Camp Smith Microgrid Controls and Cyber Security

Darrell D. Massie, PhD, PE
Aura Lee Keating, CISSP

SPIDERS Industry Day – Camp Smith, HI

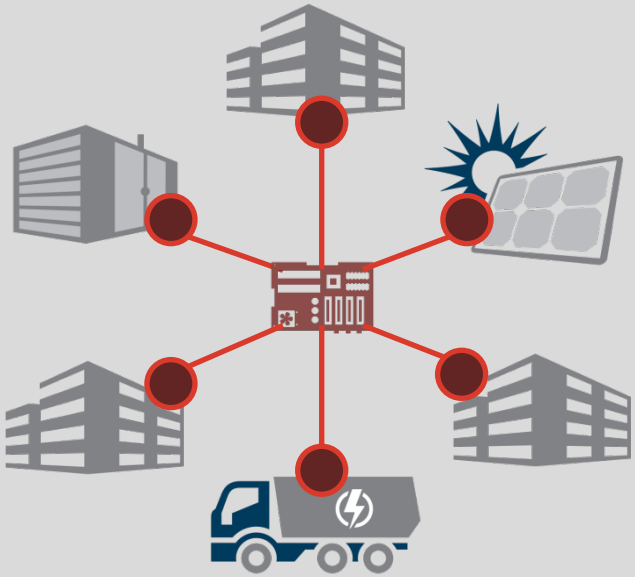
27 August 2015

ADVANCING THE POWER OF ENERGY

Microgrid Resiliency and Cyber Security

- Distributed Controls
- Communications
- Interface with other microgrids
- User Interface
- Energy Surety
- Comprehensive Security Strategy

