INL/CON-24-79912-Revision-0

Addressing Consequence within Operational Risk (O.T. Gagnon III) 9-18-2024

September 2024

Ollie Gagnon

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-24-79912-Revision-0

Addressing Consequence within Operational Risk (O.T. Gagnon III) 9-18-2024

Ollie Gagnon

September 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Addressing Consequence within Operational Risk
Why threats and security are just not that important

2024 Aviation Cybersecurity Conference

O.T. Gagnon III (Ollie), CISSP, CPP, PSP
Chief Homeland Security Advisor
Idaho National Laboratory

Transportation-Aviation-Airport Dependency Profile

(What is the most important airport infrastructure?)

FUNCTIONAL DEPENDENCY EXAMPLE: AIRPORTS

Internal Dependencies for Airport Operations

Airside Operations
- Passenger Ticketing
- Gate Operations
- Air Operations Center
- Ramp Operations & Cargo
- Runways
- Taxiways
- Apron Areas
- Deicing
- Aircraft Parking/Pushing

Communications
- Radio Equipment
- Cable TV
- Satellite Systems
- IT Servers

Landside Operations
- Terminal Facility
- Aircraft Hangars
- Cargo Terminals
- Maintenance Tunnels/Facilities
- Fueling Areas
- Mechanical/Equipment
- Pedestrian Access Tunnels
- Aircraft Fueling Equipment
- Deicing Equip & Facilities
- Food Services Area
- Fuel Storage Area

Landside Operations (cont.)
- Security Screening Area
- Inspection Areas
- Passenger Drop Off/Pick Up
- Rental Car Areas
- Baggage Handling

Safety & Security
- Security Ops Ctr
- Law Enforcement
- Fire
- EMS
- Emergency Mgmt
- EOC
- Contracted Security

Transportation
- Parking Garages
- Parking Lots
- EV Charging Areas
- Terminal Buses & Trams
- People Movers/Tram
- Helicopter Pad
- Roads/Highways

Workforce
- Airside Ops Personnel
- Landside Ops Personnel

Dependencies are relationships of reliance within and among infrastructure assets and systems that must be maintained for those systems to operate and provide services*

Types of Dependencies
- Physical
- Cyber
- Logical
- Geographic

External Dependencies for Airport Operations

Airlines

Aircraft

Air Traffic Control
- Control Facility
- Control Towers

Communications
- Fiber Optic
- Wireless
- Comms. Towers
- Cable TV
- Satellite Systems

Retail
- Food
- Shops
- Services

Safety & Security
- TSA
- Federal Air Security
- Customs & Immigration
- Local Law Enforcement
- Local Fire/EMS

Transportation
- Rideshare
- Rental Cars
- Public Transit
- Roads/Highways

Utilities
- Water
- Wastewater
- Electricity
- Garbage
- Recycling
- Petroleum
- Gas

Workforce
- Air Marshals
- TSA Agents
- FAA ATC Personnel
- Customs Personnel
- USDA Inspections Personnel
- Air Crews (Pilots & FA)
- Airline Personnel
- Airport Personnel
- Retail Personnel

*Source: https://www.cisa.gov/what-are-dependencies

Image source: INL.gov

Elements of Risk

- **Threat:** A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm.
- **Vulnerability:** A physical feature or operational attribute that renders an entity open to exploitation or susceptible.
- **Consequence:** The effect of an event, incident, or occurrence.

Assets, systems, and networks include one or more of the following elements:

