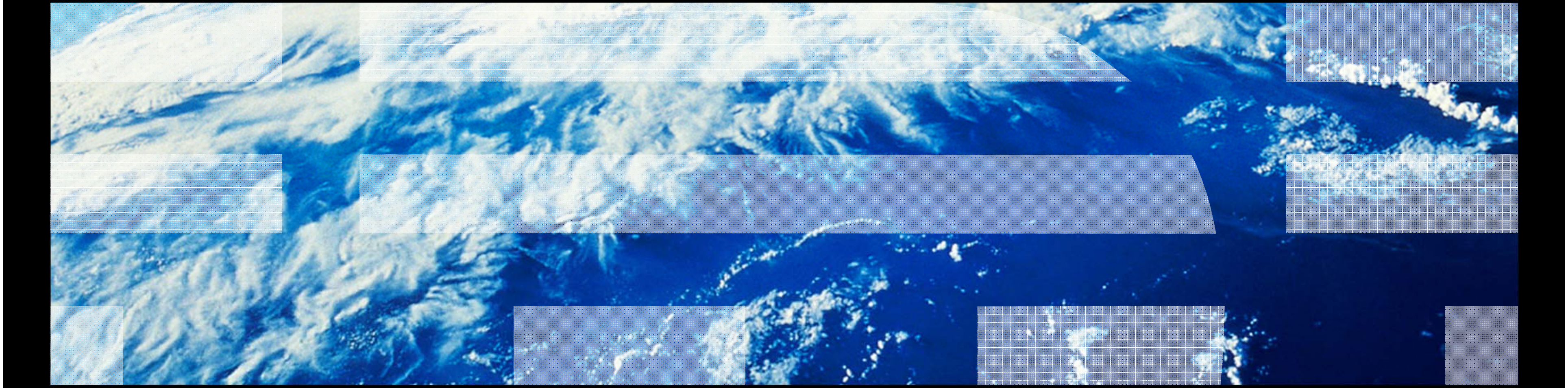
AERTC

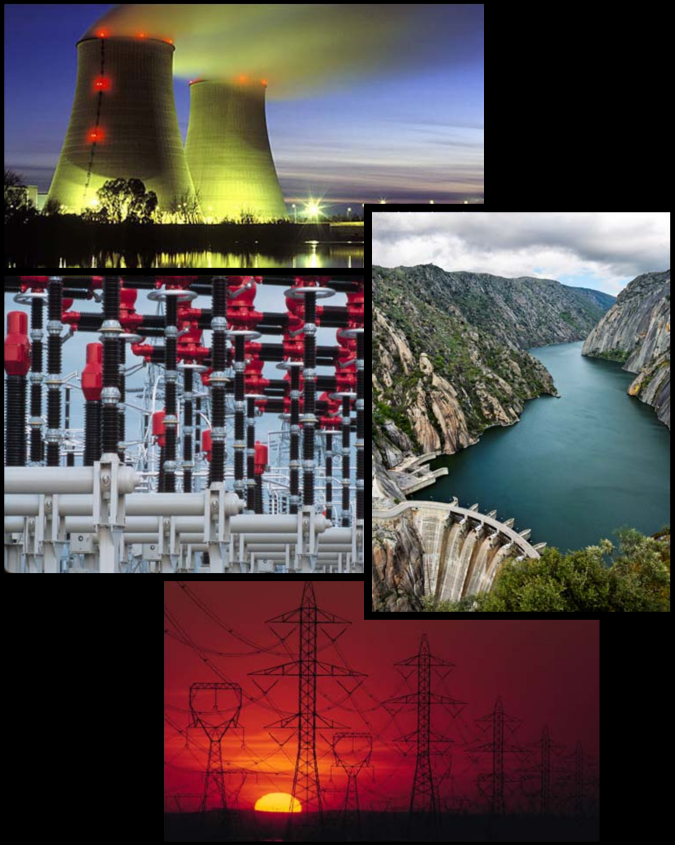
November 8, 2010

Smart Grid Security Update



Potential Impact of a Breach to Power Control Systems Could Be Severe

- Serious disruption to national critical infrastructure
- Loss of system availability
- Process interruption
- Equipment damage
- Asset mis-configuration
- Loss of data and confidentiality
- Personal injury
- Penalties resulting from regulatory violations
- Loss of customer and public trust