Camp Smith – Distributed Controller



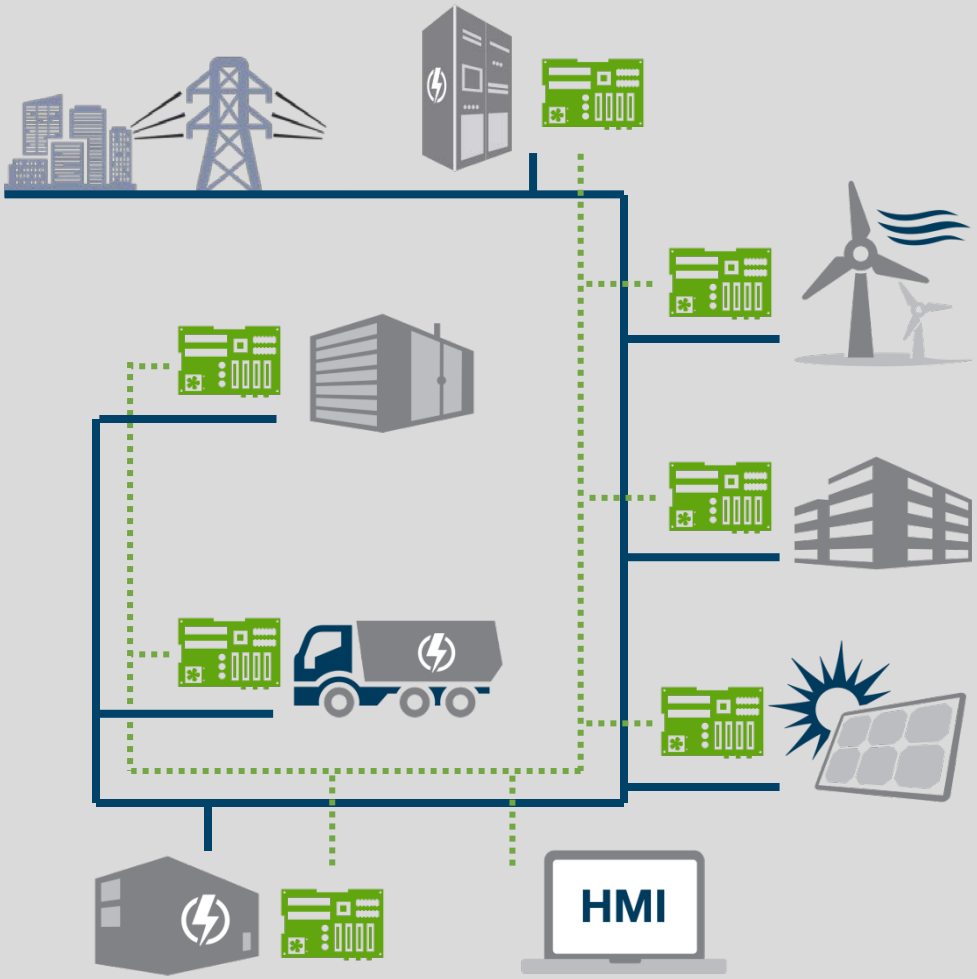
NOT THIS

- × Reflects outdated mainframe mentality
- × A central CPU is a single point of failure
- × Custom software is hard to update
- × Legacy code is vulnerable to cyber attacks
- × Unique configurations are hard to scale

