Symantec™

Why is the Smart Grid a Target?

July 30, 2012

What is the Smart Grid

Transformation – the most significant in a century

Transformation

- *The Smart Grid is the most significant change in the electrical grid in 100 years*
- *Smart Grid affects power and process manufacturing industries across the board*
- *Critical impact to Telcos and Government organizations*

Challenges

- New benefits and new risks: command systems are now more powerful but the security attack surface increases exponentially
- Massive amount of new data generated which:
  - Must be efficiently managed
  - Must be protected and customer privacy ensured
  - Must support auditing & compliance
- Scaling operations to manage tens of millions of meters and SCADA devices

> ***"Dynamic optimization of grid operations and resources."***
>
> ***"Incorporation of demand response and consumer participation."***
>
> **- Secretary Steven Chu, U.S. Department of Energy**

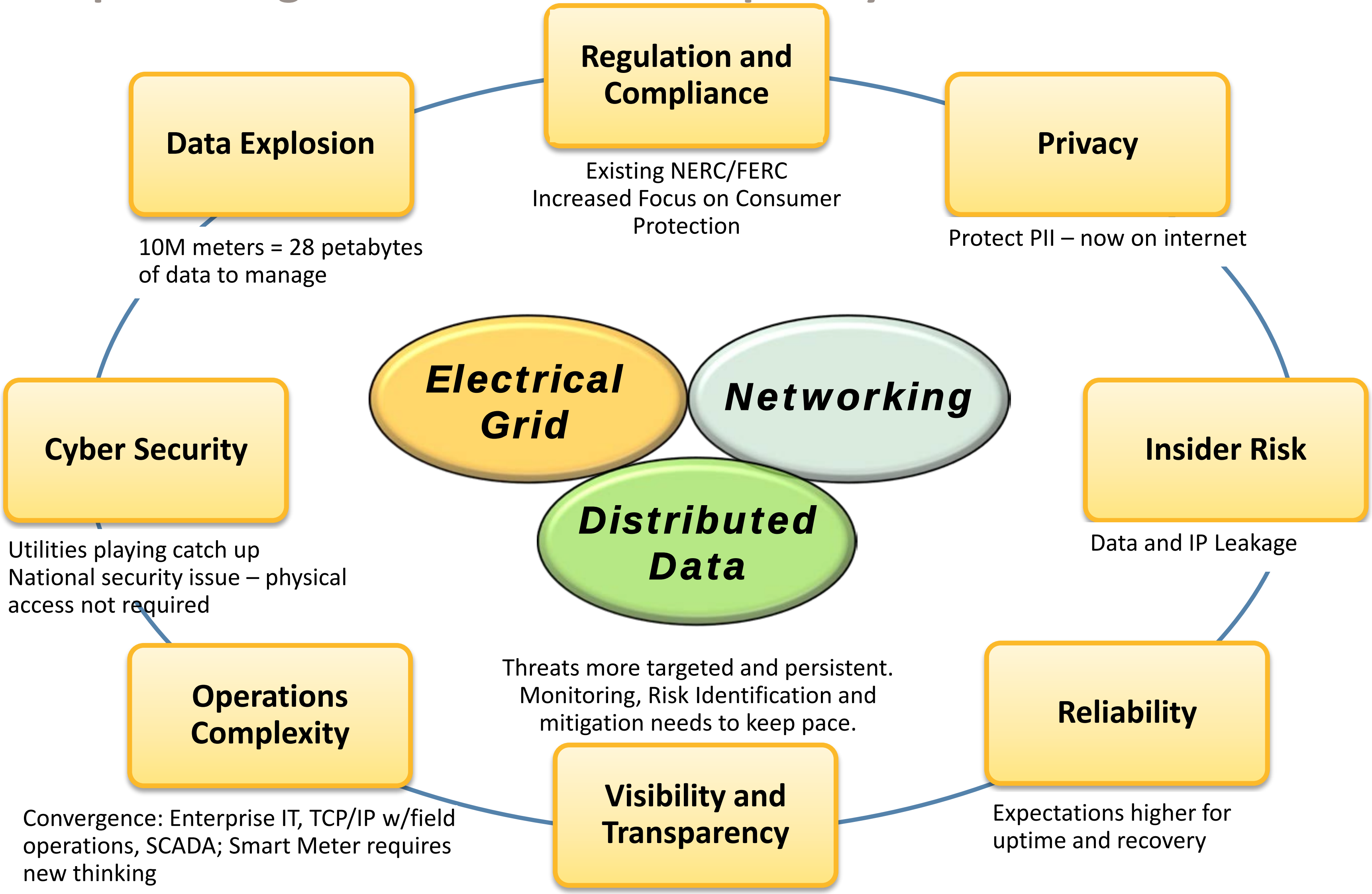
Threats

- Chinese researchers at the Institute of Systems Engineering of Dalian University of Technology published a paper on how to attack a small U.S. power grid sub-network in a way that would cause a cascading failure of the entire U.S. Grid
- InGuardian: "smart" meters that are designed to help deliver electricity more efficiently also have flaws that could let hackers tamper with the power grid in previously impossible ways
- Recent Stuxnet worm specifically targeted Windows-based SCADA environments; Duqu, Flamer info finding

The Electrical Grid is becoming an IT/IP Network

Energy Industry Challenges

Rapid Change and Increased Complexity



Regulation and Compliance

Existing NERC/FERC
Increased Focus on Consumer
Protection

Data Explosion

10M meters = 28 petabytes
of data to manage

Privacy

Protect PII – now on internet

Cyber Security

Utilities playing catch up
National security issue – physical
access not required

Electrical Grid

Networking

Distributed Data

Insider Risk

Data and IP Leakage

Threats more targeted and persistent.
Monitoring, Risk Identification and
mitigation needs to keep pace.

