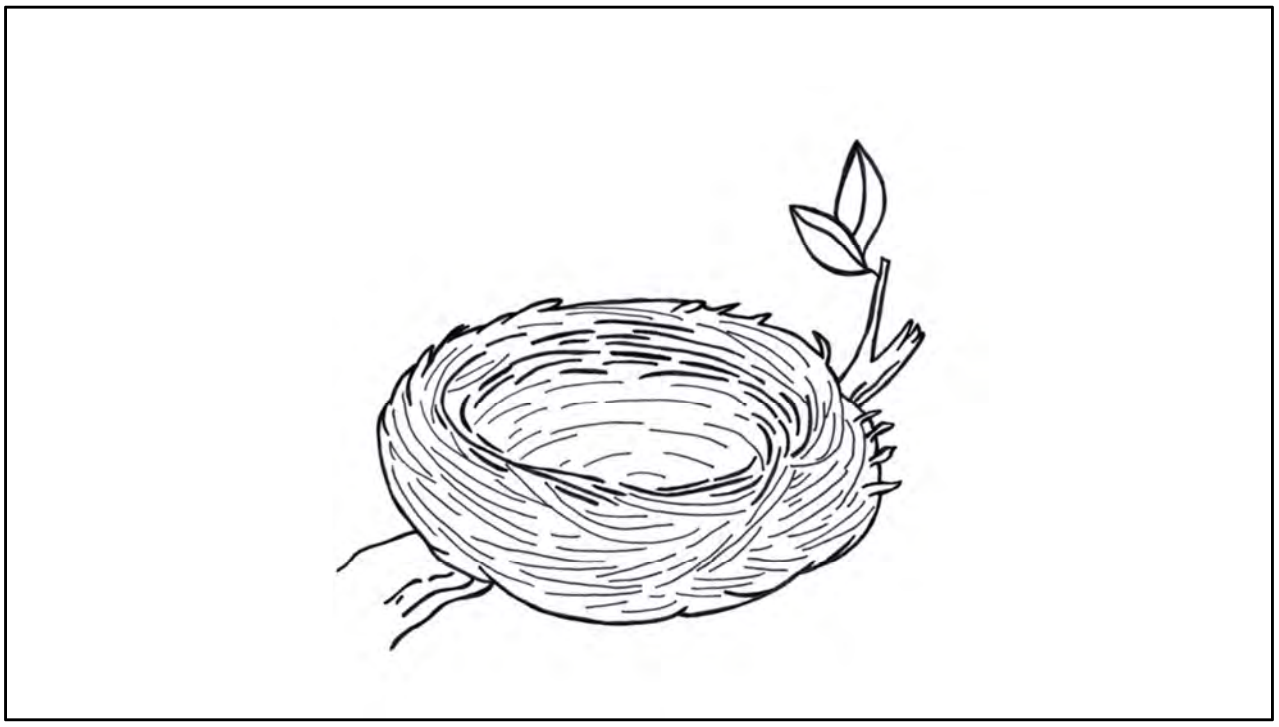
National Strategies on Cyber and Grid Security

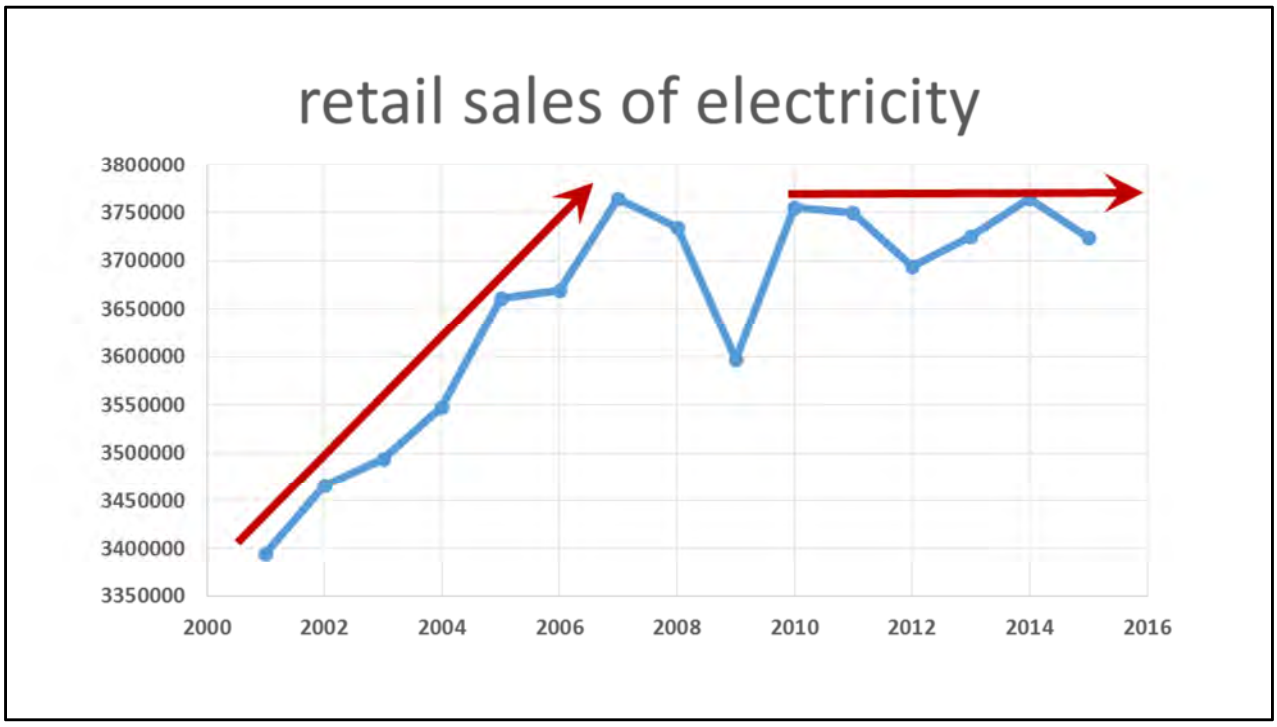
-Duane Highley, President/CEO, Arkansas Electric Cooperative Corp.
-Co-chair, Electric Subsector Coordinating Council (ESCC)

