Implementation of Resilience via Operational Controls

Website: http://cred-c.org/researchactivity/opcontrols

Researchers (UH): Wm. Arthur Conklin

Industry Collaboration:

- Chevron
- We are actively seeking additional industry partners. Contact Wm. Arthur Conklin for more details.

Description of research activity: Resiliency is an emergent property of a system. To achieve resiliency in a system requires specific elements in system design and operation. This activity looks at how operational controls that are used to achieve specific objectives such as security can be adapted and patterned by use into controls that also enable greater resiliency. Much like the top 20 security controls list, the objective is to determine and highlight how operational controls can enhance system resiliency.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This activity relates directly to objectives identified in the roadmap. Because resiliency is a foundational element behind many cybersecurity practices and is needed to achieve desired objectives, it is a foundational element involved in many aspects of the roadmap. Developing a better understanding of what constitutes actionable operational elements and how they relate to the development of system resiliency is a key step in achieving these desired objectives. Specifically, resiliency is involved in the following roadmap elements:

Strategy 1. Build a Culture of Security

1.4 Field-proven best practices for energy delivery systems security widely employed

1.5 Compelling business case developed for investment in energy delivery systems security

Strategy 2. Assess and Monitor Risk (all aspects)

Strategy 3. Develop and Implement New Protective Measures to Reduce Risk

3.1 Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available

3.5 Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions

Summary of EDS gap analysis: Cybersecurity is achieved through the employment of security controls. Operational resiliency will be achieved through operational measures. Developing the correct set of operational controls that facilitate both security and resiliency will enable energy companies to improve resiliency through normal operational elements.

Full EDS gap analysis: Cybersecurity is defined as the protection of a system and its information, restricting access to a defined set of users. This is useful in IT systems, but in energy delivery systems, a broader goal of protecting the functioning of the system within both desired operational and safety limits requires a broader definition of the protection scheme. [1] This is where resilience enters the picture. Resilience has been identified as a key element in maintaining security of our critical infrastructures. [2, 3] This project is an attempt to examine a set of operational controls that are commonly employed in IT systems, to determine how they can contribute to OT resiliency. The Oil and Gas industry is entering a period of cybersecurity maturation that will support the adoption of information on resilience, making this an ideal time to develop this information, providing the industry information necessary for its next phase of cybersecurity implementation in OT. [4]

Bibliography:

1. Roadmap to Achieve Energy Delivery Systems Cybersecurity, DOE, September 2011.
2. Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, White House, February 2013
3. Cybersecurity National Action Plan, White House, February 2016
4. The State of Cybersecurity in the Oil & Gas Industry: United States, Ponemon Institute, February 2017