CYBER RESILIENCE IN THE ERA OF ADVANCED PERSISTENT THREATS

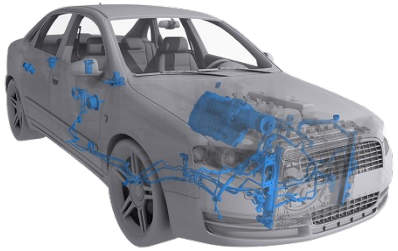
Salam Baniahmed, PhD

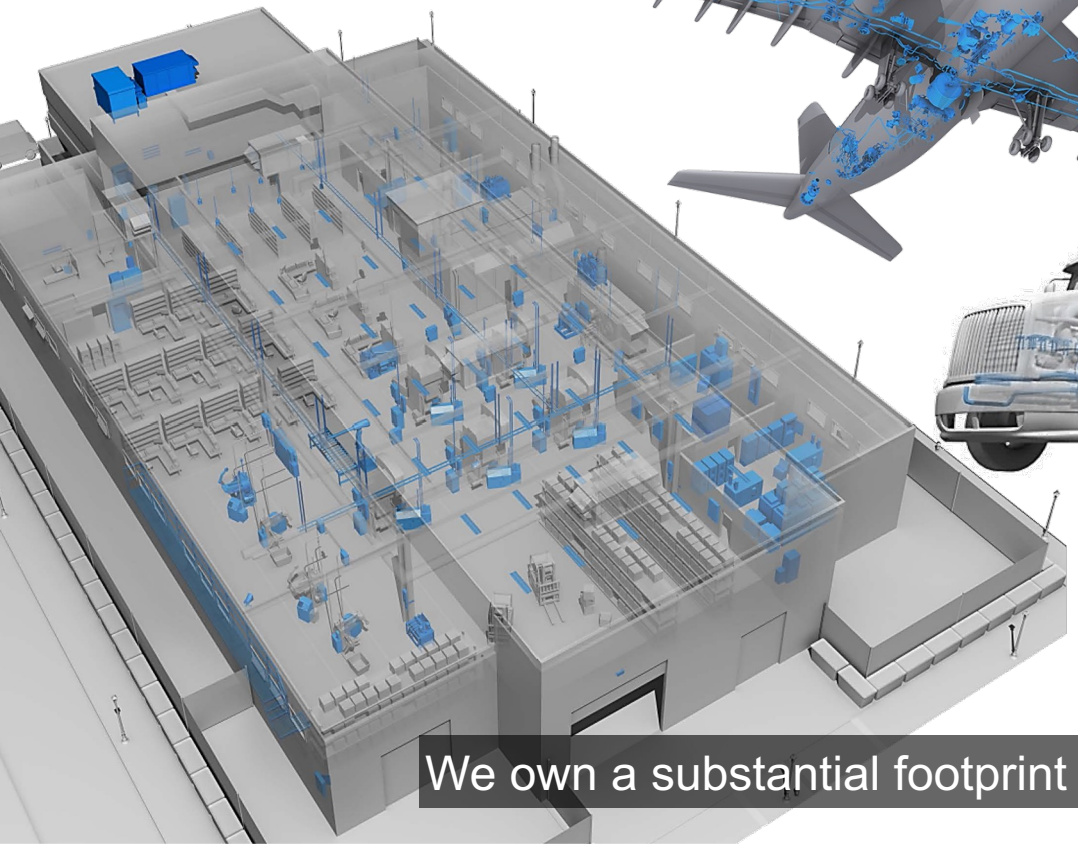
Eaton Research Labs

UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

C2SR CENTER FOR CYBER SECURITY RESEARCH
CARS
DECS

EATON CORPORATION





ELECTRICAL

- Power distribution and circuit protection
- Power quality, backup power and energy storage
- Life safety and security
- Structural solutions
- Control and automation
- Harsh and hazardous environments solutions

INDUSTRIAL

- Aerospace
- Vehicle
- eMobility

We own a substantial footprint of the “power real estate”

University IT

EATON RESEARCH LABS…CORE RESEARCH PLATFORMS

INVESTING IN CORE RESEARCH AREA WITH BROAD, LEVERAGED IMPACT ON FUTURE REVENUE GROWTH

Power Electronics

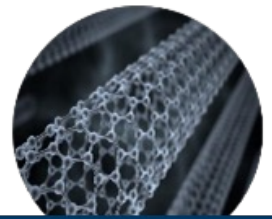
- Drives & Machines
- Solid State Circuit Protection
- Medium Voltage Power Electronics
- More Electric Aircraft
- Vehicle Electrification

Energy Systems

- Distributed Energy Resource Mgt.
- DC Distribution & EVCI
- Grid Intelligence
- Electrification
- PHM & Intelligent Machines

Additive Manufacturing

- Additive Process Dev.
- Rapid Repair



Advanced Materials & Processes

- Polymers & Nanocomposites
- Printed Electronics
- Metallurgy
- Sustainable Materials

Digital Design

- Engineering Automation
- Engineering Info. Mgt.

