Living on the Range

Critical infrastructure approach to training ranges

Training for the Fight

ICS Attacks

225k

Ukraine 2015

Three electric utilities attacked through a cyber means resulting in 225k customers out of power

200 MW

Ukraine 2016

Electric transmission substation attacked through a cyber means

SIS

Middle East Facility 2017

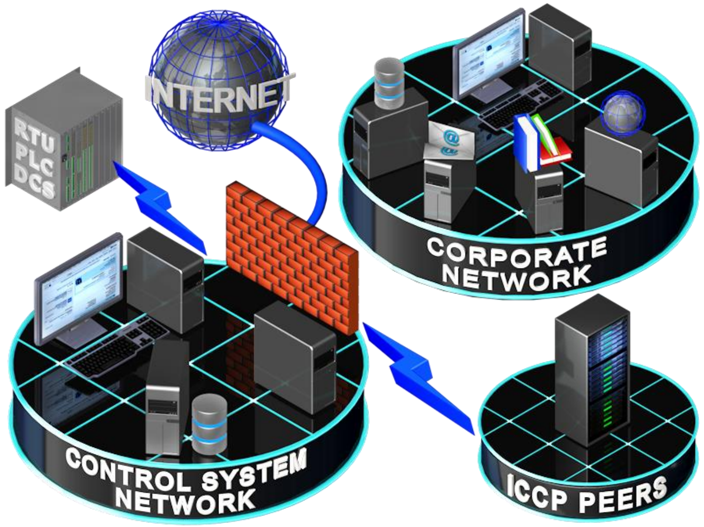
Safety Instrumented System, targeted and impacted

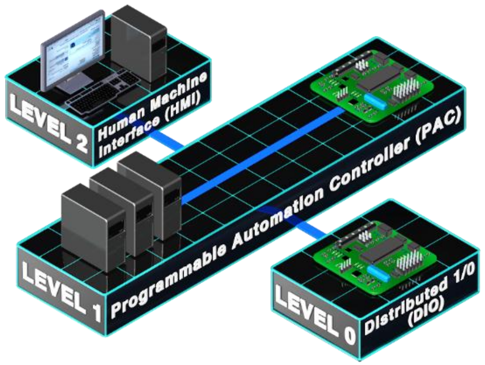
?

Combination

Safety or protection system manipulation followed by intentional control system misuse to cause equipment damage and human health and safety impact

Operational Environment Silos of Excellence




LEVEL 2 Human Machine Interface (HMI)
LEVEL 1 Programmable Automation Controller (PAC)
LEVEL 0 Distributed I/O (DIO)

Learn from Operations

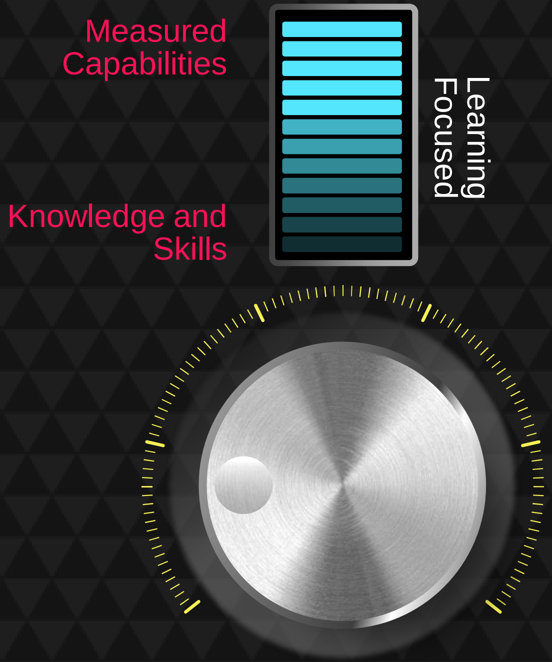
- Training
- Planning and Analysis
- Load Shed
- Emergency Operations
- Blackstart

