Report of Discussions from Breakout Sessions

Annual Industry Workshop
March 28-29, 2016

iHotel and Conference Center
University of Illinois at Urbana-Champaign

CREDC IS FUNDED BY THE U.S. DEPARTMENT OF ENERGY AND
THE U.S. DEPARTMENT OF HOMELAND SECURITY

Contents

About CREDC

The Cyber Resilient Energy Delivery Consortium (CREDC) is composed of ten universities and two national laboratories, led by the University of Illinois at Urbana-Champaign, conducting a variety of research activities in support of the cyber security and resiliency of energy delivery systems. Sponsored by the Department of Energy (DOE), CREDC follows from the earlier Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) project. CREDC's research scope has expanded to encompass energy delivery systems outside the electric power sector, including oil and gas, as well as the complexities introduced by coupled energy infrastructures. CREDC conducts activities with anticipated deliverable prototype technology in an 18- to 24-month timeframe, as well as longer-term research that anticipates the impact of emerging disruptive technologies, such as big data and cloud environments as well as the Industrial Internet of Things (I^2OT). The research is guided by an Industry Advisory Board and is often done in coordination with industry partners to maximize the beneficial impact of CREDC research on the sector.

The consortium includes researchers from Argonne National Laboratory, Arizona State University, Dartmouth College, the Massachusetts Institute of Technology, Old Dominion University, Oregon State University, the Pacific Northwest National Laboratory, Rutgers University, Tennessee State University, the University of Illinois at Urbana-Champaign, the University of Houston, and Washington State University.

The inaugural CREDC Industry Workshop was held March 28-29 at the University of Illinois, and was followed by a review/board meeting on March 30 involving the CREDC team, DOE sponsors, and the CREDC Industrial Advisory Board (IAB). The workshop featured presentations by Henry (Hank) Kenchington from the Department of Energy, Richard Jackson, CREDC IAB member and formerly with Chevron, and Tim Conway who presented an extended session based on the Ukrainian Defense Use Case. The workshop also included a number of moderated breakout discussions on topics impacting cyber resiliency of energy delivery systems (EDS), lightning talks, and a session summarizing highlights from the breakout discussions. The event concluded with a research poster session/networking reception and dinner. At the review/board meeting, the CREDC team and the IAB explored how CREDC should reach out to multiple EDS sectors, particularly oil and gas.

The industry workshop hosted 142 participants – 69 from the CREDC team and 73 from non-CREDC organizations. Nine out of ten of our Industrial Advisory Board members were able to attend both the workshop and review meeting. The poster session featured 35 research activity updates.

Archives from the industry workshop are located online at:
http://go.illinois.edu/CREDCIW16CONTENT.

Breakout Discussion Section Summaries

Participants were asked to join one of several moderated discussion groups on relevant topics impacting EDS cyber resiliency. These topics had been identified by the CREDC leadership while organizing the workshop. Each breakout discussion section was led by a moderator, and a scribe took notes during the discussion. The session topics were

- Challenges to EDS cyber resiliency from an expanding attack surface
- Regulatory Compliance
- Cross-Sector Issues
- Data Analytics for EDS Security
- Evolving Adversary
- Human Factors and Usability
- Supply Chain Security
- Workforce Development, Training, and Education

The following is a summary of the discussions in the breakout groups, edited from notes taken by session scribes.

Challenges to EDS Cyber Resiliency from an Expanding Cyber Attack Surface:

Adoption of commodity operating system and networking technologies, deployment of ubiquitous measurement and control, intelligence of field devices, integration of distributed energy resources (DER), increased use of Internet-connected devices (“internet of things”, or IoT), wireless (WiFi) connectivity, and connections to third party systems are just some of the ways in which the cyber attack surface in EDS is expanding. The growing complexity may also increase the chances of an inadvertent failure.

