INL/CON-22-66738-Revision-0

Integrating Cybersecurity with System Operations and Restoration

April 2022

Samuel Douglas Chanoski

Changing the World's Energy Future

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

INL/CON-22-66738-Revision-0

Integrating Cybersecurity with System Operations and Restoration

Samuel Douglas Chanoski

April 2022

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

Integrating Cybersecurity with System Operations and Restoration

Sam Chanoski, CISSP, GCIP, GICSP, C|EH – Idaho National Laboratory

INL/CON-22-66738

Agenda

- A good mental model for risk
- Cyber harms and risk management approaches
- Relevant system operator concepts
- Cyber implications from a resilience event example

Risk Mental Model

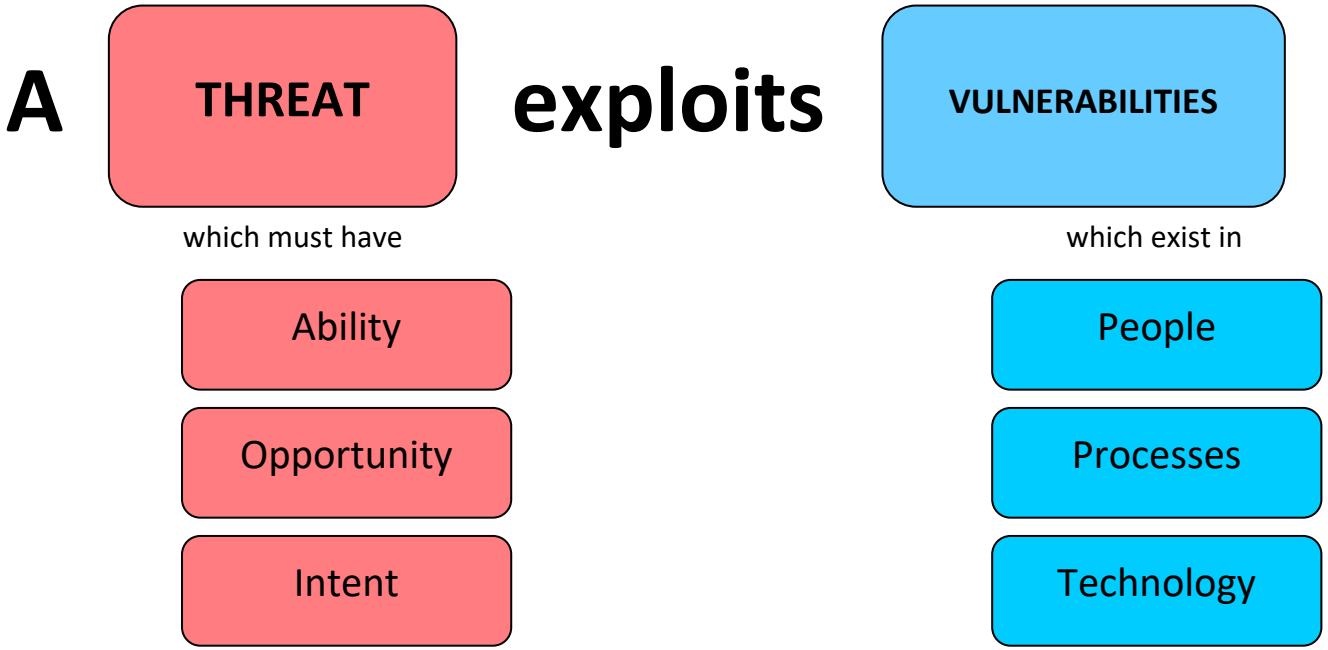