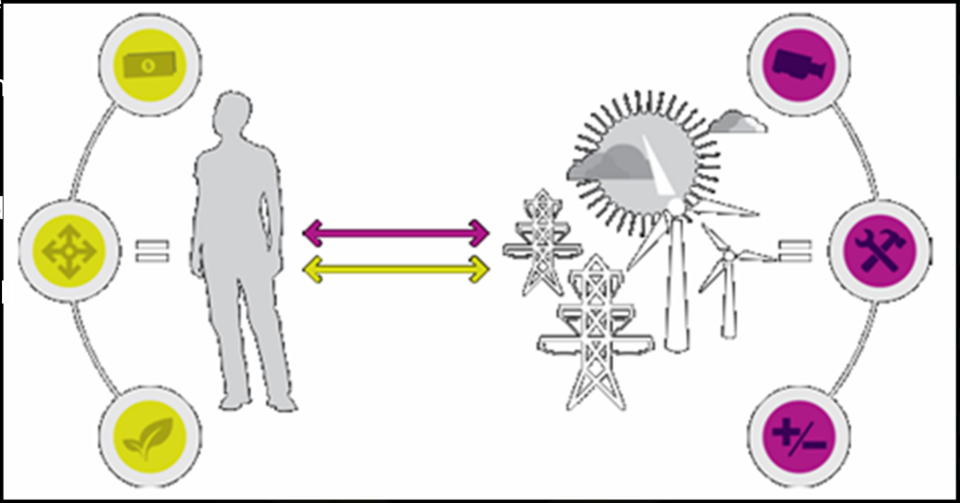
Why do we need a smarter infrastructure?

Consumers

- Take advantage of variable pricing
- Decrease carbon emission choosing clean electricity sources.
- Want more information and control
- Generate electricity and sel it back to the grid
- Want to be involved in the change

Utilities

- Automatically monitor the health of the grid
- Need to reduce the cost to serve
- Must adapt to the changing technology
- Must deliver to the customers expectations
- Desire to capitalise on new information sources
- React to changing demands
- Achieve operational transformation



