Exceptional service in the national interest

Sandia National Laboratories

Improving Microgrid Cybersecurity

Symposium on Microgrids
Niagara Falls, CA
November 20, 2016

Abraham Ellis, Ph.D.
Manager, Renewable and Distributed Systems Integration

Sandia National Laboratories
Albuquerque, NM, USA

aellis@sandia.gov

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

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

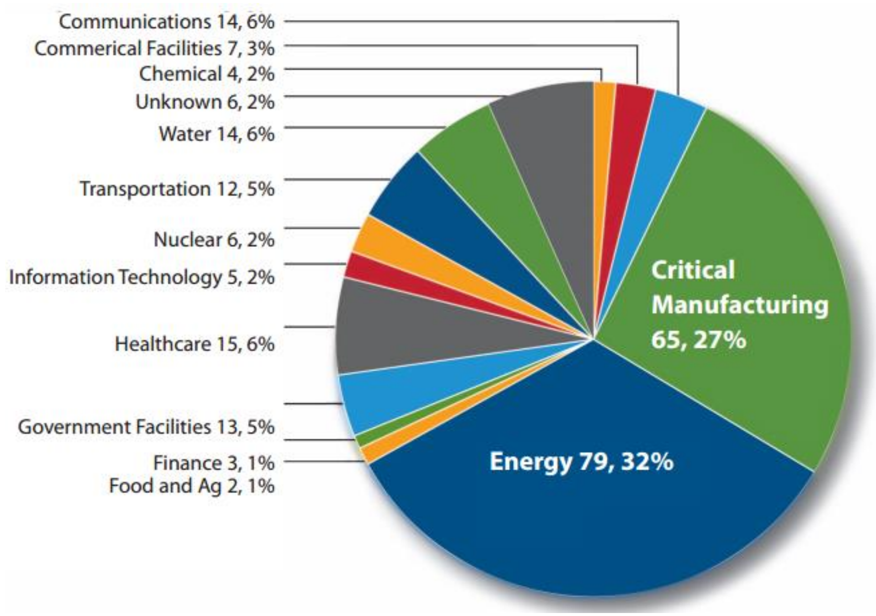
Outline

- Overview
  - Motivation and *defense-in-depth* concepts for microgrid cybersecurity
- Three ways to improving microgrids cybersecurity *
  1. Network segmentation (Microgrid Cybersecurity Reference Architecture)
  2. Hardware-based detection (WeaselBoard PLC hardware security)
  3. Better cyber-physical modeling, simulation and testing (Emulytics, SCEPTRE)
- Q&A

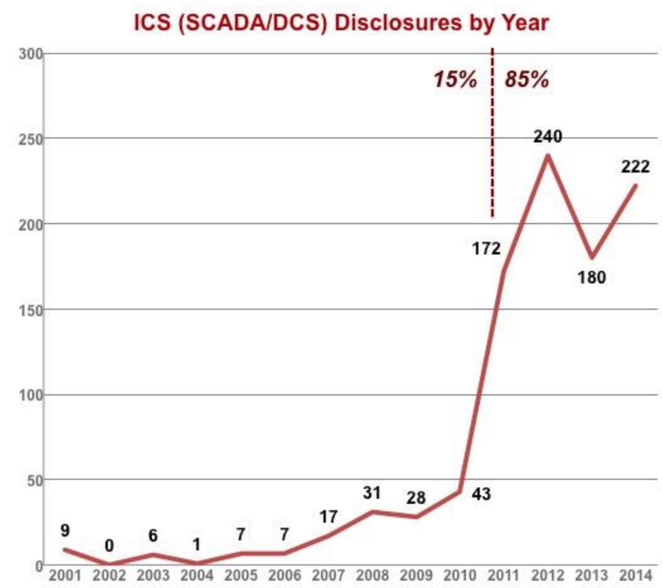
*Based on R&D work at Sandia National Laboratories, sponsored by:
- US Department of Energy Office of Electricity Delivery and Energy Reliability (US DOE/OE)
- US Department of Defense (US DOD)

Energy Systems and Critical Infrastructure

- Energy infrastructure is a common cybersecurity target
- Increased vulnerability due to higher utilization of industrial control systems (ICS), not generally designed with cybersecurity in mind
- Increasingly relevant to microgrids, especially critical applications