THIS

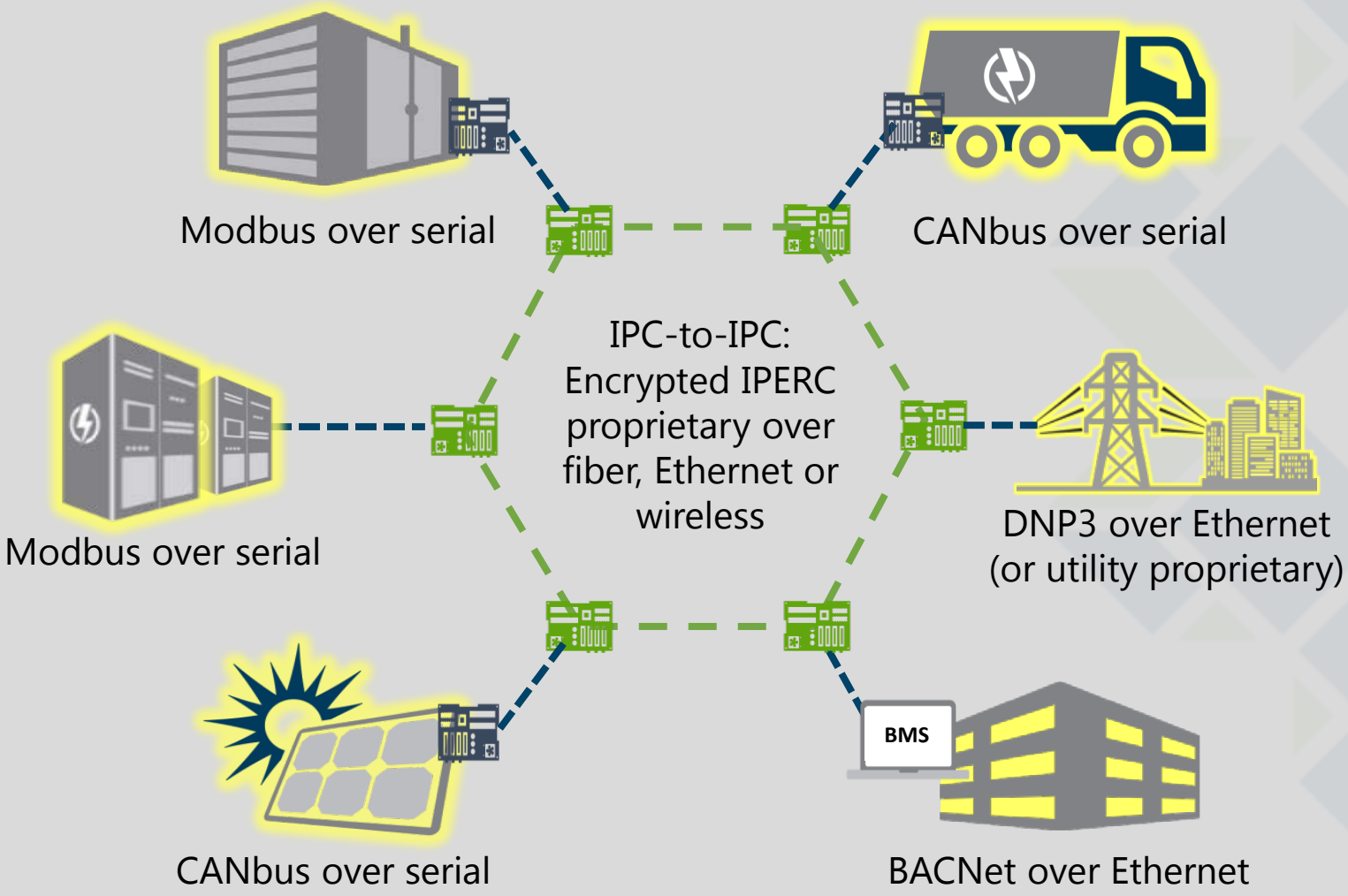
- ✓ Reflects current internet mentality
- ✓ Distributed CPUs create a resilient system
- ✓ A consistent platform facilitates updates
- ✓ Original code written for cybersecurity
- ✓ A modular approach is inherently scalable