Themes

Symbiotic

ERL is engaged in developing strategic research platforms impacting future Eaton revenues on a time horizon of 3-5 years utilizing Eaton seed investment leveraged to US Govt investment

University IT

ENERGY SYSTEMS (ES) ENABLES SOLUTIONS TO THE CHALLENGES OF MEGATRENDS

Limited resources: each person uses up to 57 kg/day of minerals to produce energy

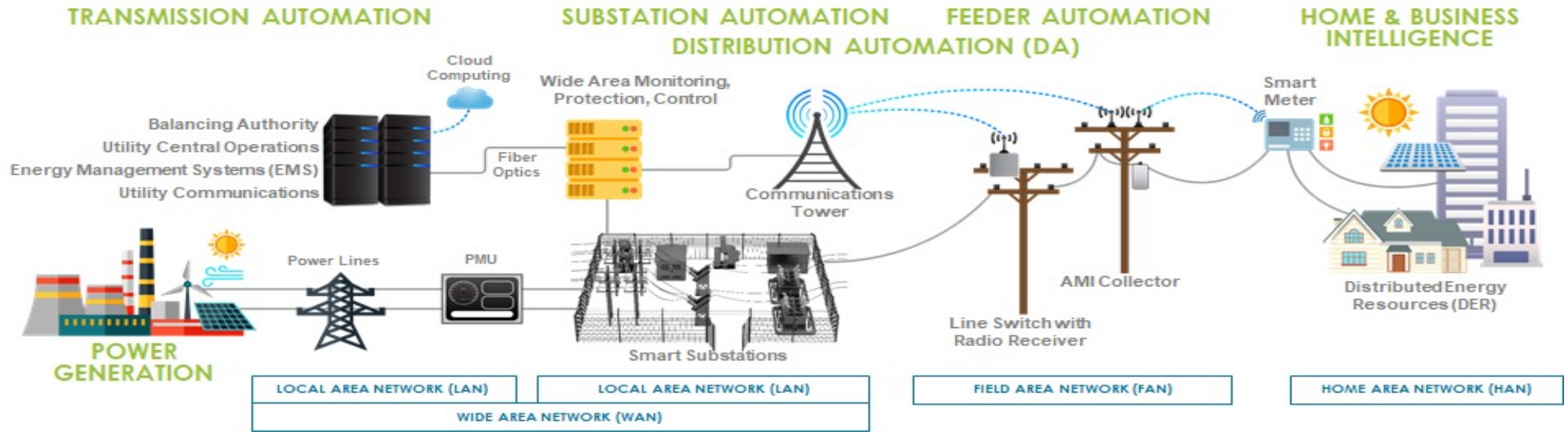
CO2 emission reduction: 50-52% reduction in U.S. from 2005 level in 2030

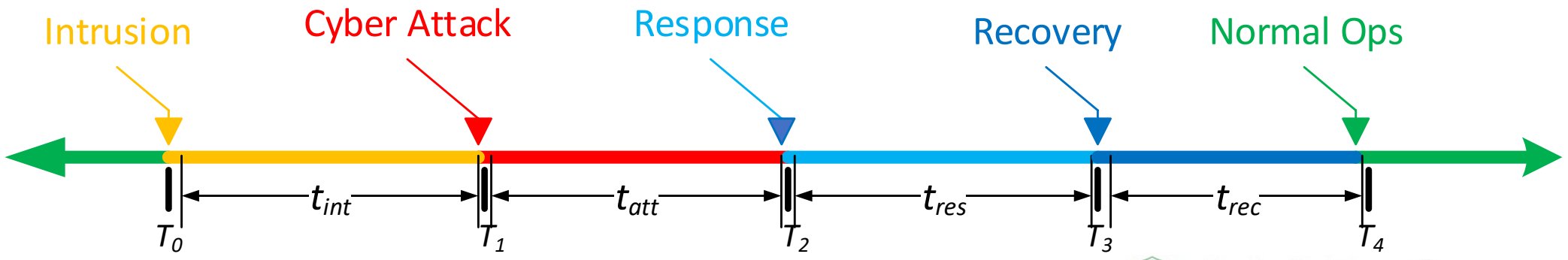
Population growth: 13% from 2010 to 2021

Mega cities: 62.5% of the world's population is forecasted to live in cities in the year of 2050.

