WEST YOST
Water. Engineered.

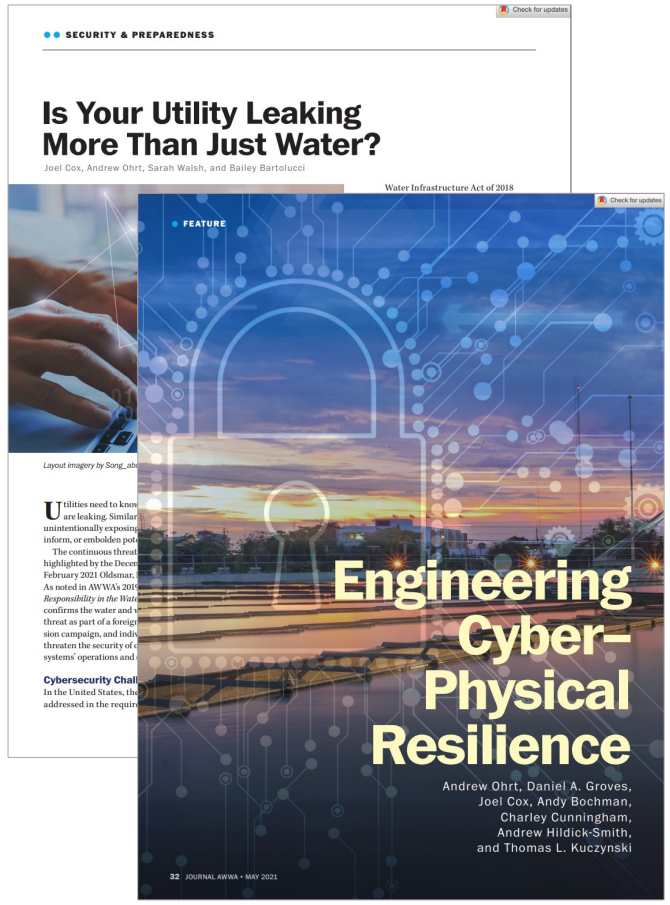
Cybersecurity and Water Infrastructure

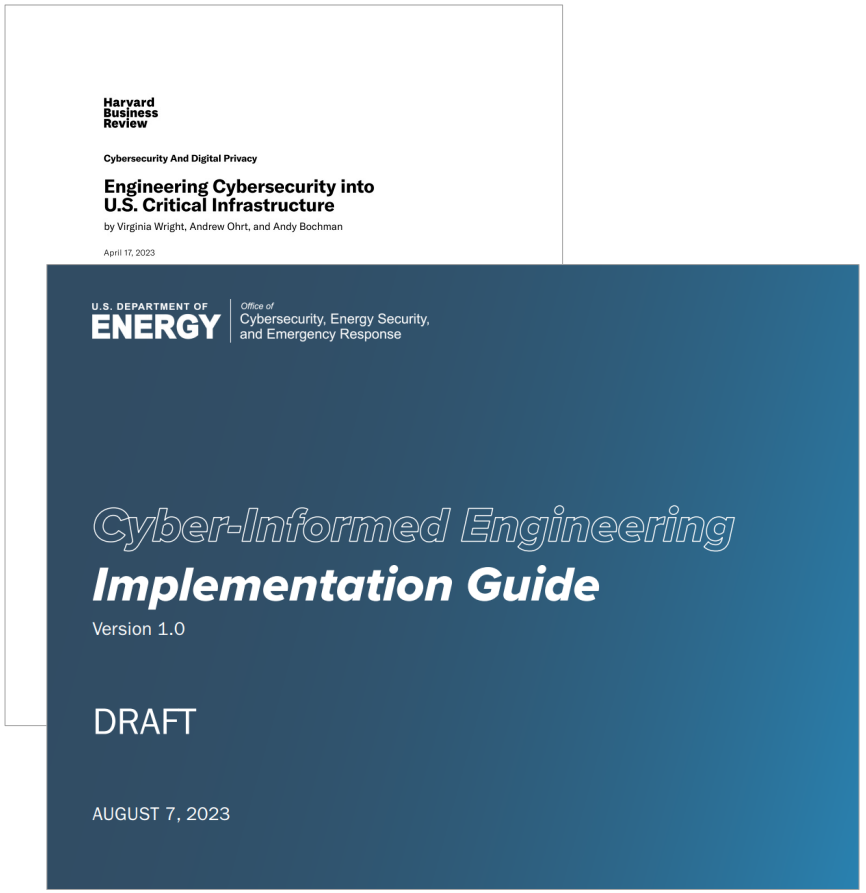
Joel Cox, GICSP, CCNA, GPEN
Andrew Ohrt, PE, CISSP
Tara Mertz

Agenda

- Threat Briefing
- Regulatory Update
- Cyber-Informed Engineering (CIE)
- Getting Started
- Questions & Answers

West Yost's Water Sector Cybersecurity Contributions





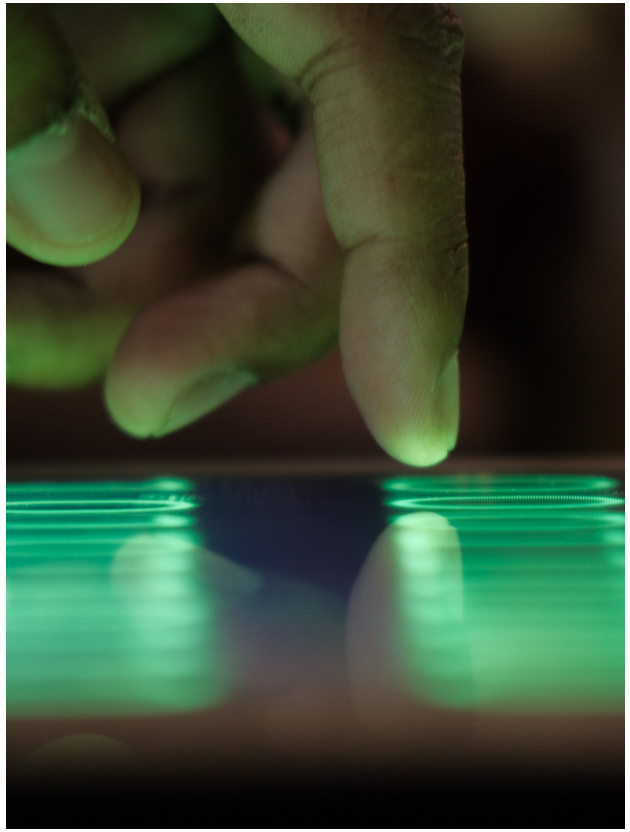
Threat Briefing

Joel Cox

Why are we here?

