M2M Technologies – The future is upon us. Is this stuff secure?

CQR 2012

San Diego, CA

Bob Lesnewich

Applied Communication Sciences

rlesnewich@appcomsci.com

732-699-3267 (office)

M2M Technologies

Advancements are a cause for security concern (examples)

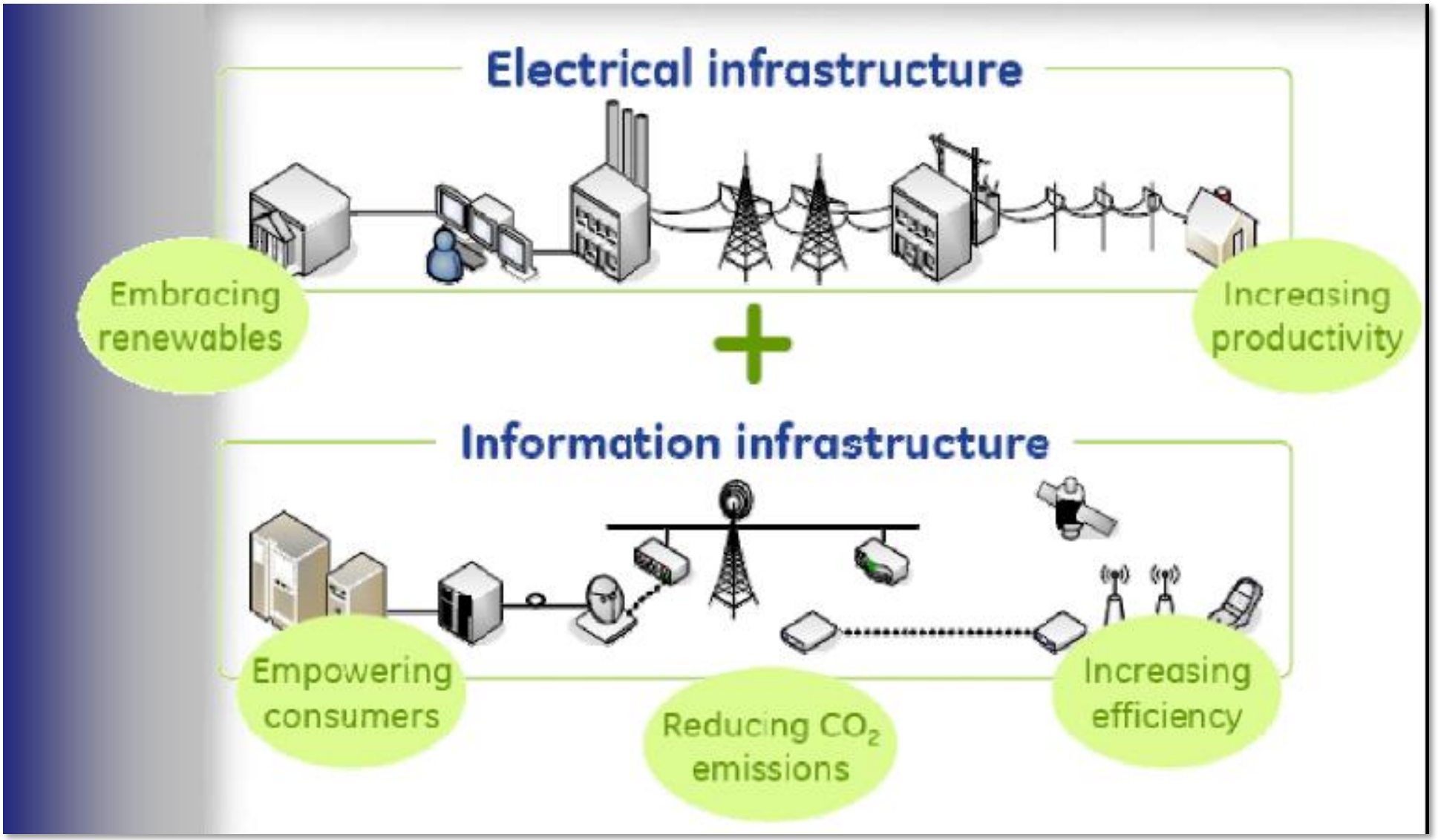
- Consumer Vehicle Networks
- Mobile Money
- In-Home Networks
- **Smart Grid**