Arkansas cooperatives provide non-profit, member-owned power to 1.2 million Arkansans, about 1/3 of the population of the state, and cover 2/3 of the land mass.

We were recently recognized as one of Arkansas' Best Places to Work by Arkansas Business Magazine



A major change has occurred in our life. After 30 years of raising kids, my wife and I have experienced it …. empty nest!
This is a big change and requires some adjusting.

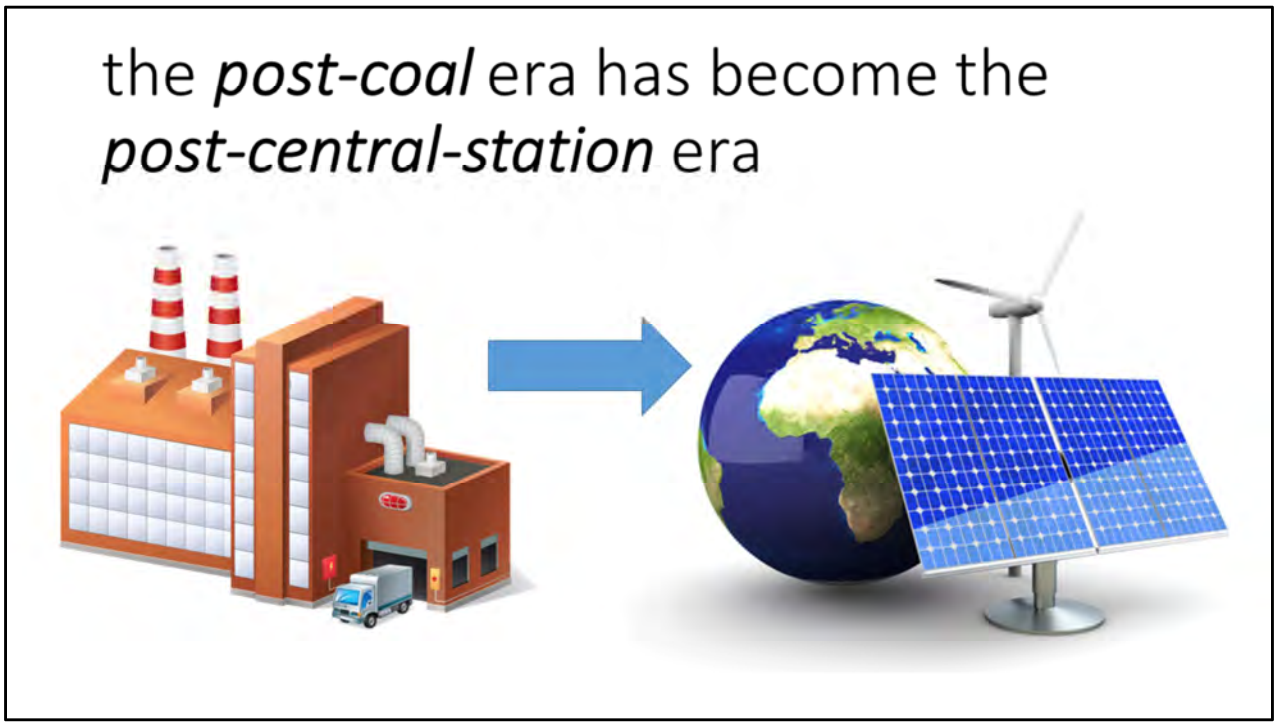


In the utility business we have also been adjusting to lots of change from business as-usual. For example, what used to be steady growth on a national level has changed.
The US has seen no net growth in electric energy sales since 2006, before the Great Recession.
(Source: EIA Monthly Report)

We have entered the Post-coal Era: Coal production dropped to its lowest level in 35 years, according to data released by the Energy Department. Coal production during the first quarter of 2016 dropped to 173 million tons, the lowest for any quarter since 1981. (The New York Times)
The largest coal companies are now bankrupt.

markets create incredible efficiency … at a cost

Organized power markets have changed the energy marketplace, bringing great efficiency and tremendous overall cost savings, but greatly increasing transmission-related costs as transmission is built to integrate remote renewables into the grid.

