This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2021-12923C

Sandia National Laboratories

Industry DAY

MOSAICS

October, 2021

SAND XXXX-XXXX P

ASSET DISCOVERY DEEP DIVE

MEGHAN SAHAKIAN

WILLIAM WAUGAMAN

JOHN JACOBELLIS

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.

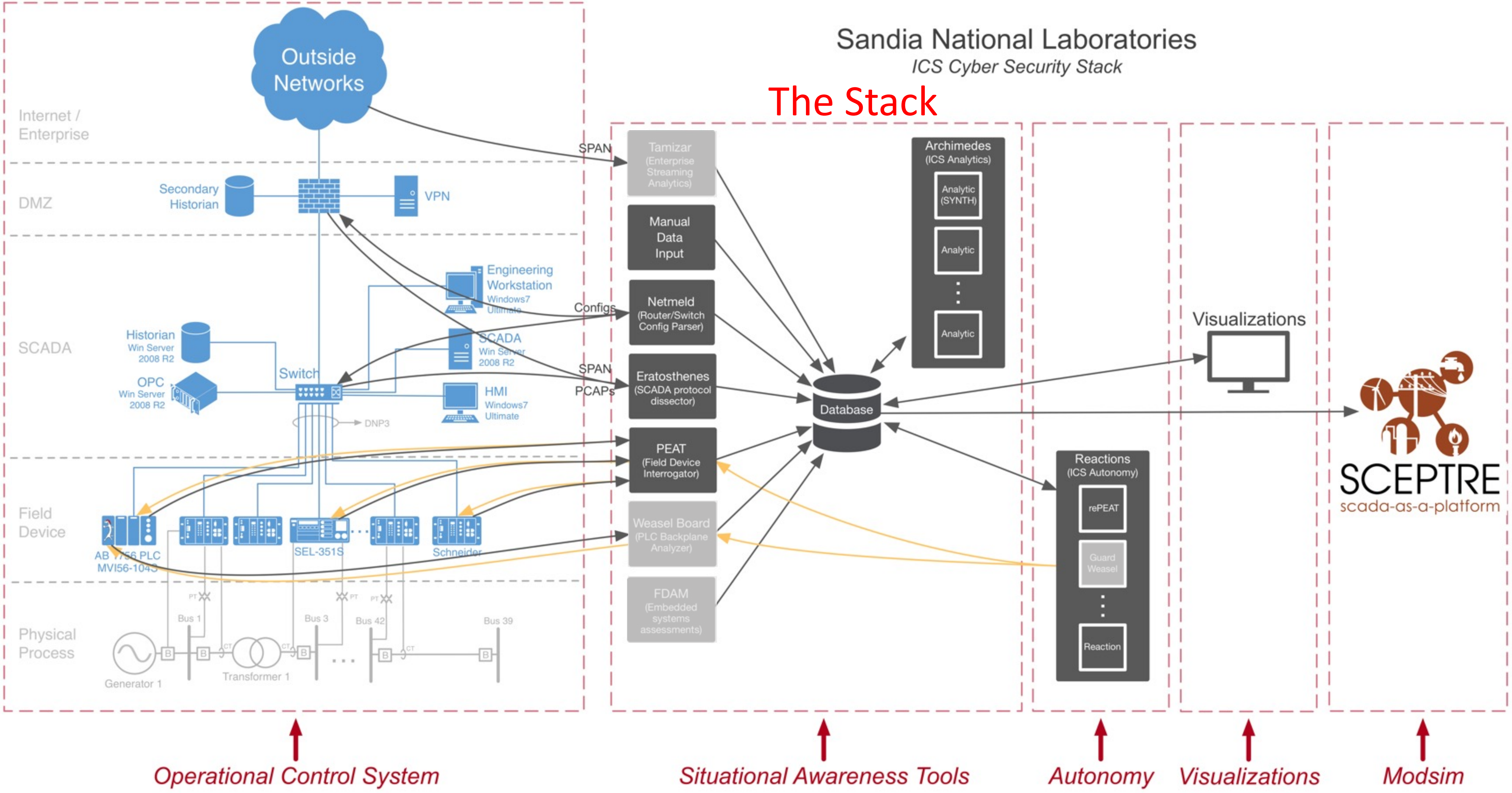
NNSA National Nuclear Security Administration U.S. DEPARTMENT OF ENERGY

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.

