Integrated Private Network for the Power Grid

STS GLOBAL inc.

Connectivity is our business

2018 Advanced Energy Conference

Prepared BY David Hershberg CEO

STS Global

Center of Excellence in Wireless and Information Technologies

1500 Stony Brook Road

Stony Brook, NY 11794-6040

Info@stsglobal.com, 631 246 5000

The Problem

Cyber Attacks & Terrorism
The U.S. Department of Homeland Security (DHS) reports that cyber attacks on the electric grid system are increasing in both frequency and sophistication. Such attacks come from a variety of different sources, including nation states and sub-national terrorist organizations. Concern over their ability to hack into U.S. power grid software and possibly disrupt the electrical supply system is growing because such an attack could be one of the quickest ways to destroy the U.S. economy.

Russia Blamed For Attacks On US Power Grid Starting In 2016

The threat of an attack on the nation's power grid is all too real for the network security professionals who labor every day to keep the country safe.

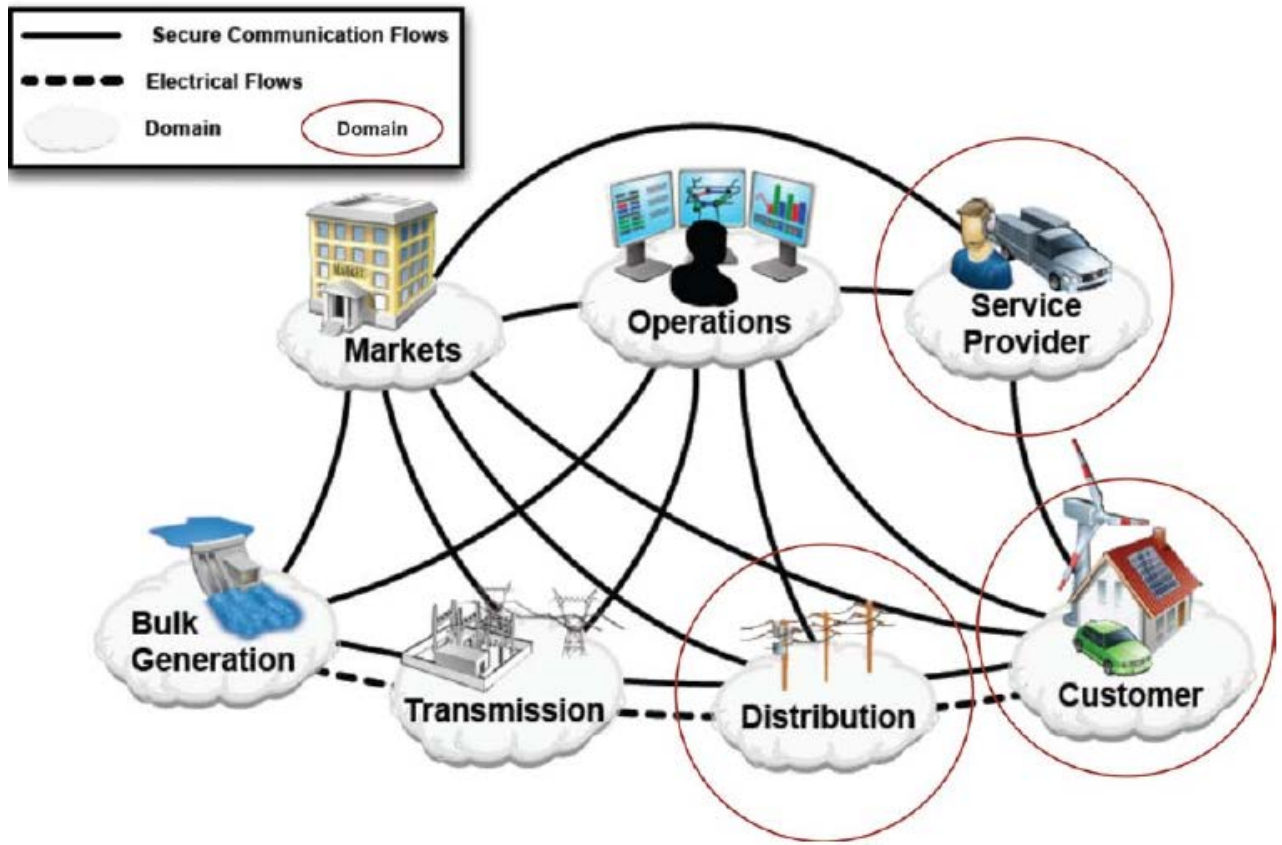
"If you think of how crippled our region is when we lose power for just a couple of days, the implications of a deliberate widespread attack on the power grid for the East Coast, say, would cause devastation," said Sen. **Susan Collins** (R-Maine).

