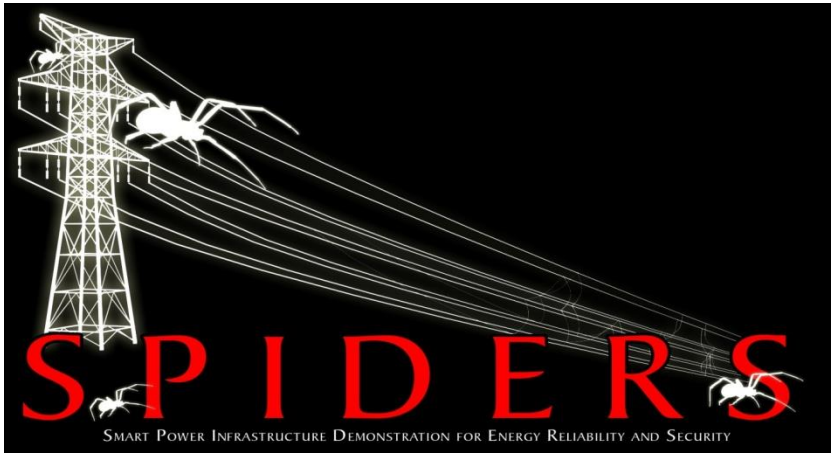


Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS)

Cyber Experimentation Overview Brief

Mr. Ross Roley
PACOM Energy Innovation Office Lead
SPIDERS Operational Manager
August 2015

SPIDERS Summary

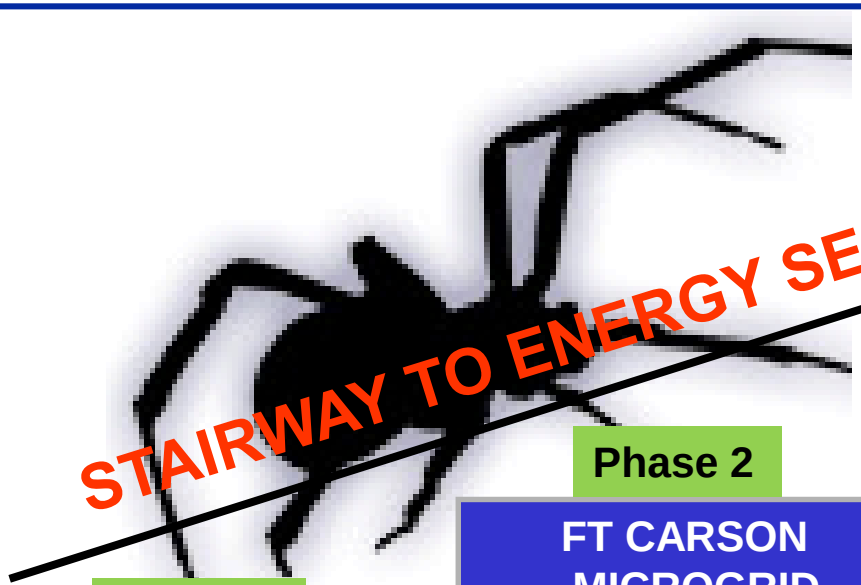
The ability of today's warfighter to command, control, deploy, and sustain forces is adversely impacted by a fragile, aging, and fossil fuel dependent electricity grid, posing a significant threat to national security.

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 with 25 Times Greater Reliability

TRANSITION

- Template for DoD-wide implementation
- Concept of Operation (CONOPS)
- Tactics, Techniques and Procedures (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

Sandia/Oak Ridge National Labs:

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

Corps of Engineers:

- Develops solicitation language for each phase

Integration contractors:

- Completes and builds design, supports system owner in accreditation

Experimentation/ Assessment

U.S. Pacific Command:

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

DHS/Idaho National Lab:

- CSET assessments X 3

Pacific Northwest Nat'l Lab:

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

Transition

Naval Facilities Engineering Command (NAVFAC):

- 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 – 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 #1 – Sandia																SNL			
3.3: Red Team Lab Experiment #2 – Sandia																		SNL	

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)

