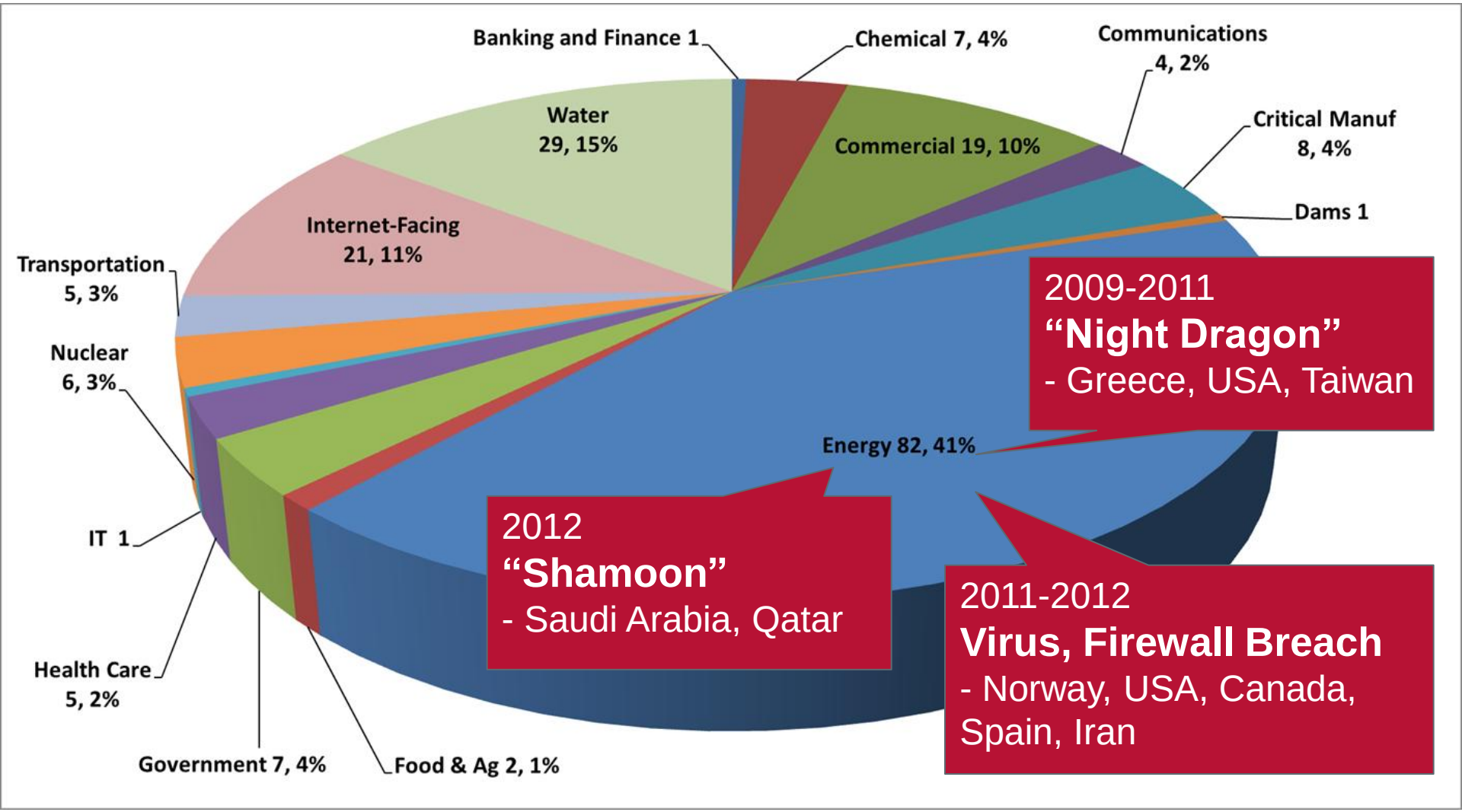

McAfee
An Intel Company
Safeguarding Smart Grids
Sentient Cyber Security for Critical Infrastructure
Lorie Wigle: VP Security Fabric McAfee/GM Intel
Raj Samani: VP CTO EMEA McAfee
Hannes Schwaderer: EMEA Energy Director Intel
September 20, 2013
SAFE NEVER SLEEPS.

