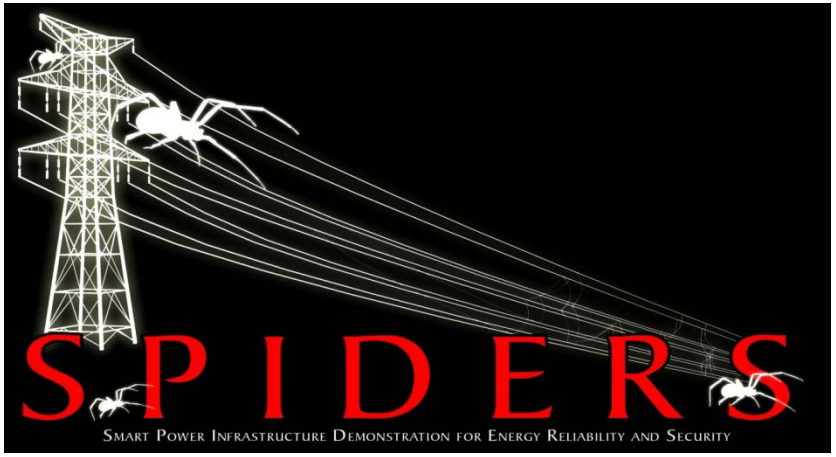


Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS)

Cyber Defense Overview Brief

Mr. Ross Roley
PACOM Energy Innovation Office Lead
SPIDERS Operational Manager
April 2014

UNCLASSIFIED

SPIDERS Summary

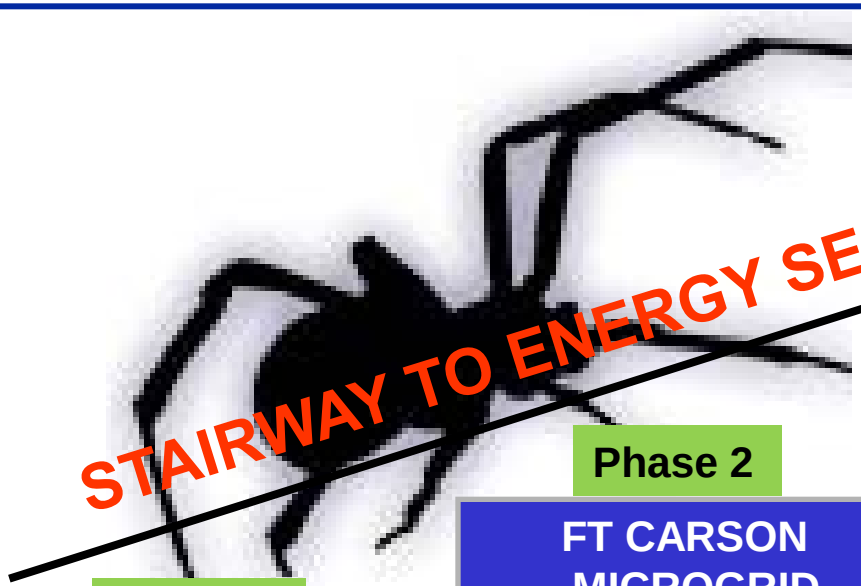
The ability of today's warfighter to command, control, deploy, and sustain forces is adversely impacted by a fragile, aging, and fossil fuel dependent electricity grid, posing a significant threat to national security.

The SPIDERS JCTD addresses four critical requirements:

- Protect task critical assets from loss of power due to cyber attack
- Integrate renewable and other distributed generation electricity to power task critical assets in times of emergency
- Sustain critical operations during prolonged power outages
- Manage installation electrical power and consumption efficiently to reduce petroleum demand, carbon "bootprint," and cost

The modern military needs to evolve its power infrastructure. New threats demand new defenses

SPIDERS Program Summary



STAIRWAY TO ENERGY SECURE INSTALLATIONS

Phase 1

PEARL-HICKAM CIRCUIT LVL DEMO

- Renewables
- Energy Management
- SCADA Cyber Test at DOE National Laboratories

Phase 2

FT CARSON MICROGRID

- Large Scale Renewables
- Vehicle-to-Grid
- Smart Microgrid
- Critical Assets
- CONUS Homeland Defense Demo

Phase 3

CAMP SMITH ENERGY ISLAND

- Entire Installation Smart Microgrid
- Islanded Installation
- High Penetration of Renewables
- Demand-Side Management
- Redundant Backup Power
- Makani Pahili Exercise

TRANSITION

- Template for DoD-wide implementation
- CONOPS
- TTPs
- Training Plans
- DoD Adds Specs to GSA Schedule
- Transition to Commercial Sector
- Transition Cyber-Security to Federal Sector and Utilities

CYBER SECURITY BEST PRACTICES

RIGOROUS ASSESSMENT WITH RED TEAMING IN EACH PHASE

SPIDERS Cyber Development Framework

Implementation

SNL/ORNL:

- "Reference Architecture" in preliminary design for Phase 2 (early draft) and 3 (more mature)

CERL:

- Develops solicitation language for each phase

Integration contractors:

- Completes and builds design, supports system owner in accreditation

Experimentation/ Assessment

PACOM:

- Cyber experiments in lab and on live microgrid for each phase

DHS/INL:

- CSET assessments X 3

PNNL:

- Operational Demonstration including cyber assessment in each phase
- Static code analysis in Phase 2 and 3

Transition

NAVFAC EXWC:

- Coordinating with ongoing Navy (and other) ICS cyber efforts
- Future integration into enterprise ICS network
- Providing data to OSD I&E's EEIM TWG to support DoD ICS cyber standards

SPIDERS Cyber Assessment Events

Cyber Security Event	FY 2011			FY2012				FY2013				FY2014				FY2015			
	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q
0.1: Red Team Lab Experiment – Idaho National Lab		INL																	
1.1: Vulnerability Assessment – JBPHH, HI									HI										
1.2: Red Team Lab Experiment – Sandia National Labs								SNL											
1.3: Red Team Live Microgrid Experiment – JBPHH									HI										
2.1: Vulnerability Assessment – Fort Carson, CO											CO								
2.2: Red Team Lab Experiment – IPERC, Boulder, CO													CO						
2.3: Red Team Live Microgrid Experiment – Ft Carson														CO					
3.1: Vulnerability Assessment – Camp Smith, HI																		HI	
3.2: Red Team Lab Experiment – TBD																SNL			
3.3: Red Team Live Microgrid Experiment – Camp Smith																			HI

Completed: **Planned:** **In Conjunction with J-BASICS:**

Cyber Assessment Event 1.2
Reference Architecture Experiment Construct

Experimental Question: How do changes in compliance and access level affect the effectiveness and security of the different microgrid control network architectures (flat and enclaved)?

Independent Variables (factors that were varied)

1. Architecture:
   - Flat network
   - Enclaved network (based on Reference Architecture)
2. Adversary Access:
   - Low, medium and high
3. Network Compliance:
   - Compliant, non-compliant

Dependent Variable (response that was measured)

1. Effectiveness of network security
   - Score of 0 – 3 for confidentiality, integrity and availability for each data exchange