Integrating Cybersecurity with System Operations and Restoration

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

IEEE Power & Energy Society General Meeting 2022

INL/CON-22-67993

Agenda

- System operator concepts
- Looking inward – securing system operator organizations
- Looking outward – securing system operator functions

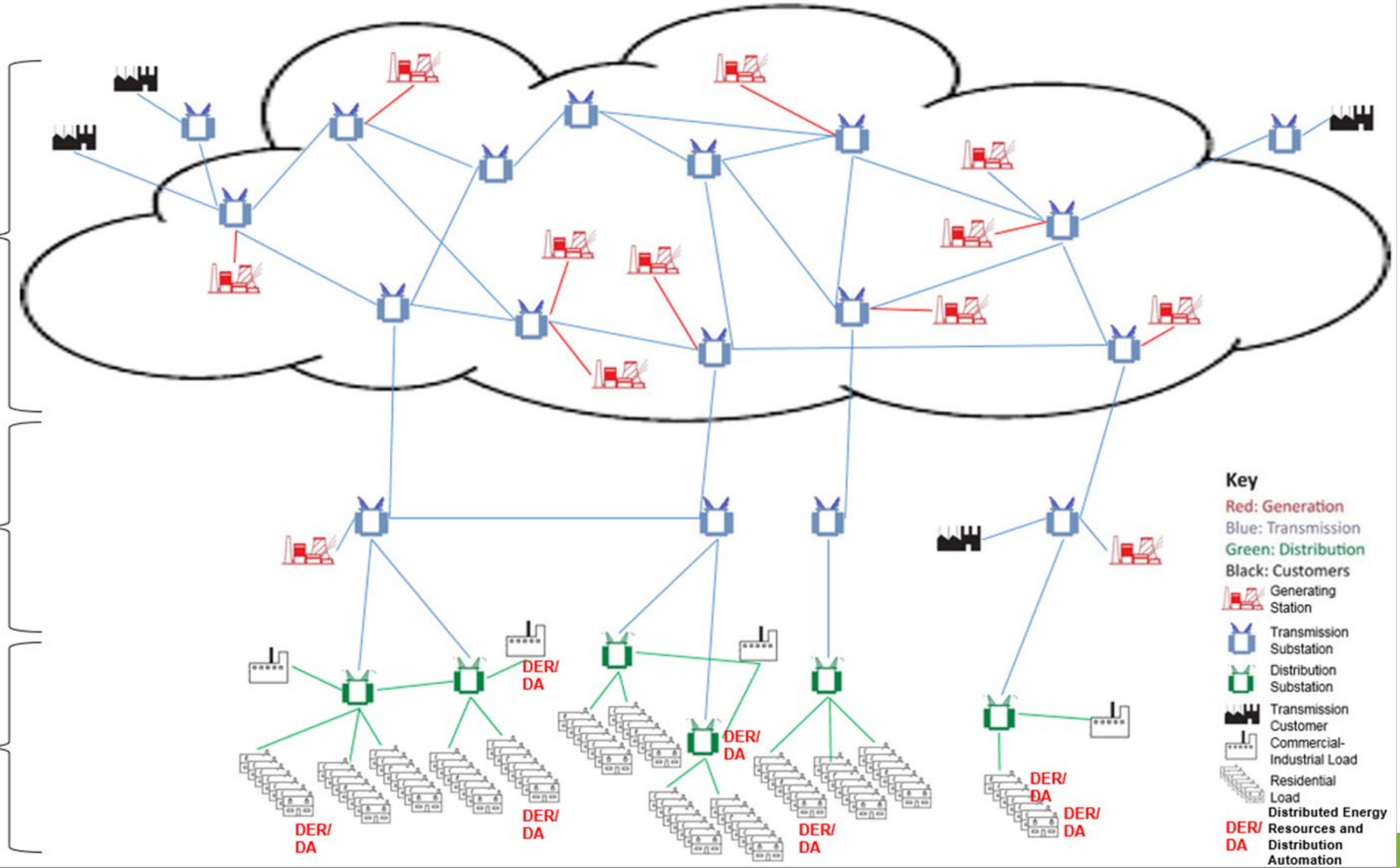
System Operator Concepts

Today's Grid: A Mental Model

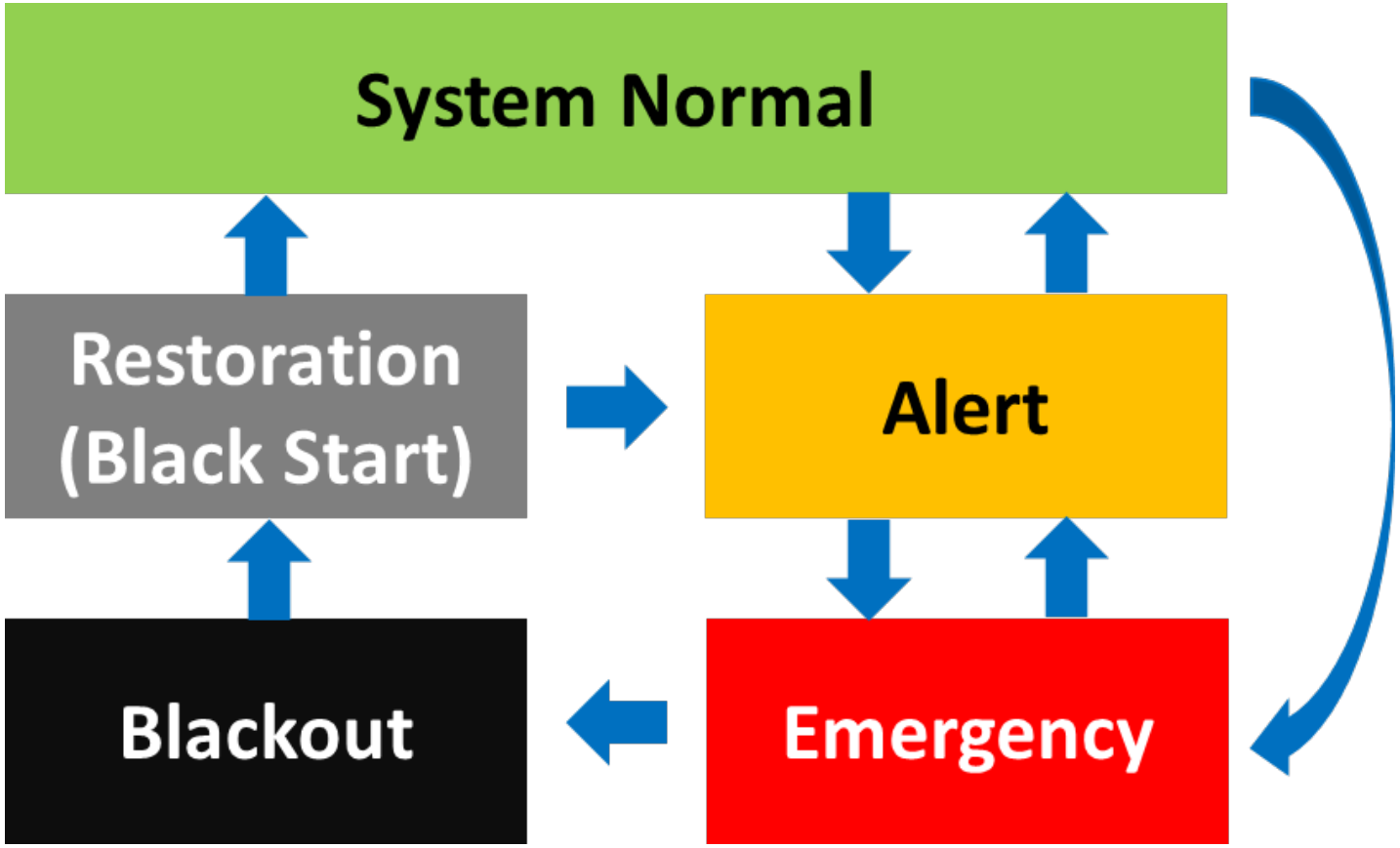
Bulk Electric System (BES): densely interconnected, highly reliable, redundant, NERC-regulated