2012 US Control Systems Incident Response



Incidents by Sector for fiscal year 2012, Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team

What are the Cyber Threat Vectors and Impact to Energy?

Cyber threats are strategic attacks aimed at disrupting industrial activity for benefits spread across monetary, competitive and political factors.

Political

This includes attacks sponsored by state or non-state actors, who attempt to disrupt industrial operations and cause large-scale destruction for political reasons.

Competitive

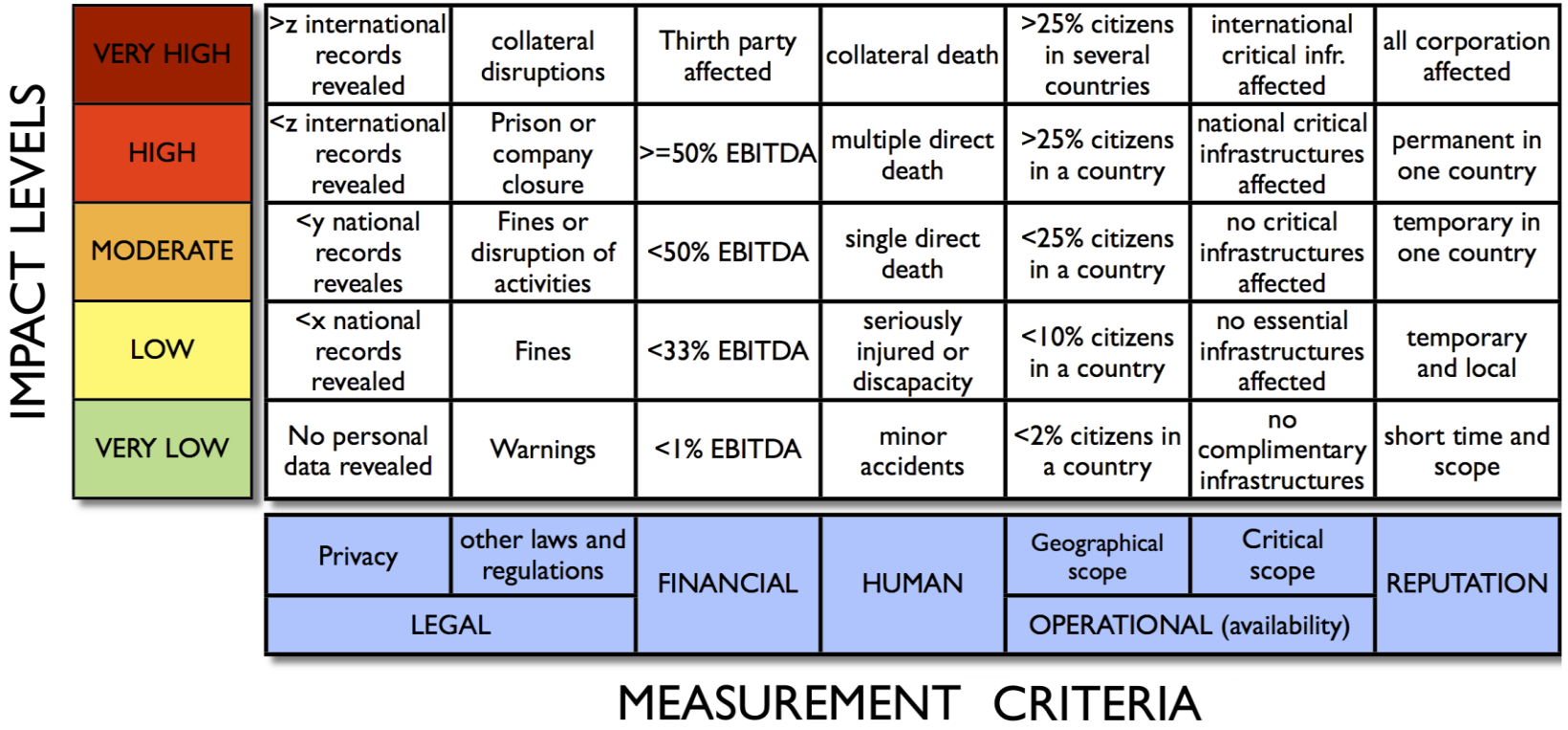
This includes attacks sponsored by competitors keen on gaining market supremacy and increasing profitability.