Work With Operations

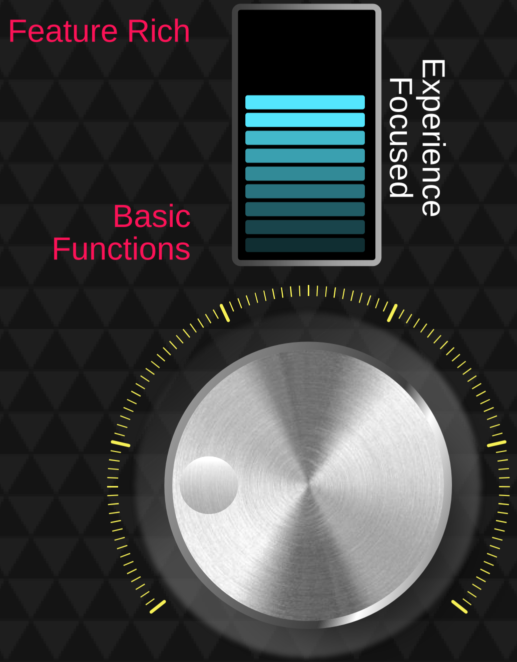
- **Cyber contingency analysis** (continuous analysis and preparing the system for the next event)
- **Cyber failure planning** (modeling and testing cyber system response to network and asset outages)
- **Cyber conservative operations** (Intentionally eliminating planned and unplanned changes, as well as stopping any potentially impactful processes)
- **Cyber load shed** (Eliminating all unnecessary network segments, communications, and cyber assets that are not operationally necessary)
- **Cyber RCA** (Root Cause Analysis forensics to determine how an impactful event occurred and ensure it is contained)
- **Cyber blackstart** (cyber asset base configurations and bare metal build capability to restore the cyber system to a critical service state)
- **Cyber mutual aid** (ability to utilize ISACs, peer utilities, law enforcement and intelligence agencies, as well as contractors and vendors to respond to large scale events)