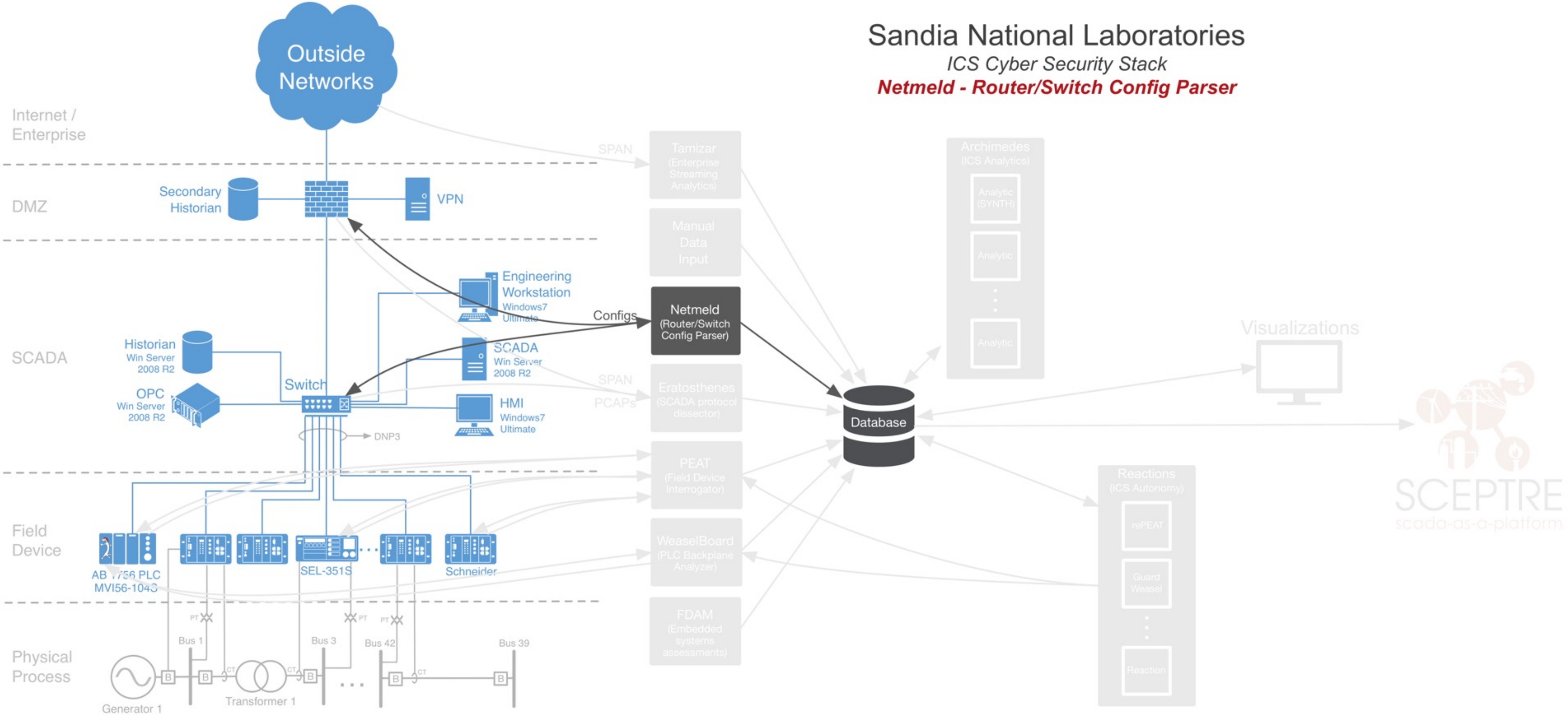
MOSAICS Baselining Capability

- Compilation of Sandia VEDAR tools, COTS, and GOTS
- Semi autonomous capability with additions through manual input
- Both serial and IP based devices
- Key is the data fusion to prevent duplicating devices that are discovered by multiple tools
- Foundational capability of MOSAICS
- Supports data collection for Model Based System Engineering as well

THE STACK


Sandia National Laboratories
ICS Cyber Security Stack
The Stack
Outside Networks
Internet / Enterprise
DMZ
Secondary Historian
VPN
SCADA
Engineering Workstation
Windows7 Ultimate
Historian
Win Server 2008 R2
OPC
Win Server 2008 R2
Switch
SCADA
Win Server 2008 R2
HMI
Windows7 Ultimate
DNP3
Field Device
AB 1756 PLC
MVI56-1043
SEL-351S
Schneider
Physical Process
Generator 1
Transformer 1
Bus 1
Bus 3
Bus 42
Bus 39
PT
CT
B
SPAN
Configs
SPAN
PCAPs
Tamizar
(Enterprise Streaming Analytics)
Manual Data Input
Netmeld
(Router/Switch Config Parser)
Eratosthenes
(SCADA protocol dissector)
PEAT
(Field Device Interrogator)
Weasel Board
(PLC Backplane Analyzer)
FDAM
(Embedded systems assessments)
Database
Archimedes
(ICS Analytics)
Analytic (SYNTH)
Analytic
Analytic
Reactions
(ICS Autonomy)
rePEAT
Guard Weasel
Reaction
Visualizations
SCEPTRE
scada-as-a-platform
Operational Control System
Situational Awareness Tools
Autonomy
Visualizations
Modsim

THE STACK - NETMELD



Sandia National Laboratories

ICS Cyber Security Stack

Netmeld - Router/Switch Config Parser

THE STACK - NETMELD

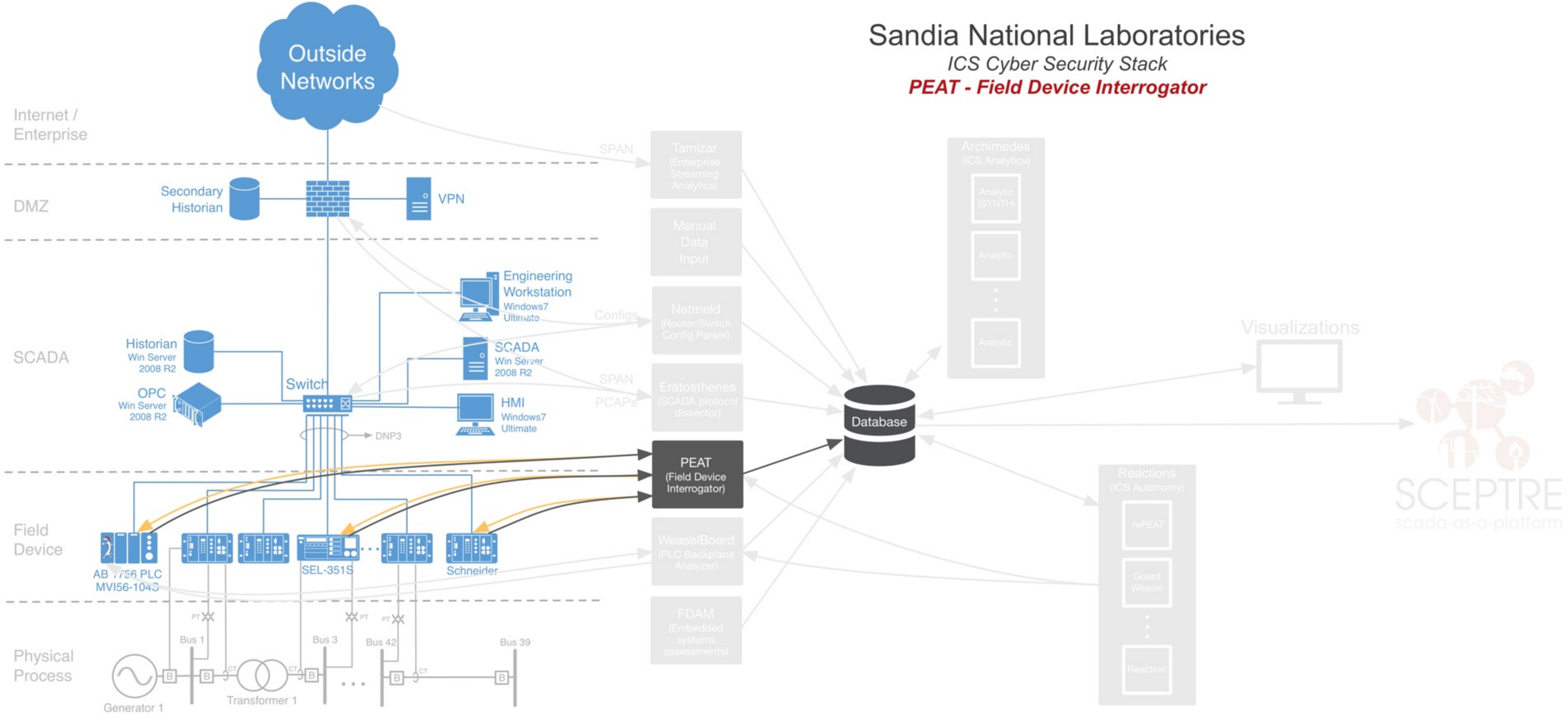
- Network device config collection and ingestion tool for mapping the TCP/IP layer of the networks
- Can be run passively on Cisco and Juniper configs collected out-of-band of control system networks
- Can also be run actively to scan the network for devices endpoints
- Generates detailed network maps of TCP/IP networks