Discussion participants noted the issue of mixed-legacy environments, where securing the interface between the old and the new presents significant challenges. Increasing complexity results in too many components to protect, so that the need to identify critical components is important. Migration of communications from legacy serial to Ethernet-based solutions, for example, increases efficiency and safety, but may introduce new vulnerabilities. On the other hand, the legacy serial communications achieve, at best, "security through obscurity."

Cyber technology in EDS consists of EDS-specific systems built upon commodity platforms and using network technology not specifically developed for EDS. Vulnerability alerts and patches for the commodity operating systems on which EDS operational technology (OT) is built can be problematic.

Third-party involvement, driven by economic factors as well as by relations with vendors, partners, service providers, and customers, presents a challenge. It is hard for EDS asset owners to understand the attack surface.

IoT was seen as a path to upgrade the infrastructure in ways not previously possible, but the sector needs to be aware of risk.

Some current approaches to addressing the challenges include:

- Security configuration backup: The ability to roll back to an earlier technology generation that cannot be compromised by some vulnerability introduced in new technology.
- VPN access to vendors for required system maintenance, as opposed to traditional access via modem.
- Certification by organizations such as the National Information Assurance Partnership (NIAP) and the International Society for Automation (ISA) Security Compliance Institute (ICSI).

Participants identified the following as important research topics:

- Software-defined networking (SDN) may eventually result in more secure and resilient communication, but the associated risks are not sufficiently understood.
- Cloud computing may address some security issues, but introduces others, and issues of time-criticality have to be addressed.
- Mobile computing is gaining increasing adoption, for example, in wireless access to distributed field devices such as poletop components in electrical systems. Under TCIPG, the University of Illinois developed a secure solution for a technician to log in securely to a tablet at the start of his or her shift (with his or her own/company's unique password), then during the day access field devices in a wireless manner via a context-aware authentication scheme between the field device and the tablet. This means that the secure access information to a field device (i.e., login password to the field device) is tied to the physical environment context (e.g., location, temperature, wind pressure) where the field device is embedded. This new password generation and with it the context-aware authentication protocol enables unique password and hence overall secure access for each field device, a significant security improvement over the common practice that all field devices share a password known to many.

- Better modeling and understanding of complex, multi-stage attacks targeting heterogeneous components.
- Continuous security monitoring, integrated with data analytics, and respecting the special availability and time-criticality constraints of EDS.

Regulatory Compliance:

This session addressed issues of regulatory compliance and best practices as these impact cyber security in EDS. Much of the discussion dealt with the degree to which a "culture of compliance" advances security.

Cyber assets in EDS are subject to a variety of regulations from a number of agencies. In the US, almost all "critical infrastructure and key assets" (CI/KR) fall under the aegis of the Department of Homeland Security (DHS). DHS generally directs use of the National Institute of Standards & Technology's (NIST) "SP800 Series" of cybersecurity guidelines in those sectors. Note that they are guidelines, not mandatory and enforceable standards under law.

The bulk power system (interstate transmission networks operating above 100kV, and mostly larger generation assets that feeds it) is unique among industrial CI/KR sectors in that it is regulated by law under the North American Electric Reliability Corporation's Critical Infrastructure Protection Standards ("NERC CIPS"). NERC's authority originates in its designation as the "Electric Reliability Organization" by the Federal Energy Regulatory Commission (FERC) as directed by Congress in Section 215 of the Electric Power Act of 2005.

Interstate pipelines are regulated by the Department of Transportation and the Environmental Protection Agency, with oversight of some elements of port and terminal operation administered by Department of Homeland Security and FERC. These regulations are largely focused on safety, environmental protection, physical security, and limited elements of control systems cybersecurity. Some states regulate utility systems in other areas such as customer privacy (data protection), but these areas are still in early stages of legal and regulatory evolution. There is also the matter of dams used to generate typically lower-volume electricity, where cybersecurity is also generally not as advanced as in other sectors.

