– MICROGRIDS –

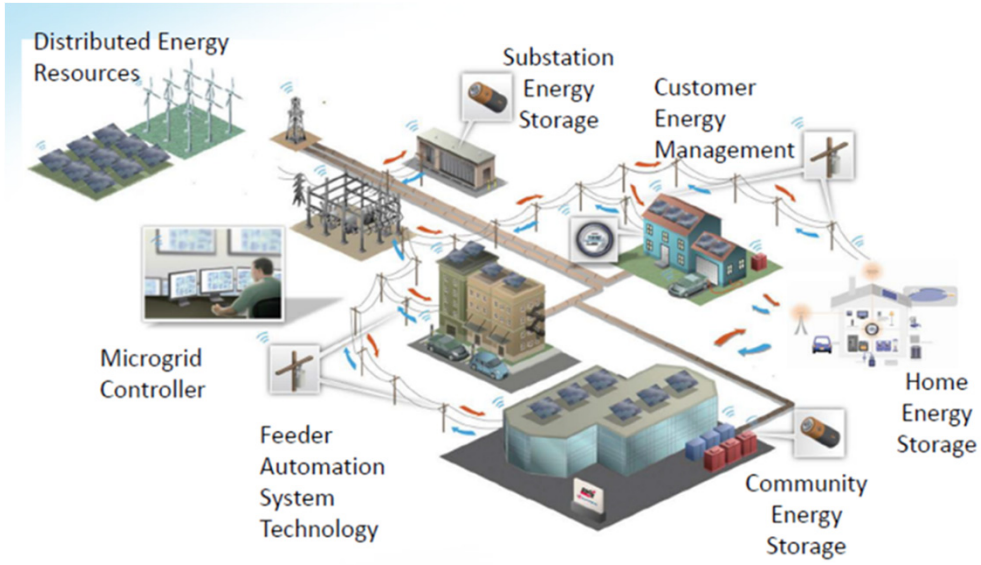
A WATERSHED MOMENT

G. H. BAKER

FOUNDATION FOR RESILIENT SOCIETIES

PRESENTATION OUTLINE

- Microgrid development history and definition
- Microgrid categories, source types
- Microgrid advantages, motivating factors
- Examples of prevalent applications
- Microgrid disadvantages/problems
- EMP/cyber/physical threats and consequences
- Grid protection – two tracks
  - Macrogrid protection
  - Role of microgrids
- Importance of designed-in protection

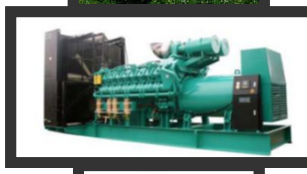


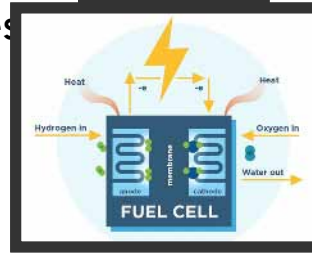
MICROGRIDS - BRIEF HISTORY AND DEFINITION

- Starting in the late 1990s, scientists and engineers in the United States and Europe began to explore decentralized solutions that could manage the integration of thousands or tens of thousands of distributed energy resources in a way that maximizes reliability and resilience in the face of:
  - **Natural disasters**
  - **Cascading power failures**
  - **Physical and cyber attacks (important note: EMP not addressed)**
- Grid architecture evolved that can manage electric generation and demand locally in subsections of the grid that can be "islanded" from the larger grid to provide critical services should the main grid fail - architecture given the name **"microgrid"**
- **Microgrid definition: "[A microgrid is] a group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid. A microgrid can connect and disconnect from the grid to enable it to operate in both grid-connected or island mode."***
- Microgrids are now emerging from lab benches and pilot demonstration sites into commercial markets, driven by
  - **Technological improvements**
  - **Falling costs**
  - **Proven track record with growing recognition of benefits.**

MICROGRID CATEGORIES AND SOURCE TYPES

- Microgrids come in varied sizes and power source types driven by type and location of system(s) to be powered.
- Categories of power source types:
  - Renewables (solar, wind, hydro, geothermal)
  - Fossil fuel (liquid and gas)
  - Nuclear power
  - Chemical storage and generation devices (batteries, fuel cells)
- Categories of applications and architectures
  - Buildings/facilities – homes, data/communication centers, hospitals, fresh/waste water facilities, government buildings, food storage, fueling facilities, etc.
  - Larger business enterprise and academic campuses – universities, research facilities (e.g. Princeton, St. Olaf College, CDC, JHAPL)
  - Communities/military bases



