INL/CON-23-70754-Revision-0

Applying Cyber-Informed Engineering to Power System Operations

January 2023

Samuel Douglas Chanoski

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-23-70754-Revision-0

Applying Cyber-Informed Engineering to Power System Operations

Samuel Douglas Chanoski

January 2023

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

IEEE PES Power & Energy Society® | IEEE

Applying Cyber-Informed Engineering to Power System Operations

Sam Chanoski, CISSP, GCIP, GICSP, C|EH
Technical Relationship Manager
Idaho National Laboratory

IEEE Integrated Smart Grid Technologies NA 2023

INL Idaho National Laboratory

INL/CON-23-70754

Agenda

- System operator concepts
- Cyber-Informed Engineering
- Putting it Together

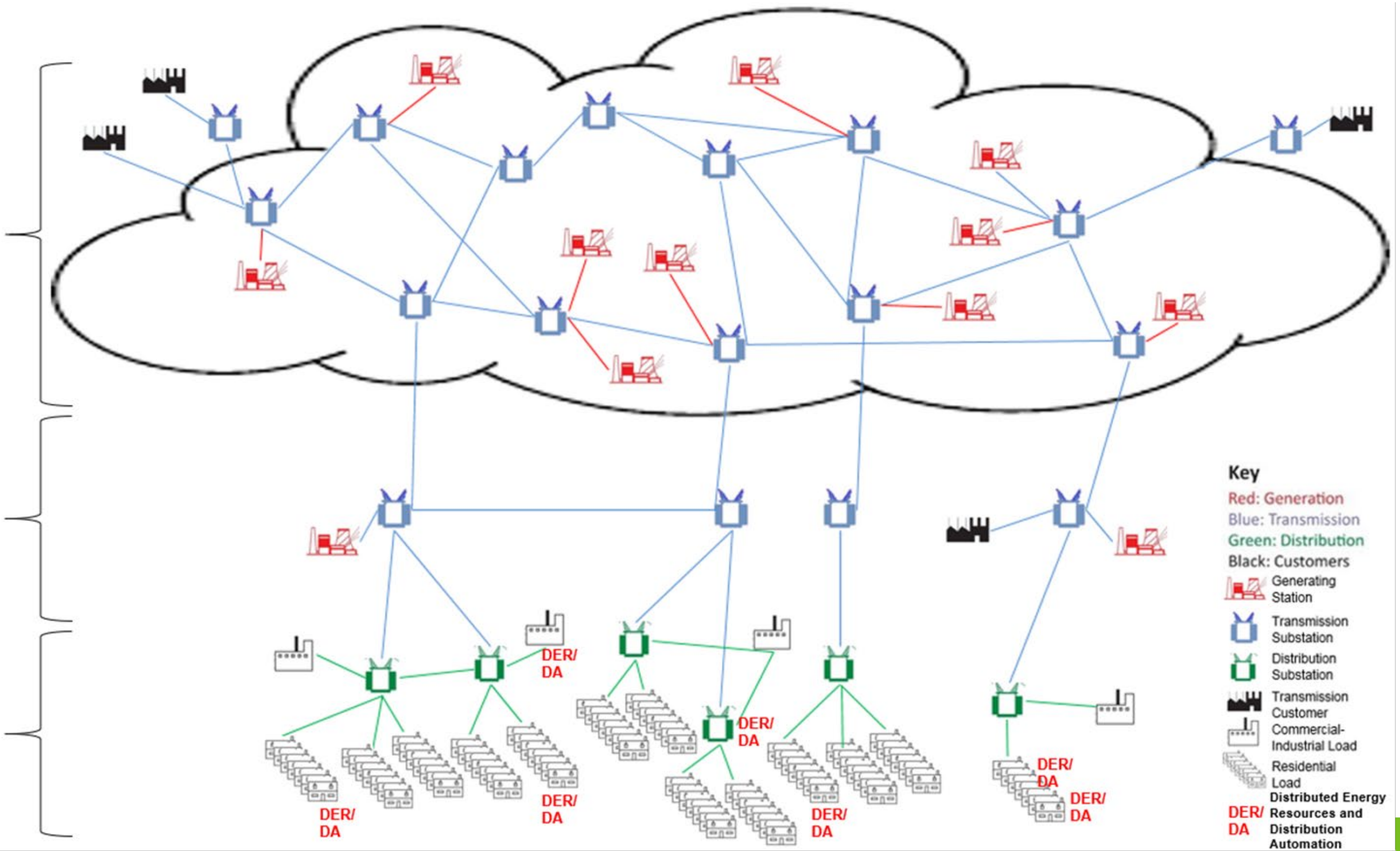
System Operator Concepts

Today’s Grid: A Mental Model

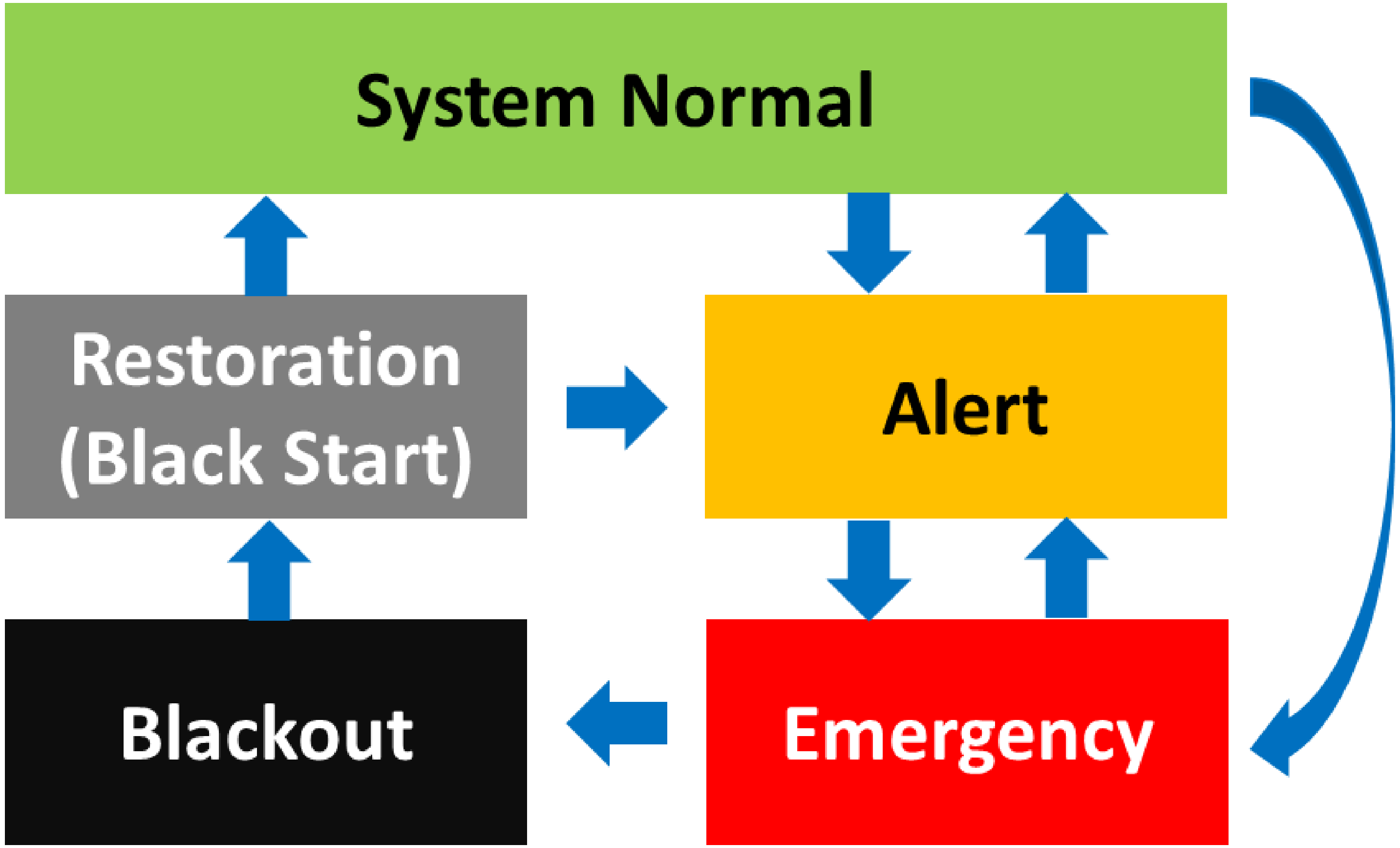
Bulk Electric System (BES): densely interconnected, highly reliable, redundant, NERC-regulated

Subtransmission: series-parallel paths from the BES to the lowest-voltage substations

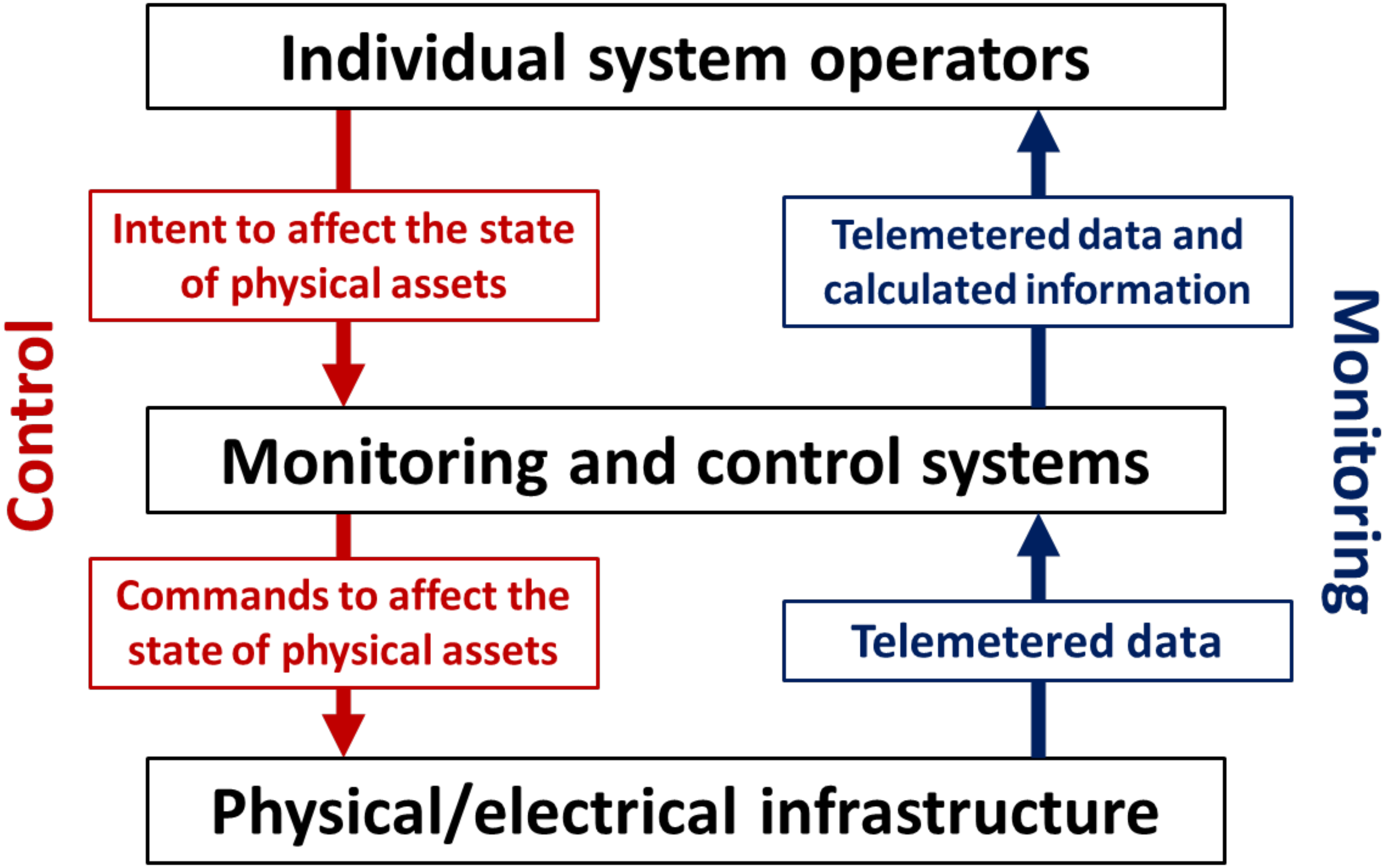
Distribution: radially connected load and DERs