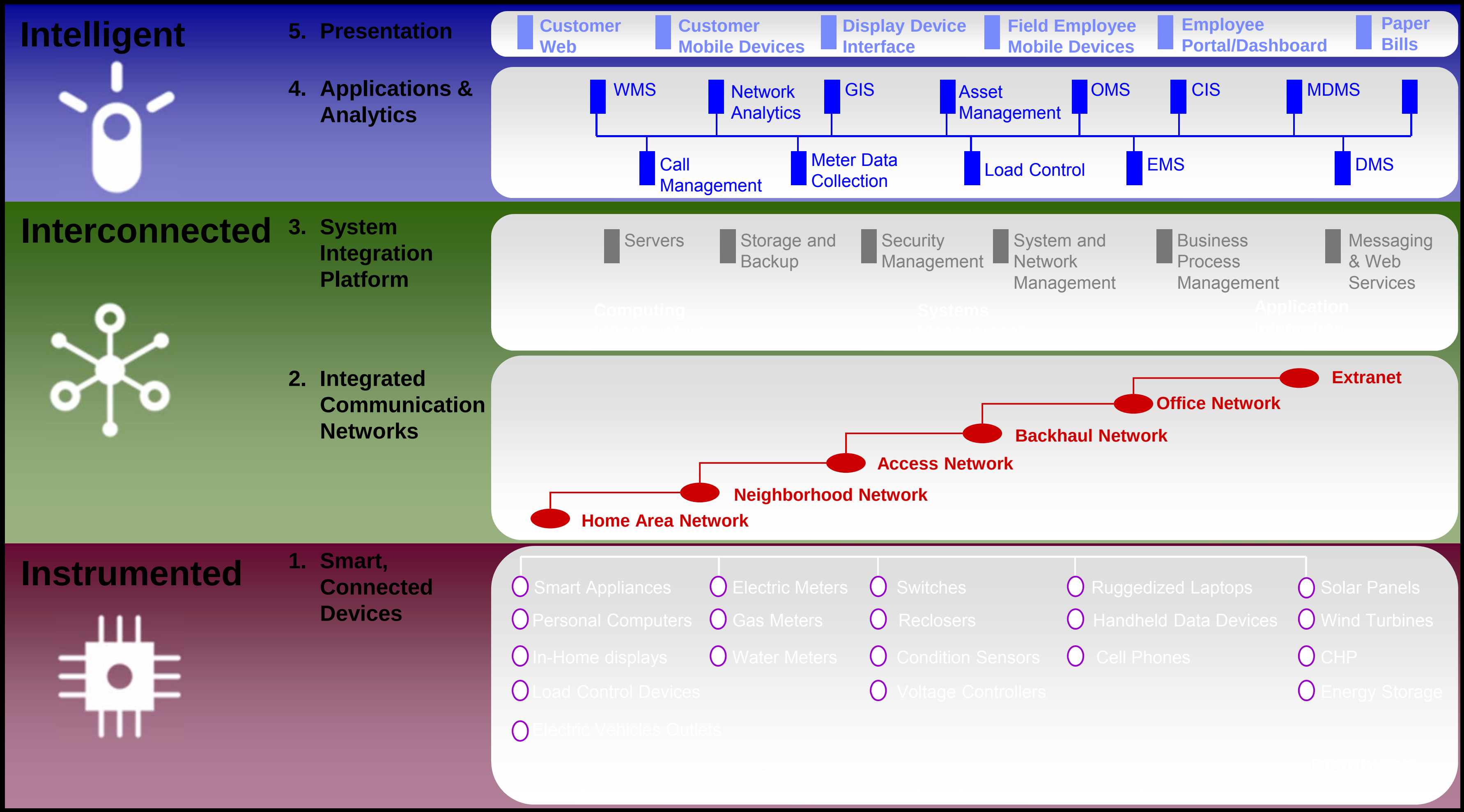
IBM Global Business Services
IBM Institute for Business Value
Plugging in the consumer
Innovating utility business models for the future
Energy and Utilities

Participatory Network

A wide variety of grid and network technology evolve to enable shared responsibility, and consumers’ strong interest in specific goals creates new markets (virtual and physical) and new product demands, which balances benefits more equally between the consumers and utilities

IBM

What is involved in a smarter energy infrastructure?



Intelligent

5. Presentation

Customer Web | Customer Mobile Devices | Display Device Interface | Field Employee Mobile Devices | Employee Portal/Dashboard | Paper Bills

4. Applications & Analytics

WMS | Network Analytics | GIS | Asset Management | OMS | CIS | MDMS

Call Management | Meter Data Collection | Load Control | EMS | DMS

Interconnected

3. System Integration Platform

Servers | Storage and Backup | Security Management | System and Network Management | Business Process Management | Messaging & Web Services

Computing Infrastructure | Systems Management | Application Integration

2. Integrated Communication Networks

Extranet

Office Network

Backhaul Network

Access Network

Neighborhood Network

Home Area Network

Instrumented

1. Smart, Connected Devices

○ Smart Appliances
○ Personal Computers
○ In-Home displays
○ Load Control Devices
○ Electric Vehicles Outlets