THE STACK - PEAT

Sandia National Laboratories

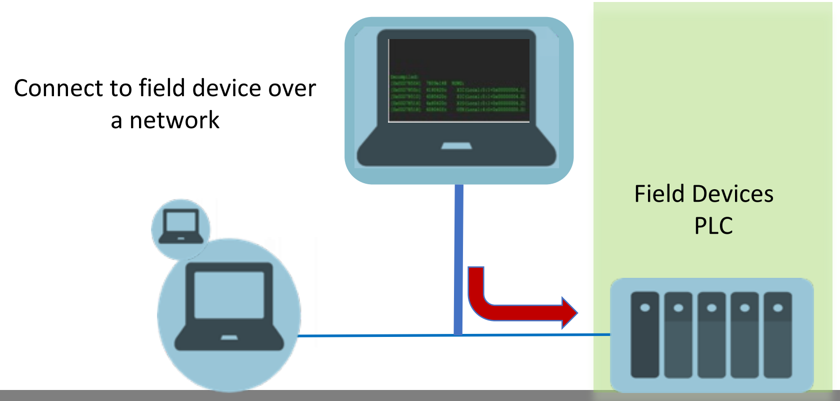
ICS Cyber Security Stack

PEAT - Field Device Interrogator

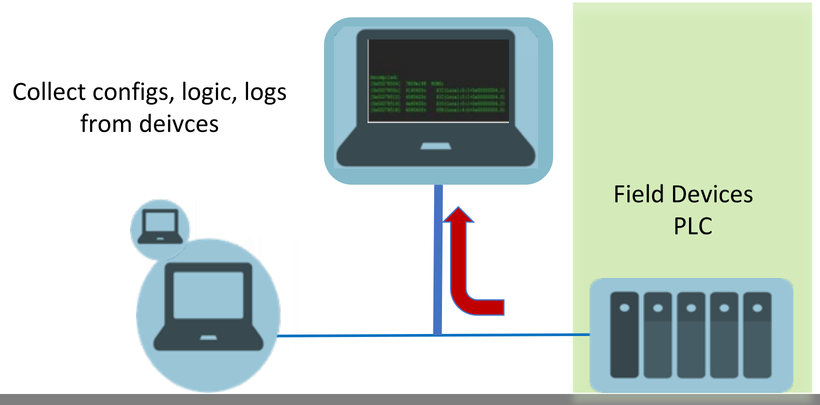


THE STACK - PEAT

- PEAT == Process Extraction and Analysis Tool
- PEAT is an OT device interrogator tool for actively OR passively pulling, parsing, and uploading artifacts from OT devices
  - Can run actively on a control network and perform network discovery (“scanning”)
  - Can run passively to parse device configs (e.g., collected from an engineer workstation)
  - Not exhaustive of all legacy field devices – majority focused on power system devices
- An API developed to enable extensibility to many device makes/models