Operations Complexity

Convergence: Enterprise IT, TCP/IP w/field
operations, SCADA; Smart Meter requires
new thinking

Reliability

Expectations higher for
uptime and recovery

Visibility and Transparency

Critical Infrastructure – In the Headlines ...

WIRED

January 24, 2012

10K Reasons to Worry About Critical Infrastructure

MIAMI, Florida – A security researcher was able to locate and map more than 10,000 industrial control systems hooked up to the public internet, including water and sewage plants, and found that many could be open to easy hack attacks, due to lax security practices.

Infrastructure software vendors and critical infrastructure owners have long maintained that industrial control systems (ICSes) — even if rife with security vulnerabilities — are not at risk of penetration by outsiders because ....

REUTERS

US infrastructure sees spike in cyber threats

Mon, Jun 18 2012

BOSTON, July 3 (Reuters) - Cyber threats reported by U.S. energy companies, public water districts and other infrastructure facilities surged last year, a new government report shows. The Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team said that it received 198 reports of suspected cyber incidents, or security threats, in 2011, more than four times the 2010 level.

EuropeanVoice.com

01.09.2011

Co-ordinate EU defences or risk losing cyber battles

By Christian Ehler and Jorgo Chatzimarkakis

The EU's agency for improving cyber-security must be given greater powers.

Imagine this scenario: all important institutions of a country find their access to the internet blocked. Highly developed software deletes vital data. The country is thrown back into the information Stone Age. There is a total information black-out. This, though, is not an imaginary scene. It has already happened in the EU ...

Forbes

June 12, 2012

To Spy On Offline Computers, Flame Malware Was Designed To Turn Humans Into 'Data Mules'

The program known as Flame has fascinated the cybersecurity industry with its sophistication and versatility as a Swiss-Army knife of cyberspying. Now researchers have discovered another unexpected tool in its data-stealing arsenal: You.

Flame can also move the target information–along with a copy of itself–onto a USB memory stick plugged into an infected machine, ...

InformationWeek

As Congress Debates Critical Infrastructure Security, Danger Grows

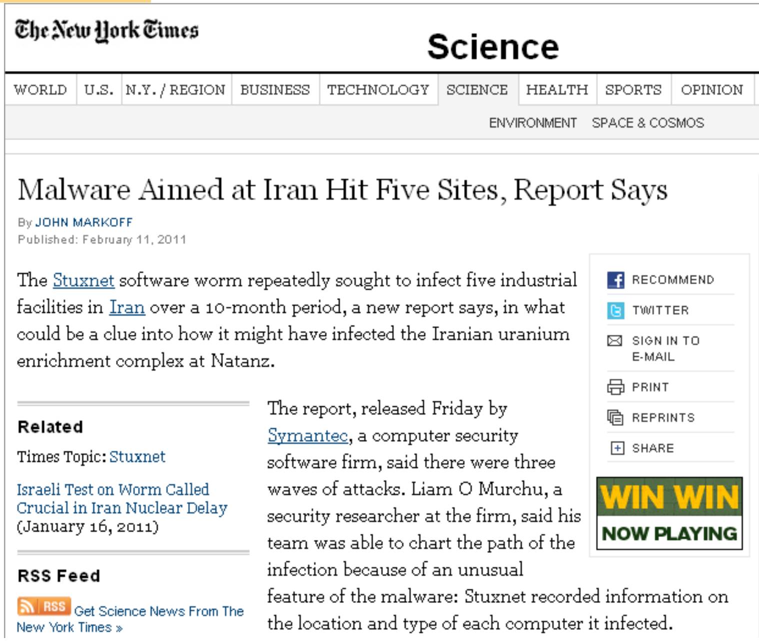
Security experts warn that new tools make it easier than ever to attack critical infrastructure control systems, as Congress debates legislative action.

By Mathew J. Schwartz InformationWeek

March 06, 2012 12:16 PM

10 Massive Security Breaches

How long might it take to properly secure the systems that comprise the critical infrastructure? Try 25 years, give or take half a decade.



Malware Aimed at Iran Hit Five Sites, Report Says

By JOHN MARKOFF
Published: February 11, 2011

The Stuxnet software worm repeatedly sought to infect five industrial facilities in Iran over a 10-month period, a new report says, in what could be a clue into how it might have infected the Iranian uranium enrichment complex at Natanz.

The report, released Friday by Symantec, a computer security software firm, said there were three waves of attacks. Liam O Murchu, a security researcher at the firm, said his team was able to chart the path of the infection because of an unusual feature of the malware: Stuxnet recorded information on the location and type of each computer it infected.

Related

Times Topic: Stuxnet

Israeli Test on Worm Called Crucial in Iran Nuclear Delay (January 16, 2011)

RSS Feed

RSS Get Science News From The New York Times »

Critical Infrastructure Security Concerns Growing ...

Changing Threat Landscape – revisited in 2011

Old Motivation

New Motivation

Newest Motivation

Fame

Fortune

Political

- Threats persist with a goal of notoriety.
- Threats are visible and indiscriminate.
- "Big splash" approach.

- Threats are fleeting with a goal of profit.
- Threats are silent and highly targeted to compromise target or steal data.

- Highly sophisticated
- Infinite financial resource
- Well-planned and executed with unprecedented levels of control.