IPERC GridMaster® Microgrid Control System

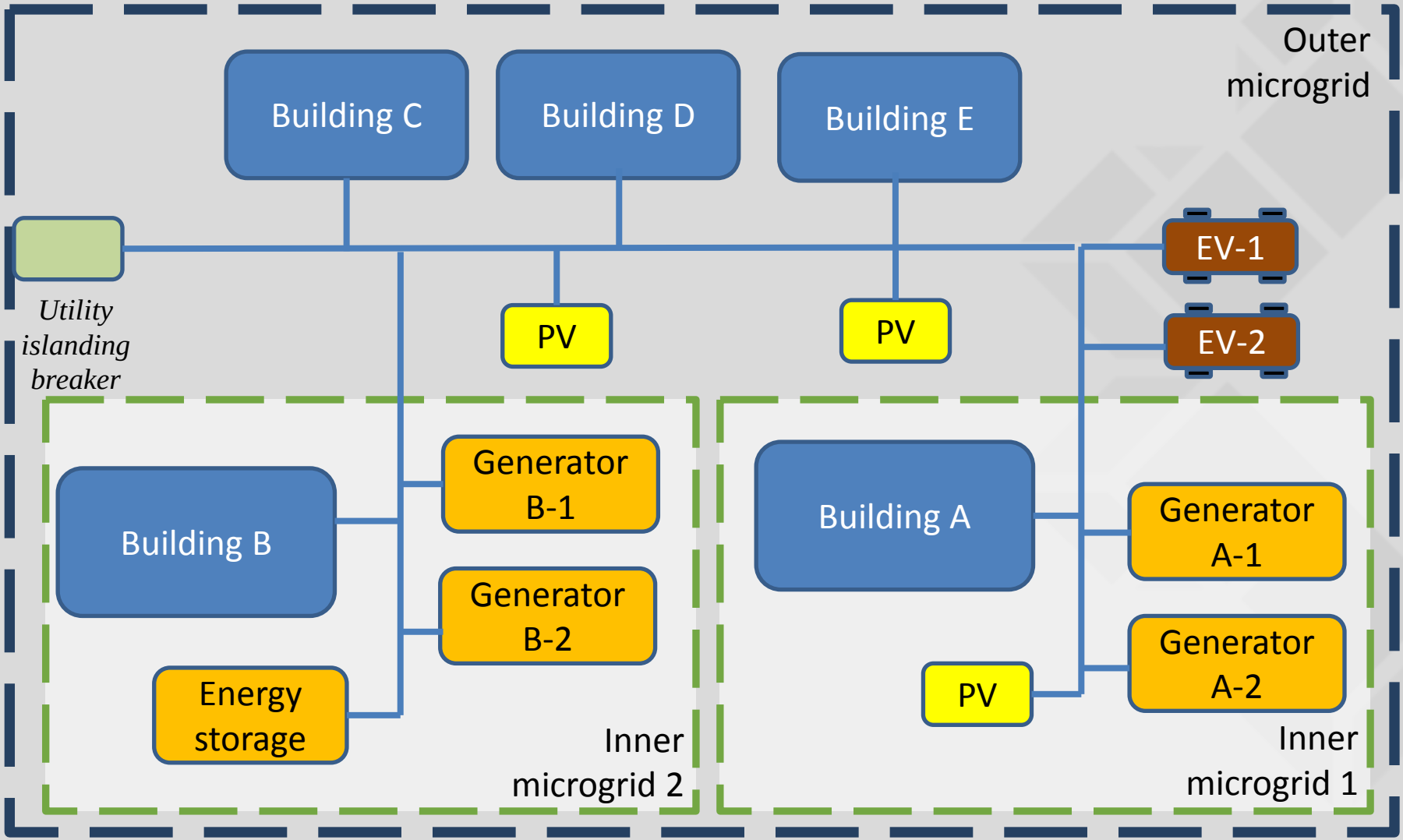


- Peer-to-peer architecture, not master-slave
- GridMaster node (IPC) located with equipment on microgrid
- Proprietary software optimizes energy use across all available sources
- Industry standards to connect to exiting or new infrastructure
- If existing components fail or new ones are added, the system automatically reconfigures itself