Monetary

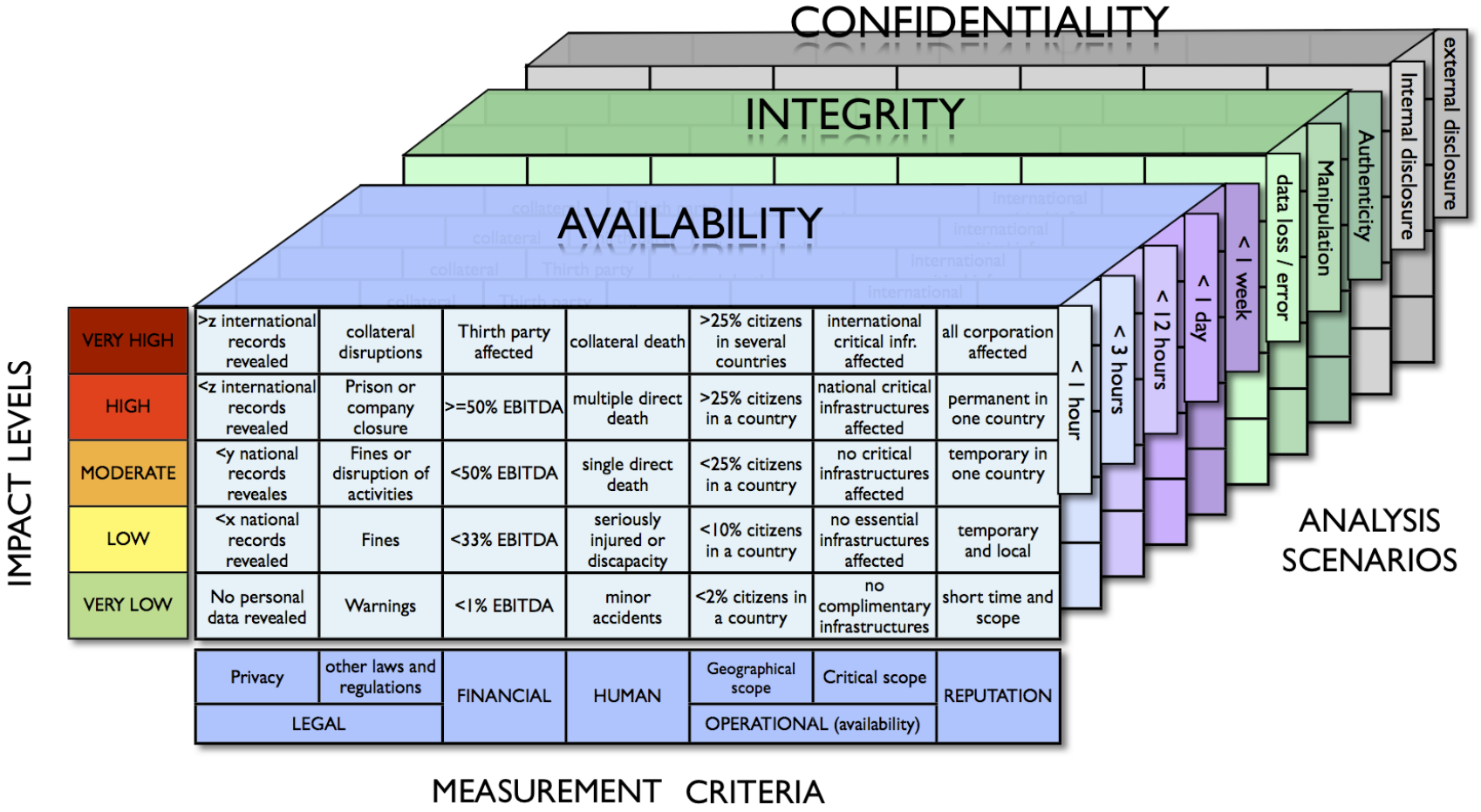
This includes attacks from internal or external sources for monetary benefits. Extortion through cyber attacks for financial gains by cyber criminals is an example for this category.