Computers & Networks

People, Identities, & Information

Espionage and Sabotage

- Attackers are increasingly developing highly sophisticated methods with the goal to penetrate rather than destruct.
- Attacks can affect critical infrastructure and embedded devices across many industries

- The goal is to do damage, destruct, influence, reach political goals, or support a conventional attack.

Two Worlds – Different Perspectives

Business Network

Production Network

1.) Confidentiality
2.) Integrity
3.) Availabilty

1.) Availabilty
2.) Integrity
3.) Confidentiality

Two worlds – main differences

	Business IT	Industrial IT
Latency	Limited relevant	High critical
Patch Management	Often up to daily	Rarely, often needs additional approval from 3rd party vendor
Management	Centralized	Often standalone
Lifecycle	3 -5 years	5 – 20 years (unsupported OS‘s like NT and older)
System changes	Often	Rarely
Availability	Reboot is accepted	24 x 7 x 356
Virus protection	Standard	Complex, and often not possible
Awareness	Good	Poor
Vulnerability checks	Standard	Rare and complex (availability)
Outsourcing	Usually	Rarely
Physical Security	Safeguarded and close areas	Unmanned and wite areas

Advanced Persistent Threats

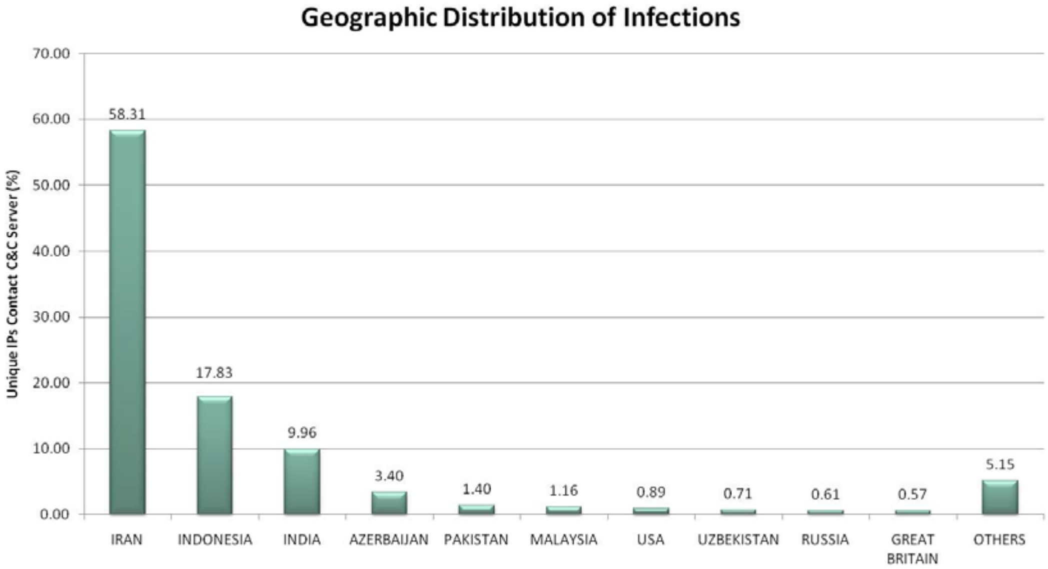
- Attack multiple industries …
  - Utilities: Water, Sewage, Gas, Power
  - Manufacturing
  - Financial
  - Automotive
  - Energy: Oil and Gas
- Sophisticated attacks created by well resourced organizations
- Stealth: APTs can stay hidden for years before discovered
- Numbers are growing: The Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team said that threats increased 4 fold from 2010 to 2011.

Industrial Security, Critical Infrastructure and Advanced Persistent Threats (Stuxnet, Duqu, Flame,...)

Stuxnet Example: Energy Industry Threats

Attackers are rapidly ramping up attacks

- Affects all popular versions of **Windows**
- Targeting known weaknesses in **SCADA** systems including automation layout design and control files
- Uses 4 Microsoft zero-day exploits, plus 1 **already known vulnerability**
- Uses 7 different self-propagation methods including USB drives
- Allows for malicious code execution on the system
- **Code signed** by Realtek Semiconductor Corporation *(Certificates were stolen)*
- Acts as a rootkit to hide itself enabling stealth movement
- Modifies and hides code on Siemens PLCs connected to frequency converters
- Attacks industrial control systems likely an Iranian uranium enrichment facility



Source: http://www.symantec.com/connect/blogs/w32stuxnet-network-information

Stuxnet: Things to Consider

Windows Systems Security

- One vulnerability known; other patches available quickly
- Application control, Intrusion Prevention, Sandboxing

Certificate Management

- Authentication of device identity
- Operations certs to authenticate device to Network Operating Center (NOC)
- Do not provision firmware without valid certificate

Air gaps: Do Not Protect

- Contractor system: was on internet, now on private LAN
- Testing, and pushing applications directly to the field
- USB drives … do not allow automatic execution

SCADA Security

- Security for SCADA systems – security needs to be built-in from the ground up

W32.Flamer in one minute

- Designed to steal information and lots of it
- Uses old & patched vulnerabilities
- Worm-like propagation capabilities, controlled through C&C servers
- Window of attack: <2010 – 2012
- Low number of infections, mostly in: Palestinian West Bank, Hungary, Iran & Lebanon
- Wide array of functionality built in & also extensible
- New features: Junction points & Bluetooth
- The work of a well organized team

W32.Flamer

vs

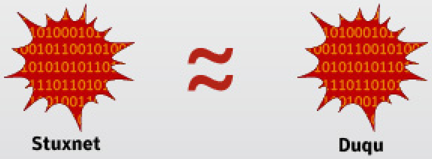
W32.Stuxnet and W32.Duqu

A quick comparison of the three threats.