Smart Grid Objectives

- Integrate Renewable Energy Sources
- Improve Operational Efficiency
- Promote Energy Conservation / Reduce Demand
- Better Asset and Infrastructure Utilization
- Support Electric Vehicles
- Obtain Clean Energy Goals
- Improve Quality and Reliability of Power

UTILITIES DEMAND HIGHER PERFORMANCE IN AN INCREASING COMPLEX ENVIRONMENT

Communications is a Core Smart Grid Enabler



Major Smart Grid Efforts

- Advanced Metering Infrastructure (AMI)
- Substation and Distribution Automation
- A Secure Communications Infrastructure
- Renewable Energy Resources
- Research (more not mentioned)
  - Distributed Grid and Microgrid Management
  - Energy Storage

Challenges of Managing an Advanced Distribution System

YOUR LARGEST NETWORK

EXPOSED NETWORKS

COMPLEX NETWORKS

FIELD AREA NETWORKS

PROPRIETARY

NEW TECHNOLOGY

Automated Sectionali… & Reclosers

Automated Switched Cap Banks

PV Generation

INVERTER

…mmunity

…torage

…ess Line Sensors &

Feeder Metering

AMI/HAN

Direct Load Control

- Automatic Restoration and Feeder Reconfiguration
- Advanced Regulators & Sensors
- S… P…

THE INDUSTRY LACKS CAPABILITIES THAT PROVIDE VISIBILITY AND SITUATIONAL AWARENESS INTO FANS

Field Area Networks (FAN) Security & Management Challenges (1)

- A wide area, multi-vendor, heterogeneous network with a variety of wireless and wired technologies
- The largest network a utility will deploy - millions of intelligent ends to manage, many connected over low bandwidth channels
- Endpoints are tightly integrated, resource-constrained embedded systems - not a desktop system!
- FANs operate in an unprotected environment and they are vulnerable
- Significant amounts of proprietary radio systems and a mix of proprietary and standards-based networking protocols, some of which have yet to be adequately vetted
- Frequent equipment updates are expensive/prohibitive & Software will not fix all problems = “Networks are forced to operate with multiple vintages of hardware with different vulnerability profiles”

FAN Security & Management Challenges (2)

- New ad-hoc/self-forming networks are more dynamic and less understood in practical terms
- Network technology is still immature – communications security, implementation improvements, performance
- A lack of tools to support EMS/DMS operations and security functions
- No commercial solutions available to monitor FAN traffic and detect security anomalies/intrusion or software bugs
- No independent monitoring capabilities to help mitigate supply chain cyber risks
- Few tools to manage security and network performance as compared to enterprise networks

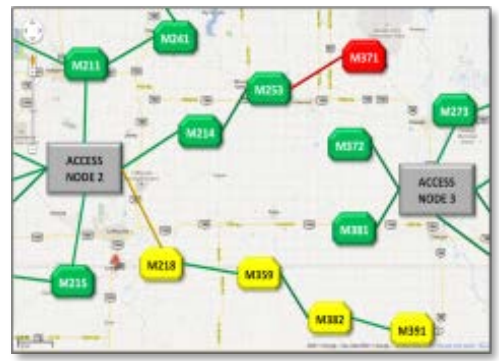
THE INDUSTRY LACKS CAPABILITIES THAT PROVIDE VISIBILITY AND SITUATIONAL AWARENESS INTO FANS

FAN Smart Grid Technologies

- FAN Analyzer
  - Probe-based, packet capture and decomposition system that can independently monitor proprietary and standards-based mesh traffic.

- FAN IDS
  - Probe-based and head-end IDS designed to detect anomalies and signs of attack in AMI/DA networks

- FAN Data and Network Visualization
  - An intelligent combination of data analytics and graphical presentation
  - Creates rich information views to support business, operations, engineering and security processes within a utility



M2M Technologies

M2M is changing the world and creating complex security and reliability concerns.

Today's speakers will provide insights as to what their industries and companies are doing to make M2M secure and reliable:

- Mahbubul Alam - CISCO
- George Dobrowski - Huawei
- Tom Hussey - Ubiquisys