Statement by Anna Scaglione, ASU

Chairman Bay, Commissioners, thank you for inviting me to contribute to this discussion.

One of the key issues with cyber-security is the inherent complexity of the task – there is no silver bullet. But information and visibility of the system is pivotal to detect and adapt to the inevitable vulnerabilities of cyber-physical infrastructures. A good example of how visibility can be gained is the deployment of thousands of Phasor Measurements Units (PMU) in the US. We are slowly seeing their benefits and more recently understanding their potential in aiding cyber-physical security.

The emphasis on modeling is certainly important (and I will go back to this point), but models are never perfect. Learning algorithms based on real data (particularly PMU data) capture aspects that are too difficult to model accurately or enormously painful to get right. I wish also to remark that most of these efforts in gaining visibility on the grid are still top down, and mostly concerned with the transmission grid. But with the increasing penetration of solar PVs and the potential of electrification of the transportation system, not to mention an aging distribution infrastructure, there is a need and opportunity to explore a third way, which is encourage the placement of intelligence and sensors at the distribution level. What I mean is not expanding or improving the Advanced Metering Infrastructure, but influencing directly what happens behind the meter and sensing pervasively the distribution grid. Perhaps the main methamorphosis should be at the distribution level and regulation should ensure that the transmission operations do not get in the way.

I would like to point out an important aspect about the power infrastructure by comparing it with other critical infrastructures.

- *In Transportation Networks*
  - *There is flow control (traffic lights, tolls) to manage congestion but largely it relies on "myopic" driver decisions*
  - *This is possible because there is feedback to the user: the service latency*
  - *Weather issues can be mitigated encouraging wise driver decisions*
- *In Communication Networks*
  - *Such as the Internet, cellular, Wireless Local Area Networks*
  - *human beings are not involved in the resource allocation → decentralized access protocols regulate million of points locally to contain congestion and cause gradual degradation*
  - *Feedback to the users is the service latency (or lack of service)*
- *In Power Systems Networks*

- *The resource allocation centralized at large (>100mW) and long term scales (>=5 min.) and local control does the rest*
- *The feedback to the users are black out. Their size often very large*

The surplus generated by electric power is largely due to the fact that the system is "plug and play" and energy is cheap and available.
Given the size and complexity of the grid, it is quite reliable and this relative success is an obstacle, as the different stakeholders do not want to invest in improvements and are not able to see the risk and the benefits of implementing best practices. They often do not understand that unlike weather events, cyber-attacks come without prior warning. Sensors in place could pick up anomalies and anticipate the future effects of an attack, but they of course have a cost. Understanding what to do about the risk, even if the first basic steps merely entail implementing best practices indicated in standards, is brain-power cost the industry is reluctant to invest.

But we are facing an exciting transition: industrial networked control is getting cheaper and even personal, not only being deployed by utilities at medium voltages but it is entering our homes, for our personal convenience, not necessarily to help the grid. Many see this as an expansion of the attack surface. But that brings about the opportunity of having many more responsive points that can be used to mitigate problems and going beyond the plug and play model that is strongly favoring fossil fuel generation, to a model that integrates intermittent renewables.

Digitizing the system and managing access to grid could allow graceful degradation in the face of daily congestion and emergencies, while maintaining the same ease of use for the public. In my opinion, we should embrace innovation and not give in to the argument that less information is more security or that we gain security by obscurity. We did not continue to use horses because cars could cause lethal accidents. In addition, digital systems become unnecessarily complicated and vulnerable when they are poorly designed.

We also have to recognize that we have made strides in the last ten years, especially in terms of regulation, research and awareness, if not application in the field, and are continuing to learn.

The Ukraine power grid attacks, the Stuxnet malware, Maroochy Water Station wireless jamming attack confirmed the now well-accepted principle that securing communications in the control area networks perimeter is of paramount importance. The good news is that there is evidence that the Ukraine event in particular could have been avoided by complying to the NERC CIP standard. The bad news is that the CIP and PRC standards are very often violated.

