



# Should critical infrastructure be “smart”?

Jason Stradley



BT Global Services

# Agenda

- What is a Critical Infrastructure?
- What is the Smart Grid?
- Drivers
- The Players
- Smart Grid Components and Basic Architecture
- Security Challenges & Opportunities
- Meeting those Challenges
- Conclusions
- Questions
- References

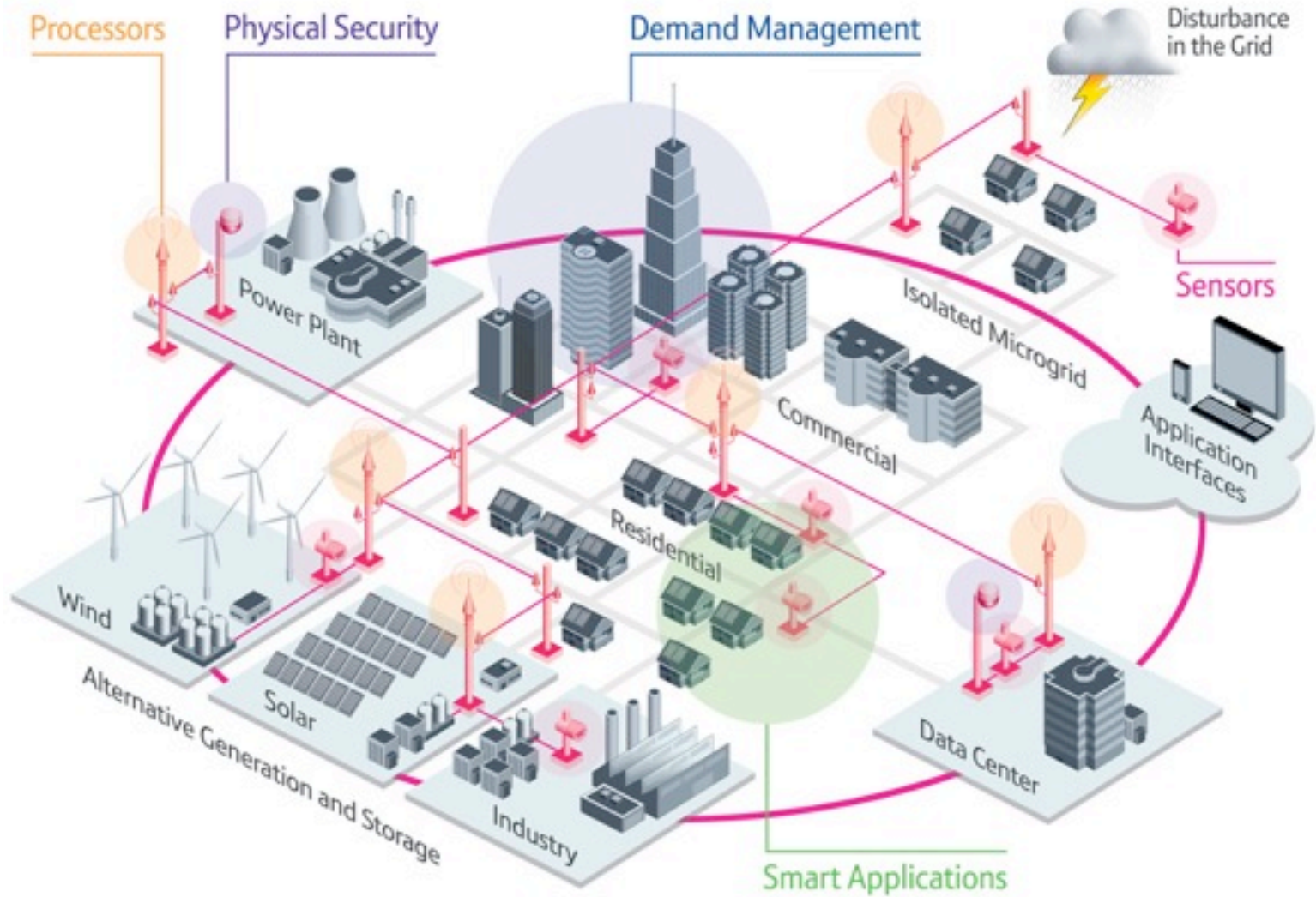
# What is a “Critical Infrastructure”

- **The framework of interdependent networks and systems** comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole.
- **Services and capabilities so vital** that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.

*Congressional Research Service Report to Congress, October 2004*



# What is Smart Grid



## A More Pragmatic Definition of the Smart Grid

*The Smart Grid encompasses the technology that enables us to integrate, interface with and intelligently control innovations such as wind turbines, plug-in hybrid electric vehicles and solar arrays and much more.*



# Smart Grid Business Drivers & Needs

## Business Trends & Drivers

## Consumer Needs

### Exponential Data Growth

- Rising Concerns on data security
- Carbon legislation

ation technology for data and network security

### Exponential Device Growth

- Ipv4 capacity exhausted by mid 2011
- Integration and migration issues over and above those attributable to smart grid

n strategy for Ipv6, Strategies for migration of IPv4 and IPv6 security controls

### Supply-Side Constraints

- Demand exceeding supply
- Carbon legislation

ng Infrastructure (AMI), Demand Response S

### Aging Workforce

- Knowledge retention issues
- ~30% of the workforce retiring in the next 5 years

through IT and OT (Operational ems

### Public Safety

- Grid is vulnerable to acts of terrorism and natural disasters

s, overhauls and replacements with "smart"

### Regulatory Concerns

- NERC-CIP; FERC; EPA; PUC's
- Data retention; energy efficiency; renewables

uilt in, not bolted on afterwards

### Economic Loss

- Outages cost US businesses > \$100B on an average year

he grid and automation in backend

# Smart Grid Business Drivers and Needs

- **Reliability**

- 5 massive blackouts over the past 40 years, 3 of those in the last 9
- More blackouts and brownouts are occurring due to
  - The slow response times of mechanical switches,
  - A lack of automated analytics, and
  - “Poor visibility” – a “lack of situational awareness” on the part of grid operators.
- This blackout issue has far broader implications than consumers waiting at home for the lights to come on.
  - Plant production stopped, Perishable food spoiling,
  - Traffic lights dark, and Credit card transactions rendered inoperable.

- **Economic Loss**

- A rolling blackout across Silicon Valley totaled \$75 million in losses.
- In 2000, the one-hour outage that hit the Chicago Board of Trade resulted in \$20 trillion in trades delayed.
- The Northeast blackout of 2003 resulted in a \$6 billion economic loss to the region.

# The Players



Energy Industry



Government



Consumers

# Energy Industry



**Generation**



**Transmission**



**Brokering and  
Distribution**



**Customer  
Operations**



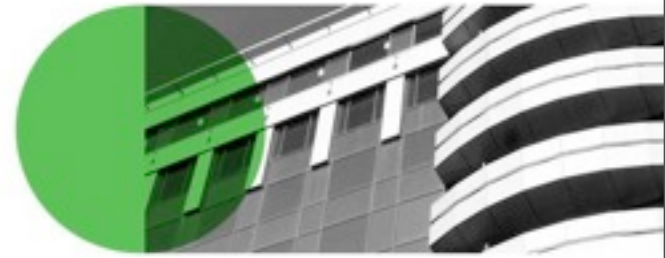
# Government

Some of the government agencies that are stakeholders in the Smart Grid initiative

- **NIST** – National Institute of Standards & Technology
- **FERC** – Federal Electric Regulatory Commission
- **NERC** – NA Electric Reliability Corporation
- **ISO-IEC** – International Electrochemical Commission
- **DOE** – Department of Energy
- **FCC** – Federal Communications Commission
- **DHS** – Department of Homeland Security
- **DOD** – Department of Defense
- **DOC** – Department of Commerce
- **GAO** – Government Accountability Office
- **GSA** – US General Services Administration
- **FBI** – Federal Bureau of Investigation



# Consumers



**Residential**



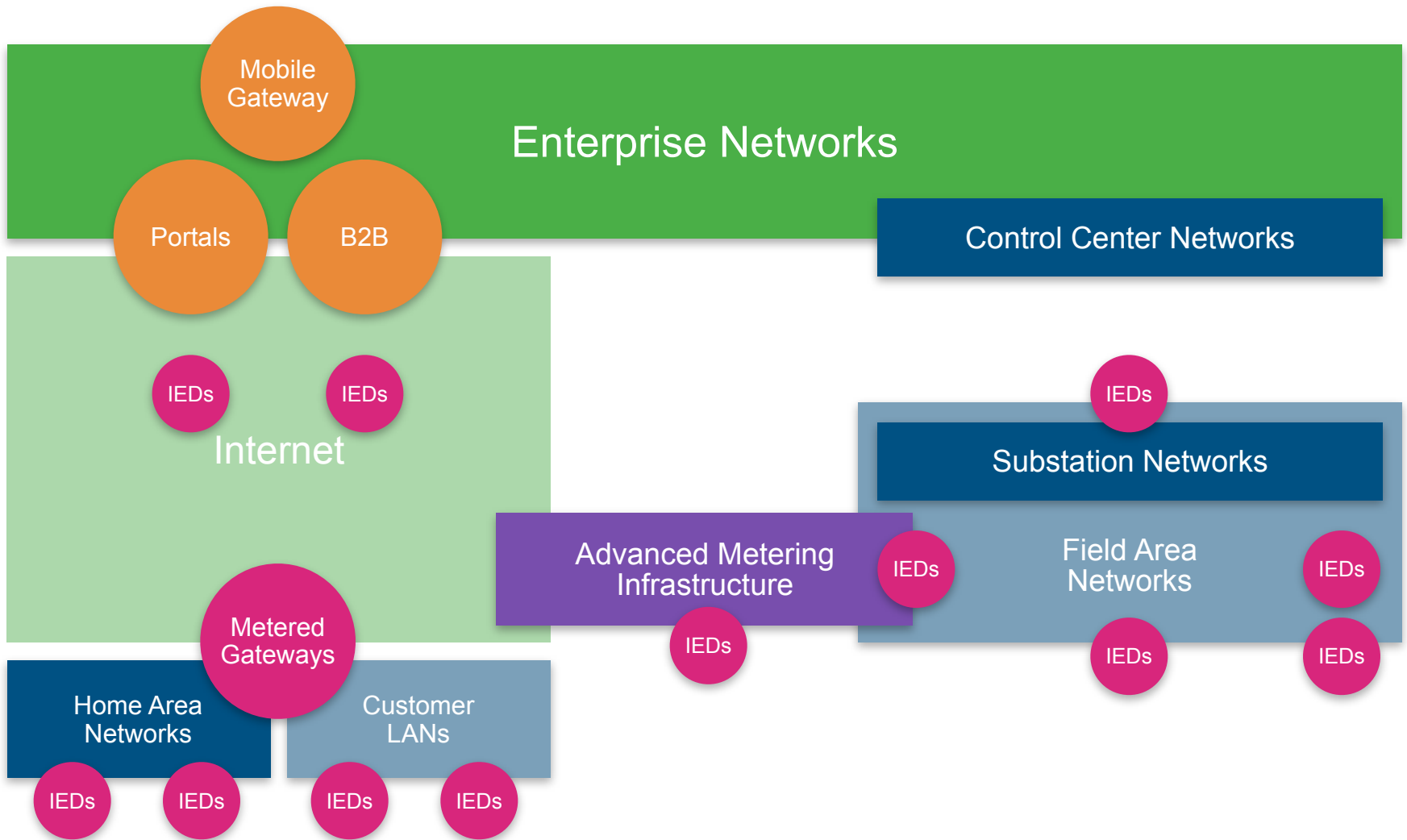
**Commercial**



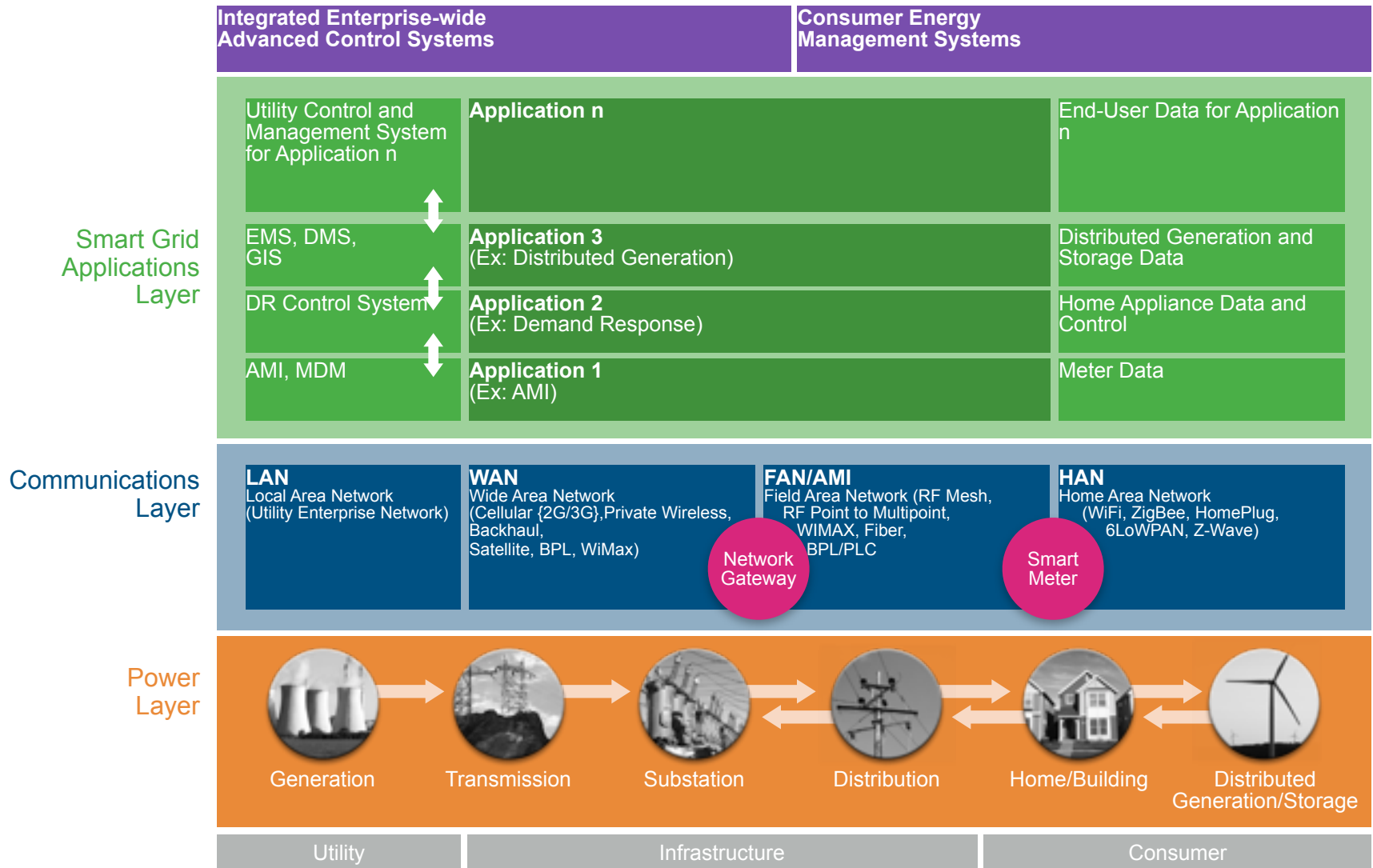
**Industrial**



# Smart Grid Components

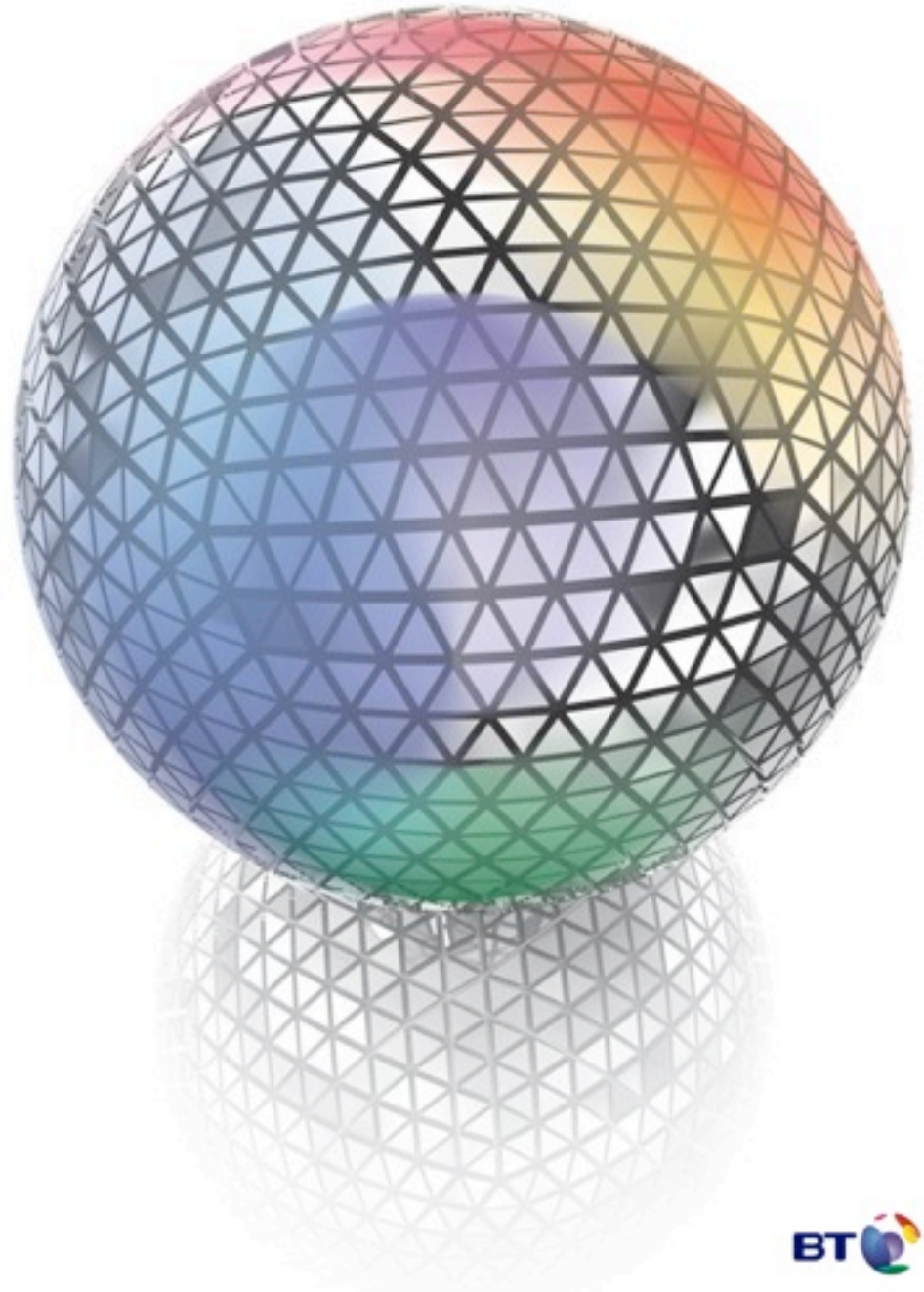


# End-to-End Smart Grid (High Level Taxonomy)



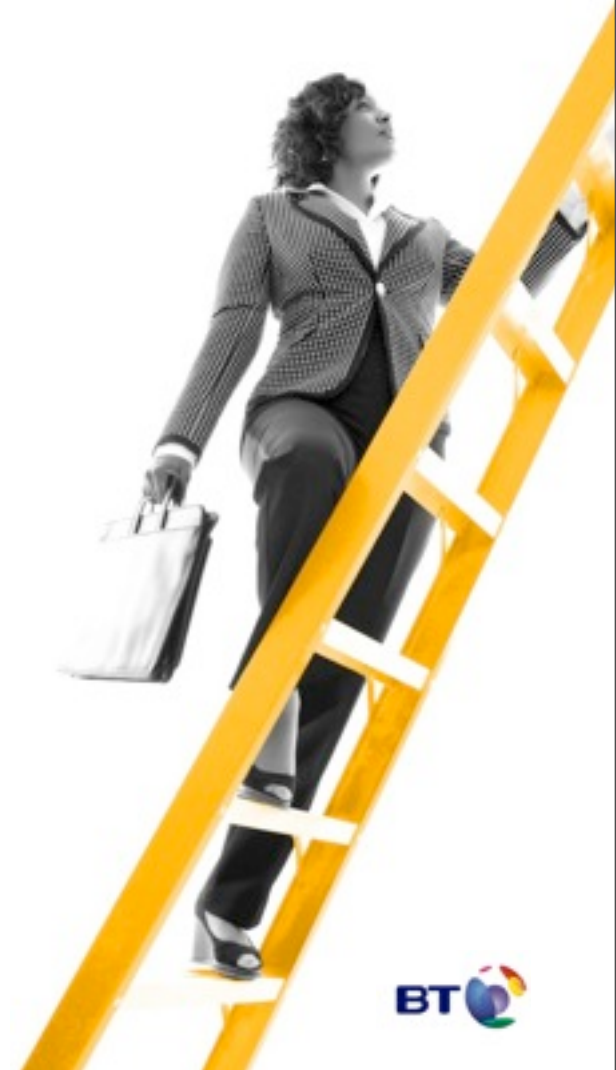
# Integration Technologies

- Firewalls, IDS/IPS etc.
- Webservers
- IPsec, SSL, TLS
- PKI – lots and lot of certificates
- Wireless
  - 802.11. long-haul 900 MHz
  - 802.15.4. aka Zigbee
  - WiMax
- Front End Processors
- System Bridges
- Remote station processing



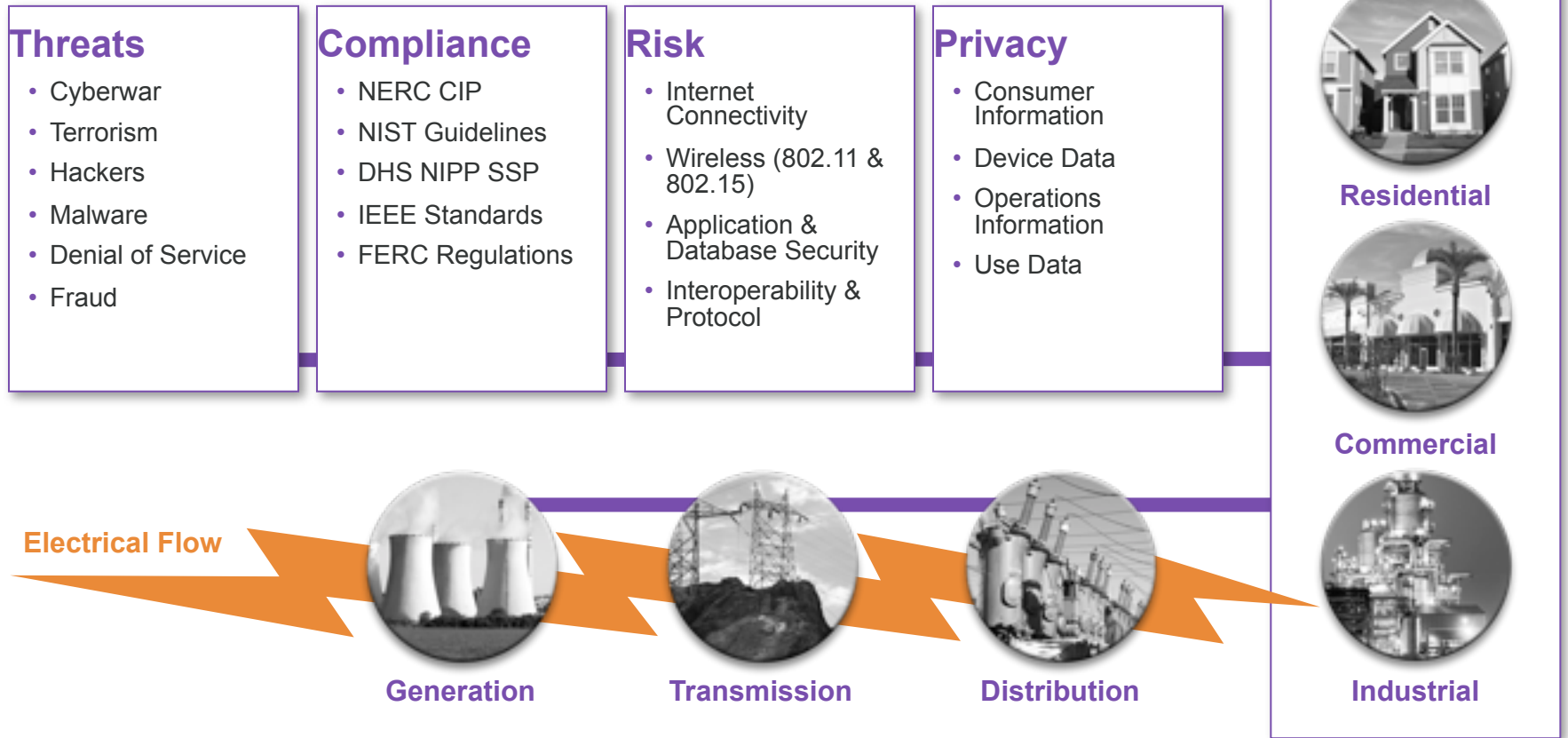
# Smart Grid Challenges & Opportunities

- A result of moving to a Smart Grid Ecosystem we will:
  - Introduce tens of millions of IP based devices onto the internet
  - Drive the need to perfect digital certificate key management systems as a national if not global infrastructure
  - Accelerate the exhaustion of the IP V4 address pool
  - Contribute to and perhaps be a major driver of IP V6 adoption
  - Integrate power generation control systems that have traditionally been physically isolated with administrative and financial systems across public networks
  - Drive the need to make this integration not only secure, but robust and operable in real-time across It systems and field equipment
  - This integration increases the overall complexity of the grid. This increase in complexity may introduce vulnerabilities, increase attack surface and be a catalyst for unintentional and unforeseen errors
  - Introduce potential privacy concerns for the consumer



# Smart Grid Security Challenges

Introduction of complex technology and networking into an already complex system



# Smart Grid Attack Surface

- Wide Area Networks – DDoS Attacks
- Metro Area Networks – Fiber Cuts - Sabotage
- Enterprise Networks – All the vulnerabilities that we know and love
- Mobile Gateways – Unauthorized access – session masquerading
- Portals – Information gathering
- B2B – Information modification
- Advanced Metering Infrastructure – Changing or hedging energy cost rates
- Substation Networks – Sabotage – theft of services
- Field Networks – Eavesdropping, hijacking services
- IEDs - Intelligent End Devices – zombies, botnets
- Home Area Networks – Privacy infringement
- Customer LANs – See Enterprise Networks
- DCP/DCP – Data Control/Collection Points – End point vulnerabilities



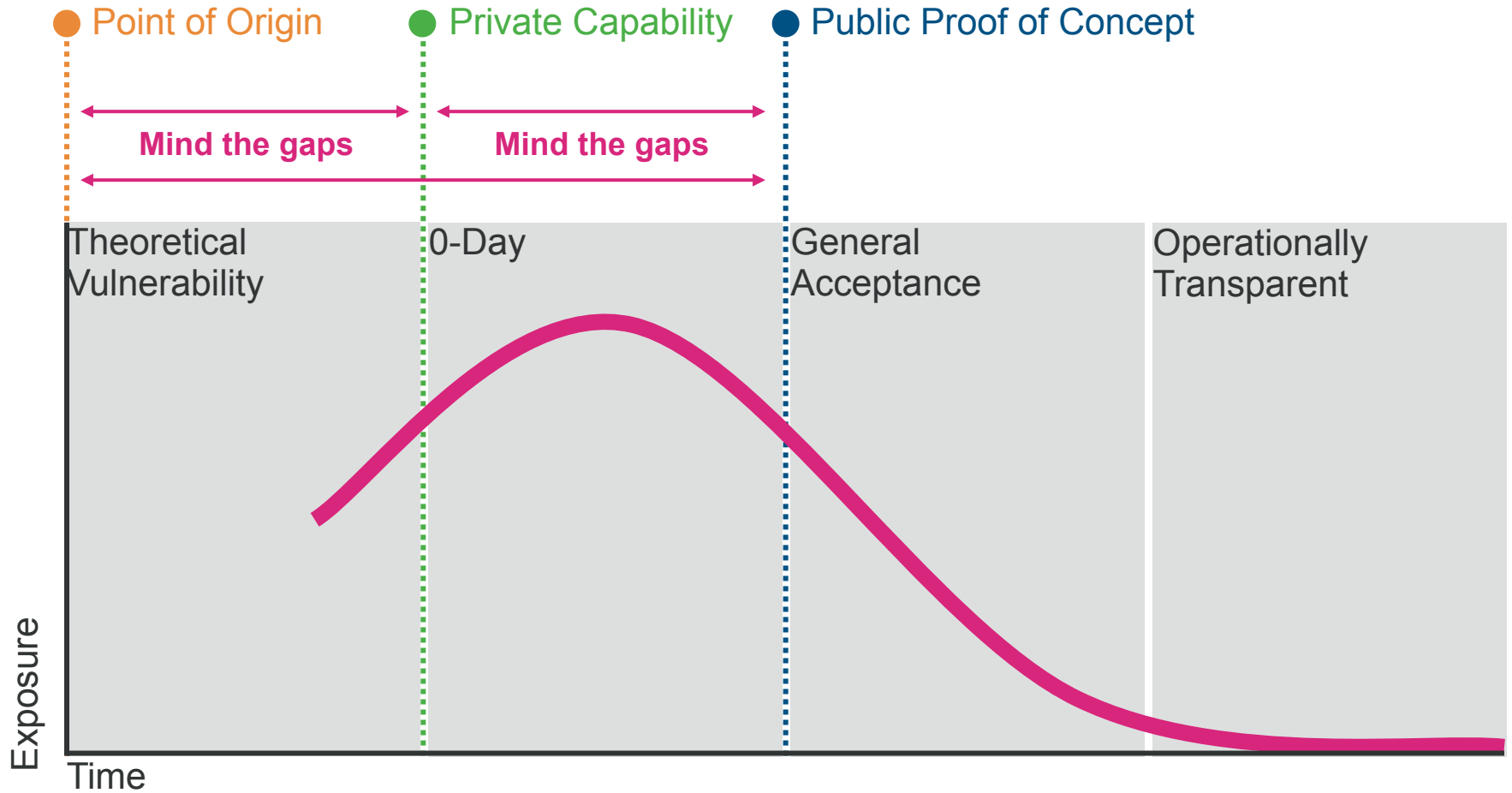
# Non-Technical Vectors

- Stupid Human Tricks
- Cost Avoidance Pitfalls
- Tactical versus Strategic
- Lack of effective regulations [one would think heavily regulated but much around security is voluntary and self regulated]



# POOH – Point of Origin Hacking

## Risk Management



# Scary Theoretical Risks

- DDoS attacks on the power grid
- Voltage Spike that destroys endpoints and infrastructure
- Highly coordinated attacks that turn the grid on itself
- Covert data channels that leverage the grid (botnet control channel that can't be disconnected)
- Appliances establishing Facebook accounts



# Risk, Reward and Reasonable Response

- Scenario 1 – Stuxnet, successful malware engine to infiltrate and impact industrial control systems
  - Risk – Industrial control systems using embedded Windows Operating Systems are exposed.
  - Reward - Not having your nuclear reactor go on-line on time!
  - Reasonable Response – Ensuring that there are sufficient safeguards and controls to compensate for the exposures associated with using industrial control systems using embedded Windows Operating Systems.
- Scenario 2 – Everyone knows when I am home!
  - Risk – Privacy Breach from sharing my electrical meter information on Google
  - Reward – Personal habits can be synthesized from this data
    - Power usage will vary when someone is home/not home
  - Reasonable Response – Don't share information just because it is possible.



## In Conclusion

- The question of “To Smart Grid” or “Not To Smart Grid” is a moot one. It is coming at us like a multi-engine locomotive. As an industry we need to work within this revolution and understand the risks and the ways to mitigate those risks very quickly.
- The deluge of new devices, technologies and the integration of those technologies with those that already exist will create an attack surface from a security perspective, the size of which far exceeds anything previously seen.
- The ultimate benefits of the Smart Grid far outweigh the risks.
- To fully leverage the Smart Grid Consumers (Residential, Commercial, Industrial) will need to become much more educated in the management of their own energy use.



# References

- GE's UTOPIAN Vision
- [http://ge.ecomagination.com/smartgrid/#/landing\\_page](http://ge.ecomagination.com/smartgrid/#/landing_page)
- Augmented Reality Technology applied to Smart Grid
- [http://ge.ecomagination.com/smartgrid/#/augmented\\_reality](http://ge.ecomagination.com/smartgrid/#/augmented_reality)
- NIST Framework and Roadmap for Smart Grid Interoperability
- [http://www.nist.gov/public\\_affairs/releases/upload/smartgrid\\_interoperability\\_final.pdf](http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf)
- Microsoft Smart Energy Reference Architecture
- <http://download.microsoft.com/.../microsoft%20smart%20energy%20reference%20architecture.pdf>
- US investments in Smart Grid Training
- <http://www.consumerenergyreport.com/2010/04/12/us-invests-in-smart-grid-training/>
- End-to-End" Smart Grid (High-Level) Taxonomy
- <http://www.greentechmedia.com/articles/read/defining-an-end-to-end-smart-grid/>
- Summaries of Use, Application, Cybersecurity, and Functionality of Smart Grid Interoperability Standards Identified by NIST
- <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTStandardsSummaries>

# Questions

- Jason Stradley
- Jason.stradley@usc-bt.com