Typical GridMaster Communications



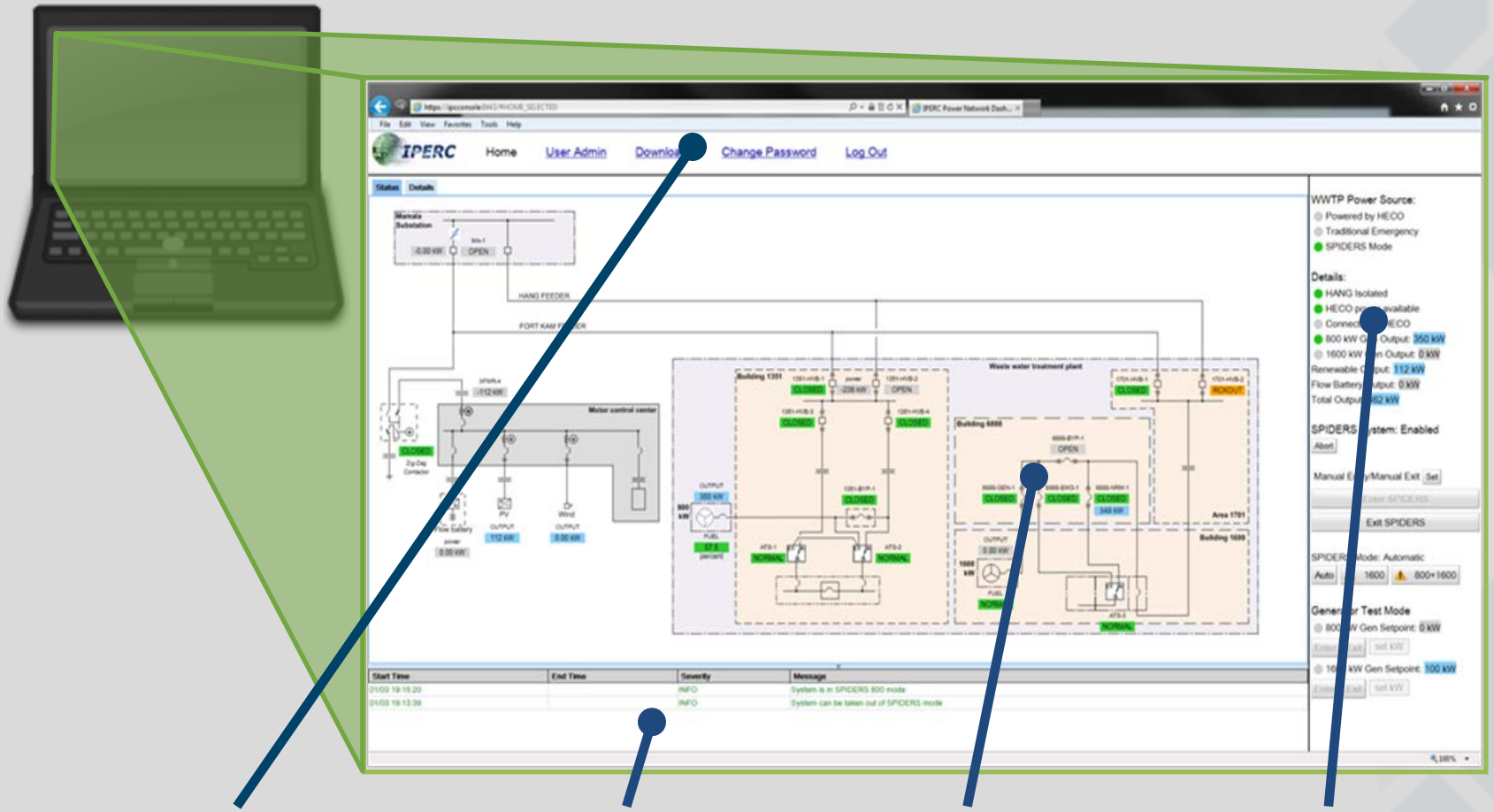
Multiple Grids – Notional Schematic



SPIDERS Graphical User Interface

- Designed in-house by IPERC
- Runs on any browser
- No custom software required
- Dedicated security-hardened desktops and laptops
- Role-based Access
  - **Administrator**: can add/delete/ edit users and passwords
  - **View user**: can view values but cannot set control
  - **Control user**: can view values and set controls
  - **Data user**: can download archived microgrid data values

Graphical User Interface: Features



Energy Surety = Electrical Resilience + Security

Microgrids deliver elements of Energy Surety
Safety, Security, Reliability, Recoverability, Sustainability

Electrical

- Optimize source vs. load
- Prioritized load-shedding
- Redundant controls
- Critical loads met 100%
- Stable power, ancillary services, power quality
- Improved integration of renewables

Security

- Protected data
- Intrusion protection
- Best practices
- DoD, NIST Controls
- Device and OS hardening
- Network security
- Monitoring, Patching, Recovery

Evaluating and testing microgrid functionality is fairly straight forward.
Cybersecurity guidelines for Industrial Control Systems are evolving.

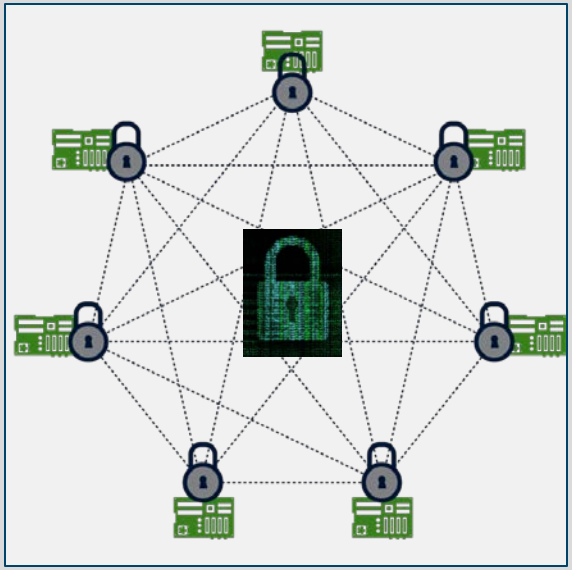
Comprehensive Security Strategy

Camp Smith Cybersecurity Guidelines Applied

- **DoD 8500 Series** - DoD Information Assurance Certification and Accreditation Process (DIACAP), including 8500.2 IA controls
- **Security Controls –** Security Technical Implementation Guides (STIGs), Security Content Automation Protocol tool (SCAP), vendor guidelines

Testing & Evaluation

- JCTD Red Team Attacks
- HBSS, ACAS Functionality for ICS
- Navy Validation Team T&E
- DHS Cyber Security Evaluation Tool (CSET)