Operating a Dynamic Grid



Human-Machine System of Systems



Individual system operators

Intent to affect the state of physical assets

Telemetered data and calculated information

Control

Monitoring

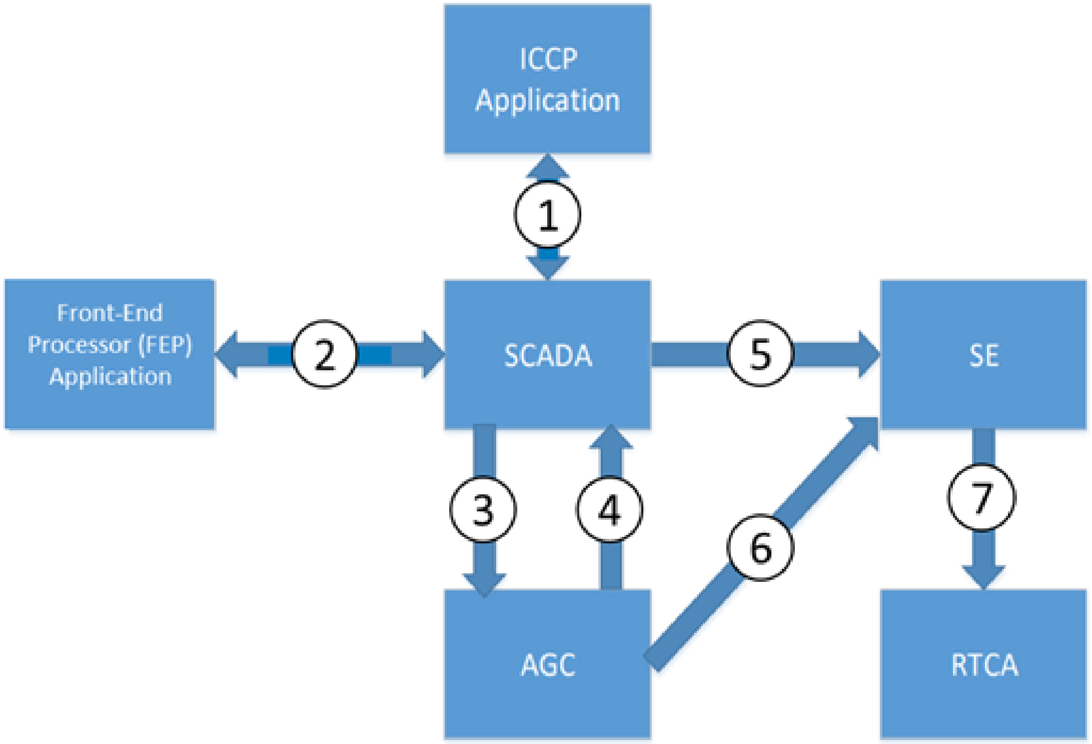
Monitoring and control systems

Commands to affect the state of physical assets

Telemetered data

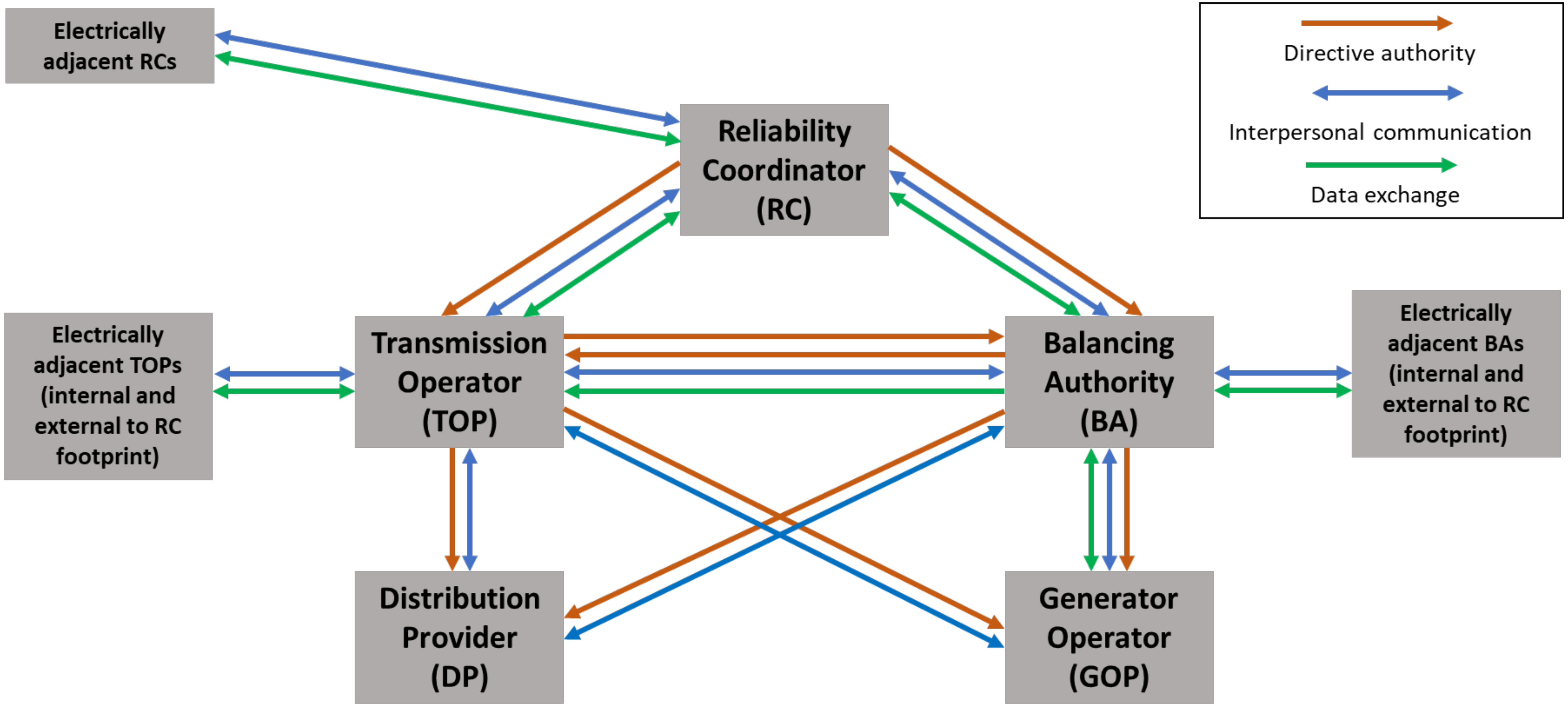
Physical/electrical infrastructure

Interdependent Tools



1. External data between ICCP and SCADA (bidirectional)
2. RTU/IED data and commands between FEP and SCADA (bidirectional)
3. Telemetered status and analog value data from SCADA to AGC
4. Updated set-point controls calculated by AGC
5. Equipment status, electrical quantities, and operating mode data from SCADA to SE
6. Generator status from AGC to SE
7. Base case solution from SE to RTCA

Organizational Team of Teams


Electrically adjacent RCs
Reliability Coordinator (RC)
Directive authority
Interpersonal communication
Data exchange
Electrically adjacent TOPs (internal and external to RC footprint)
Transmission Operator (TOP)
Balancing Authority (BA)
Electrically adjacent BAs (internal and external to RC footprint)
Distribution Provider (DP)
Generator Operator (GOP)

“Convergence”

	Information Technology (IT)	Operational Technology (OT)	Industrial Control Systems (ICS)