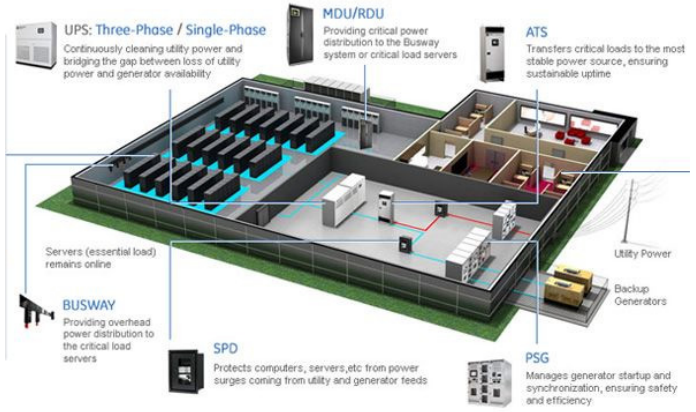


MICROGRID ADVANTAGES/MOTIVATING FACTORS

- Overcome reliability problems with large, regional electric power grids due to weather, cyber, physical, and EMP/GMD vulnerabilities
  - →Reduce unacceptably high risks of extended electric grid outages via standby generation availability
- Inherent 'islanding' capability for protection and blackstarting grids during recovery.
- Replace aging electric infrastructure
- Enhance power quality
- Provide flexible, distributable energy resource (DER) architecture renewable energy resources.
- Create efficiencies using intelligent control systems linking system components.
- Enable dual heat and power generation capability
- Provide reliable electricity to areas with no access to an electric grid
- Reduce particulate and gas environmental emissions

PREVALENT MICROGRID APPLICATIONS

- Data/Comm Centers
- Airports
- Hospitals
- Military Bases/ Communities



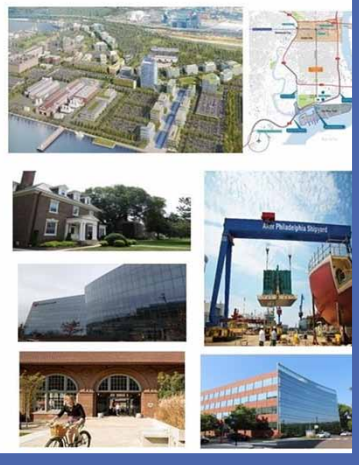
The Navy Yard, Philadelphia – A Community Microgrid

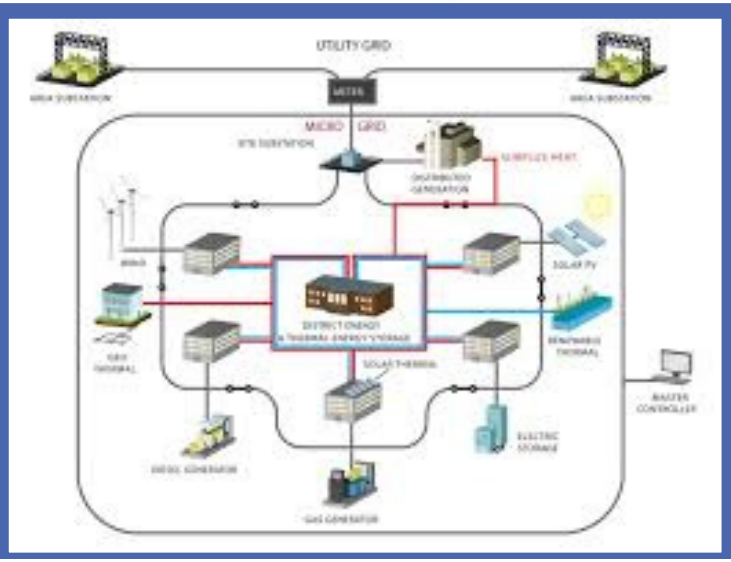
Owner Representative – Philadelphia Industrial Development Corp (PIDC)

