Sandia National Laboratories

Exceptional service in the national interest

SANDIA NATIONAL LABORATORIES

Cyber-Physical Mission Capabilities

Dr. Meghan Sahakian

Sandia National Laboratories

2024 Pacific Operational Science & Technology (POST) Conference

March 4-7, 2024

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

SAND2024-02123C

SANDIA IS A FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTER (FFRDC) MANAGED AND OPERATED BY

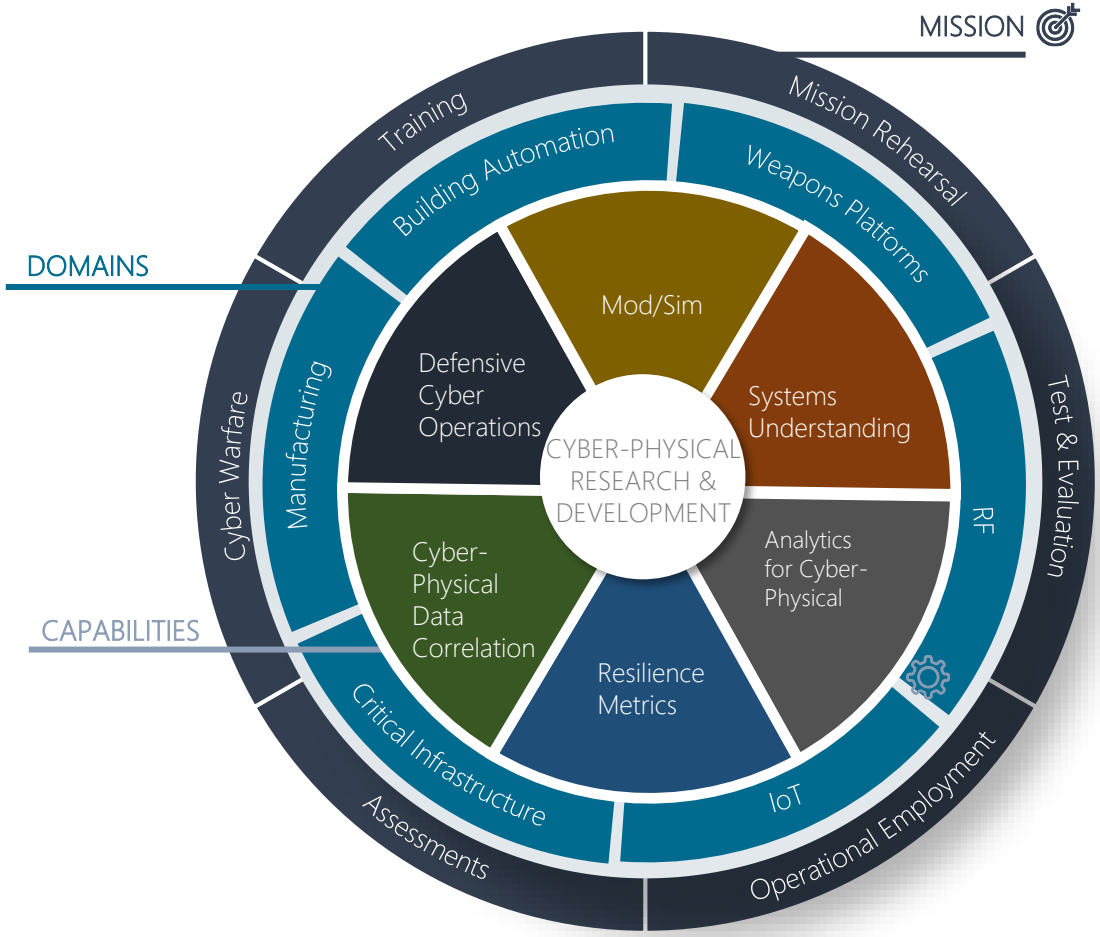
National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc.

Government-owned, contractor-operated

FFRDCs are long-term strategic partners to the federal government, operating in the public interest with objectivity and independence and maintaining core competencies in missions of national significance