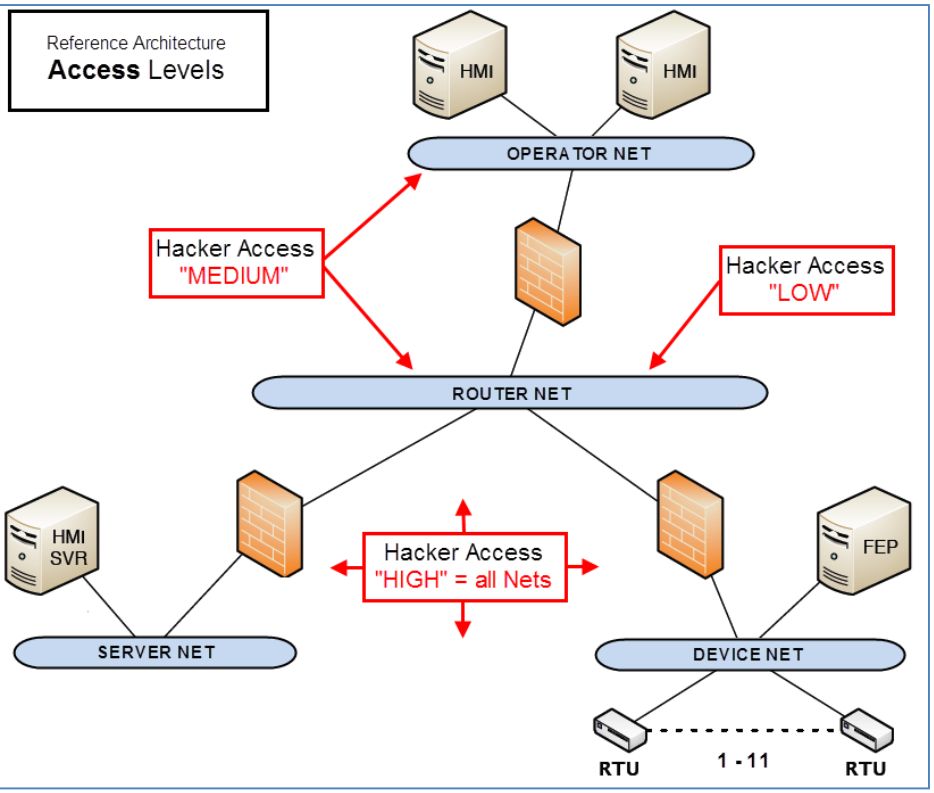
1. Architecture:
   - Flat network
   - Enclaved network (based on Reference Architecture)
2. Adversary Access:
   - Low, medium and high
3. Network Compliance:
   - Compliant, non-compliant

Dependent Variable (response that was measured)

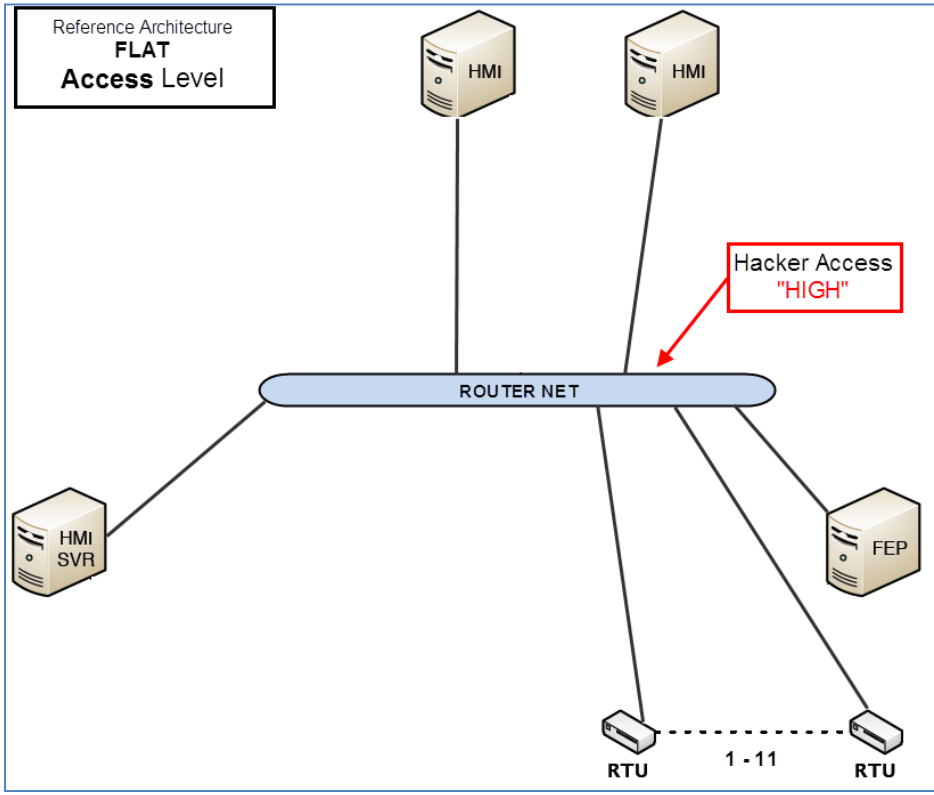
1. Effectiveness of network security
   - Score of 0 – 3 for confidentiality, integrity and availability for each data exchange