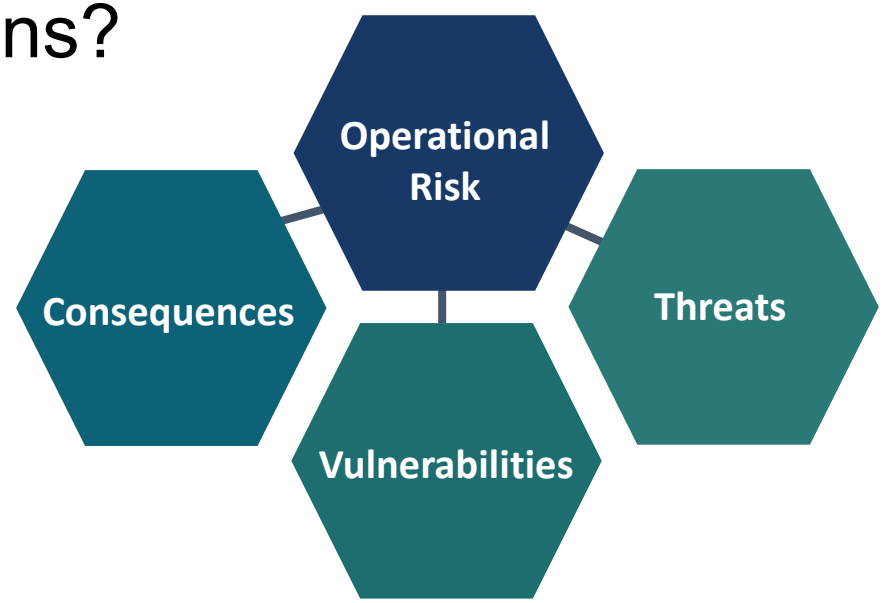
Physical – tangible property;

Cyber – electronic information and communications systems, and the information contained therein, and

Human – critical knowledge or functions of people uniquely susceptible to attack.

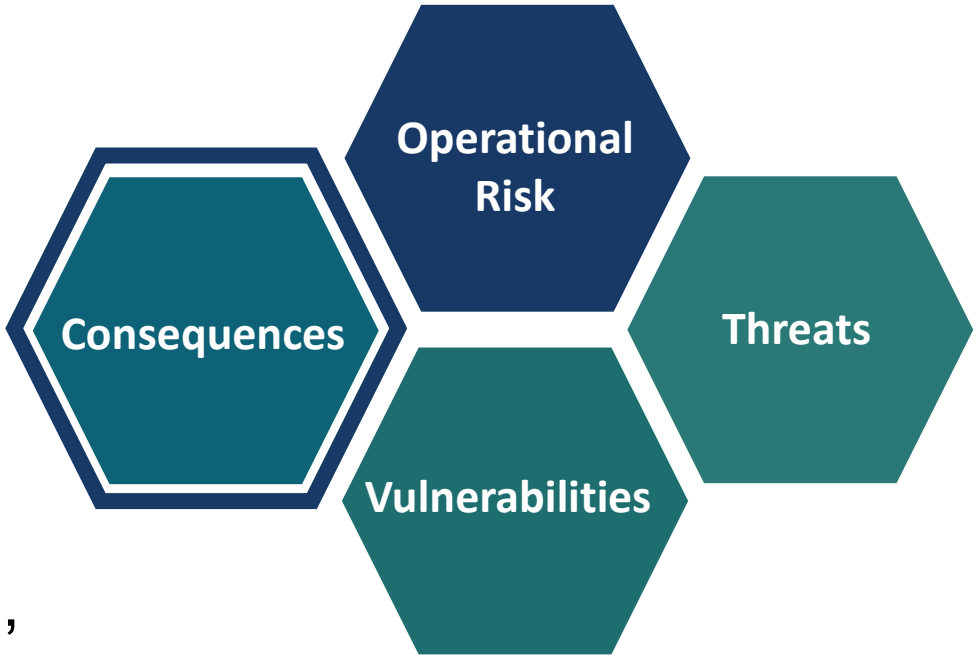
How well do you know your operational risks?

Can your team list the top three critical systems, including their priorities, cyber and physical dependencies (internal/external), degree of IT/OT convergence, key stakeholders (internal/external), and the incident response and recovery plans?



Operational Risk

- Captures “the **uncertainties and hazards** a company faces when it attempts to do its day-to-day activities.”
- Results from “**breakdowns in internal procedures, people, and systems**,” and focuses on “how things are accomplished within an organization.”
- Determined by analyzing the **consequences**, vulnerabilities, and threats within its procedures, workforce, and systems.



Before an organization can consider **vulnerabilities** within and **threats** to its operations, it must first have a solid understanding of the **consequences** existing inside it’s infrastructure environment.

Operational Risk (cont.)

Considerations:

- Infrastructure vs. Critical Infrastructure
- Security vs. Resilience
- Dependency vs. Interdependency

Operational Risk (cont.)

Reality	Challenge
Most entities know all the components to be binned, their connections, their complexities, and their potential **consequences**.	Knowledge is fractured into **operational silos** within the entity and/or all the **right people** needed to contribute to understanding the infrastructure environment are not part of the process.