Energy Systems provides solutions to challenges of megatrends by enabling renewable integration, electrification, grid resiliency and energy management.

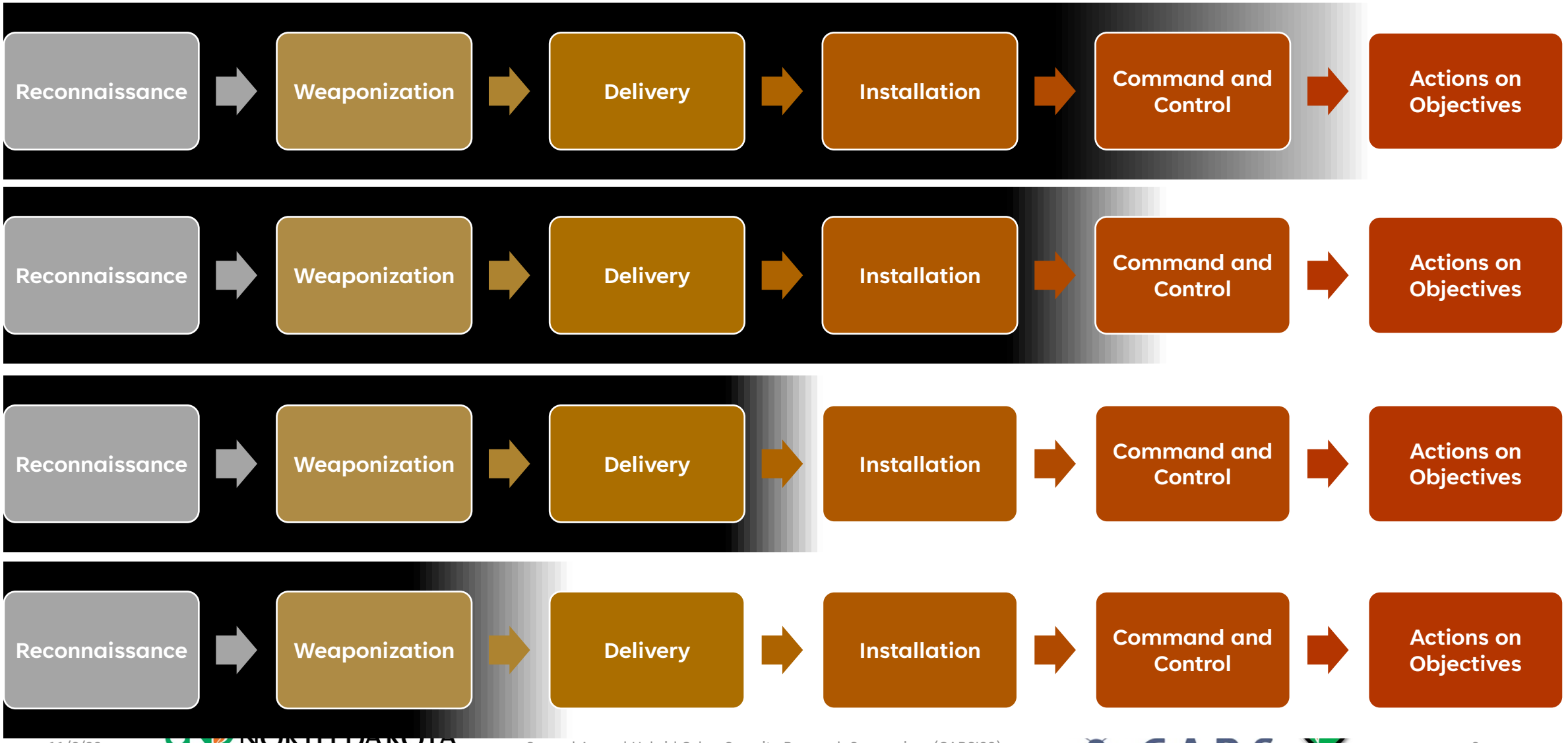
INTRODUCTION



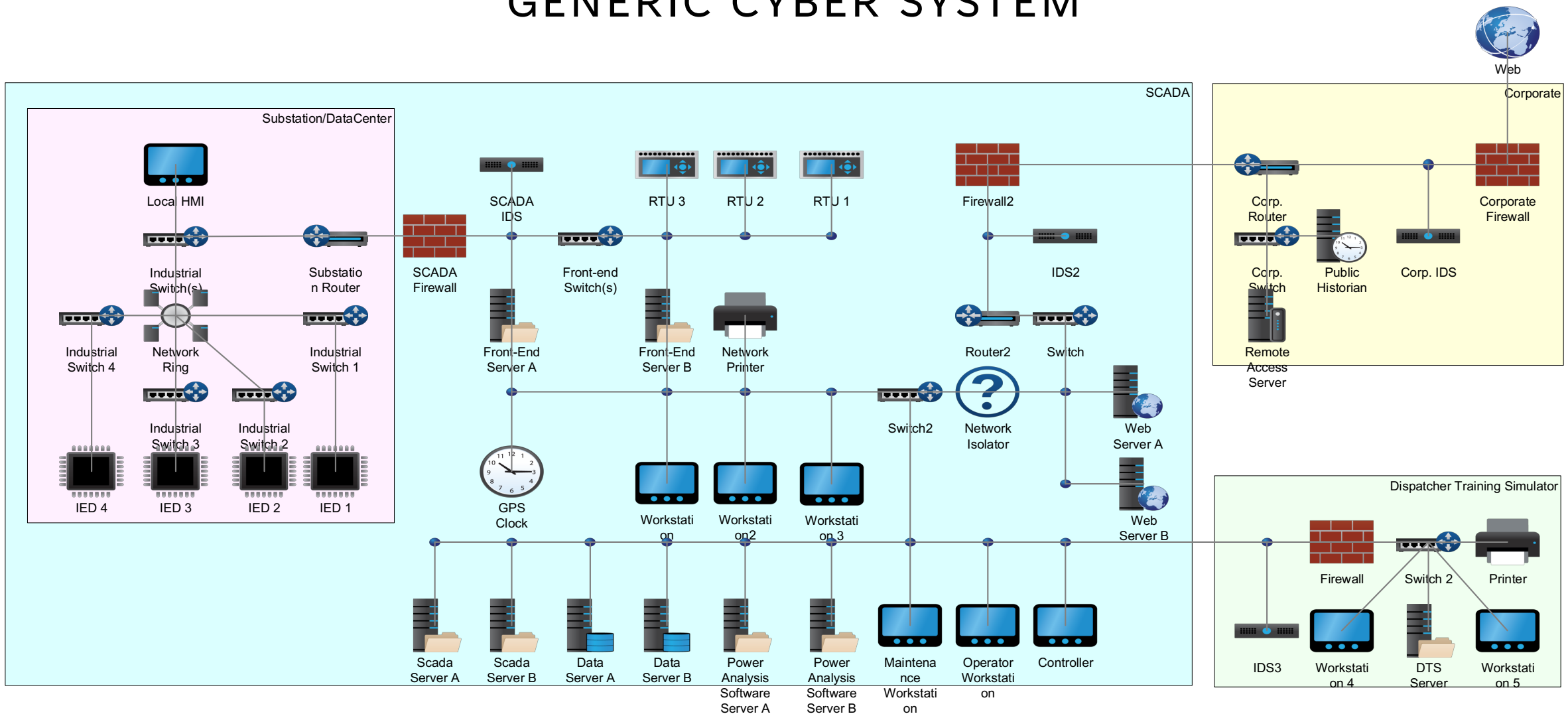


University IT

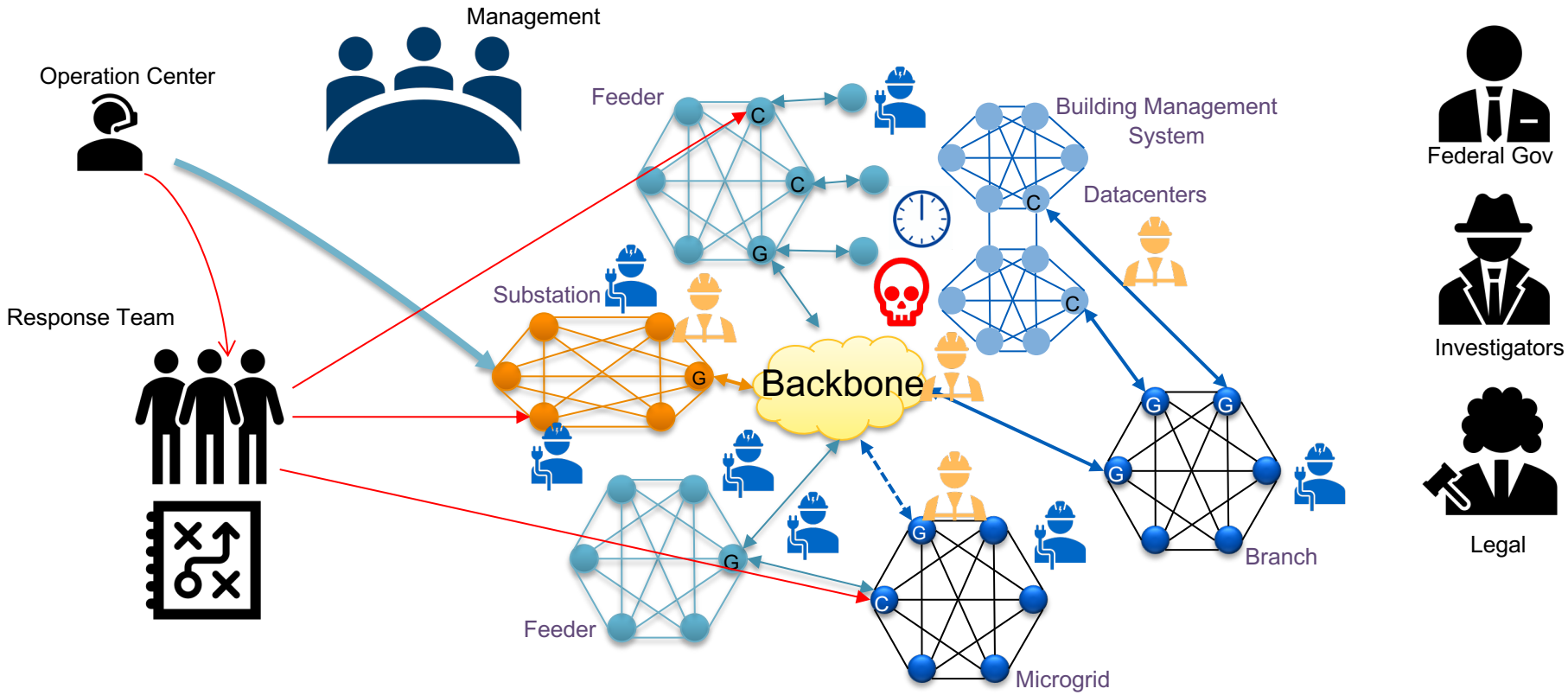
CYBER KILL CHAIN – GENERAL