All three threats appear to be developed by teams of attackers, rather than a lone individual.

All three threats were discovered within the Middle East

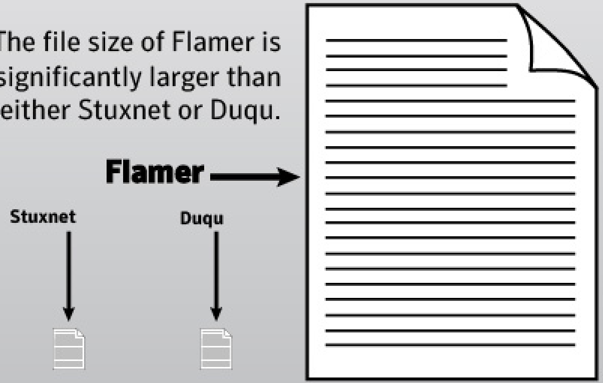
The code base behind Stuxnet and Duqu are similar.



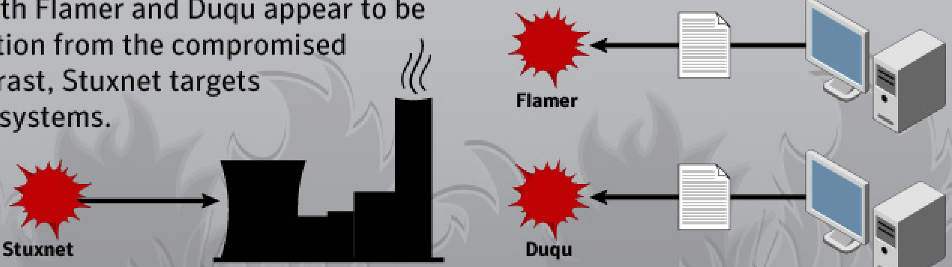
The code base from Flamer is different from the other two.

All three threats were advanced persistent threats that targeted industrial or government systems.

The file size of Flamer is significantly larger than either Stuxnet or Duqu.



The purpose of both Flamer and Duqu appear to be to gather information from the compromised computer. In contrast, Stuxnet targets industrial control systems.



Symantec.

BWI ranking of Industrial Vulnerabilities

BWI ranking	BWI Vulnerability descrption	Business IT - Product Matching
1	Non authorized using of remote access	One time password authentication, system lockdown, event correlation
2	Online attacks over the Office and Enterprise Network	Compliance automation, firewalls, system lockdown, event correlation, scanning (gateway, file, anti-virus, etc)
3	Attacks again standard ICS components (Application Server, DB)	Compliance automation, firewalls, system lockdown, scanning
4	(D) DOS attacks	Log and event correlation
5	User and Sabotage	Compliance automation
6	Attacks over remote devices (USB)	Data encryption, compliance automation, firewalls, system lockdown, scanning
7	Read and write of messages over the ICS network	Data loss prevention, compliance, scanning, firewall and intrusion prevention/detection
8	Unauthorized access to resources	Compliance, scanning, firewall and intrusion prevention/detection
9	Attacks agains network and network components (Man-in-the-middle Attack)	Log and event correlation, intrustion prevention / detection
10	Technical issues	Compliance automation

Electrical Grid: IT and Operations Architecture

Grid Technology

Content

Data at Rest

- Customer billing
- Personal data / privacy
- Data retention
- Compliance
- MDM (meter) data hub

Infrastructure

- Servers
- Storage
- Gateways
- Grid IT asset management

Network/Cloud

Data in Motion

- Private & public cloud / networks
- Networks are IP based

Embedded Devices

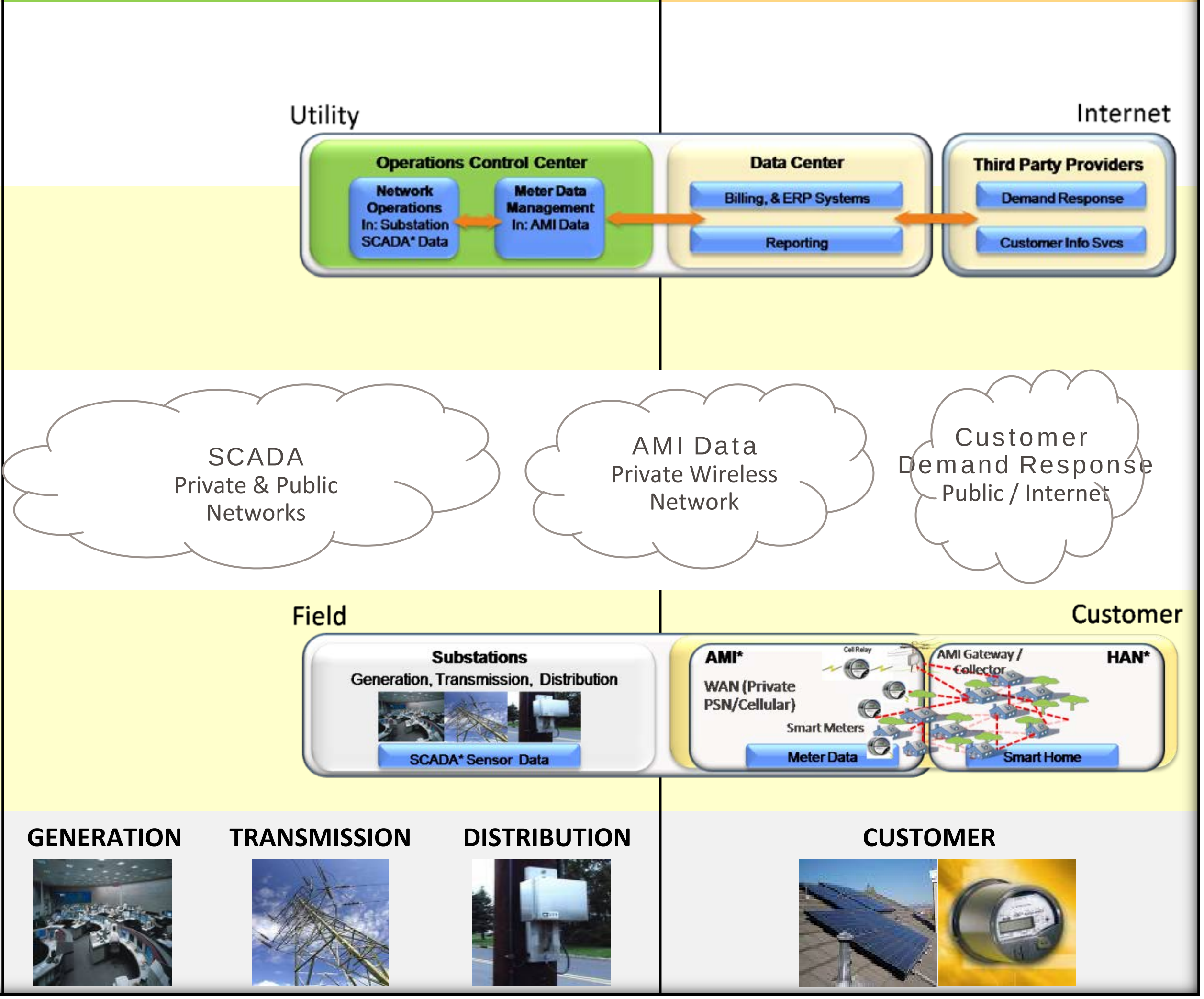
Data in Use

- Substations: Windows XP embedded (XPe), Linux, Intel
- Meters: ARM, Flash

Electrical Grid

Operations

Service Providers



Security Architecture for the Smart Grid

Approaches | **Operations** | **Service Providers**

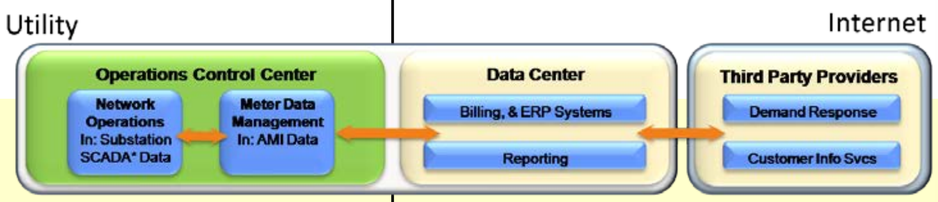
Content

Data at Rest

- Data-centric security: authenticate devices & people; mine, encrypt & protect data
- Compliance

Infrastructure

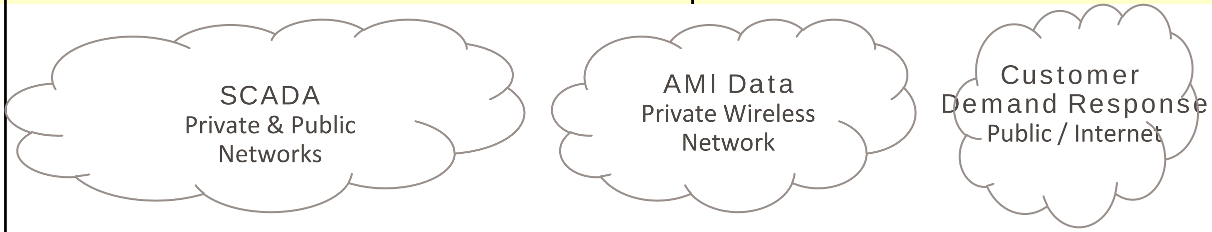
- Server hardening
- Efficient storage management
- Disaster recovery
- Asset management



Network/Cloud

Data in Motion

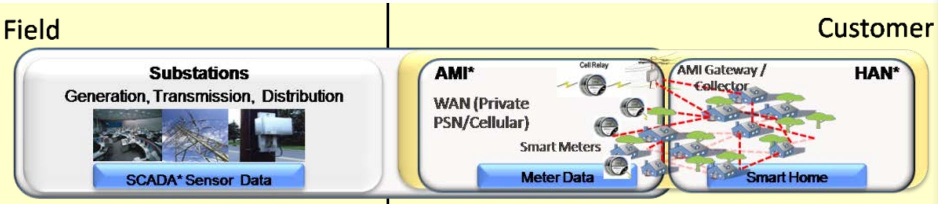
- Hosted Services - security, certificate & key management
- Hosted PKI
- Network access control



Embedded Devices

Data in Use

- Harden substation Windows systems
- Authenticate devices (AMI, SCADA)
- Encrypt data
- Client Management



Electrical Grid

GENERATION

TRANSMISSION

DISTRIBUTION

CUSTOMER

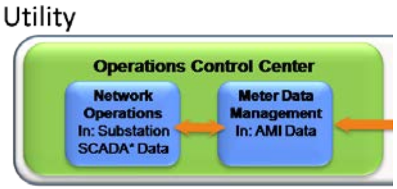
Solutions

Securing and Managing Information: Associating Assets and Data with Identity

	Approach	*Solutions*	*Benefits*
Content *Data at Rest*	• Data protection • Data categorization, discovery, & control • Security detection & response • Compliance	• Backup • Policy-based Control of information, categorization & Information archiving and cataloging • SEIM: Incident detection , correlation, reporting and management with workflow • Automated compliance	• Long term retention of data • Control access to critical information; discovery of pertinent data • Security incident management • Lower cost compliance, data integration
Infrastructure	• Server hardening • Efficient storage / Disaster recovery • Intrusion Detection	• Server and host lockdown with application whitelisting • Storage management and disaster recovery • Anti-virus, intrusion protection for hosts and servers	• Fine grained application, resource control • Increasing capabilities in cloud, efficient management of storage, disaster recovery • Protection of entire head-end and back office environment
Network/Cloud *Data in Motion*	• Cloud security Services • Certificate & key management • Network Access Control • Critical data monitoring	• Global Information Network – Honeypot • Authentication, One time passwords, key management • Intrusion prevention / detection • Data Loss Prevention	• Early warning for attacks (Conficker, Stuxnet) • Trust services - encryption, certificate & key management w/hosted PKI: device to data center • Proactive IDS/IPS security w/ zero day protection & behavioral / reputation based design • Control critical information before allowed outside firewall
Embedded Devices *Data in Use*	• Secure windows endpoints in substations • Encrypted data, authentication for AMI & SCADA networks	• Remote Anti-virus • System lockdown and hardening • Application whitelisting • Data encryption and device authentication and user authentication / credentials based on user certificates	• Small footprint agent for application control, granular resource access control, change control and configuration management • Trust for devices and users ; secure configuration management and provisioning
	Electrical Grid	**GENERATION** **TRANSMISSION** **DISTRIBUTION**	**CUSTOMER**

Symantec Smart Grid Solutions – ‘Four Pillars’

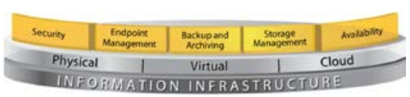
Operations Security

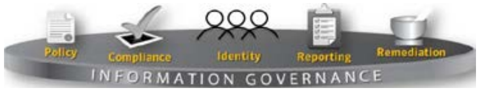

Utility
Operations Control Center
Network Operations In: Substation SCADA* Data
Meter Data Management In: AMI Data

- Utilize ‘defense-in-depth’ techniques
- Leverage years of network security experience in IP world

- Make state of the art IT security solutions ubiquitous in the operations control centers
- Utilize Common Data model: information shared among solutions to meet regulatory compliance needs

Manage Data Explosion





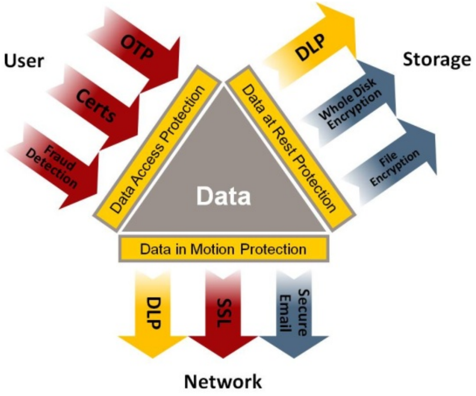
Information Infrastructure

- Storage management
- Data protection
- Archiving
- Legal discovery

Information Governance

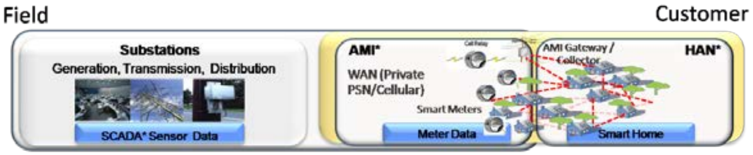
- Compliance
- Control access
- Regulatory & auditing
- Customer Privacy
- Reporting

Embed Security with Data



- Encrypt information
- Authenticate devices
- Manage keys
- Manage certificates at scale
- Managed / hosted PKI & device level certificates

Manage Endpoints



- Manage Windows sub-station automation systems
- Securely update device firmware e.g. AMI collectors
- Securely invoke SSL services through trusted mechanisms resident on device

Industrial challenges across various dimensions

Data Deluge & Complexity

Data Growth & Complexity

- *Unstructured data increasing as percentage of information growth*
- *Data growth and storage needs growing at astronomical rates*

Availability

Outage Management

- *Security focus requires focus on understanding and controlling operational environment: therefore can help with outage detection and management*

Security & Insider Risk

Threats

- *Early warning on threats and vulnerabilities critical*
- *Rapid detection of security attacks*
- *Effective response*

Management

Endpoint Management

- *Secure endpoint is a well managed endpoint and vice versa*
- *Managing nodes at scale is first line of defense for security*

Compliance & Privacy

Compliance and Privacy Protection

- *Compliance, required by regulatory bodies, can also help provide an management infrastructure*
- *Increasingly, end customers are focused on privacy*

Ideas to consider

- Public – Private partnership
- Develop early warning system
- Joint effort of utilities, security industry and government to share information to provide early warning of attacks wherever they occur

Summary

- Industrial Security is complex
- Industrial Security is a process and not a single product
- Industrial Security Solutions should be open to 3rd party vendors
- Compliance approach should be the prefered method and starting point
- Industrial Security needs experienced security expertise

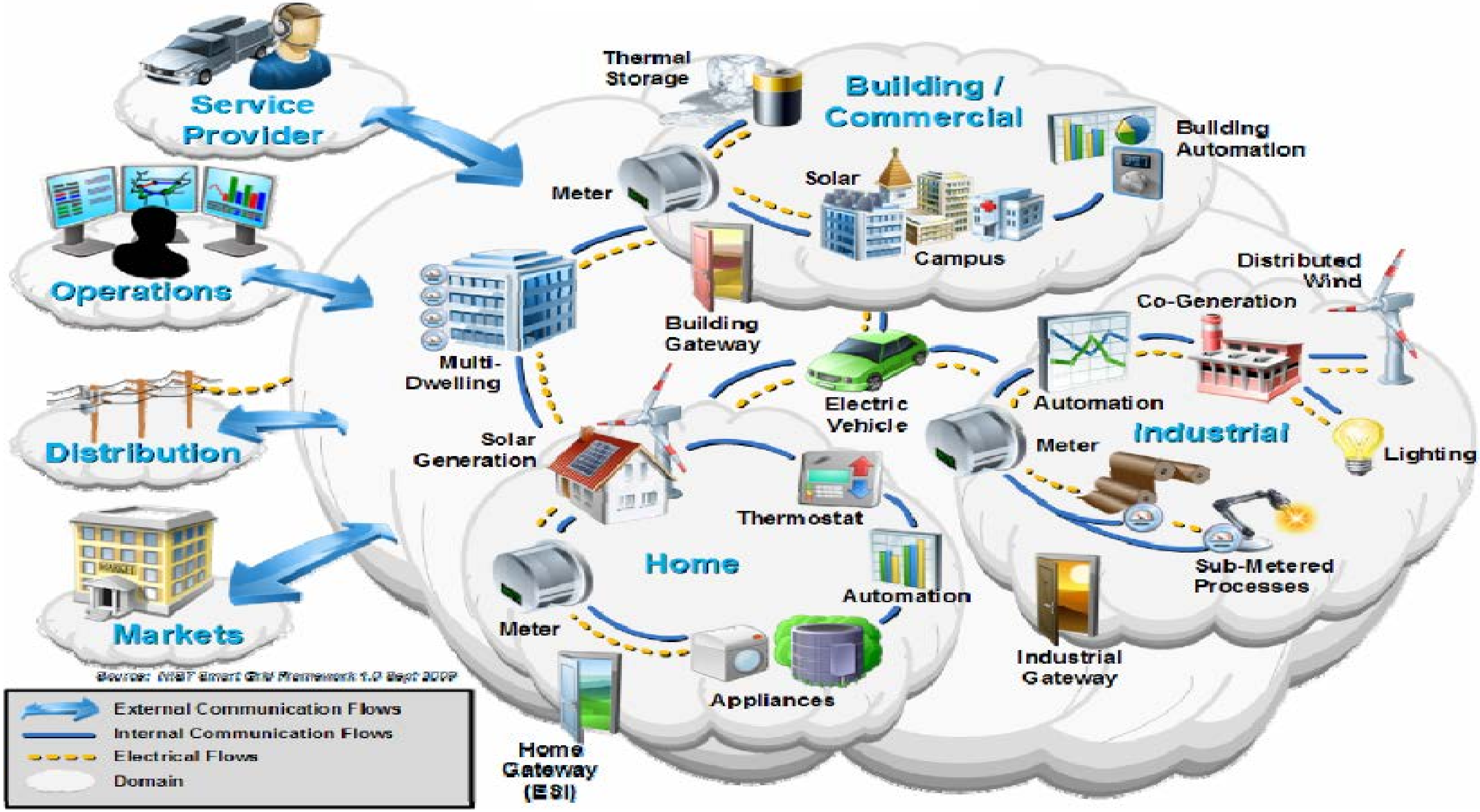
Thank you!

