Implementation of Resilience via Operational Controls

Art Conklin, University of Houston

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security | cred-c.org

Security in IT vs. OT

- IT security
  - CIA associated with authorized user and data flow

- OT security
  - Continued safe operation of the system regardless of changes in the environment

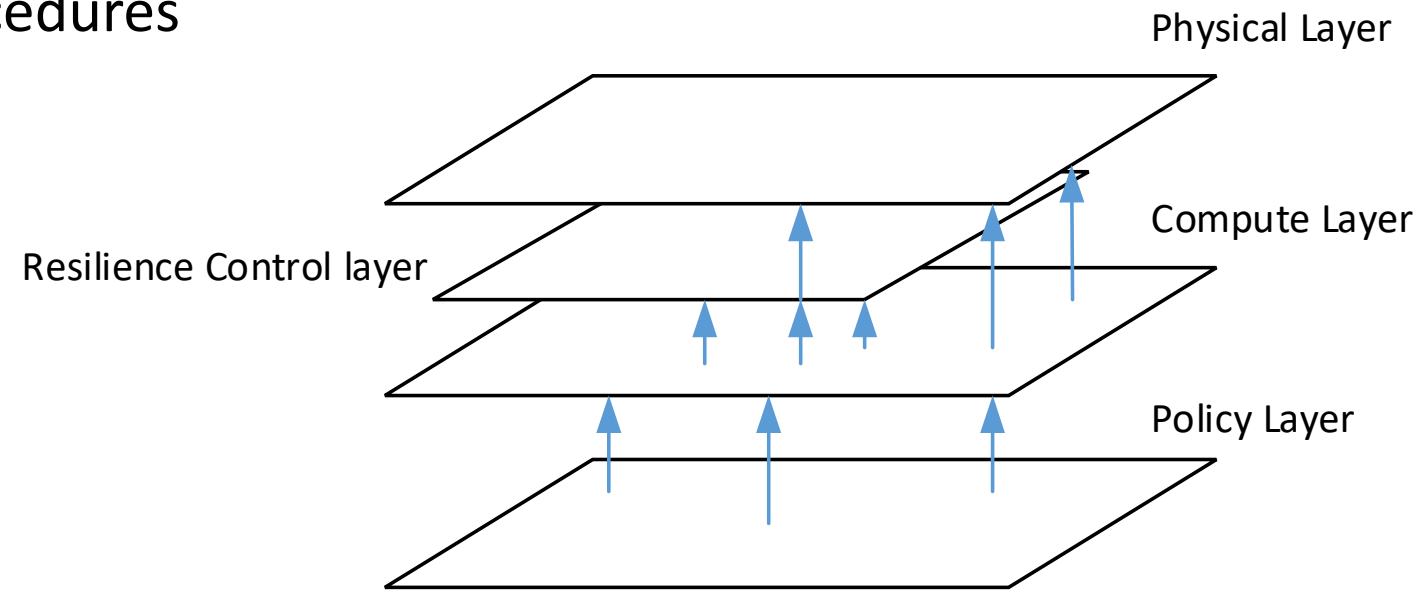
What is resilience

- Cyber Resiliency
  - “The emergent property of a system that can continue to carry out its mission after disruption that does not exceed its operational limit”
  - “The ability of a system to anticipate, withstand, recover from, and/or evolve to improve capabilities in the face of, adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function.”

- Anticipate
- Withstand
- Recover
- Evolve

Tools

- Policy Layer
  - BC/DRP/COOP
  - Resiliency Policies and Procedures
- Compute Layer
  - Redundancy
  - Security
  - Layers (Purdue Model)
- Resilience Control Layer
  - Safety
  - Interlocks



System Emergent Property

- Must be engineered in to emerge
  - FMEA - how does system operate under failure situations
  - Threat Modeling - where does the disruption come from
  - Safety Systems - Purdue model and isolationism

- Determining what is proper is non-trivial - Process specific
  - What are resilient modes?
  - What are resilient operations?

Implementation of Resilience via Operational Controls

- Resiliency is an emergent property of a system.
  - Emergent properties are not defined by single system elements
  - Emerge as a result of system interactions
- To achieve resiliency in a system requires specific elements in system design and operation.
- Determine how operational controls affect system resiliency.
  - Operational controls are used to control security – another emergent property.
  - Controls are used all the time.
  - Which controls can improve resiliency.

Implementation of Resilience via Operational Controls

- 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 target greater resiliency.
  - Create a top 20 resiliency controls list, the objective is to determine and highlight how operational controls can enhance system resiliency.
  - Production of an operational controls checklist and associated documentation for implementation.

- Top 20 Controls – key concept – built from analyzing offense

Top 20 Controls (security in OT)

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Software
3. Secure Configurations for All
4. Secure Network Engineering
5. Limitation and Control of Network Ports, Protocols, and Services
6. Boundary Defense
7. Secure Configurations for Network Devices
8. Maintenance, Monitoring, and Analysis of Security Audit Logs
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Incident Response Capability
11. Malware Defenses
12. Data Recovery Capability
13. Controlled Use of Administrative Privileges
14. Penetration Tests and Red Team Exercises
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Loss Prevention
18. Continuous Vulnerability Assessment and Remediation
19. Application Software Security
20. Wireless Device Control

How to get to resiliency

- Anticipate
- Withstand
- Recover
- Evolve

- Apply to controls

- What is offense in OT

- Loss of View
- Loss of Control

- Denial of View
- Denial of Control
- Denial of Safety

- Manipulation of View
- Manipulation of Control
- Manipulation of Safety

Top 20 Controls (resiliency in OT)

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Software
3. Secure Configurations for All
4. Secure Network Engineering
5. Limitation and Control of Network Ports, Protocols, and Services
6. Boundary Defense
7. Secure Configurations for Network Devices
8. Maintenance, Monitoring, and Analysis of Security Audit Logs
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Incident Response Capability
11. Malware Defenses
12. Data Recovery Capability
13. Controlled Use of Administrative Privileges
14. Penetration Tests and Red Team Exercises
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Loss Prevention
18. Continuous Vulnerability Assessment and Remediation
19. Application Software Security
20. Wireless Device Control

- Anticipate
- Withstand
- Recover
- Evolve

CREDC

Why we aren't there

- Security controls "defend" the information side of the process including control functions
- The process has its own modes and paths
  - Ever increasing temperature ← when to recognize, when to control
  - Steady state vs. stuck
- Resilience requires more than normal control
  - Anticipate
    - Where are we now
    - Where are we going
    - When will we move to extremis

Most action today is withstand in nature

- Prevent the hit from hurting us

- Now looking at the “ICS Attack Phenomenon”
  - Malware got on your system (problem #1)
  - You lose Visibility and Control (problem #2)
  - Your system no longer really yours (problem #3)

- We get #1 – withstand
- We need to work on #2 and #3 – this is where we are thinking and working

Next Steps

- Look at attack: change of process control logic
  - How will controls see the change
  - How will we recognize the change
  - Today's controls will see attacks (some) and deviations (some)
  - Today's controls cannot see process change

- How can NSM give us insight?

Questions?

Art Conklin

waconklin@uh.edu