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

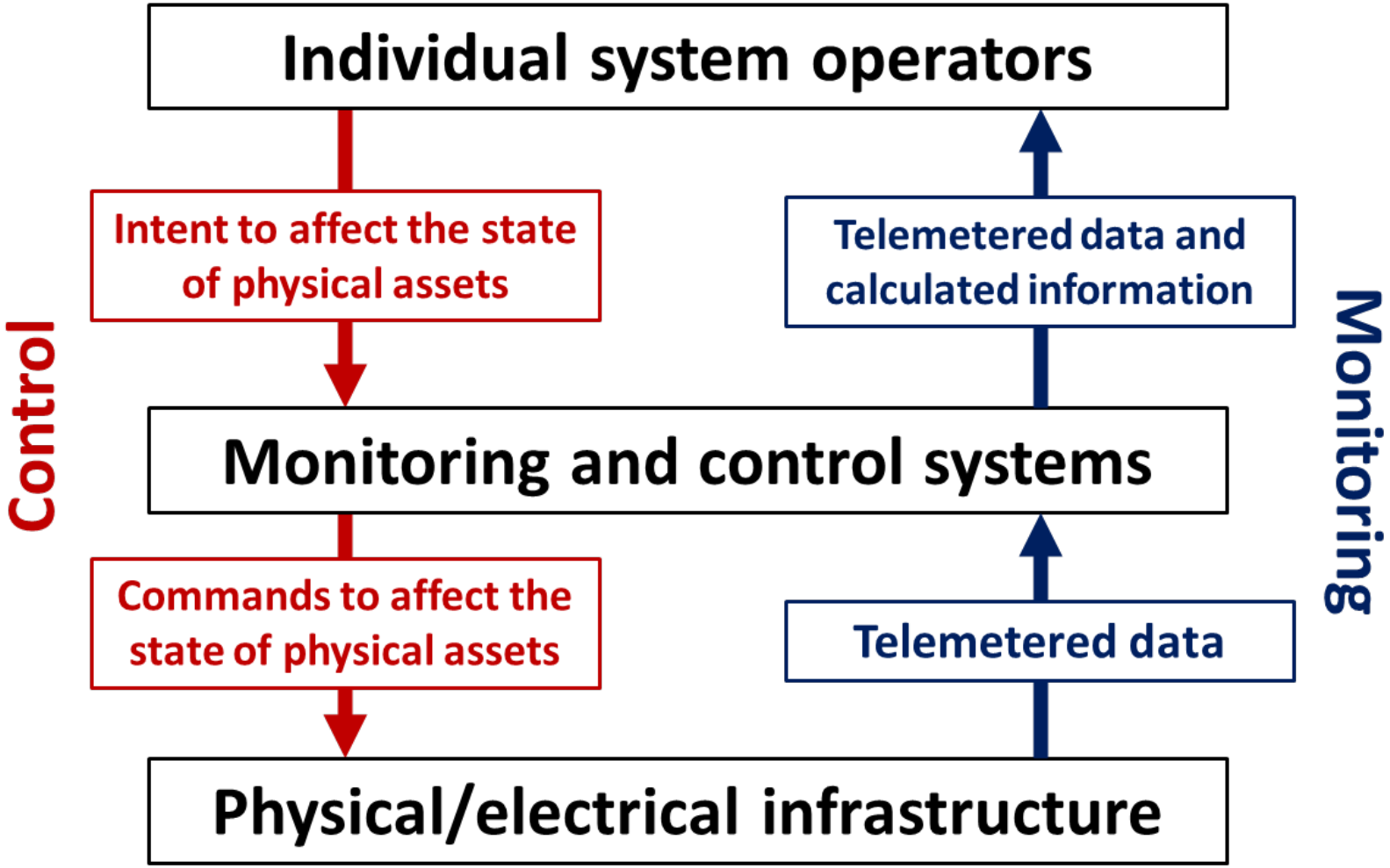
Distribution: radially connected load and DERs