Recent Insider Threat Reports

- **March 2019:** A former employee at a Kansas-based WWS facility unsuccessfully attempted to threaten drinking water safety with unrevoked user credentials to remotely access a facility computer post-resignation.
- **June 2023:** FBI charged former contract employee at a WTP in Discovery Bay, CA, for an intentional computer attack. The individual uninstalled the main operational and monitoring system and then turned off the servers running those systems.



Recent Advisories

CYBERSECURITY ADVISORY

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Release Date: May 24, 2023 **Alert Code:** AA23-144a

Mitigation measures for network administrators:

- Establishing activity baselines (particularly for remote access and administrative actions) and identifying baseline outliers.
- Scanning the network for known IOCs and unusual activity.
- Blocking listed IP addresses and user-agents from the EPA alert.

OT Cyberattack Strategies Continue to Evolve

Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology

KEN PROSKA, JOHN WOLFRAM, JARED WILSON, DAN BLACK, KEITH LUNDEN, DANIEL KAPELLMANN ZAFRA, NATHAN BRUBAKER, TYLER MCLELLAN, CHRIS SISTRUNK

NOV 09, 2023 | 18 MIN READ

https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

Regulatory Update

Andrew Ohrt

How are our regulatory drivers changing?

Cybersecurity Regulatory Updates

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

Voluntary until final ruling—will become regulation

- https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

"The Cyber-Rule" – EPA Cybersecurity for the Water Sector

Requirement to evaluate cybersecurity during PWS sanitary surveys

- https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SS%20Guidance_508c.pdf

Cybersecurity Regulatory Updates

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

Voluntary until final ruling—will become regulation

- https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

"The Cyber-Rule" – EPA Cybersecurity for the Water Sector

Requirement to evaluate cybersecurity during PWS sanitary surveys

- https://www.epa.gov/system/files/documents/2023-03/230228_Cyber%20SSE%20Guidance_508c.pdf

CIRCIA Updates

Model Definition of a Reportable Cyber Incident[50]

A reportable cyber incident is a cyber incident that leads to, or, if still under the covered entity's investigation, could reasonably lead to any of the following:

(1) a substantial loss of confidentiality, integrity, or availability of a covered information system, network, or operational technology;
(2) a disruption or significant adverse impact on the covered entity's ability to engage in business operations or deliver goods, or services, including those that have a potential for significant impact on public health or safety or may cause serious injury or death;
(3) disclosure or unauthorized access directly or indirectly to non-public personal information of a significant number of individuals; or
(4) potential operational disruption to other critical infrastructure systems or assets.

Harmonization of Cyber Incident Reporting to the Federal Government

September 19, 2023

Homeland Security

Office of Strategy, Policy, and Plans

Proposed Model Legislation

Establish a Water Risk & Resilience Organization

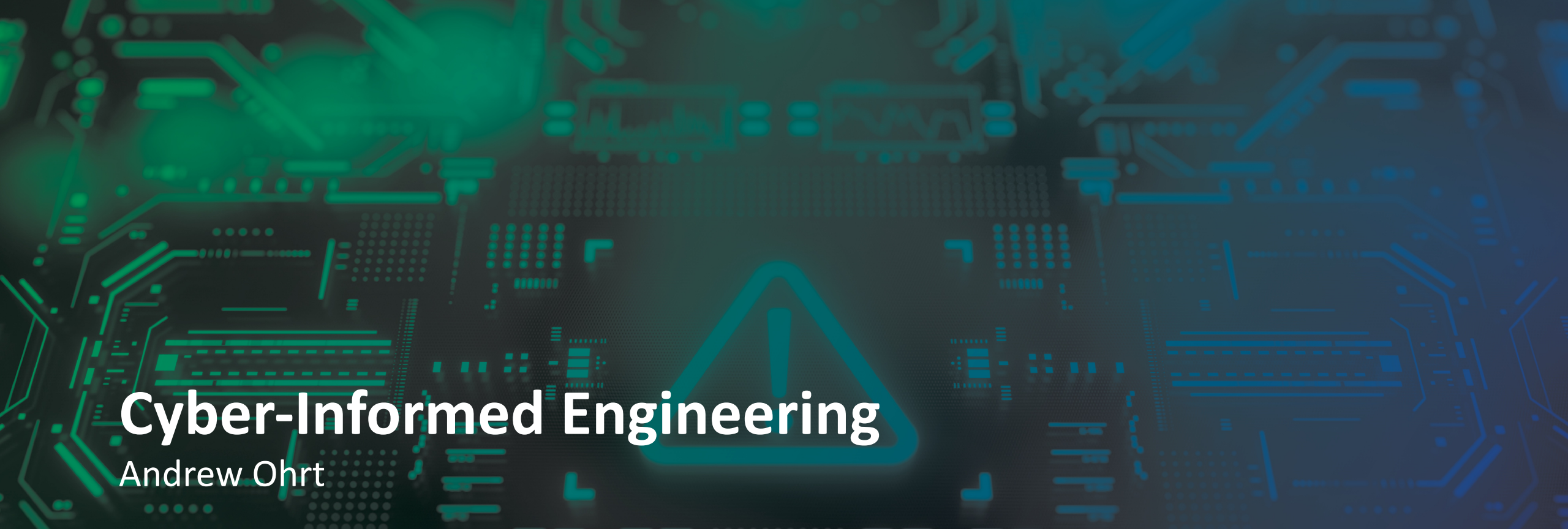
Water and Wastewater Infrastructure Cybersecurity Improvement Program

Resource and Empower the EPA

Direct More of the EPA's Funding Toward Cybersecurity

Cybersecurity Circuit Rider Program for Rural Water and Wastewater Infrastructure