Efforts to Date

- **Energy delivery systems are the backbone of the energy sector - a network of processes that produce, transfer, and distribute energy and the interconnected electronic and communication devices that monitor and control those processes. Energy delivery systems include control systems, the brains that operate and monitor our energy infrastructure.**
- **Two examples of such systems are the Supervisory Control and Data Acquisition (SCADA) and the Distributed Control Systems (DCS). Most system designs did not anticipate the security threats posed by the integration of advances in computers and communication such as off-the-shelf software and operating systems, public telecommunication networks, and the Internet.**
- **Energy delivery systems have become more productive and efficient, but the energy sector is faced with an unprecedented challenge in protecting systems against cyber incidents and threats**

  CEDS program activities fall under five project areas, guided by the *Roadmap to Achieve Energy Delivery Systems Cybersecurity*. They are:

- **Build a Culture of Security**
- **Assess and Monitor Risk**
- **Develop and Implement New Protective Measures to Reduce Risk. Through rigorous research, development, and testing, system vulnerabilities are revealed and mitigation options are identified which has led to hardened control systems.**
- **Manage Incidents. Facilitate tools for stakeholders to improve cyber intrusion detection, remediation, recovery, and restoration capabilities.**
- **Sustain Security Improvements. Through active partnerships, stakeholders are engaged and collaborative efforts and critical security information sharing is occurring.**
- **OVER 100 GOVERNMENT, OGANIZATIONS ,UNIVERSITIES ,PRIVATE AND PUBLIC COMPANIES ARE INVOLVED IN THIS EFFORT**