Disaggregating Risk

THREAT

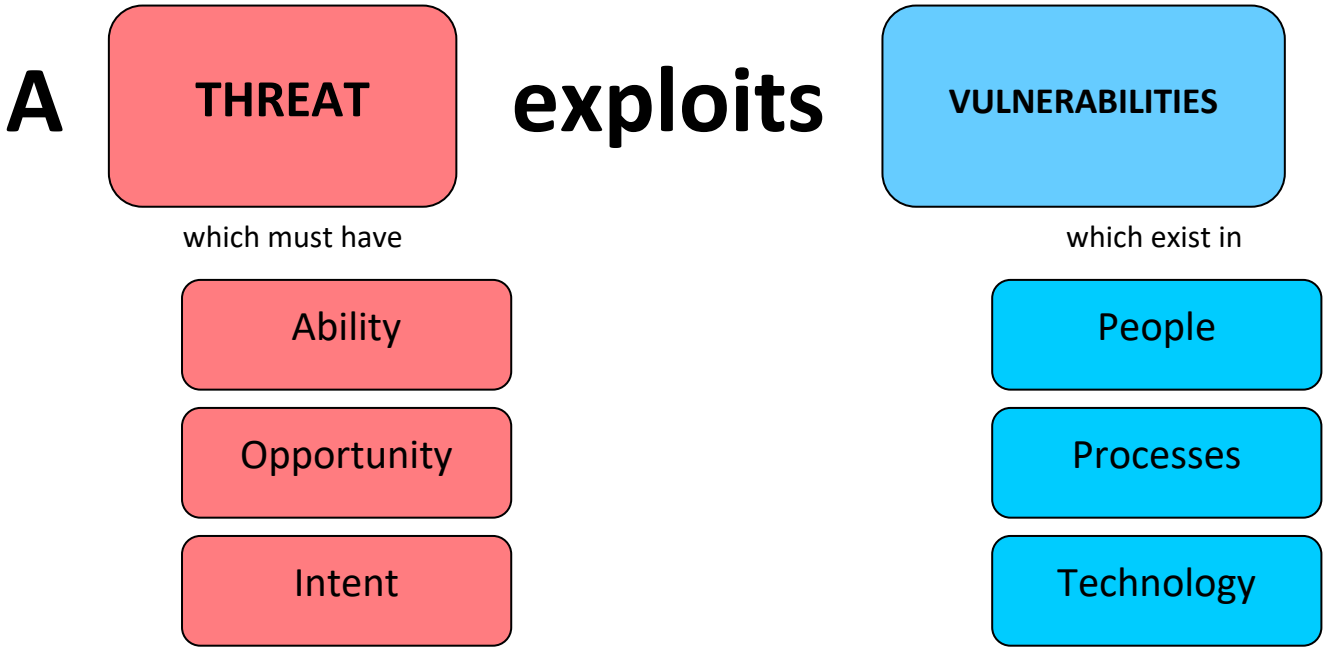
which must have

- Ability
- Opportunity
- Intent

Disaggregating Risk



Disaggregating Risk



~Likelihood

Disaggregating Risk

A **THREAT** **exploits** **VULNERABILITIES** **to impose** **CONSEQUENCES**

which must have

- Ability
- Opportunity
- Intent

which exist in

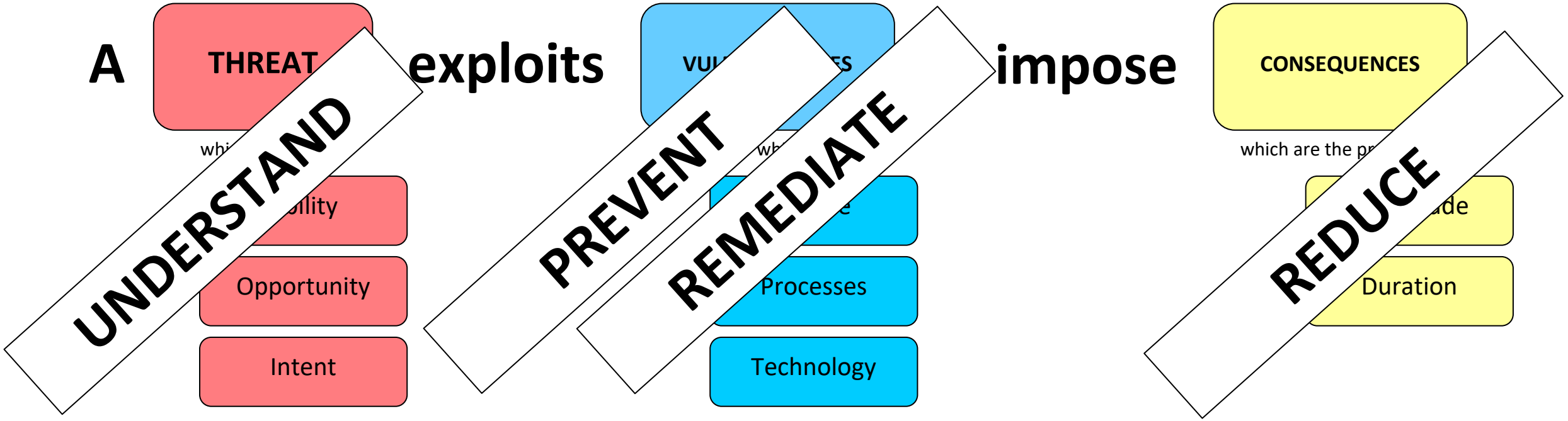