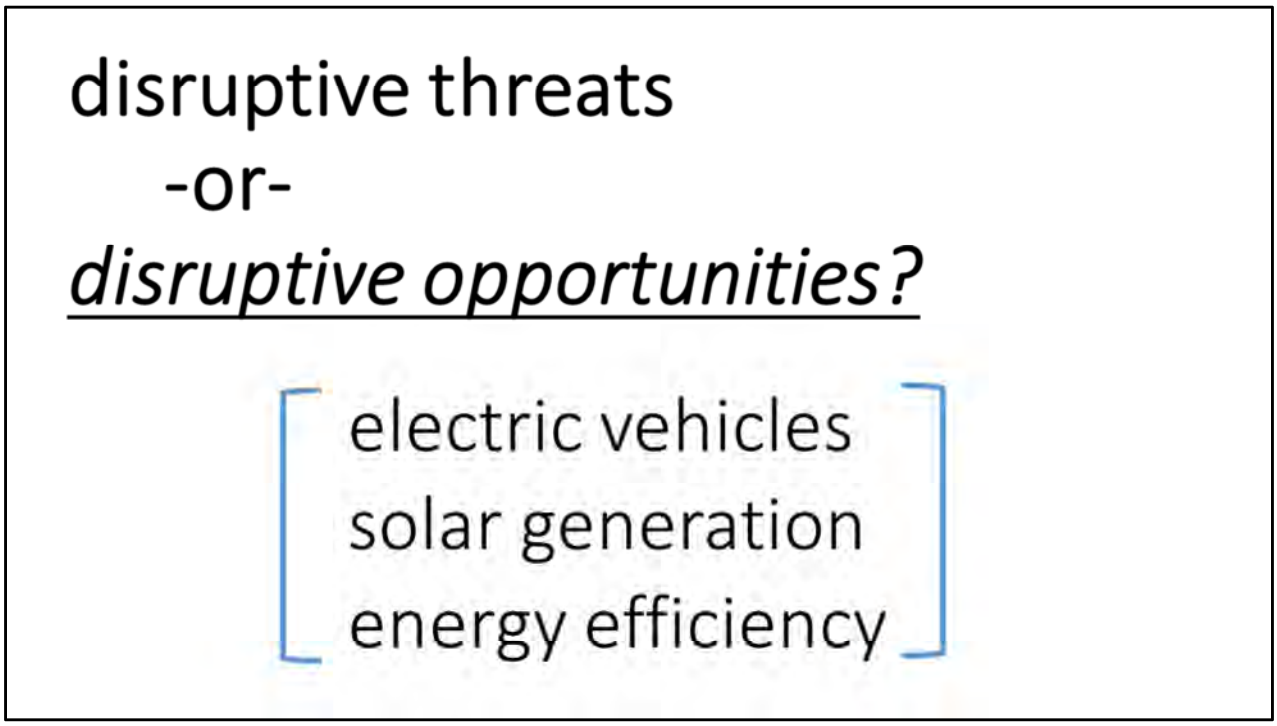


Five years ago I announced that we had entered the post-coal era. Utilities were no longer going to take the risk to commit to building a new coal unit. EPA Rules have now effectively outlawed coal-based generation. Now with increasing energy efficiency, self-generation, and new renewable resources, we have entered the post-baseload era. Most utilities are no longer planning to add anything other than renewables and peaking generation for the foreseeable future. This is the lowest-risk plan for most utilities, and it is the case in Arkansas.

new players

Apple has announced their entry into energy markets as a market participant, to be able to buy and sell energy. And why would they want to do that?

