Transitioning SPIDERS JCTD

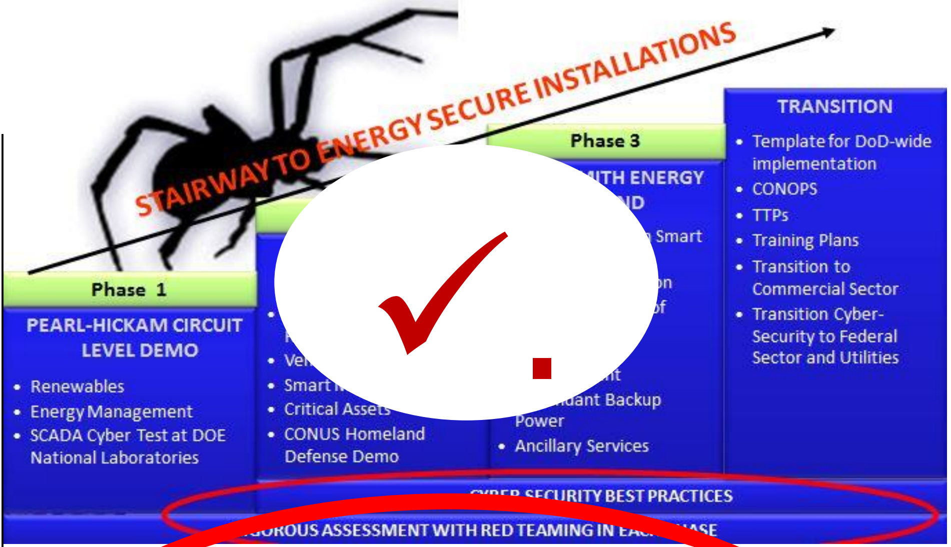
Bill Anderson, XM, California Trapdoor Spider
Director, Utilities Engineering & Management
NAVFAC EXWC Port Hueneme, CA
[bill.anderson1@navy.mil]

SMART POWER INFRASTRUCTURE DEMONSTRATION FOR ENERGY RELIABILITY AND SECURITY (SPIDERS) JOINT CAPABILITY TECNOLOGY DEMONSTRATION (JCTD)

Description

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.

- ❑ **Objective, demo to:**
- ✓ **Protect task cri power due to cyber-attack.**
- ✓ **Integrate rene d energy generation concepts to po times of emergency.**
- ✓ **Sustain critical o onged power outages.**
- ✓ **Manage installation e er and consumption efficiency, to reduce petroleum demand, carbon "bootprint," and cost.**



STAIRWAY TO ENERGY SECURE INSTALLATIONS
Phase 1
PEARL-HICKAM CIRCUIT LEVEL DEMO
• Renewables
• Energy Management
• SCADA Cyber Test at DOE National Laboratories
• Ve
• Smart
• Critical Assets
• CONUS Homeland Defense Demo
Phase 3
ITH ENERGY
ND
Smart
on
of
nt
ndant Backup Power
• Ancillary Services
TRANSITION
• Template for DoD-wide implementation
• CONOPS
• TTPs
• Training Plans
• Transition to Commercial Sector
• Transition Cyber-Security to Federal Sector and Utilities
CYBER SECURITY BEST PRACTICES
OROUS ASSESSMENT WITH RED TEAMING IN EA ASE

Benefits & Capabilities

- ✓ **Reduction on e ction on operational costs associ n loss**
- ✓ **Minimize ch ucture and maximize us**
- ✓ **Avoid unnece ailure points**
- ✓ **Minimize disrupt stallation operations during construction and testing**
- ✓ **Provide "N+1" generation redundancy for critical operations**
- ✓ **Do No Harm: Built in fail safe modes revert to traditional (facility-dedicated) back up power operations**

Key Transition Products and Deliverables

Military:

- ✓ **Three Demonstration Microgrids --Tested and Operational (JBPHH, Ft. Carson and Camp Smith)**
- ✓ **Full Project Documentation for each**

DOE, DHS & Industry:

- ✓ **Three "Industry Day" events (over 400 attendees) with technology presentations and project tours.**
- ✓ **Project Documentation and Reports (Posted on SPIDERS JCTD website)**
- ✓ **Input to UFC 4-010-06 CYBERSECURITY (Pre-Final target 30 September '15)**