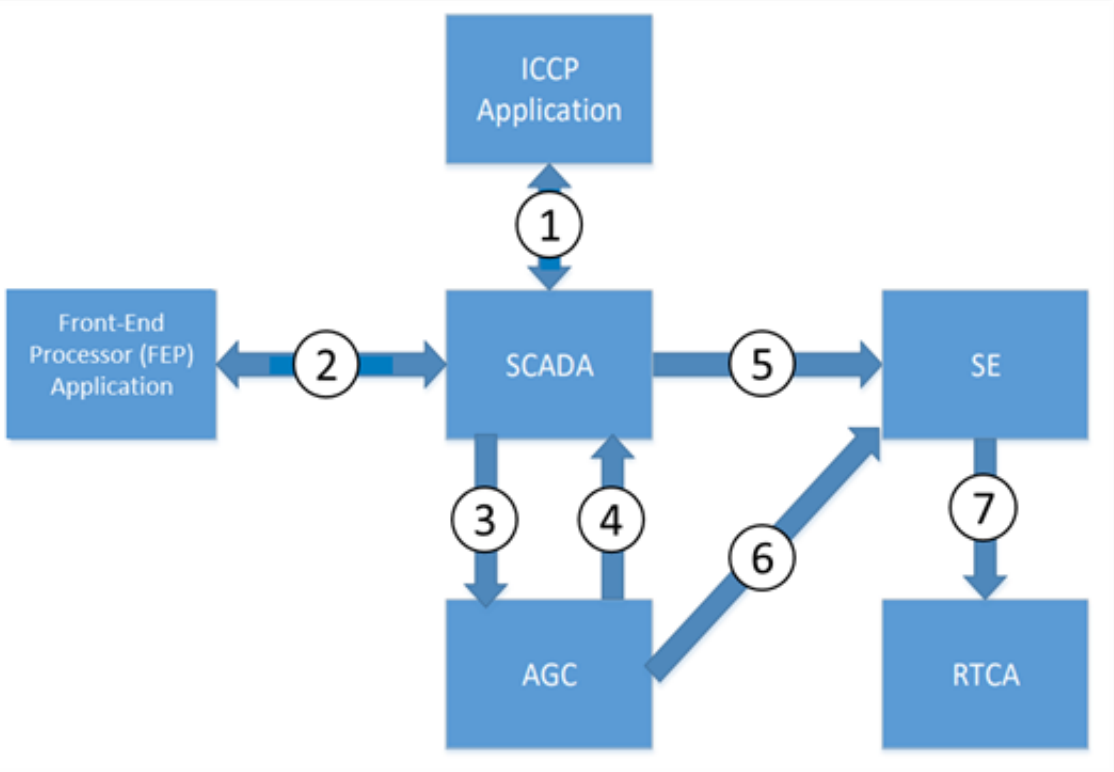
Operating a Dynamic Grid



Human-Machine System of Systems

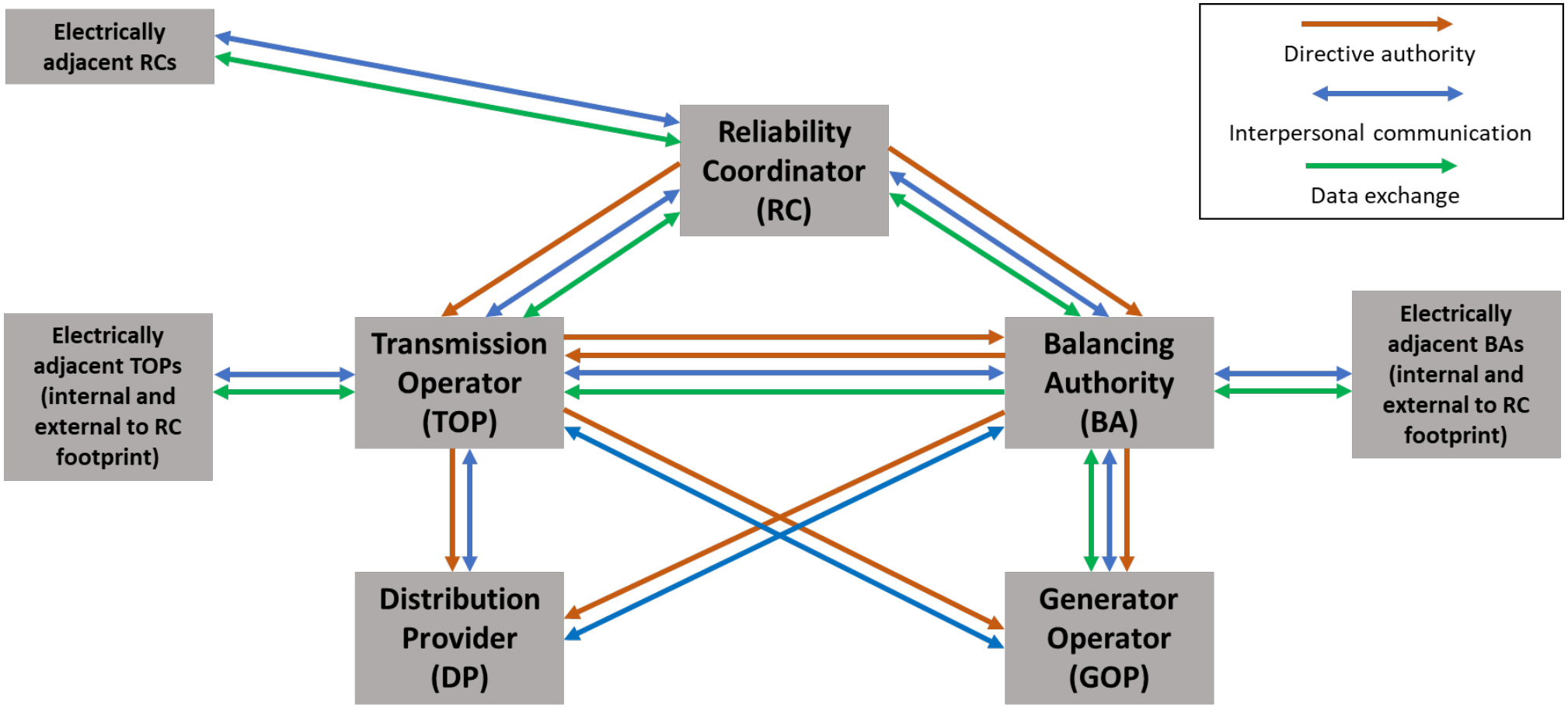


Interdependent Tools