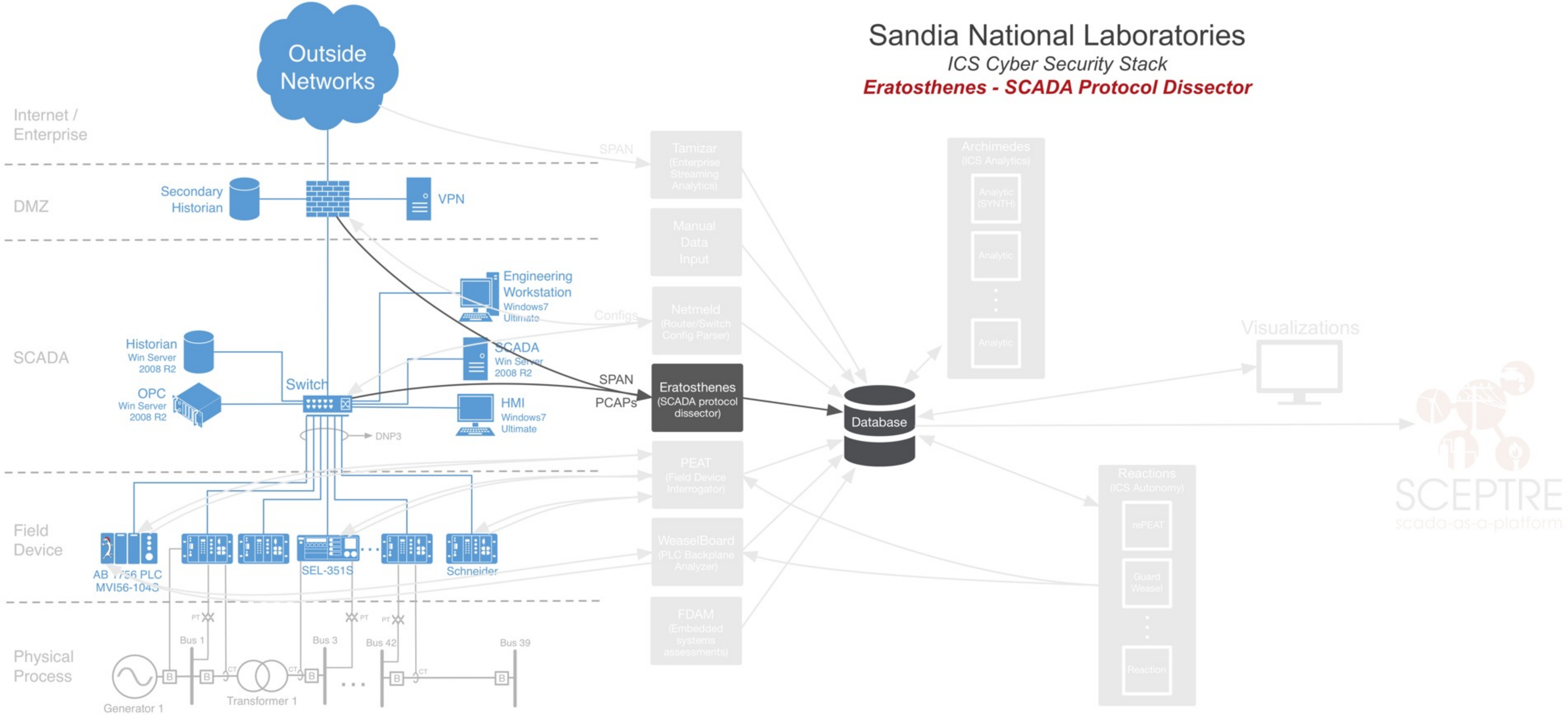


Connect to field device over a network



Collect configs, logic, logs from deivces

THE STACK - ERATOSTHENES



Sandia National Laboratories

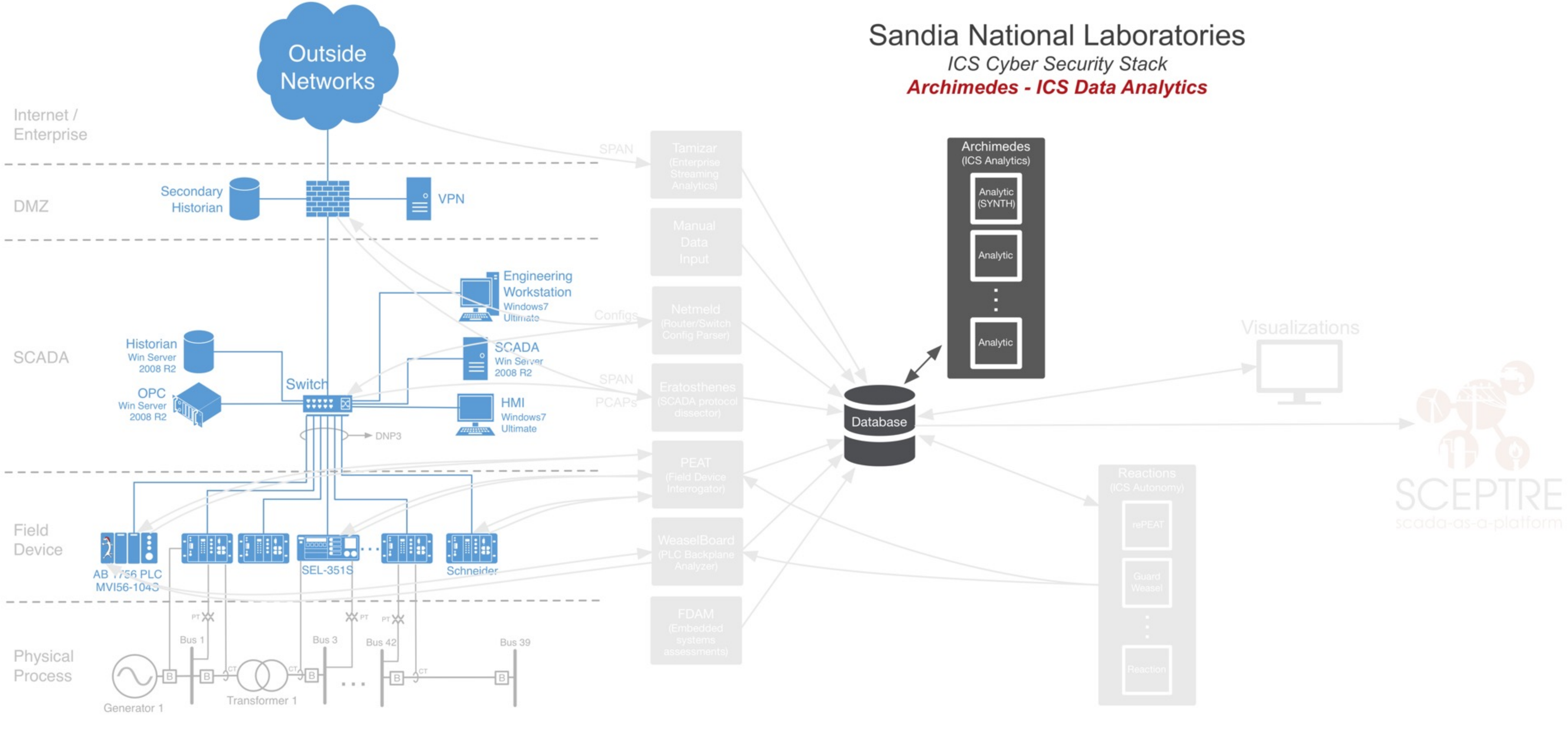
ICS Cyber Security Stack

Eratosthenes - SCADA Protocol Dissector

THE STACK - ERATOSTHENES

- Eratosthenes provides SCADA protocol dissectors to enable deep packet inspection at the register address level
- Dissected protocol traffic at the TCP/IP and serial level is indexed into data stores
- Can be run in streaming on live packet/serial captures or passively on collected PCAPs
- SCADA protocol register resolution allows behavioral analytics to be built for the specific context of the end-process