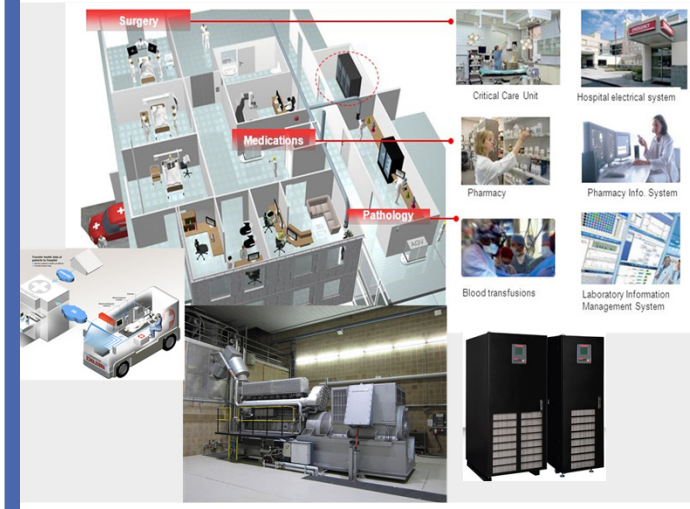
Mission:
PIDC implements economic development initiatives which retain and generate jobs throughout Philadelphia

Navy Yard Today
- 150+ Companies
- More than 12000 People
- In Excess of 7.6 Million SF Occupied
- $700+ million of private investment

PIDC Serves all market segments
- Technology
- Higher Education – R&D
- Industrial / Manufacturing
- Medical
- Community/Small Business
- Cultural & Tourism
- Commercial /Offices

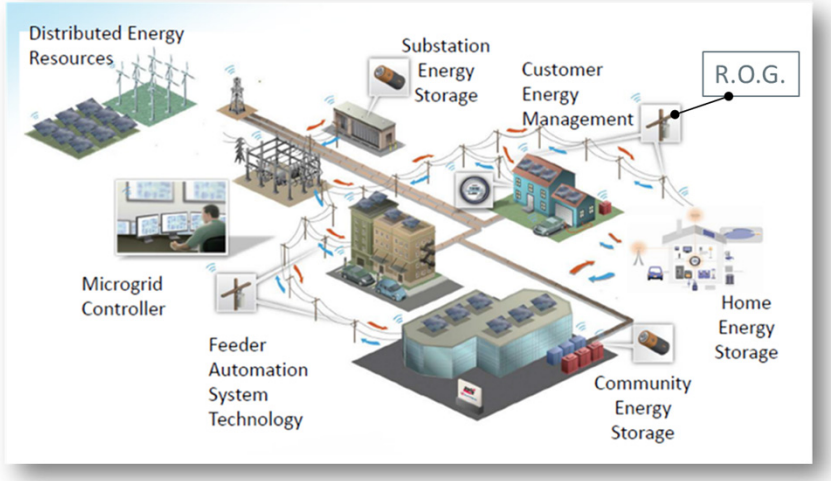






MICROGRID DISADVANTAGES/PROBLEMS

- Microgrids have internal vulnerabilities
  - Electronic sensing and control systems required to balance generation and load - susceptible to cyber and electromagnetic-caused debilitation
- Microgrids complicate the operation of the larger macrogrid (rest of grid or 'ROG')
  - Microgrids add additional layers of complexity to the electric grid – increasing the "vulnerability of complexity"
  - Intermittent renewable energy sources can introduce rapid load swings to ROG
  - Power backfeed from microgrids can cause disruption and safety problems in ROG
  - Physical/logical connectivity between microgrid and ROG increases
    EMP and cyber vulnerabilities
- If not designed with built-in protection, microgrids increase internal and ROG vulnerabilities to
  - Cyber threats
  - Electromagnetic threats including EMP, GMD, RF weapon

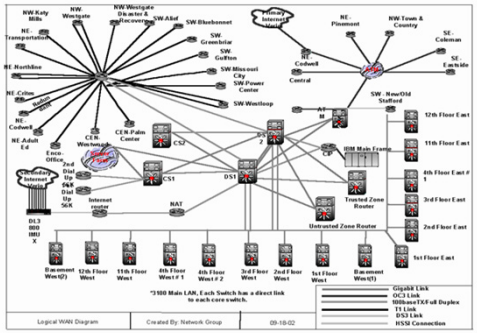


We are at a "Watershed Moment" in tech history

- **Incorporating Cyber/EMP protection in microgrid design and installations will greatly enhance grid survivability**
- **Omitting Cyber/EMP protection will lead to grid resilience mayhem**