Operationalize your cyber defense and response approach

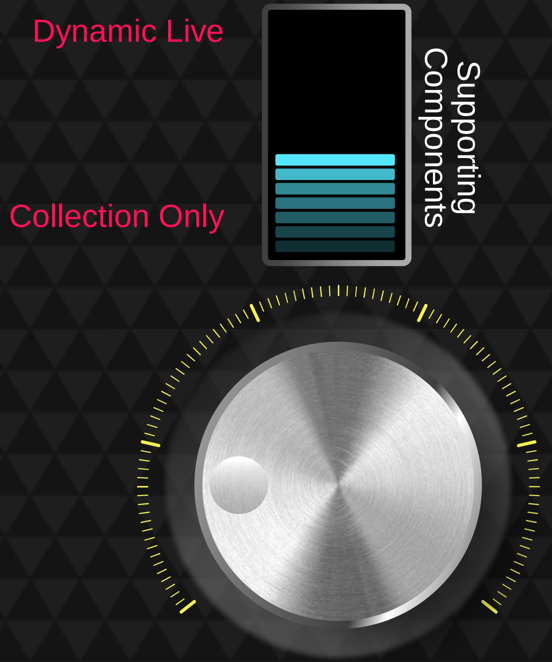
Where to Invest



Content Focused Learning Objectives

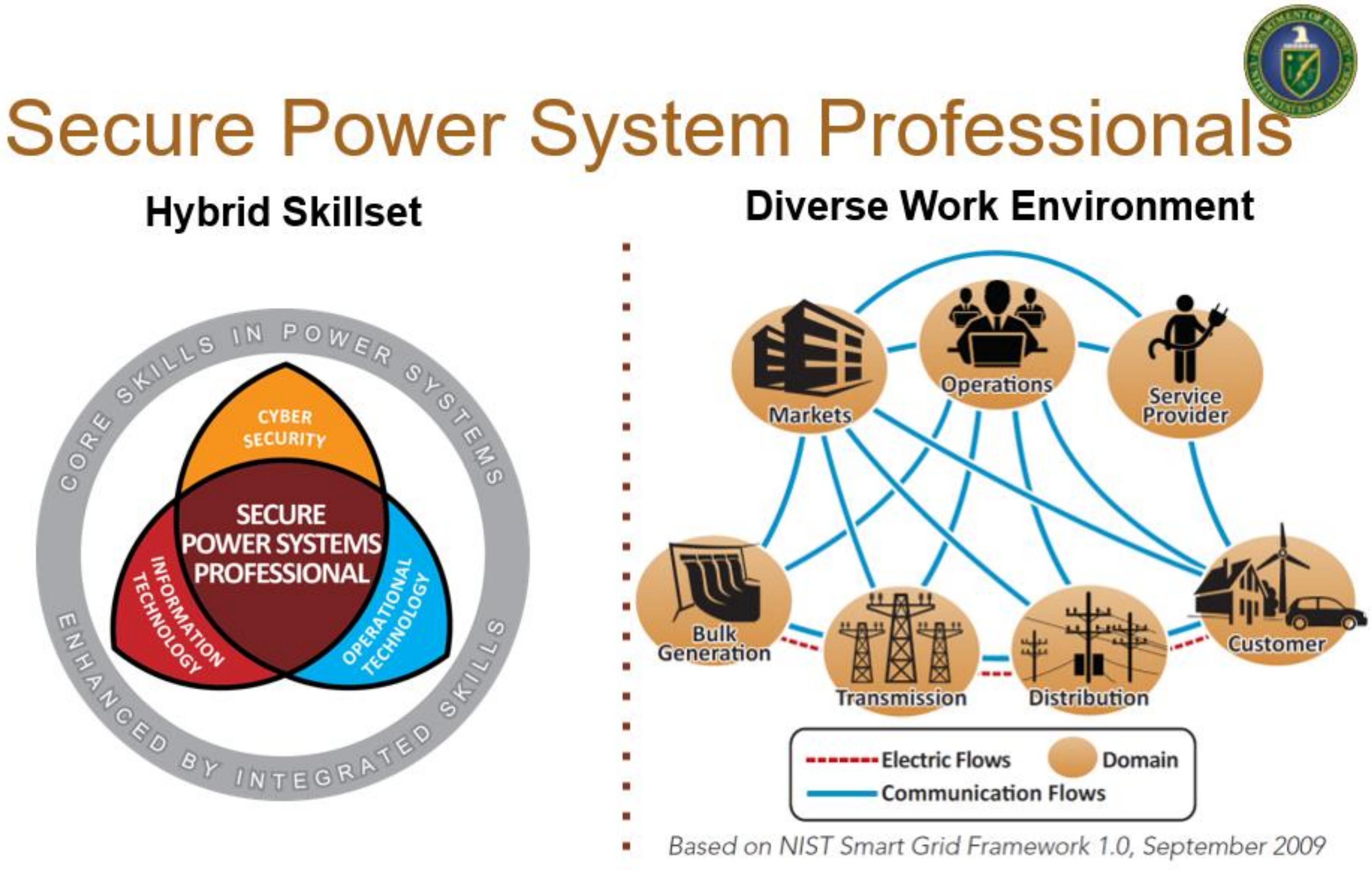


Authoring and Delivery Platform