Purpose	• Processing information	• Processing information about physical processes	• Directly controlling physical processes
Software	• Many unrelated general purpose COTS applications on each host	• Purposeful COTS applications	• Single-purpose proprietary applications
OS	• Windows, macOS, Linux	• Windows, macOS, Linux	• Embedded RTOS
Hardware	• Commodity workstations and servers	• Dedicated commodity workstations and servers	• Purposeful devices
Resembles	• IT systems	• IT systems	• Grid infrastructure
“Triad”	• C-I-A	• A-I-C	• S-R-P

Cybersecurity Opportunities

Function	Category		Opportunity
Identify	ID.AM	Asset Management	
	ID.BE	Business Environment	✓
	ID.GV	Governance	
	ID.RA	Risk Assessment	✓
	ID.RM	Risk Management Strategy	
	ID.SC	Supply Chain Risk Management	
Protect	PR.AC	Identity Management and Access Control	
	PR.AT	Awareness and Training	✓
	PR.DS	Data Security	
	PR.IP	Information Protection Processes and Procedures	
	PR.MA	Maintenance	✓
	PR.PT	Protective Technology	✓
Detect	DE.AE	Anomalies and Events	✓
	DE.CM	Security Continuous Monitoring	✓
	DE.DP	Detection Processes	✓
Respond	RS.RP	Response Planning	✓
	RS.CO	Communications	
	RS.AN	Analysis	✓
	RS.MI	Mitigation	✓
	RS.IM	Improvements	
Recover	RC.RP	Recovery Planning	✓
	RC.IM	Improvements	✓
	RC.CO	Communications	✓

