FERC Reliability Technical Conference
Panel I: 2015 State of Reliability Report

Remarks by Dr. S. Massoud Amin

Chairman of the Texas Reliability Entity (TexasRE), Chairman of the IEEE Smart Grid, and Independent Director on the Board of Directors of the Midwest Reliability Organization (MRO)
Director and Honeywell/H.W. Sweatt Chair at the Technological Leadership Institute (TLI), Professor of Electrical & Computer Engineering, University of Minnesota

June 4, 2015

Mr. Chairman, Distinguished Commissioners, panelists, staff and guests. Good morning and thank you for this opportunity, and for your committed efforts in ensuring the reliability of our most critical infrastructure.

Today you will hear from experts a summary of the State of our system – Activities, Accomplishments, and Challenges ahead. Together we will review the reliability of the bulk power system, which continues to improve in many aspects, and will consider pathways forward.

As a board member of the TexasRE and MRO, I have the opportunity to collaborate with impressive colleagues at every level (including at the Texas RE, MRO, REs, NERC, FERC and executive leaderships, Board members, MRCs/representatives of registered entities and the broader stakeholders). I enjoy our shared vision, mission, values, and commitment to excellence in assuring a foundational area that really matters to our economy, security and quality of life — particularly as our industry and the Electric Reliability Organization (ERO) evolve and improve.

I quote from Mr. Dan Skaar "*Today's regulation supports and sustains a state of "reliability mindfulness" across the industry and has encouraged investments and innovation. Hundreds of millions of dollars of investments have been made to our infrastructure to increase reliability and prevent blackouts. These investments include protection systems upgrades, state of the art vegetation management techniques, improved accuracy of facility ratings and advancements to control systems security.*"

Some statistics related to both TexasRE and MRO Regions' progress show that:

1. Event trending index. This demonstrates that both the frequency and severity of events has declined since mandatory standards began in 2007. Fewer, less severe events.
2. Compliance trending index. This demonstrates that the severity level of violations peaked in 2011 as a result of CIP standards and has steadily declined since then. Fewer, less severe violations.

While our industry has undergone significant evolution in the past five years, much more is yet to come. Over the next year, even over the next five to ten years, and beyond, our industry will continue to face some major challenges in forward thinking and many opportunities that will require action. To put all this in perspective, we can frame pressing issues, key drivers, and potential pathways forward. As I see it, here are the top 10 drivers for change in the electric power sector, in no particular order.

1. Acceleration of efficiency (energy intensity dropping 2%/yr.);
2. Distributed generation and energy resources (DG & DERs), including energy storage & microgrids;
3. More cities interested in charting their energy future;
4. District energy systems;
5. Smart Grids;
6. Electrification of transportation;
7. New EPA regulations, such as for greenhouse gases under Section 111(d) of Clean Air Act;
8. Demand response (and 3rd-party aggregation of same);
9. Combined heat & power (CHP), plus waste heat recovery; and
10. The increasingly interstate and even trans-national nature of utilities (and contractors too, which leads to security concerns).

These drivers in turn lead to some important questions throughout the 4 major North American Interconnections, both for the utility, as a business, and for regulators, as makers of policy:

1. What business models may develop, and how will they successfully serve both upstream electricity market actors?
2. What key distributed energy technologies can disrupt the power sector? Impacts of DG and DER on reliability, and need for end-to-end transparency.
3. E.g., how might distributed energy resources, such as solar panels or plug in vehicles in garages, affect power system operations, markets, and regulations?
4. What effects could these new business models have on incumbent utilities, and what opportunities may exist for other industry sectors to capitalize on these changes?
5. How will regulation need to evolve to create a level playing field for both distributed and traditional energy resources?
6. What plausible visions do we see for the future of the power sector, including changes for incumbent utilities, new electricity service providers, regulators, policymakers, and consumers?
7. What measures are practical and useful for critical infrastructure protection (CIP) and the security of cyber physical infrastructure? Energy consumers?

To answer these questions, we must address a number of new challenges, such as how to integrate large-scale stochastic (uncertain) renewable generation (connected also to EPA rules), electric energy storage, distributed generation, plug-in hybrid electric vehicles, and demand response (smart meters). We must also realize methods to deploy and integrate new synchronized measurement technologies, new sensors, and new system integrity protection schemes. In addition, we'll need better models (GEN and Loads) in many of our regions.