Defense In Depth

- Multi-layered security integrated in system development

Defense In Depth

Policies, Procedures, Training & Awareness

Physical Security

Perimeter Protection

Monitoring, Forensics

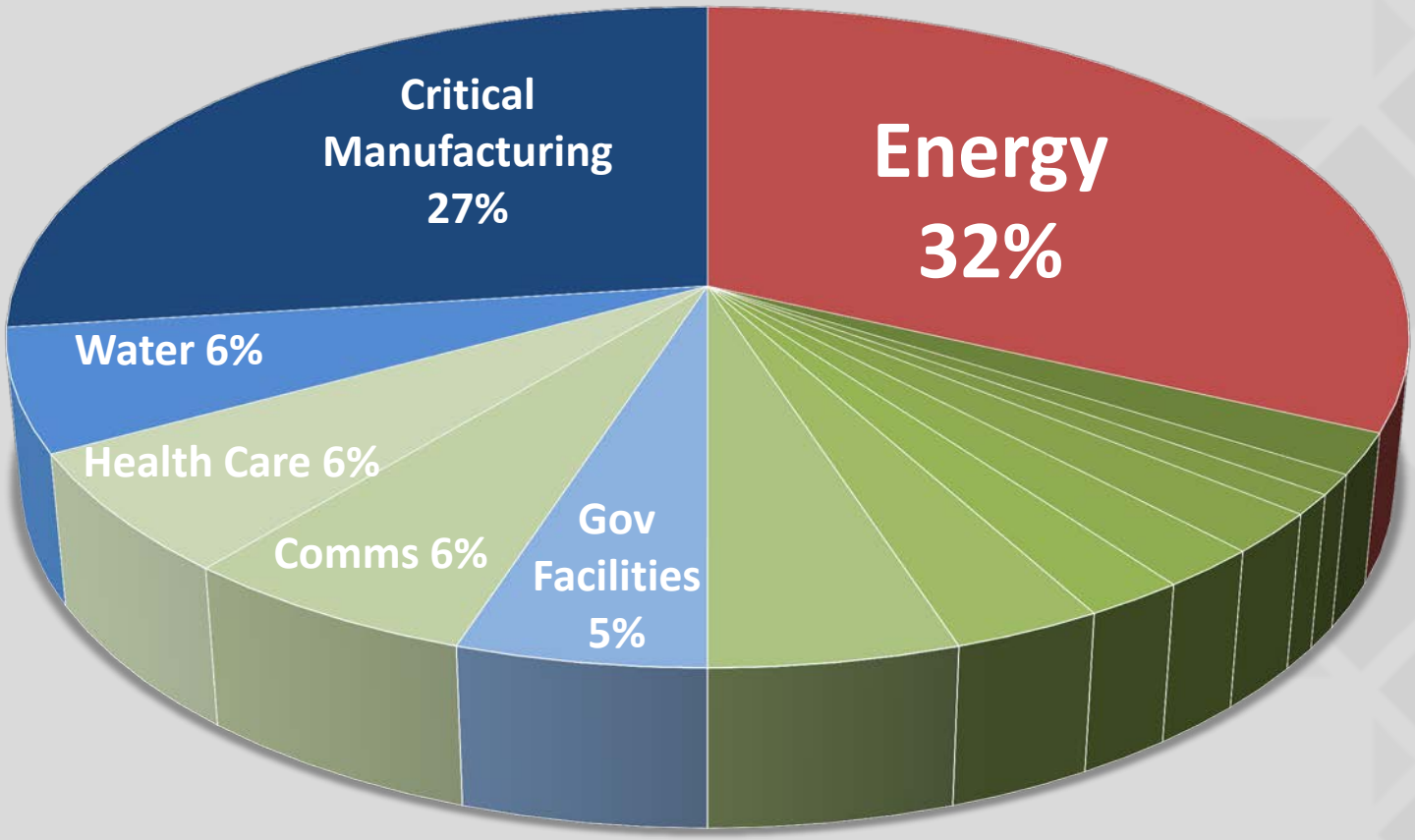
Encryption

Host Based Security

Access Control

Recovery, Patching

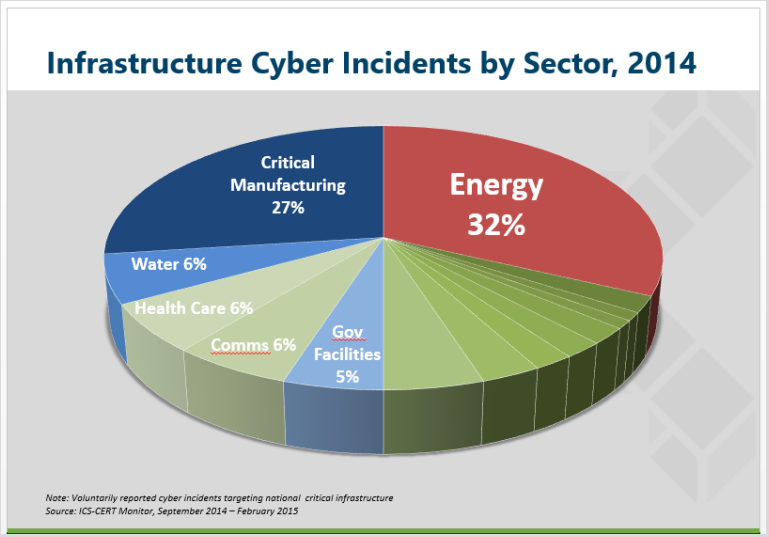