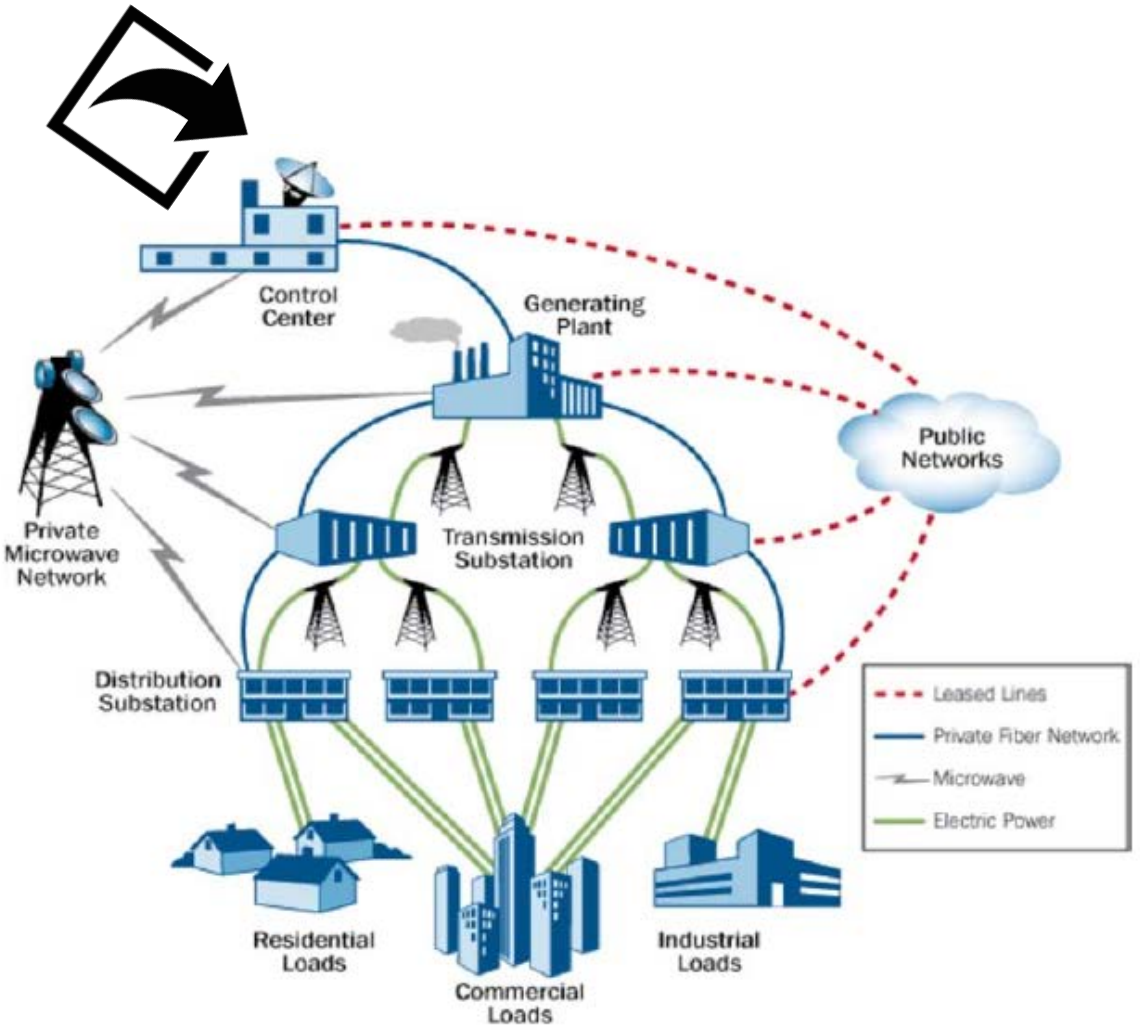

Secure Communication Flows
Electrical Flows
Domain
Domain
Markets
Operations
Service Provider
Bulk Generation
Transmission
Distribution
Customer

Roadmap to Achieve Energy Delivery Systems Cybersecurity

September 2011

Energy Sector Control Systems Working Group

Supporting the Electricity Sub-Sector Coordinating Council, Oil and Natural Gas Sector Coordinating Council, and Government Coordinating Council for Energy



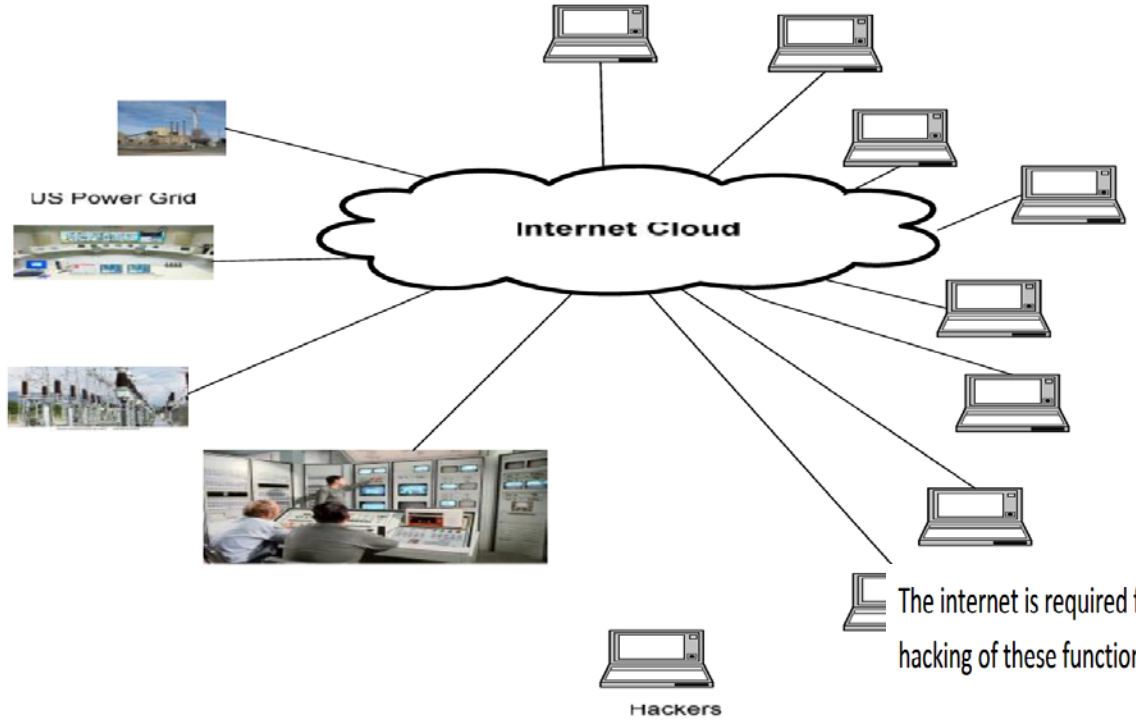
Has 66 pages, satellite mentioned once for vehicle communications. Over 100 organizations working on Cyber security

