Real-Time Assurance for Critical Infrastructure and ICS

Mark Hall
Cyber Security Executive
mark.hall@raytheon.com
16 October 2012

Raytheon
Customer Success Is Our Mission

Copyright © 2012 Raytheon Company. All rights reserved.
Customer Success Is Our Mission is a registered trademark of Raytheon Company.

Agenda

- The Threat is Real
- CIP Security Challenges
- Approach to a Solution
- Summary & Questions

Probability—Not “if”, but “when” (Open Source Material)

2000: In Queensland, Australia, having been turned down for a job a computer expert took revenge. Using a notebook PC and a radio transmitter, he seized control of a wastewater facility on 46 separate occasions.

~264,000 gallons of sewage spilled

2007: Israeli jets bombed a suspected nuclear-reactor site in northeastern Syria. Syrian air-defense radar failed to detect the warplanes.

Speculation that the Israeli Air Force took advantage of a "kill switch" feature built into chips within the radar systems.

2010: Stuxnet is the first to exploit vulnerabilities, compromise security, and inject code into industrial control systems (ICSs). Reprograms ICSs by modifying code to make them work in a manner the attacker intended, hiding those changes from the operator.

Iran’s Bushehr Nuclear Power Plant

Consequences—Energy System Failures

- **1996:** 7.5 million customers across 11 western states and two Canadian provinces lost power, some for several hours. The estimated economic losses :$2 billion **(lightning)**

- **2000:** 550,000 customers in New Mexico - transmission line failure **(grass fire)**

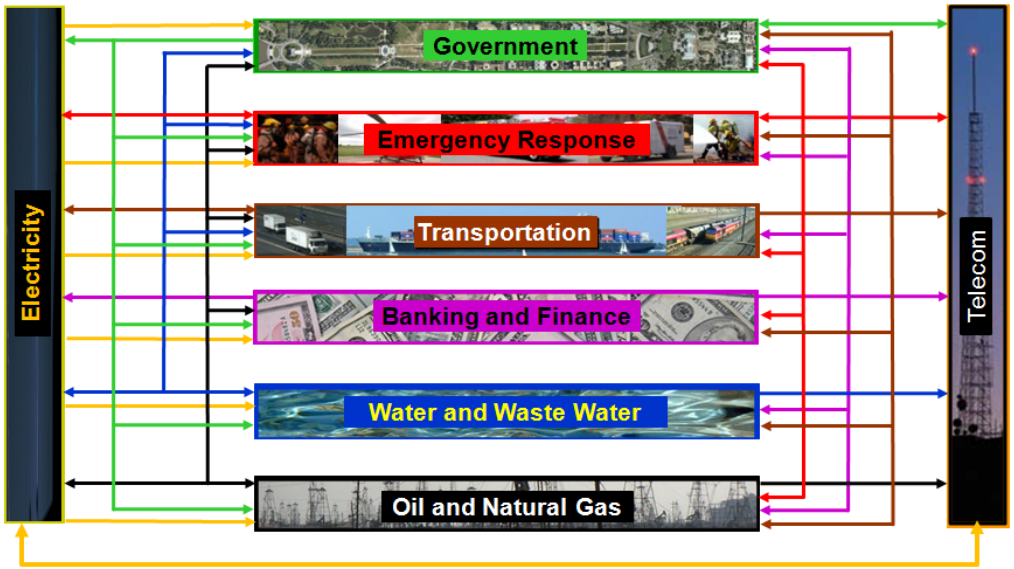
- **2003:** Blackout in New York City and neighboring areas, carried with them incurred costs of up to $10 billion **(SCADA failure)**

- **2005:** All of southern and central Iraq, parts of Baghdad, all of Basra and the only port Umm Qasr for 7+ hours by a cascading effecting multiple power plants. **(sabotage)**

- **2012:** Largest electrical blackout in history, ~2000 miles, 670 million people, 2+ days. **(SCADA failure??)**