Infrastructure Cyber Incidents by Sector, 2014



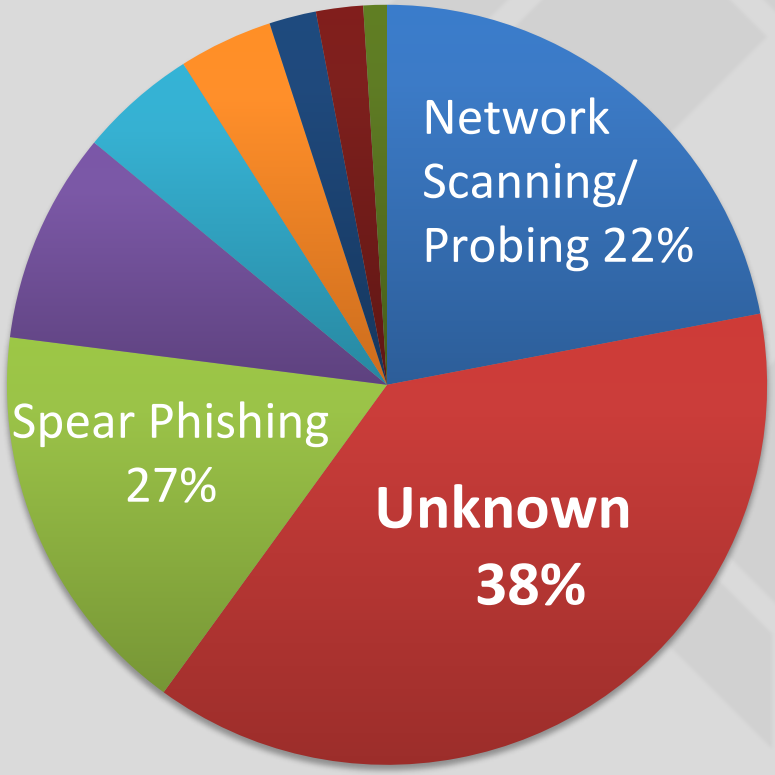
Note: Voluntarily reported cyber incidents targeting national critical infrastructure
Source: ICS-CERT Monitor, September 2014 – February 2015

Industrial Control System Monitoring

Majority of ICS-CERT Incidents - Unknown Origins
SPIDERS Camp Smith – Delivers Monitoring and Forensics Capabilities