THE STACK - ARCHIMEDES



Sandia National Laboratories

ICS Cyber Security Stack

Archimedes - ICS Data Analytics

THE STACK - ARCHIMEDES

- An extensible library of analytics for ICS cyber situational awareness
- Analytics are implemented as building block to be combined for various use cases
- Analytics can be
  - Behavioral
  - Signature based
  - Statistical
  - etc.
- Provides the foundations on which baselining, real-time anomaly detection, and response is built

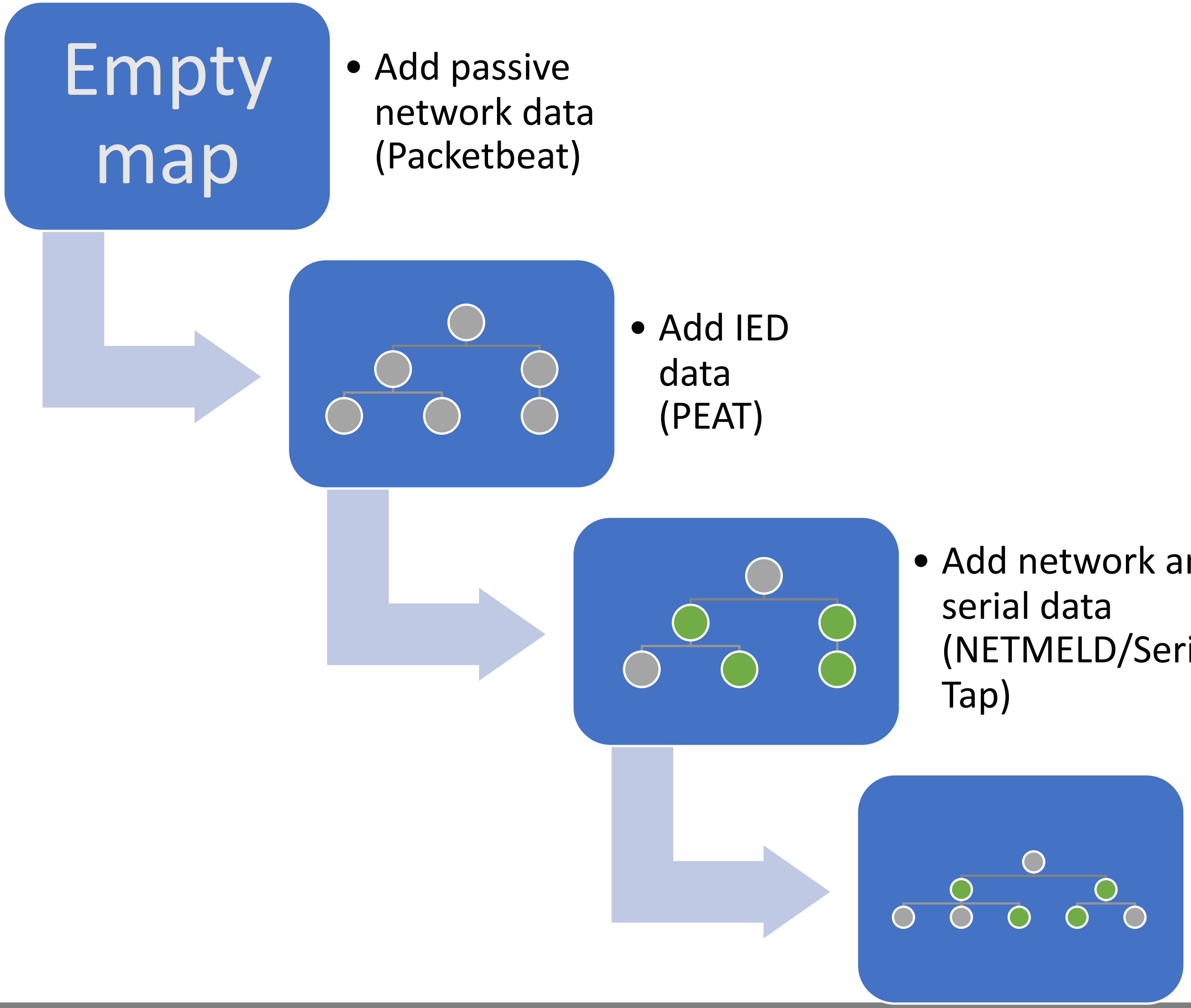
BASELINE TOOL FUNCTIONAL OVERVIEW

- Collect raw data passively, actively, or both
- Fuse data into a single annotated network map
- View map
- Compare baseline map to current map
- Alert on changes

BASELINING TYPES

Baseline Type	Data Type	Data Parsing/collection Tools	Change Monitor/Alerting Tools	Monitoring Process Type	Viz Tool
Network Behavior (passive)	Pcaps, live traffic	Packetbeat, IDS's, firewalls	Archimedes, IDS's, firewalls	Continuous	Kibana, proprietary viz's
Network topology (passive)	Pcaps, live traffic	Packetbeat, Grassmarlin, Netmeld	Archimedes	Batch	Gephi
	Router/Switch configs (ingested offline)	Grassmarlin, Netmeld	Archimedes	Batch	Gephi
OT configuration (passive)	Project files (from host, ingested offline)	PEAT	Archimedes	Batch	Gephi
Network topology (active)	Router/Switch configs (pulled from devices)	Netmeld	Archimedes	Batch	Gephi
	Nmap scan/pingsweep				
OT configuration (active)	Device configuration (pulled from device)	PEAT	Archimedes	Batch	Gephi