- **Facility Engineer/Maintenance** and **Security Manager** have as much to contribute to understanding the cyber and physical infrastructure environment as the **Operations Manager/Director and Chief Information Officer**.
- **People (internal/external)** involved in directing, operating, maintaining, and supporting the cyber and physical infrastructure environment are essential to understanding and ultimately enhancing security and resilience.

The Realities of Cyberspace

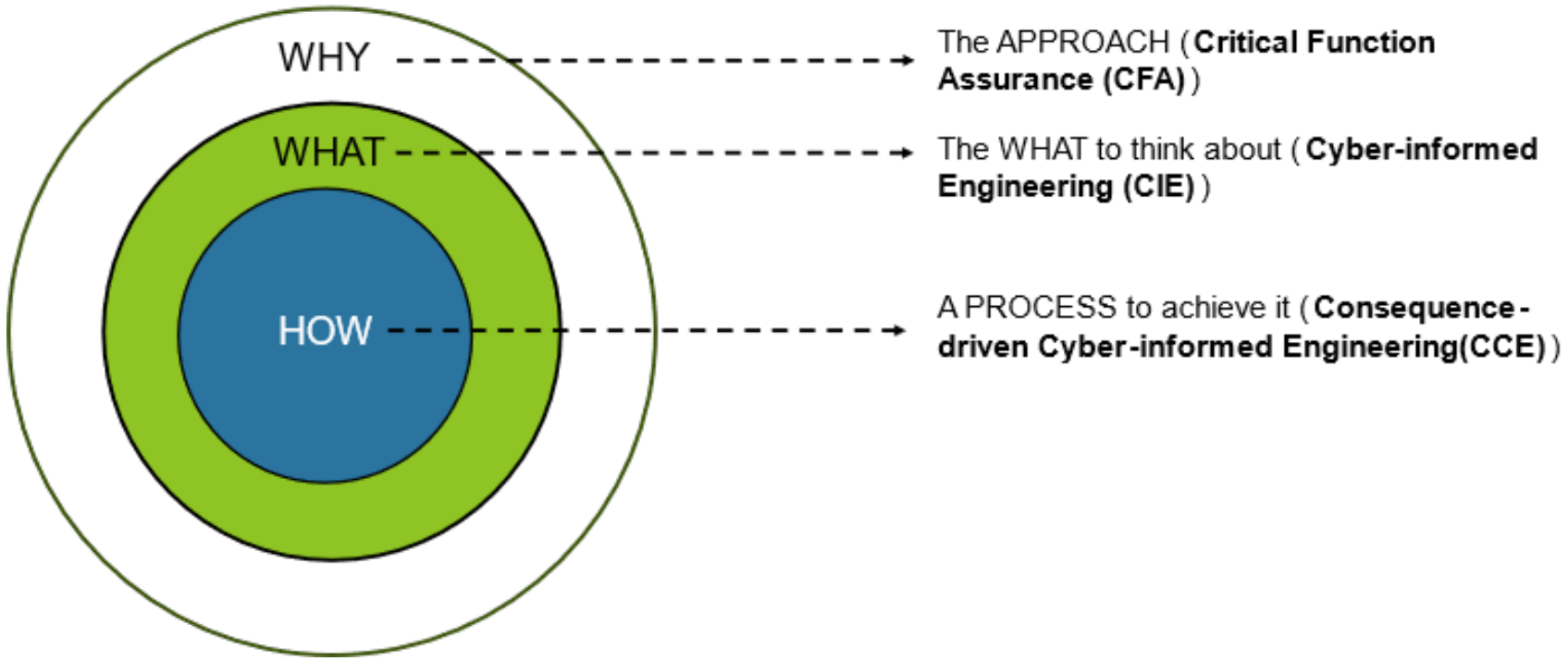
INL's technical doctrine is based on the following assumptions:

- **Existing security efforts are insufficient** to protect control systems and the infrastructure they support against catastrophic technical attacks.

- **A determined, well-resourced and patient adversary *WILL* succeed** in penetrating and exploiting a critical infrastructure network.

Given time and resources, cyber attackers WILL ***have success***

Disrupting Cyber-enabled Sabotage on Critical Functions



Critical Function Assurance

Cyber-Informed Engineering

CCE Consequence-driven Cyber-informed Engineering

Understanding CFA, CIE and CCE (cont.)