The Problem

Independent Network US Power Grid (DRAFT)

As long as the US power grid control and monitor utilizes the internet, the grid will be susceptible to hacking and disruption. Figure 1 describes a system connected to the internet along with thousands of potential hackers. The only perfect solution to this problem is a completely private network to control and monitor all aspects of the grid. This white paper describes such a network that can be implemented at low cost and quickly.

Figure 1 the internet solution



The internet is required for customer contact and billing. While these are mandatory functions and hacking of these functions would cause some problems the grid would not be affected.

The Concept

To implement a completely private and secure network we are proposing a satellite system using Ka band with very narrow beams . Gateway earth stations for each region of the grid would provide connections to the remote locations that are monitored and controlled. Each of these gateways would be connected to a nationwide network operations center by a dedicated encrypted fiber. By using large antennas at the gateway even if someone could attempt to set up a potential interference it would be impossible to do even if the interferer could locate in the narrow beam footprint.

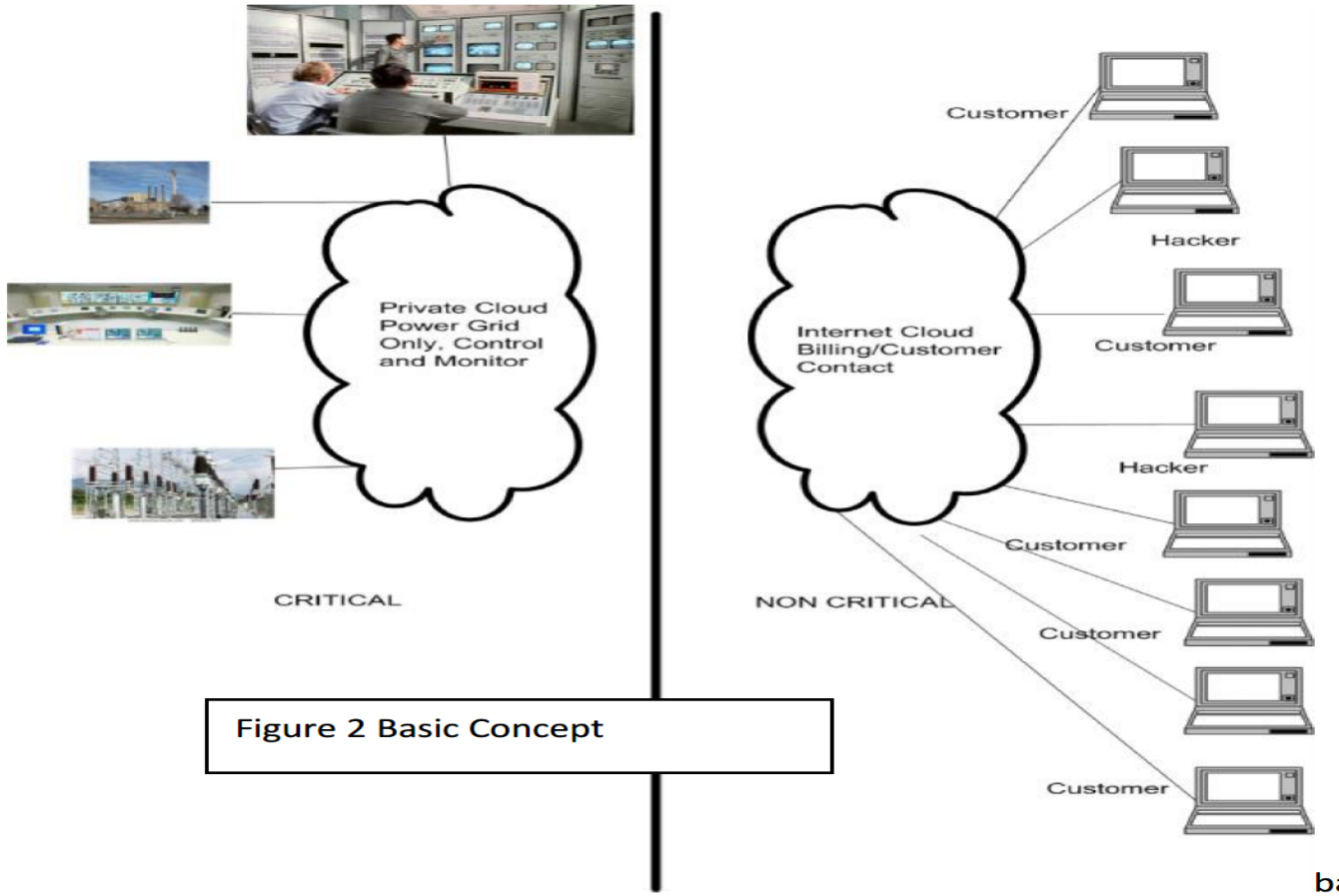
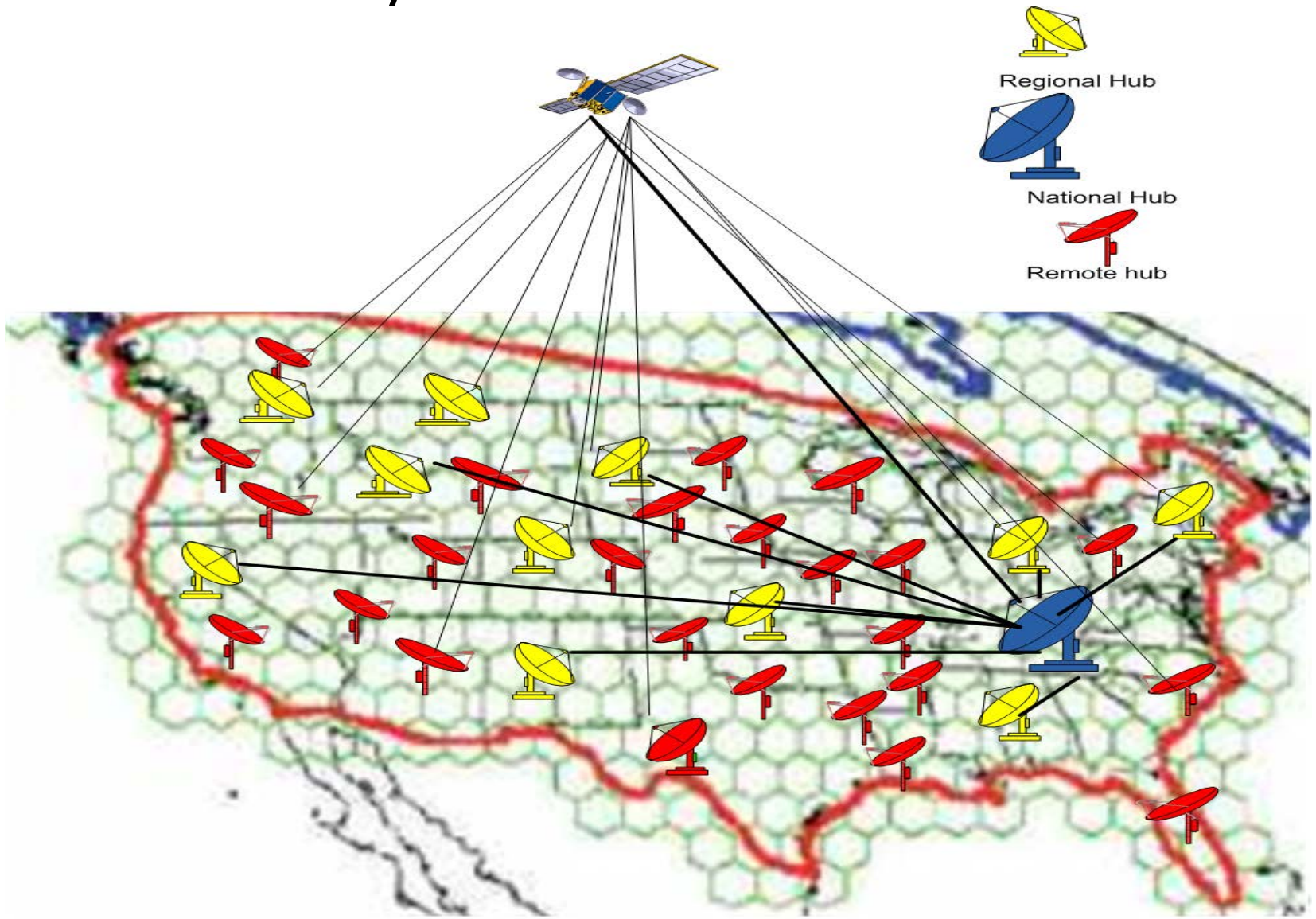