○ Electric Meters
○ Gas Meters
○ Water Meters

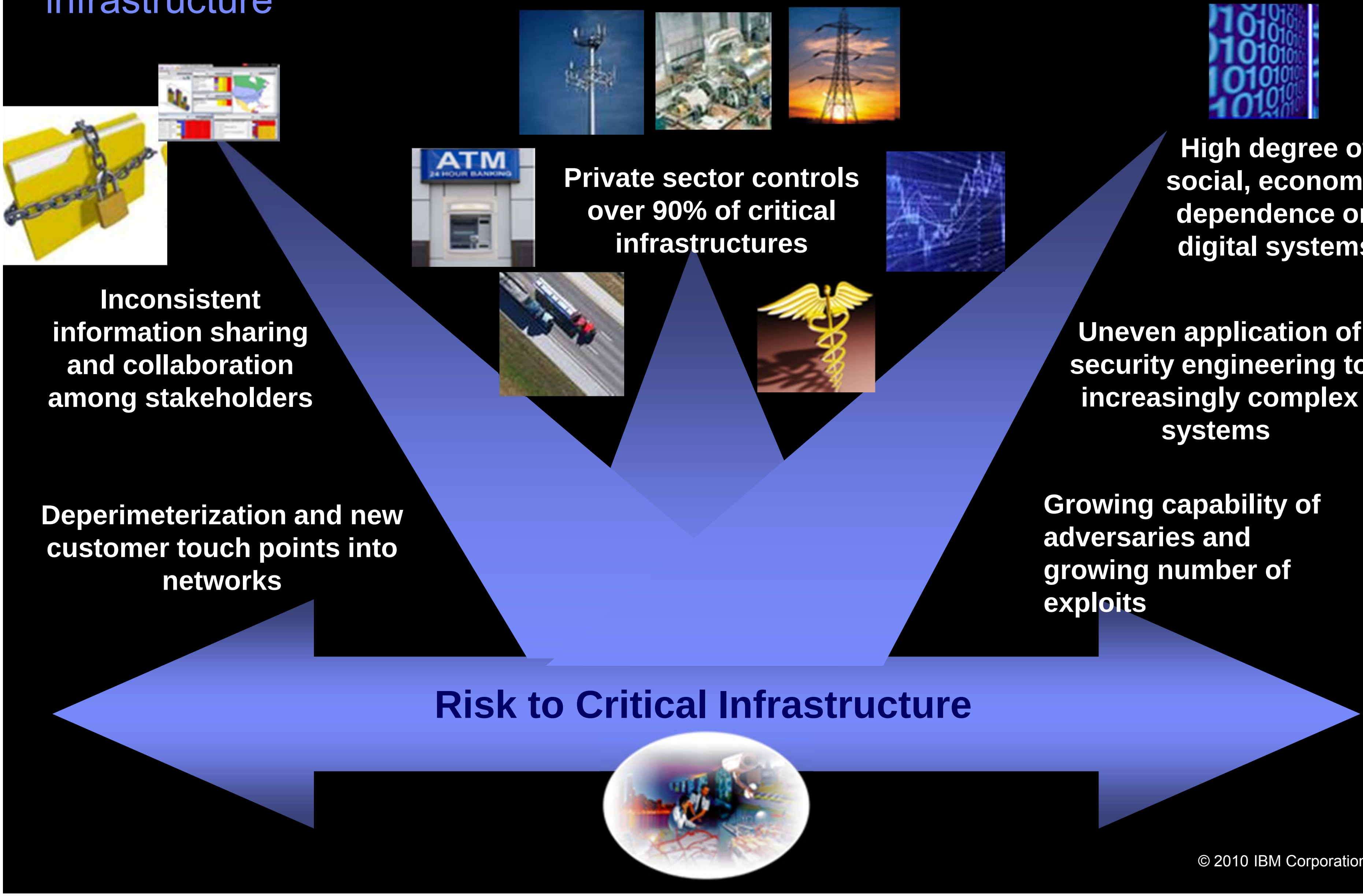
○ Switches
○ Reclosers
○ Condition Sensors
○ Voltage Controllers