Cyber Assessment Event 1.2
Reference Architecture Experiment Networks

Enclaved Network



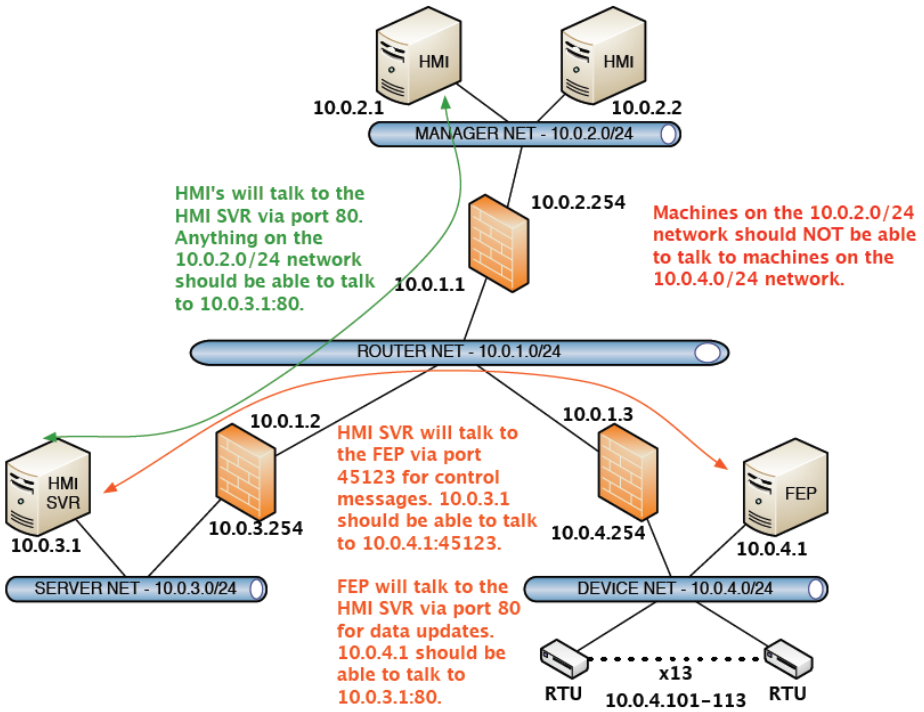
Flat Network



A “compliant” and “non-compliant” version of each network was built. The “non-compliant” network included common Industrial Control System (ICS) vulnerabilities.

Cyber Assessment Event 1.2
Reference Architecture Experiment Scoring

Networks scored points for successful defense of data exchanges against the red teams.