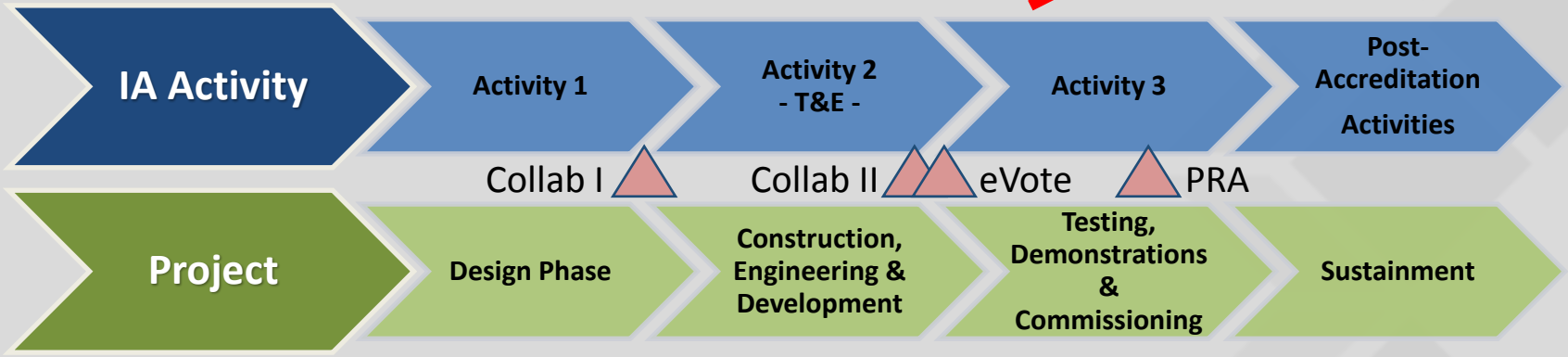
Incidents by Access Vector



Note: Voluntarily reported cyber incidents targeting national critical infrastructure
Source: ICS-CERT Monitor, September 2014 – February 2015

Camp Smith Accreditation

APPROVED



Activity 1

Establish Team

Register the System

Initiate eMASS package

Initiate Security Plan

Select Controls

Activity 2

Implement Controls

Develop Security Plan

eMASS Entries and Artifacts

Testing & Evaluation

Generate Risk Assessment Report & POAM

Activity 3

Hold eVOTE of Collab II

Mitigate Remaining Findings

Receive PRA

System Owner Acceptance

CSET Report

Camp Smith Lessons Learned, Confirmed

Early Collaboration

- Identification and early engagement of the future system owner
- Platform Enclave Leads and Administrators
- Cross-functional Team

Testing & Evaluation

- Independent Testing Important
- Controls validation and penetration yielded unique findings

Security Measures

- Host-based Security
- Network Segmentation/Enclaving

Dr. Darrell Massie
darrell.massie@IPERC.com
www.IPERC.com

Aura Lee Keating
auralee.keating@IPERC.com
www.IPERC.com

GridMaster™ Features & Capabilities

- Proprietary IPERC microgrid control unit
- Includes:
  - Single-board computer
  - Component interfaces
  - Communication interfaces
  - Hosted software
- Designed and tested for extreme conditions

Why Microgrids? Infrastructure is Exposed

San Jose Mercury News

Experts: Sniper attack on PG&E site points to power grid's vulnerability to terrorism

By Steve Johnson

sjohnson@mercurynews.com

POSTED: 02/05/2014 06:45:20 PM PST | UPDATED: 5 DAYS AGO

A sophisticated sniper attack in April that riddled PG&E's Metcalf power substation in South San Jose with bullets may have been an act of domestic terrorism, two experts say, underlining concern that the nation's electricity grid is vulnerable to sabotage.

While the FBI says there is no evidence that terrorists were involved, Jon Wellinghoff, former chairman of the Federal Energy Regulatory Commission, said the attack was "very well planned and well executed by very highly trained individuals," a conclusion shared by a top PG&E official. Wellinghoff added that "a coordinated attack could put this country in a world of hurt for a long time."

Based on his review of the evidence and a tour of the Metcalf plant with some military experts, he said the assault was "the most significant incident of domestic terrorism involving the grid that has occurred" in North America.

But the FBI, which is the primary agency looking into the incident -- doesn't share his conviction.

"We do not believe it is related to domestic or international terrorists," said FBI spokesman Peter Lee, noting that the case is still under investigation and no one has been arrested. He added that there is no evidence linking it to several other attacks on the power grid in Arkansas, where a man undergoing psychiatric evaluation was charged with the crimes last year.

PG&E spokesman Brian Swanson

"…a coordinated attack could put this country in a world of hurt for a long time."

Source: http://www.mercurynews.com/crime-courts/ci_25072628/attack-pg-e-substation-sparks-concerns-about-possible

Inner and Outer Microgrids