

# 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.

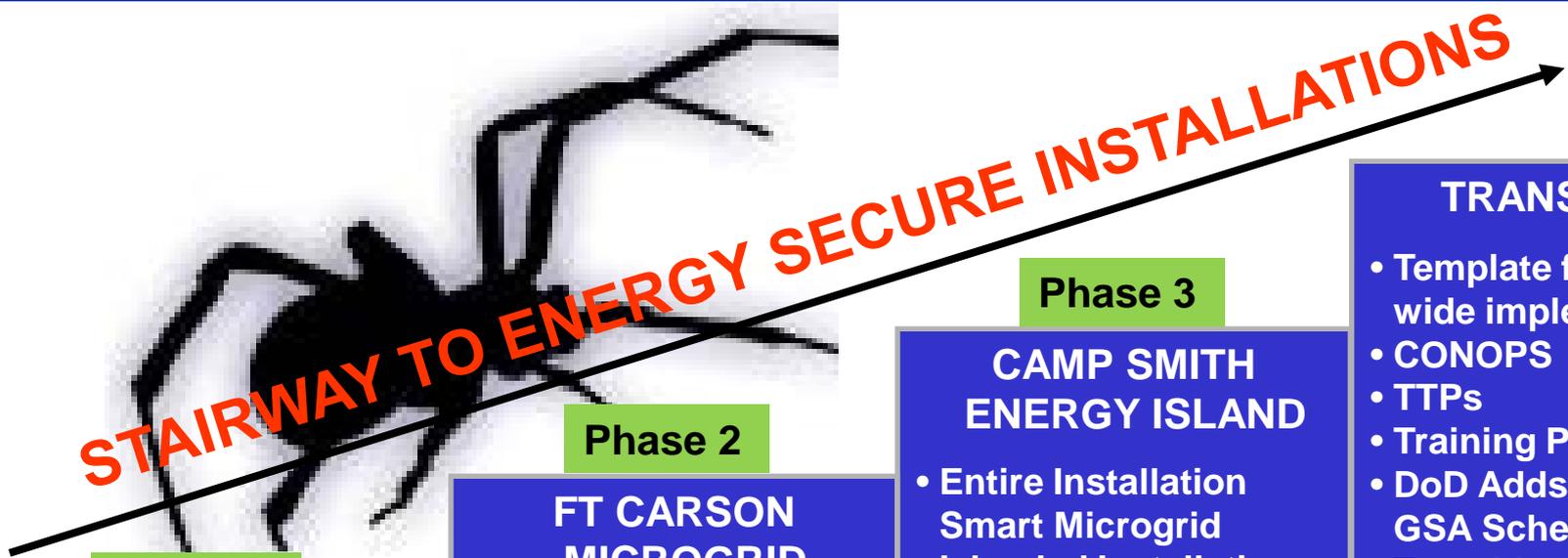
The SPIDERS ICTD addresses four critical requirements:

- 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 "footprint," and cost

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



# SPIDERS Program Summary



## 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

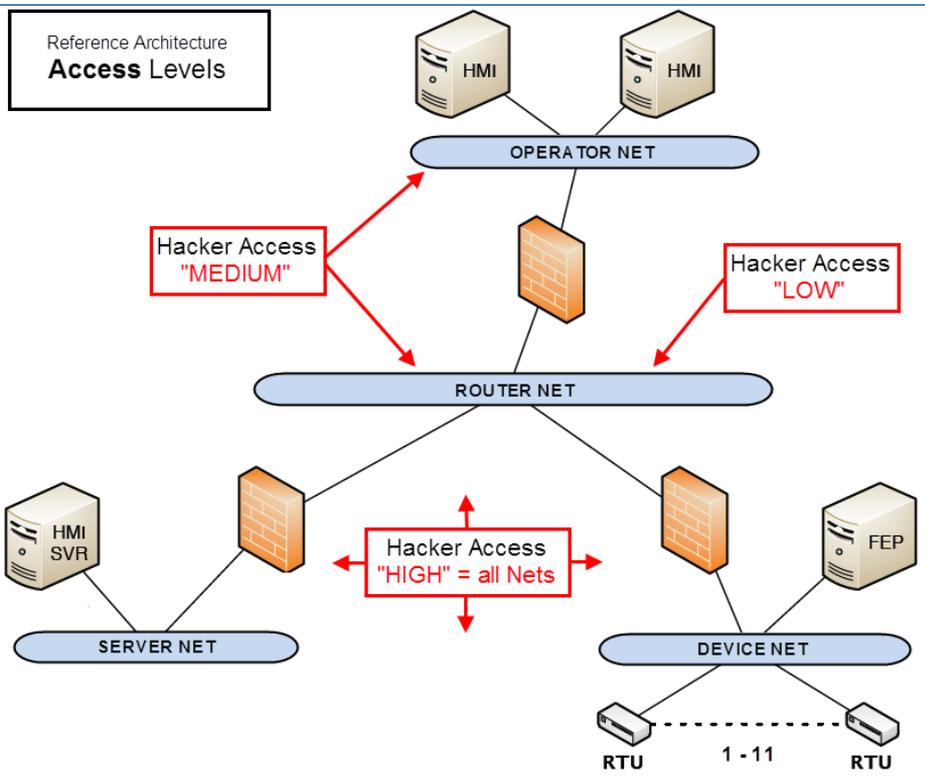
UNCLASSIFIED



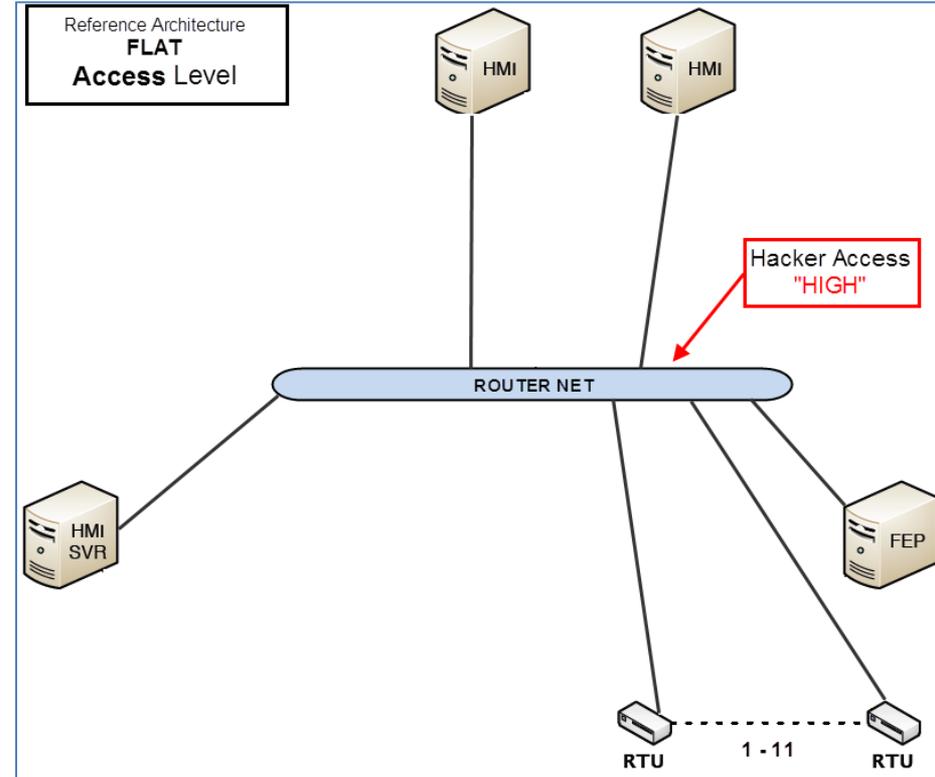
# Cyber Assessment Event 1.2

## 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 ICS vulnerabilities.

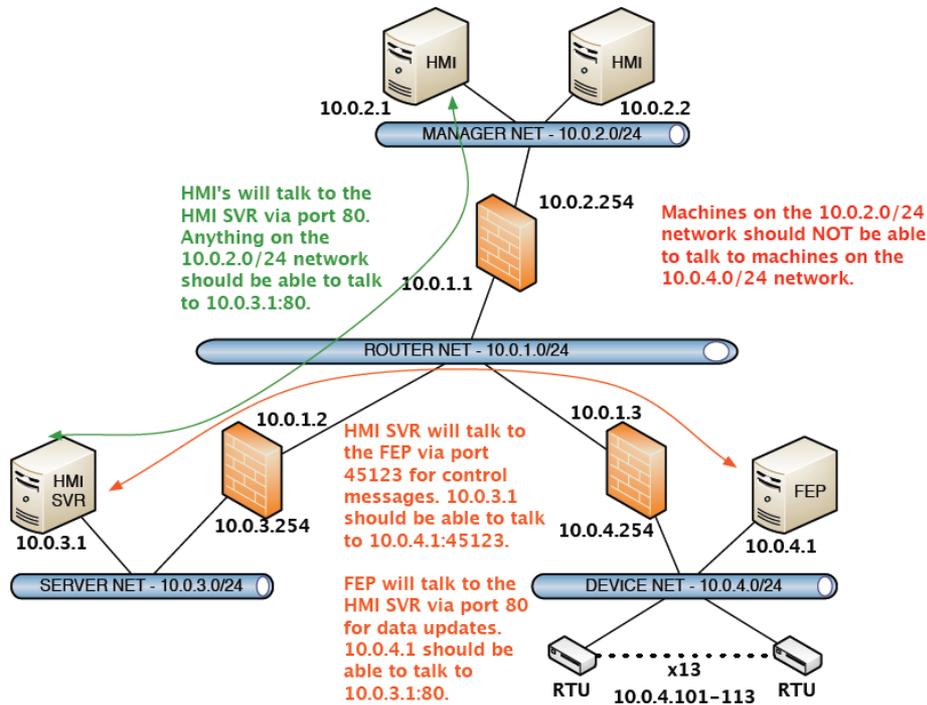
UNCLASSIFIED



# 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

UNCLASSIFIED

# 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%

UNCLASSIFIED



# Cyber Assessment Event 1.3

## JBPHH Red Team Experiment Results

### Key Takeaways:

SPIDERS JBPHH microgrid cyber security rated as **“Excellent”**

- Unable to vary architecture, compliance and access
- N/A for integrity due to ROE
- Max for Confidentiality due to encryption

### Lesson Learned:

- Further validated scoring system and test methodology
- Demonstrated the ability to experiment on a **live microgrid** with ROE

Architecture/Score	Availability (Max: 15)	Confidentiality (Max: 9)	Integrity (Max:N/A)	Total Score (Max:24)	Percentage (Max: 100)