Amend the Clean Water Act to Require Wastewater Systems to Perform Risk and Resilience Assessments



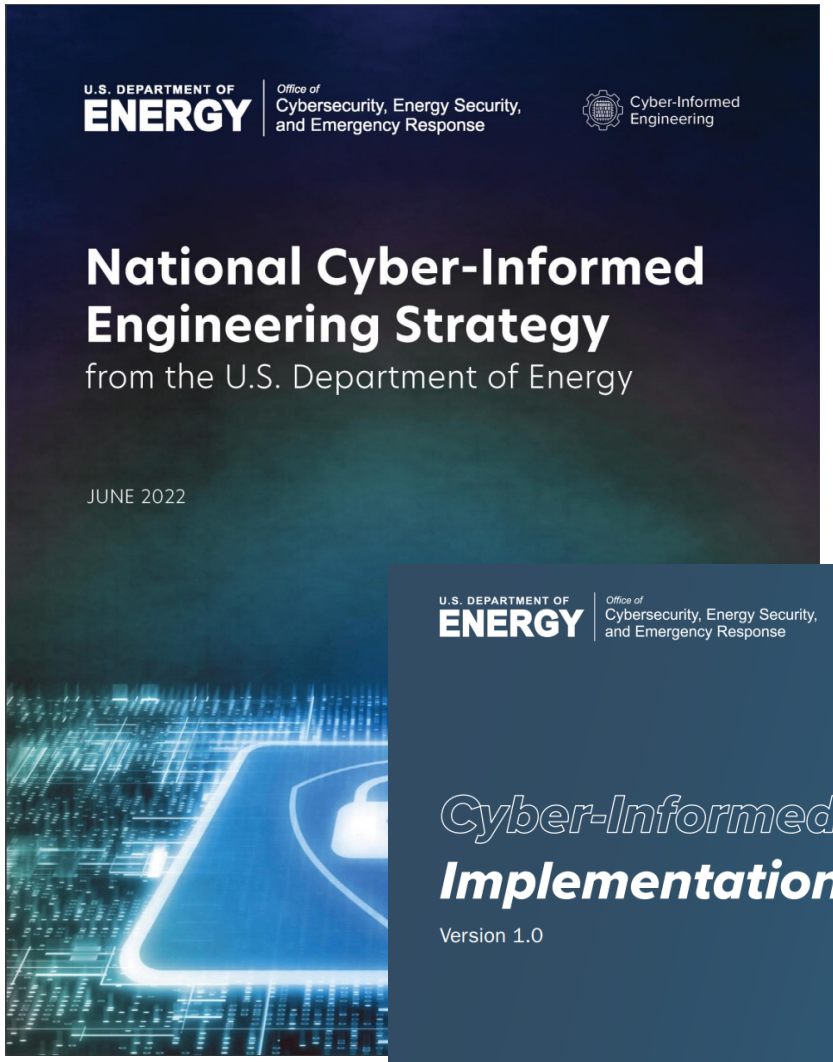
Cyber-Informed Engineering

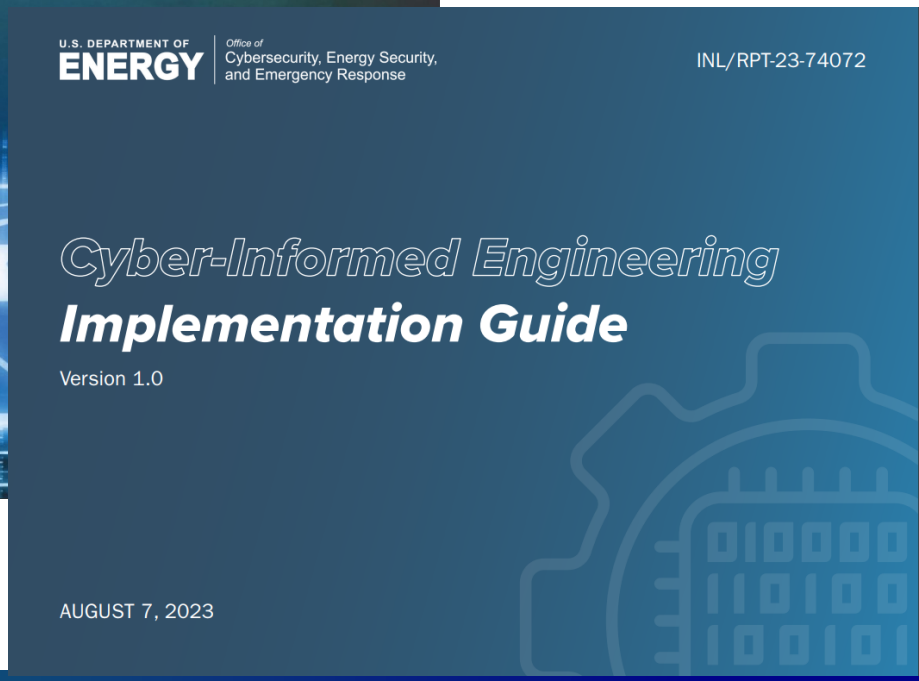
Andrew Ohrt

We have the opportunity to “build-in” *cyber-resilience* instead of “bolt-on” *cybersecurity*.

What Does CCE Look Like Fully Implemented?