Reference Architecture Data Exchange Scores

Cyber Experiment Scoring Opportunities		
Human-Machine Interface Client/Human-Machine Interface Server		
Information Assurance Required	Read	Write
Confidentiality	medium (2)	medium (2)
Integrity	high (3)	medium (2)
Availability	medium (2)	medium (2)
Maximum Score - 13	7	6
Human-Machine Interface Server/Front-End Processor		
Information Assurance Required	Read	Write
Confidentiality	medium (2)	medium (2)
Integrity	high (3)	medium (2)
Availability	medium (2)	medium (2)
Maximum Score - 13	7	6
Front-End Processor/Remote Terminal Units		
Information Assurance Required	Read	Write
Confidentiality	low (1)	medium (2)
Integrity	high (3)	high (3)
Availability	high (3)	high (3)
Maximum Score - 15	7	8

Cyber Assessment Event 1.2
Reference Architecture Experiment Results

Key Takeaways:

If attacker has limited network access points:

- Enclaving improves network security
- Enclaving mitigates vulnerabilities of non-compliant networks

Lesson Learned:

- Validated scoring system and test methodology

Architecture/Score	Availability (Max: 14)	Confidentiality (Max: 11)	Integrity (Max: 16)	Total Score (Max:41)	Percentage (Max: 100)
Flat/Non-Compliant (All Access)*	0	0	8	8	**19.5%**
Flat/Compliant (All Access)*	0	9	14	23	**56.1%**
Enclaved/ Non-Compliant/ High Access	0	0	8	8	**19.5%**
Enclaved/ Compliant/ High Access	0	9	14	23	**56.1%**
Enclaved/ Non-Compliant/ Medium Access	6	7	11	24	**58.5%**
Enclaved/ Compliant/ Medium Access	6	9	14	29	**70.7%**
Enclaved/ Non-Compliant/ Low Access	6	11	16	33	**80.5%**
Enclaved/ Compliant/ Low Access	6	11	16	33	**80.5%**

Cyber Assessment Event 1.3
JBPHH Red Team Experiment Results

Key Takeaways:

SPIDERS JBPHH microgrid cyber security rated as "Excellent"

- Validated the results from the lab
- Unable to vary architecture, compliance and access
- N/A for integrity due to Rules of Engagement

Lesson Learned:

- Further validated scoring system and test methodology
- Demonstrated the ability to experiment on a live microgrid with ROE
- 10x more richness of data in the lab than on a live microgrid (2 data points versus 24) due to ROE and configuration constraints

Cyber Assessment Event 2.2
Vendor Lab Experiment Construct

Experimental Question: How do changes in various hardware and system operating methodologies affect the functionality and security of the different SPIDERS architectures?

Independent Variables (factors that were varied)

1. Whitelisting:
   - None
   - Medium
   - Medium-High
   - High
2. Throttling the Data Rate:
   - Throttled (10/100 Mb) versus Un-throttled (10/100/1000 Mb)
3. Enclaving:
   - 1 versus 2 Enclaves
4. Access:
   - Network Switch versus HMI

Dependent Variables (responses that were measured)

1. Effectiveness of network security
   - Score (0–3) for confidentiality, integrity & availability of each exchange
   - Latency of data traffic

Cyber Assessment Event 2.2
Vendor Lab Experiment Results

Key Takeaways:

Overall security assessed as "Excellent"

- Whitelisting improves network security
- Throttling improves network security

Lessons Learned:

- Encryption prevents red team from impacting confidentiality and integrity
- IPv6 limits red team attack options
- Microgrid on/off has no effect on red team success
- Instituted latency scoring

Architecture/Score	No White-listing	Medium White-listing	Med-High White-listing	High White-listing	Total
Switch/ 2 enclaves/ Throttled	81%	96%	N/A	96%	**91%**
Switch/ 2 enclaves/ Un-throttled	81%	88%	88%	88%	**87%**
Switch/ 1 enclave/ Un-throttled	88%	88%	88%	81%	**87%**
HMI/ 2 enclaves/ Un-throttled	96%	88%	96%	88%	**92%**
Total	87%	90%	91%	88%	

Cyber Assessment Event 2.3
Fort Carson Red Team Experiment

Key Concepts:

- Validated the results from the IPERC lab
- Strict rules of engagement
- Compare throttling strategies
- 2nd ever DoD red team event on a live microgrid
- CIA scoring system needs refinement