Project Documents:

Documents for Secure NORTHCOM Portal

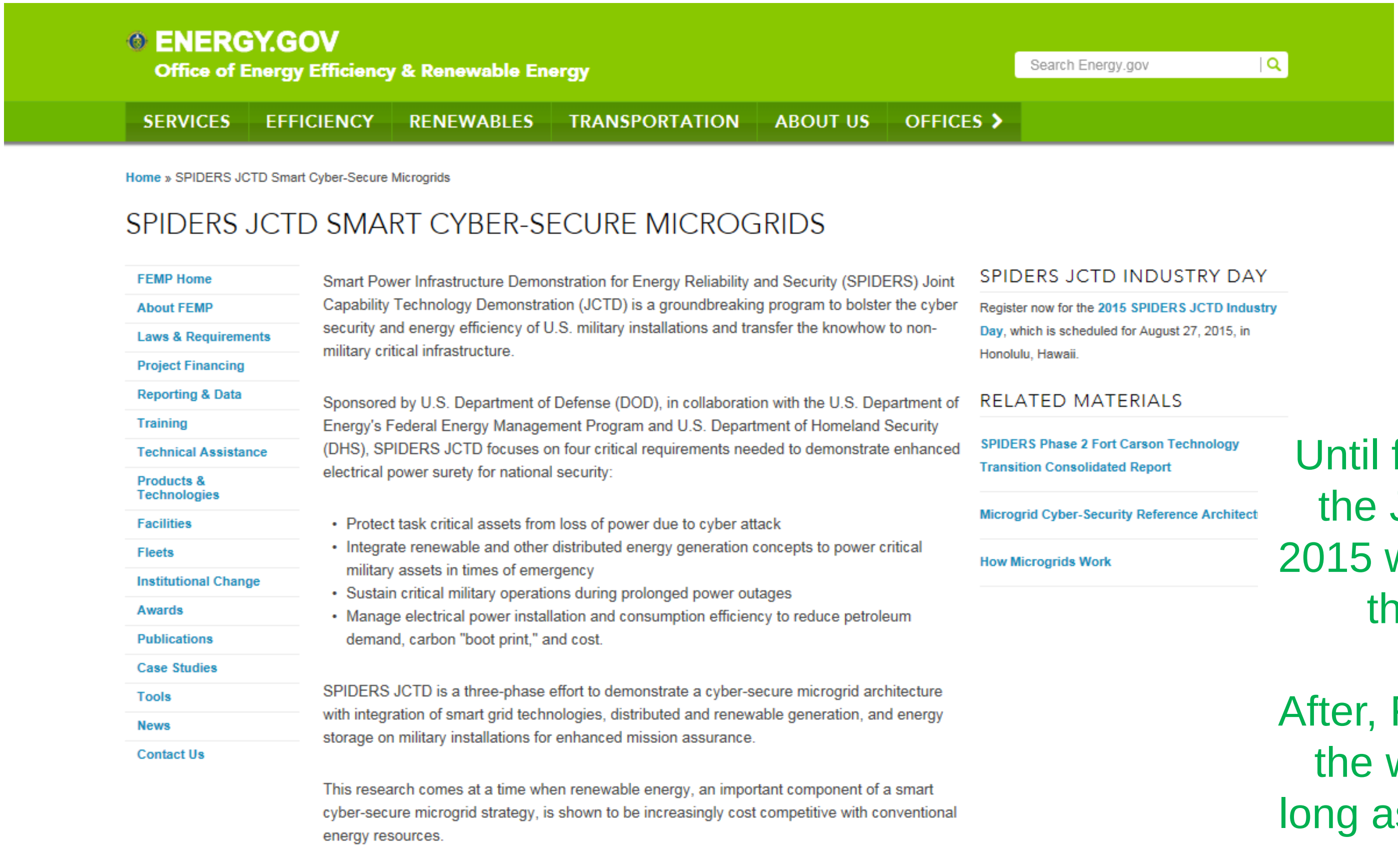
1. Engineers Report
2. Utility Assessment
3. Transition Agreement
4. Cyber Report
5. CONOPS
6. O&M Manual
7. Training Report
8. Industry Day Presentations

Public Information

1. Phase 1&2 Public Report
2. Industry Day Presentations (cleared)
3. Phase 3 / Project Summary Report
4. UFC 4-010-06 CYBERSECURITY, currently in review, Pre-Final Version 30-Sept.