> *Engineers incorporate cybersecurity practices into their body of knowledge, including engineering minimum requirements and specifications, for physical […] infrastructure systems that incorporate digital controls.*





CIE Implementation Guide

Abstract

This Implementation Guide describes the principles of Cyber-Informed Engineering (CIE) and outlines questions that engineering teams should consider during each phase of a system's lifecycle to effectively employ these principles. It describes what it means to engineer systems in a cyber-informed way, rather than offering a comprehensive, step-by-step process or procedure for CIE implementation. This guide complements—but does not replace—the application of cybersecurity standards or practices currently in place within an organization. Engineers and technicians that design critical energy infrastructure installations can use this Implementation Guide to integrate the 12 principles of CIE into each phase of the engineering lifecycle, from concept to retirement. The guide is aimed at system or design engineers, rather than software engineers or operational cybersecurity practitioners. The engineers who design, build, operate, and maintain the physical infrastructure are best positioned to leverage a system's engineering design to diminish the severity of cyber attacks or digital technology failures. CIE expands cybersecurity decisions into the engineering space, not by asking engineers to become cyber experts, but by calling on engineers to apply engineering tools and make engineering decisions that improve cybersecurity outcomes. CIE examines the engineering consequences that a sophisticated cyber attacker could achieve and drives engineering changes that may provide deterministic mitigations to limit or eliminate those consequences. « less

First Sector-Specific Guidance to Include CIE

WATER SECTOR CYBERSECURITY RISK MANAGEMENT GUIDANCE

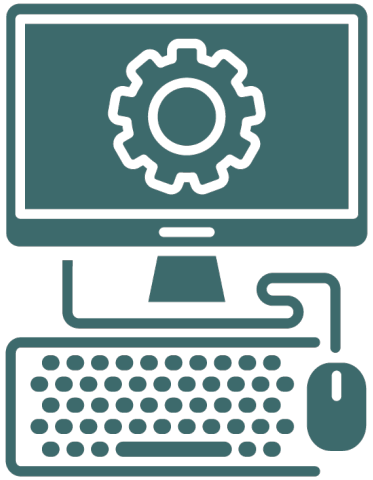
Prepared by West Yost Associates

American Water Works Association

Dedicated to the World's Most Important Resource®

Control ID	Control description	Additional Details/Examples	Priority	Control Status
CIE-1	A program is in place to engage engineering staff in understanding and mitigating high-consequence and constantly evolving cyber threat throughout the engineering life-cycle including: design, implementation, maintenance, and decommissioning.	Engineering staff is fully aware of the potential for a cyber breach. They design electrical and mechanical systems to provide functionality in the case of a SCADA system compromise.	3	Fully Implemented and Maintained

Why Cyber-Informed Engineering?