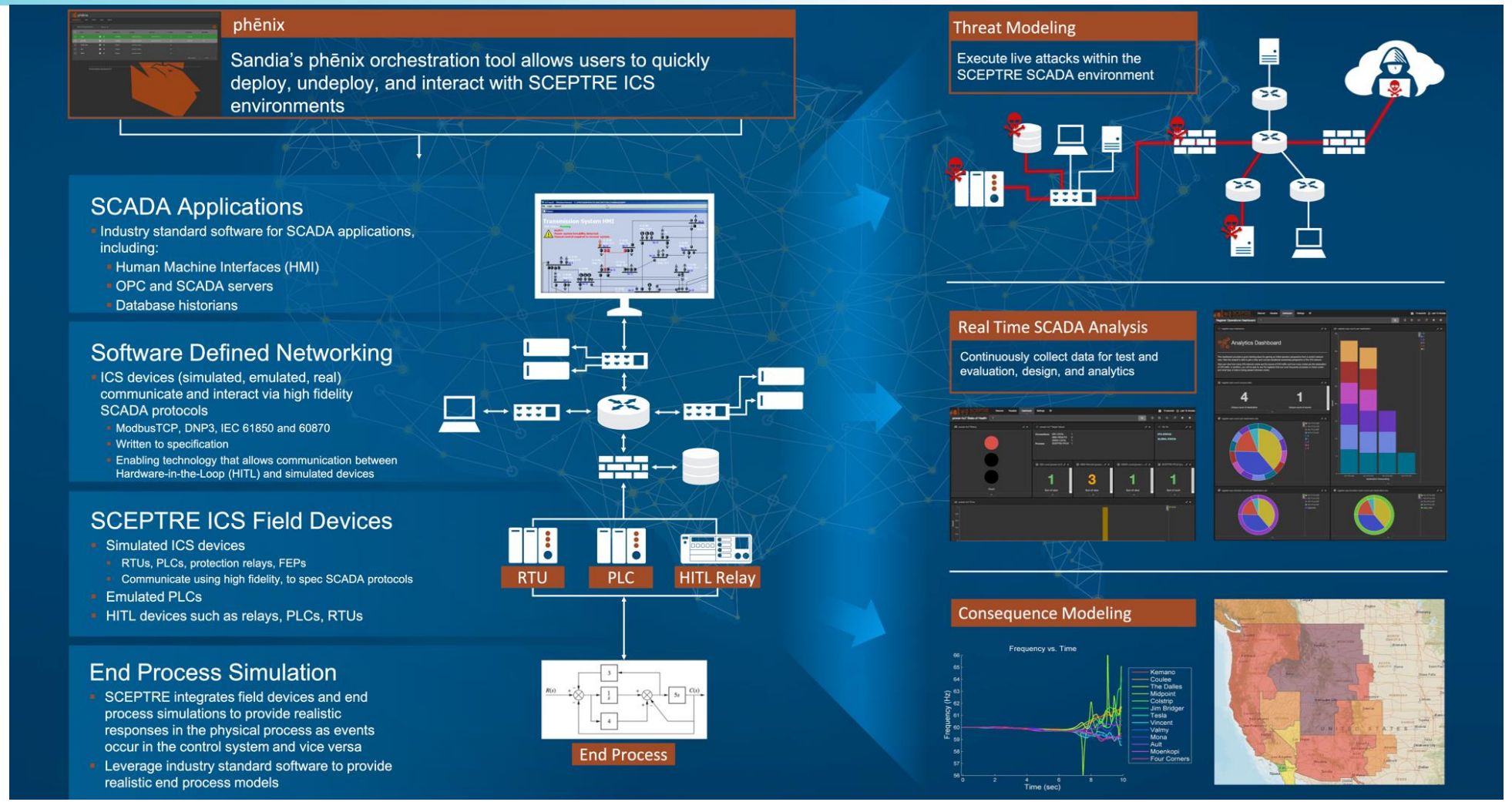
CYBER-PHYSICAL MISSION R&D

- Recent years have witnessed the **increasing synergy between the computational technologies and physical components**. A Cyber-Physical System (CPS) is composed of **a collection of interconnected devices that interact with the physical world**. It integrates computation and communication aspects together with control and monitoring techniques.
- The Cyber-Physical Mission R&D group provides research and development in the cyber-physical domain for national security missions. The sub-domains that we specialize in are informed by the needs of our sponsors and their mission drivers.
- Our group builds multi-disciplinary teams to assess a Cyber-Physical Systems (CPS) from a systems view down to individual components on the system.
- Our group maintains a wide variety of skillsets and capabilities.



MOD/SIM

SCEPTRE | INDUSTRIAL CONTROL SYSTEM EMULATION PLATFORM



ANALYTICS FOR CYBER-PHYSICAL SYSTEMS

Vedizar | IT/OT HUNT AND FORENSIC PLATFORM

Vedizar is a cybersecurity software platform combining several SNL-developed capabilities into one modular Information Technology (IT) / Operational Technology (OT) hunt and forensic platform. It can read in many different IT/OT data types for analysis to tell a more complete story. Vedizar includes a library of analytics to answer questions like

- WHAT ARE THE DEVICES ON MY NETWORK?
- HOW DO THE DEVICES ON MY NETWORK COMMUNICATE?
- ARE ANY DEVICES SHOWING SUSPICIOUS BEHAVIORS?
- ARE ANY DEVICES ACTING OUT OF THE ORDINARY?
- ARE ANY PHYSICAL PROCESSES RUNNING ABNORMALLY?