Source: US DHS ICS-CERT monitor, 2015



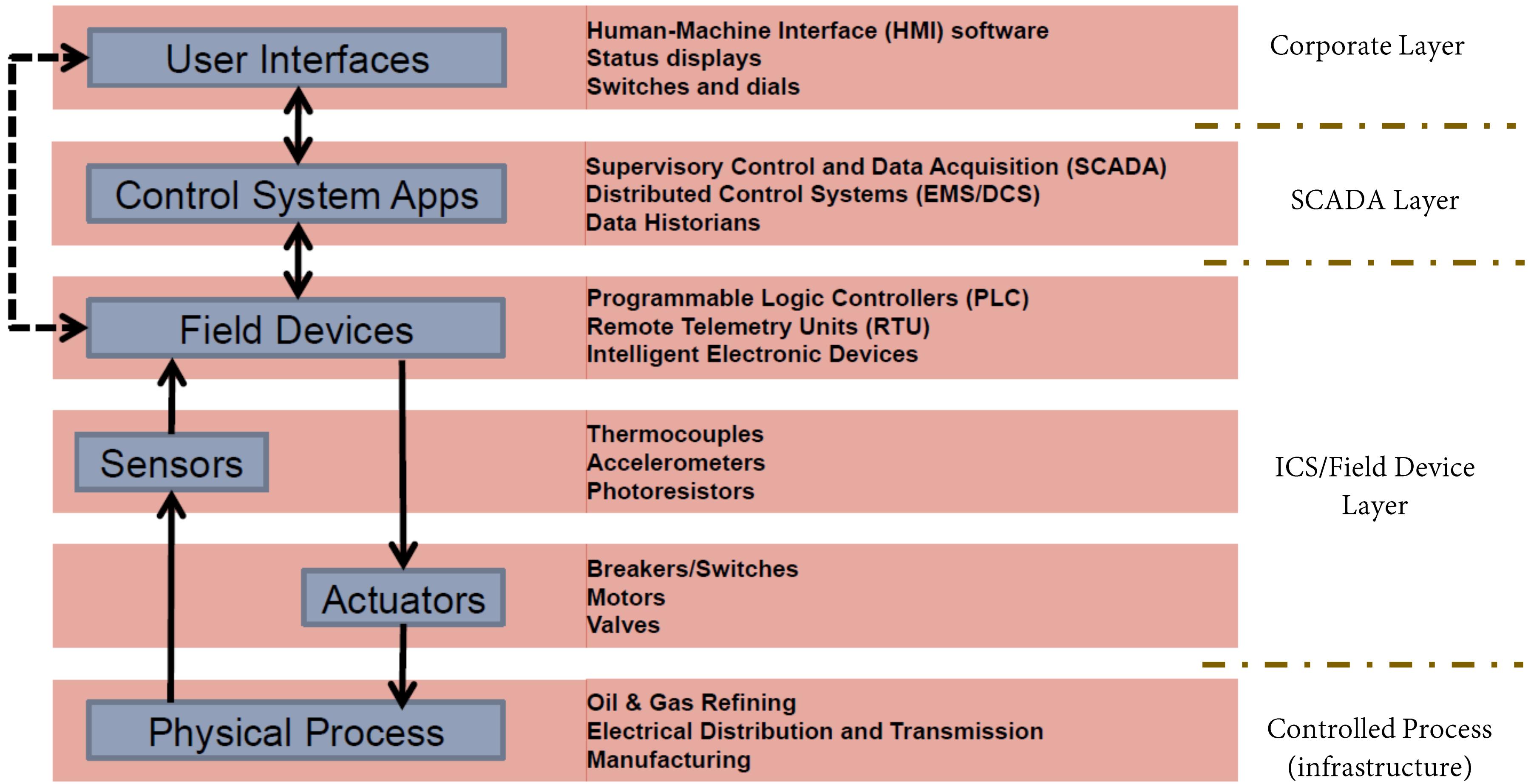
Source: Open-Source Vulnerability Database (OSVDB)

Defense-in-Depth Concepts

- Defense-in-depth concept
  - Multiple security layers addressing *People*, *Technology* & *Operations* vulnerabilities
  - Common in high security applications (e.g., DOD)
- Four stages of cybersecurity defense-in-depth
  1. **Protection**
     - » Policies & procedures (authentication, physical security)
     - » Network security (e.g., Network segmentation, encryption)
  2. **Detection**
     - » Real-time monitoring, situational awareness
  3. **Response**
     - » Contain consequences, impact
     - » Readiness: Planning and decision support tools
  4. **Restoration**
     - » Recover system functionality

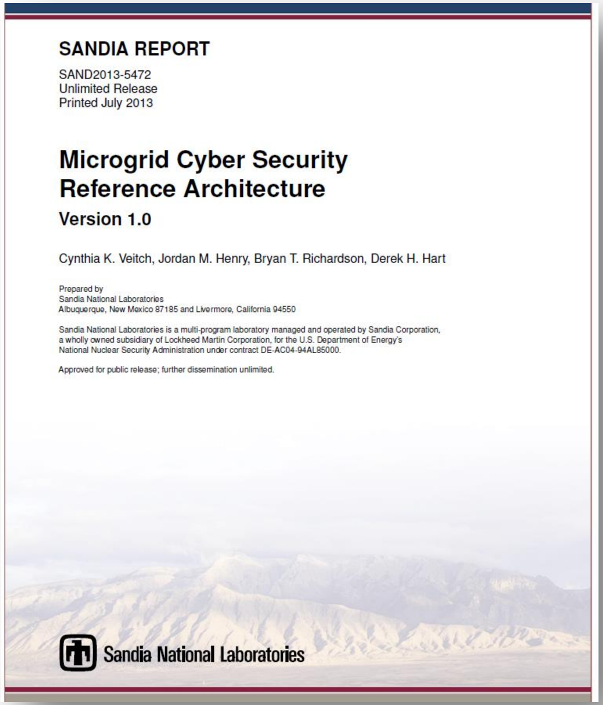
Control System Architecture

- Room for improving cybersecurity in all layers and interfaces



Cyber Security Reference Architecture

- Recommendations for the design and implementation of secure microgrid control systems
  - Focus on *network segmentation* best practices and design criteria
  - Goal is to reduce vulnerability, consequences and recovery time
- Design process
  1. Identify all *actors* (microgrid operator, network administrator, corporate user, vendors, …)
  2. Describe *data exchange* requirements (type, volume, reliability, confidentiality, etc.) See report templates.
  3. Define *enclaves* with similar security and actors
  4. Define enforceable *functional domains* for IEDs
  5. Design and apply other cybersecurity controls (network interface firewalls, monitoring, ...)