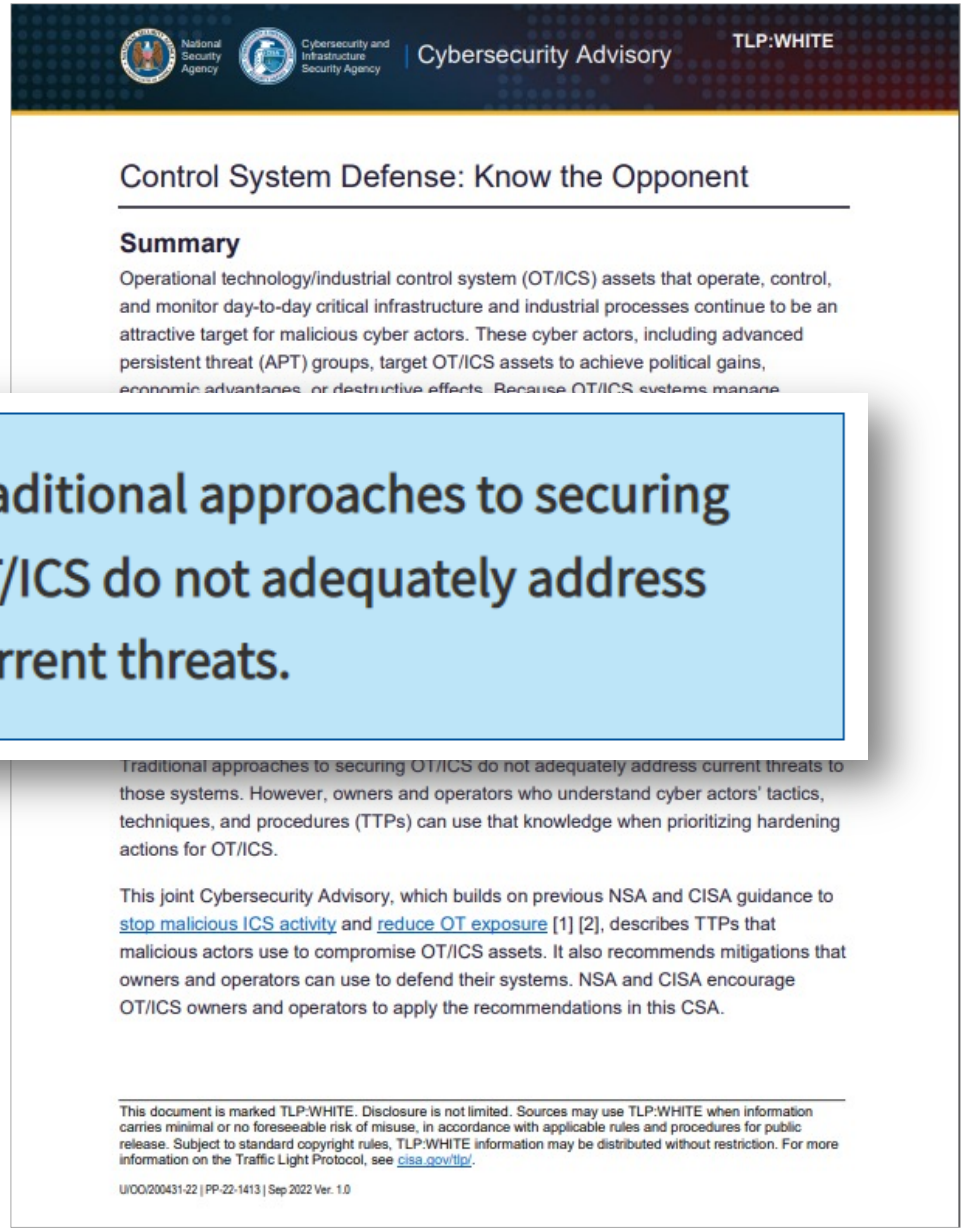
At First:
Analog Only

Current Elements:
- Digital design
- Monitor
- Connect
- Control

CISA Alert AA22-265A: Control System Defense: Know the Opponent

September 22, 2022

https://www.cisa.gov/uscert/ncas/alerts/aa22-265a



*“Not every **cyber problem** requires a **cyber solution**”*

AMY THOMAS
American Public Power Association

CIE Principles

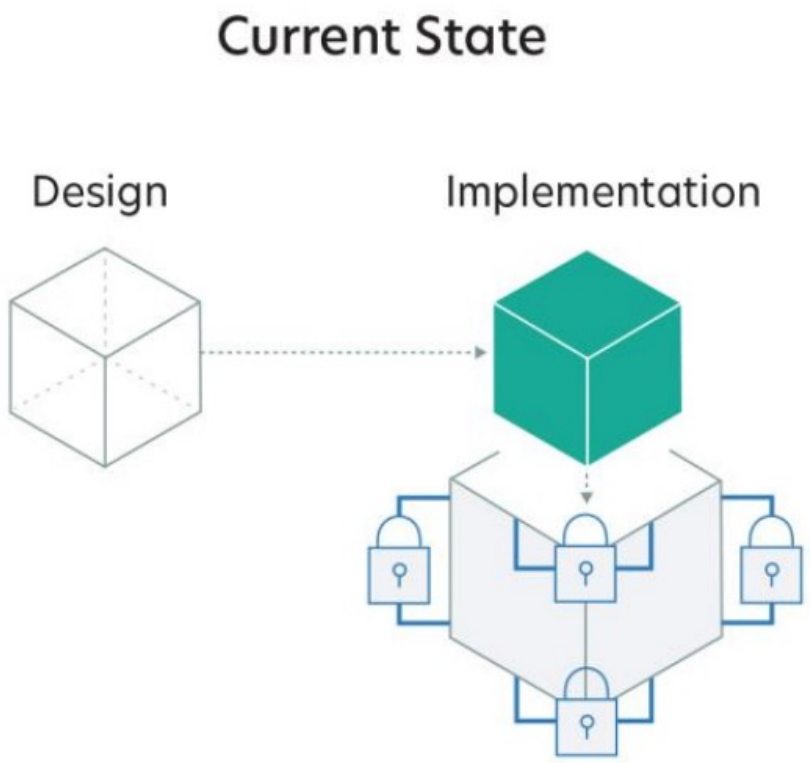
Design & Operations	Organizational
Consequence-focused Design	Interdependency Evaluation
Engineered Controls	Digital Asset Awareness
Secure Information Architecture	Cyber-secure Supply Chain Controls
Design Simplification	Planned Resilience With No Assumed Security
Resilient Layered Defenses	Engineering Information Control
Active Defense	Cybersecurity Culture

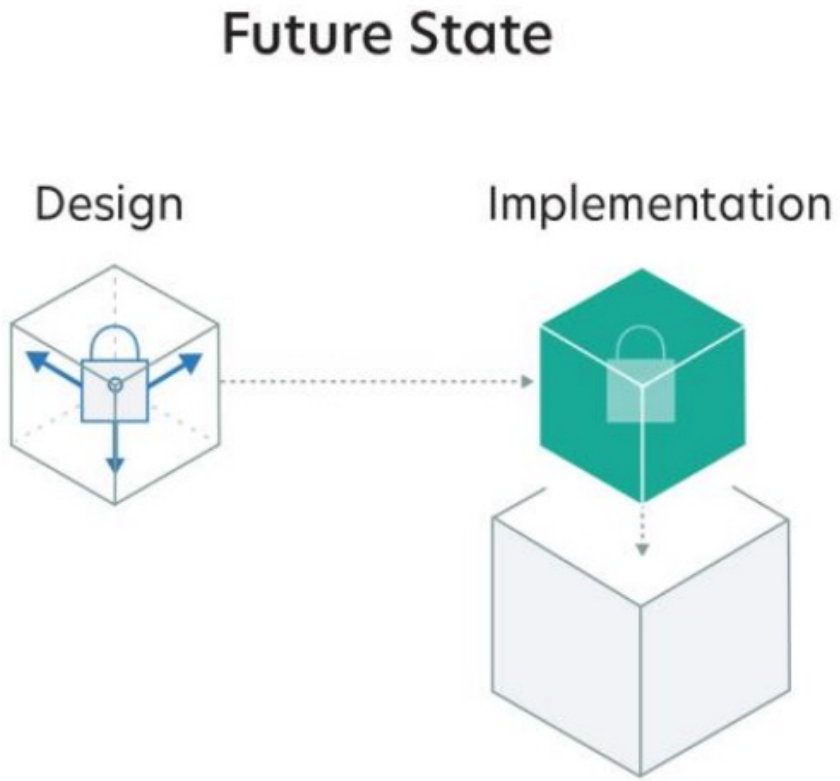
Getting Started

Tara Mertz

Don’t let perfect be the enemy of great.