Cyber-Informed Engineering

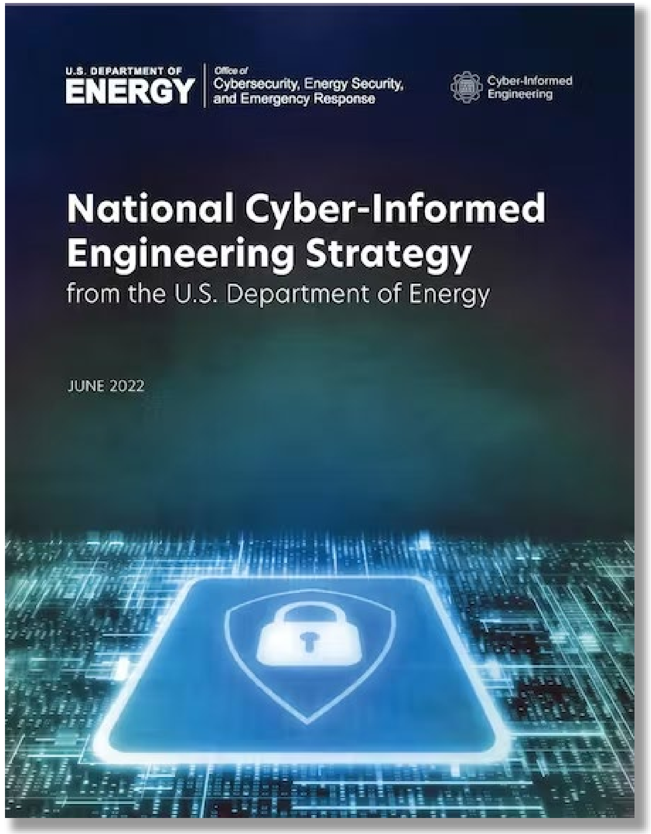
Cyber-Informed Engineering (CIE)

- Consistent observation that **engineers and technical staff** are **not aware** of how cyber threats affect digital designs and operations

- Need to ensure that **inherent risks of digital technology** (which manifest through failure, error, malign disruption, or compromise) are considered and mitigated in the **earliest possible stages** of the design lifecycle

Cyber-Informed Engineering (CIE)

- CIE uses **design decisions** and **engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to “engineer out” cyber risk** throughout the design and operation lifecycle, rather than add cybersecurity controls after the fact.
- Focused on **engineers and technicians**, CIE provides a framework for cyber education, awareness, and accountability.
- CIE aims to engender a **culture of security** aligned with the existing industry safety culture.
- For more information: https://inl.gov/cie/