Figure 2 Basic Concept

The number of remote locations consisting of power stations, switching centers, power plants, substations etc could be many thousands easily covered by a VSAT network. The use of narrow satellite footprints and encryption secures the network.

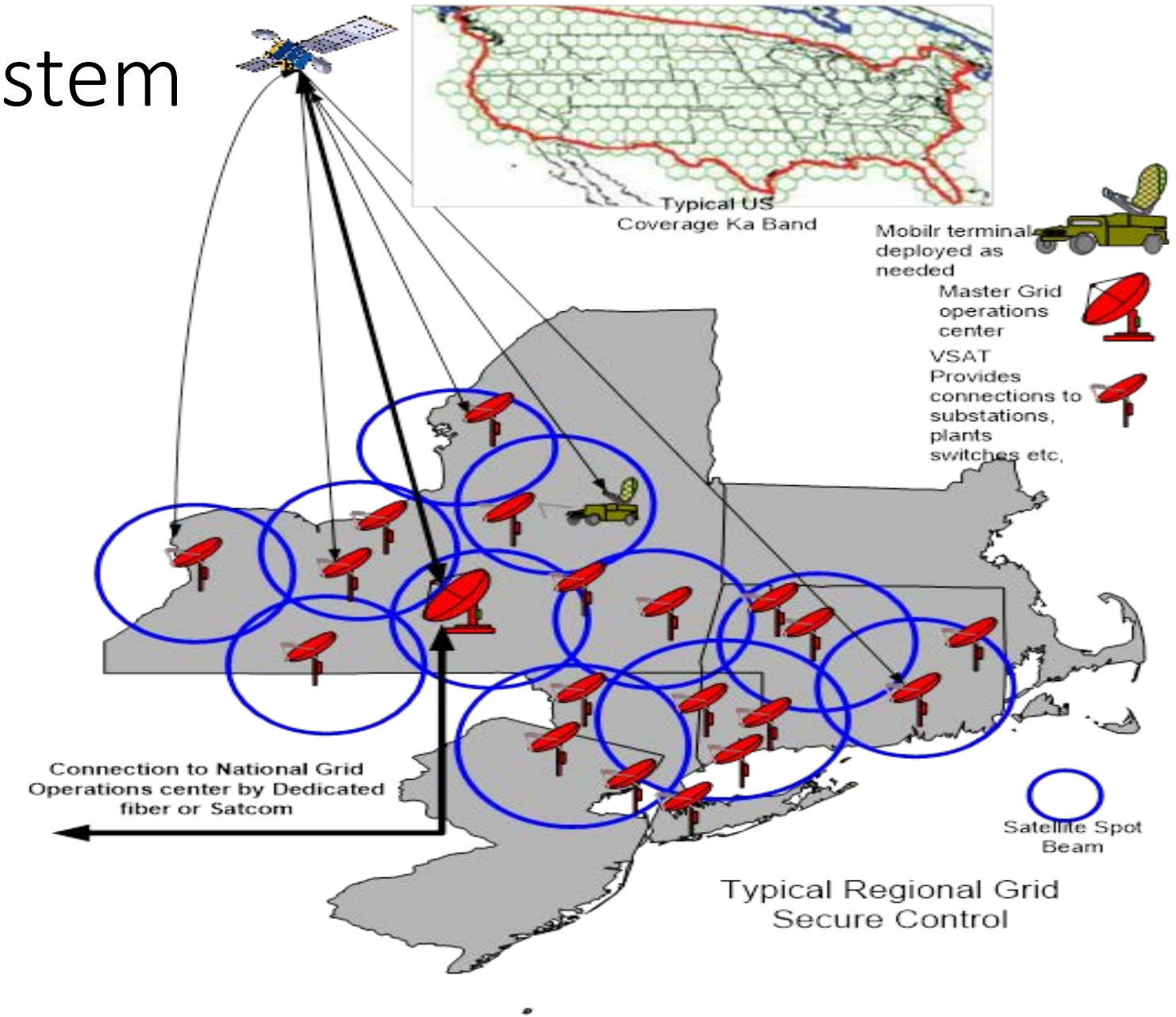
Nationwide System