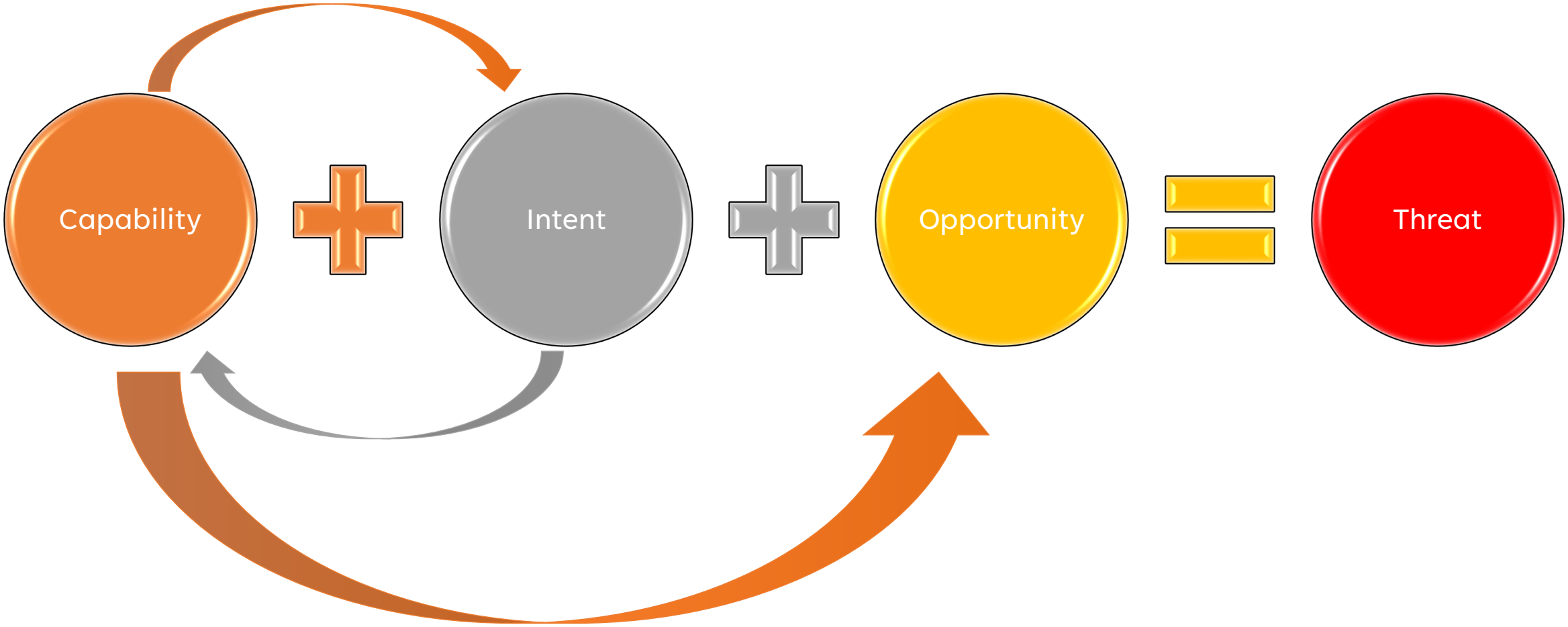
GENERIC CYBER SYSTEM



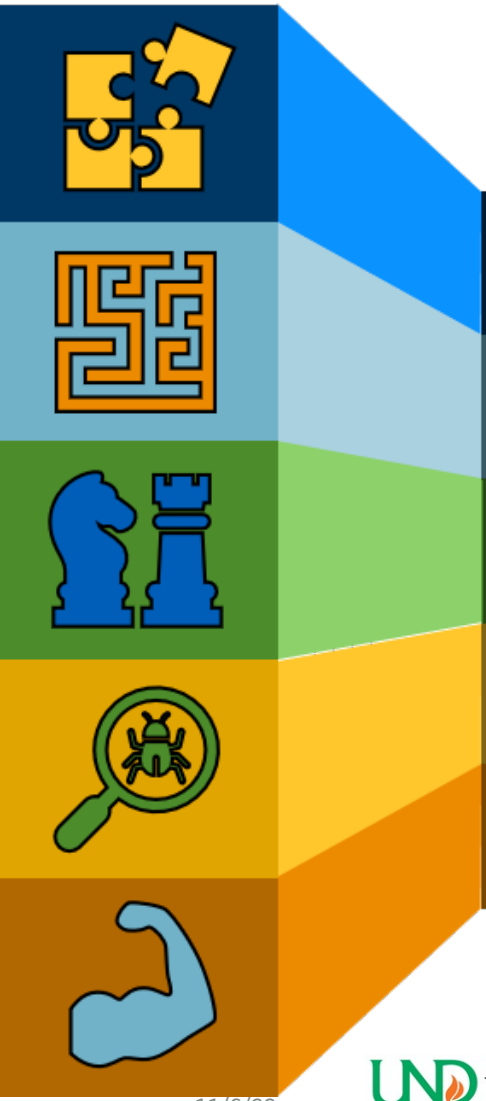
CYBER INCIDENT STAKEHOLDERS



HOW **“NOT”** TO MEASURE THREAT!



SECURE DESIGN PRINCIPLES



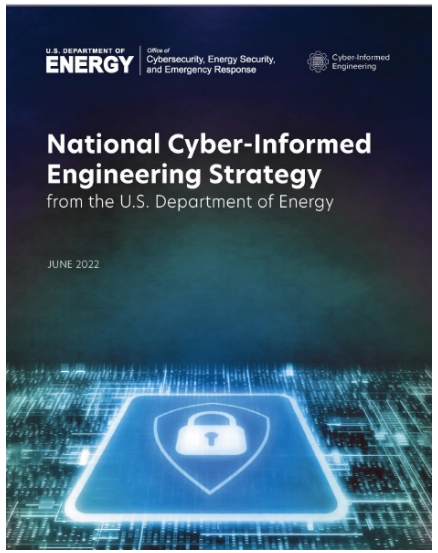
Establish the context	Determine *all* the elements which compose your system, so your defensive measures will have no blind spots.
Making compromise difficult	An attacker can only target the parts of a system they can reach. Make your system as difficult to penetrate as possible
Making disruption difficult	Design a system that is resilient to denial of service attacks and usage spikes
Making compromise detection easier	Design your system so you can spot suspicious activity as it happens and take necessary action
Reducing the impact of compromise	If an attacker succeeds in gaining a foothold, they will then move to exploit your system. Make this as difficult as possible

https://www.ncsc.gov.uk/

SECURITY VS RESILIENCY

University IT

NATIONAL CYBER-INFORMED ENGINEERING STRATEGY



Vulnerabilities may not be captured at the design stage.