- People
- Processes
- Technology

which are the product of

- Magnitude
- Duration

~Likelihood

Disaggregating Risk



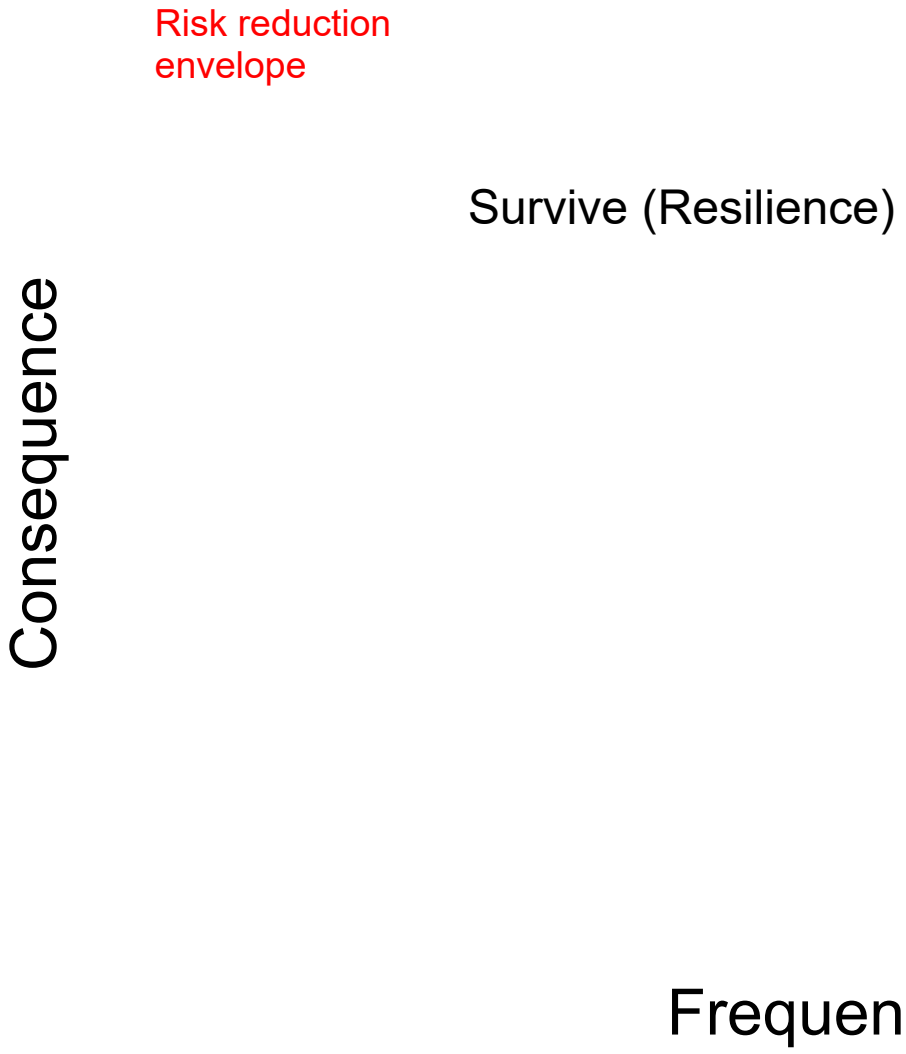
~Likelihood

Managing Cyber Harms

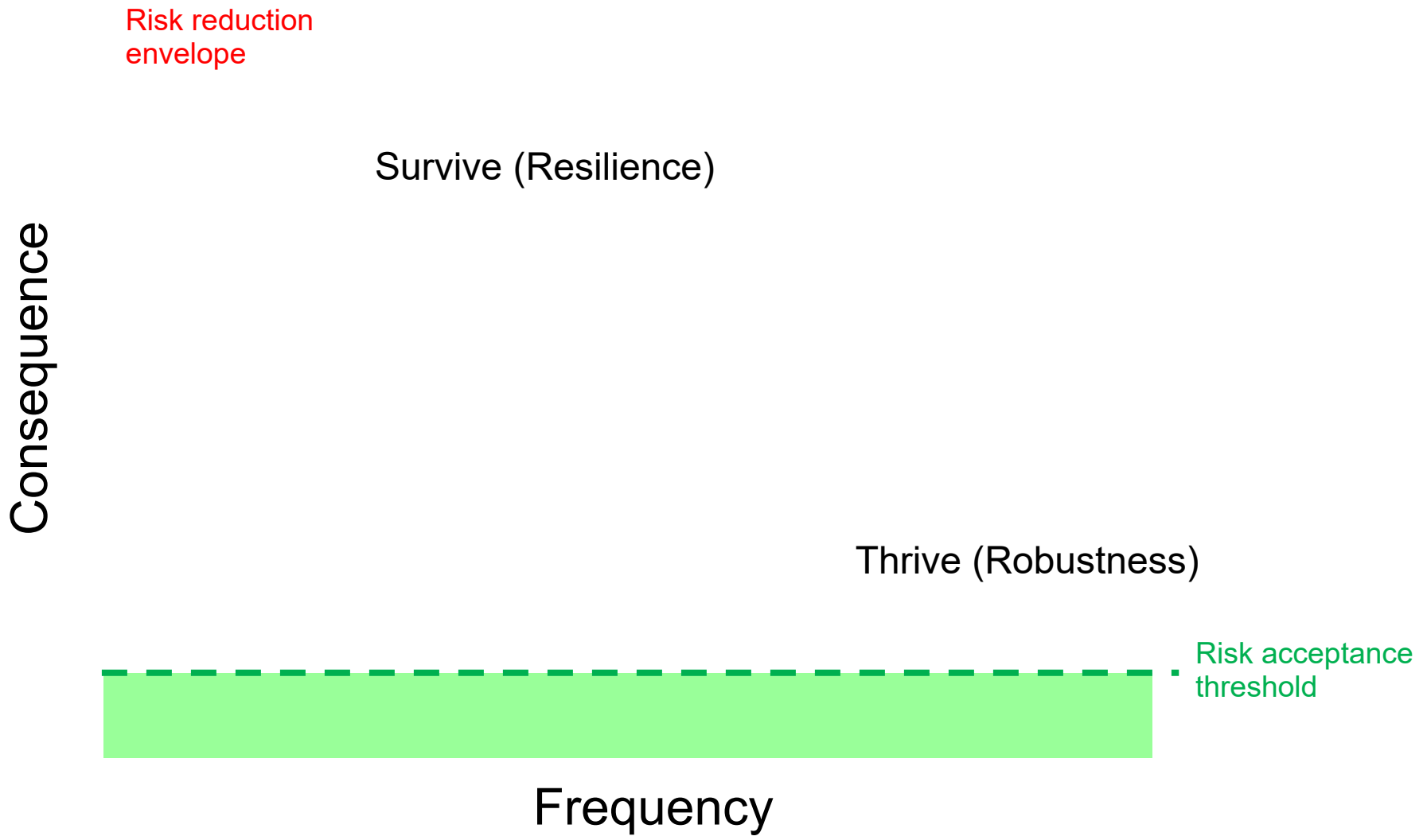
Cyber Harms and Management Approaches

Frequency

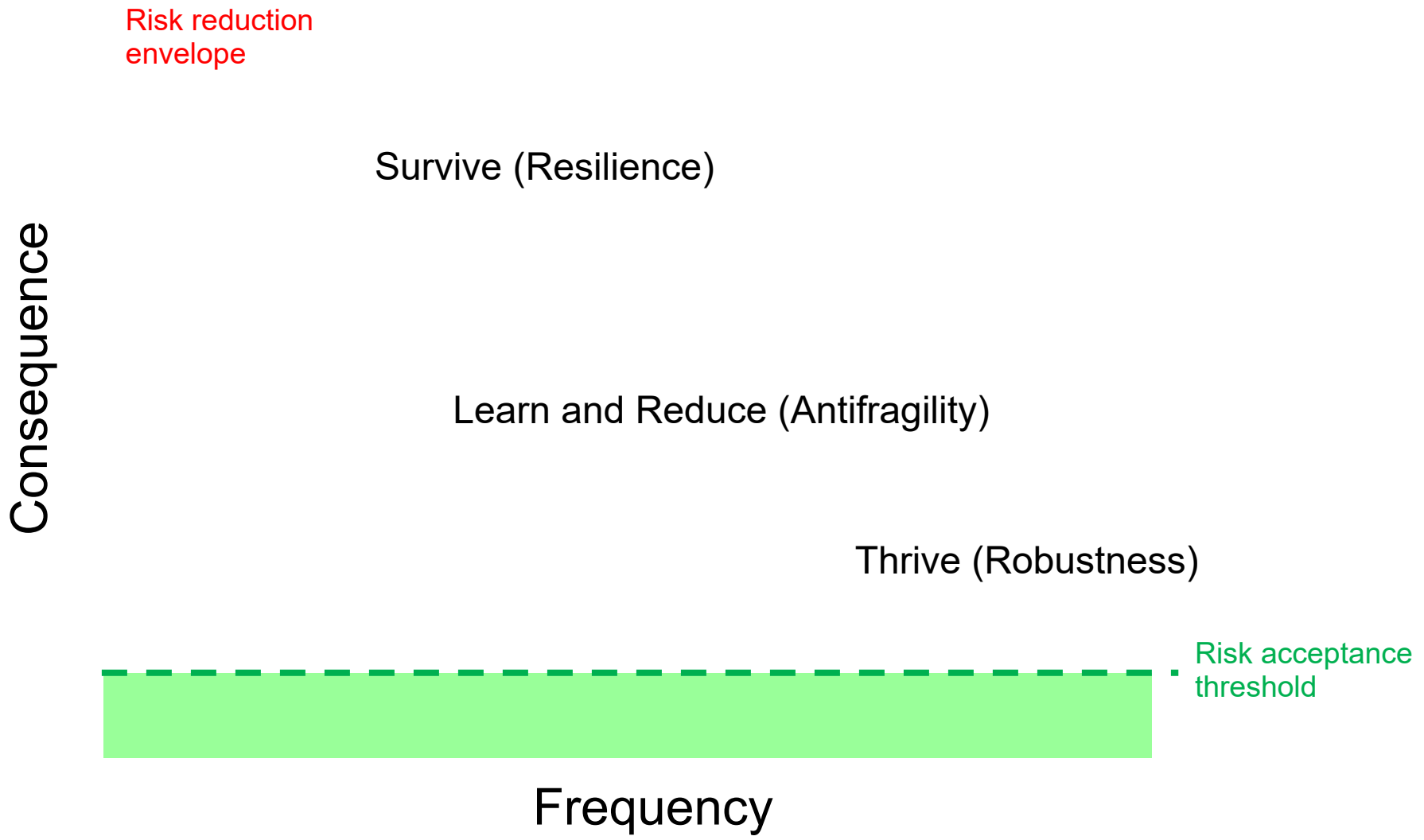
Cyber Harms and Management Approaches