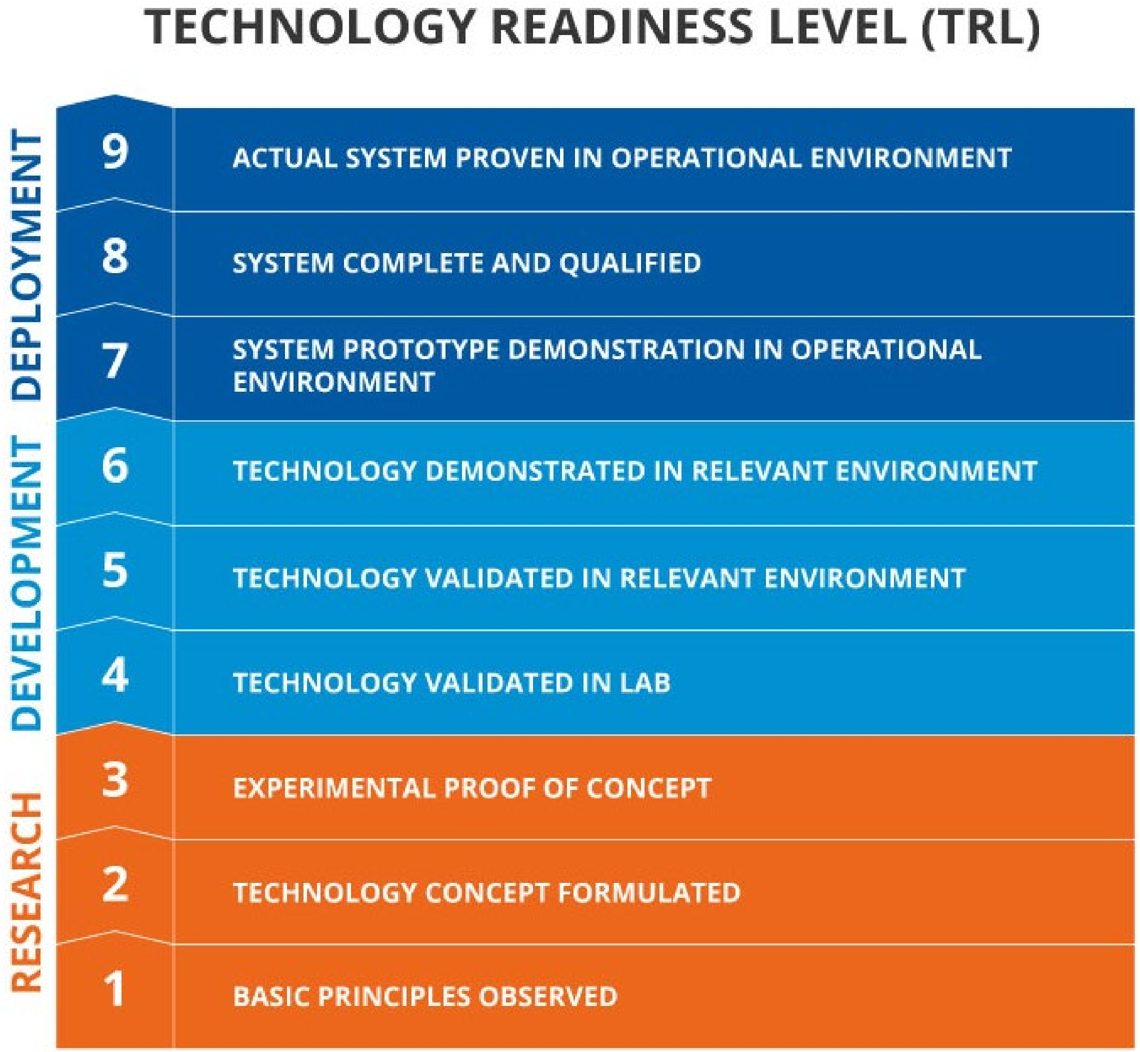


U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response | Cyber-Informed Engineering

National Cyber-Informed Engineering Strategy
from the U.S. Department of Energy

JUNE 2022

CIE in Technology Readiness Levels



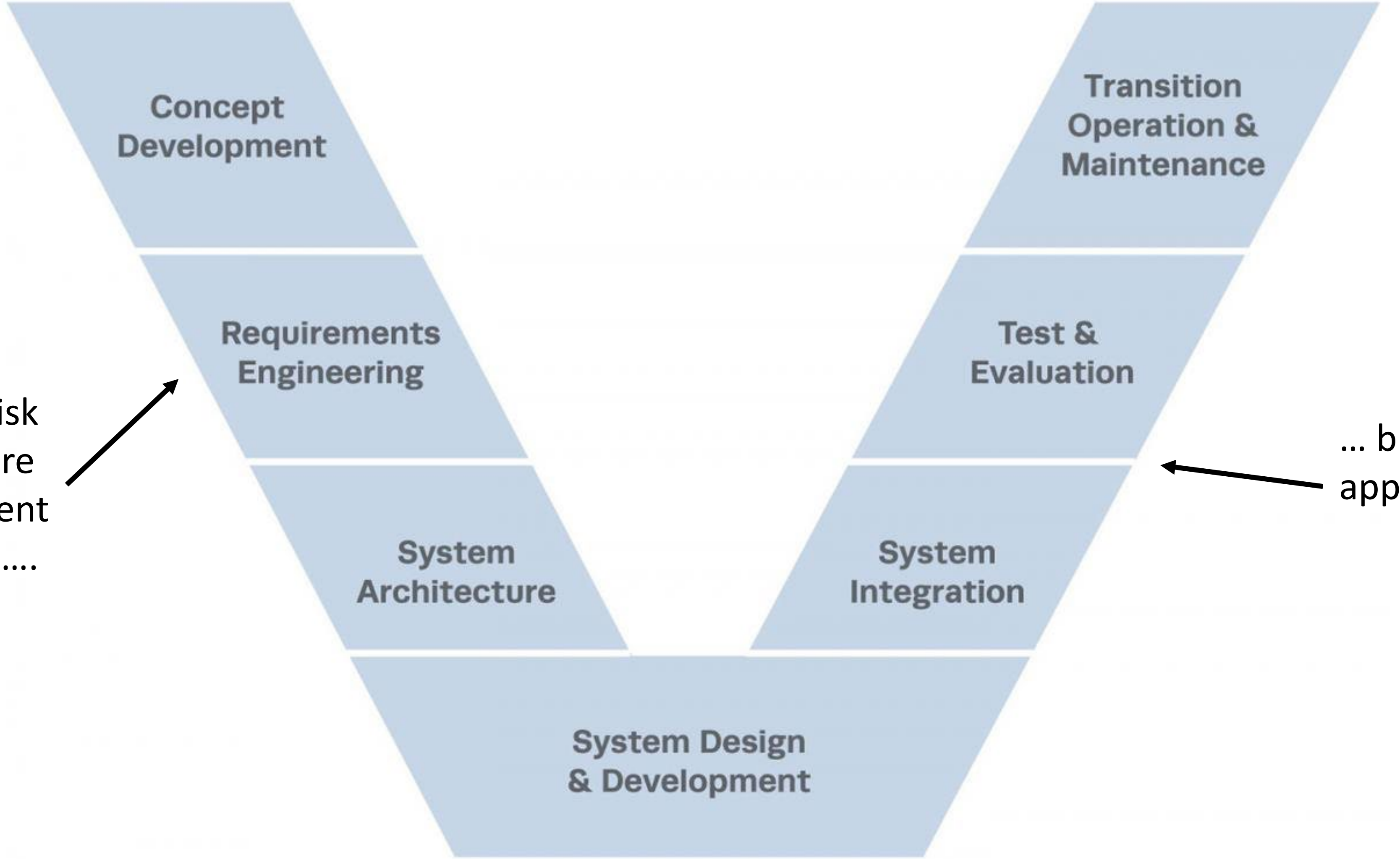
TECHNOLOGY READINESS LEVEL (TRL)

DEPLOYMENT	9	ACTUAL SYSTEM PROVEN IN OPERATIONAL ENVIRONMENT
	8	SYSTEM COMPLETE AND QUALIFIED
	7	SYSTEM PROTOTYPE DEMONSTRATION IN OPERATIONAL ENVIRONMENT
DEVELOPMENT	6	TECHNOLOGY DEMONSTRATED IN RELEVANT ENVIRONMENT
	5	TECHNOLOGY VALIDATED IN RELEVANT ENVIRONMENT
	4	TECHNOLOGY VALIDATED IN LAB
RESEARCH	3	EXPERIMENTAL PROOF OF CONCEPT
	2	TECHNOLOGY CONCEPT FORMULATED
	1	BASIC PRINCIPLES OBSERVED

Traditional OT Cybersecurity risk mitigations are usually applied here…

… but are more effective and efficient when applied here.