Infrastructure and Artifacts

Skillset Mix



Secure Power System Professionals

Hybrid Skillset

Diverse Work Environment

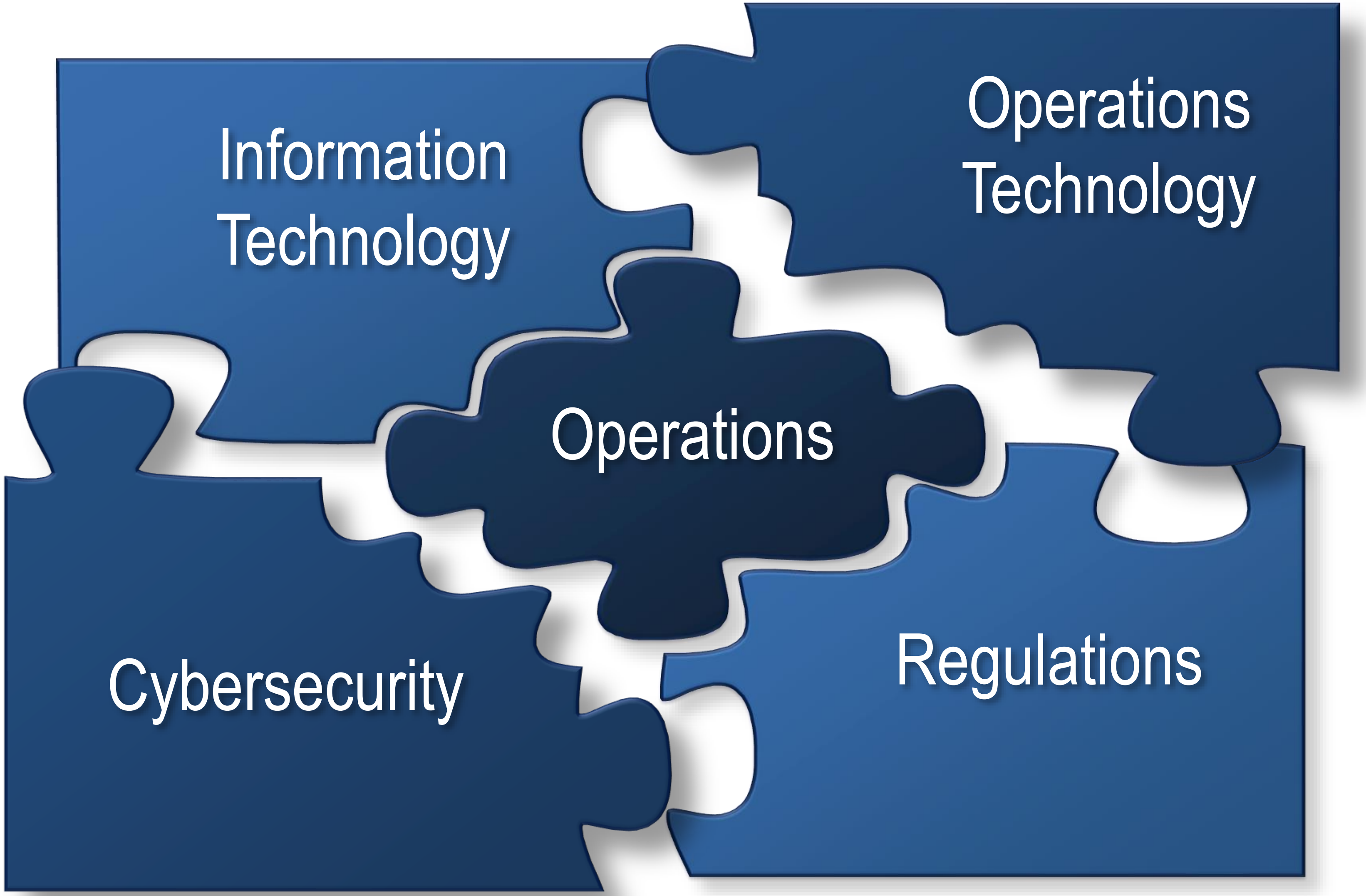
Based on NIST Smart Grid Framework 1.0, September 2009