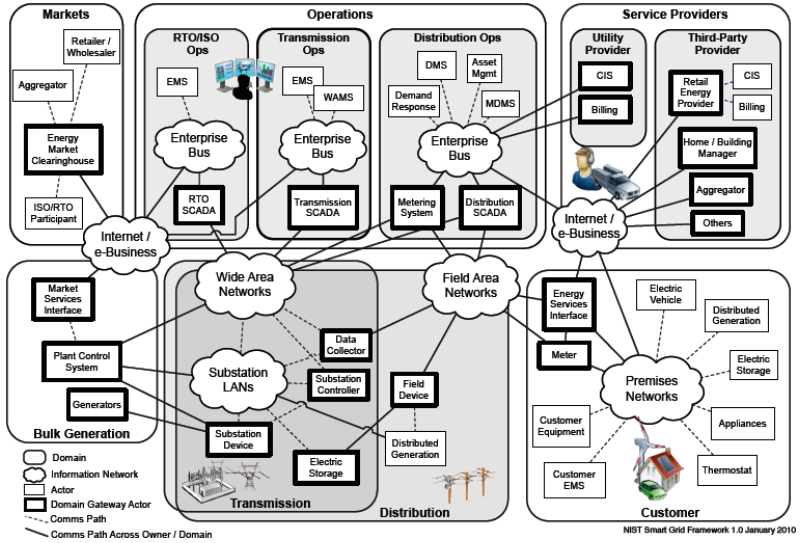
Images courtesy of NY Times

More Efficient or More Vulnerable?



Critical Infrastructure Interdependency

Smart Grid Reference Architectures



Source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, January 2010

Hacking—It's No Longer a Game

1980-2000

- ***Demographics***
  - Highly educated
  - College-aged men
  - Independent
- ***Motivation***
  - Glory (bragging rights)

2000-2012

- ***Demographics***
  - Highly educated
  - Mature adults
  - Sponsored by nation-states or religious groups
- ***Motivation***
  - Resale of information
  - Espionage
  - Terror

Perpetrator Goals

Deny
- Incapacitation
- Deliberate Exposure
- Scavenging

Deceive
- Spoof
- Malicious Logic

Disrupt
- Natural disaster
- Corruption
- Obstruction

Damage
- Misappropriation
- Theft
- Misuse

Destroy
- Physical destruction
- Cause harm

Threat Analysis

	Physical Effect	Cyber Effect
Physical Attack	Explosives Natural Disaster	Process Disruption
Cyber Attack	Stuxnet	Denial of Service