- **Critical Function Assurance (CFA)** is a **foundational approach** to identifying, prioritizing, and mitigating the risk that is inherent in the delivery of critical functions that depend on digital technology. ***(WHY)***

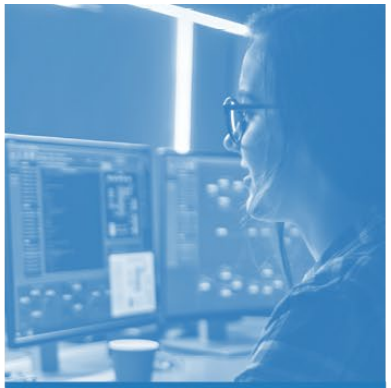
- **Cyber-informed Engineering (CIE)** is a **series of principles** focused on integrating cybersecurity considerations into the conception, design, development, and operation of any physical system that has digital connectivity, monitoring or control related to the delivery of a critical function. ***(WHAT)***

- **Consequence-driven Cyber-informed Engineering (CCE)** can be thought of as a **repeatable process** to apply elements of CFA and CIE to achieve assurance of critical functions. ***(HOW)***

Pillars of the National CIE Strategy

Awareness

Promulgate a universal and shared understanding of CIE

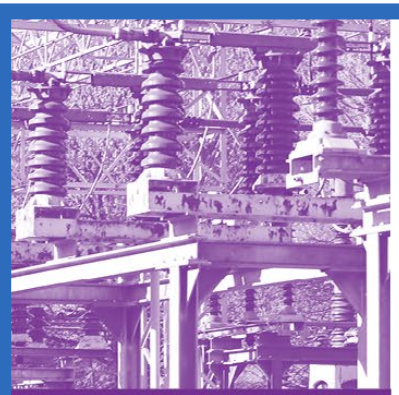


Education

Embed CIE into formal education, training, and credentialing

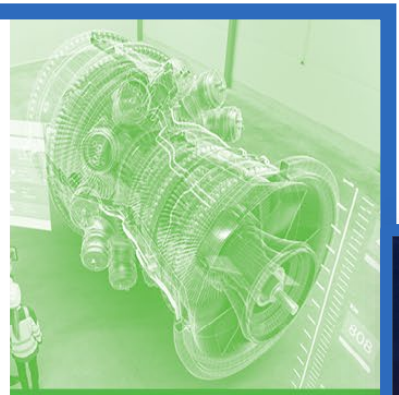
Development

Build the body of knowledge by which CIE is applied to specific implementations



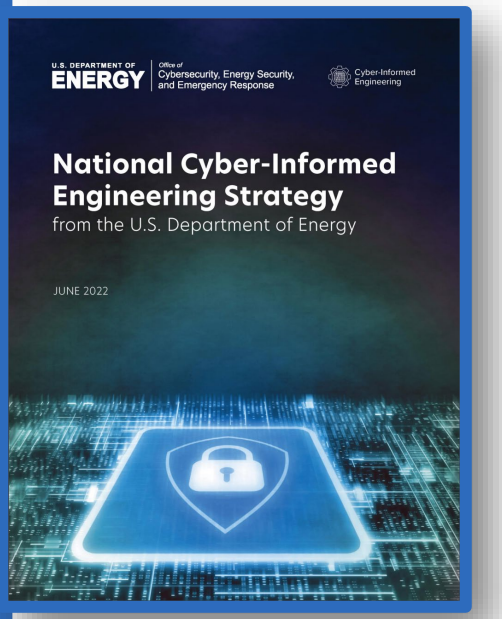
Current Infrastructure

Apply CIE principles to existing systemically important critical infrastructure



Future Infrastructure

Conduct R&D and develop an industrial base to build CIE into new infrastructure systems and emerging technology



https://www.energy.gov/

CIE Principles (What to think about)