BEHIND THE SCENES EXAMPLE



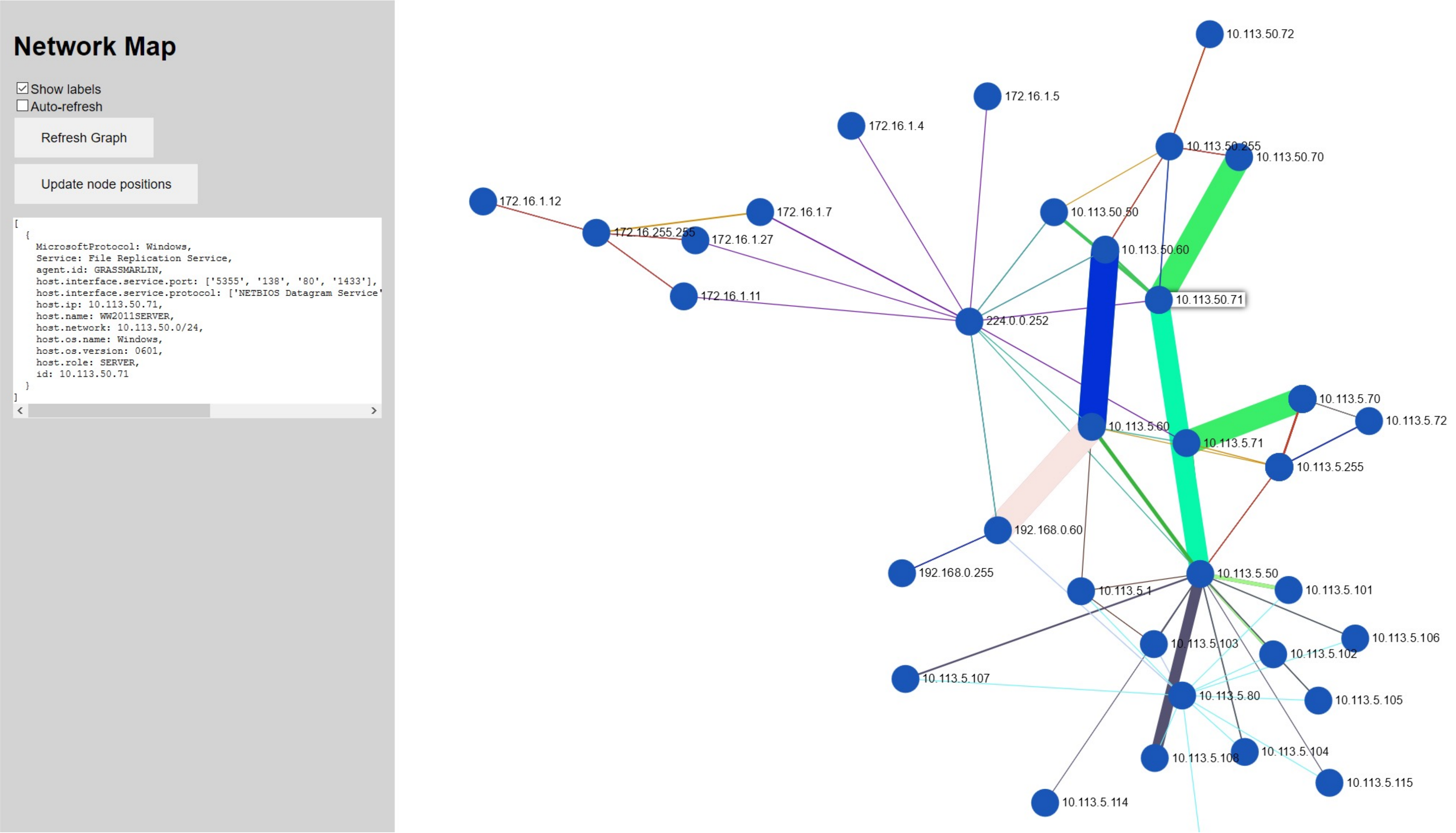
- Add passive network data (Packetbeat)

- Add IED data (PEAT)

- Add network and serial data (NETMELD/Serial Tap)

- Final graph

EXAMPLE BASELINE OUTPUT



Network Map

☑ Show labels

□ Auto-refresh

```
[
  {
    MicrosoftProtocol: Windows,
    Service: File Replication Service,
    agent.id: GRASSMARLIN,
    host.interface.service.port: ['5355', '138', '80', '1433'],
    host.interface.service.protocol: ['NETBIOS Datagram Service'
    host.ip: 10.113.50.71,
    host.name: WW2011SERVER,
    host.network: 10.113.50.0/24,
    host.os.name: Windows,
    host.os.version: 0601,
    host.role: SERVER,
    id: 10.113.50.71
  }
]
```

BASELINING TYPES

- Network behavior: Alert when we see something suspicious across the network
- Network topology: The network should be static, alert if the topology changes unexpectedly
- Field device configuration: Alert if a device’s (PLC, RTU, relay, etc.) configuration changes (such as a firmware update)

NOVEL ADDITIONS FOR MOSAICS

- Incorporation of serial data
- Integration of MOSAICS sensors
  - Nozomi (network traffic)
  - Winlogbeats (host agents)
- Automating baseline capability
  - Demisto orchestrator