Deny

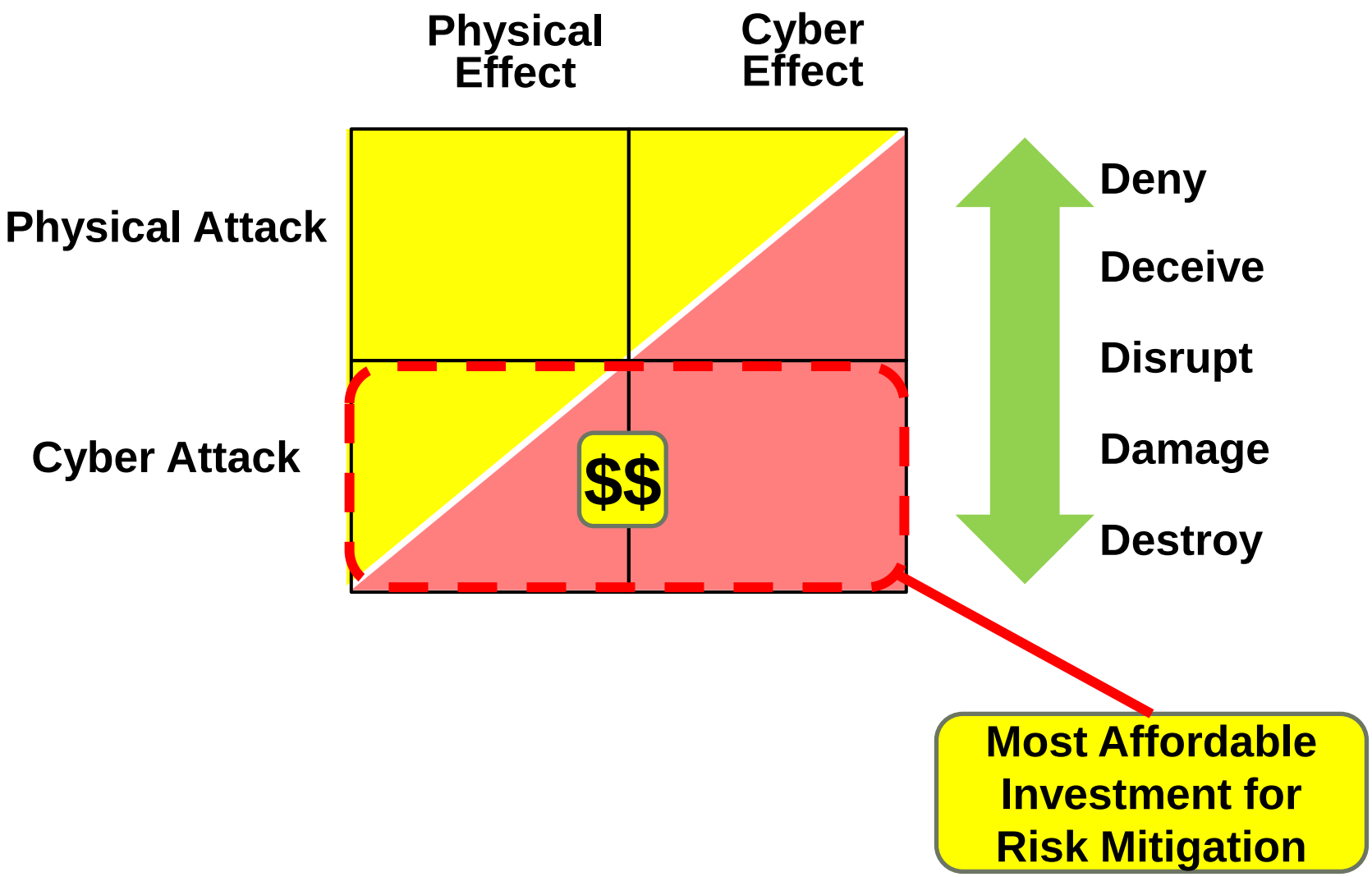
Deceive

Disrupt

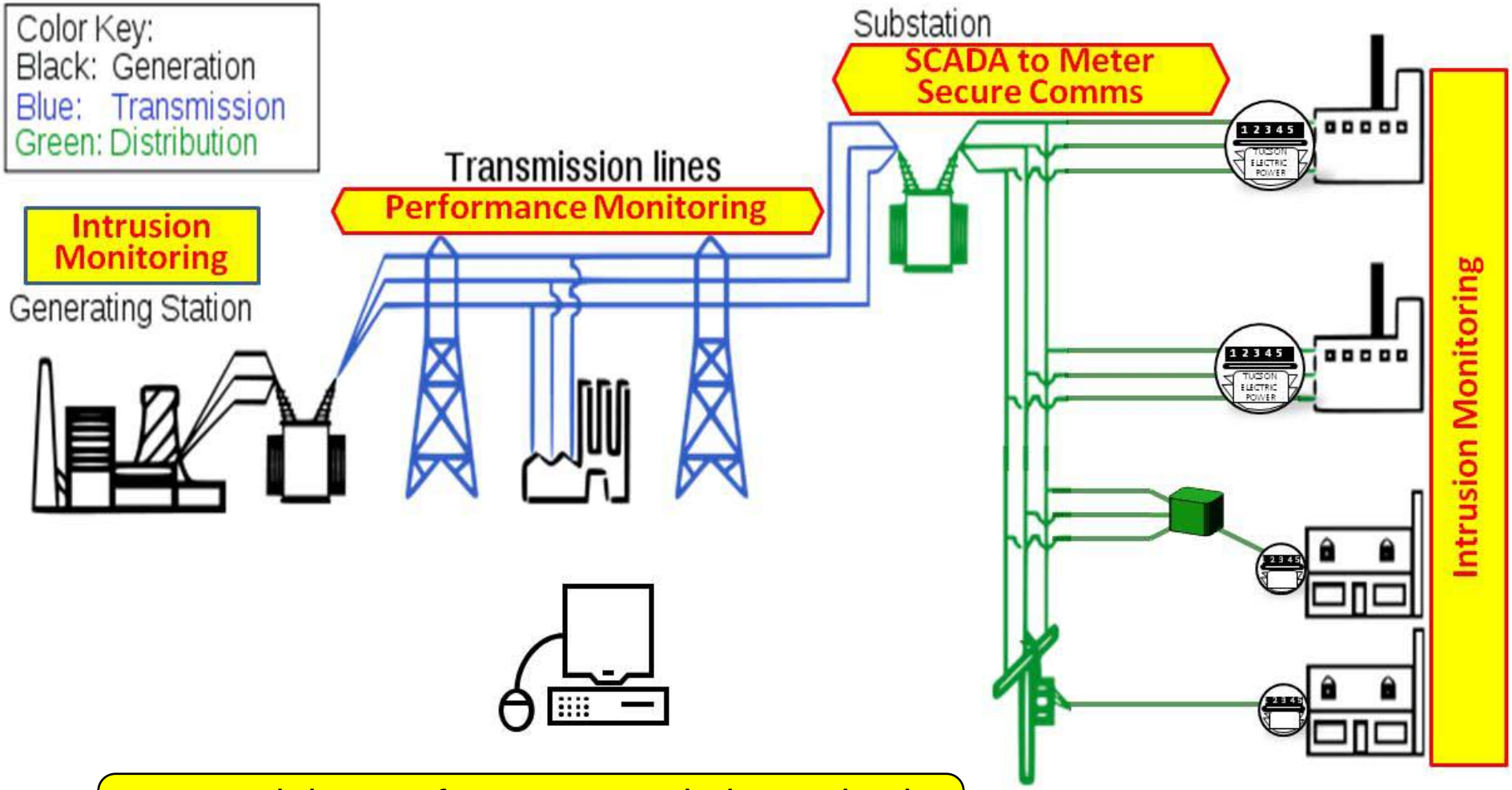
Damage

Destroy

Threat Analysis



Cyber Security Technology Gaps



Real-time performance needed to maintain competitive edge and profitability

Critical Infrastructure Security Challenges

- Communications and network threats (Cryptoography, Man in the Middle, Spoofing)
- Configuration and logic
  - Access Control
  - Key Management
  - Data Loss/Information Disclosure
  - Privilege Escalation
- Back Doors, Trojans, Virus, Worms & Easter Eggs
- Denial of service
  - Buffer overflows
  - Format string attacks
- Attacks on field devices
  - Data integrity
  - No data encryption
- Physical security

Parallels across DHS—Commercial—DoD Spectrums

Increased reliance on automation & technology creates cost saving opportunities, but also results in risks

Countermeasures for Security Challenges

- Control ***access*** to resources and services
  - Access control (e.g. firewalls, proxy servers, secure comms)
  - Data diodes and intrusion detection capabilities
  - Trusted “multi-level” solutions

- Monitor ***transfer*** of data across networks
  - Allow only trusted transfers for critical components
  - Audit and logging of traffic facilitates troubleshooting, performance tuning, and forensic analysis
  - Trusted “multi-level” solutions

- Approve relevant security ***policies*** for ICS & SCADA networks
  - Relevancy for current and anticipated future threat environment
  - Tailored to CIP protocols and functionality
  - Required level of security vice prudent level of security
  - Policies based on authorized uses of network data