Flat/Non-Compliant (All Access)*	N/A	N/A	N/A	N/A	N/A
Flat/Compliant (All Access)*	0	9	N/A	9	37.5%
Enclaved/Non-Compliant/High Access	N/A	N/A	N/A	N/A	N/A
Enclaved/Compliant/High Access	N/A	N/A	N/A	N/A	N/A
Enclaved/Non-Compliant/Medium Access	N/A	N/A	N/A	N/A	N/A
Enclaved/Compliant/Medium Access	N/A	N/A	N/A	N/A	N/A
Enclaved/Non-Compliant/Low Access	N/A	N/A	N/A	N/A	N/A
Enclaved/Compliant/Low Access	N/A	N/A	N/A	N/A	N/A

UNCLASSIFIED



# Cyber Assessment Event 2.2

## IPERC 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 (same as JBPHH)
  - Medium (same as Fort Carson)
  - Medium-High (Experimental)
  - High (Proposed for Camp Smith)
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

UNCLASSIFIED



# Cyber Assessment Event 2.2

## IPERC 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
- **Validated** scoring system and test methodology
- 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%	<b>91%</b>
Switch/ 2 enclaves/ Un-throttled	81%	88%	88%	88%	<b>87%</b>
Switch/ 1 enclave/ Un-throttled	88%	88%	88%	81%	<b>87%</b>
HMI/ 2 enclaves/ Un-throttled	96%	88%	96%	88%	<b>92%</b>
Total	87%	90%	91%	88%	