The goal of regulation is to increase security of EDS operations, and the role of compliance is to demonstrate that this has been done, in the form of auditable artifacts for verification. However, some motivation behind regulation stems from the belief that in the past voluntary adoption of best cybersecurity practices has not been effective relative to risk to public well-being. There is a widespread perception in the utility sector that regulatory compliance with respect to EDS cybersecurity can become an end in itself, without necessarily improving security. The standards say very little about how protection must be accomplished. But internal utility legal staffs have in some instances been overzealous to ensure that findings of non-compliance are avoided, seemingly at any cost. Accordingly, large administrative systems have been developed by utilities, motivated by assembling what is needed to document proof of compliance. The end goal is clearly effective cybersecurity, but emphasis has been placed on compliance proof by many EDS asset owners.

In spite of these concerns, participants in the discussion agreed that EDS sectors are doing a decent job addressing cybersecurity, even if dealing with cyber issues has been a "cultural upheaval" (in the words of one participant), especially in the area of "field asset management,"

pertaining to securing dispersed cyber assets in substations. Regulators at all levels will generally concede that the electric sector has come far in improving cybersecurity, albeit in some ways still not effective relative to degree of risk.

The participants identified the following areas as roles for research by CREDC:

- Compliance tools which are simple and usable.
- Tools that demonstrate compliance and simultaneously improve security.
- Islanded asset management ("Islanded Asset" is a cyber asset not connected to a network, possibly for reasons of security or compliance. Managing such assets, in the sense of reconfiguration, software update, or downloading audit logs requires physical access).
- Tools for baselining EDS equipment and secure, auditable change management.
- Security analysis of Software-Defined Networking (SDN) and Network Functional Virtualization (NFV), which many feel have promise in improving security of network edges and segments.
- Security analysis to support wireless communications within the concepts of the standards, possibly modifying them to align with the security objectives.
- Transition and commercialization of the results of the foregoing research.

Cross-Sector Issues:

Many EDS stakeholders are active in multiple EDS sectors. Many providers of OT and industrial control systems have customers in multiple EDS sectors. There are also sector inter-dependencies that should be explored. While there are important differences between OT in various EDS sectors, there are a number of similarities, particularly when we consider cybersecurity.

- Many EDS are characterized by components with widespread geographic distribution. Supervisory control and data acquisition (SCADA) systems control dispersed assets, such as electric power transmission and distribution as well as O&G transmission and distribution pipelines, and distributed control systems (DCS) control processes in a local area, such as electric generation control in electric power, or process control within O&G refineries and processing plants. In both the electric and O&G sectors, a DCS often interfaces with one or more SCADA systems.
- Long-lived assets. The cybersecurity issue of legacy and mixed-legacy systems arises in multiple EDS, and is in some sense difficult to address in the long term, because the lifecycle of the "cyber" part of a cyber-physical component is much shorter than that of the "physical" part. Legacy systems often present challenges to the adoption of some security measures in EDS, because they may be too constrained as far as computation and communication capacity to support encryption or survive aggressive vulnerability assessments.
- Supply chain management is a challenge. Manufacturers and suppliers of ICS hardware and software for all EDS sectors are global companies. Subassemblies and firmware may

be developed in a global supply chain. Asserting that rogue functionality has not been inserted somewhere in the development cycle is a common concern across EDS.

- Similar best-practice reference architectures, with the objective of strict separation between IT and OT and segmenting networks and devices according to functional zone.
- Some systems and communication protocols are common across the EDS sectors.
- Vendors in general provide components to multiple sectors. The systems provided by vendors to different sectors have similar software architectures and may even share the same codebase.
- With respect to customer-level gas and electric service, there are similar business models and components on the customer and distribution sides. For example, utilities that provide gas as well as electric service are deploying customer-premise smart meters for both gas and electric.

There are differences in EDS implementations of OT and security efforts. One of the most significant differences between EDS is the regulatory environment and compliance requirements discussed previously.