SANDIA REPORT
SAND2013-5472
Unlimited Release
Printed July 2013

Microgrid Cyber Security Reference Architecture

Version 1.0

Cynthia K. Veitch, Jordan M. Henry, Bryan T. Richardson, Derek H. Hart

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

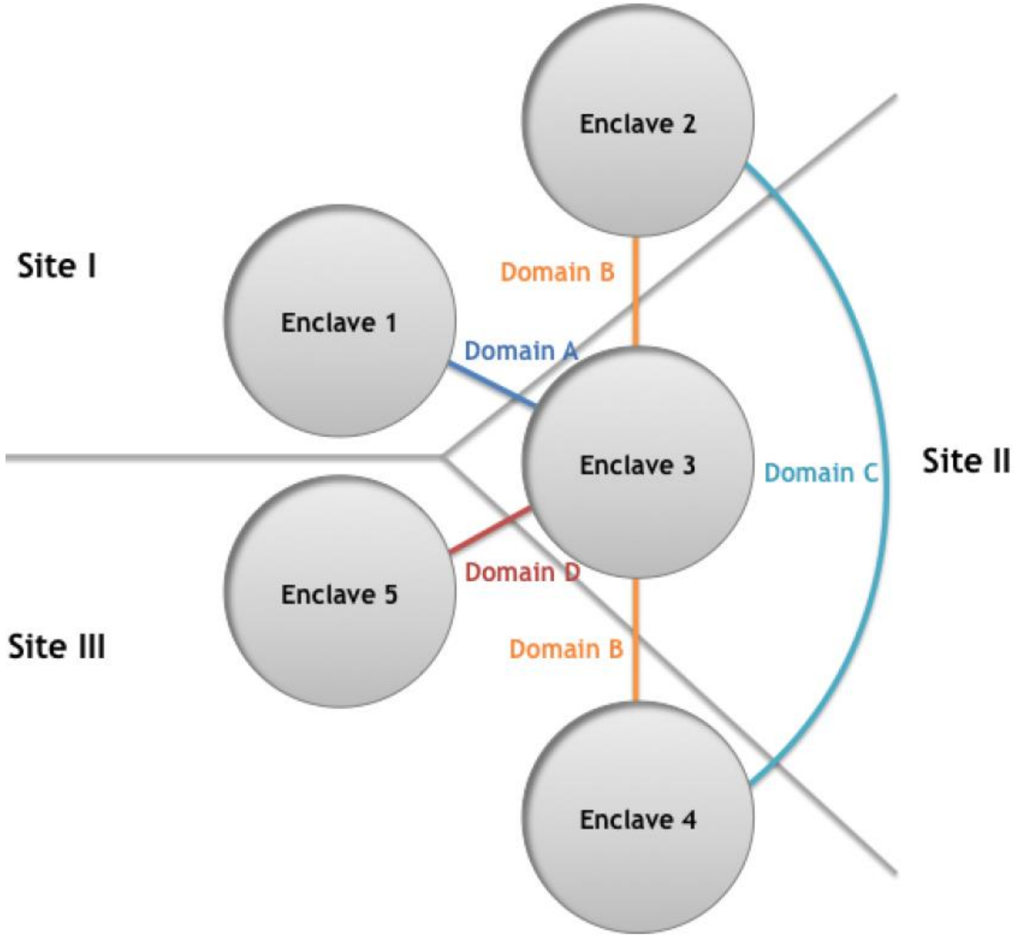
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