Getting Started





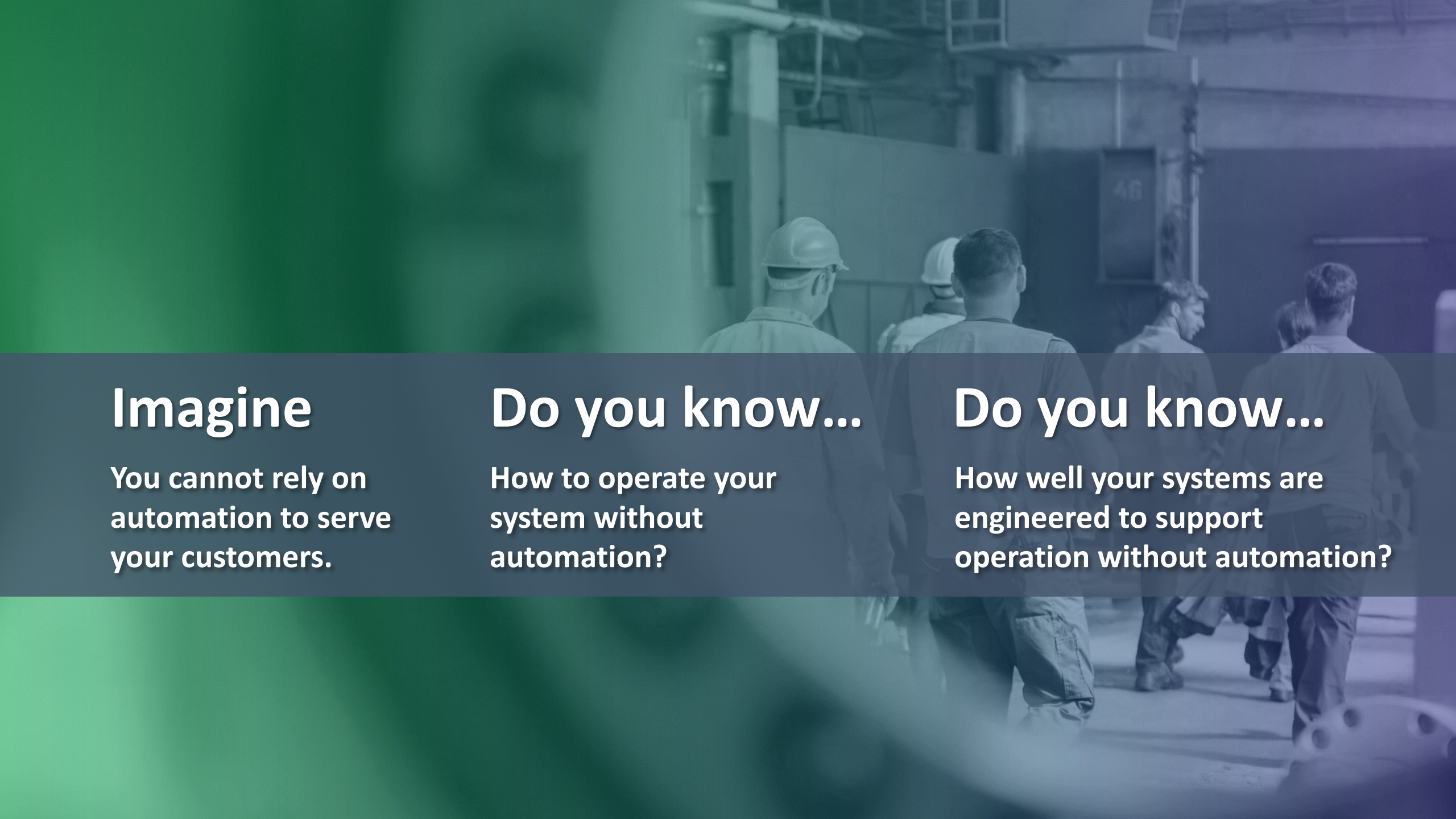
Designing to “Assume Breach”

Cyber-Physical Protections

- Water main overpressure concerns
- Pressure switch downstream of each pump, wired to pump controller

Dear Engineer,

How bad could your day be if a malicious cyber-actor gains control of your system?



Imagine

You cannot rely on automation to serve your customers.

Do you know…

How to operate your system without automation?

Do you know…

How well your systems are engineered to support operation without automation?

A Day Without SCADA®

GOAL: Drive management, operations, and engineering improvements to allow the extended delivery of critical functions in the absence of automation.

