# 

# Implementation of Resilience into Operational Controls Wm. Arthur Conklin, PhD

#### RESILIENCE IS THINGS WORKING CORRECTLY

#### CYBERSECURITY CONTROLS

**Operational Data and Controls** 

Environmental Influences

> Process Stability



Physical Security

Process Control Influences

Cybersecurity Controls

IT Threat is aimed at Data Objective is to Protect Data



Security is managed using controls.



ΟΤ

Threat is aimed at loss, denial, or manipulation of control, or safety.

> Objective is control of operations, safety, and uptime

Reuse Cybersecurity Controls to Influence Resiliency

#### **PROJECT ROADMAP**

**RESEARCH VISION** 



### **Resilient Controls**

Using existing Security Controls, refine the list into a set of controls that promote resilience

SANS Top 20 Security Controls NIST 800-53 Security Controls NIST 800-82 Security Controls

Cybersecurity controls operate through Confidentiality, Integrity, and Availability (CIA) of the data.

Key Cybersecurity Controls for Resiliency:

- 1. Boundary Defense/Secure Network Engineering
- 2. Limitation and Control of Network Ports, Protocols, and Services.
- 3. Inventory of Authorized and Unauthorized Devices
- 4. Inventory of Authorized and Unauthorized Software
- 5. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- 6. Controlled Use of Administrative Privileges
- 7. Maintenance, Monitoring, and Analysis of Security Audit Logs
- 8. Security Skills Assessment and Appropriate Training to Fill Gaps
- 9. Incident Response Capability/NSM

10.Security Auditing

#### FOCUS ON RESILIENCY

#### For IT, Measure via CIA

#### RESILIENCY

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

OT security objective: Keep the system operating within nominal parameters in a safe manner.

Actively seeking industry partners to examine how to measure resiliency and control effectiveness.

#### CONTACT US

Art Conklin: waconklin@uh.edu

Research Project:

https://cred-c.org/researchactivity/implementation-resilienceoperational-controls

# CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

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

#### For OT, Measure how?

#### HOW DO YOU MEASURE RESILIENCE?