Implementation of Resilience via Operational Controls

Wm. Arthur Conklin, Gregory Anderson

GOALS

- Determine factors which enable system resiliency.
- Enumerate security controls with resiliency effects.
- Develop a documented list of security controls with respect to cyber resiliency.
- Validate the list of security controls promoting resiliency with industry partner.

FUNDAMENTAL QUESTIONS/CHALLENGES

- Resiliency is easy to define: an emergent property of a system that enables it to remain operational within some range of acceptable conditions even when outside forces or failures result in deviation from desired controlled state. Systems that are resilient also have the ability to re-enter a properly controlled state.
- Resiliency is a result of system properties: hence the emergent property aspect.
- The challenge is in determining what generic elements can lead to resiliency.
- Secondary challenge is in industry acceptance of security controls being positive elements in a system.
- We understand the elements for risk: avoidance, transference, mitigation, and acceptance. We need analogs for resiliency.
- For security, we manage with controls. Controls will also be used for resilience, but the challenge is in which controls. In security, we choose controls based on risk and threat environment.
- Examining controls based on risk and threat elements that are targeting the control aspect of the system.
- Fundamental objective: determine which controls result in greater resiliency.

RESEARCH PLAN

- Determine system definition of resilience. ✓
- Explore elements of common security controls with respect to resiliency effects.
- Document effects of controls that appear to have an effect on resiliency and tie into context of resiliency design elements.
- Produce a list of resiliency controls and effects.
- Find an industry partner.
- Validate resiliency controls list with industry partners.

RESEARCH RESULTS

- Project is on-going.
- Resiliency has been defined in operational terms (previous project).
- Examining resiliency affect across a wide range of security controls.
- Examined current and historical Common Security Controls for suitability – have the initial cut and are working the details for each control.
- A key result is that although many of the top 20 Security Controls will work in an OT environment, their efficacy both in terms of improving security and resiliency are highly questionable. This makes the proper selection of the correct subset of these controls a key architectural element in the design of these systems.
- The security control of network security has been dropped from the IT set, but it is the most important control in the OT space, highlighting one of the stark differences between IT and OT with respect to controls.

BROADER IMPACT

- Security controls are a tried and true element in IT security programs and with the convergence of IT and OT security an understanding of the influence of various security controls on OT resilience is important.
- Resiliency is essential in OT systems, it forms the basis for predictable, reliable operations.
- The “security objective” of an OT system is the continued operation of the system within desired parameters and in a safe fashion. Resiliency plays a large role in ensuring this outcome, so the challenge is how to build controls to assist the resiliency element.

INTERACTION WITH OTHER PROJECTS

- This project includes the merging of the project: Lightweight Cyber Security Resiliency Framework into this project.
  - What came from the framework – operational definition of resiliency in OT systems

FUTURE EFFORTS

- Complete the element by element examination.
- Develop a foundational set of controls, with resiliency expectations and explanations.
- Test with an industry partner.

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY