



Smart Grid Security

Gib Sorebo
Assistant Vice President/Chief Security Engineer

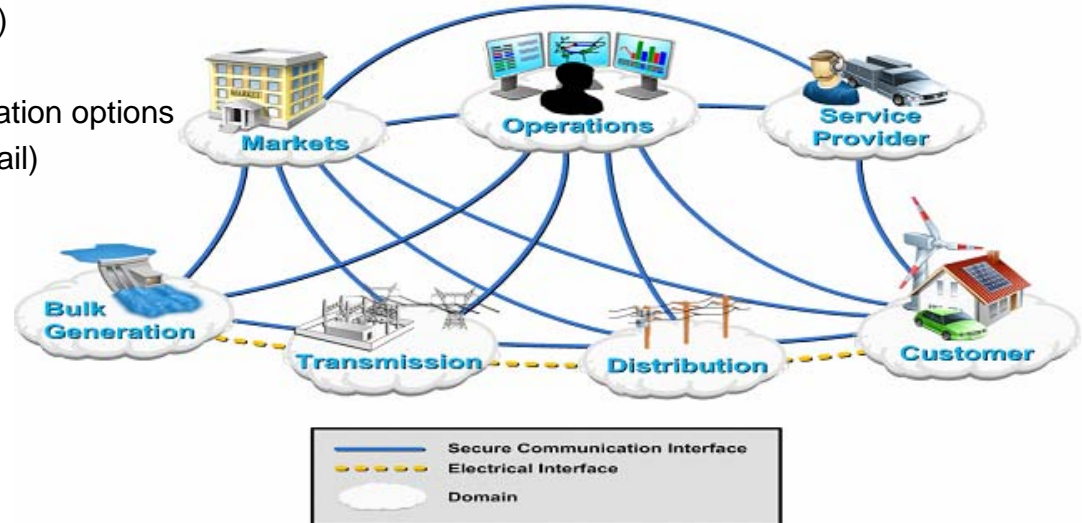
Kansas Corporation Commission | September 18, 2009



Smart Grid Definition



- Smart Grid is the overlay of an information system on the power system that provides increased visibility and control
- The Smart Grid will facilitate customer participation and provide new opportunities and applications much the same as the Internet did for communications
 - Self heal and rapidly respond to interruption or failures
 - Empower and incorporate the consumer
 - Resist security attacks (supply and operation)
 - Provide power quality for 21st century users
 - Accommodate a wide variety of power generation options
 - Enable electricity markets (wholesale and retail)
 - Optimize asset utilization

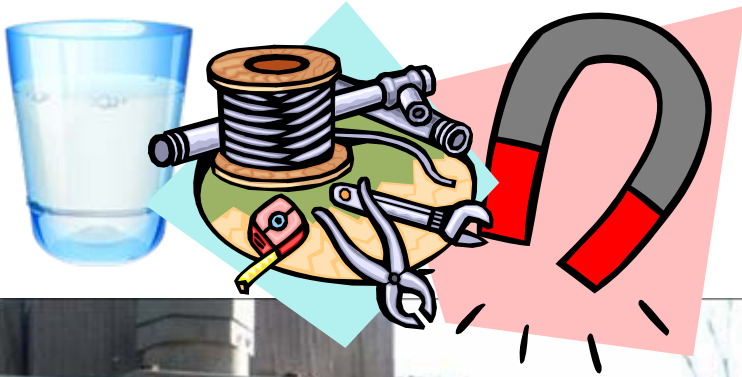


Source: National Institute of Standards and Technology

So What's Different?



And the Threats?



Cyber Threats are Real



“Smart Grid may be vulnerable to hackers”

CNN, March 21, 2009

“Electricity Grid in U.S. Penetrated By Spies”

Wall Street Journal, April 8, 2009

“Copper Thieves Threaten U.S. Infrastructure, FBI says”
Source: Wired Magazine, December 3, 2008

And So Are the Harms...



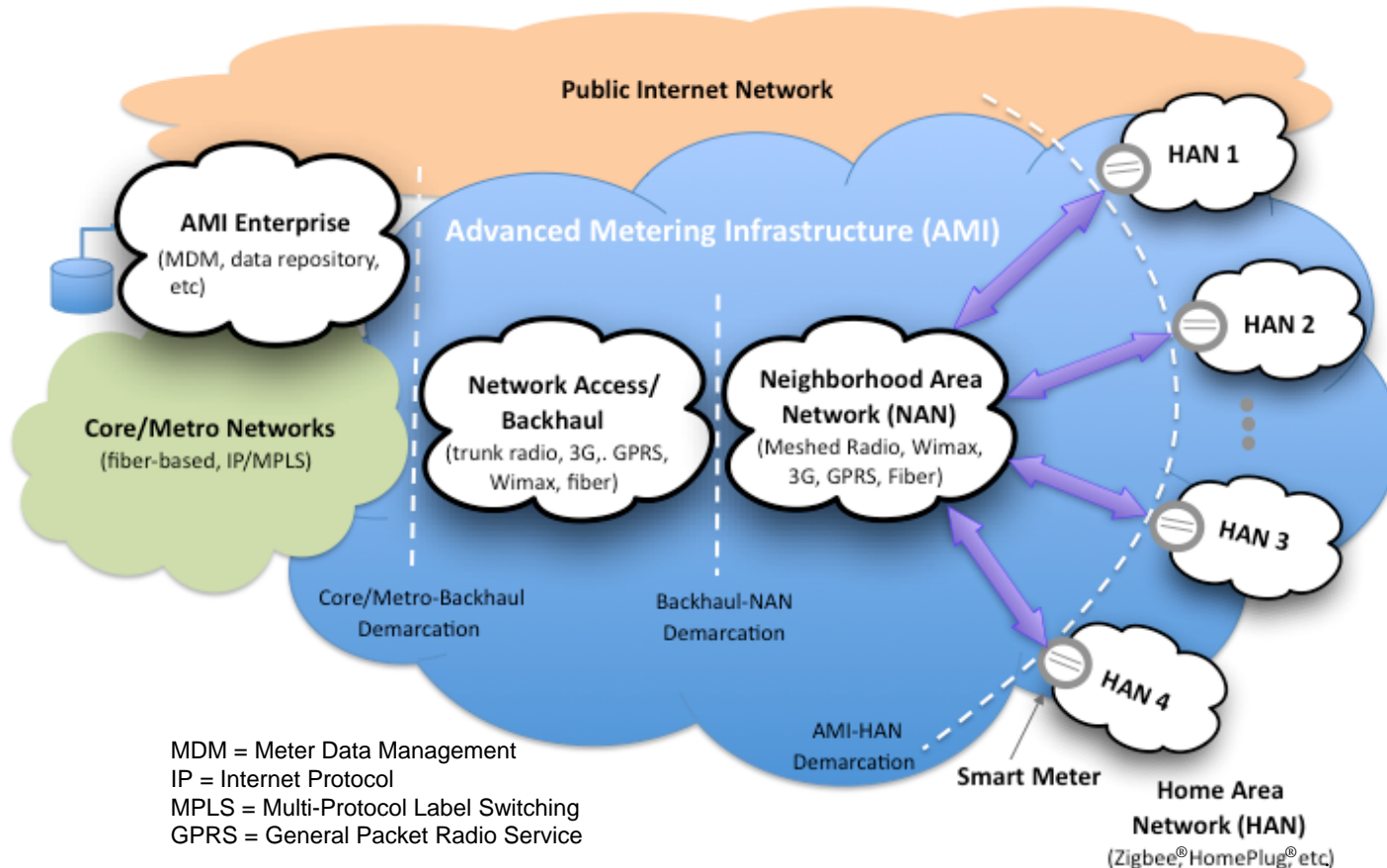
Photos from U.S. Geological Survey, USGS/Rolla, Mo. Used with permission.

- **1998:** Telephone switch hack closes an airport
- **2000:** Gazprom central control is hacked
- **2000:** Australian hacker causes environmental harm by releasing sewage
- **2001:** Hackers protesting U.S./China conflict enter U.S. electric power systems
- **2003:** Power outages in northeastern United States occur
- **2003:** Worm shuts systems down at Davis-Besse nuclear plant
- **2006:** Zotob virus shuts down Holden (GM Holden Ltd.) car manufacturing plant
- **2007:** Aurora demonstration shows damage a remote hacker can cause physical harm to a generator

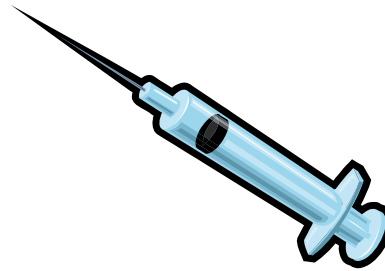
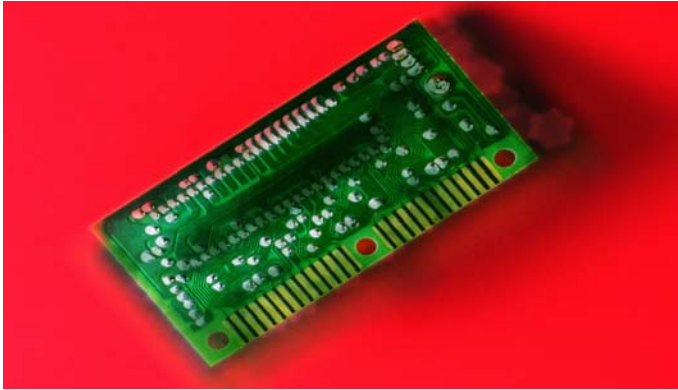
So What Are Some Smart Grid Threats?



Advanced Metering Infrastructure (AMI) Reference Architecture

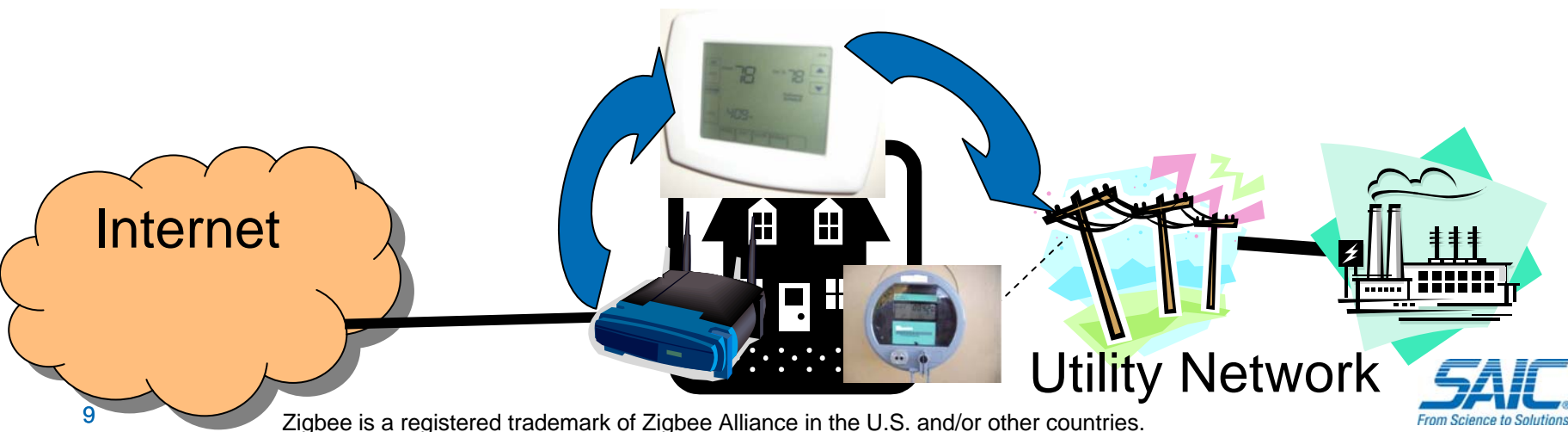


Home Area Network (HAN)



“...a method for bypassing the encryption on ZigBee® wireless chips...”
Forbes, April 30, 2009

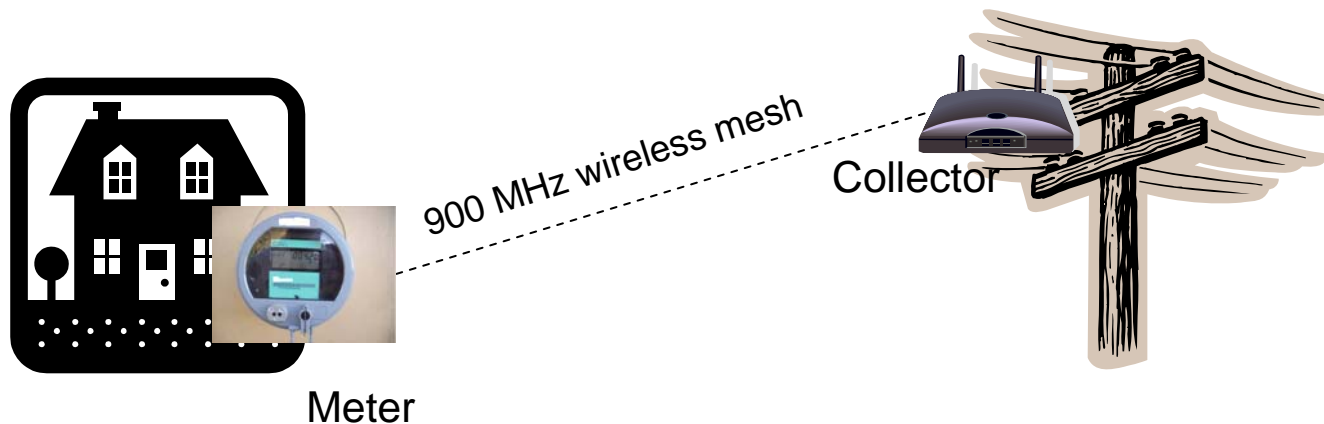
Consumer is in control



Neighborhood Area Network (NAN)



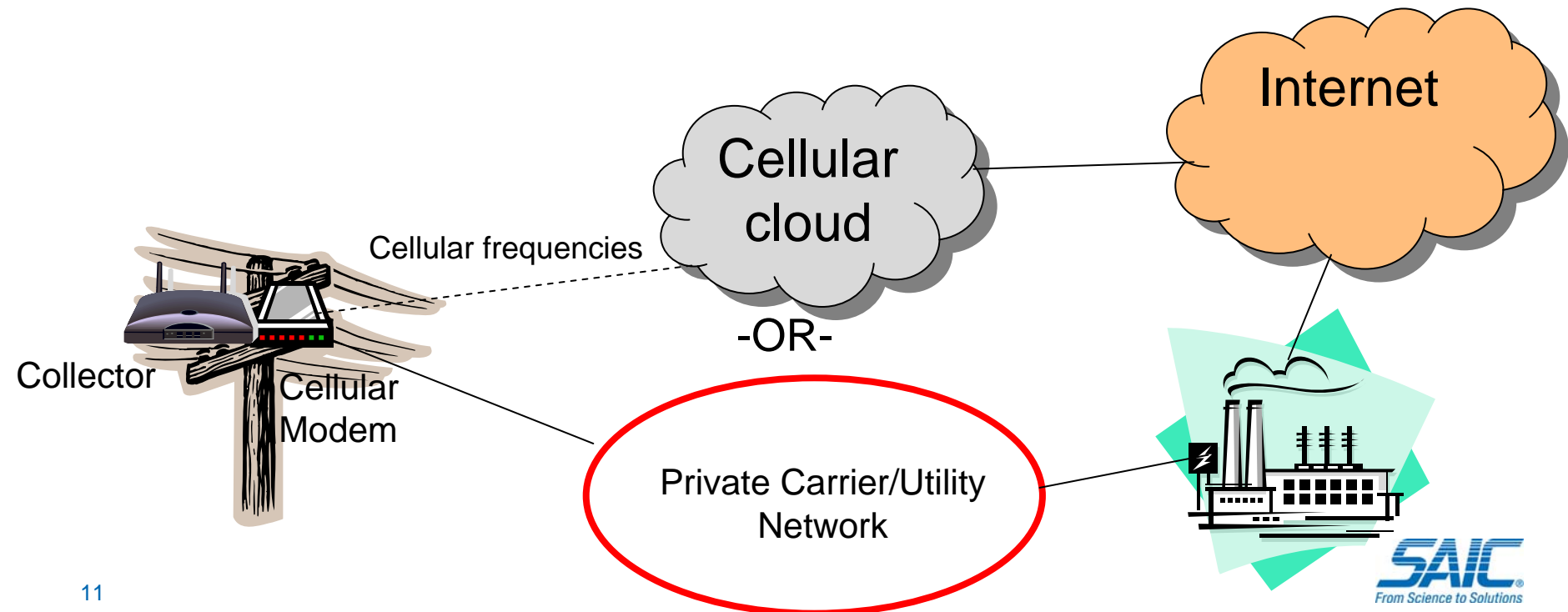
- Physical tampering
- Wireless eavesdropping/jamming
- Meter/collector spoofing
- Password compromises



Wide Area Network (WAN)



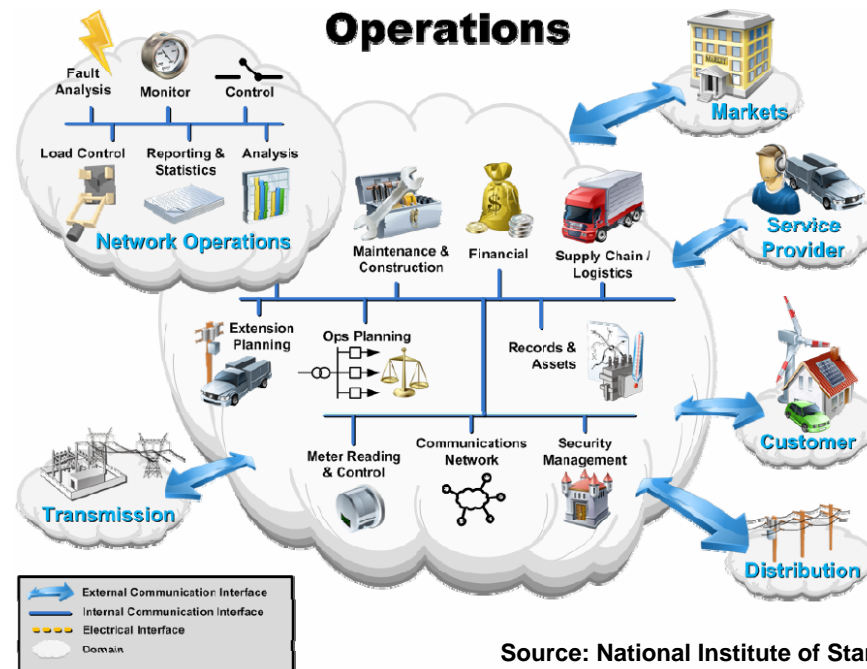
- Cellular cloud shared by all local cellular subscribers
- Most carriers don't prioritize this traffic for utilities
- Depends on reliability of Internet path



Operations Network

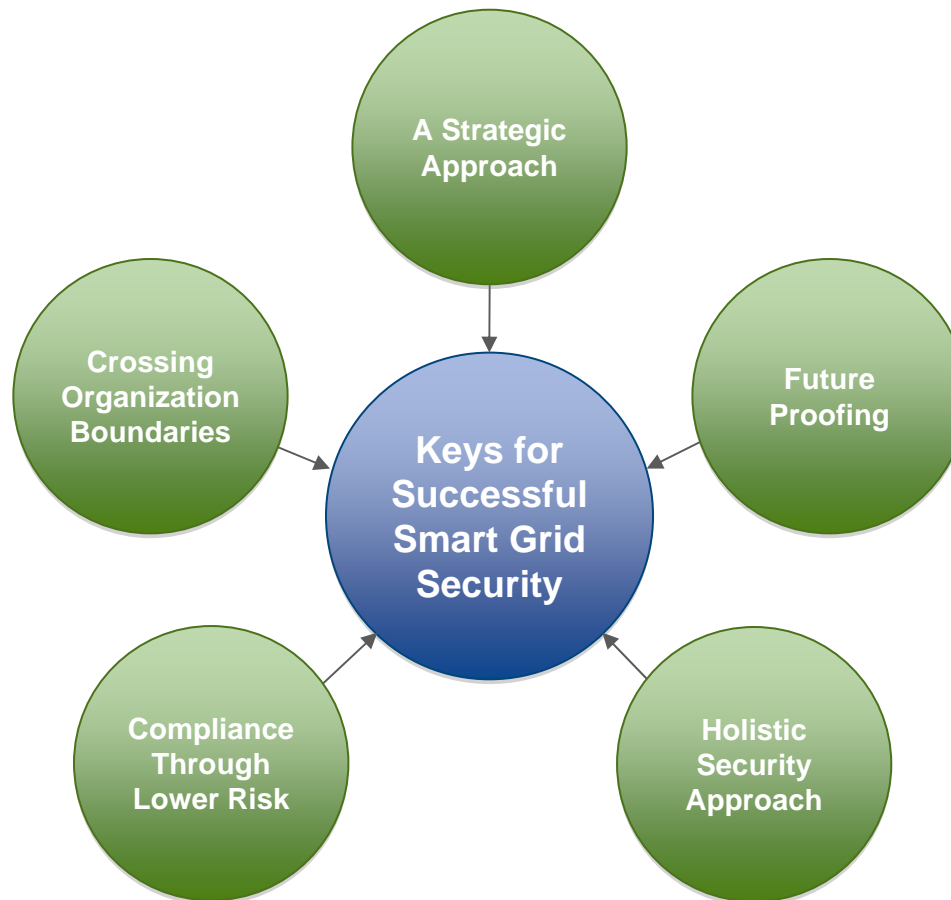


- Least defined part; most still in development
- Involves multiple parties (marketers, generators, etc.)
- Insider/partner threat a serious concern

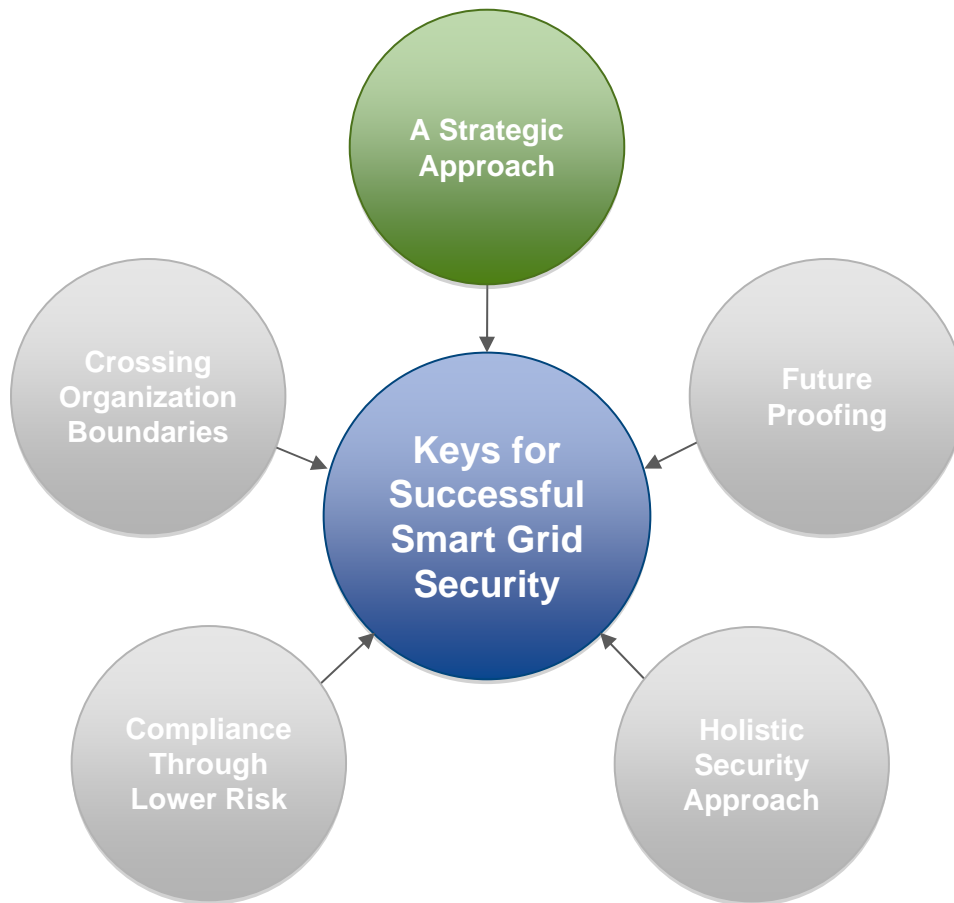


Source: National Institute of Standards and Technology

Keys for Successful Smart Grid Security



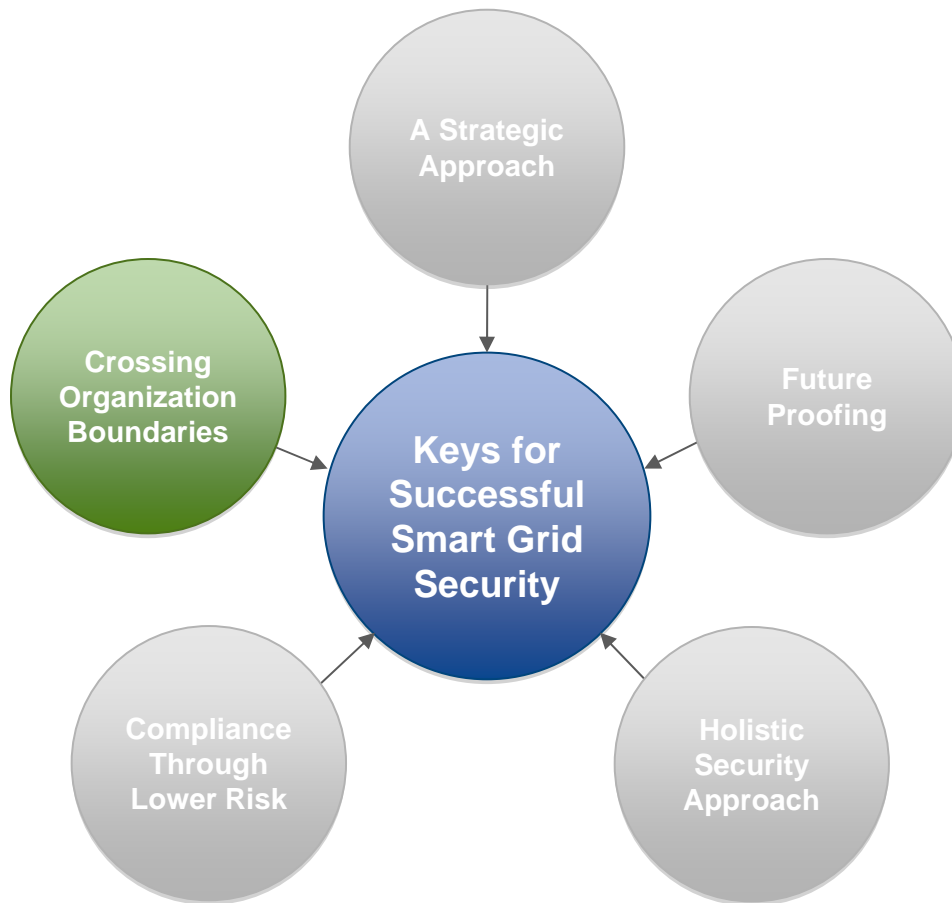
A Strategic Approach



Technology without strategy is chaos.

- Boxes, services, audits, testing, software, widgets
- What does it all mean?
- Will any of it work together?
- You don't buy software without some kind of enterprise strategy
- Don't try to secure critical infrastructure investments without one!

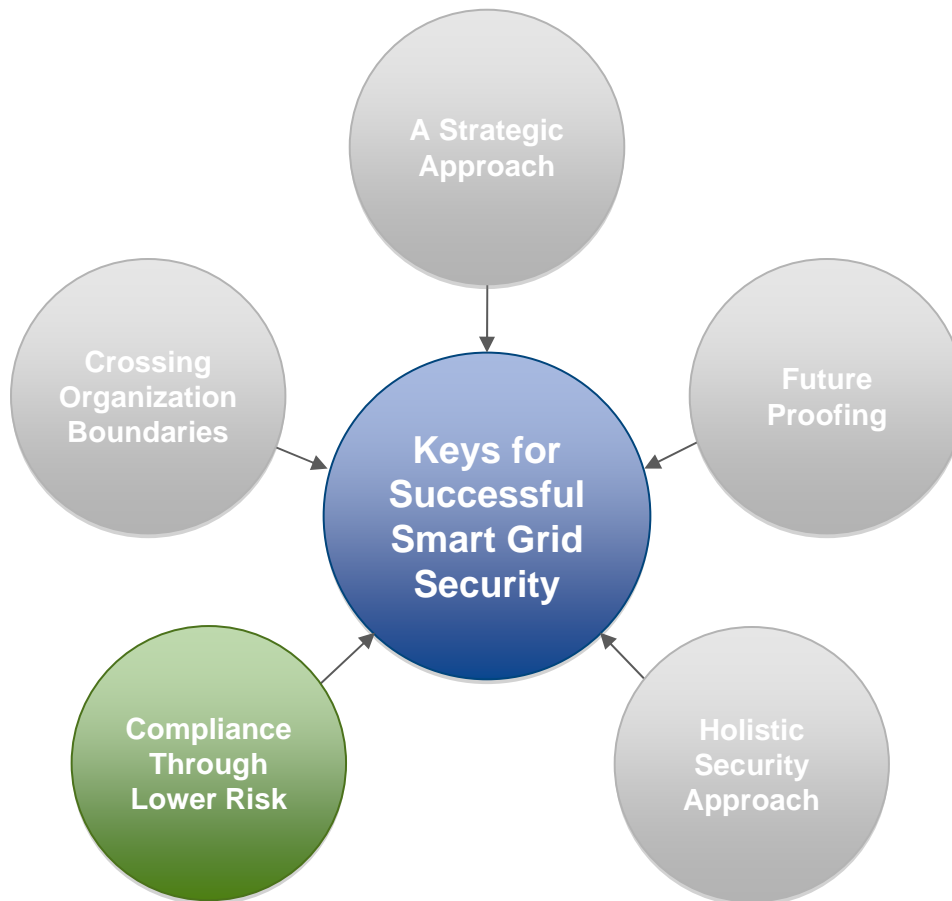
Crossing Organizational Boundaries



A technological and process transformation of the business cannot happen with static and stove-piped organizations.

- Enterprise IT has a lot to offer in managing these types of challenges
- Not a perfect fit, but a start
- How can it be adapted to an adjusted mission?
- Reinventing the wheel elsewhere can be expensive and challenging

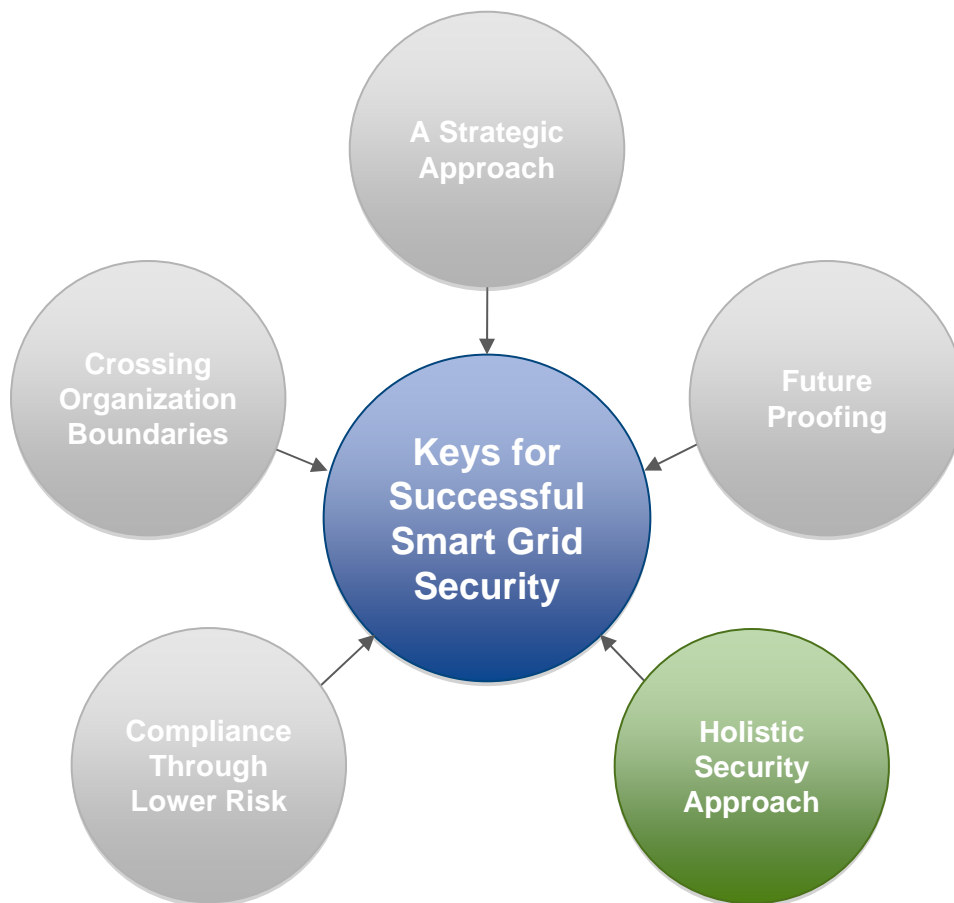
Compliance Through Lower Risk



Compliance is not security, nor is it risk management

- Don't wait for mandates to define your minimum obligations. It likely will not address your real security needs.
- Considered and appropriate risk management strategies and security solutions will line up with mandates. The reverse is not necessarily true.

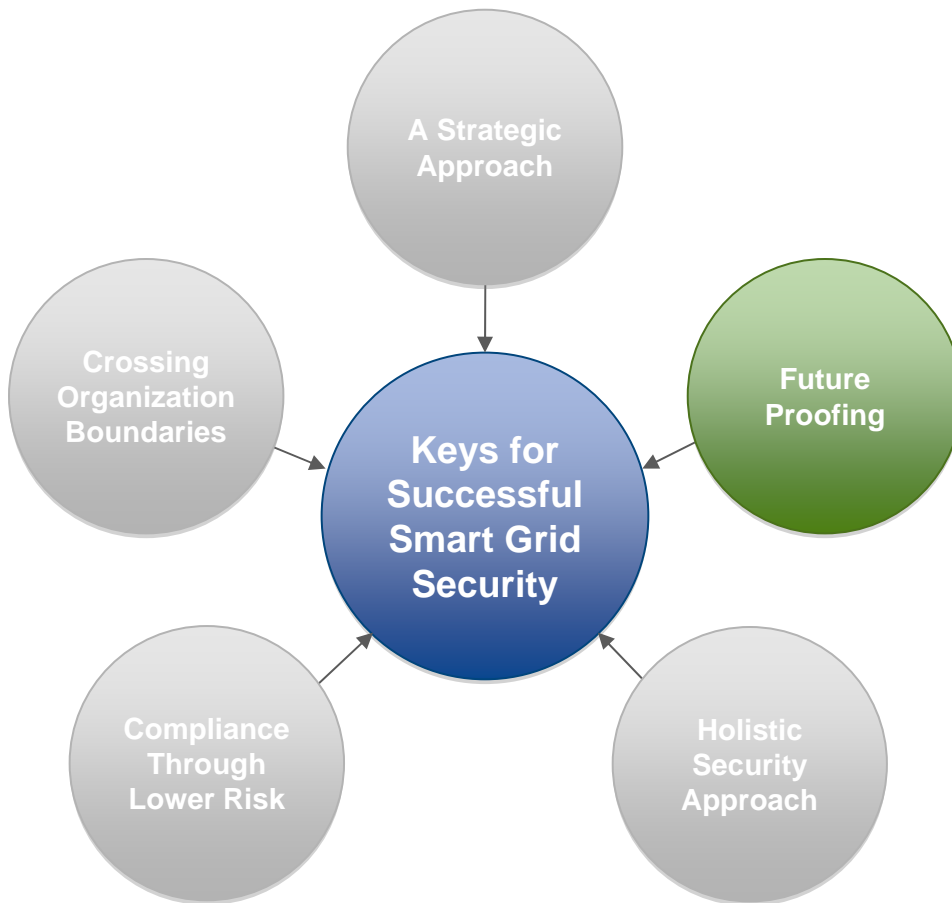
Holistic Security Approach



Focus beyond the asset
“capabilities” discussion

- Understanding capabilities is part of developing and implementing a security response to risk
- People and processes are what will help to ensure actual security every day afterward
- Don't follow the marketplace trap of assuming “the box/vendor does that.” The box does not manage anything; it just does what it is told.

Future Proofing



Defending a 20-year field investment will necessarily flex the latter portions of the security life cycle, so consider it up front

- Protect against what you know are issues
- Monitor and measure proactively to manage complexity and internal risks
- Respond to new threats with dedicated resources
- If you are going to do it yourself, know what you are getting yourself into

Final Considerations



For public utilities commissions

- Ask how security is addressed for each component
- Don't accept assurances that all products used were built to be secure
- Ask to see risk assessment documentation
- Ensure security is budgeted for and individuals are assigned responsibility

For utilities

- Insist that vendors document their security controls
- Ensure service providers (for example, telecommunications companies, meter data processors) are included in risk assessment and provide sufficient information
- Integrate security between operations and enterprise

Questions?



Thank You.

Gib Sorebo

SAIC AVP Chief Security Engineer

tel: 703-676-2605 | email: sorebog@saic.com