Microgrids and Energy Security

Sponsored by

CONSTRUCTION LLC
UNISTA
Moderator: Capt. Michael Blount, P.E., F.SAME, USN (Ret.), Vice President, Federal Division, Balfour Beatty Construction

Speakers:

- Kevin Whitt, P.E., Utilities and Energy Product Line Manager, NAVFAC Atlantic
Grid Security and Microgrid Solutions
Getting on with it...Sustaining the Nation’s Critical Infrastructure after a Catastrophic Grid Event

Presented to the SAME JETC
By: The Honorable William C. (Bill) Anderson
May 21, 2014
Mission First
Mission First

Power is Everything
We Won’t Send our Brightest and Best into a “Fair Fight”
There is an elephant in the room…

The nation’s hardened IT and Comm infrastructure rests on a fragile foundation
How Secure are our National Security Assets?

Of DOD’s 34 most critical global assets, 31 rely on commercially operated electricity grids for their primary source of electricity.

October 2009 GAO report
How Secure are our National Security Assets?

Of DOD’s 34 most critical global assets, 31 rely on commercially operated electricity grids for their primary source of electricity.

October 2009 GAO report

In most cases, neither the grid nor on-base backup power provides sufficient reliability to ensure continuity of critical national priority functions and oversight of strategic missions in the face of a long term (several months) outage.

2008 Defense Science Board Report
So, what’s the source of the risk?

The nation’s grid is our fragile foundation...sources of risk include:

- Natural Disasters...Super Storm Sandy/Hurricane Katrina
- Circuit Overload/Failure...2003 Northeast Blackout
- Solar Flares...Canada 1989
- Cyber Attack
- EMP (Electromagnetic Pulse Detonation)
- Physical attack on grid infrastructure...San Jose sniper attack

- The risk of a long term widespread outage triggered by a manmade event – a theoretical risk a few years ago...very real today
- Grid Technology is the “Achilles Heel”
  - Our system sophistication provides an asymmetric advantage to protagonists who are not as dependent as we are on modern electronics as well as natural events.
  - Reliance on internet-based smart grid technology makes it vulnerable.

So, what happens when the Smart Grid goes dumb?
And the practical effect?

Cold War Era USAF General Curtis LeMay made famous the quote “bomb them back to the stone age”...

• The effect of taking out factories, harbors, bridges, etc.

Today, our lesser capable adversaries can have the same effect by rendering our technologically-advanced assets crippled

…weaponry that leaves a society with no operable infrastructure…maybe the cruelest outcome possible
We Understand the Threat…
So, Where’s the Action?

In light of the increasing threat of cyber-attack, numerous security experts have called on Congress to provide a federal entity with the necessary authority to ensure that the grid is protected from potential cyber-attacks and geomagnetic storms. Despite these calls for action, Congress has not provided any governmental entity with that necessary authority.

May 21, 2013 report by staff of CM Markey and Waxman
Islanding Critical Infrastructure

First question…what is critical infrastructure?

• Answer depends on the length of the outage
Islanding Critical Infrastructure

First question…what is critical infrastructure?

- Answer depends on the length of the outage

The ability to operate strategic assets for long duration fully disconnected from the grid essential in the maintenance of national security

- Local autonomy over power generation source, distribution assets and infrastructure served
- Local feedstocks for generation assets a must
- Community assets supporting the strategic assets must be considered

Advanced Hybrid Microgrids Offer the Solution
Islanding Critical Infrastructure

First question…what is critical infrastructure?
• Answer depends on the length of the outage

<table>
<thead>
<tr>
<th>LEVEL 4</th>
<th>&gt;1 MONTH</th>
<th>Home Fatigue</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Supporting Essentials of Home Life</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Long-Term Medical</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEVEL 3</th>
<th>1 MONTH</th>
<th>Personal Operations Support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Support of Nutrition, Sleep, Hygiene</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clinic Level Medical</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEVEL 2</th>
<th>1 WEEK</th>
<th>Operational Support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Systems Supporting Intel and Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Medical Triage</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEVEL 1</th>
<th>1 DAY</th>
<th>Mission Critical:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Data Centers/Communication Assets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Area Cooling…Basic First Aid</td>
</tr>
</tbody>
</table>
So, how do we attack the problem?

**Energy Surety** is the cornerstone for implementing local power generation that manages critical assets through Microgrid technologies.

