WIRAB Webinar Series: Cybersecurity of Utility Industrial Control Systems

December 1, 8, & 15, 2017

Presented by Roger Hill, Veracity Industrial Networks, and Earl Shockley, InPOWERd LLC
in collaboration with the Western Interconnection Regional Advisory Body

This series educated policymakers on the cyber threats faced by electric utilities and their control systems, discussed resiliency in the power grid and control systems to mitigate these threats, and facilitated a discussion about the pros and cons of enacting state policies designed to enable better cybersecurity practices.

Take-away Messages:

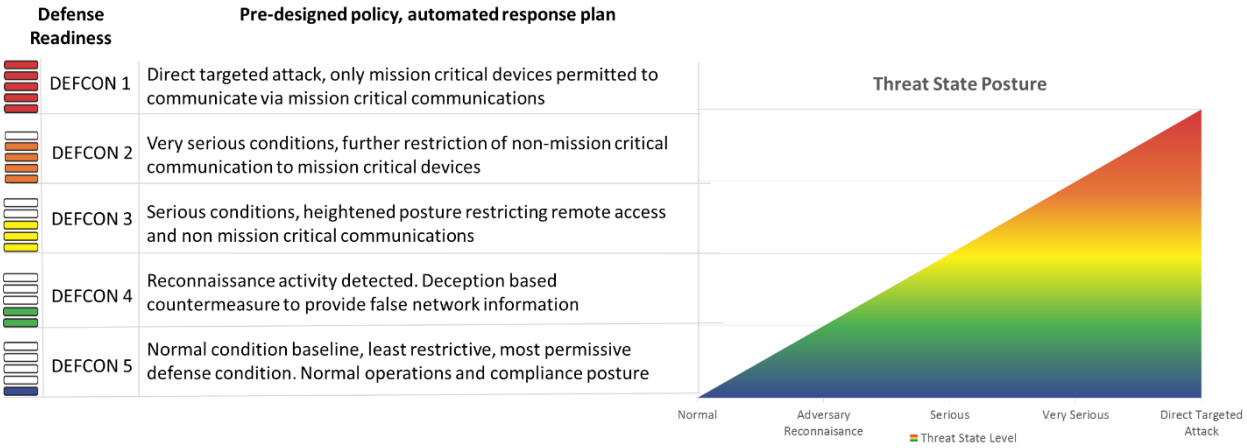
- **Industrial Control Systems (ICS)** are used to automate physical processes to increase productivity and efficiency, decrease downtime, insure quality, and improve safety and reliability. For utilities, ICS are the systems used to control actions (either automated or manual) on the electric grid such as switching equipment in and out of service, changing output of a generator, etc. Cybersecurity of ICS focus on safety and the protection of things (equipment, people, etc.) more than the protection of data or information.

- **Threats to utility ICS** can be bad actors like a nation state hacker or terrorist group, but most commonly the primary threat to ICS are the threat of an insider, which is typically non-malicious (misconfiguration and/or misuse) but can be malicious (revenge).
    - **Challenges with securing ICS** include the lack of visibility into devices on the networks, the legacy infrastructure that are on 10-20 year life cycles, lack of subject matter experts, and overall convergence of the cyber and physical realms. These challenges can lead to unintended vulnerabilities.

- **Compliance does not necessarily equal security.** Compliance is snapshot of how a security program meets a specific set of security requirements at a given moment in time. Compliance corresponds to a set of specific requirements that change slowly, not the daily dynamic changes within the security landscape. Compliance is necessary, but it only establishes a minimum baseline level of competence and protection. Compliance should never be the blueprint and it does not necessarily lead to good security, but a good security almost always leads to good compliance.
    - **Regulators and decision makers can help utilities go above and beyond the minimum requirements** by inquiring about a utility's tools and practices it uses to go beyond standard compliance. **Look for best practices** such as conducting table top exercises to test security, automating manual processes to minimize potential human error, practicing sound change management, etc. These types of activities are not likely spelled out in standard requirements, but can demonstrate that a utility manager is serious about maintaining a secure system.
    - **Leverage experts from security institutions**, such as National Guard or Department of Homeland Security, to test and work with utilities on security practices and then share lessons learned.

- **Resiliency** is defined as the ability to reduce the magnitude and/or duration of a disruption by anticipating, absorbing, adapting and/or rapidly recovering from a potential disruptive event. Resilient systems do not have to be complex systems, but they must be well designed.
    - **Complexity is the enemy of security.** Complex systems allow for multiple opportunities where the system can be infiltrated and protection systems can be circumvented without even the system owner knowing it has been compromised. Complex systems can be difficult for owners to manage, relying on subject matter experts that may not always been available. The simpler a security program, the more effective that program may be, especially in the long run.
    - **The industry is moving towards a Threat State Model approach** to provide centralized planning to allow for 100% visibility of all devices and communications. This creates a foundation for high-quality situational awareness. Threat States are mapped to defense reediness conditions (e.g. DEFCON 1-5) that represent a distinct pre-designed and pre-tested security policy.

Threat State Model



- **Technology innovation and commercialization** is first driven by original research conducted by well-funded research institutions such as in academia, the national labs, etc. but this original research does not necessarily lead to the adoption or commercialization of new technology. Companies and entrepreneurs need the incentive or to see benefit to their bottom line to bring new technology to market.
    - **State and provincial policies can drive the adoption of innovative and new technology** through rules and regulations that are not too prescriptive but rather performance based. **State and provinces can then incentivize better performance** by inspiring problem solving at all levels, from technology innovation and research at the research institutions down to commercialization at businesses.

More information, including recording and slides, from the webinar series can be found HERE.

Eric Baran Western Interstate Energy Board ebaran@westernenergyboard.org	Roger Hill Veracity Industrial Networks roger@veracity.io	Earl Shockley InPOWERd LLC earl.shockley@inpowerd.com