UNCLASSIFIED



# Cyber Assessment Event 2.3

## Fort Carson Red Team Experiment

### Key Concepts:

- **Validate** the results from the IPERC lab
- **Strict rules of engagement**
- Compare throttling strategies
- 2<sup>nd</sup> ever DoD red team event on a **live** microgrid

Architecture/Score	No White-listing	Medium White-listing	Med-High White-listing	High White-listing	Total
Switch/ 1 enclave/ Throttled	N/A	?%	N/A	N/A	?%
Switch/ 2 enclaves/ Un-throttled	N/A	N/A	N/A	N/A	N/A
Switch/ 1 enclave/ Un-throttled	N/A	?%	N/A	N/A	?%
HMI/ 2 enclaves/ Un-throttled	N/A	N/A	N/A	N/A	N/A
Total	N/A	?%	N/A	N/A	

UNCLASSIFIED



# BACKUP Slides

UNCLASSIFIED



# SPIDERS Phase 2 Cyber Experimentation Objectives

## **Objectives for Events 2.2 and 2.3 (IPERC and Ft. Carson):**

1. Support SPIDERS JCTD objectives
2. Mitigate risk by vetting candidate cyber security solutions before implementation on live DoD grids
3. Provide lessons learned for Camp Smith microgrid cyber design
4. Make quantitative and statistically meaningful comparisons of the cyber security attributes of candidate solutions of different modality
5. Make qualitative comparisons of other aspects of the candidate solutions (e.g. practicality, scalability)
6. Demonstrate functionality of candidate solutions
7. Build knowledge and gain insight for potential follow-on experiments/demonstrations and design work
8. Identify vulnerabilities and recommend mitigation solutions
9. Provide feedback to DIACAP and Platform IT accreditation policymakers

UNCLASSIFIED



# Fort Carson Live Microgrid Cyber Experiment

## Scenario Rules of Engagement

### **ROE for Event 2.3 (Fort Carson, CO):**

1. Conduct the experiment in both SPIDERS microgrid mode with no generators running and the control system operating in the background and also in grid connected mode during Industry Day demonstrations
2. Department of Public Works (DPW) will preconfigure the electrical distribution system switching to limit the operation to the designed microgrid designed boundaries
3. Incorporate items discovered in the IPERC lab experiment during SPIDERS microgrid mode periods of operation. These may be tested as a specific excursion with the microgrid running at Ft Carson and with approval of DPW
4. No devices will be added to the SPIDERS microgrid that change the function of the architecture
5. There will be no scoring of the integrity metric for this experiment (with the exception of Rule #4 below); limited scoring of the availability metric and full scoring of the confidentiality metric
6. Red team integrity attempts (control message injection) of IPC6-10 (EVSEs) are allowed for demonstration purposes
7. No physical changes to the wiring are allowed
8. Access to the network will only be allowed through the opened Ethernet ports on the HMI (access point #1) and the network switch (access point #2)

**UNCLASSIFIED**



# Fort Carson Live Microgrid Cyber Experiment

## Red Team Rules of Engagement

### **Red Team ROE for Event 2.3 (Fort Carson, CO):**

1. Operating System level exploits of Linux and Windows operating systems (HMI, GUI server, and IPCs) are off-limits
2. Probes of IPCs6-10 (EVSEs) are allowed, but other IPCs should be avoided
3. Fuzzing or randomly changing bytes is off-limits (TBD based on results of the lab experiment)
4. Man in the middle attacks will only be used to intercept and disrupt data exchanges. They will not be used to manipulate or inject data
5. Use of BreakingPoint by the red team is not allowed (pending lab results, and will be allowed only to a comfortable level of stress based on the lab results)
6. A “black list” of IPs that are off limits will be given to the red team once initial network mapping demonstration has been completed as well as a “white list” of IPs that are available as targets

UNCLASSIFIED