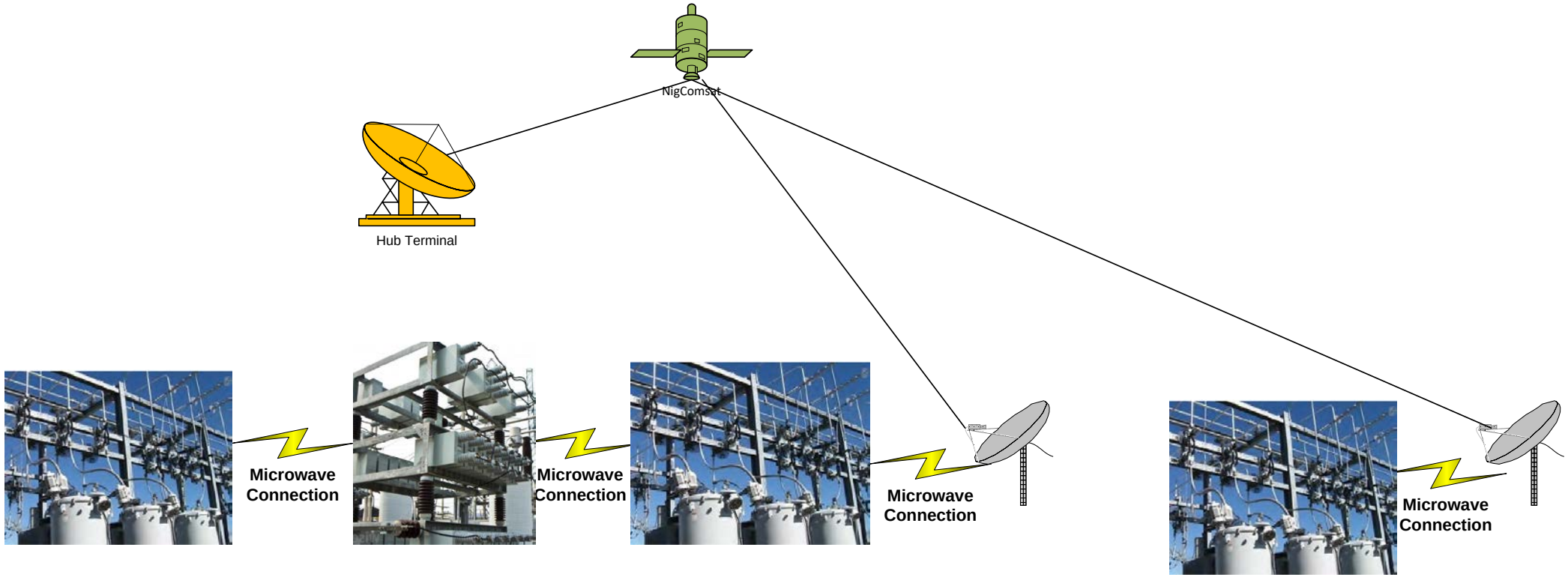
Nationwide System

Each manned location would have a secure room and the operators will be screened and cleared to operate in the network.

Regional System



Connection Options



Multiple Mesh Connections single Satellite Connection

High Density Area

Single Satellite Connection System

Low Density Area