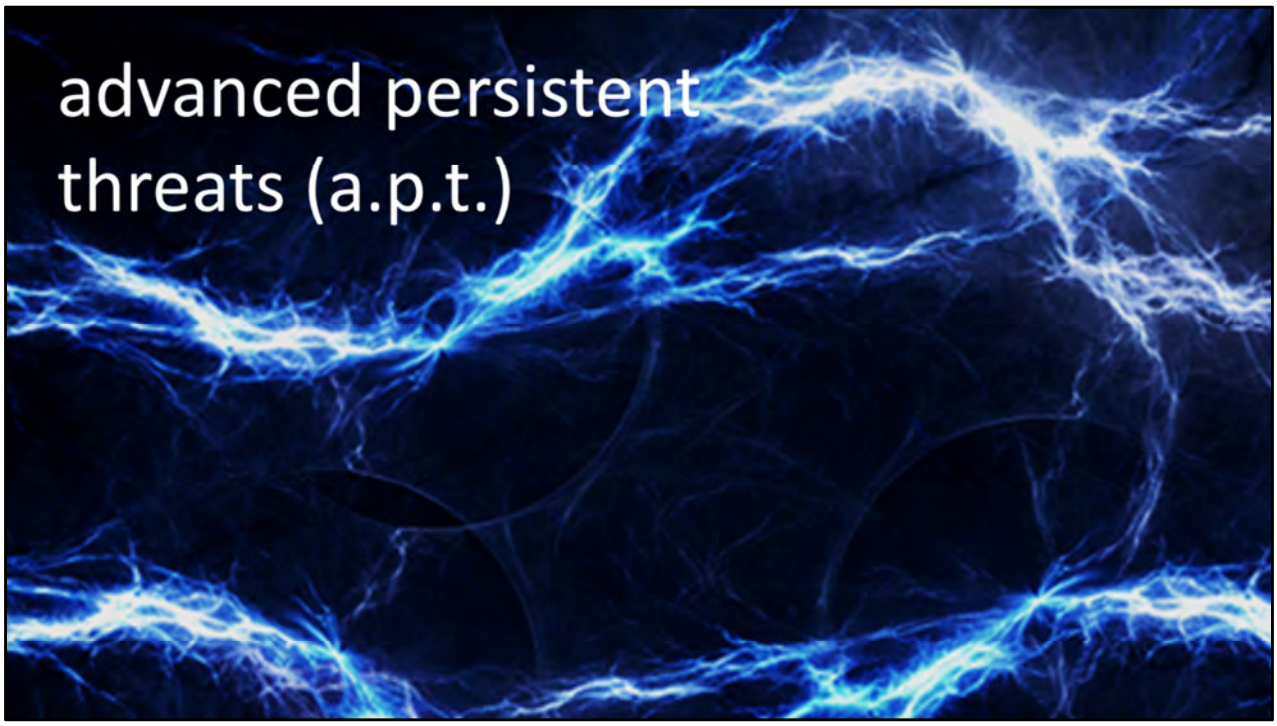
Why? That's why.
Imagine Apple selling an electric vehicle along with the contract for the electricity to power it.
Imagine them using the batteries in that vehicle to balance energy on the grid … a new source of revenue.



All these items – electric vehicles, solar generation, and energy efficiency – can be characterized as disruptive threats. We prefer to look at them as disruptive opportunities. We cannot stop these technologies from advancing – and we shouldn't – they are being driven by economics and consumer desire. As utilities, we need to learn to modify our business models to allow us to survive and even thrive as these changes occur.

new threats

This represents a new kind of unanticipated threat. How many have played it? How many ARE CURRENTLY playing it?
Example – a friend that suddenly found hundreds of cars stopping in front of her house.
A bad example – people climbing substation fences to capture the Pokemon monster.
Digital technologies and social media are enabling a new type of threat that we have to stay on top of.



Then we have APT – advanced persistent threats – Black Energy et al, such as was used in Ukraine attack.
(describe the attack)

Today utilities find themselves on the front lines of an international Holy War, directed at our infrastructure. North America has been protected by its oceans, and we have not had to fight a war on our soil, but today, digital technology allows our enemy to attack us from afar.
(describe ISIS recruiting video) This is a Holy War for them. Our adversaries will not be easily deterred.

Historically we built our utility networks on a system of trust. We have not planned and designed our networks with the thought of needing to be prepared for intentional attacks by foreign adversaries.

Koppel: “There is no plan.”

Ted Koppel hit the speaking circuit promoting his book, “Lights Out”. He claims that the electric utility industry and the Federal Government has “no plan” to prevent or recover from an intentional cyber or physical attack. He is wrong.

is there a
better plan?

Ted's recommendation: buy freeze dried food. You need to be prepared for a multi-month grid-wide outage.
Is this the best we can do?

defense in depth

- redundancy is our first line of defense

Historically Utilities built their systems to withstand all manner of natural disasters – tornadoes, hurricanes, ice storms, floods, earthquakes, squirrels and raccoons. An amazing amount of redundancy is built-in: facilities are designed to deliver the highest potential customer demand, experienced on the hottest or coldest days of the year, with the most critical facilities out-of-service. Because of this redundancy, we have many multiples of excess capacity on the grid on normal days. This is why the grid doesn't go down every time a power plant trips or a transmission line falls out of service. Its why the attackers in California were unsuccessful in their attack on a substation, and despite disabling 14 of the 17 transformers not a single customer lost power.

DHS: Sixteen Sectors

After 9/11 DHS established sixteen critical infrastructure sectors. Energy is one of those sectors, managed under the DOE as the "sector specific agency" or SSA. Arguably, electric energy is the most critical of the critical sectors, as so many of the others rely significantly on electric energy, such as water, communications, and banking.

The electric sector is one of only two sectors today (the other being finance) that are subject to mandatory, enforceable standards for cyber and physical security, issued by FERC and developed by subject matter experts under NERC. We just issued the fifth revision to those standards this summer – CIP5. Audits are routinely conducted. Violators are subject to fines and penalties. Compliance is not a choice for us, it is required.

"...we have to work ***beyond the standards*** to communicate between the government and industry to make sure threat information is shared and responses can adapt rapidly."

However, standards take a long time to develop. The grid wasn't built overnight. It is a complex interconnected system of generation, transmission, distribution and load which must all be coordinated. Changes have to be thought out and carefully implemented. This does not fit well with an area where new attacks are developed daily, an area in which our adversaries and looking to exploit each and every weakness. How can we respond more quickly?