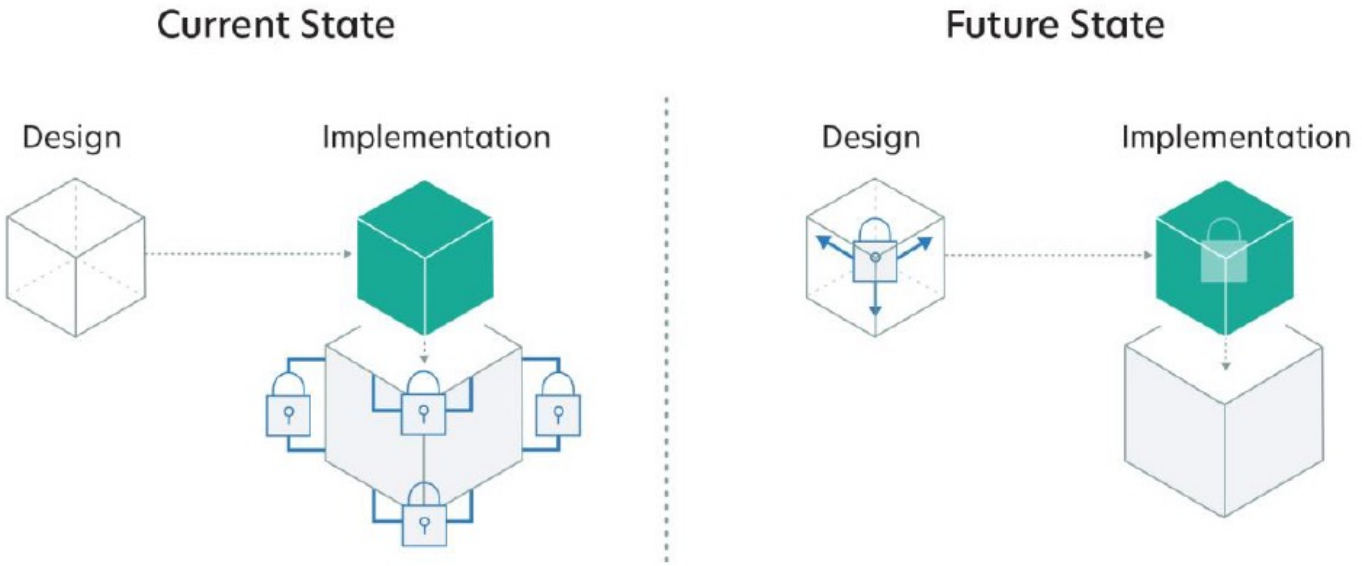


*Figure by: The U.S. Department of Energy's (DOE) National Cyber-Informed Engineering (CIE) Strategy Document https://www.energy.gov/ceser/articles/us-department-energys-doe-national-cyber-informed-engineering-cie-strategy-document

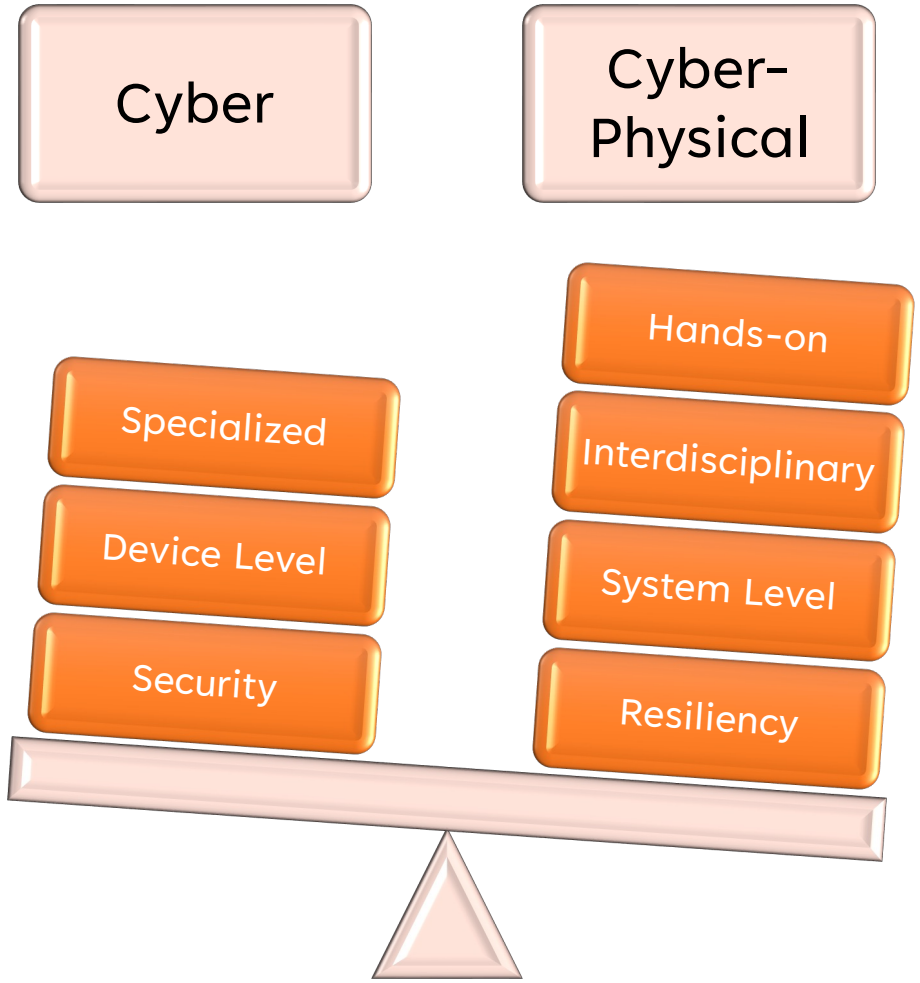
"Planned resilience with no assumed security— Expect that any digital component or system may be compromised at some point during its lifecycle, and plan for continued operation during and after a cyber attack that degrades digital controls. Implement a zero-trust architecture to the greatest degree possible."*