ASTEE : A Trusted Multi-Level Cross Domain Solution

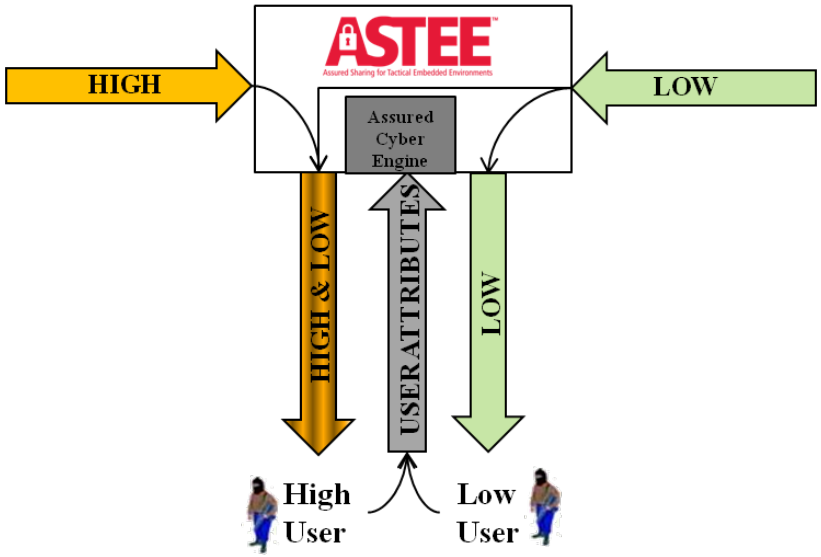
Raytheon

Capabilities

- Low cost, small form factor information assurance appliance—software & COTS hardware—leverages DoD technology
- Certifiable attribute-based access control (allows only authenticated **AND** authorized users)
- Secure real-time data transfer between stations
- Tailorable security policies for changing operational requirements
- Scalable for all levels of service (e.g. generating stations, substations, primary & secondary customers)