This is one answer – a public/private partnership between the highest levels of government and industry. I serve as co-chair along with representatives from the investor-owned and municipal sector. About 30 utility CEOs meet regularly with our counterparts in government – deputy secretaries, assistant secretaries, and even the secretary level, to improve our response and recovery from physical and cyber attacks.

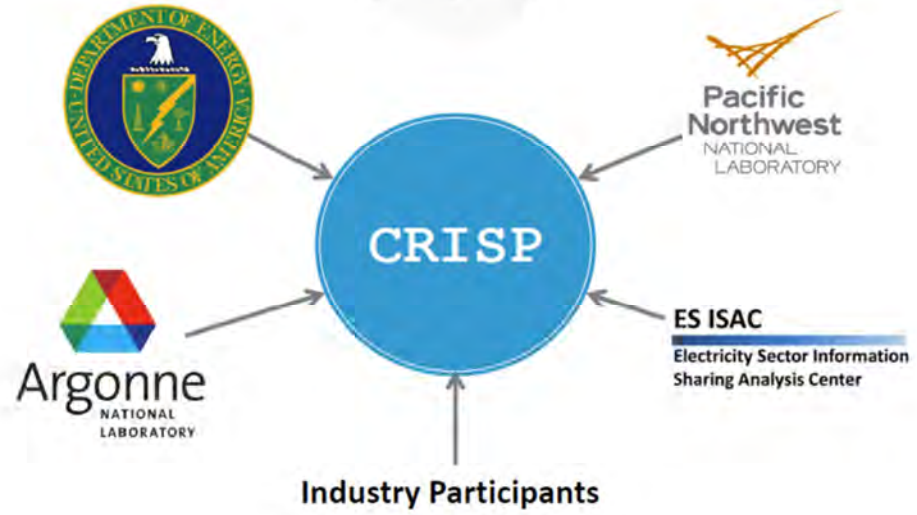
Information Sharing

DOE/DHS/White House/FBI/NSA/DOD

Our CEOs hold security clearances allowing them to receive confidential threat briefings from our government counterparts. When we understand the threat, we can mobilize industry resources to neutralize it.

Tools and Technology

- CRISP (Cyber Risk Information Sharing Program)

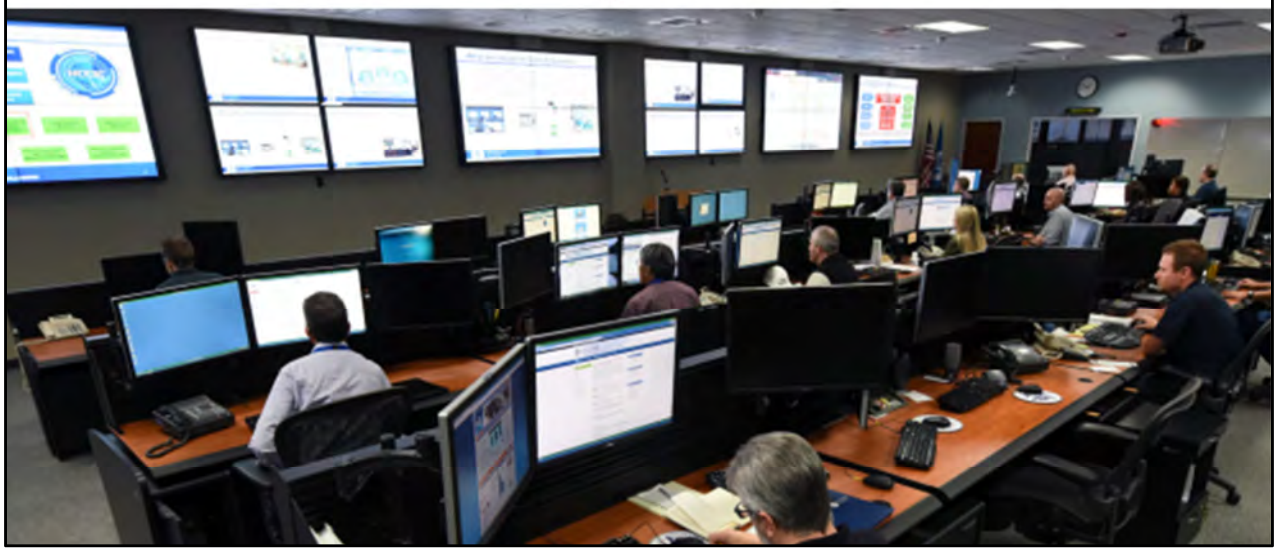


We have developed this tool in conjunction with the federal labs. It allows us to partner with the labs to leverage their knowledge of threats by sharing real-time information from utility networks. Today about 75% of all electric customers are covered by this technology, the details of which are classified. To cover the remaining 25%, which represent thousands of smaller utilities, we need to develop a less expensive and more flexible tool. This work is underway.