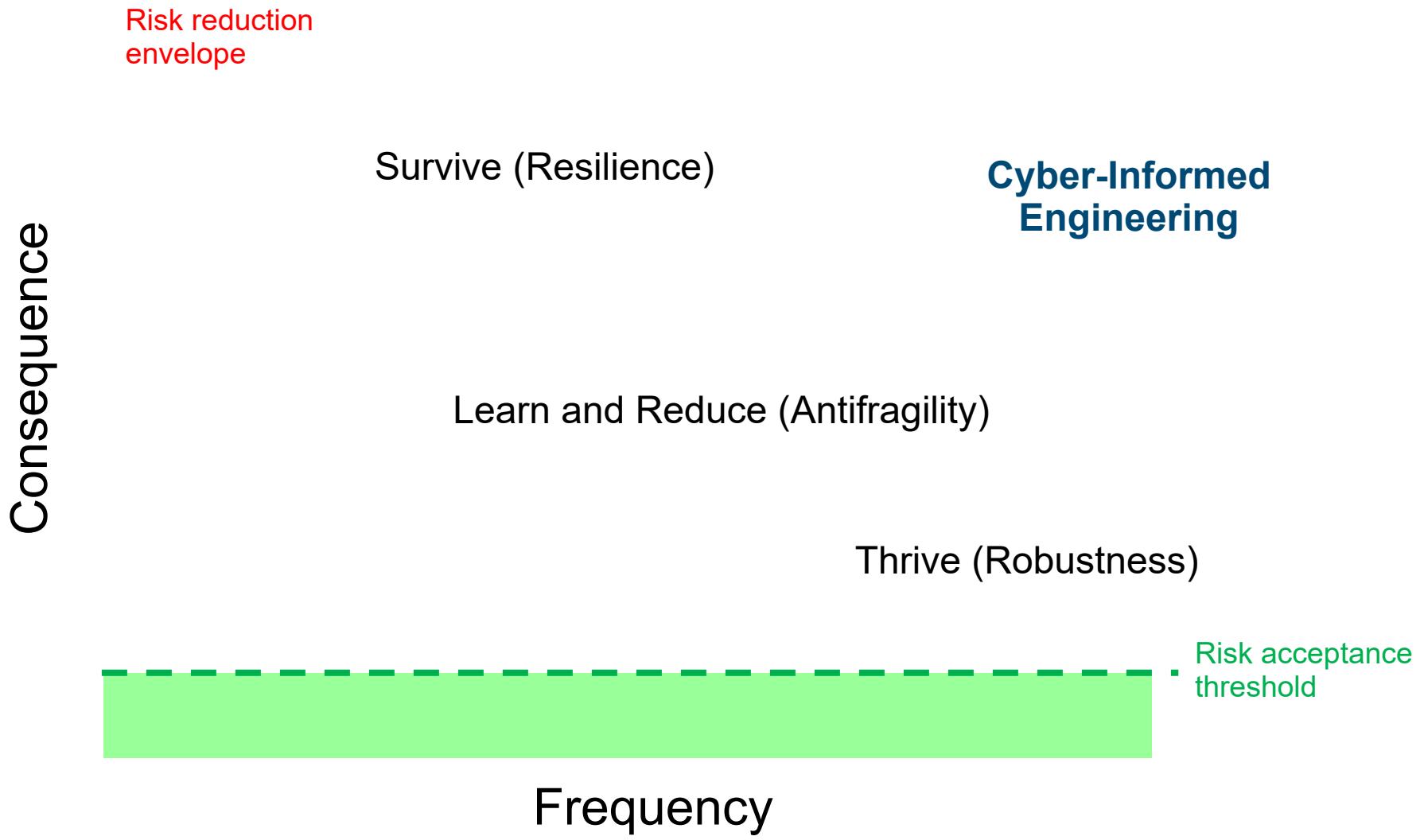
Cyber Harms and Management Approaches



Cyber Harms and Management Approaches

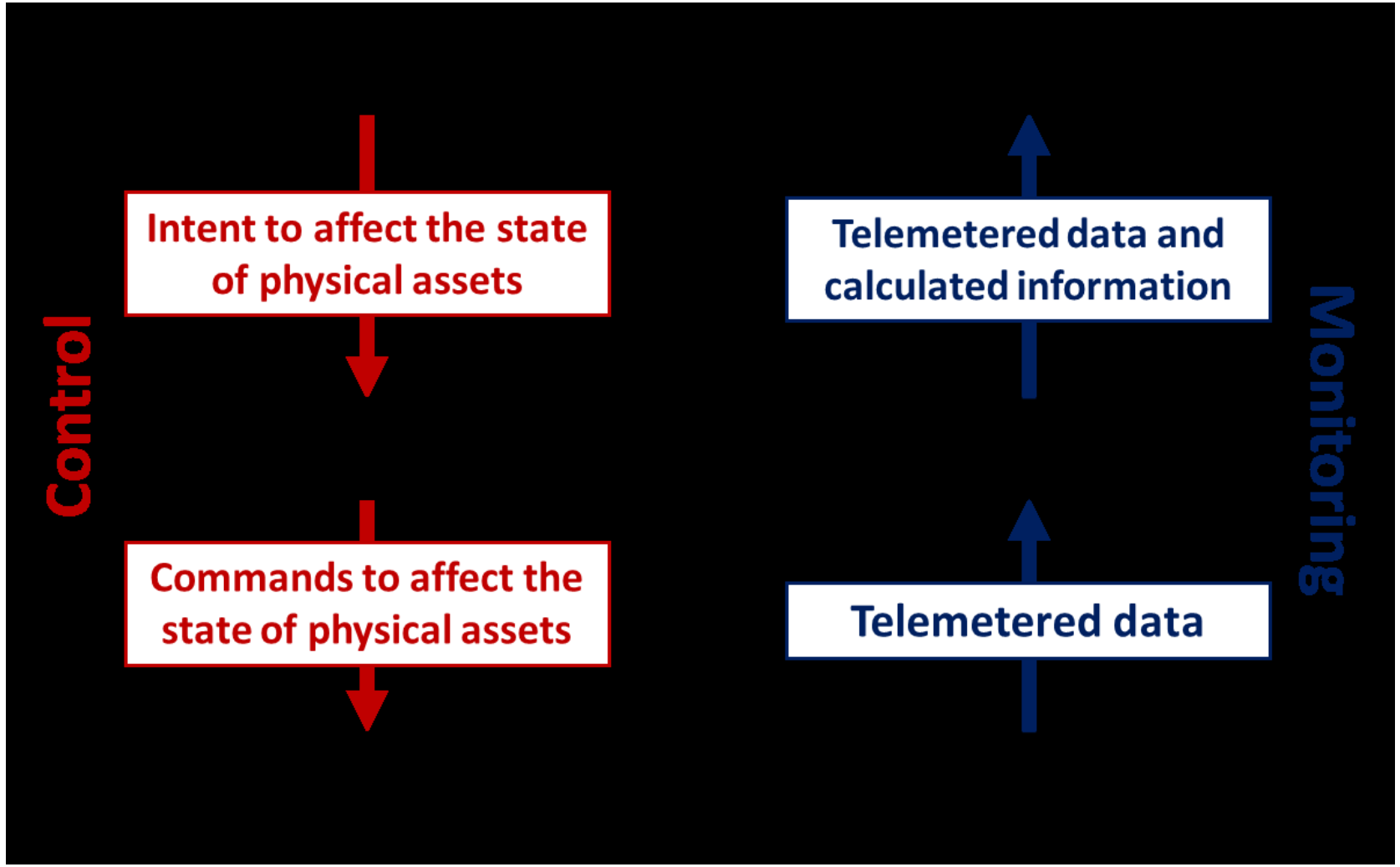


Cyber Harms and Management Approaches



System Operator Concepts

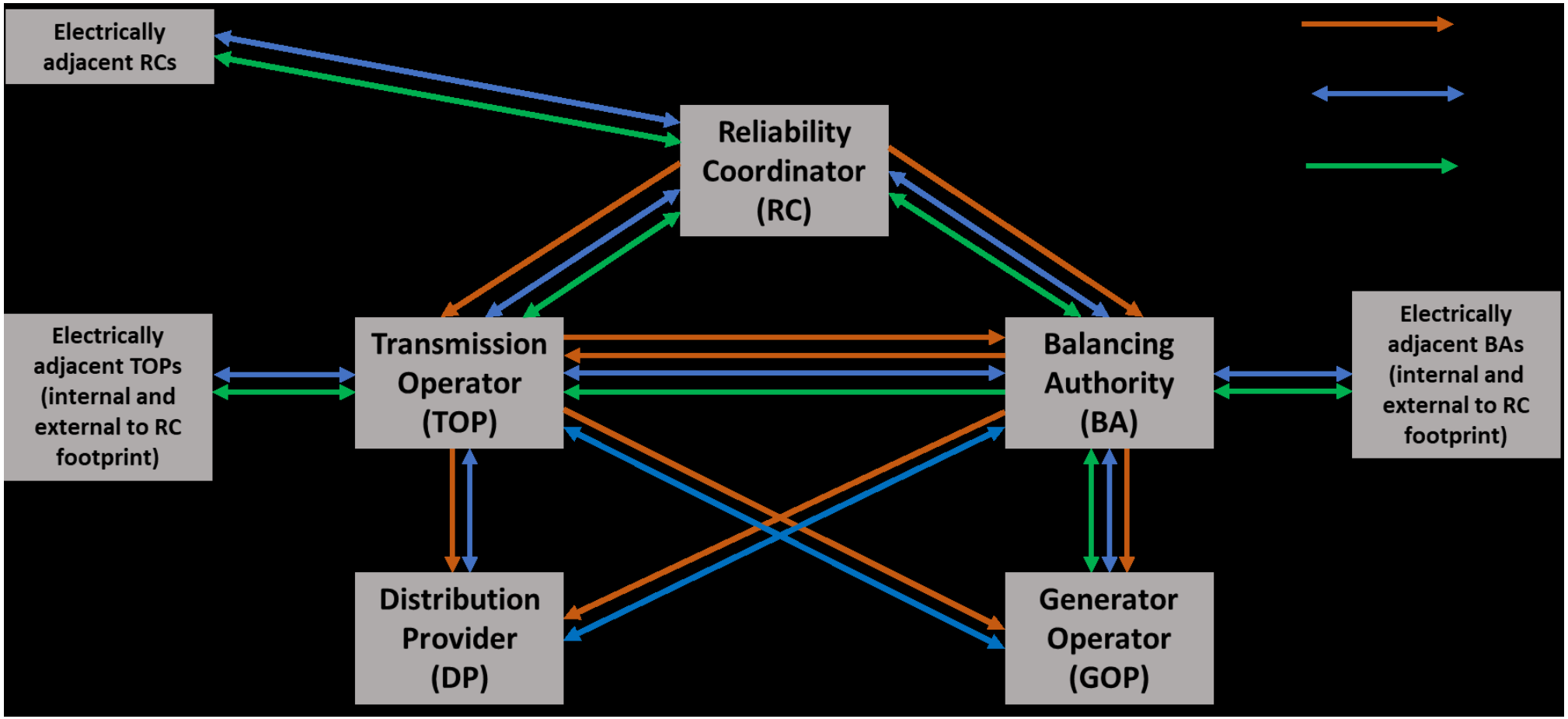
Human-Machine System of Systems



“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

Organizational Team of Teams