We are only as good as our registered entities, and we have many terrific ones in our regions. Every utility has a unique customer base, business model, legacy system, and its own interests at stake in providing reliable, affordable power while promoting resiliency in the face of a myriad of vulnerabilities. While the system complexity has increased during the past 20 years, and

considering how different systems are across the country, we have developed the expertise to manage these differences, as together we aim to maintain and improve quality of life through a highly reliable grid, as Mr. Dan Skaar noted "*From the very beginning of mandatory compliance, we have encouraged investments in reliability, rather than just monetary penalties. Investments resulting from enforcement actions have included accelerated aging asset replacement, upgraded tools and training and increased staff to address cybersecurity and protection systems."*

The next five years, and the decade beyond that, will be even more dynamic, evolving and exciting. Considerations for Assuring Reliability on a Longer-term Horizon: The addition of a longer-range look at strategic issues is a valuable addition to the strategic planning activities to be able to anticipate beyond-the-horizon issues. In the dynamic environment we are in, we need the ambidexterity to be able to both monitor and detect possible future events and map out a procedure in response to a variety of scenarios in the face of uncertainty.

In summary, regulation is working – we are reducing risk to the bulk power system as the report shows, while weather events continue to rise. But, we need to do more:

- First, we need to integrate better feedback loops into the standards, and to close these loops where they have never been closed before. Together with NERC we need to triangulate events back into the standards process to address any gaps. For example, what percentage of events had corresponding violations which were contributory to the event? I believe we need an answer to determine whether the standards are sufficient for reliable operations – preventing cascading events.
- Second, we should elevate our focus towards resiliency and restoration in the future.
- Third, our North American interconnection is safe and we are keeping the lights on, however its reliability, effectiveness, and affordability are increasingly being questioned. Much work remains to be done. The challenge is to reduce uncertainties over what regulators will do next and what investors will do next. As Ms. Anne Pramaggiore, ComEd CEO, noted: "Today's regulatory framework is keeping us locked into the 20th century."

In addition to my comments that I shared with you, attached please find an addendum provided for your reference on the next few pages. There are a few questions and a subset of recommendations from the IEEE Quadrennial Energy Review (QER) report for the U.S. DOE, which I hope are pertinent to your discussions and potential action.

The answer to these will undoubtedly take extended discussions with the various stakeholder groups. As noted earlier, the cost of developing and deploying a modernized stronger, more secure and smarter grid for the country is cost effective and should be thought of as an investment in the future – in a secure, reliable, and entrepreneurial future – that will pay back over many decades to come as the energy backbone of our 21st century economy.

*** * * * * * * ***

Thank you.

Addendum:

Question 1: *What do you feel is the most important thing the electric regulatory industry should accomplish over the next five years?*

> **Answer**: It is imperative that we reduce uncertainty for investments in the grid, in innovation and research and development, in modernizing entire systems and encouraging development of capable human capital.
>
> Think systems, be forward thinking, be strategic, know the past, be open to innovation, develop a fresh outlook at what can realistically be achieved—what are the resultant primary, secondary and tertiary consequences? I quote HL Mencken, "For every complex problem, there's a single solution that is simple, neat and wrong!" Develop capabilities to understand and address such interdependent complex systems. As these systems interact with each other, there are many solutions that can come together under what we call design thinking. It involves care, patience, time and resoluteness not to fail. For more information on these thoughts, please read my article, "We are not in Kansas anymore" in the September/October 2011 edition of the Midwest Reliability Organization (MRO) newsletter.

Question 2: What are the persisting security concerns and what can be done?