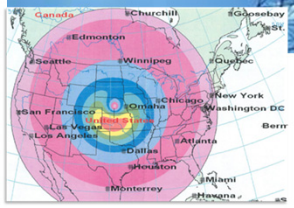
GROWING VULNERABILITY CONCERNS

- In addition to normal weather and Murphy's Laws, grid is known target for cyber, EMP and physical threats
- Growing reliance on electronic control of critical infrastructures
  - e.g. Process Control Systems (PCS), SCADA systems, IoT
- Growing dependence on telecommunication networks and the Internet
- Power grid and supporting infrastructure protection is sparse or missing
- The President's National Security Telecommunications Advisory Committee (NSTAC) early concerns about Long-Term Outage (LTO) of electric power grid involving interruption of electricity for months to years over large geographic regions
- In a cruel irony, as society becomes more and more reliant on uninterrupted power, the grid becomes more and more vulnerable unless intentionally protected.

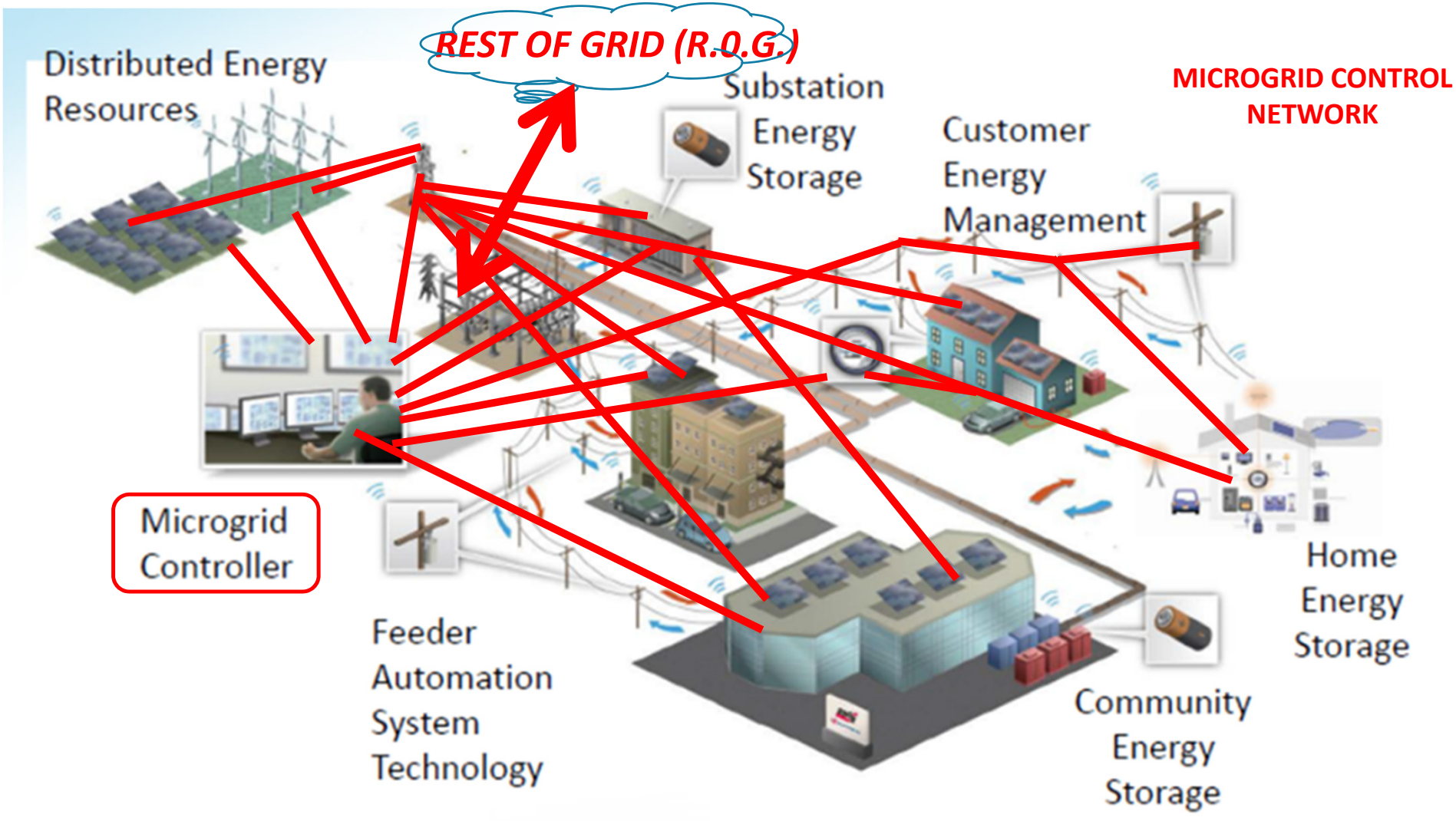


NEW THREATS HIGHLY ASYMMETRIC

- Physical Threats
  - Small number of actors can shut down North American grid for months to years
  - FERC Chairman – attack on 9 substations is sufficient
  - Physical attack on Metcalf Substation nearly succeeded in depowering Silicon Valley
- Cyber Threats
  - Unaddressed malware trojan implants could shut down large portions of grid on command
  - Aurora project demonstrated generator self-destruction by remote cyber control of breakers
  - During 2015-2016 Russian hackers shut down large sector of Ukraine's power grid.
  - In 2018, federal officials revealed Russians had penetrated the computers of multiple U.S. electric utilities gaining access privileges sufficient to cause power outages.
- Electromagnetic events capable of continental-scale grid damage and long-term outages
  - Single event can shut down continental grid
  - 10-12% annual probability of solar superstorm GMD
  - North Korea's stated threat to use EMP against the U.S.
  - Nuclear EMP highest intensity currents/voltages, solar GMD close second
  - Electric Power Grid is highest risk infrastructure due to long lines

