

AD11-6-000 FERC Technical Conference

February 8, 2011

Statement of Ron Litzinger

President, Southern California Edison Company

Good afternoon, Chairman Wellinghoff, Commissioners, and FERC staff. I am Ron Litzinger, President of Southern California Edison Company. Thank you for holding this conference on reliability issues and inviting me to speak. My company is committed to maintaining reliability and striving for operational excellence – a commitment I know is shared by many other members of our industry and supported by FERC. My remarks today focus on emerging challenges to the reliability of the bulk power system that our industry will face over the next decade. In particular, I will highlight four issues that I expect to significantly impact electric grid reliability in the years ahead: the need for holistic regulation, integration of large-scale renewable resources, cyber security issues posed by Smart Grid deployment, and wide-area situational awareness.

Holistic Regulation

I will use the impact of potential EPA regulations to illustrate the need for a holistic approach to regulation. Several environmental regulations that are in development pose significant potential reliability impacts to the bulk power system, including those relating to: (1) Section 316(b) of the Clean Water Act, mandating cooling towers, (2) the Clean Air Transport Rule, adjusting the allocation of SO₂ and NO_x allowances, (3) Hazardous Air Pollutants and Maximum Achievable Control Technology (HAPs/MACT), and (4) Coal ash hazardous designations.

There is a wide range of variability to the outcome of these regulations, particularly if they are ultimately acted upon in piecemeal fashion. It is therefore difficult to predict their effects on the continued operation of the existing fleet of generating units, particularly in California with respect to

units currently relying on once-through-cooling technologies. Litigation and Congressional action add even more variables to be considered. It is in this general environment of uncertainty that generation owners must make decisions on environmental control technology.

NERC recently reviewed the impact of such regulations on reliability. It found the combined suite of EPA regulations could shut down between 33-70 GW of capacity by 2015. Some may disagree with the magnitude of NERC's findings, but the concerns are real. The unintended consequences of overly aggressive or poorly timed regulations can be severe, particularly where there is direct conflict with other federal and state policy objectives.

From a plant closure and reliability standpoint, the federal government should review these rules holistically to assess their collective impacts on the electric grid and their compatibility with other policy objectives, rather than considering one regulation at a time. FERC can play an essential role in this process by working with EPA, DOE, and OMB to ensure that such a holistic analysis takes place.

Integration of Renewable Resources

Renewable resources are increasingly being developed on a large scale. In California for example, investor-owned utilities are operating under a mandate to obtain 33% of the energy we sell annually from qualified renewable resources by 2020. Integrating dramatically increased levels of wind and solar resources into the existing electric grid will present two major challenges.

First, wind and solar generation often must be located far from the loads those resources are procured to serve. In order to be successful in building the transmission necessary to deliver renewable power to our customers, we must continue to streamline the transmission siting and licensing process to allow for more prompt and certain approvals. Federal land use agencies play a critical role in transmission siting and can be a source of delay. FERC's coordination with these agencies to reinforce the need for

timely action could assist in ensuring the reliable deployment of renewable resources.

Second, the output of renewable generation is by definition variable and intermittent. Large scale integration of these nontraditional resources will require significant investment in additional devices such as Static VAR Compensators (SVC) to stabilize voltage, and backup resources to match this variable output to the variable load. In addition, the renewable resources will need to be able to “ride through” routine system faults so that the necessary resources do not disconnect from the system and exacerbate the situation.

Backup resources for renewables can include: fossil generation, energy storage devices, and demand response programs. Effectively coordinating the operation of the renewable resources with their backups requires improved intelligence and control of the grid to maintain and improve reliability. These improvements are part of “Smart Grid” technologies. SCE, like many utilities across the country, is modernizing its electricity grid to improve the grid’s reliability and efficiency. SCE’s Smart Grid will enable us to deliver more renewable energy into the system, give our customers more power to control their energy use and costs, and improve reliability.

Smart Grid and Cyber Security

The Smart Grid requires greatly expanded communications between intelligent devices with increased reliance on open protocols and networked communication systems. Allowing more devices to communicate with each other while providing security against cyber, physical, and data privacy threats is a matter of high priority.

NERC’s CIP standards will play a key role in ensuring cyber security as Smart Grid technologies are further deployed. Smart Grid technologies span all the way from generation to the retail customer. Accordingly, those aspects of the Smart Grid that are deployed within the bulk power system will certainly be subject to CIP standards. To ensure appropriate protections apply in an integrated fashion across the Smart Grid, it will be

essential to coordinate NERC's efforts with those of state entities that develop standards for distribution-level components of the Smart Grid.

Because cyber threats are sophisticated and rapidly evolving, there is no single technology or set of standards that can guarantee cyber security. Consequently, our response to rapidly evolving cyber security risks should include not only regulation of today's technologies but proactive, collaborative engagement by regulators and industry in the design of tomorrow's solutions, based on robust system security engineering, comprehensive cyber security frameworks that encourage innovation and agility, and enhanced governance. It will also be essential to establish appropriate protocols and processes to share real time and actionable threat information between the appropriate government agencies and the private sector.

Efforts in this regard are underway for early adopters, and will need to be broadened as Smart Grid technologies are further deployed. For example, with regard to sharing actionable threat information, my company and a number of other industry representatives are engaged in the DOE-sponsored AEP/Lockheed Martin project to build a Utility Industry Security Operation Center. There are also opportunities today for utilities, vendors, security researchers, and other Smart Grid stakeholders to collaborate on security requirements, architectures, and design approaches through professional societies and user groups. The pace of changes in technology, process, and people for the new grid systems – as well as the threats to and vulnerabilities of the systems – will require regulators, vendors, and utilities alike to be agile and to work in partnership to best provide our customers with a reliable and secure electricity delivery system.

Situational Awareness

In recent years, the degree of interconnection and power exchange between systems has greatly increased, leading to a need for Wide Area Monitoring (WAM) and Wide Area Control (WAC). Looking ahead, enhanced wide area situational awareness and controls will be needed to manage voltage stability and VAR resources. Wide area situational

awareness means that system operators will have immediate shared visibility of emerging threats to transmission grid stability over the entire interconnection, and not just their own portion of it.

As noted earlier, the addition of renewable resources will complicate the balancing act between load and generation. As such, wide area monitoring and controls will be necessary, on an interconnection-wide basis, to optimize system operations. This can be facilitated by, among other things, the deployment of Phasor Measurement Units (PMUs), which provide bulk system information at speeds previously unavailable. Armed with such information, we will be able to take proactive corrective measures to avoid large-scale blackouts before the system reaches a breaking point. Such a PMU system requires the exchange, storage, and manipulation of vast quantities of data over a high bandwidth system. Effective broad deployment of these PMU systems will be a multi-year effort requiring active coordination within the industry and support from our regulators.

Thank you for the opportunity to provide these remarks today, I look forward to your questions.