> **Answer:** As CIP 5 and cyber-physical programs are implemented and protections put into place, difficult choices will have to be made about how to handle a number of trade-offs:
>
> - **Outdated regulatory framework.** One important constraint on regulatory oversight of security protection is the split jurisdiction over the grid, which is keeping us locked into the 20th century infrastructure. The bulk electric system is under federal regulation but the distribution grid, metering, and other aspects of the grid are regulated by individual states. Overlapping and inconsistent roles and authorities of federal agencies can hinder development of productive, public-private working relationships, thus a new model for these relationships is required for infrastructure security. For instance, a stockpiling authority, be it private or governmental, could obtain long lead-time equipment based on the power industry's inventory of critical equipment, which must include the number and location of available spares and the level of interchangeability between sites and companies. Clearly, further standardization of equipment will reduce lead times and increase the interchangeability of critical equipment. For example, the typical, state-level regulatory approach – cost-of-service rate making and volumetric pricing – puts IOUs and microgrids at odds. Most states regulate synchronous interconnections based on IEEE 1547 (please see section 1 of the IEEE QER report for more details) and FERC's small generator interconnection procedures (SGIP) in FERC Order 2006.
>
> - **Controls and Communication** - Protection of power generation, transmission and distribution equipment is insufficient to guarantee delivery of electricity because widespread, coordinated denial of control and communication systems could cause significant disruption to the power grid. This includes SCADA systems, communications between control systems, monitoring systems and business networks. However, the power management control rooms are currently well-protected physically, although they may have cyber vulnerabilities. NERC requires a backup system and there are also manual workarounds in place. The Federal Energy Regulatory Commission (FERC) is working toward a common set of security requirements that will bring all electric sector entities up to at least a minimum level of protection.

- **Investments in security**. Although hardening some key components—such as power plants and critical substations—is highly desirable, providing comprehensive physical protection for all components is simply not feasible or economical. Dynamic, probabilistic risk assessments have provided strategic guidance on allocating security resources to greatest advantage. However, pathways to cost recovery and making a business case for security investments/upgrades, often pose challenges.

- **Security versus efficiency and ROI.** The specter of future sophisticated terrorist attacks raises a profound dilemma for the electric power industry, which must make the electricity infrastructure more secure, while being careful not to compromise productivity. Resolving this dilemma will require both short-term and long-term technology development and deployment along with supportive public policy for cost recovery, which will affect fundamental power system characteristics, spurring development of new business models/strategies.

- **Centralization versus decentralization of control.** For several years, there has been a trend toward centralizing control of electric power systems. The emergence of regional transmission organizations, for example, promised to greatly increase efficiency and improve customer service. But we also know that terrorists can exploit the weaknesses of centralized control; therefore, smaller and local semi-autonomous systems would seem to be the system configuration of choice (analogous to platoons during warfare with local autonomy, while coordinated with the overall mission of the operation). In fact, strength and resilience in the face of attack will increasingly require the ability to bridge simultaneous top-down and bottom-up decision-making in real time—fast-acting and totally distributed at the local level, coordinated at the mid-level and aligned with executive objectives.

What are some specific examples and actions required to improve security and resilience of the system?

✓ ***POLICY REMAINS THE SINGLE BIGGEST INFLUENCE ON THE BUSINESS CASE***

Example -- Microgrids: A 2013 white paper, "Results-based Regulation: A Modern Approach to Modernize the Grid," addresses the limitations of cost-of-service regulation and offers alternative regulatory models that each state could consider adopting.

A recent study of policies relating to microgrid adoption in Minnesota reveals that state regulatory policies often don't address microgrids at all. But the Minnesota study suggests that state policy define and acknowledge the opportunities presented by microgrids to achieve state policies regarding energy surety and the adoption of renewable energy sources and to "ensure that microgrids are properly valued and considered in energy resource and policy initiatives." The Minnesota study identified both regulatory and legislative steps to achieve these objectives. FERC policy covers DG-related projects up to 20 megawatts (MW) and how they interconnect with interstate transmission systems, relevant if the project plans to sell wholesale power into an independent system operator (ISO). FERC has issued a NOPR that it will amend its SGIP and SGIA (small generator interconnection agreement) to "ensure the time and cost to process small generator interconnection requirements will be just and reasonable and not unduly discriminatory".

State-level PUCs wield the most influence. Many states are reviewing related policies as they balance utility interests with ESCO competition and the needs of the commercial/industrial and residential utility customer sectors. A state-level, results-oriented regulatory approach that rewards utilities for adopting innovations that directly benefit their customers may encourage microgrid adoption.