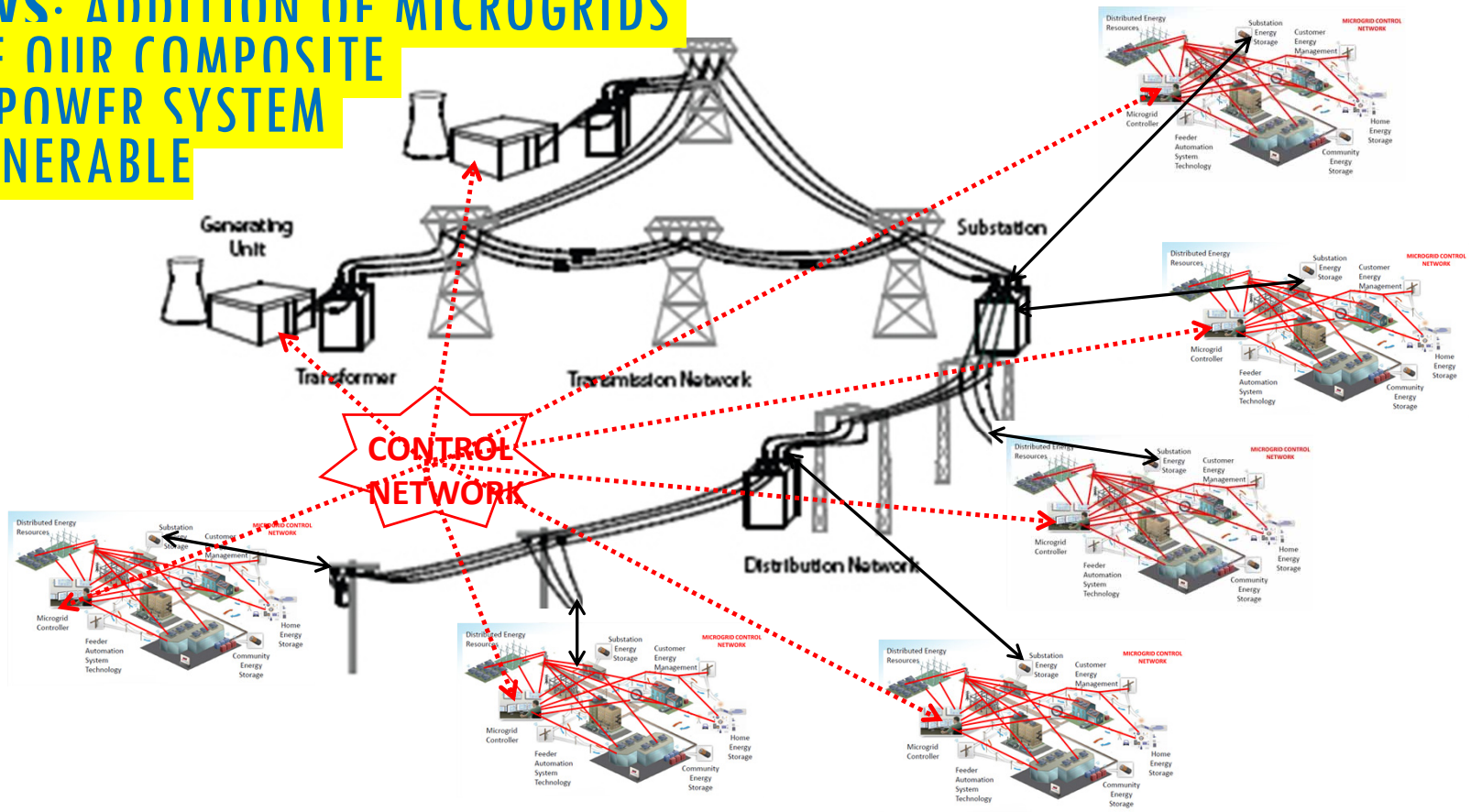


MICROGRID CONTROLS PROVIDE CYBER & EMP ATTACK VECTORS

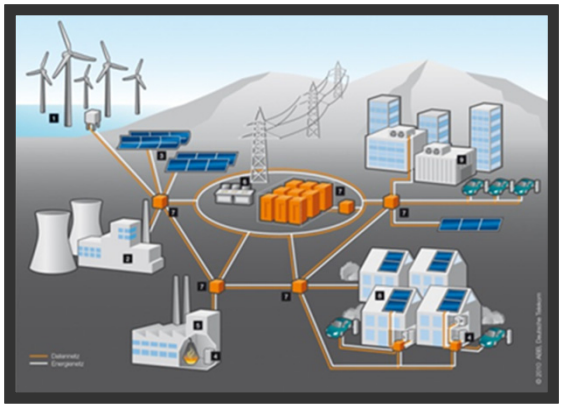


MICROGRIDS ALSO PROVIDE CYBER & EMP ATTACK VECTORS TO LARGER GRID (R.O.G.)

BAD NEWS: ADDITION OF MICROGRIDS CAN MAKE OUR COMPOSITE ELECTRIC POWER SYSTEM MORE VULNERABLE



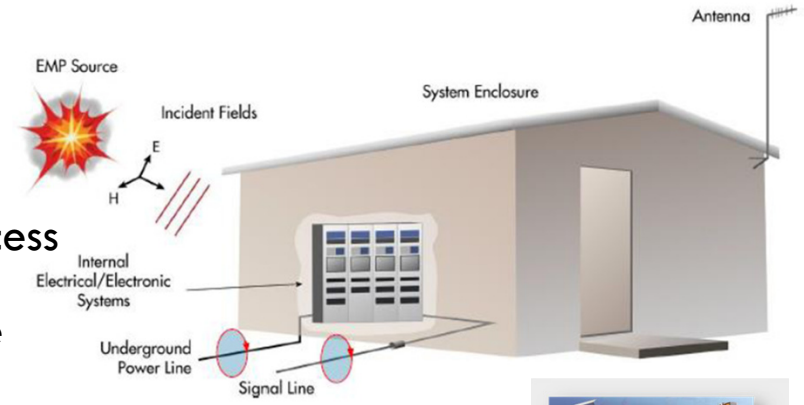
GOOD NEWS: WITH DESIGNED-IN PROTECTION, MICROGRIDS CAN BE MUCH MORE RESILIENT + HELP PROTECT R.O.G.



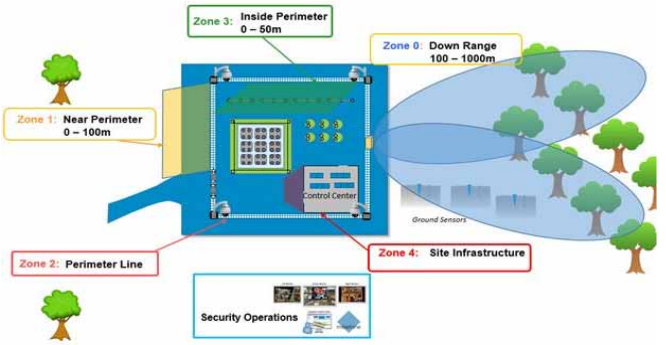
- Air gaps, firewalls, software to isolate microgrid communication and control networks from the R.O.G. control systems and cloud.
- Small land area of microgrids and internal short line interconnects makes them virtually immune GMD and late-time EMP (E3) threats
  - True only for microgrid in island mode, isolated from ROG long-lines.
- Application of proven EMP design techniques insure microgrid survivability
  - Shielding of critical electronic control systems/boxes
  - Application of surge arrestors on conductive cable penetrations/terminals
  - Use of optical fiber interconnections for all control signal lines.