University IT C2SR CENTER FOR CYBER SECURITY RESEARCH CARS DECS

RESEARCH EFFORTS ON CYBER RESILIENCY

- Change in perspectives.
- Research & Development on automating incident response management.
- Goal:
  - Speed up incident response (minimize the human factor).
  - Improve forensics data preservation at the OT level (black box).
  - Seamless cyber-physical restoration (including cyber hygiene).

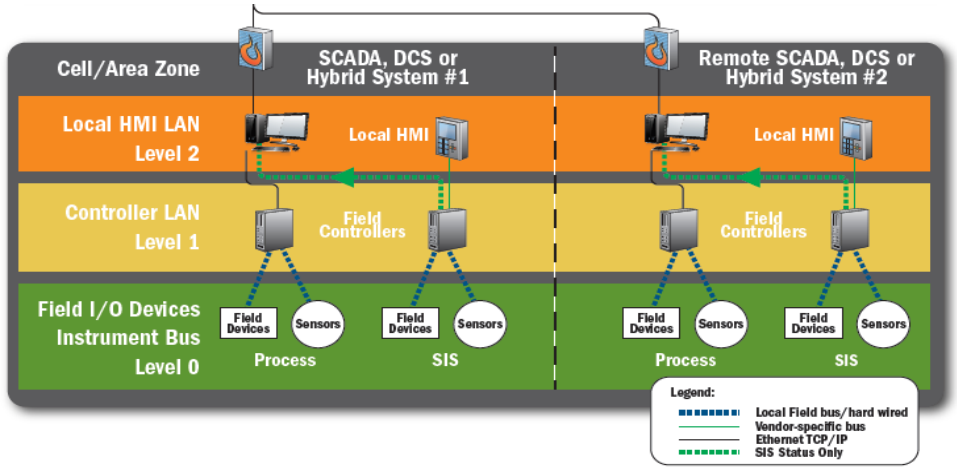
NIST 800-16 V2

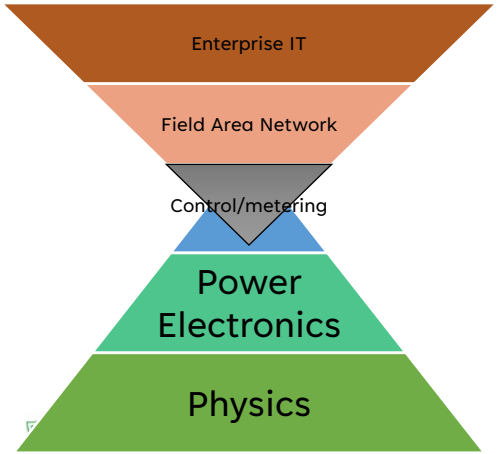


University IT C2SR CENTER FOR CYBER SECURITY RESEARCH CARS DECS

RESEARCH EFFORTS ON CYBER RESILIENCY

- More PE penetration in Energy Systems supports cyber resiliency functions.
- Cybersecurity market is trending towards Cyber-Physical Resiliency.
- Embedded cyber-physical PE device design should consider supporting resiliency functions while maintaining security measures at device and system levels.
- Main functions include Automated incident response, aided recovery, post incident forensics.





University IT

Thank You for Listening!

Salam Baniahmed, PhD
Eaton Research Labs

salamabaniahmed@eaton.com

Salam BaniAhmed
Engineering Specialist, Cyber-Physical Resiliency, Eaton Research Labs. Senior Mem...

https://www.linkedin.com/in/asbani