In terms of a federal role in microgrid-related policy development, states will continue to exercise (and defend) their role in microgrid-related policy-making. With access to resources – possibly facilitated by

the U.S. DOE – on related technology and standards, regulatory reform and stakeholder impacts, however, state regulators can create policies that favor microgrid development and balance the diverse interests involved.

FERC's small generator interconnection procedures (devised by SGIP, embodied in FERC Order 2006) also are relevant to this discussion.

State policies may also need to evolve with standards through a regular, consistent process, both to encourage microgrid development and reward utilities for cooperating with a customer benefit that cuts into its revenue. Policy and standards should work in hand-in-hand.

One area ripe for revision: Where a state has a restrictive definition for DG capacity for its interconnection requirements. Current rules require large microgrid proposals to forge unique agreements with a utility at great cost and uncertainty.

California regulators have articulated many of the issues that policy must address, as has the National Regulatory Research Institute. Both efforts provide an in-depth look at the complexity and interrelated nature of many microgrid-related policy issues as utilities, independent system operators, ESCOs, customers and other stakeholders are linked technologically and in wholesale and retail markets.

Critical regulatory issues currently being reviewed include, among many others:

- How costs and benefits are apportioned to myriad stakeholders (and how that affects cost recovery for utilities),
- Whether a microgrid relies on the distribution system (or transmission system) for backup and how that might affect reliability,
- Whether and how to treat non-utility microgrid sponsors as utilities, and
- Multiple possible business models for utilities offering microgrids.

Metrics, Best Practices, and Roadmaps: Establish metrics on workforce and identify policies that facilitate necessary workforce development activities by the regulated companies. There is a workforce crisis coming that could affect customer services and costs so it is in the public interest that regulators increase their oversight of workforce development.

Select a lead organization (perhaps DOE) to facilitate regulator / industry dialog by designing and holding workforce workshops for NARUC, FERC and NERC that create situational awareness for state and national regulators. The NERC System Operator Certification and Training program should be used as an example of a successful program for regulated training. Initially the focus should be on the workforce whose performance is most directly connected to reliability, such as system operators, linemen, planning engineers, protection engineers/technicians and substation operators. DOE can convene a cross functional group of experts to include industry, government agencies (DOL, DOE, NSF, DHS, and DOD) and regulators for the purpose of reviewing current practices in workforce benchmarking and create metrics to quantify the threat posed to the electric grid's performance by insufficient replacement workers. DOE could seek out opportunities to co-fund industry education and training programs (IEEE examples include Scholarship Plus, WISE, Plain Talk) and fund student and innovation competitions.

Improving Existing Survey and Assessment Tools: In generation, FERC has in the Form-1 a large amount of the material needed to support an assessment of the adequacy of the generation fleet. There are operational and maintenance aspects that are not included in the Form-1. FERC Forms 714 and 715 provide some, but not all of this information and Form 556 provides information on smaller generation facilities. Again the existing FERC data would not provide a complete survey, but it is a strong starting point to develop survey results from. For sales, forecasts, usage, and other consumption related information the Energy Information Agency (EIA) provides the best starting point.

Recommendation for a survey of the electrical infrastructure:

- Bring together the industry and end-user stakeholders to look at the existing survey tools, and define the overall needs for an industry wide set of survey tools. This working group should provide a clear requirements document on what needs to be surveyed, and the depth that the survey needs to cover.
- Determine what existing materials can be used to support the survey requirements, minimizing new data collection.
- Provide adequate resources to complete a survey tool set that supports the requirements that were developed by the stakeholder group and uses the data from existing sources.
- Working with an industry working group, define how the survey tool will be used both improving the infrastructure and in any regulatory actions. The tool set will fail, if there is no consensus among the stakeholder groups. A solid survey tool set for both self-assessments will provide a data driven way for the industry to determine where to focus research, standards development, training, staffing, and operational improvements for the industry. With the rapid changes in the environment this will allow the better deployment of scare resources.

