4 – Real Power DER Functions: The scheduling of energy storage devices is of high importance to maintain reliability of the distribution system.
- Section 4 - DER Response to Emergencies: "Utility receives notification that a microgrid disconnected or reconnected from the utility grid. (L)" This should be of High importance. Knowledge that a microgrid is connected to the utility grid during an outage is imperative in maintaining worker safety.
- Section 5.1.2 - Notification of Alarms: Stakeholders should reexamine in order to determine what requirements are required for utility notification of alarms. Utility needs are likely less than that of the plant operator or maintainer. Utility needs are best expressed in terms of a de-rating of plant capabilities.
- Section 5.2.1 - Administrative Information for Aggregators: Utilities need administrative processes and messages determined for all resource types and not just aggregators.
- Section 5.3: States, "Performance: Real-time capabilities, e.g. 1-10 second interactions, high availability." – This should be modified to state that this is "near real-time." Additionally, there are also other timing issues in this section that may merit further examination by the SIWG to ensure that they can be met.

II. CYBERSECURITY AND PRIVACY COMMENTS

SDG&E provides the following responses to the questions posed in Section 6 of the SIWG document.

A. What are the utility security policies for interacting with non-utility sites and equipment where the data to be exchange has operational impacts?

SDG&E does not have a security policy or standard specific to interactions with non-utility sites and equipment, but SDG&E has cybersecurity policies and requirements that are based upon industry best practices, frameworks, and regulatory requirements,

such as NIST 800-53, NERC CIP, and NISTIR 7628. The goal for future interactions is to meet or exceed those established baseline level of security controls centered around ensuring integrity, AAA, availability, confidentiality and privacy of our customers.

B. What utility security procedures must be followed by such non-utility sites in order for operational data to be exchanged? In particular, how can new DER sites be "registered" and tested for security compliance?

SDG&E's practice when commissioning a new SDG&E owned/operated DER site is to assign a cross functional team to address the various areas of expertise required. This includes both IT and OT personnel.

The IT team includes a cybersecurity subject matter expert ("SME") whose function is to ensure the DER site meets applicable cybersecurity requirements. The cybersecurity SME also tests the various DER components and their associated cybersecurity controls to ensure risks have not been introduced and all cybersecurity requirements have been met.

In response to how DER sites can be registered and tested for security compliance, the closest example of this happening today is how customers register Home Area Network devices to be associated with their Smart Meters. The existing HAN device testing process might be able to serve as a starting point for establishing a future streamlined DER registration process. A key aspect of that process which currently helps ensure cybersecurity requirements are met for HAN devices is the 3rd party accreditation/conformance testing which includes cybersecurity test cases.

This may be one starting point but further analysis is required to determine if this the best approach.

C. Are there different security requirements for different types of sites, e.g. small < 10 MW DER sites versus > 10 MW sites?

All sites, regardless of MW size, should be held to a baseline level of security requirements. The safety of SDG&E's customers and employees, the reliability of the grid, and privacy of customers' data are top priorities. Additional security requirements may be appropriate for larger sites.

D. Have these security policies and procedures been clearly established or are they still being worked on?

Cybersecurity requirements have been established based upon industry best practices, frameworks, and regulatory requirements. No specific DER site policies and procedures have been established as such. The SIWG should investigate already established cybersecurity industry best practices and set a baseline level of cybersecurity requirements for smart inverters.

E. Are there specific security technologies that must be used? Are there specific technologies that must not be used?

SDG&E's cybersecurity approach to technology selections is to be vendor agnostic as much as possible while adopting open standards to ensure interoperability. The goal is to meet requirements. The specific vendor or technology acting as the control to meet the requirement should not matter as long as interoperability is maintained.

F. Some security technologies are specific to different communication protocols - are there preferred protocols from a security perspective?

SDG&E does not have a preferred protocol from a security perspective as long as cybersecurity requirements are met and interoperability is maintained. Introducing automation and improving efficiencies where possible is preferable but not at the expense of security or interoperability. SEP 2.0 may provide a good starting point for the discussion.

G. Is there agreement that at least authentication and data integrity must be ensured?

Yes, data integrity needs to be ensured as operational decisions are being made based upon this data. Authentication is a key consideration when control capabilities are involved as this could potentially impact customer/employee safety and grid reliability.

H. When should non-repudiation / accountability be ensured?

Authentication, authorization, and accounting (aka accountability) should always be ensured. Non-repudiation would be a good control to include, although it can be difficult to implement, manage, and maintain, especially in consumer/customer devices.

I. When should confidentiality be ensured?

Ensuring the privacy and confidentiality of customers' data is a top priority of SDG&E, and should be maintained always. Encryption should be used based upon the situation and scenario (such as RF communications and public internet communications).

J. How is key management expected to be handled? PKI? What Certificate Authorities can/must be used?

Key management is not an easy task. However, it is an important process in PKI to maintain the chain of trust. SDG&E suggests looking at how key management is outlined in other established industry best practices (such as SEP 2.0) and using those as a starting point.

K. Will Role-based Access Control (RBAC) be used to constrain the permitted actions?

RBAC is a type of an authorization control normally associated with human owned accounts (or end users; e.g. read only, operator, engineer, etc.). Non interactive accounts (sometimes called functional, service, or application accounts) can use RBAC authorization; however function Access Control Lists (ACLs) could potentially be leveraged.

SDG&E would like high level authorization controls to be included in the specification. Investigating the use of digital certificates over the use of stored user names and passwords for authentication and authorization controls should be pursued.

L. Are these cyber security requirements accepted by all California utilities or are there major differences?

SDG&E cannot speak on behalf of the other utilities. SDG&E believes, however, that the California IOUs leverage already established standards, frameworks, and regulatory requirements and would use those as a starting point for the discussion (such as SEP 2.0, IEC 62443, NERC CIP, NISTIR 7628, NIST 800-53).

M. What other cyber security issues need to be resolved?

The SIWG should examine the storage of secrets (password, keys, digital certificates, etc.) on any consumer or customer device because safeguarding such information is essential to maintaining system security.

Disabling developer or manufacturer ports/inputs such as JTAGs, serial ports can lead to easy extraction of firmware, secrets, and memory. Since physical security of consumer and/or customers' premise devices cannot be guaranteed, security of ports and inputs becomes critical.

It may be worthwhile to investigate a third party conformance process (similar to the testing HAN devices) to ensure Smart Inverter devices are free from major

cybersecurity vulnerabilities and conform to the other specifications (protocols, functional use cases, etc.).

III. CONCLUSION

SDG&E appreciates the opportunity to provide the foregoing comments.

November 10, 2014