Legal
Financial
Operational
Human
Reputation

Risk and Correlating Impact



Risk Assessment



Security & Privacy Approaches* Addressing Concerns

McAfee An Intel Company

Prescriptive Approach

IEC 62351

- Defines explicit security measures for CP-based and serial protocols

NERC/CIP

- Mandatory standards issued by NERC (North-American Electrical Reliability Corporation) to protect critical infrastructures

IEC 61850-90-5

- Addresses security for synchrophasor communication in terms of integrity (based on HMAC) and optional confidentiality (using AES) for key management

Risk-based Approach

ISO/IEC 27001

- Formally specifies a management system that is intended to bring information security under explicit management control.

ISO/IEC 27002

- Provides best practices recommendations on Information security management.

EG2 Report

- Report of the Task Force Smart Grid Expert Group 2 on "Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection".

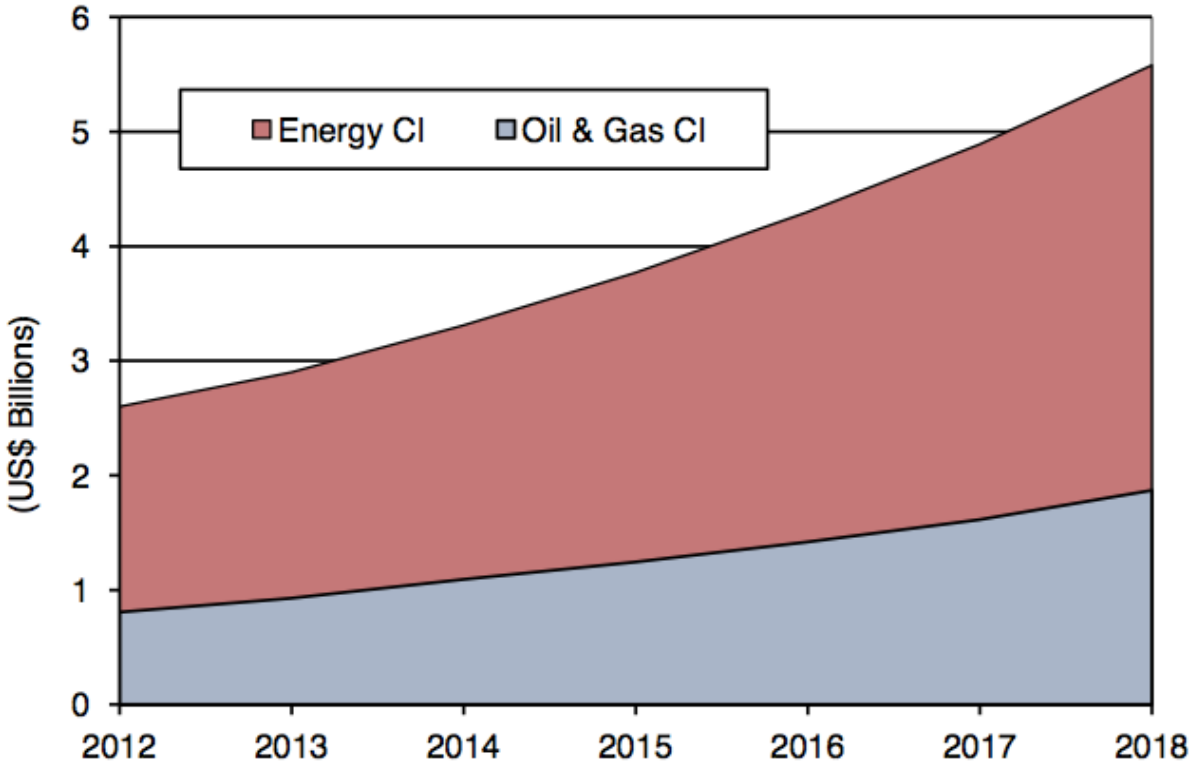
NIST IR-7628

- U.S. non prescriptive recommendations for Smart Grid Cyber Security

* This list is not comprehensive

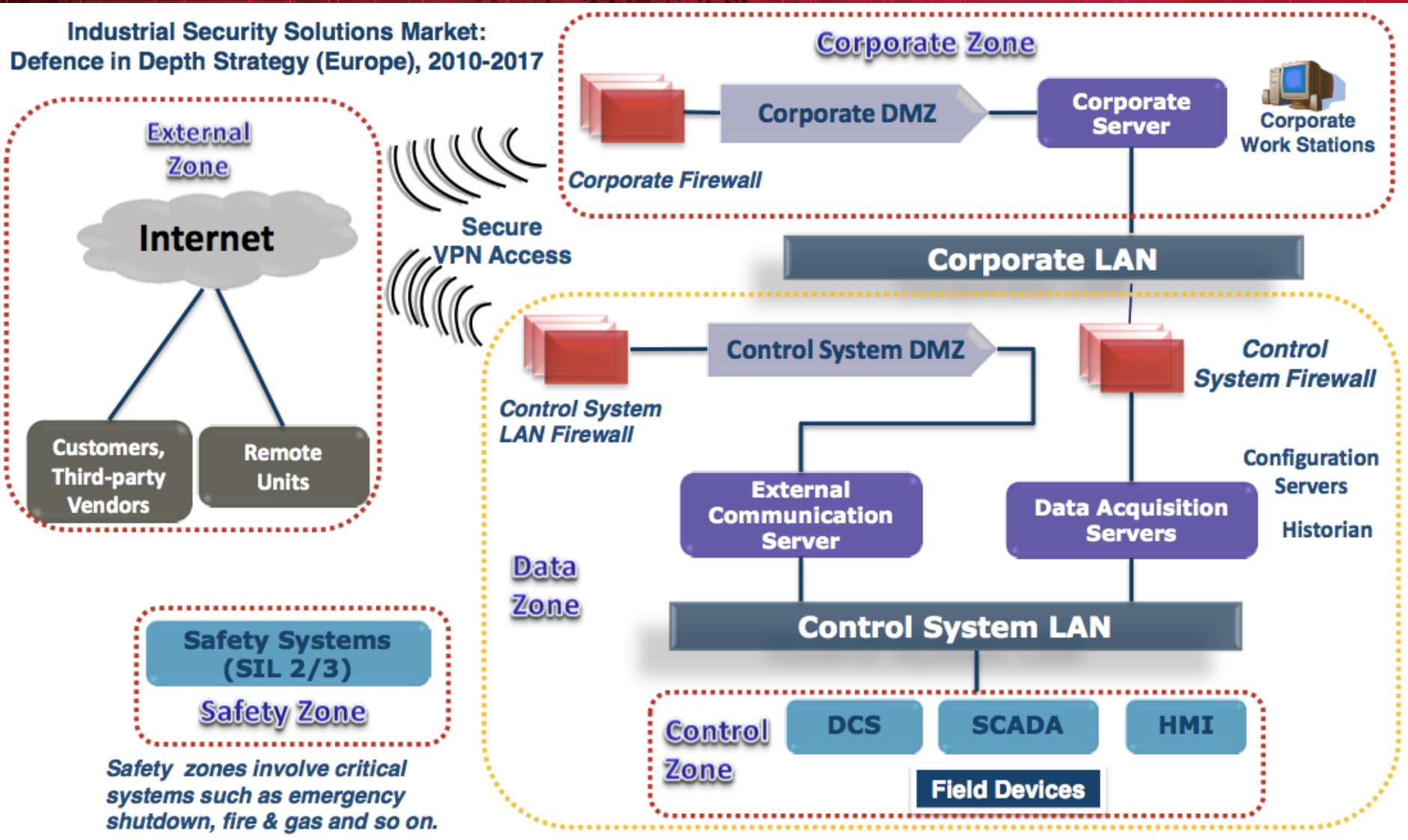
Global Energy Security Spend

Chart 3: Energy versus Oil & Gas CI Security Spending
World Market, Forecast: 2012 to 2018 (Source: ABI Research)