CIE in Systems Engineering



OT Cybersecurity risk mitigations are more effective and efficient when applied here….

… but are usually applied here.

Principles of CIE

Design and Operations

Consequence-focused design

Engineered Controls

Secure information architecture

Design Simplification

Resilient layered defenses

Active defense

Organizational

Interdependency evaluation

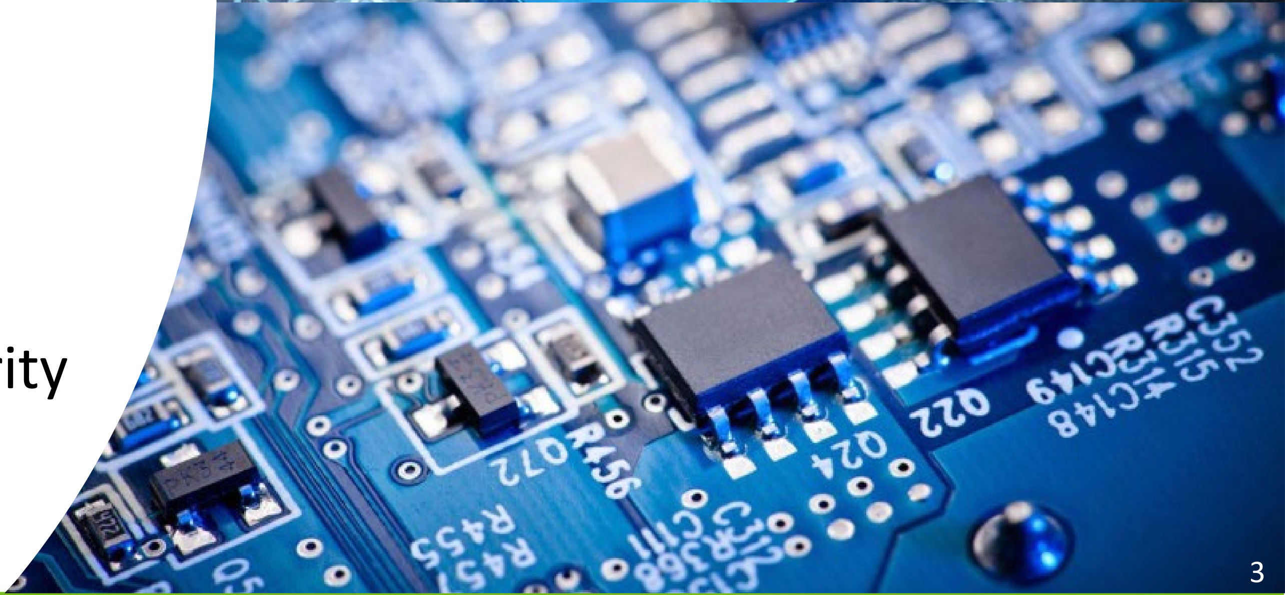
Digital asset awareness

Cyber-secure supply chain controls

Planned resilience with no assumed security

Engineering information control

Security culture



Putting it Together

CIE Principles Relevant to SysOps

Design and Operations

Consequence-focused design

Engineered Controls

Secure information architecture

Design Simplification

Resilient layered defenses

Active defense

Organizational

Interdependency evaluation

Digital asset awareness

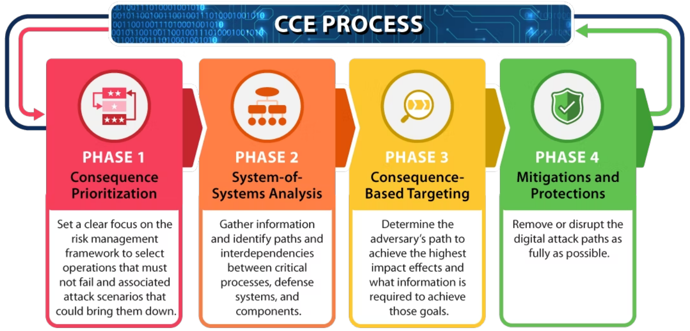
Cyber-secure supply chain controls

Planned resilience with no assumed security

Engineering information control

Security culture

How do *YOU* CIE?



