RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: MBS-109

Better Securing the Now and the Next: Applying Engineering First Principles to Achieve Demonstrably Better Cybersecurity

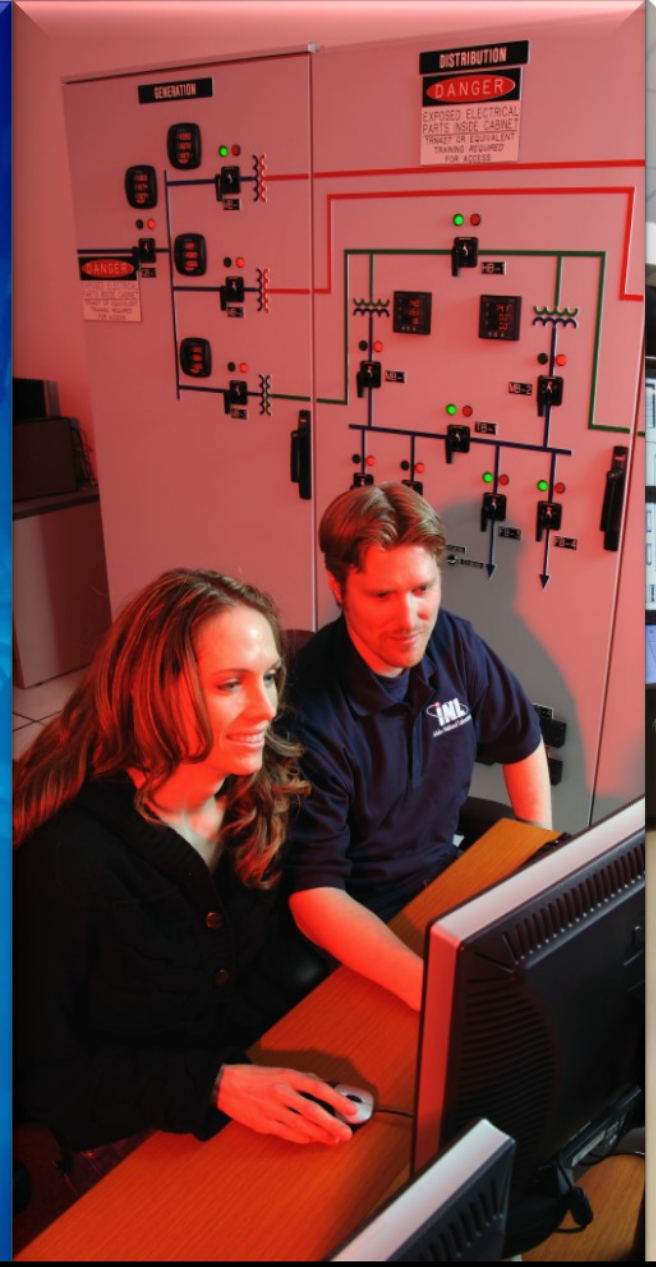
Andy Bochman

Senior Grid Strategist
Idaho National Lab
@andybochman

Virginia Wright

Energy Sector Portfolio Manager
Cybercore Integration Center
Idaho National Lab

INL is:



Nuclear Energy RD&D

Control Systems Cyber

Nuclear Energy Cyber

Grid Resilience

Evolution of Engineering

Engineering as a Bridge

Engineering is unique as a linking discipline:

- To the world of science
- To the world of technology and society
- As a source of innovation/economy