Enclaves and Functional Domains

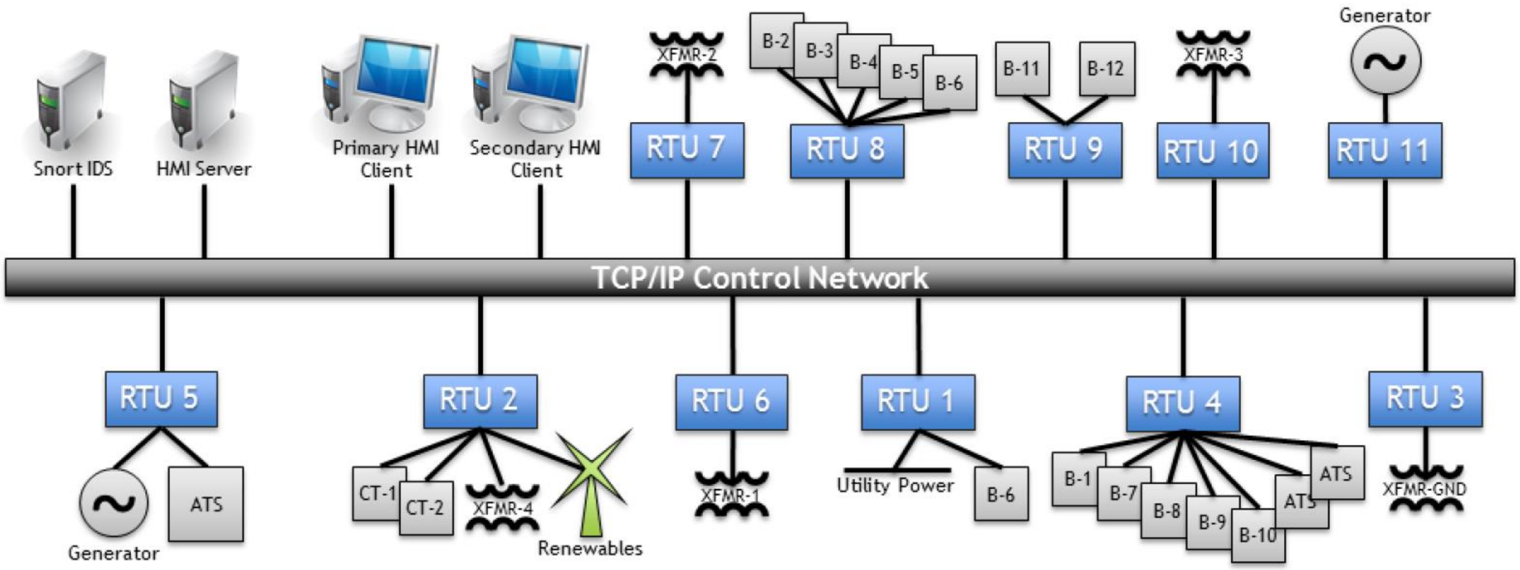
- Enclaves
  - Defines a trusted environment under a single authority and security policy
  - Enclaves are selected based on common attributes for QoS, security, and data requirements
- Functional Domains
  - Defines allowable access and data exchange to allow actors in different enclaves to collaborate securely



Source: Microgrid Cyber Security Reference Architecture V1.0, Sandia Report SAND2013-5472, July 2013

Microgrid Control Network Example

- Typical control system network configuration is flat
  - Relies mostly on security policy (e.g., authentication), maybe hardening.
  - Not a good example of defense-in-depth:
    - All actors could accidentally or maliciously access all data, applications and physical assets within the microgrid
    - Potential impacts are not contained



Data Exchange Worksheet

Source: Microgrid Cyber Security Reference Architecture V1.0, Sandia Report SAND2013-5472, July 2013

Example →

Data Exchange Attributes for *Automated Grid Management and Control (AGMC) Operations*

Source	*HMI server*	*HMI client*
Destination	*HMI client*	*HMI server*
Exchange		
Type	monitor	control
Interval	seconds	minutes to hours
Method	unicast	unicast
Priority	low	medium
Latency Tolerance	high	medium
Data		
Type	breaker status, kW output, kVAr output, voltage magnitude and angle phase, line flow	breaker control, kW output control, voltage control
Accuracy	2 decimal places	2 decimal places
Volume	bytes	bytes
Reliability	informative	important
Information Assurance		
Confidentiality	medium	medium
Integrity	high	medium
Availability	medium	medium

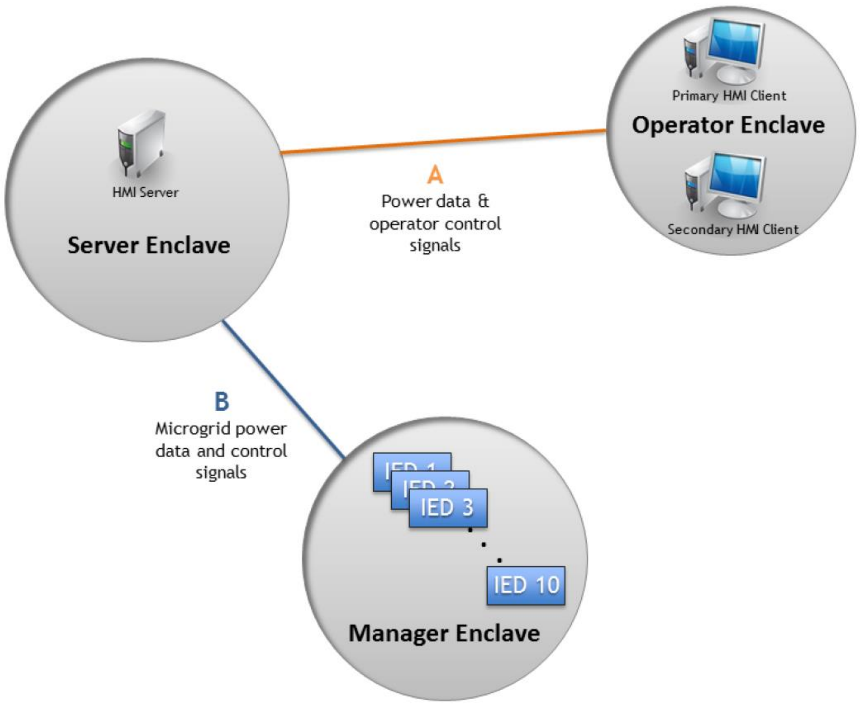
Data Exchange Worksheet Format

↓

	Attribute	**Description**	**Example Values**
Exchange	Type	Type of data exchange to occur	monitor, control, report, write
	Interval	How often data exchange occurs	e.g. milliseconds, seconds
	Method	How data will be exchanged	unicast, multicast, broadcast
	Priority	Relative importance of exchanging the data	high, medium, low
	Latency Tolerance	Tolerance to delayed control or delayed data exchange	high (delays do not affect operation), medium, low
Data	Type	Type of data to be exchanged	voltage, setpoint, status
	Accuracy	Necessary precision/timeliness of data	significant digits, time units
	Volume	Amount of data to transferred per exchange	e.g. bytes, kilobytes, etc.
	Reliability	Necessity of access to control processes and data	critical, important, informative
Information Assurance	Confidentiality	Importance of preserving restrictions to control processes and information access (based on risk to system operations and/or system security)	high, medium, low
	Integrity	Importance of preventing unauthorized changes to control processes or data, including authenticity (based on reliability with respect to operations)	high, medium, low
	Availability	Importance of timely and reliable access to control processes and data (based on priority and latency tolerance with respect to operations)	high, medium, low

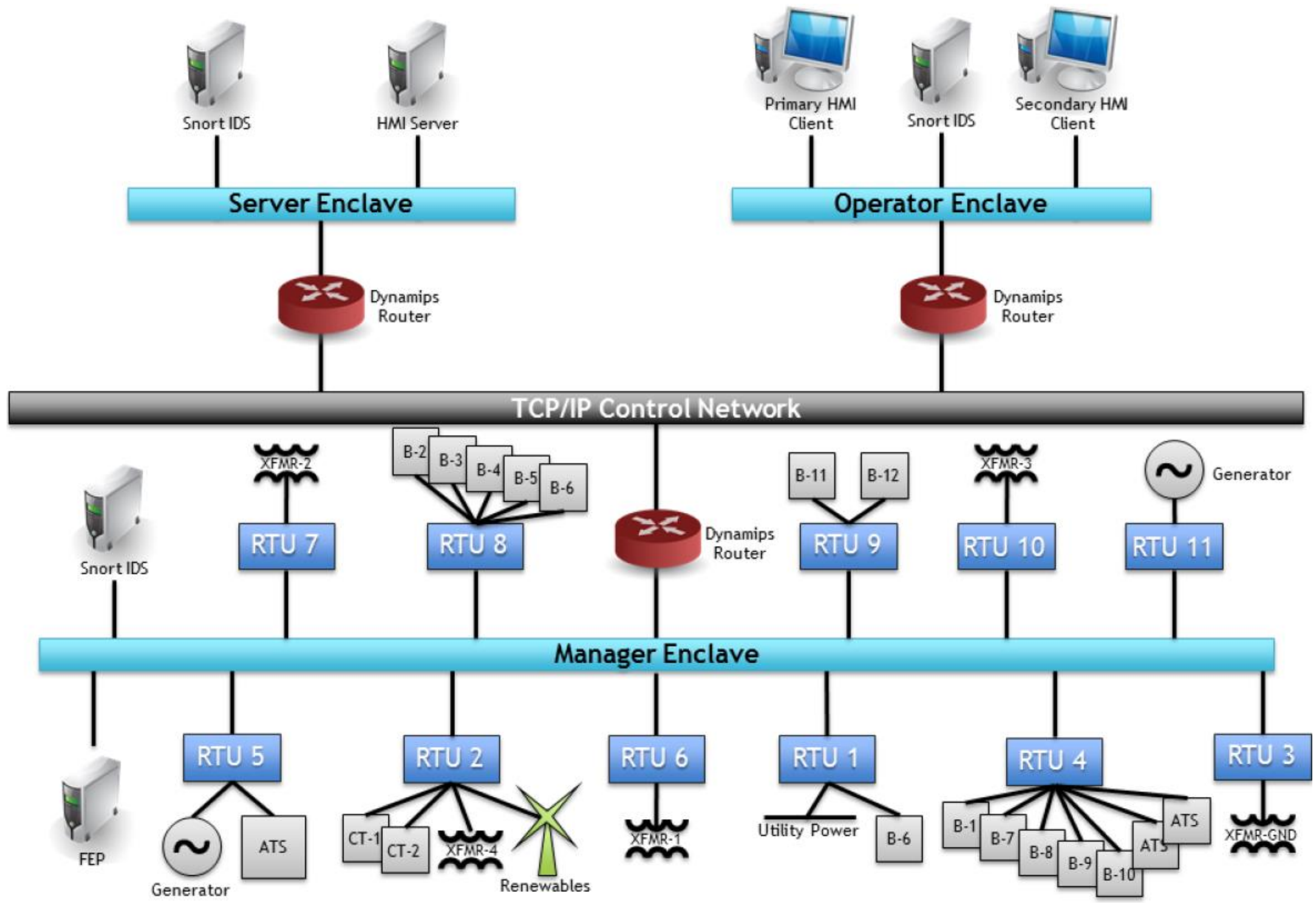
Microgrid Network Segmentation Example

- Suppose we are designing a microgrid with controllable generators, storage, and network elements managed by IEDs
- Could define 3 enclaves based on data and security requirements
  - **Operator:** Primary and backup HMIs
  - **Server:** HMI server, EMS or controller
  - **Manager:** Intelligent electronic devices (IEDs) controlling or managing microgrid switches, flow devices, generators, demand response, etc.
  - Each enclave includes a network intrusion detection and prevention