- **Goal:**
  - Secure/resilient IT and communication assets *require* secure/resilient/load managed/power factor conditioned energy.
  - The ability to create energy islands for the long term operation of critical infrastructure is a *must* to provide the appropriate level of supply security.

- **Identify Mission Critical Sites:**
  - Operational Readiness – Homeland Security and Department of Defense
  - Islands of Refuge – Local Community Airports, Hospitals, etc.

- **Leverage Proven Technology:** Microgrid demonstration projects prove the viability of the solution.

- **Budget and Financing:**
  - Move Budgets from standby generation to grid-tied optimized power generation assets
  - Engage private financer’s to offset costs for on-site Generated Power
  - Leverage State Grants: Microgrid, Alternative Energy, etc.

- **Engage Private Public Partners**
  - State, Local Community, Utility, Financial, Federal, Energy Surety Providers
Energy surety is an evolving quest

End-to-End Cost/Platform Flexibility is Critical

Plan long term/turnkey...build in blocks

- Based on priorities and budgets...address multiple needs

Evaluate Microgrid Technology Applications

- Can the technology adapt?
- Flexibility to build a platform in an unrestricted manner?

Leverage Existing Assets:

- Upgraded vs replace...build on what you have

Short term cost versus long term consequences:

- Avoid “proprietary” products, systems and/or designed. Open protocols a must
- Evaluate based on long term life cycle cost
- Service requirements over life of the system..
- Did you lock your self out of have full and open competition on future system upgrades?
Solutions that Seamlessly Integrate with the Grid

- Integrate at IOC
- Primary Grid-Tied Distributed Generation
- Islanded Mode
- Black Start
- Reintegration to Restored Grid
Questions?

The Honorable William C. (Bill) Anderson
Director – Strategy and Business Development
Eaton Corporation
Direct: 202 297 6765
Cell: 202 309 8656
williamcanderson@eaton.com
Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS)

Joint Capabilities Technology Demonstration
SPIDERS Overview

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.

• SPIDERS JCTD Objectives
  • Protect task critical assets from loss of power due to cyber attack
  • Integrate renewables and other distributed energy generation concepts to power task critical assets in times of emergency
  • Sustain critical operations during prolonged power outages
  • Manage installation electrical power and consumption efficiency, to reduce petroleum demand, carbon “bootprint”, and cost

SPIDERS primary objective is mission assurance.
Cyber Threat to Energy Sector

Incidents Reported by Federal Agencies


Major Incidents Reported in FY12

Source: DHS ICS-CERT Monitor Oct-Dec 2012
E.O. 13636 (12 February 2013)

The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.

It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.
Today – Backup Operations

Loss of Backup Generator(s)

- **Mission Critical**
- **Not Mission Critical**
- **Backup Generator (On)**
- **Automatic Transfer Switch**
- **Breaker/Switch**
- **Point of Common Coupling (Main Breaker)**

Diagram:
- MAIN SUBSTATION
- PCC
- BREAKER
- RENEWABLE ENERGY SOURCE
- ATS (SPARE)
- ATS
- ATS
Backup Generator(s) shutdown for Maintenance or Power Optimization

Switches/Breakers controlled by SPIDERS cyber-secure Energy Management System (EMS)

- **Mission Critical**
- **Not Mission Critical**
- **Backup Generator (On)**
- **Automatic Transfer Switch**
- **Breaker/Switch**
- **Point of Common Coupling (Main Breaker)**

**SPIDERS Backup Operations**
Expected SPIDERS Outcomes

PEARL-HICKAM CIRCUIT LVL DEMO
- Renewables (8-9%)
- Two Diesel Gens
- Energy Management
- VSE SCADA Test at Idaho National Lab

FT CARSON MICRO-GRID
- Large Scale Renewables (35-50%)
- Vehicle-to-Grid
- Smart Micro-Grid
- Four Gens
- Cyber Security
- Critical Assets

CAMP SMITH ENERGY ISLAND
- Entire Installation Smart Micro-Grid
- Islanded Installation
- High Penetration of Renewables
- Demand-Side Mgmt
- Redundant Backup Power
- Seven Gens
- Makani Pahili Hurricane Exercise

TRANSITION
- Template for DoD-wide implementation
- CONOPS
- TTPs
- Training Plans
- DoD Unified
- Facilities Criteria
- Transition to Industry
- Transition to Federal Sector and Utilities
- System Architecture
- Cyber-Security