Other than direct experience, there is still gap in guessing what could happen. It requires simulating and analyzing jointly the coupling between information networks, power networks and controllers.
As Prof. Ilic mentioned in the previous panel, from the research side studying and modeling cyber physical attacks scenarios is still extremely difficult. I commend her continuing research effort in bridging this gap.
Many of the difficulties and issues lie in simulating realistically the power systems side, because of the endemic lack of data.
While in the computer networks field simulations on synthetic systems are a well established practice for testing their limits, and to verify mitigation strategies in cases of failures, for power systems those that do not have privileged or costly access to real data, rely on small test cases dwarfing the real power system and the functionalities of many controllers and subsystems in the field. Their functionalities are also often obscure, because of proprietary standards, custom design, that dominate the control industry, while in communication networks typically standards are open.

Going back to the point made about information sharing in the prior panels, the Cybersecurity Information Sharing Act of 2015 (CISA 2015) and the Fixing America's Surface Transportation (FAST) Act are steps in the right direction. But regulation needs to be compatible with the economic forces that are competing with compliance and cooperation objectives, adopting a system of carrots and sticks.

Perhaps what would help is to make it easy to share information. What may delay information sharing is addressing "how", from setting rules but also looking at the nuts and bolts on how digital information can be exchanged and queried securely, helping remove engineering barriers, as rules are set. What one wants to avoid is burdensome auditing processes that absorbs precious resources and can stifle useful innovation.

From my perspective it is readily apparent that we also need to find a way to share data for research purposes that allow realistic simulation and in some cases emulation of what goes on in the cyber-physical grid, without necessarily disclosing the true information about the system, yet giving information that can reproduce behaviors and trends that can be troublesome. As I mentioned test cases available for research dwarf the system at such a level that it remains questionable how techniques would perform in the field. Now this is, in principle, an easier problem to address than sharing information for operational purposes. There is a potential for the information to be "anonymized" and while this would not solve the problem of a real immediate threat, it would allow us to gain precious understanding about the threats that are looming out there, and invent new technologies to manage failures. There is significant research currently, for instance, in anonymizing medical records, or marketing information to protect consumers privacy. Some of these ideas have been directed to SmartMeter data, but they are not directly applicable to

anonymizing information for modeling systems. Advances in how to maintain digital privacy of the kind of data that are useful in the context of cyber-physical security would be a major gamechanger in my view.

Also, I wish to add that there is a significant barrier is that individuals that have deep technical knowledge about computer networks and power systems are still very few. This is in spite of the fact that a lot of the technological innovation in the sector comes by integration of embedded intelligence networking and sensing capabilities. I have to commend DOE efforts in sponsoring interdisciplinary research in Academia and in National Labs that is trying to overcome these barriers. I need to also mention that research institutions throughout the country are in the process of growing their programs in this interdisciplinary area

The other big question is how we can deal with evolving reliability issues? Very broad guidelines can help but in general complex regulation often stifles innovation. A standardization process should start at the engineering level, because is the engineering and physics that really determines what is possible and the creativity of the engineers that drives innovation and innovation that drives adoption. Nobody is excited about patching an existing system.

In this sense I see two aspects that can change.
First of all, I believe great benefit could come by doing almost away with closed proprietary standards and technologies. Suppliers of controllers, vendors and software and networks and their customers should sit at a common table and promote common open standards, helping the compatibility and interoperability of such standards, incorporating concrete innovation that has provable benefits or defining standards that are interoperable. Once again, this seems counter to the idea that we will have security, we tend to think that security is obtained by obscurity, but in fact it is important to share the collective burden of understanding and opening a technology is also the best way of "debugging it" and facilitating its seamless deployment. There can be multiple standards but often better and more timely standards emerge as the winners. I believe this process would also facilitate addressing other issues, like creating technology that is proven to mitigate electromagnetic pulses for instance. Also one should encourage innovative standards that facilitate the replacement and monitoring of transformers, as we know many are reaching their lifecycle almost simultaneously.
However, this would not be sufficient. The second action that could address the evolving reliability issues is to invert the approach and perhaps open more the regulation but set up a process to evaluate and approve standards as well as new proprietary technologies, rather than regulating it before it is proposed. This process could be similar to the approval of new drugs by the FDA, potentially involving institutions like NIST that have broad expertise, academics and lab researchers that are vetted to have no conflict of interest. ARPA-e and DOE have emphasized significantly the need of transitioning

research into technology, particularly in the grid security sector where the industry does not necessarily have sufficient staff with the necessary expertise to tackle the problem. I believe that preferential pathway for approving technologies that emerge from such projects, particularly those that are best aligned with urgent strategic objectives in the energy sector, may create a virtuous cycle.