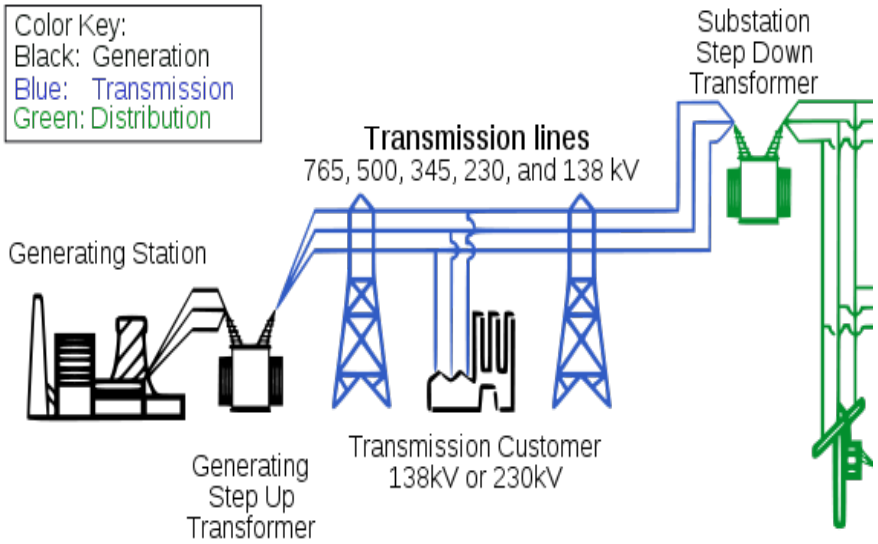
Operational Benefits

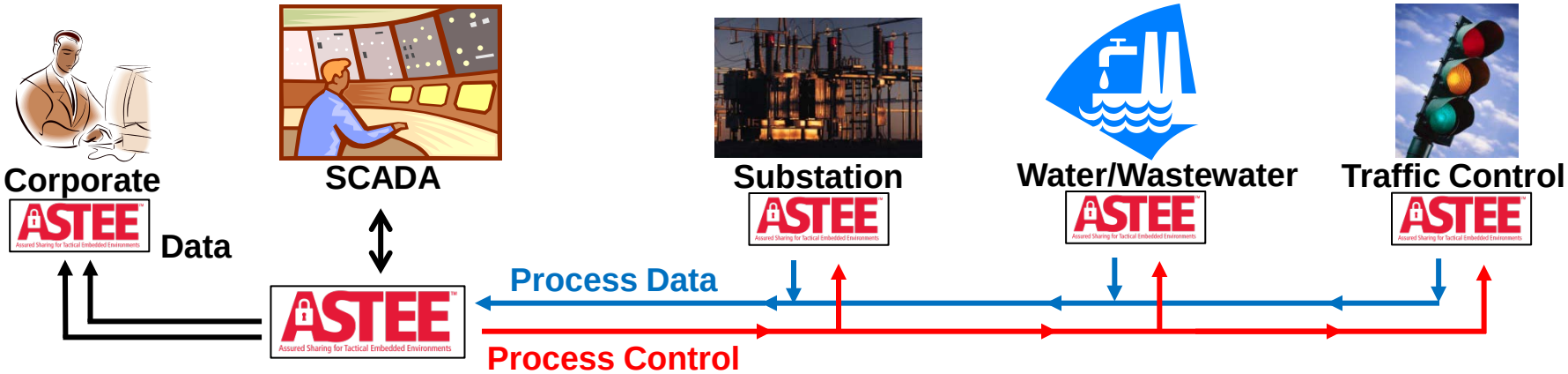
- Enhanced operational effectiveness and efficiency (e.g. lower cost per kwh)
- Streamlined certification & accreditation to meet emerging policy mandates