Jose Iglesias
Vice President
Symantec Corporation
Jose_iglesias@symantec.com

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Appendix

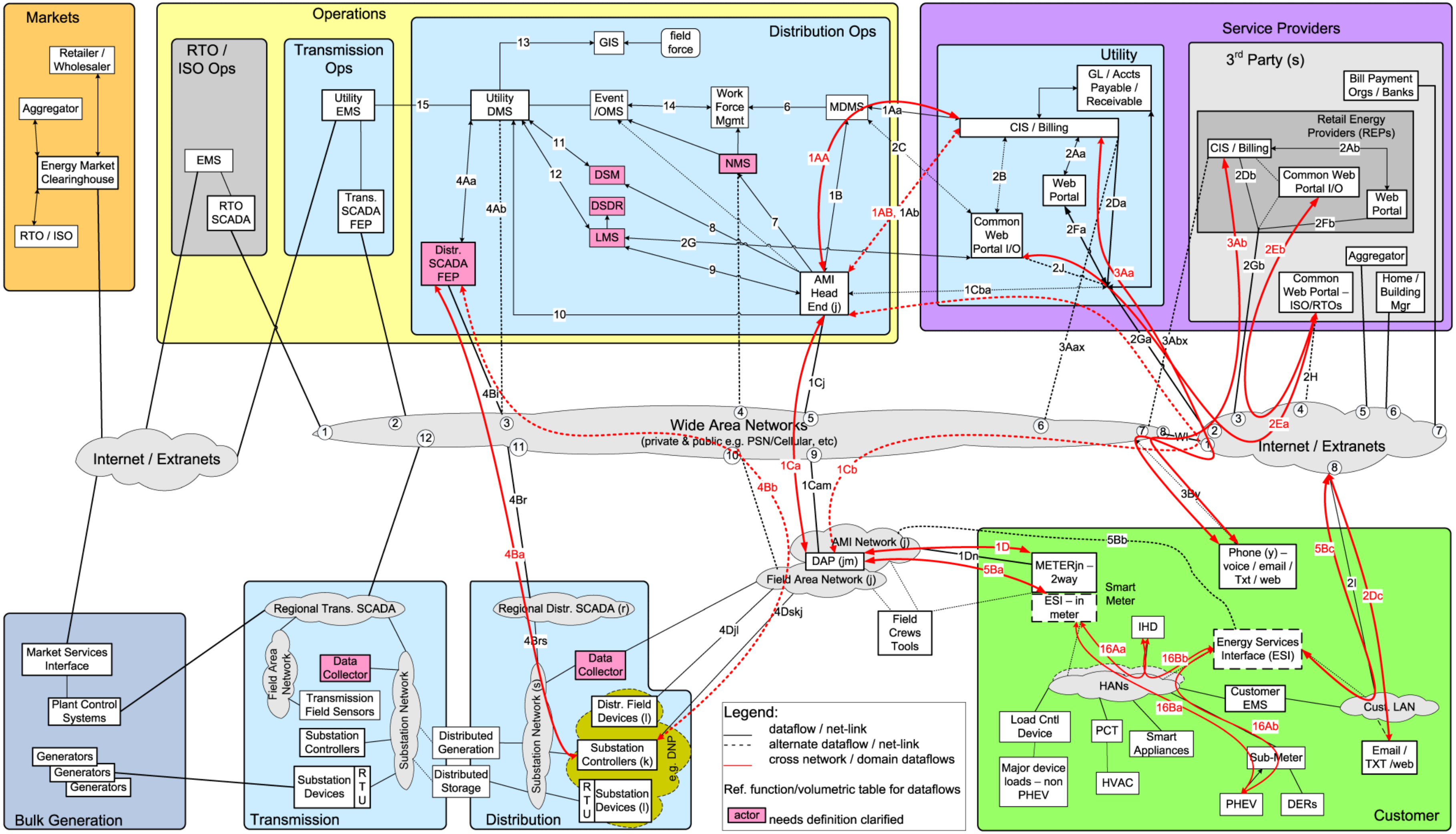
NIST Roadmap for Smart Grid Interoperability



Source: NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0

Smart Grid Conceptual Actors / Data Flow Diagram – Cross Domain Network Focused – OpenSG / SG-Network TF

DRAFT 01Feb10
Base – file SG-NET-diagram-r0.4a.vsd
page size: ANSI-D



Legend:

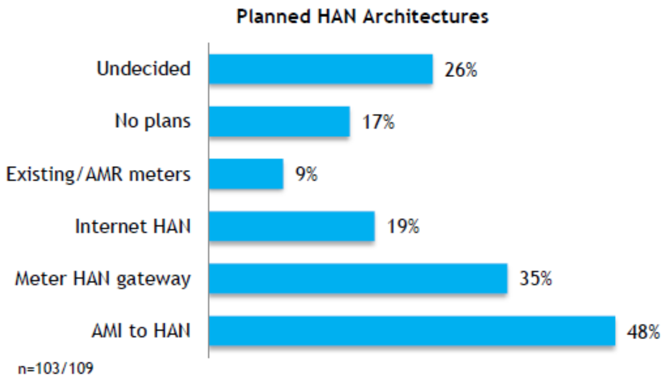
dataflow / net-link
alternate dataflow / net-link
cross network / domain dataflows

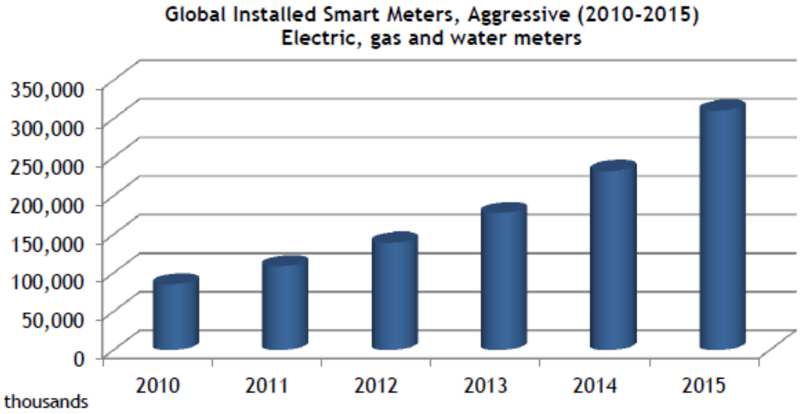
Ref. function/volumetric table for dataflows

actor needs definition clarified

Smart Grid Market is Global

- Mainly North America, European and Asian market
- Up to **300m smart meters installed worldwide in 2015[1] (85m installed in 2010)** are expected
- Europe with its 200m households will surpass North America as the largest smart metering market within the next 5 years[1]
- Asia will be the fastest growing market during the next 5 years[1]
- US Smart Grid market is expected to grow from $5.6bn in 2010 to $9.6bn in 2015[2].
- Net investment required to build US smart grid over next 20 years is approx. $338bn - $476bn[3]. Net benefit in same time frame is approx. $1,294bn - $2,028bn[3].





[1] ON World, Smart Metering, 2011

[2] GTM Research, U. S. Smart Grid Market Forecast 2010 - 2015

[3] EPRI, Estimating the Costs and Benefits of the Smart Grid, 2011