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

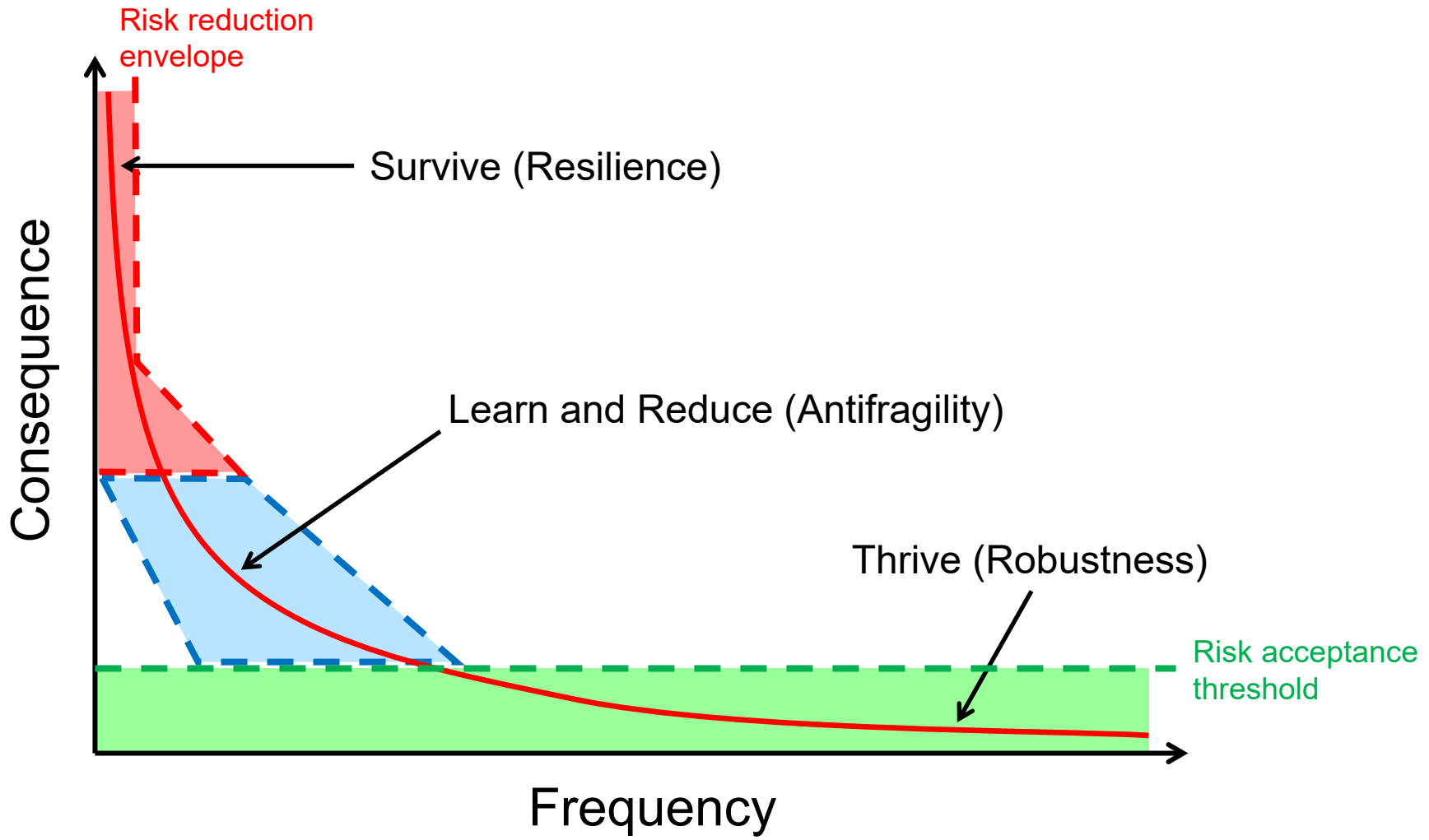


Looking Inward

“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
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