Pertinent IEEE QER recommendations to the U.S. DOE, for your consideration:

Markets and Policy

- Use the National Institute of Standards and Technology (NIST) Smart Grid Collaboration or the NARUC Smart Grid Collaborative as models to **bridge the jurisdictional gap** between the federal and the state regulatory organizations on issues such as technology upgrades and system security.
- More transparent, participatory and **collaborative discussion** among federal and state agencies, transmission and distribution asset owners, regional transmission operators (RTOs) and independent system operators (ISOs) and their members and supporting research is needed to improve these parties' understanding of mutual impacts, interactions and benefits that may be gained from these efforts.
- Continue working at a federal level on better **coordination of electricity and gas markets** to mitigate potential new reliability issues due to increasing reliance on gas generation; and update the wholesale market design to reflect the speed at which a generator can increase or decrease the amount of generation needed to complement variable resources.

Asset Management:

- Support **holistic, integrated approach** in simultaneously managing fleet of assets to best achieve optimal cost-effective solutions addressing the following: **Aging infrastructure, Grid hardening (including weather-related events, physical vulnerability, and cyber security) and System reliability**.
- **Urgently address managing new Smart Grid assets** such as advanced metering infrastructure (AMI) and intelligent electronic devices.
- Encourage utilities to investigate practical measures to shorten times to replace and commission equipment failures due to extreme events or other reasons.
- In the case of long-duration interruptions, all utilities should adopt improved measures to provide customers with a timely estimate of when power is to be restored.
- When extreme events occur it is important for post-event reviews to determine impacts and lessons learned for better management of future events.
- Infrastructure security requires a **new model for private sector-government relationships**. Overlapping and inconsistent roles and authorities hinder development of productive working relationships and operational measures.

- Perform **critical spares and gap analysis**. A detailed inventory is needed of critical equipment, the number and location of available spares and the level of interchangeability between sites and companies. Mechanisms need to be developed for stockpiling long lead-time equipment and for reimbursement to the stockpiling authority, be it private or government. Other approaches include standardizing equipment to reduce lead times and increase interchangeability.
    - U.S. DOE should continue to work with industry to ensure that the protection of spares and all assets is carried out and that transportation of large equipment is feasible. We further recommend actions that might lure domestic manufacturing back into the U.S. for units 300 KV and above. (Progress in this area has been made with post-9/11 efforts initiated by EPRI's Infrastructure Initiative in September 2001 to March 2003, as well as with the EEI STEP (Spare Transformer and Equipment Program), which has been in place since 2004. Utilities should also continue to work with industry and manufacturers to expand the existing self-healing transformer programs, such as efforts now underway by EPRI and ABB. Further, many utilities have mutual aid agreements on spares.
- Increased federal R&D for emerging technologies that may impact T&D grids, including new types of generation, new uses of electricity and energy storage, with an additional focus on deployment and integration of such technologies to improve the reliability, efficiency and management of the grids.
- Application of proactive widespread condition monitoring, integrating condition and operational data, has been shown to provide a benefit to real-time system operations, both in terms of asset use and cost-effective, planned replacement of assets.

Reliability, Security, Privacy, and Resilience

- Facilitate, encourage, or mandate that secure sensing, "defense in depth," fast reconfiguration and self-healing be **built into the infrastructure**.
- Mandate consumer data **privacy and security for AMI system**s to provide protection against personal profiling, real-time remote surveillance, identity theft and home invasions, activity censorship and decisions based on inaccurate data.
- Support alternatives for utilities that wish to reduce or eliminate the use of wireless telecom networks and the public Internet where there might be concerns about increased grid vulnerabilities. These alternatives include the ability for utilities to obtain private spectrum at a reasonable cost.
- Improve **sharing of intelligence and threat information** and analysis to develop proactive protection strategies, including development of coordinated hierarchical threat coordination centers – at local, regional and national levels. This may require either more security clearances issued to electric sector individuals or treatment of some intelligence and threat information and analysis as sensitive business information, rather than as classified information. National Electric Sector Cybersecurity Organization Resource (NESCOR) clearing house for grid vulnerabilities is an example of intelligence sharing.
- Speed up the development and enforcement of **cyber security standards**, compliance requirements and their adoption. Facilitate and encourage design of security from the start and include it in standards.
- Increase investment in the grid and in R&D areas that assure the security of the cyber infrastructure (algorithms, protocols, chip-level and application-level security).