Typically, OT components in EDS sectors collect measurements at multiple points in a process (temperature and pressure in an O&G system, voltage and current in an electric system), analyze those measurements according to computer models of system operation, and then issue control commands to maintain safe and efficient operations and respond to dispatch requests, typically with a human operator in the loop. Some of the attacks of concern across EDS sectors include:

- Attacks to the communications, which can blind the operator to the current state of the system.
- Misconfiguration, in which the settings on a device are altered so that it will respond inappropriately to certain system states. This can be a dormant attack in the sense that the attack may not be evident until certain system states arise (for example, a relay may be configured to trip at a current level within the rating of the line in question, causing an unnecessary outage, or a valve may be configured to remain closed even in the case of a dangerous overpressure).
- False data injection/ false measurement injection, with the intent of triggering incorrect and potentially dangerous control actions. This can be accomplished by compromising measurement components or injecting false measurements into network traffic.
- False command injection, in which the adversary issues incorrect commands to control devices. This can be achieved by compromising the HMI from which control commands are typically issued, or by injecting false commands into the network traffic.
- Man-in-the-middle (MITM) attacks, in which an adversary intercepts and modifies or retransmits the command or measurement traffic on the network. (This can be an adversary's strategy for either false data or false command injection.)

- False view, in which the HMI is compromised to lead the operator to believe that the system state is something other than what it actually is at any given time.
- Undetected and unauthorized changes to firmware and programs involved in the operation of the EDS. The compromised system may present a greater risk than false commands or false data attacks would.
- Blended attacks involving simultaneous or near-simultaneous attacks against physical and cyber components, perhaps (for example) to degrade a cyber response to the physical attack.

Interdependencies among EDS infrastructures have been characterized in terms of four general categories, as follows:

- Physical interdependency (e.g., the material output of one infrastructure is used by another). A petroleum products pipeline making use of commercial electricity to pump fuel oil to the electric company's generators is one example of physical interdependence between infrastructures.
- Cyber interdependency (e.g., infrastructures utilize electronic information and control systems). A telecommunications infrastructure supporting SCADA or other control systems for EDS or water systems is an example of cyber interdependency.
- Geographic interdependency (e.g., infrastructures are co-located in a common corridor). A natural gas pipeline located in the right-of-way corridor of a high-kVA transmission line is an example of geographic interdependence between infrastructures. Large O&G installations typically include on-site power generation and water treatment.
- Logical interdependency (e.g., infrastructures are linked through financial markets). A natural gas market center (hub) receiving information on current pricing, purchase contracts, and short-term storage agreements is an example of logical interdependence between infrastructures.

Data Analytics for EDS Security:

The development of data analytics for EDS requires exploring new techniques that are specific to their operational technologies, whose unique properties include their system models, data sources and physical measurements, and timeliness of analysis. Currently, different EDS domains (e.g., refineries, power systems) employ a variety of analytic techniques to improve control and safety of their systems, some that are fully automated and some that are partly automated and require a human in the loop. These current systems can be used as a starting point where we can learn from already effective data analytic techniques for EDS domains to improve the overall robustness to new threats that can come from their complex cyber-attack surface. For example, oil and gas domains commonly deploy protective safety systems that utilize data analytic techniques based on simplified system models to alarm operators to unsafe conditions. Similarly, power systems utilize analytic techniques to ensure the safe operations of the infrastructure, including a suite of protection systems and contingency analysis applications based on sensor feeds and simulation.

Large and distributed EDS infrastructures create challenges in identifying correct bounds on models for types of analysis. Information sharing is a key problem, as researchers must have access to accurate data and models. While the physical systems are interconnected, data

pertaining the different parts of the system may not be shared or may be limited. Accurate system models are fundamental for the success of any data analytic technique to attain situational awareness. The modeling must be done at the appropriate time scale and scope for the type of response and decision that is expected from the analytics.