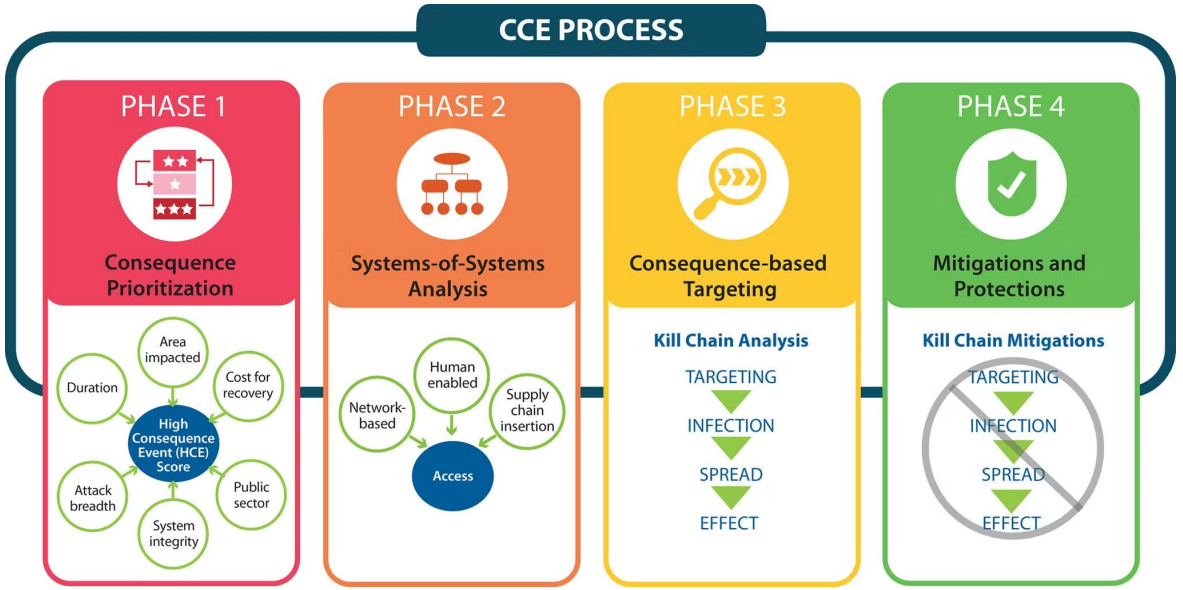
Cyber Harms and Management Approaches

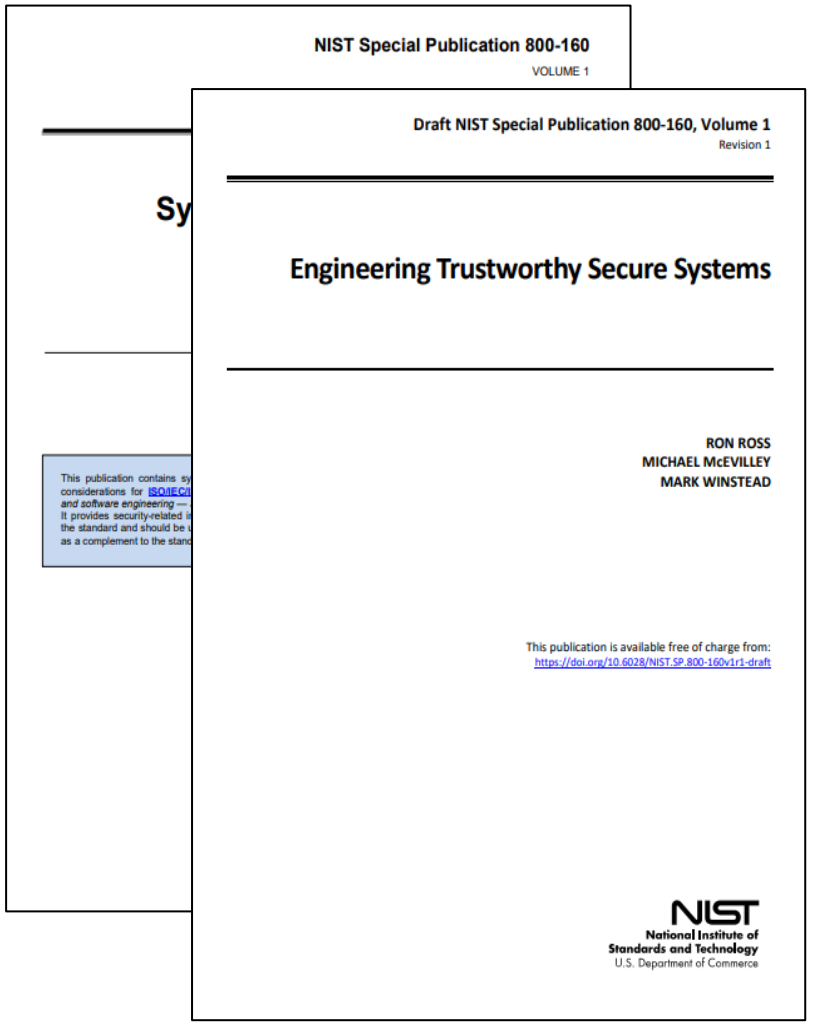


Standards-based Approaches

- IT security management and controls
  - ISO 27001 and 27002
  - NIST Cybersecurity Framework and SP 800-53
- OT/ICS security management and controls
  - ISA/IEC 62443 family
- Industry-specific technical guidance
  - IEEE standards, particularly C37.240
  - IEC 62351 family

Resilience Approaches





Looking Outward

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	✓

Identify

- Business Environment
  - Highlight and explain dependencies and interdependencies
- Risk Assessment
  - Enumerate and prioritize consequences
  - Incorporate industry experience for infrequent risks

Protect

- Awareness and Training
  - Involve cyber-enabled consequences in operations drills and sustainment training scenarios
- Maintenance
  - Incorporate security drivers into routine checks and testing
  - Assure infrequently used capabilities remain viable
- Protective Technology
  - Defensible OT architecture
  - Proactive system posture based on security threat

Detect

- Anomalies and Events
  - Conscious recognition and characterization of anomalies
- Security Continuous Monitoring
  - Develop and incorporate security-driven contingencies into automation and human monitoring tasks
- Detection Processes
  - Escalation from individual recognition to organizational cognizance
  - Cross-checks of operations and cybersecurity data

Respond

- Response Planning
  - Harmonize security into existing plans
  - Standing information requirements
- Analysis
  - Current and contingency operational impacts (safety, reliability, cost)
  - Trust in potentially impacted systems and unique restoration considerations
- Mitigation
  - Posturing the system to accommodate digital isolation and eradication activities

Recover

- Recovery Planning
  - “Cyber blackstart” and restoration without tools
  - Prolonged degraded operations
- Improvements
  - Causal analysis and corrective actions
  - Learn from other organizations’ experience
- Communications
  - Sharing observations, insights, and lessons learned with industry

Questions?

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

Idaho National Laboratory

https://inl.gov/cyote/
https://inl.gov/secureENERGY/
https://inl.gov/cie/