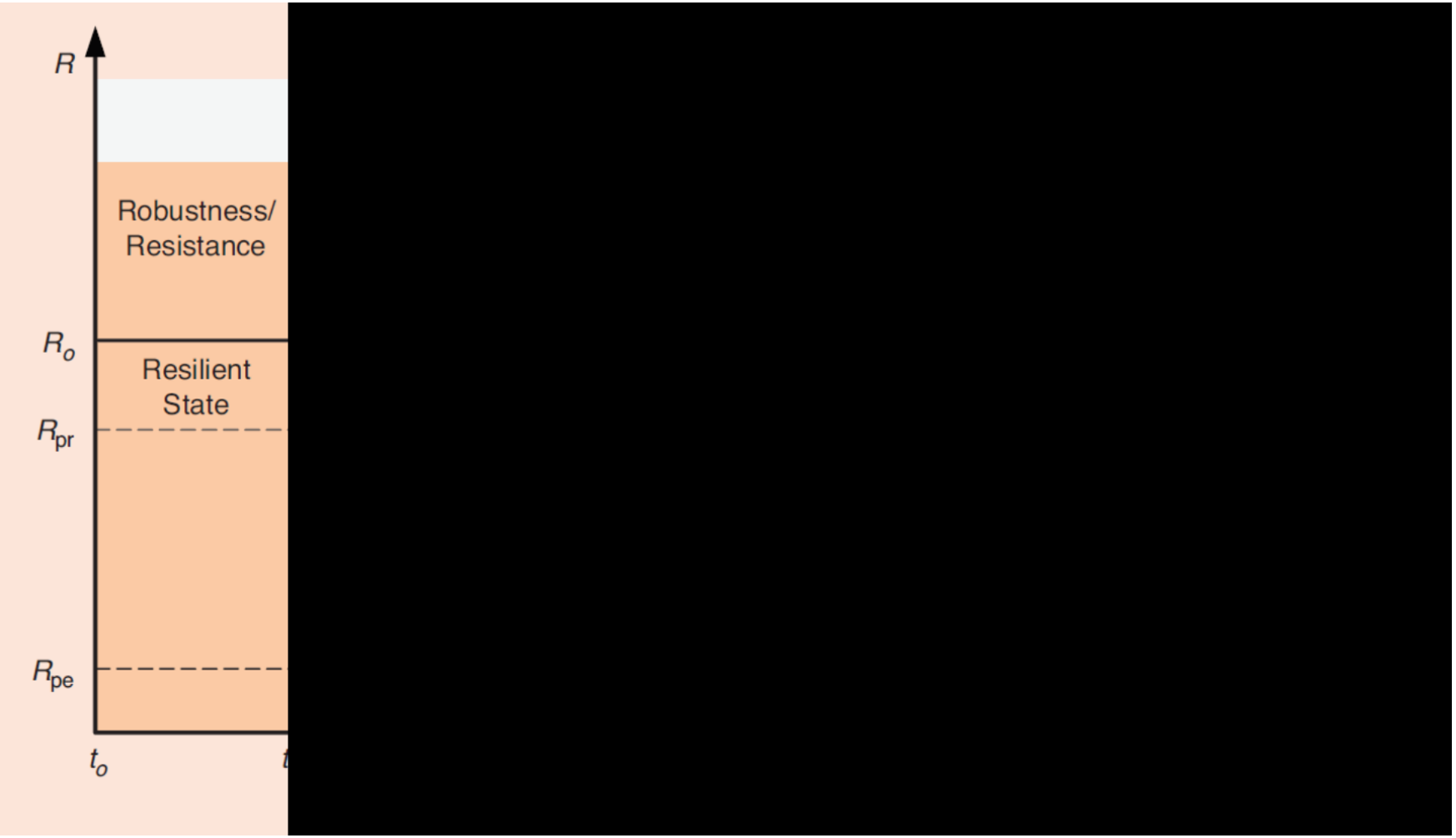


Cybersecurity Opportunities

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	✓

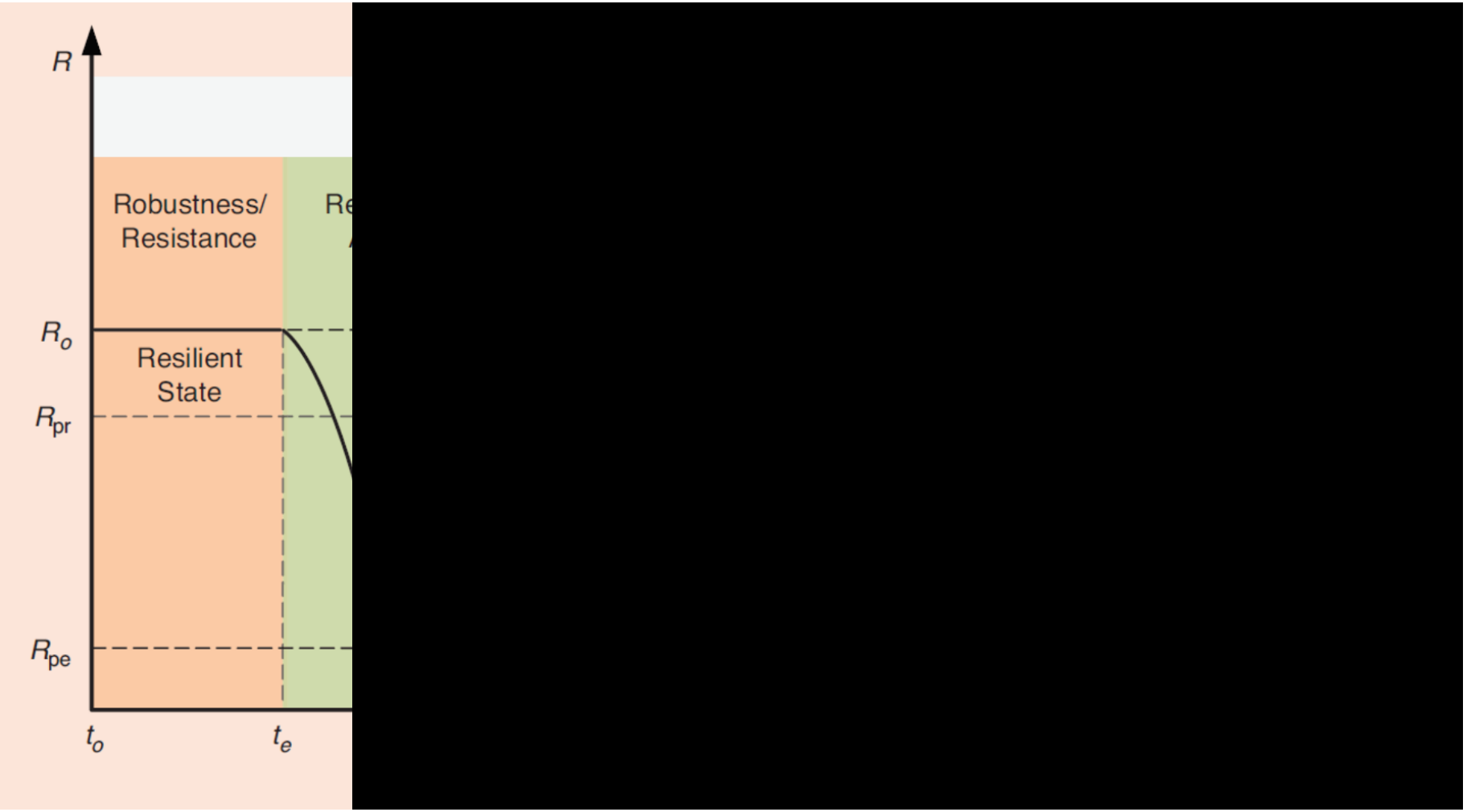
Resilience Event Example

How it plays out in the real world



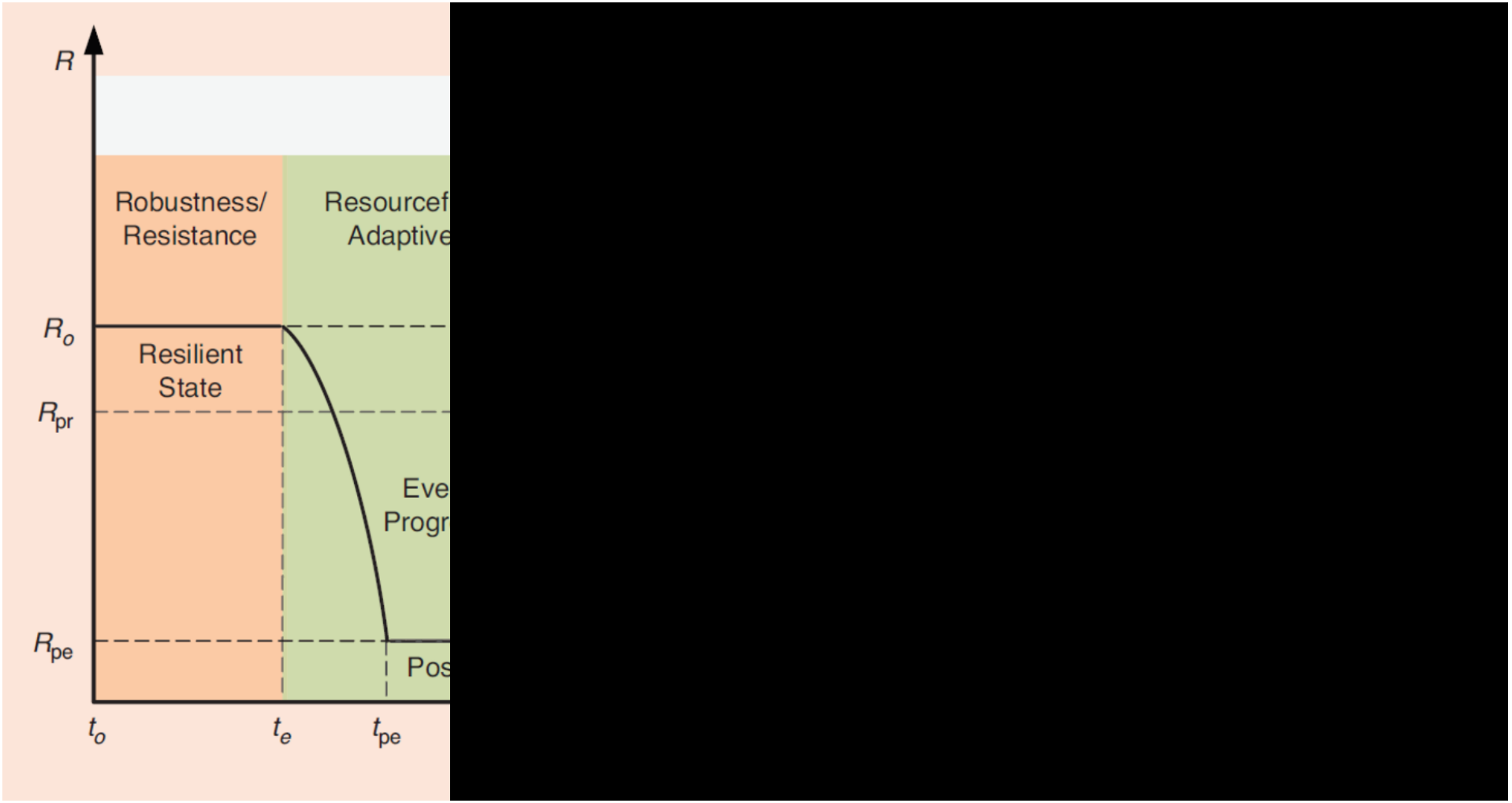
Adapted from Panteli, M., and Mancarella, P., "The grid: Bigger, stronger, better?", I*EEE Power & Energy Magazine*, May-June 2015