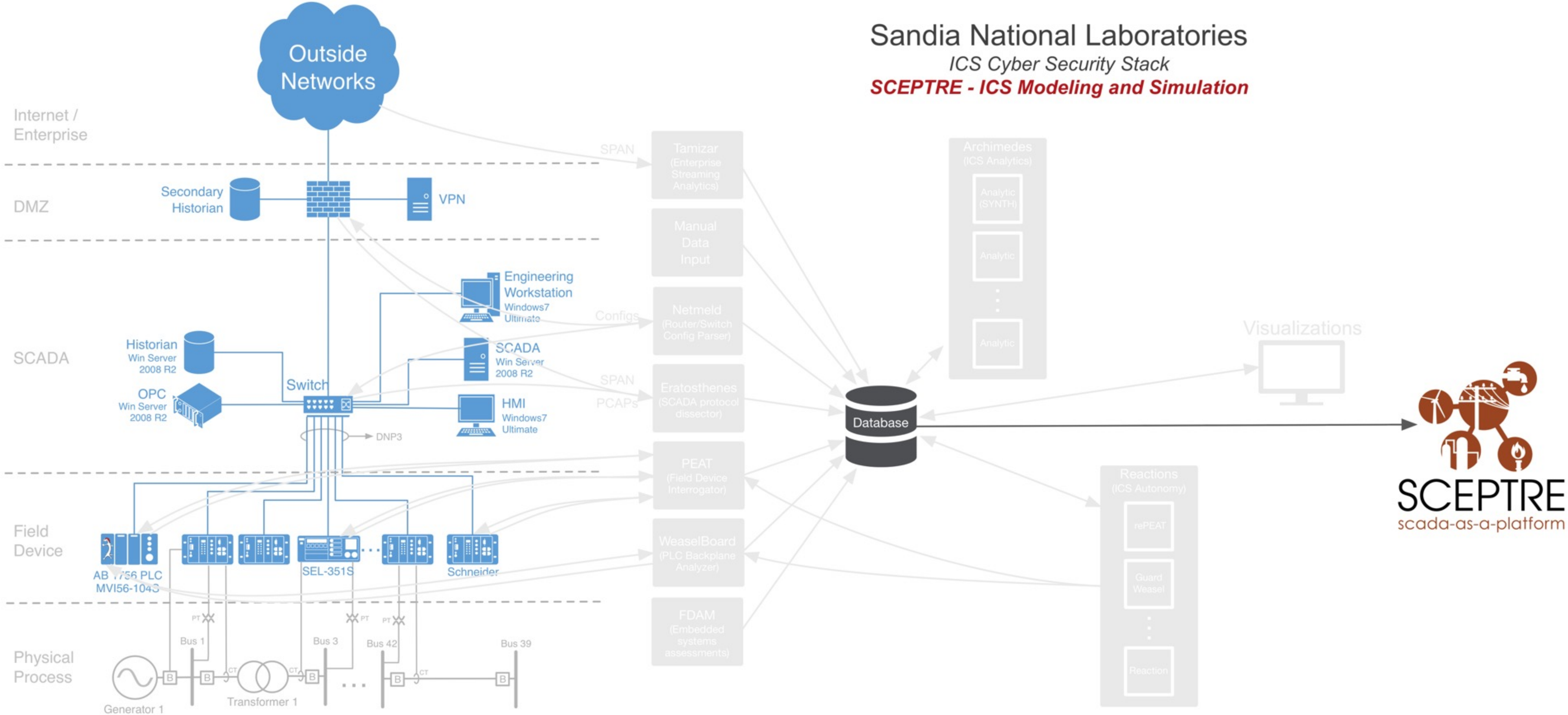
SNL ICS CYBER SECURITY BASELINE USE CASES

- Map-to-Model (M2M) and Deception Networks
- ICS-specific baselining
- Real-Time Anomaly Detection
- Testing and Evaluation
- Malware Analysis
- Training and Mission Rehearsal
- Autonomy for Automated Response

Questions?

BACKUPS

SCEPTRE



Sandia National Laboratories

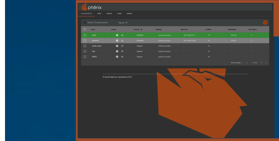
ICS Cyber Security Stack

SCEPTRE - ICS Modeling and Simulation

SCEPTRE
scada-as-a-platform™

Sandia National Laboratories

SCEPTRE provides a comprehensive ICS/SCADA modeling and simulation capability that captures the cyber/physical impacts of targeted cyber events on critical infrastructure and control systems



phēnix

Sandia's phēnix orchestration tool allows users to quickly deploy, undeploy, and interact with SCEPTRE ICS environments

SCADA Applications

- Industry standard software for SCADA applications, including:
  - Human Machine Interfaces (HMI)
  - OPC and SCADA servers
  - Database historians

Software Defined Networking

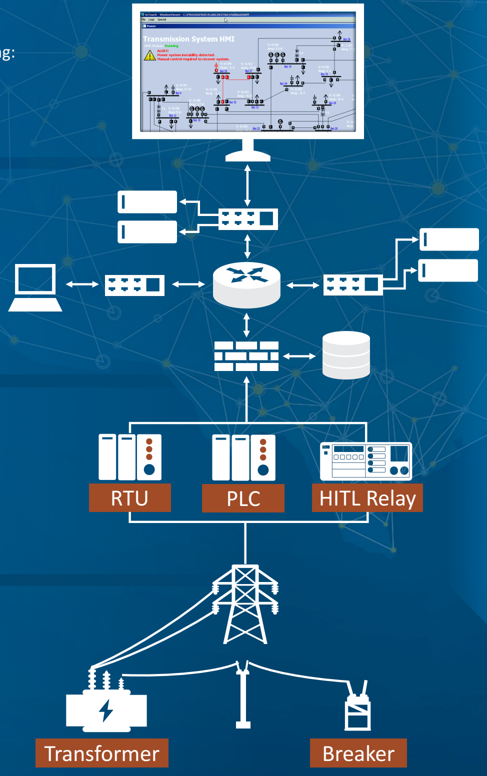
- ICS devices (simulated, emulated, real) communicate and interact via high fidelity SCADA protocols
  - ModbusTCP, DNP3, IEC 61850 and 60870
  - Written to specification
  - Enabling technology that allows communication between Hardware-in-the-Loop (HITL) and simulated devices

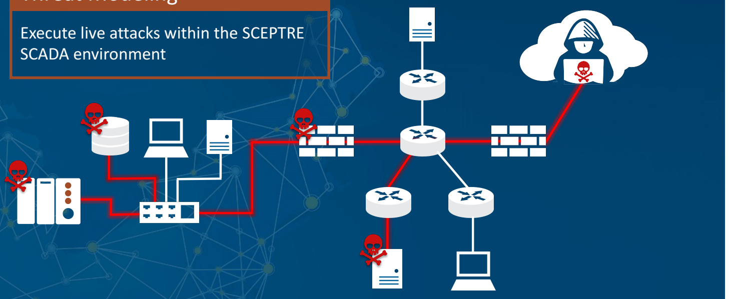
SCEPTRE ICS Field Devices

- Simulated ICS devices
  - RTUs, PLCs, protection relays, FEPs
  - Communicate using high fidelity, to spec SCADA protocols
- Emulated PLCs
- HITL devices such as relays, PLCs, RTUs