Electricity - Information Sharing and Analysis Center

Each sector has an ISAC; we encourage all entities to join one. It allows us to share threat information and bring it into one central location for enhanced situational awareness. Daily, weekly, and monthly reports are distributed between industry, government, and our cross-sector partners. Think of it like something from a James Bond movie. We even have a "Q" developing cool tools to thwart our attackers.

NCCIC: National Cybersecurity and Communications Integration Center



Information from the various ISACs is integrated into this center, run by DHS. It helps us connect the dots on potential attacks that may span multiple sectors simultaneously.

Response and Recovery – Cyber Mutual Aid

Much like the mutual aid that utilities offer each other following a major storm event, Cyber Mutual aid has been developed to allow utilizes to request assistance in a major cyber event by sharing critical staff and other resources.

STEP: Spare Transformer Equipment Program

There is a program for sharing critical spare transformers, which are no longer manufactured domestically and can have an 18 month lead time. STEP is managed by EEI, coops and munis can participate. It meets the concern expressed by FERC Chairman Moeller which he imprudently shared with the Wall Street Journal.

Spare Connect

Think of this as Speed Dating for utilities – find your match, someone that is likely to have similar equipment. You get together and share parts.
(In real dating, you are usually looking for that person with ***different*** equipment)

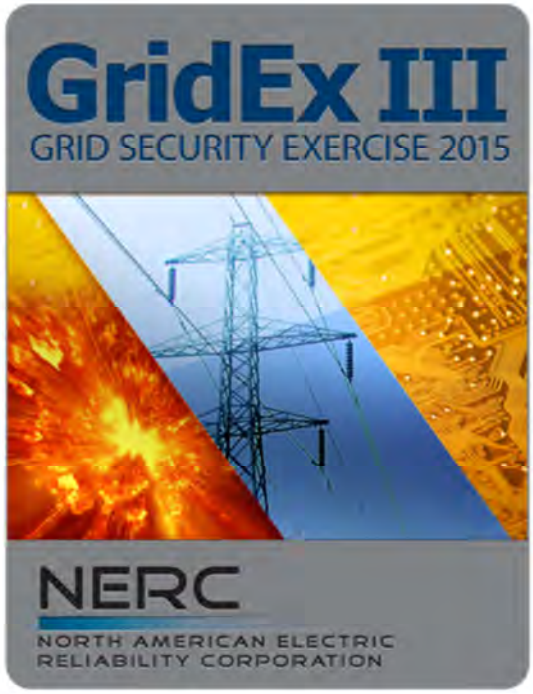
114th Congress F.A.S.T. Act

- **SEC. 61004. STRATEGIC TRANSFORMER RESERVE.**
- (a) FINDING.—Congress finds that the storage of strategically located spare large power transformers and emergency mobile sub- stations will reduce the vulnerability of the United States to multiple risks facing electric grid reliability, including ***physical attack, cyber attack, electromagnetic pulse, geomagnetic disturbances, severe weather, and seismic events.***

Congress approved the FAST act last year which gives the President special authority in the event of an attack, and establishes a strategic transformer reserve.

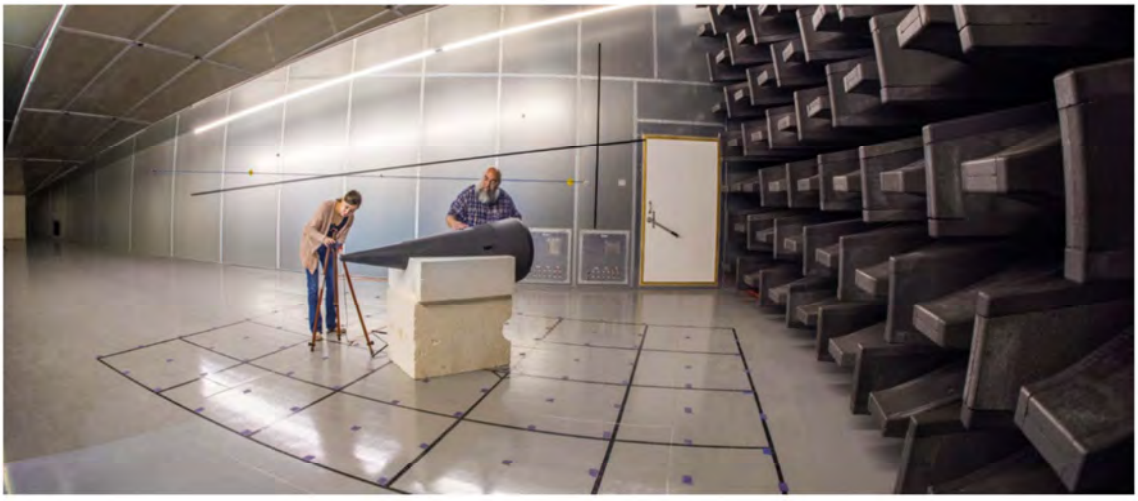
Preparedness, Drills

- GridEx III, over 4400 participants
- Next exercise November 15-16, 2017
- "cross-sector" exercise
  - Financial/Communications/Electric
- "Playbook"
- National Cyber Incident Response Plan
  - per PPD-41
  - DHS lead, coordinated with DOD and DOE
  - To be issued October 2016
  - 30-day comment period



As an industry we practice disaster response and recovery in concert with our local, state and federal emergency response partners. I encourage all states to participate in GridEX IV in November 2017. In a disaster, you get the performance which you have practiced and drilled. If you don't practice you will probably find yourself unprepared.