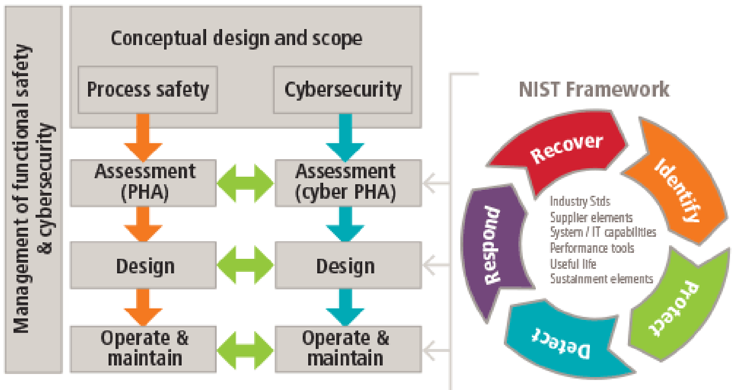
CCE PROCESS

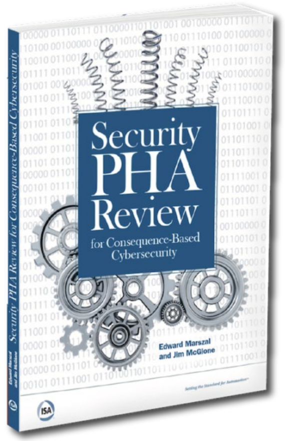
PHASE 1
Consequence Prioritization
Set a clear focus on the risk management framework to select operations that must not fail and associated attack scenarios that could bring them down.

PHASE 2
System-of-Systems Analysis
Gather information and identify paths and interdependencies between critical processes, defense systems, and components.

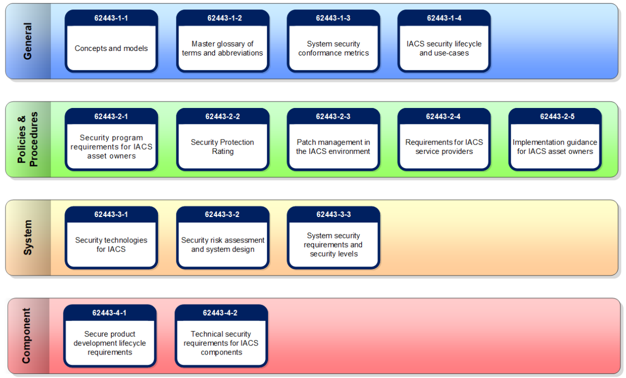
PHASE 3
Consequence-Based Targeting
Determine the adversary's path to achieve the highest impact effects and what information is required to achieve those goals.

PHASE 4
Mitigations and Protections
Remove or disrupt the digital attack paths as fully as possible.

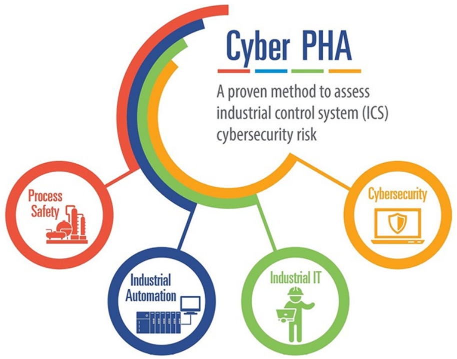




Security PHA Review
for Consequence-Based Cybersecurity
Edward Marszal and Jim McGlone

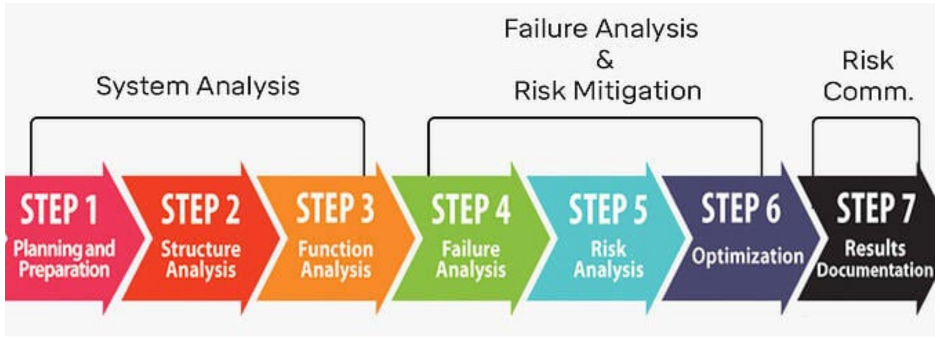


General	62443-1-1 Concepts and models	62443-1-2 Master glossary of terms and abbreviations	62443-1-3 System security conformance metrics	62443-1-4 IACS security lifecycle and use-cases	
Policies & Procedures	62443-2-1 Security program requirements for IACS asset owners	62443-2-2 Security Protection Rating	62443-2-3 Patch management in the IACS environment	62443-2-4 Requirements for IACS service providers	62443-2-5 Implementation guidance for IACS asset owners
System	62443-3-1 Security technologies for IACS	62443-3-2 Security risk assessment and system design	62443-3-3 System security requirements and security levels		
Component	62443-4-1 Secure product development lifecycle requirements	62443-4-2 Technical security requirements for IACS components			



Cyber PHA

A proven method to assess industrial control system (ICS) cybersecurity risk



System Analysis
Failure Analysis & Risk Mitigation
Risk Comm.
STEP 1 Planning and Preparation
STEP 2 Structure Analysis
STEP 3 Function Analysis
STEP 4 Failure Analysis
STEP 5 Risk Analysis
STEP 6 Optimization
STEP 7 Results Documentation

Questions?

Sam Chanoski, CISSP, GCIP, GICSP, C|EH
Technical Relationship Manager
Idaho National Laboratory
samuel.chanoski@inl.gov.net

https://inl.gov/cie/
https://www.energy.gov/ceser/securing-energy-infrastructure-executive-task-force