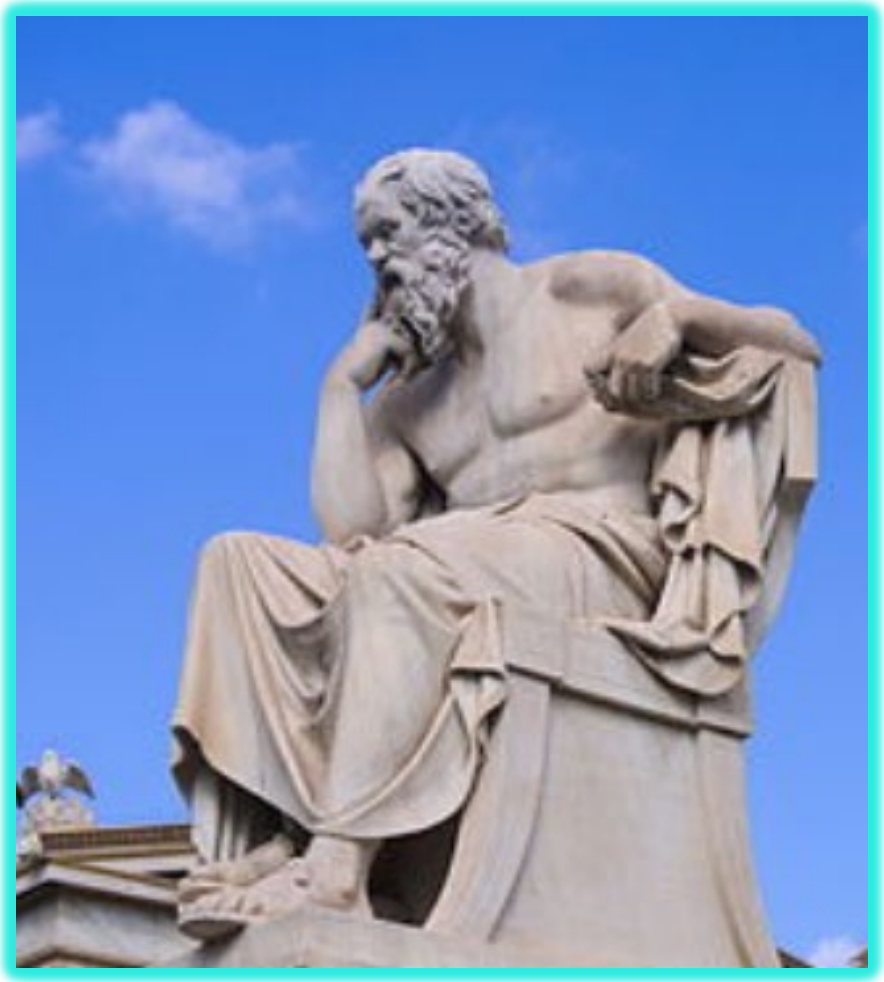
- Venkatesh “Venky” Narayanamurti, Former Harvard Dean, School of Engineering & Applied Sciences (SEAS), https://www.youtube.com/watch?v=L9DymHZH9cs

Why Cyber-Informed Engineering (CIE)?

- Because traditional engineering methods do not account for cyber risk
- And engineering curriculums do not include cyber
- And bolt-on IT security solutions do not work well for digital industrial control systems
- Sees potential to “engineer-out” many security risks

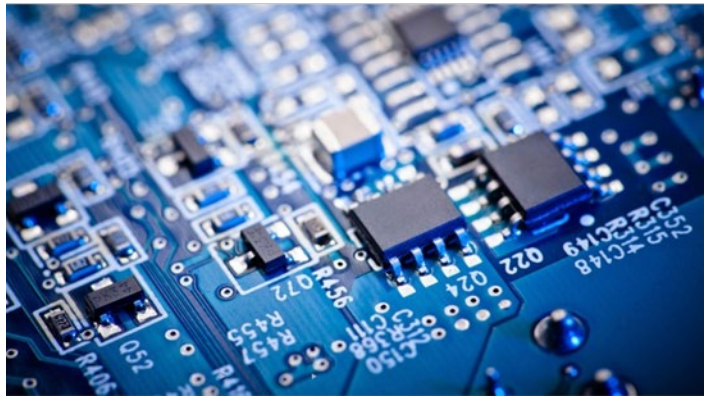
What is CIE?

- Definition: Including an awareness of cyber security challenges in the engineering process of digital and non-digital systems
- What is it?: A philosophy for characterizing the risks presented by digital technologies
- Objective: Promulgation of an updated engineering strategy, informed by an acute awareness of the cyber threats, with engineering-based methods for mitigating such risks