EMP Research – EPRI/DOE

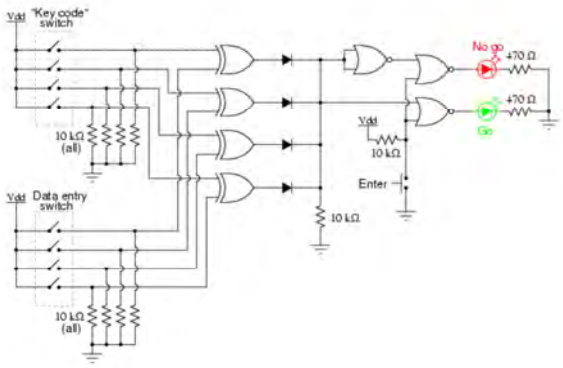


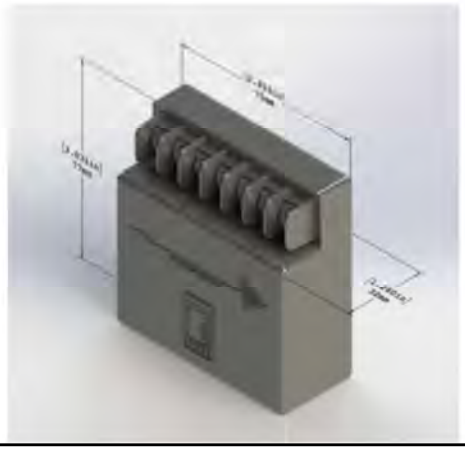
The Electric Subsector Coordinating Council visited Sandia Labs to see their testing facilities. They test nuclear weapons under the types of impulses and irradiation that might occur in a nuclear attack. Because of this unique testing capability, they can be a partner with utilities as we research ways to mitigate the effects of a potential Electromagnetic Pulse Attack or portable directed energy Electromagnetic Pulse weapons.

Another one of Sandia's magnificent testing apparatus, capable of sending a high-intensity pulse of radiation into large utility equipment for testing. We look forward to implementing the fruit of this testing.