How it plays out in the real world



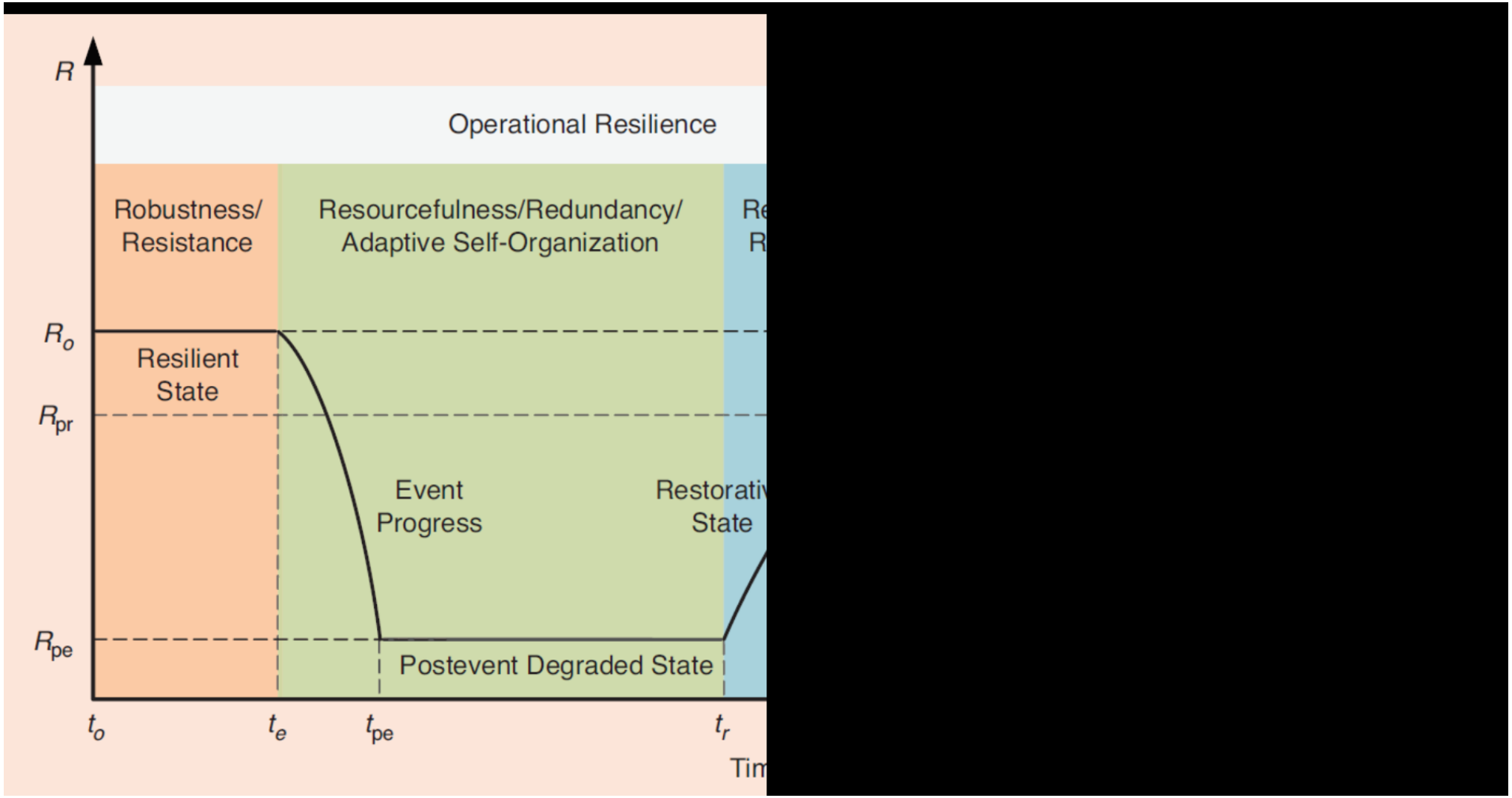
Adapted from Panteli, M., and Mancarella, P., "The grid: Bigger, stronger, better?", I*EEE Power & Energy Magazine*, May-June 2015