What We Need

Unicorns

Yeti’s

Making Yeti-Corns



ICS 612 Approach

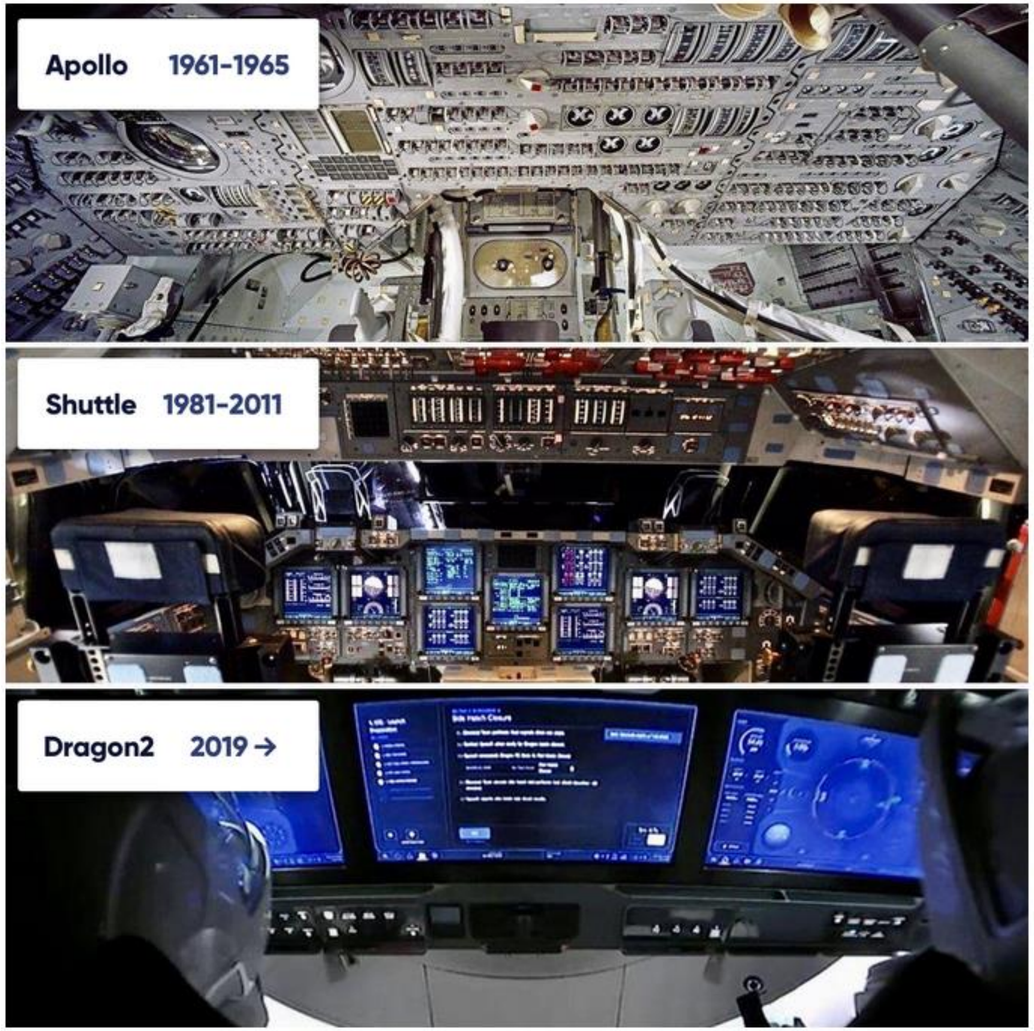


Image Ref: https://uxdesign.cc/

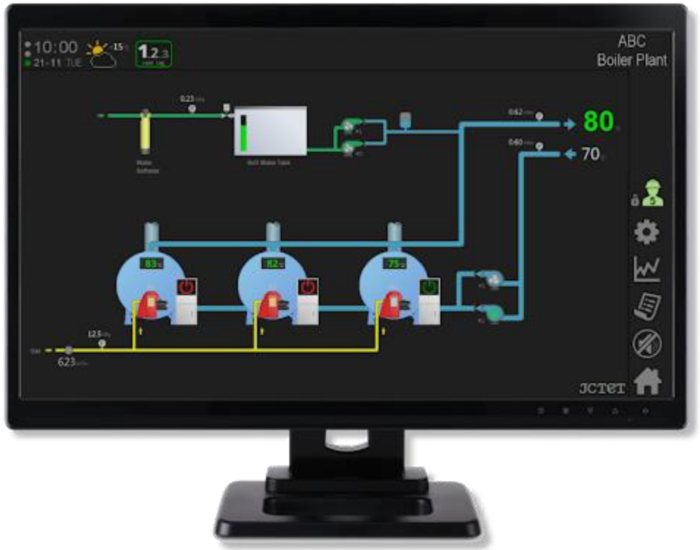
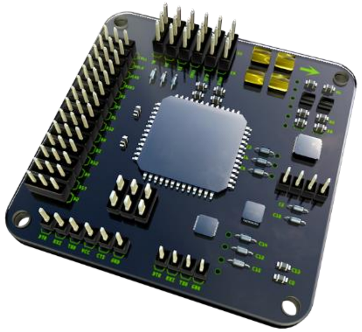