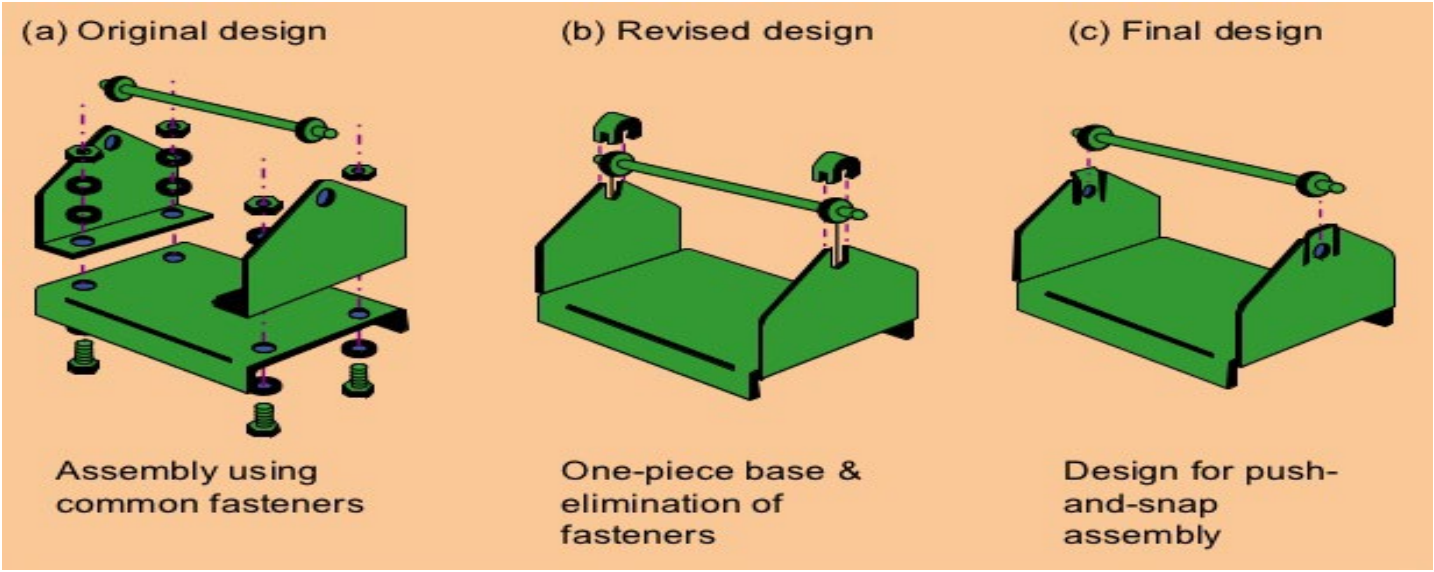
CIE: Framework Elements

- Consequence/Impact Analysis
- Systems Architecture
- Engineered Controls
- Design Simplification
- Resilience Planning
- Engineering Information Control
- Procurement and Contracting
- Interdependencies
- Cyber Security Culture
- Digital Asset Inventory
- Active Process Defense



Applied CIE Example: Design Simplification

- Reduce design to minimum necessary
- Be aware of latent functionality
- Consider non-digital technology where it fits
- Use ALARA (As Low as Reasonably Achievable) as a metaphor



How to Begin to Apply CIE Concepts

- Sooner:
  - Contact INL for a specific briefing
  - Grab the Cyber-informed Engineering technical report: https://www.osti.gov/biblio/1369373-cyber-informed-engineering
  - Begin to socialize with engineers/operators and cyber security specialists planning projects
- Later:
  - If interested, contact INL for help inculcating into ongoing projects
  - Be on the lookout for future research enriching CIE to apply to new technology development and to provide richer tools to implementers

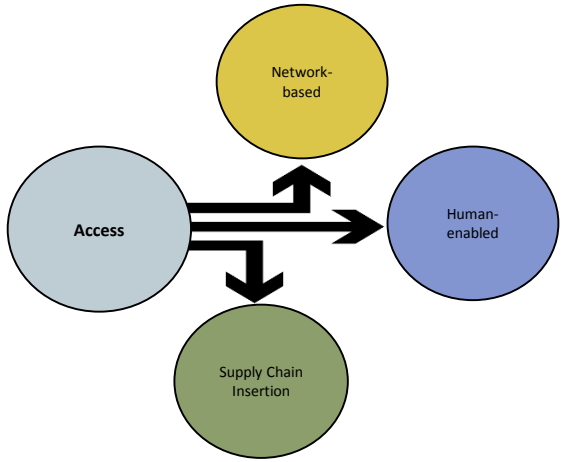
1st Harvest: Consequence-driven Cyber-informed Engineering (CCE)

- Acknowledges breaches ongoing at critical infrastructure orgs
- Admits even the best cyber hygiene doesn't stop certain adversaries
- Posits engineering solutions to block or limit the consequences of attackers' best efforts

Seeks to change how organizations understand and manage their strategic cyber risks

Introducing the CCE Methodology

Step 1	Step 2	Step 3	Step 4
Consequence Prioritization	**System of Systems Breakdown**	**Consequence-based Targeting**	**Mitigations and Protections**