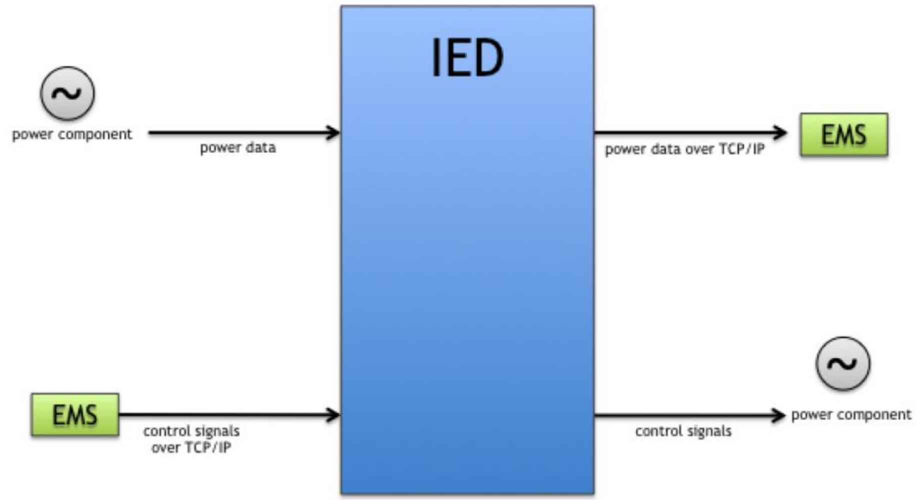
Source: Microgrid Cyber Security Reference Architecture V1.0, Sandia Report SAND2013-5472, July 2013

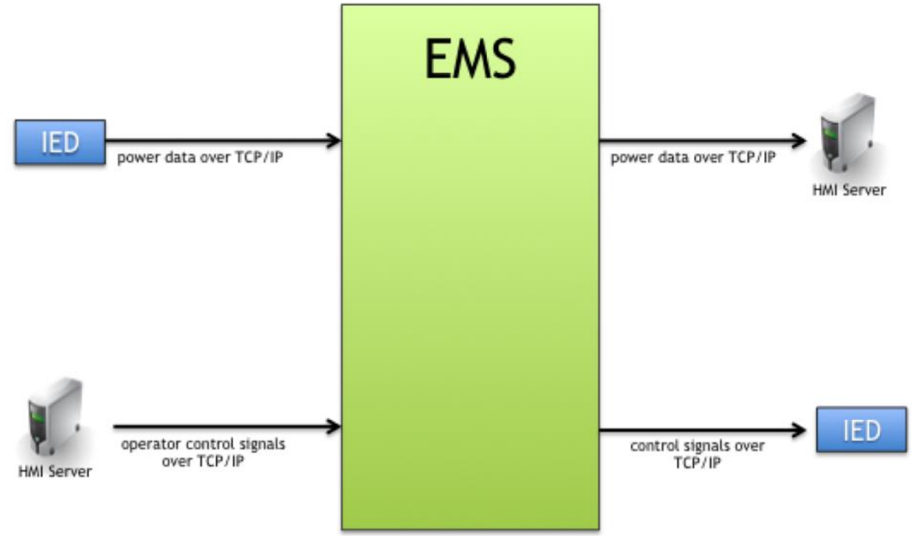
Microgrid Network Segmentation Example



Functional Domains – Examples

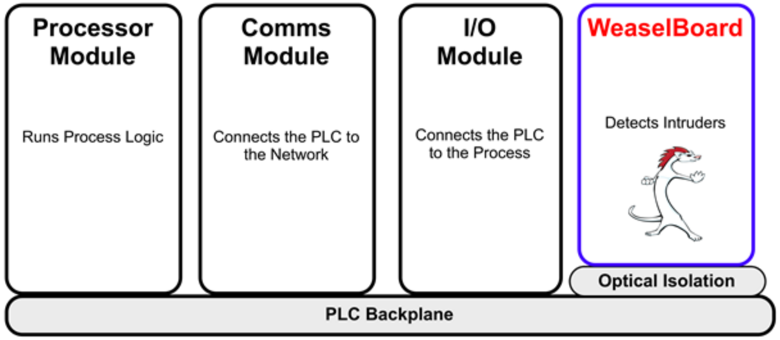
- IED functional domain
  - Receive data from a power device via serial connection, send *information* to EMS over TCP/IP
  - Process information from power device or from EMS, send *command* or *data request* to a power device via serial connection
- EMS functional domain
  - Receive data from IEDs, send *information* to HMI over TCP/IP
  - Process information from IEDs or operator via HMI, send *command* or *data request* to IEDs