COMPOSITE GRID PROTECTION

- Two-pronged protection approach needed:
  1. Global macrogrid (ROG) protection – longer term process involved – in the meantime…
  2. Local protection of new microgrid installations to assure resilience of local critical infrastructure services



- More Good News: We know how to harden – demonstrated protection standards/guidelines exist
  - EMP/GMD: IEC and Military Standards applicable
  - Cyber: Existing standards apply only to the bulk power system
    - For microgrids, best practices are known
    - Caution: Industrial Control System protection is different than IT protection
    - Microgrids better able to avoid internet connections and establish air gaps than macrogrid if considered in microgrid design phase
  - Physical security benchmarks and standards available
    - ASD(HD&ASA) DCIP Standards and Benchmarks helpful, viz. AP-5 DCIP Electric Power Standards and Benchmarks
    - DoD-HDBK-2000.12 H



A PLEA FOR DESIGNED-IN EMP/CYBER/PHYSICAL PROTECTION

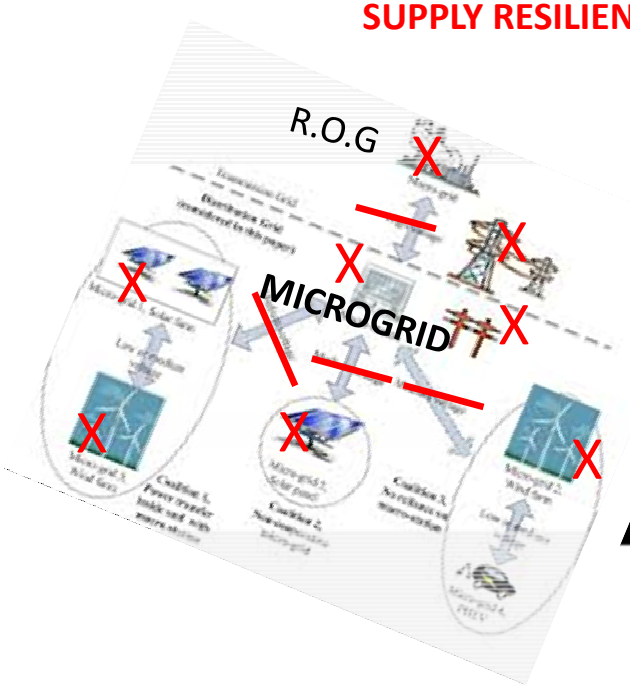
- Installation of unprotected microgrids actually harms resilience of existing infrastructure – increases "vulnerability of complexity"
  - Added layers of cyber/EMP vulnerability inherent in control systems, interconnecting pathways
  - Includes failures due to Murphy's laws and Malefactor actions
- DoD experience with facility and weapon system hardening indicates designed-in protection costs are 10X lower than retrofit protection (2-5% vs. 20-50%)
- We are at a watershed where we must decide between:
  - CARPE DIEM for designed-in protection on microgrid installations yielding much improved electricity supply resilience, or
  - Proceed in lazy-faire manner to increase local and regional electric supply vulnerability

"WATERSHED MOMENT"