Global Energy Security Spend for 2013 > $2B

Energy IT / OT Security - Defense In Depth



Security Connected
Weaving the pieces together

McAfee
An Intel Company

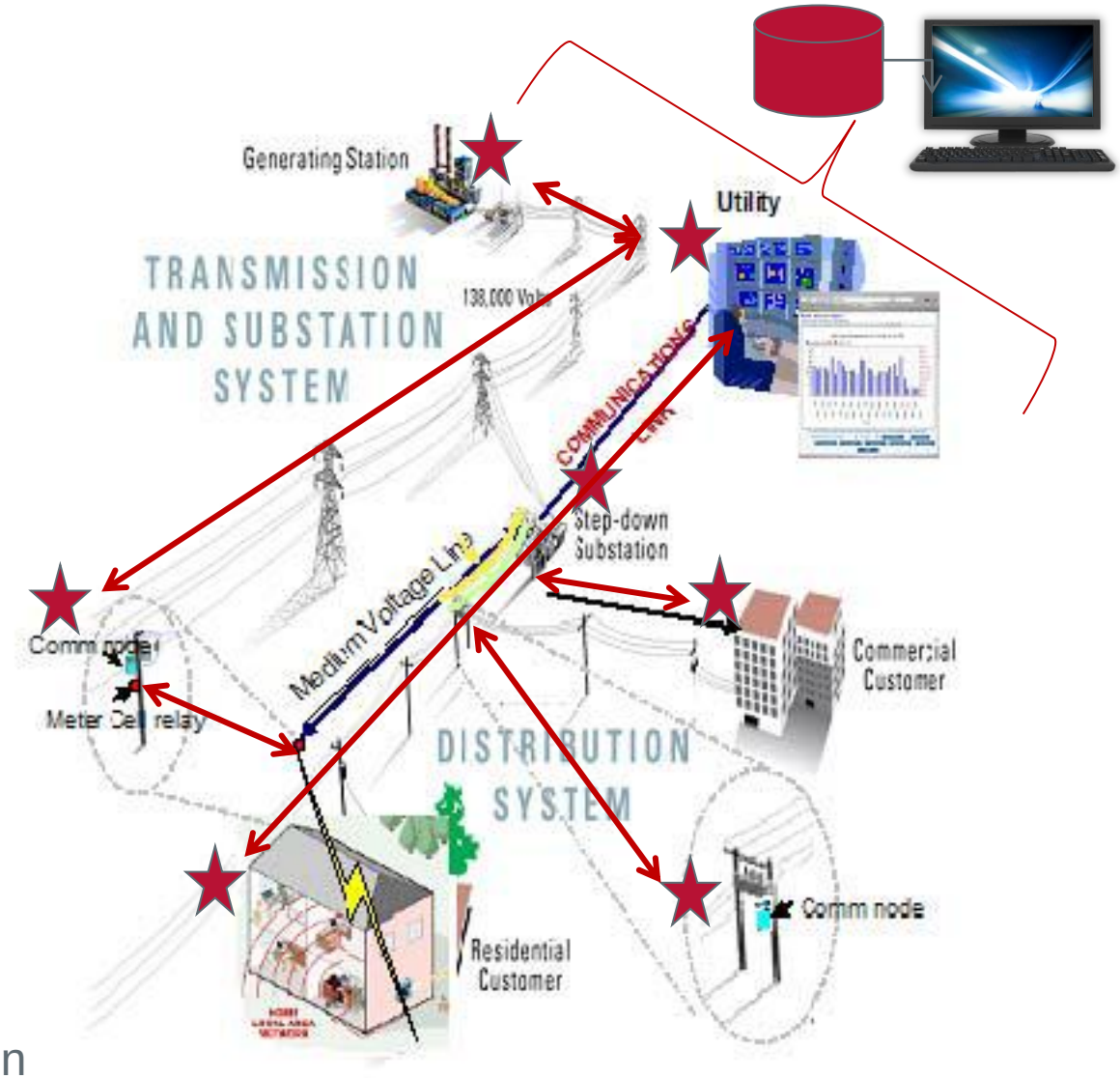
Prime Objectives

- Defense in Depth
- End-to-end real-time situational awareness
- Comprehensive analysis and remediation

Harden servers, gateways and end points and protect their applications