SPIDERS JCTD Website “Landing Pad”

Links to JCTD documents & related information



Home » SPIDERS JCTD Smart Cyber-Secure Microgrids

SPIDERS JCTD SMART CYBER-SECURE MICROGRIDS

Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) Joint Capability Technology Demonstration (JCTD) is a groundbreaking program to bolster the cyber security and energy efficiency of U.S. military installations and transfer the knowhow to non-military critical infrastructure.

Sponsored by U.S. Department of Defense (DOD), in collaboration with the U.S. Department of Energy's Federal Energy Management Program and U.S. Department of Homeland Security (DHS), SPIDERS JCTD focuses on four critical requirements needed to demonstrate enhanced electrical power surety for national security:

- Protect task critical assets from loss of power due to cyber attack
- Integrate renewable and other distributed energy generation concepts to power critical military assets in times of emergency
- Sustain critical military operations during prolonged power outages
- Manage electrical power installation and consumption efficiency to reduce petroleum demand, carbon "boot print," and cost.

SPIDERS JCTD is a three-phase effort to demonstrate a cyber-secure microgrid architecture with integration of smart grid technologies, distributed and renewable generation, and energy storage on military installations for enhanced mission assurance.

This research comes at a time when renewable energy, an important component of a smart cyber-secure microgrid strategy, is shown to be increasingly cost competitive with conventional energy resources.

SPIDERS JCTD INDUSTRY DAY

Register now for the 2015 SPIDERS JCTD Industry Day, which is scheduled for August 27, 2015, in Honolulu, Hawaii.

RELATED MATERIALS

SPIDERS Phase 2 Fort Carson Technology Transition Consolidated Report

Microgrid Cyber-Security Reference Architect

How Microgrids Work

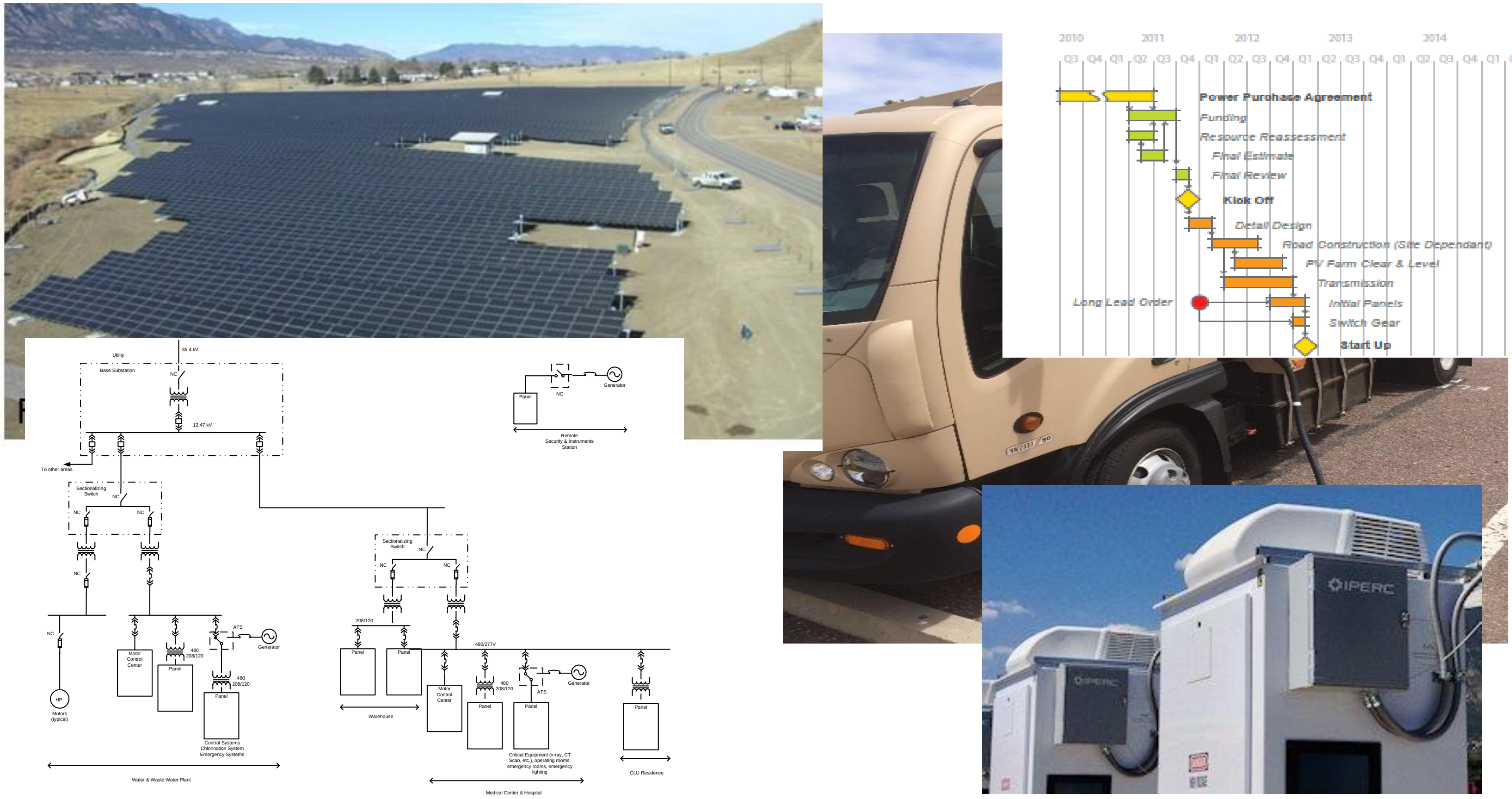
Until final closure of the JCTD in Dec. 2015 we will maintain the website.