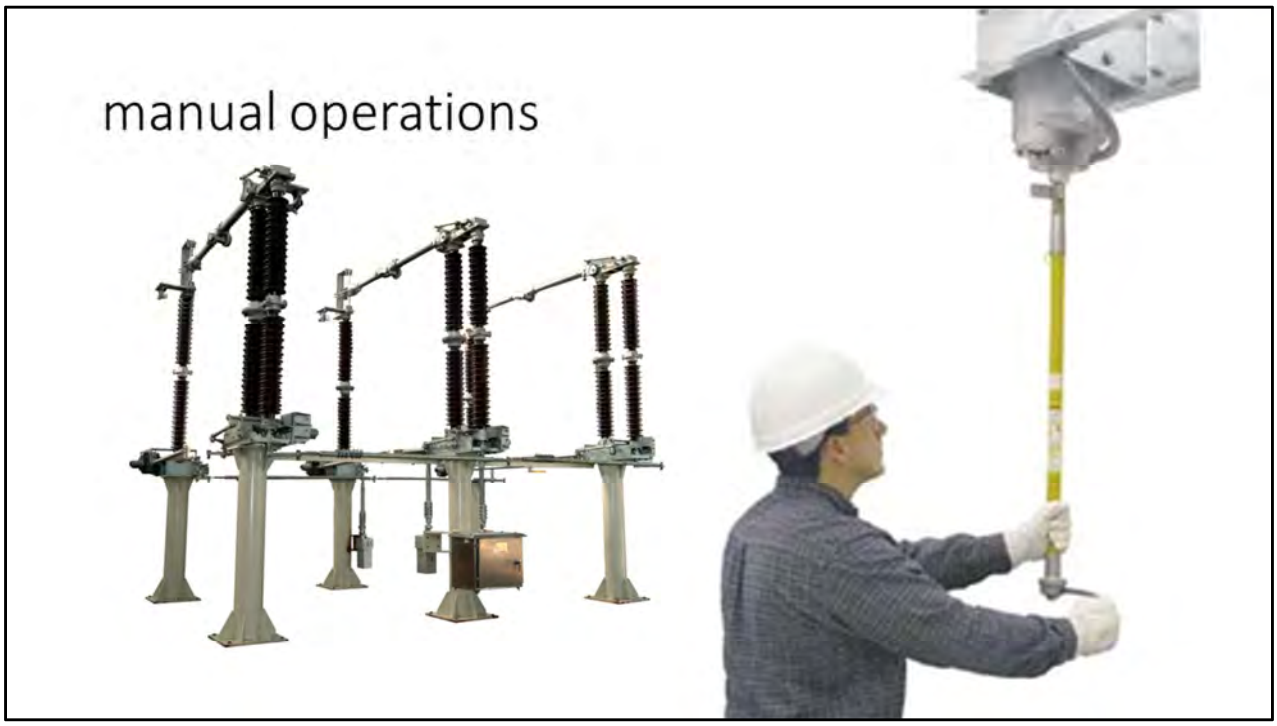
new (old) technology

- rediscovering analog circuits





Remember Q, the guy at the utility-operated James-Bond-like intelligence scanning place? He is helping to develop analog devices, which cannot be hacked, to supplement our existing digital controls to prevent certain types of cyber attacks. By converting some of our equipment from digital back to analog we can avoid a number of emerging threats. This is just one example of the new way of thinking that must sweep across all aspect of our society as we adapt to a world where intentional attack is all around us. Even our little system sees 200,000 electronic attack attempts per hour. To repel these our technicians have to be right every time. The enemy only has to be right once to succeed.



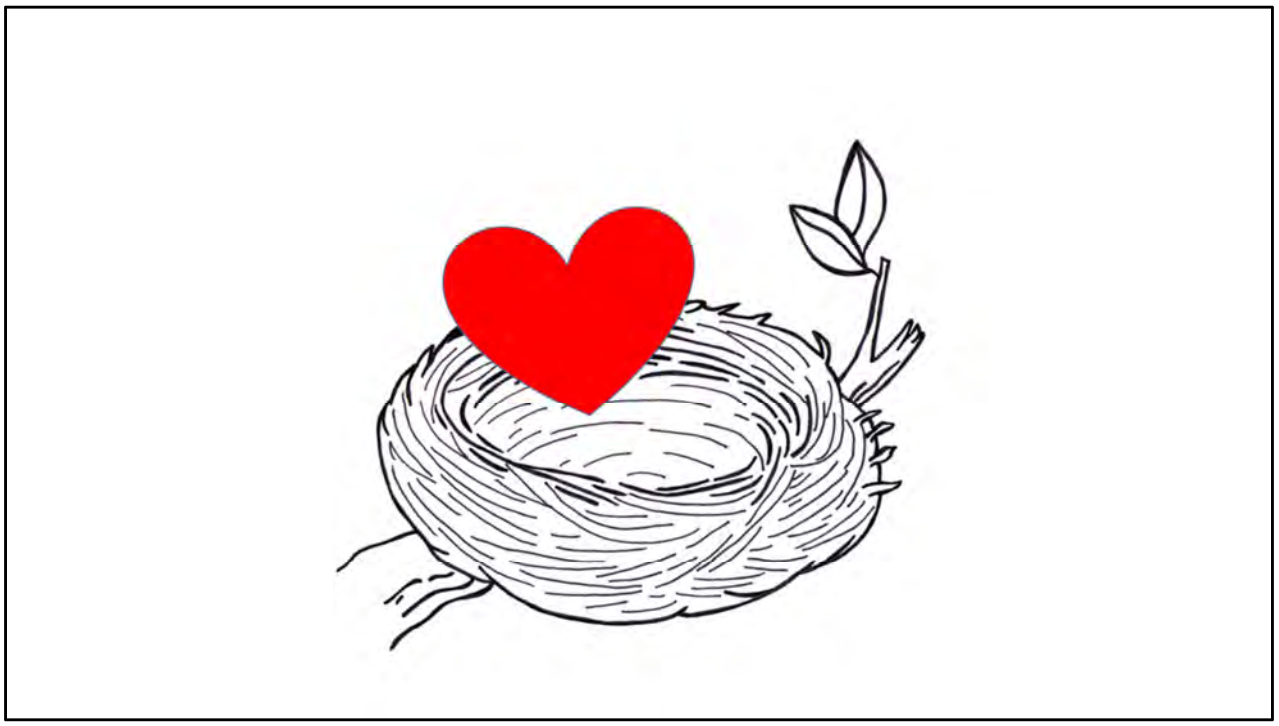
Another area that we are exploring – manual operations. Just like the old days, we can always send operators out to the substations to manually operate switches. This was done in order to recover from the Ukraine cyber attack which disabled the utilities' control computers.

Transition Planning

A November meeting has already been scheduled with transition teams from both Clinton and Trump. We want to keep the momentum of our efforts and not lose any ground in the transition from one administration to the next.

Ted was wrong.

I want to leave you with this: Ted was wrong. There IS a plan. We work closely with our government counterparts to continually improve it. We practice response and recovery. And while we cannot promise that there will never be a successful attack (after all, this is warfare) we can say that we are doing everything that we can think of to make the success of any attack extremely unlikely. Our enemies continue to develop new threats daily. This is war. We cannot rest.



All this sounds negative, but in reality I am very optimistic about our future. We just have to change our way of thinking about security and change the way we design and operate our utility systems, by realizing that we can no longer trust the public and just prepare for natural disasters and equipment failures. We now must consider intentional threats. This is a change, but one that we can adapt to. Just as my wife and I have adapted to our empty nest and rediscovered new ways that we can enjoy life together, we as a utility industry can also adapt and change. It's what we've done for every threat before, and it's what we'll do for this one too. Thank you for inviting me to speak today.

reliable • affordable • responsible