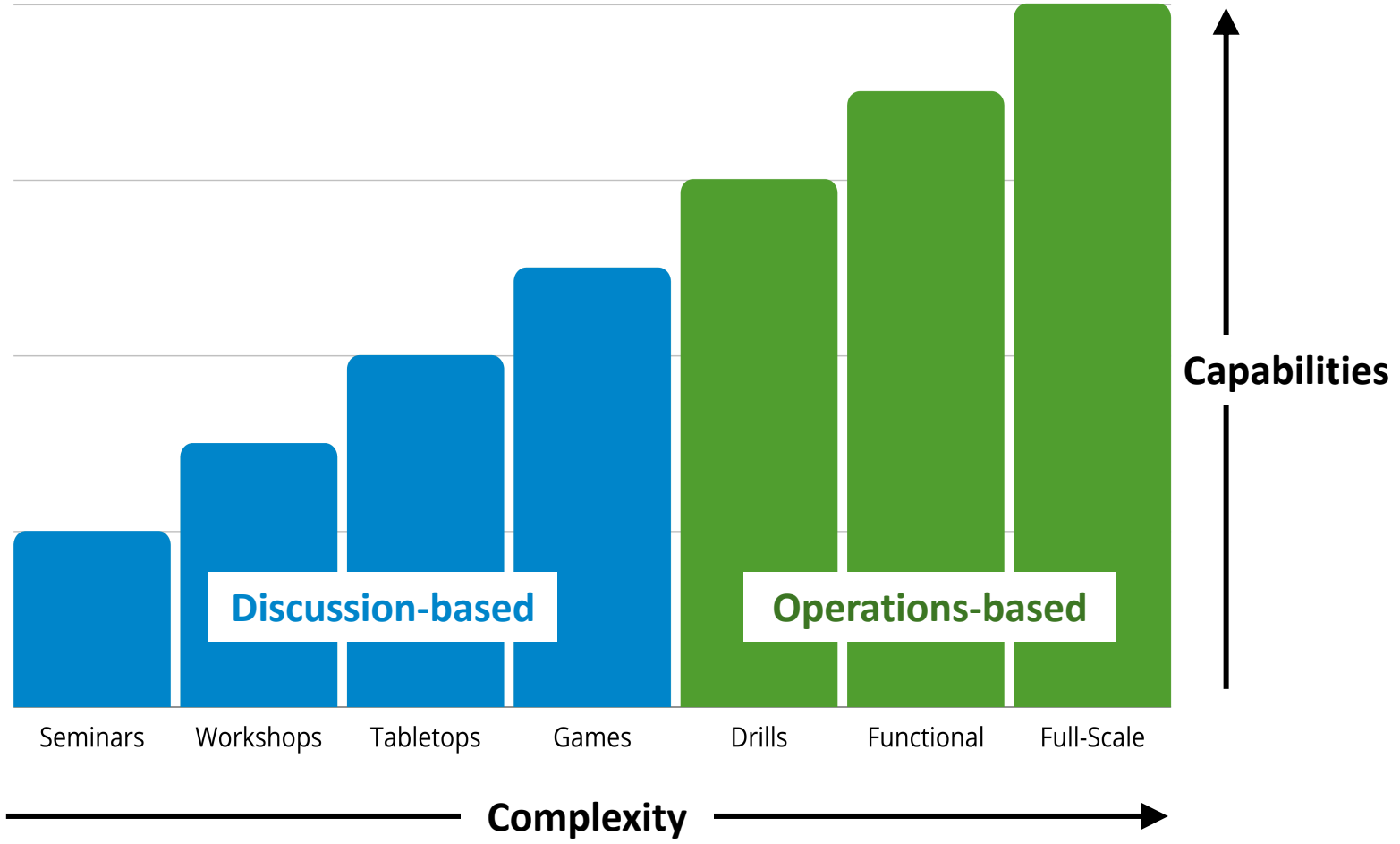
A Day Without SCADA®

APPROACH

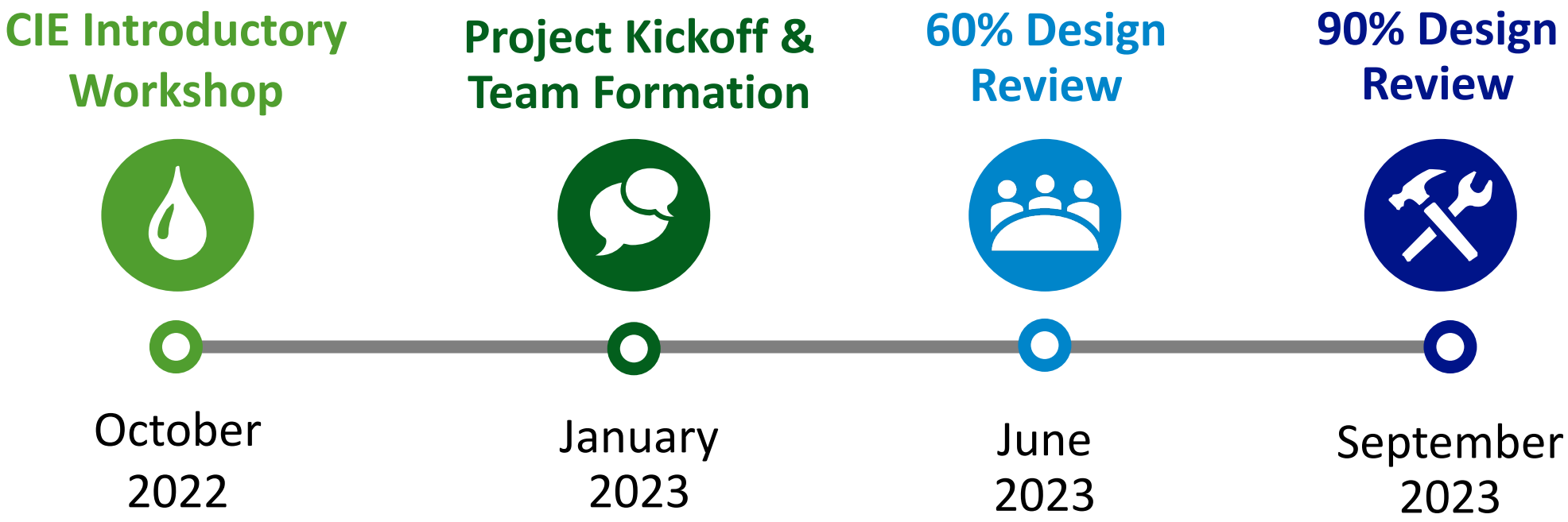
Crawl ▸ Walk ▸ Run

Capabilities Under Evaluation:

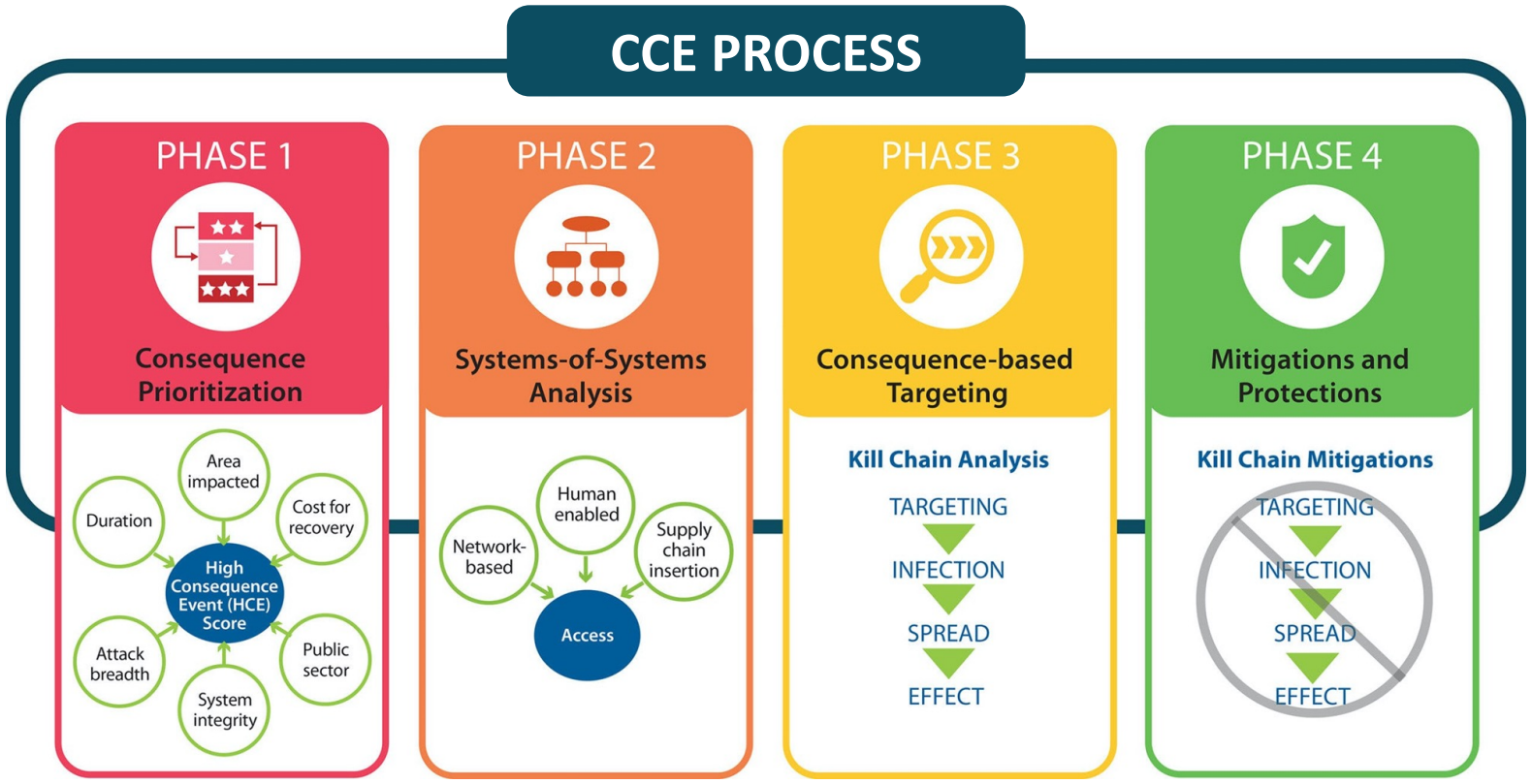
- Staff knowledge
- System engineering
- Regulatory compliance