RIGOROUS ASSESSMENT WITH RED TEAMING IN EACH PHASE

UNCLASSIFIED
SPIDERS Technical Progress

Phase 1 – Joint Base Pearl Harbor-Hickam
- Operational Demonstration Completed January 2013
- Cyber assessment conducted in February 2013
- Functional Results
  - **30.4 percent increase in power endurance** based on a fixed quantity of fuel
  - 42 percent reduction in carbon emissions
  - **39.2 fold (3,920%) improvement in power reliability** (expressed as percentage of time the critical load is not served (CLNS))
  - Control System protection functioned as designed

UNCLASSIFIED

147KW SOLAR

MAIN SUBSTATION

ATS

UV Treatment

Waste Water Treatment Plant (WWTP)

Five Vertical Axis Wind Turbines (10kW each)

Hydrogen Refueling Station (HRS)

Fuel Cell

10500 gallon diesel tank (shared)

1500kW Caterpillar diesel

600kW Rolls Royce diesel

2500kVA transformer (11.5kV/480V)

3000kVA transformer (44kV/480V)

Electrolyzer and hydrogen storage (3000kg)
SPIDERS Technical Progress

Phase 2 – Fort Carson
- System Integrator contract award – Awarded June 2012 (Burns & McDonnell)
- Lessons in Renewable Energy Penetration of greater than 50 percent
- Control System Cyber Security - Accreditation
- Plug-In Electric Vehicles (PEV)
  - Energy Storage - 80 to 120 KWh each
  - Two-way charging stations
  - Mobile “Thumb Drives”
- Integrated Assessment Plan and test data that supports government and industry objectives
SPIDERS Phase 2 Cyber Assessment/Experimentation Plan

Lab Assessment/Experiment:
- PNNL vulnerability assessment to include static code analysis
- Actual IPERC hardware-in-the-loop
- 2 week PACOM red team experiment to explore enclaving/architecture strategies

Live Grid Experiment at Fort Carson:
- Strict Rules of Engagement (ROE)
- 2 week PACOM red team experiment to verify lab results

CSET Assessment:
- Cyber Security Evaluation Tool (CSET, offered free by DHS) assessment conducted by PNNL would be combination of lab, live and remote data collection

Schedule:
- 72-hr ops demo 21-24 Oct 13 to include Network Architecture Verification and Validation (NAVV) analysis by DHS
- 2-week lab cyber test in Mar 14 timeframe
- 2-week live cyber test in Apr or Jun 14
SPIDERS Technical Progress

Phase 3 – Camp Smith

- Preliminary System Design complete – Sandia National Labs
- System Integrator – RFP Feb 2014; Anticipate Award Early May 2014
- Fence to Fence Microgrid – Covers entire base
- Renewable Energy – PV Rooftop and Carport Covers
- Control System Cyber Security
- Tied to HECO Commercial Grid – Best Economic Advantage
  - Generates savings to defray the cost of energy security
  - Manages demand charge through peak shaving
  - Provides ancillary services to commercial utility
  - More efficient fuel use during emergencies
SPIDERS Partners

- USPACOM, USNORTHCOM DOE, and DHS
- 5 DOE National Laboratories
- USACE/ERDC-CERL
- Military Services
- Naval Facilities Engineering Command (Bill Anderson, 805-982-3764)
- Local Utility Companies
- States of Hawaii & Colorado
- Private Sector
Transition Plan

• Transition Products and Deliverables
  – NAVFAC Lead; Pacific Northwest Nat’l Lab (PNNL) support
  – DIACAP certification, Platform IT accreditation
  – Assessment Reports, CONOPS and TTP
  – HW and SW system specification and architecture packages
  – Training Package, Safety Requirements, O&M Manuals, Spares
  – Demonstration Results, Performance Data, Business Case Data
  – Residual Equipment

• Key Transition Steps, Actions and Activities
  – Determine Key End-User Performance Metrics
  – DoD Unified Facilities Criteria (UFC) Review
  – DoD UFC Change Requests; New UFC Development
  – Data Delivery to DOE, DHS, Industry

• Industry Transition
  – Utility Reps: APPA, EEI, EPRI, NRECA
  – Policy/Regulatory: FERC, NERC, NARUC, NASEO, MEG
  – Standards: NIST
  – Equipment Manufacturer Assoc: UCA, NEMA