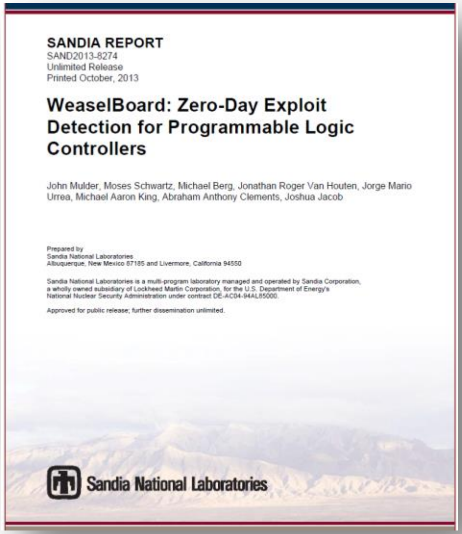




Field Device Security

- Vulnerability of field devices (e.g., PLCs) is a challenging issue
  - Lack of situational awareness locally
  - Limited response and recovery recourses
- Sandia is working on technologies to address this gap
  - WeaselBoard: Locally monitor PLC backplane traffic in real time
  - On-board analytics to detect, alarm and block
  - Industry partnerships




SANDIA REPORT
SAND2013-8274
Unlimited Release
Printed October, 2013

WeaselBoard: Zero-Day Exploit Detection for Programmable Logic Controllers

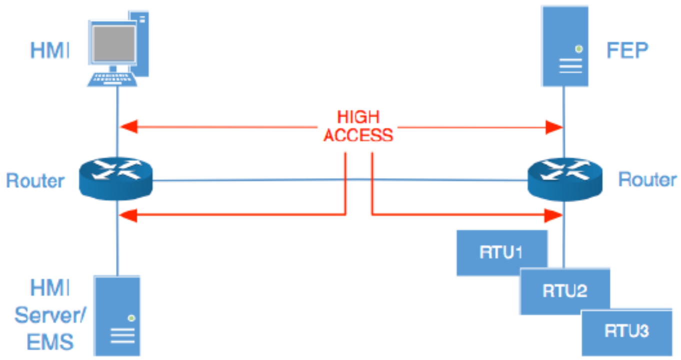
John Mulder, Moses Schwartz, Michael Berg, Jonathan Roger Van Houten, Jorge Mario Urrea, Michael Aaron King, Abraham Anthony Clements, Joshua Jacob