Fortunately, there are other properties which simplify the monitoring of EDS compared to other domains where data analytics are used. For instance, in IT models of end-nodes where human can be in the loop, one must often incorporate complex and non-deterministic human behaviors, while in EDS the physical infrastructure is bound to behave according to very specific physical laws which makes the data feed from physical sensors often easier to model. Unfortunately, the gap that exists lies in the development of accurate system models, or of methods to adaptively derive model parameters from the data. Another issue is that, currently, there is a lack of real-world data to help support the research, design and validation of models, as most utilities and vendors categorize information regarding the operation of their cyber systems as proprietary (often more so than the physical models). Improved anonymization techniques and the ability to generate models that are realistic could help address this concern in the future.

These analytical techniques will require accurate and consistent data in order to produce meaningful results. While phasor measurement units (PMUs) provide a significant amount of accurate data for the power grid, there are concerns that we will become overly dependent on this data. This may be catastrophic if we overly focus on certain data types and overlook other key data points. For instance, safety mechanisms in EDS traditionally ignore the analysis of the configuration and traffic in control area networks, which could indicate if the data are trustworthy. Small errors in either the data, or our interpretation of the data, could lead to inaccurate conclusions and overconfidence. Furthermore, as mentioned before, lack of oversight on the process that delivers the data to the analysis engines undermine the ability to determine the trustworthiness of the various data sources that are used to perform the analytics. On the other hand, attacks can go under the radar of data analytics even if all of these aspects are taken in consideration by carefully crafting attacks that evade algorithms intended to detect bad data. Analytical techniques based on learning may produce opportunities for intelligent attacks that exploit “concept drift” by inducing small changes over time in order to cause the learned system to consider these changes normal.

Timeliness is another key factor as different system operation and security activities are performed at different timescales. Some tasks, such as intrusion detection and response, may need to collect and process data in real-time in order to prevent the attack from damaging the EDS. However, other functions, such as forensic analysis and data sharing have much longer timescales. Researchers must work with EDS operators to ensure that their techniques work within the appropriate timescales.

Evolving Adversary:

Stuxnet and more recently the Ukraine incident demonstrate that attacks against OT are not hypothetical, and can have significant destructive impact. The most advanced attacks are increasing in sophistication, but today’s sophisticated attack requiring the backing of a nation state or major crime syndicate is tomorrow’s ordinary hacker toolkit.

The group noted that adversaries are becoming more aware of the physical aspect of EDS, having moved beyond repurposing IT attacks. The implications of ransomware attacks, for example, in which an adversary locks up a system (by encrypting the file system) have different impact and criticality in EDS than in conventional IT.

The group identified information sharing as a means of maintaining awareness of evolving adversaries, but the consensus was that EDS stakeholders are not doing this well enough. There are disincentives to sharing information in the case one's system is compromised. There are commercial initiatives from, for example, Google and Symantec to facilitate this. There are also various information sharing and analysis centers (ISAC) for critical infrastructure sectors, including energy. It was noted that adversaries share information on systems and attack techniques, with the evolution of what might be termed adversary marketplaces.

In summary, techniques to characterize the evolving adversary and anticipate future attack strategies include more effective information sharing, tracking adversary marketplaces, and participation in conferences such as DEFCON.

Human Factors and Usability:

A frequent complaint about cyber security solutions is that they are difficult to use and can get in the way of actual operational requirements. Well-intentioned users may circumvent security controls simply to get their jobs done. Also, many OT operators justifiably view availability as the most critical security property, and may consider practices such as shared passwords acceptable so that any operator can run the system. Issues raised in the discussion included:

- There is a mismatch between usability and security standards and practices. This is especially acute in OT where IT security practices can be problematic.
- The human is the weakest link (although a vocal minority felt the opposite: rather than blaming the humans for not matching the technology, we should fix the technology to match the humans). We need to figure out the physical and cognitive limitations of the people using the system.
    - Cultural change is a significant factor in usability - people will do things differently if they understand how doing so enhances EDS security.
    - Build security into the system to enforce security (shrink the usability space) - because changing people is hard and can take a long time
    - Train people about IT security differently, and train OT people to understand why safety is important. Narratives that actually say what would happen in case of a breach would motivate people to be safe.
- Make technology more usable by providing tools to assist the user in uncertain environments

(Note: The previously described TCIPG research into authentication in field device environments addresses the shared password issue in a usable manner).