After, FEMP will keep the website up as long as information is relevant.

http://energy.gov/eere/femp/spiders-jctd-smart-cyber-secure-microgrids

Google: SPIDERS JCTD smart cyber secure microgrids

Reference Microgrid Design
& NAVFAC Microgrid Design Guide



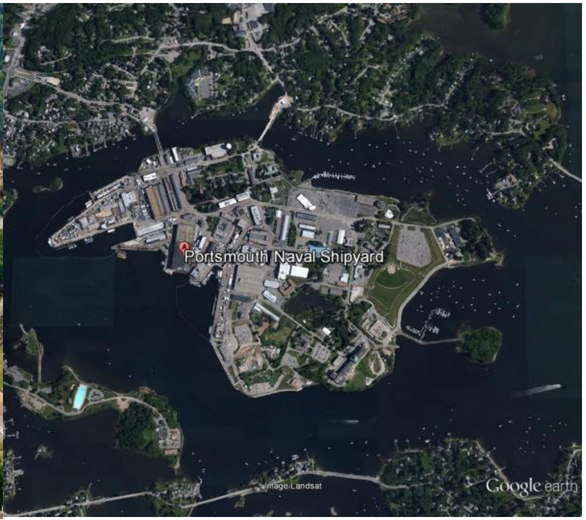
They told me to set up a microgrid!!!!
“Now What??”

Microgrids in Planning

Diego Garcia
Image © 2015 DigitalGlobe
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
© 2015 Google
Google earth

Diego Garcia

Walter Reed
National Military Medical Center
[Bethesda Medical Center]



Portsmouth Naval Shipyard

NAVFAC's DERGOS
(Distributed Energy Resources Grid Optimization Service)
team will be conducting project development support to maximize energy security benefits

Marine Corps Base Camp Pendleton

A few references:

DHS

"DHS Can Make Improvements to Secure Industrial Control Systems"

www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-39_Feb13.pdf

North American Electric Reliability Corporation (NERC),

Cyber Attack Task Force,

http://www.nerc.com/comm/CIPC/Pages/Cyber%20Attack%20Task%20Force%20CATF/Cyber-Attack-Task-Force-CATF.aspx

Final Report

http://energycollection.us/Companies/NERC/Cyber-Attack-Task-Force.pdf

NIST

NISTIR 7628 Revision 1, Guidelines for Smart Grid Cybersecurity (3 volumes)

http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

IEEE,

IEEE Cyber Security Site – Resources, Extensive information

http://cybersecurity.ieee.org/resources.html