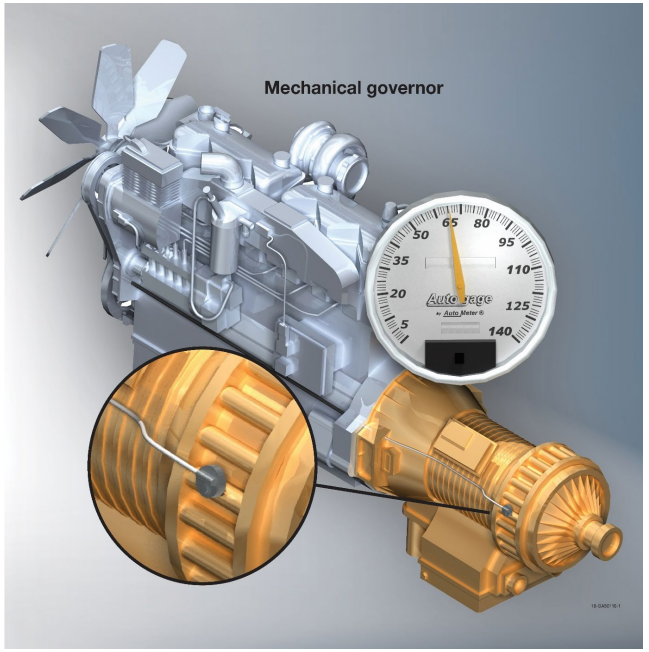
Kill Chain Analysis

Targeting → Infection → Spread → Effect

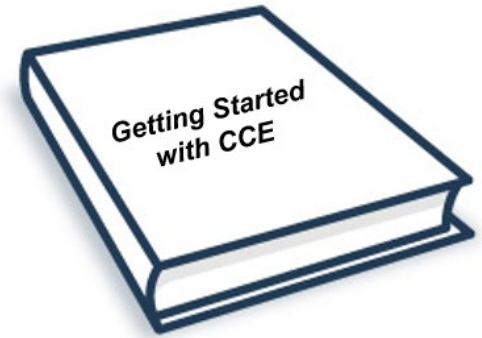
Kill Chain Mitigations

Targeting Infection Spread Effect

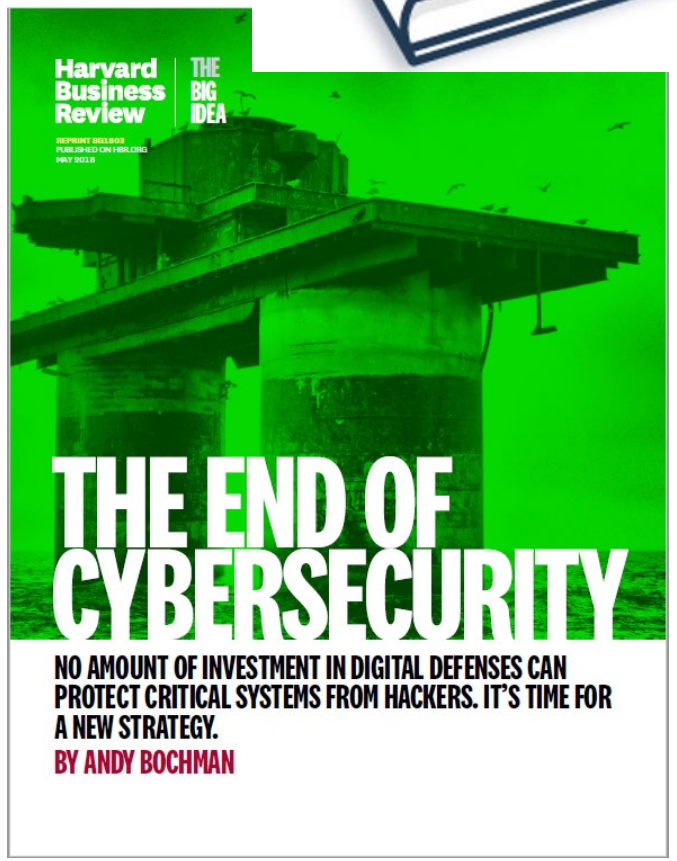
Applied CCE Examples: Analog/Out-of-band Backstops



How to Begin to Apply CCE Concepts



- Sooner:
  - Begin to socialize HBR concepts with senior leaders and engineer/operators
  - Keep an eye open for the Getting Started with CCE guide
- Later:
  - Read the Intro to CCE book for practitioners, expected publication date: 2H2020
  - If interested, contact INL for potential 2-day orientation engagement



Idaho National Laboratory

“THINK LIKE A HACKER, BUT ACT LIKE AN ENGINEER.”

Marty Edwards, Automation Federation (former Dir ICS-CERT)

Idaho National Laboratory


INL
Idaho National Laboratory