As next steps, the group suggested continuing the discussion, convening meetings with users and vendors, and research into cultural change as it applies to security.

Supply Chain Security:

Manufacturing is now a global undertaking, and most modern OT equipment has components, subassemblies, and firmware built or developed in multiple countries. While acceptance testing can verify that a component or system performs its designed function, it is difficult in practice to establish that it does not contain additional rogue functionality. This session identified concerns arising from this reality, and explored ways to achieve trust in OT systems.

Supply chain security is viewed as a major concern across all EDS sectors.

Based on the discussion, the group listed supply chain issues of interest to various stakeholder communities during system lifecycle in the following table.

	Vendor	Distributor/Integrator	Customer
Design/Build	Common minimum features/standards/certifications across international markets Hardware-integrity of subcomponents Software-use of open source Insider (developer) threats: bad guys have lots of patience		How does the customer specify cyber-requirements? What is involvement of customer with managing supply chain risks?
Delivery/Installation		Very long distribution chain vs minimal chain (different issues) Tracking/installing per vendors' instructions Insider threat	Acceptance Testing
Operation	How does vendor know what patch level exists at each customer? How does vendor know who currently owns its products? React to security defects Root cause analysis for defects		Verifying chain of custody Patch management Root cause analysis

The group also identified the following "Meta issues:"

- Who owns the risk?
- Role of secure code development techniques.
- How do open testing and certification fit?
- What is the role of government?

Workforce Development, Training, Education:

The required skills of energy delivery system professionals continue to evolve and expand. The challenge is to retain the skills of the existing workforce that knows how to operate the systems

without the advanced controls while growing a workforce that also has critical cybersecurity skills as well as the sophisticated knowledge required for system operation. Developing this modern EDS workforce requires clearly defining tasks and responsibilities and creating a well-defined path leading toward an energy delivery security career.

Attendees in this break-out session included representatives from industry, academia and research laboratories. During this session it was noted that university students need an incentive to pursue special training and courses to become energy cyber security professionals. Energy-related industries and educational institutions need to communicate with each other and develop partnerships to identify necessary skills and to develop training opportunities for current and future energy cyber security professionals. It was determined that an EDS cyber security professional must be prepared to address security from the perspective of people, policy, process, and technology. Unfortunately, the people (user) component is often overlooked when designing and implementing EDS. EDS security needs to take into account that people are critical to the security of their systems. Effective communication is required to alter the culture and to empower users to take ownership of this security problem.

In order to bring about informed policy decisions, better public awareness of the issues and opportunities facing modern energy delivery systems is essential. Consumer education is needed to effectively implement grid modernization programs such as electricity demand response plans and distributed energy integration solutions. Pre-college outreach can encourage interest in EDS careers and enhance communication with the public.

Addressing the following questions will strengthen effective workforce development:

- How can we interest young people in energy security as a career?
- What are the requirements and qualifications needed to be an effective EDS security professional?
- How can we define content for courses, training, and certifications?
- What can educational institutions do to prepare and produce future EDS cyber security professionals?
- How can we fill the generation gap for cyber security experts in the energy sector? Should retiring experts train the young?
- How can we work toward simplifying the standards to convey key ideas to users?
- How can EDS stakeholders engage the public to achieve environmentally responsible, secure, and efficient energy systems?

The group determined, after much discussion, that we could not answer these questions in the workshop time allotted. To continue the discussion a mailing list was implemented and both CREDC and industry were invited to join.

Funding Acknowledgement and Disclaimer

Acknowledgement
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780.