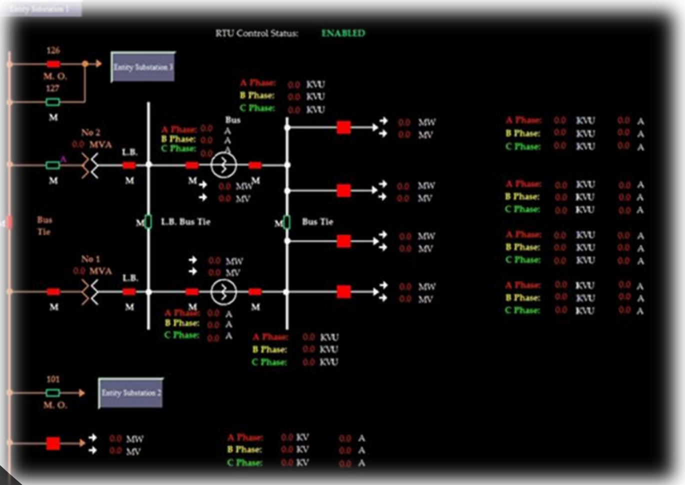
Image Ref: http://www.jctet.com

In Class Range – Individual Learner

- Day 1 – Local Process
- Day 2 – System of Systems
- Day 3 – ICS Network Management
- Day 4 – ICS Systems Management
- Day 5 – Process Down