Power Simulation

- SCEPTRE integrates field devices and power simulations to provide realistic responses in the physical process as events occur in the control system and vice versa
- Leverage industry standard software to provide realistic end process models



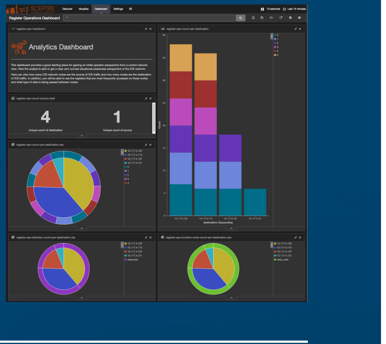


Threat Modeling

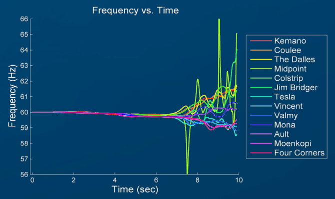
Execute live attacks within the SCEPTRE SCADA environment

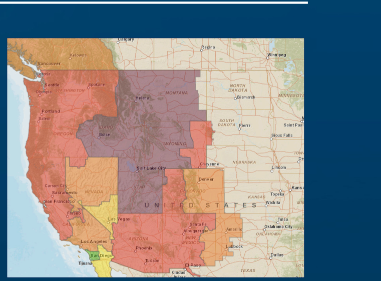
Real Time SCADA Analysis

Continuously collect data for test and evaluation, design, and analytics



Consequence Modeling

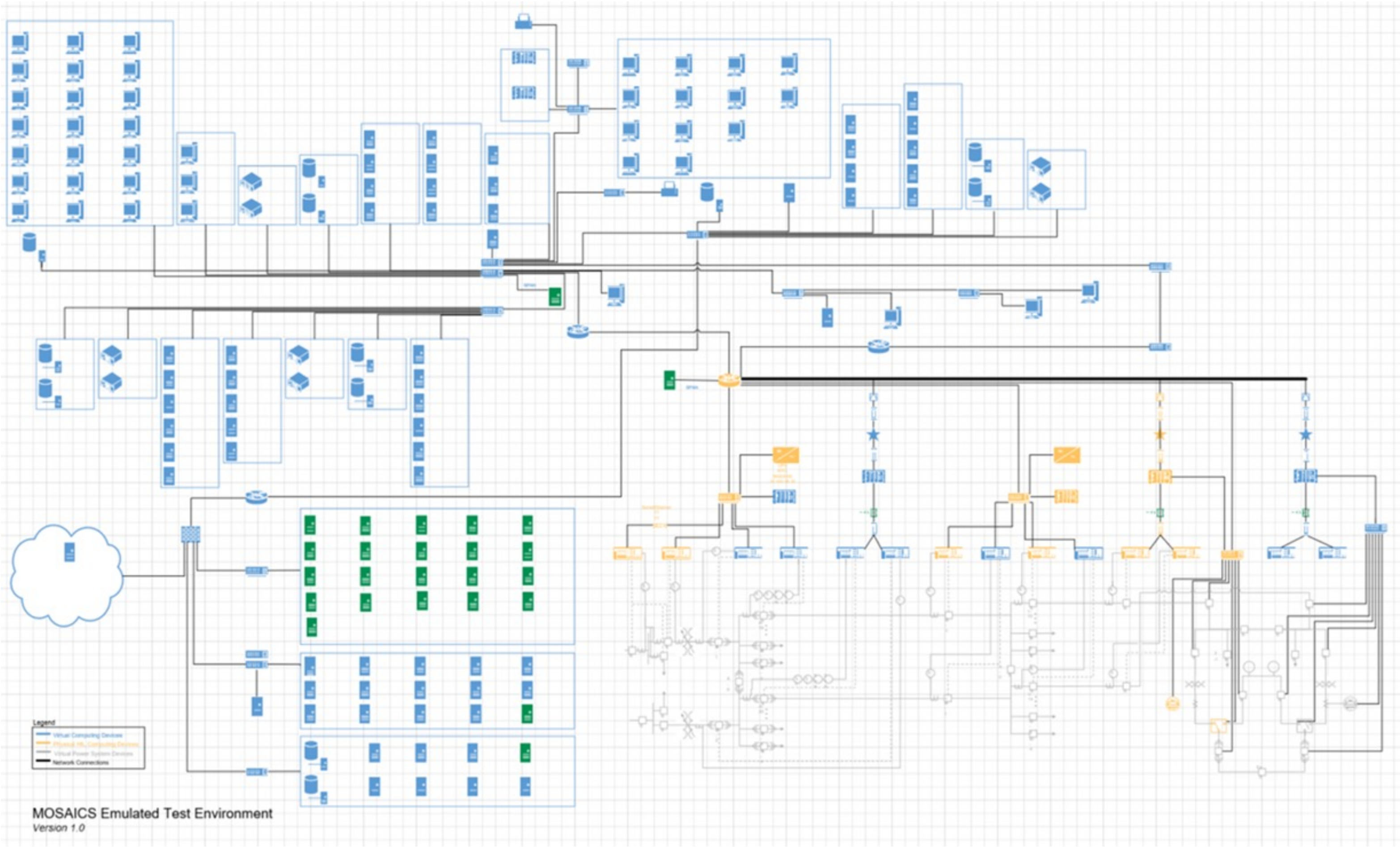




SAND2018-3766 C

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-NA-0003525.

MOSAICS: SCEPTRE ENVIRONMENT


Legend
Virtual Computing Devices
Physical HIL Computing Devices
Virtual Power System Devices
Network Connections
MOSAICS Emulated Test Environment
Version 1.0