Secure every node connection and data transmission

Correlate all security events for panoramic visualization, rapid analysis, decisive action



Security Connected Platform for Hardening Critical Infrastructure

McAfee An Intel Company

Embedded Security

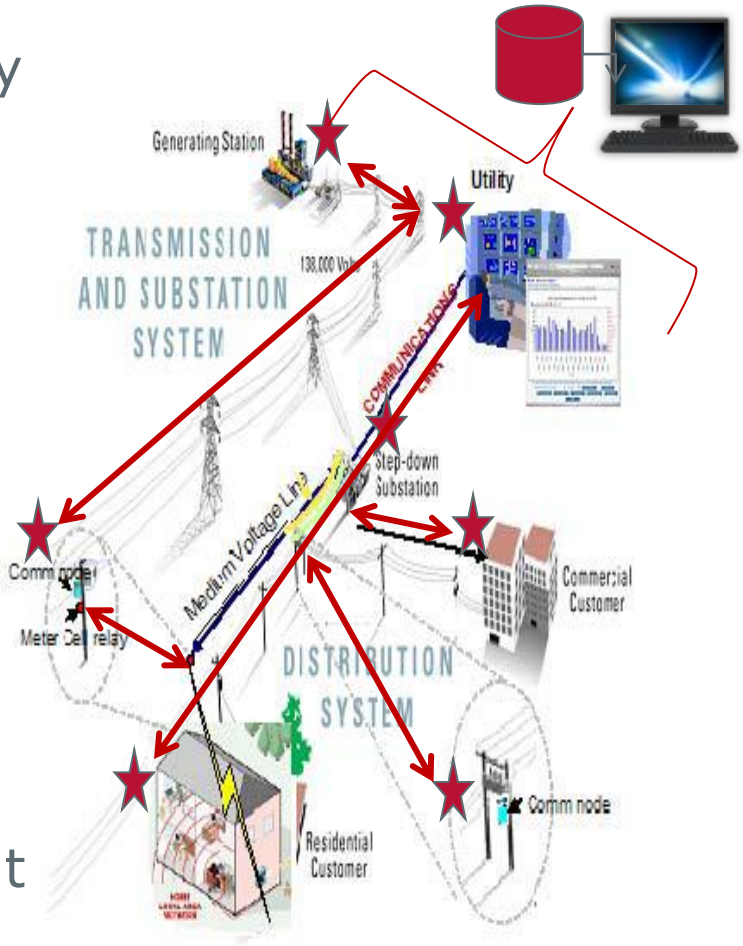
- McAfee Deep Defender, Integrity Control
- Wind River OS/Hypervisor/IDP
- Intel HW-assisted security