How it plays out in the real world



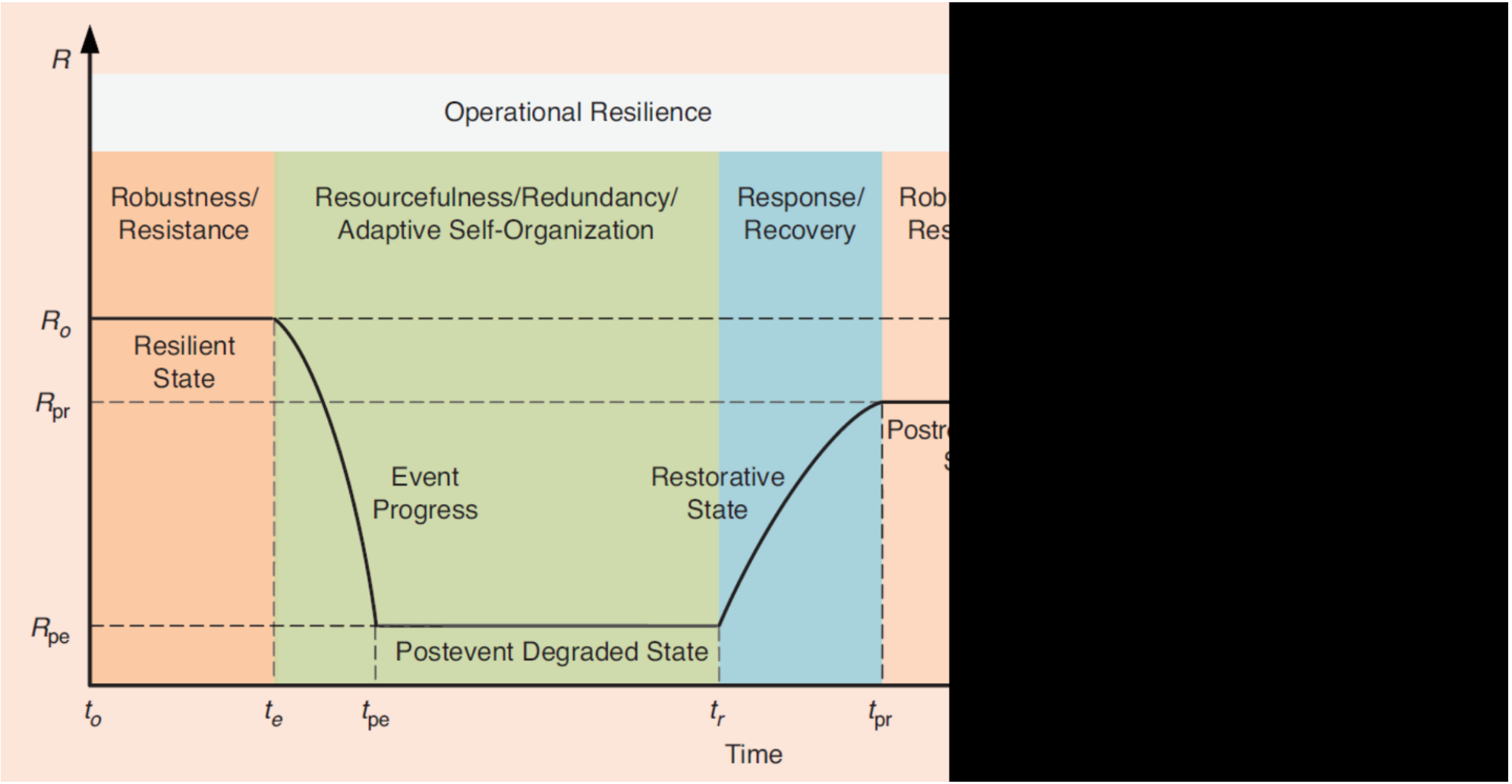
Adapted from Panteli, M., and Mancarella, P., "The grid: Bigger, stronger, better?", I*EEE Power & Energy Magazine*, May-June 2015

How it plays out in the real world



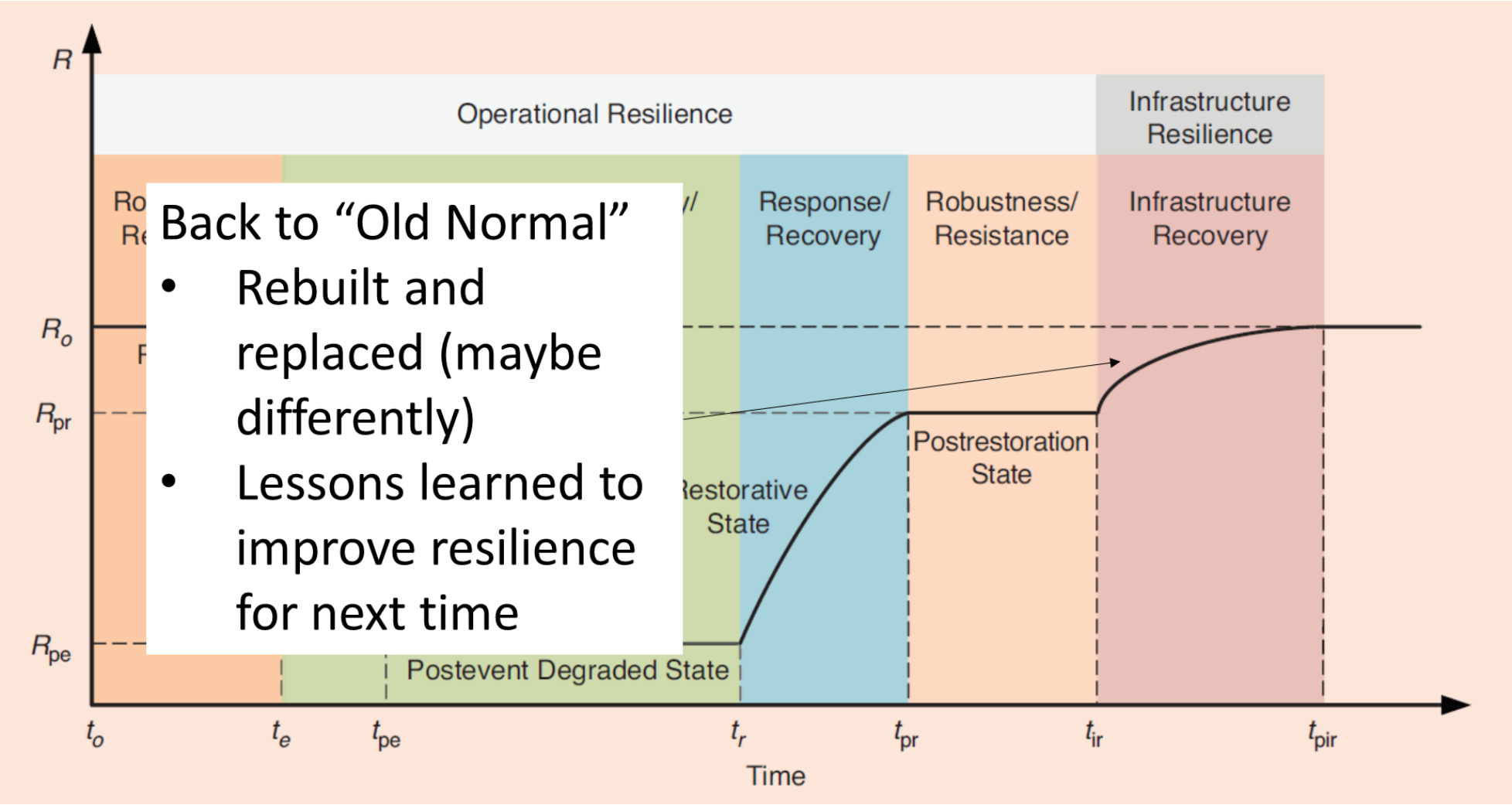
Adapted from Panteli, M., and Mancarella, P., "The grid: Bigger, stronger, better?", I*EEE Power & Energy Magazine*, May-June 2015

How it plays out in the real world



Adapted from Panteli, M., and Mancarella, P., "The grid: Bigger, stronger, better?", I*EEE Power & Energy Magazine*, May-June 2015

How it plays out in the real world



Back to "Old Normal"

- Rebuilt and replaced (maybe differently)
- Lessons learned to improve resilience for next time

Adapted from Panteli, M., and Mancarella, P., "The grid: Bigger, stronger, better?", *IEEE Power & Energy Magazine*, May-June 2015

Thank You!

samuel.chanoski@inl.gov

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