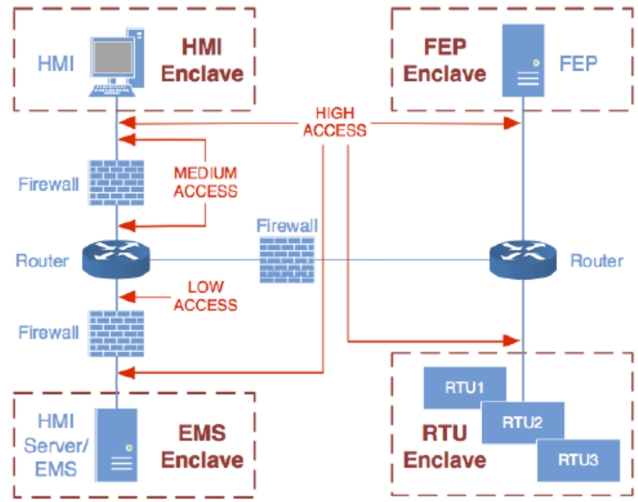
Sandia National Laboratories

More information: http://www.weaselboard.com/

Cybersecurity Analytics

- Red Team assessments and quantitative security performance scores



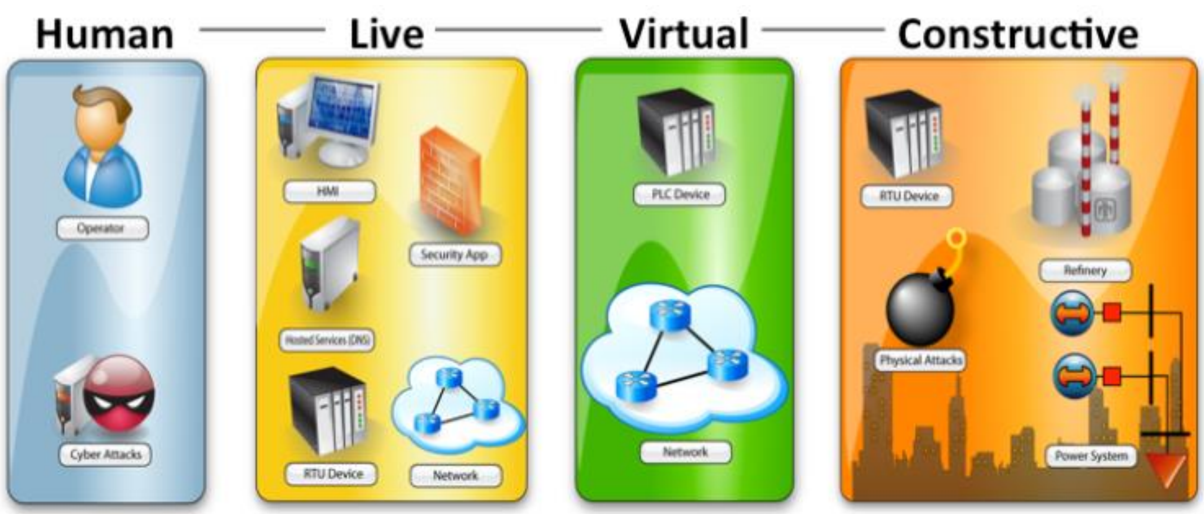


Functional Domain	Read/Write	Confidentiality	Integrity	Availability	Subtotal	Total
HMI-Server	Read	2	3	2	7	13
	Write	2	2	2	6	
Server-FEP	Read	2	3	2	7	13
	Write	2	2	2	6	
FEP-RTU	Read	1	3	3	7	15
	Write	2	3	3	8	
Totals	Both	11	16	14	41	41

Architecture	Access	Compliance	Confidentiality	Integrity	Availability	Total
Flat	High	Insecure	0	0	8	8
		Hardened	9	0	14	23
Enclaved	High	Insecure	0	0	8	8
		Hardened	9	0	14	23
	Med-ium	Insecure	7	6	11	24
		Hardened	9	6	14	29
	Low	Insecure	11	6	16	33
		Hardened	11	6	16	33
Maximum Possible Score →			11	16	14	41

Cybersecurity Analytics

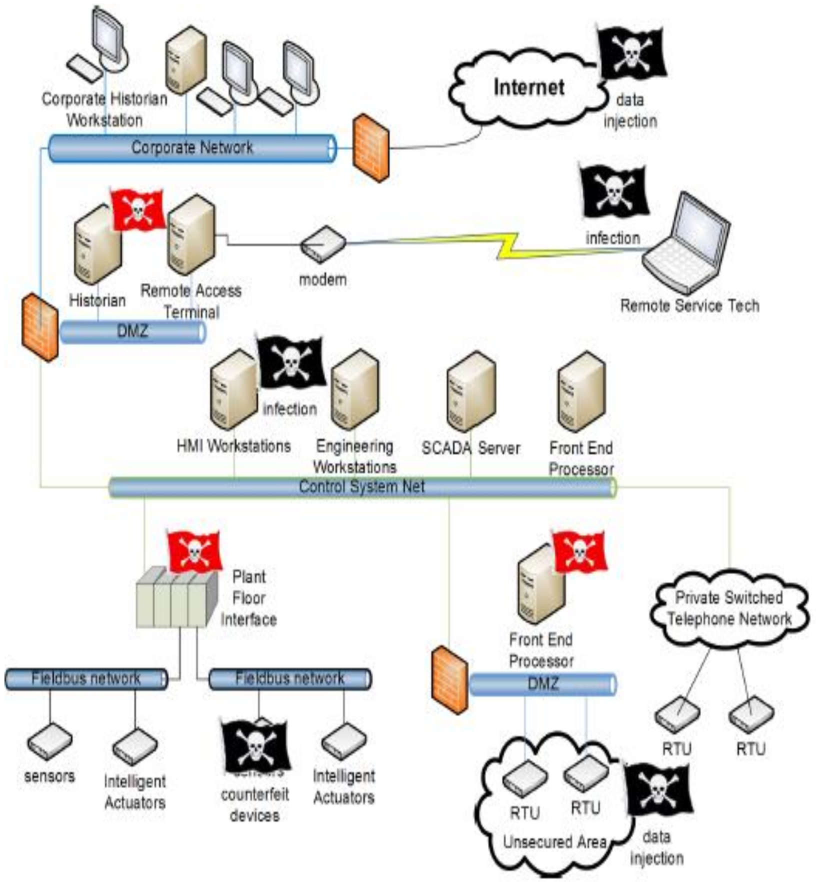
- High fidelity, scalable cyber-physical analysis is difficult
  - Interdependent complex ICS and physical infrastructure
  - Limited capability to model ICS threats and map to physical system consequences
- Sandia's *Emulytics*™ approach combines emulated, simulated, and physical testbed environments
- SCEPTRE is a unique tool for high-fidelity ICS mod/sim/test



More information:
https://vimeo.com/178492617

Emulytics: ICS Mod/Sim/Test Environment

- Model ICS devices w/ SCEPTRE
  - Remote Terminal Units (RTU)
  - Programmable Logic Controllers (PLC)
  - Protection Relays
- Model control center server/services
  - Actual SCADA/EMS/DCS software running real or virtualized hardware
- Model comms network using live-virtual-constructive approach
  - Real devices (routers, switches)
  - Emulated devices (Dynamips, Vyatta)
  - Simulated devices via OPNET Modeler



Questions? Comments?

Abraham Ellis

Sandia National Laboratories

aellis@sandia.gov

www.sandia.gov/missions/defense_systems/cybersecurity.html