https://vimeo.com/386099502

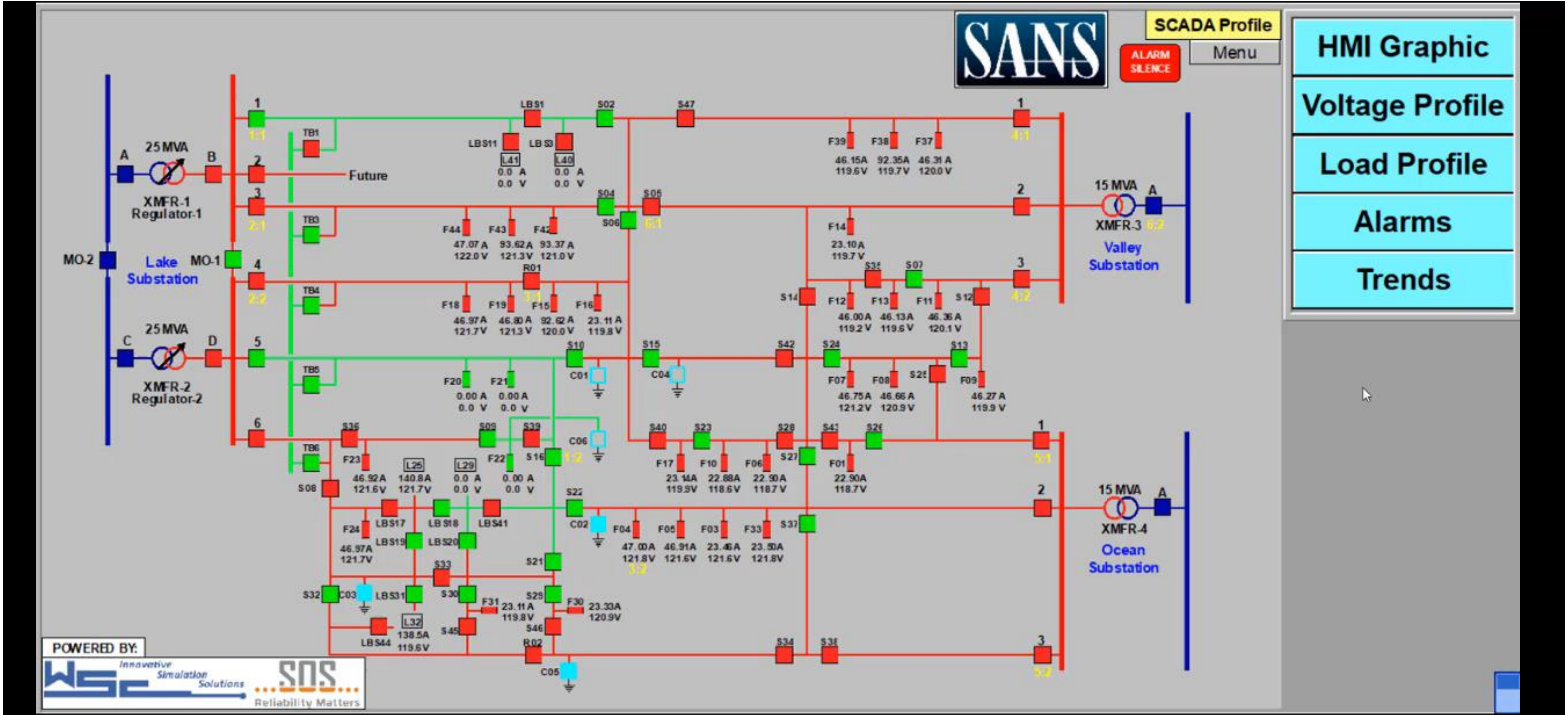


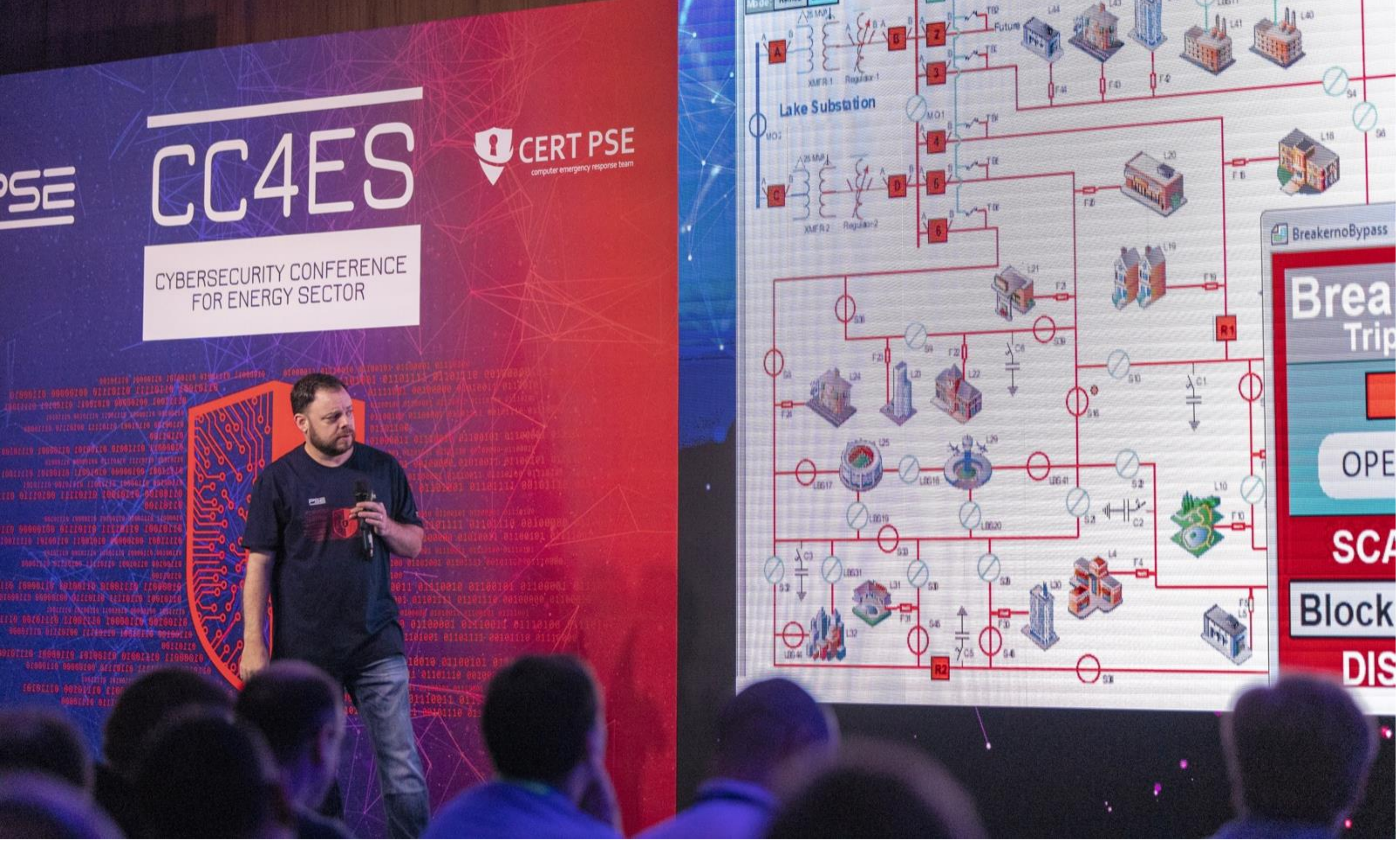


RTU Control Status: ENABLED

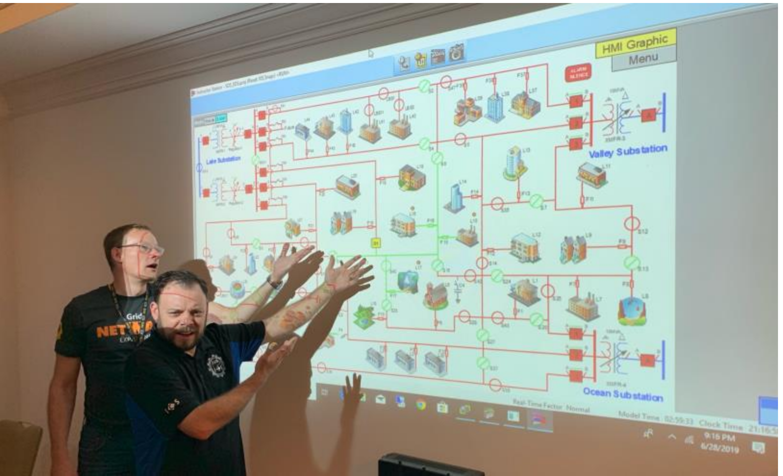
sans.org/netwars/grid

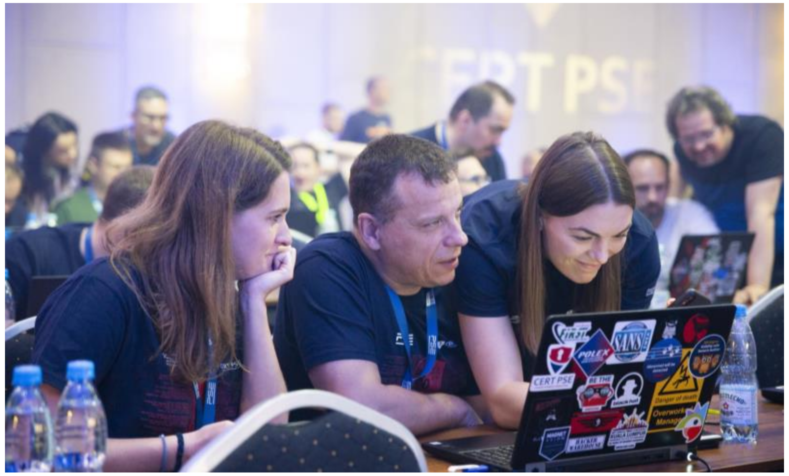
Cyber to Physical - Operationalized Cyber Training Range




PSE
CC4ES
CYBERSECURITY CONFERENCE FOR ENERGY SECTOR
CERT PSE
computer emergency response team
Lake Substation
BreakernoBypass

GRID
NETWARS


HMI Graphic
Menu
Lake Substation
Valley Substation
Ocean Substation


CERT PSE

CONTACT INFORMATION

Thank You for Joining!

CONTACT
Tim Conway
tconway@sans.org

I will join Phil in the Slack virtual hallway

ICS RESOURCES
https://ics.sans.org
https://ics-community.sans.org/
Twitter: @sansics