CIE Case Study



Consequence-Driven, Cyber-Informed Engineering (CCE)



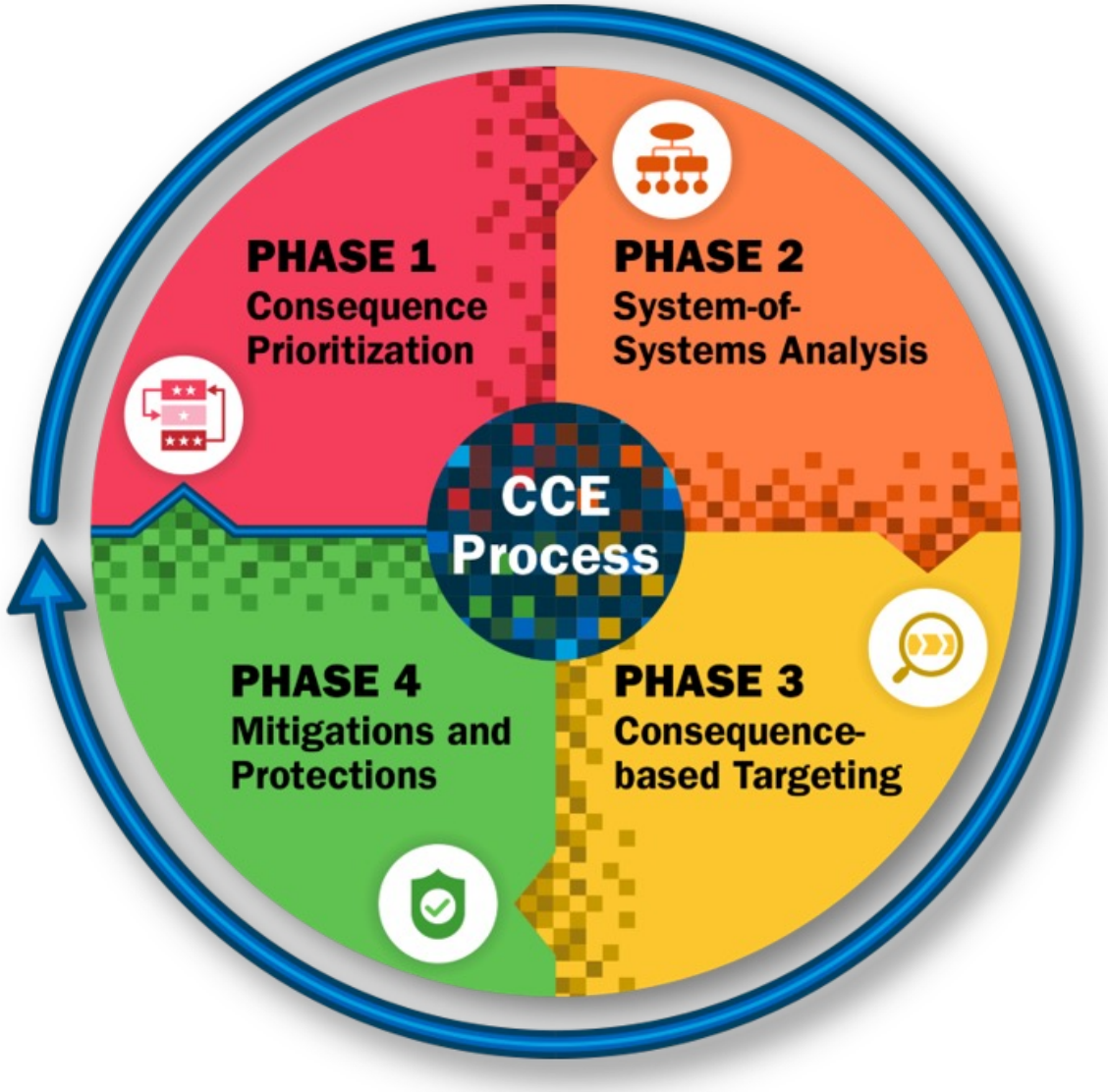
GOALS OF CCE

Protect critical functions from existing and emerging threats

Proactively prepare for next generation of cyber-enabled sabotage

90% Design Review: Lessons Learned

- Many new client staff engaged
- Drawings are key
- **Integrate CCE concepts**
  - **Unverified Trust**
  - **Commander's Intent**
  - **High-Consequence Events**
- Integrate governance
- Extensive comments are expected
- Provide more time for discussion



Applying CIE – Expected Outcomes

Improved Cyber-Resilience

- Cyber-physical
- Cyber-hygiene

Returns

- Less rework by IT/OT cyber staff
- Improved O&M

Questions

Andrew Ohrt, PE, CISSP
aohrt@westyost.com

Joel Cox, GICSP, CCNA, GPEN
jcox@westyost.com

Tara Mertz
tmertz@westyost.com

Connect with Andrew, Joel, and Tara for more information.