https://www.energy.gov/

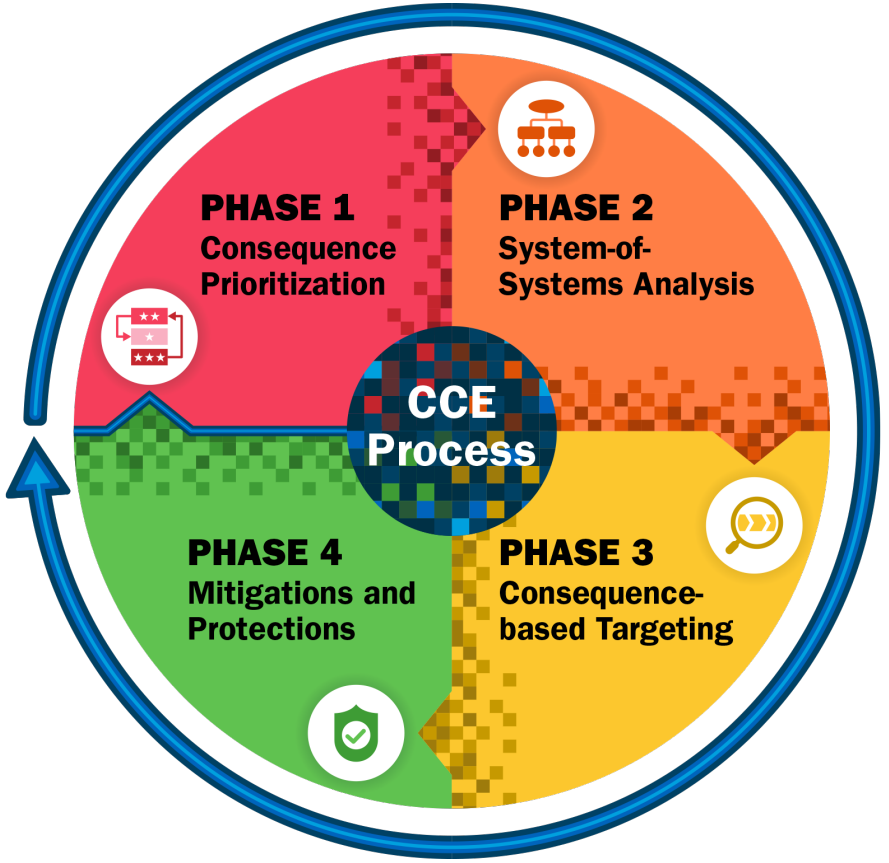
Principle	Key Question
Consequence-Focused Design	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
Engineered Controls	How do I implement controls to reduce avenues for attack or the damage which could result?
Secure Information Architecture	How do I prevent undesired manipulation of important data?
Design Simplification	How do I determine what features of my system are not absolutely necessary?
Layered Defenses	How do I create the best compilation of system defenses?
Active Defense	How do I proactively prepare to defend my system from any threat?
Interdependency Evaluation	How do I understand where my system can impact others or be impacted by others?
Digital Asset Awareness	How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?
Cyber-Secure Supply Chain Controls	How do I ensure my providers deliver the security we need?
Planned Resilience	How do I turn “what ifs” into “even ifs”?
Engineering Information Control	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
Cybersecurity Culture	How do I ensure that everyone performs their role aligned with our security goals?

SECURITY

Consequence-driven, Cyber-informed Engineering (CCE) (How to achieve it)

Structured Evaluation to Achieve Functional Assurance

CCE is a structured process to apply CIE principles to **understand how cyber-enabled sabotage could result in events that threaten national security and business viability, then identify the engineering changes or operational controls** that eliminate or significantly reduce the risk of those events.



2019 R&D 100 Award winner for cyber protection of critical infrastructure

https://inl.gov/national-security/cce/

DOE CIE and DHS CISA SBD Relationship

"While CISA's **Secure by Design** campaign by itself has great implications for society at writ large and especially the ICS community, I do want to take a moment to also acknowledge how **this effort critically intersects with and supports the Department of Energy's Cyber-Informed Engineering work which supports the resilience of our infrastructure** by ensuring that we're engineering cyber-attacks out of the system."

"Look, partnership is fundamental, innovation is critical. **Balancing and strongly moving forward on both fronts will be essential to ensuring the security of the nation's critical infrastructure**."

Cyber-Informed Engineering

Jen Easterly, Director
Cybersecurity and Infrastructure Security Agency

Hack the Capitol
May 30, 2024

+/- 160 software companies

https://cisa.gov

Addressing Consequence within Operational Risk: Why threats (plus vulnerabilities) and security are just not as important…

as…

Consequence (First Risk Consideration) and Resilience (Desired Outcome)

Thank You!