Network Security

- McAfee IPS and Firewall
- Stonesoft

Security Monitoring & Management

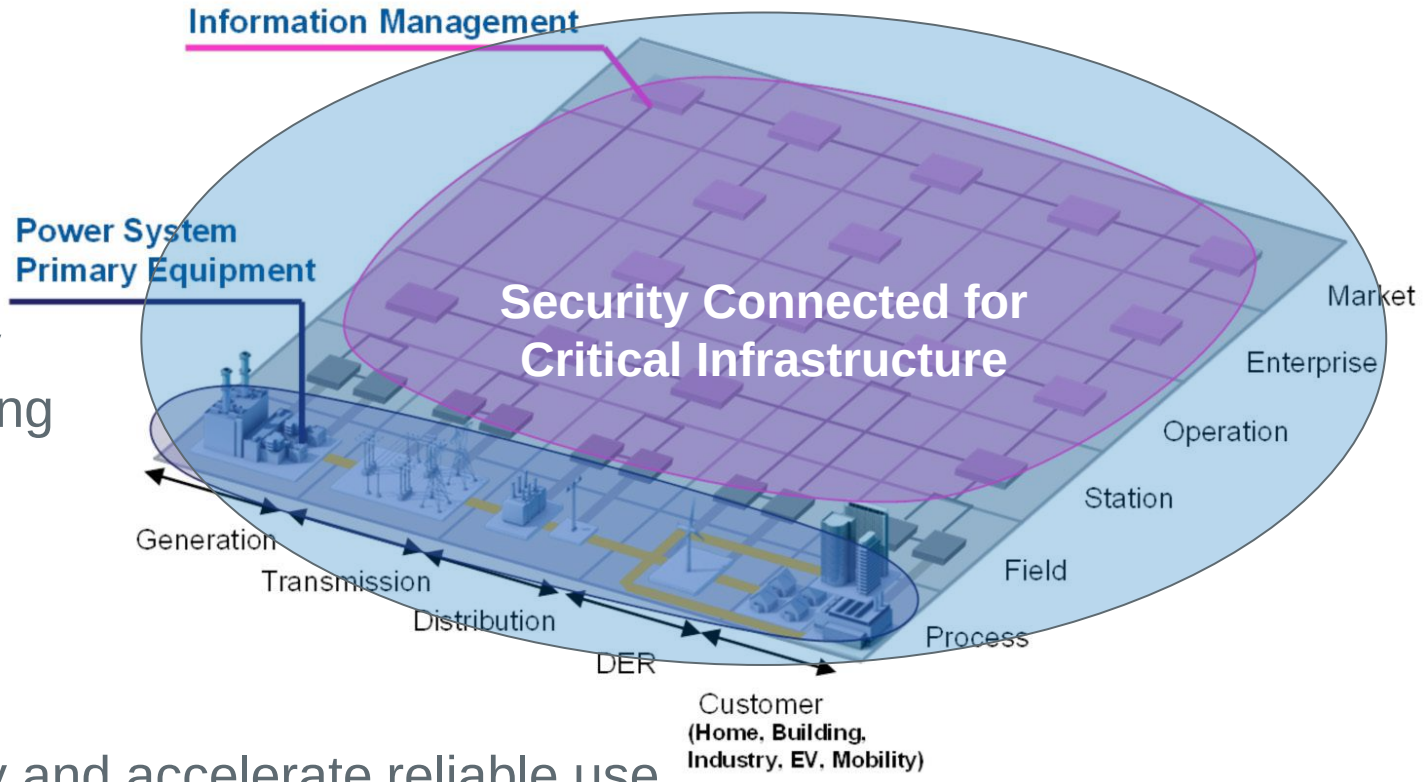
- Enterprise Security Management (ESM/Nitro)
- ePolicy Orchestrator (ePO)



Unique Embedded-to-Enterprise Integrated Security Vision for Critical Infrastructure

McAfee: Achieve end-to-end availability and QoS with confidentiality and integrity reliably enforced

Wind River: Reduce complexity and cost of delivering secure embedded infrastructure and control systems



Intel: Simplify and accelerate reliable use of hardware-based security technologies

Questions? Then it's Panel Time!

Additional Information and Resources

Intel Grid Insights: http://gridinsights.energycentral.com
Twitter: Lorie Wigle -> @lwigle
Raj Samani -> @Raj_Samani

McAfee Security Connected: Twitter #securityconnected
http://www.mcafee.com/us/enterprise/reference-architecture/index.aspx

Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure, by Raj Samani and Eric D. Knapp
(Book available at Amazon.com)