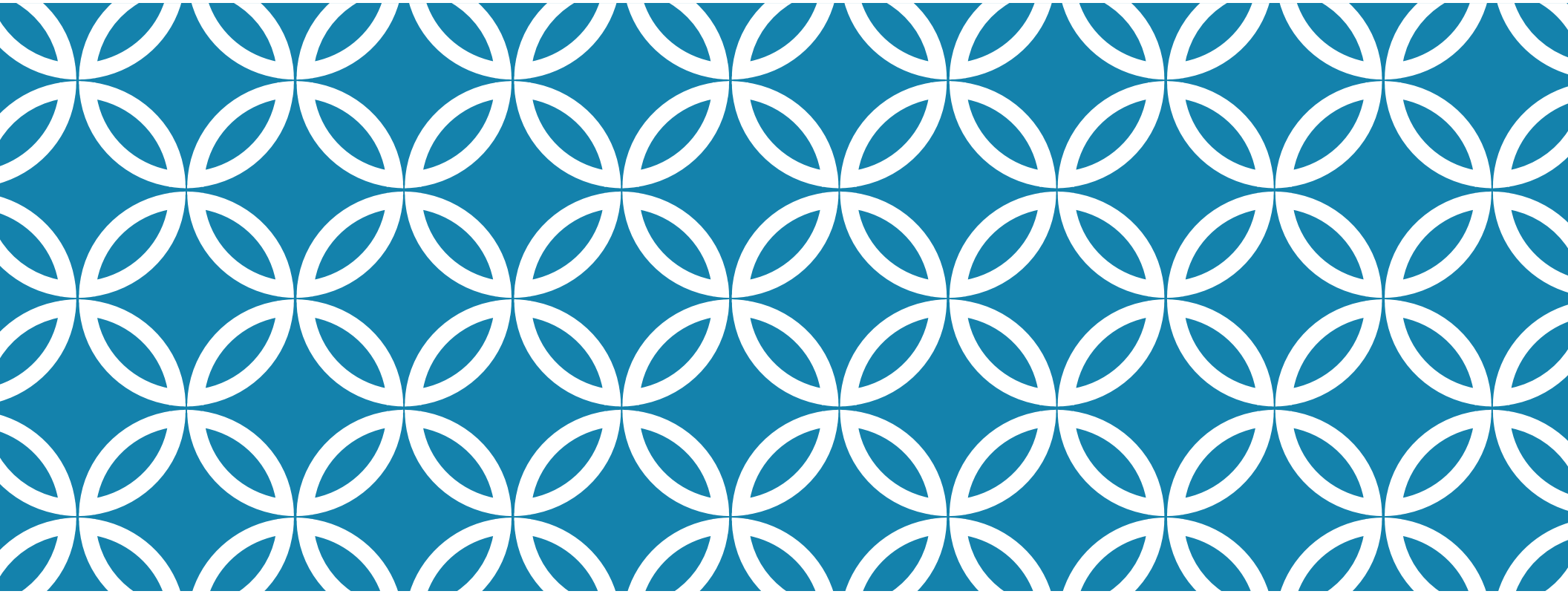
DECISION

<u>UNPROTECTED</u> MICROGRID INSTALLATIONS
DECREASED OVERALL ELECTRIC SUPPLY RESILIENCY

<u>DESIGNED-IN</u> MICROGRID PROTECTION
INCREASED OVERALL ELECTRIC SUPPLY RESILIENCY



MICROGRID IMPLEMENTATION WATERSHED



FINIS

MICROGRID RISKS – A PLEA FOR DESIGNED-IN PROTECTION

GEORGE H. BAKER
FOUNDATION FOR RESILIENT SOCIETIES

Abstract

Microgrids are rapidly transitioning from research and test beds into commercial markets and installations. The maturity of the technology is evidenced by the application of microgrids to replace significant portions of Puerto Rico's electric grid in the aftermath of 2017 hurricanes Harvey and Maria. Microgrids offer many benefits including enhanced reliability, reduced life cycle costs, improvements in power quality and efficiency, demand reduction, reduction in fossil fuel emissions by using renewable and nuclear generation, demand reduction, and installation flexibility for both urban and rural applications. The microgrid market is forecast to reach $31B by 2027.

However, microgrids may not be a silver bullet solution for problems associated with the larger electric power "macrogrid." Because of organic digital monitoring and control systems, microgrid networks are highly susceptible to cyber attacks and normal or intentional electromagnetic interference-caused debilitation. Energy storage technology supporting renewable energy systems is expensive and can fail catastrophically. Furthermore, integration of microgrids into the larger existing electric power networks, without attention to protection engineering, actually increases the vulnerability of the resulting network of electric power networks. Care must be taken in design and installation of microgrids because of the complexity they add to the larger electric power system including added cyber attack pathways, transient current and voltage surges engendered by rapid changes in solar and wind generation output, and microgrid component susceptibility to nuclear and pulse-power EMP threats. We are at a historic technological juncture with distributed microgrid energy sources gaining momentum in displacing bulk electric power. We must now insure that combined physical security, cyber security and EMP protection engineering are incorporated in the initial designs of microgrids to avoid increasing the vulnerability of our electric power networks.

BRIEFING OBJECTIVES

Presentation objectives

- Define microgrids
- Illuminate microgrids' advantages and disadvantages
  - Look at motivating factors for widespread microgrid implementation
  - Provide examples of prevalent applications
  - Look at down-side of added complexity
- Explain electromagnetic/cyber/physical threats and consequences
  - Look at issues related in protecting EPG
  - Emphasize microgrid benefits for avoiding long-term-outages (LTOs) of electric power grid
  - Warn that failure to protect microgrids makes total grid more vulnerable
- Explain importance of designed-in protection