Core Competencies

CYBER THREAT HUNTING

COMPUTATIONAL ANALYTICS

CYBER-PHYSICAL DATA CORRELATION

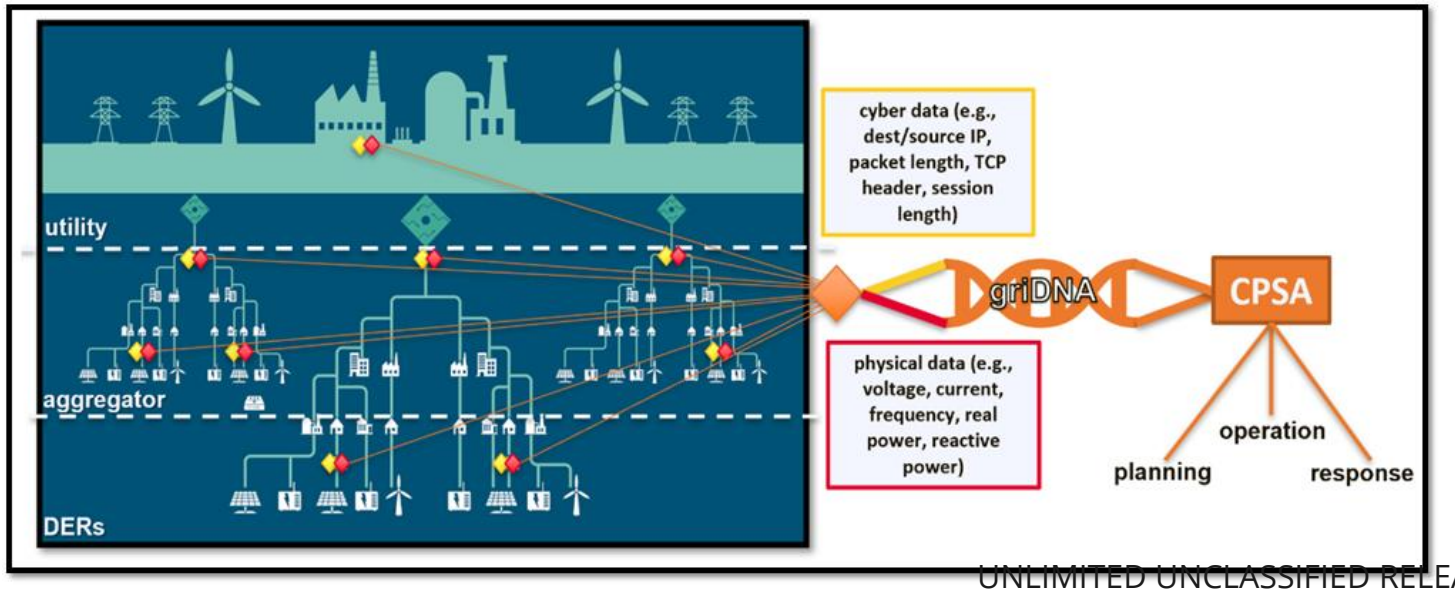
#1 What are the cyber-physical characteristics or features of industrial control systems?

#2 How do we understand the relationship between cyber and physical system features?

#3 How can we leverage this understanding for improved situational awareness and detection of abnormalities?

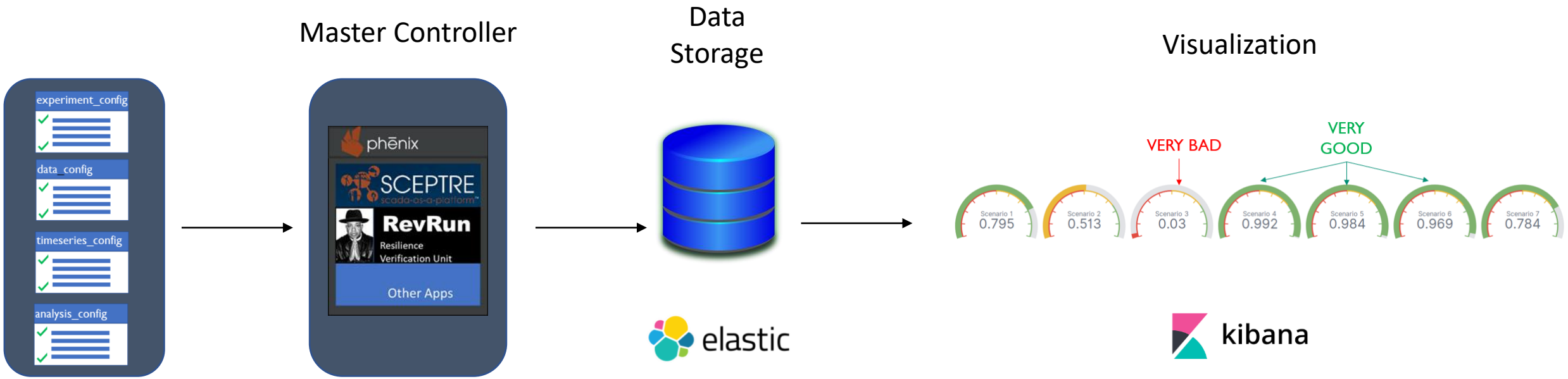
#4 How can we develop effective cyber-physical mitigations that comprehensively improve system conditions?

#5 How do we integrate cyber-physical tools with existing cyber-only or physical-only mechanisms?



RESILIENCE METRICS

RevRun | QUANTITATIVE CYBER RESILIENCE METRICS LIBRARY



RevRun is designed to

- Be highly customizable
- Be fully automated
- Produce quantitative data to compare threats and architectures

THANK YOU

mgaliar@sandia.gov