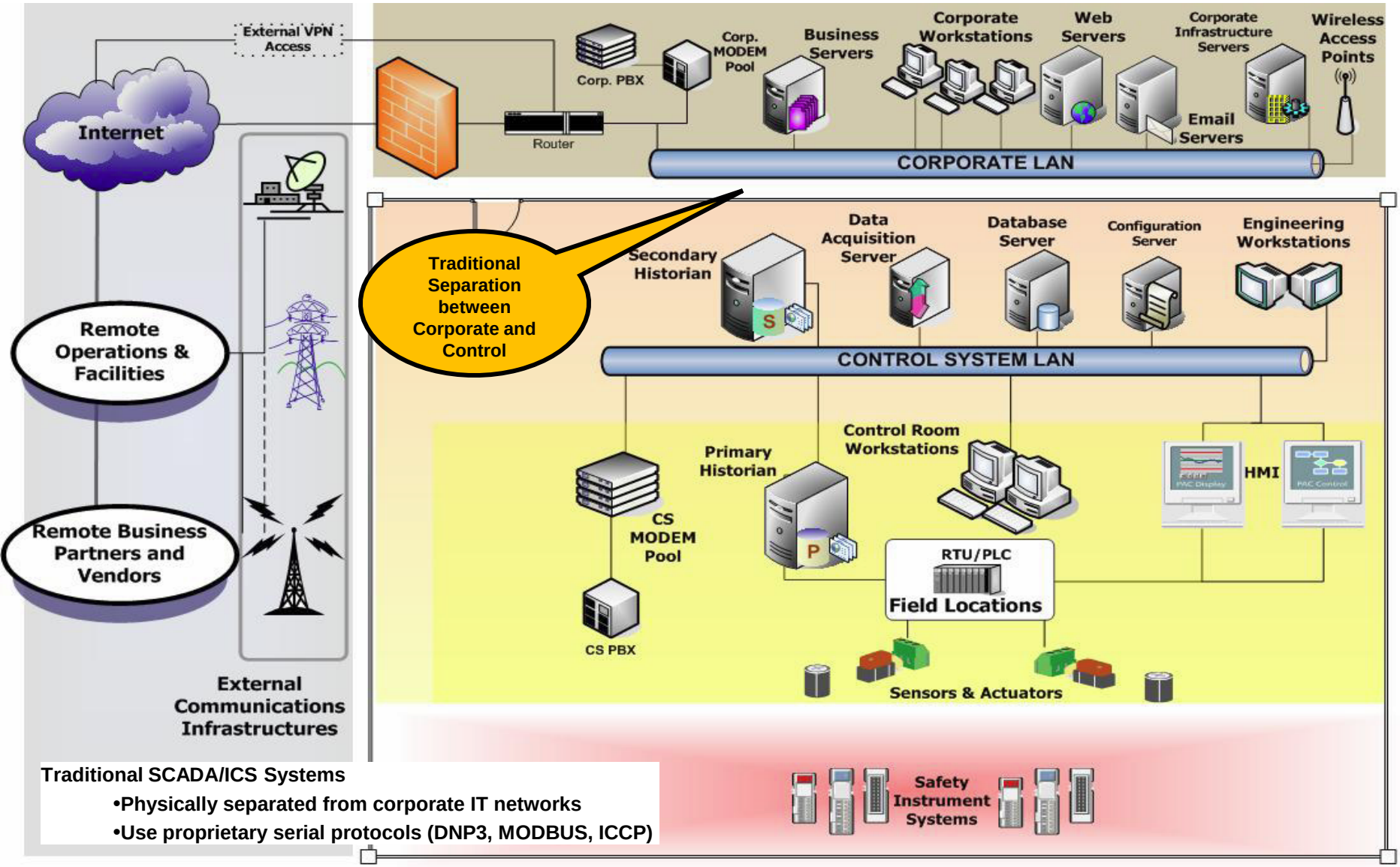
ASTEE: Notional Application to CIP

- Interfaces with common protocols (e.g. UDP, TCP)
- Supports mixed SCADA / PLC / DCS architectures
- Controls both access and transfer
- Full two-way capability for less cost than one-way data diodes





Notional Isolated Control Network

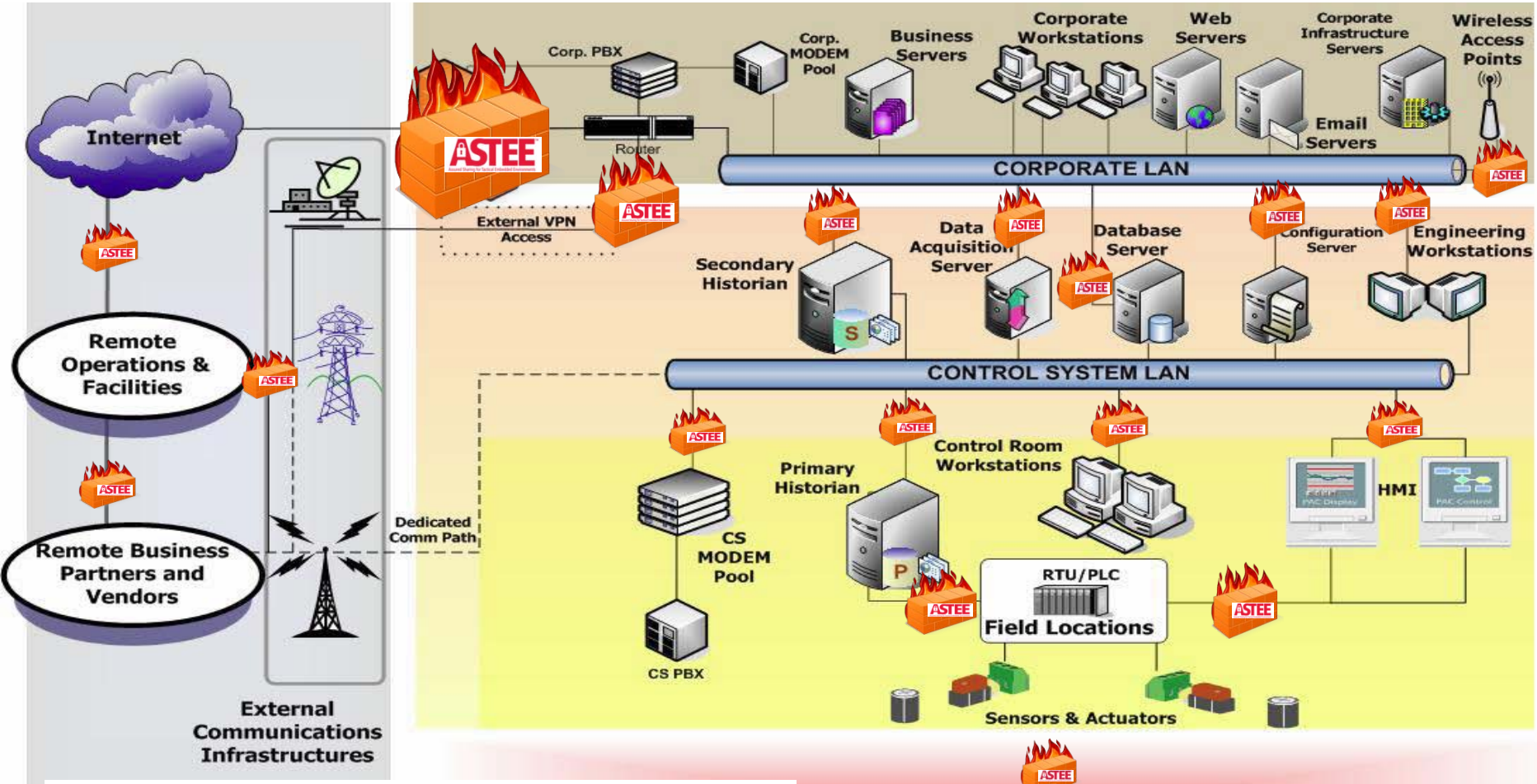


Traditional SCADA/ICS Systems

- **Physically separated from corporate IT networks**
- **Use proprietary serial protocols (DNP3, MODBUS, ICCP)**

Graphic courtesy of DHS *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies October 2009*

Notional SCADA/ICS "Defense in Depth"



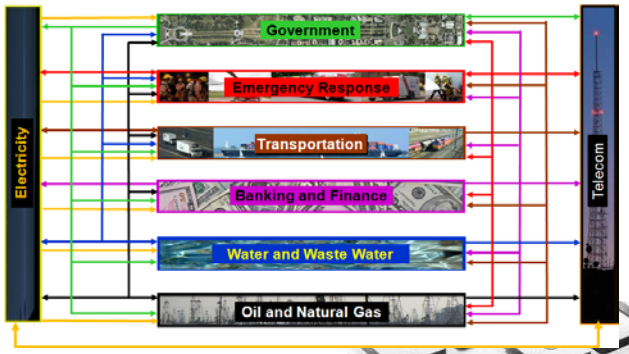
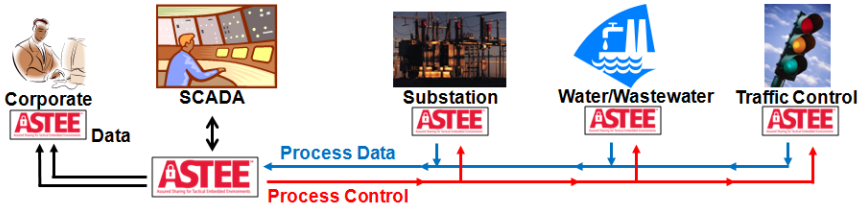
Today's SCADA/ICS Systems

- **Connected to corporate IT networks—exposed to Internet risks**
- **Proprietary protocols modified for TCP/IP or use gateways**
- **Control software reliance on COTS for cost savings**

Graphic courtesy of DHS *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies October 2009*

Summary

- Interconnection of critical infrastructure creates both efficiencies and vulnerabilities



- Threats are real and are maturing daily
- Cyber security is most affordable investment opportunity
- Resiliency is key to managing vulnerabilities
- Novel approaches like multi-level cross domain solutions can affordably manage risk