○ Ruggedized Laptops
○ Handheld Data Devices
○ Cell Phones

○ Solar Panels
○ Wind Turbines
○ CHP
○ Energy Storage

In-home | Smart | Substation | Mobile | Distributed

Many factors shape the degree and nature of the risk to our cyber infrastructure



Inconsistent information sharing and collaboration among stakeholders

Deperimeterization and new customer touch points into networks

Private sector controls over 90% of critical infrastructures

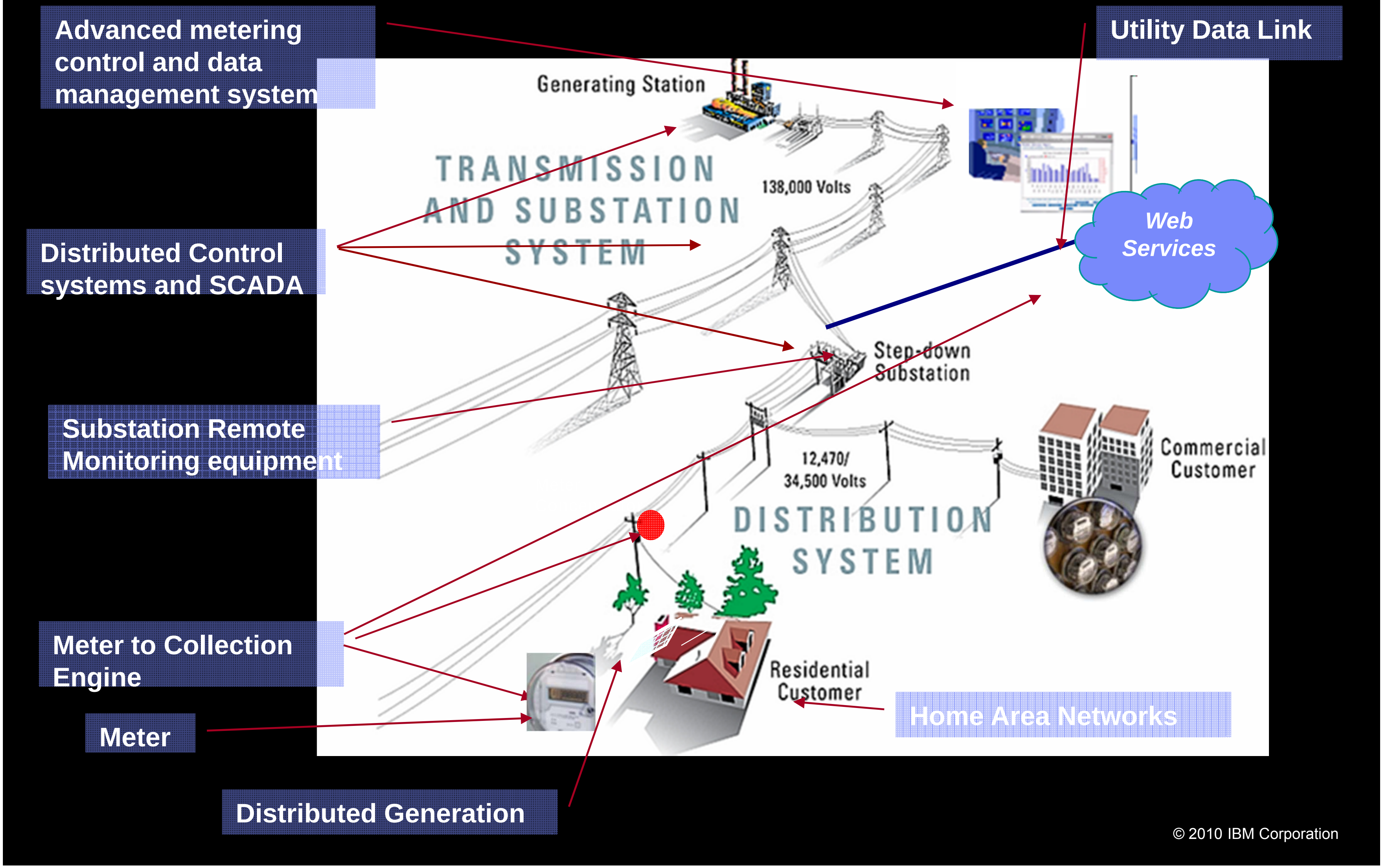
High degree of social, economic dependence on digital systems

Uneven application of security engineering to increasingly complex systems

Growing capability of adversaries and growing number of exploits

Risk to Critical Infrastructure

A Smart Grid needs security management across the supply chain



Advanced metering control and data management system

Utility Data Link

Distributed Control systems and SCADA

Substation Remote Monitoring equipment

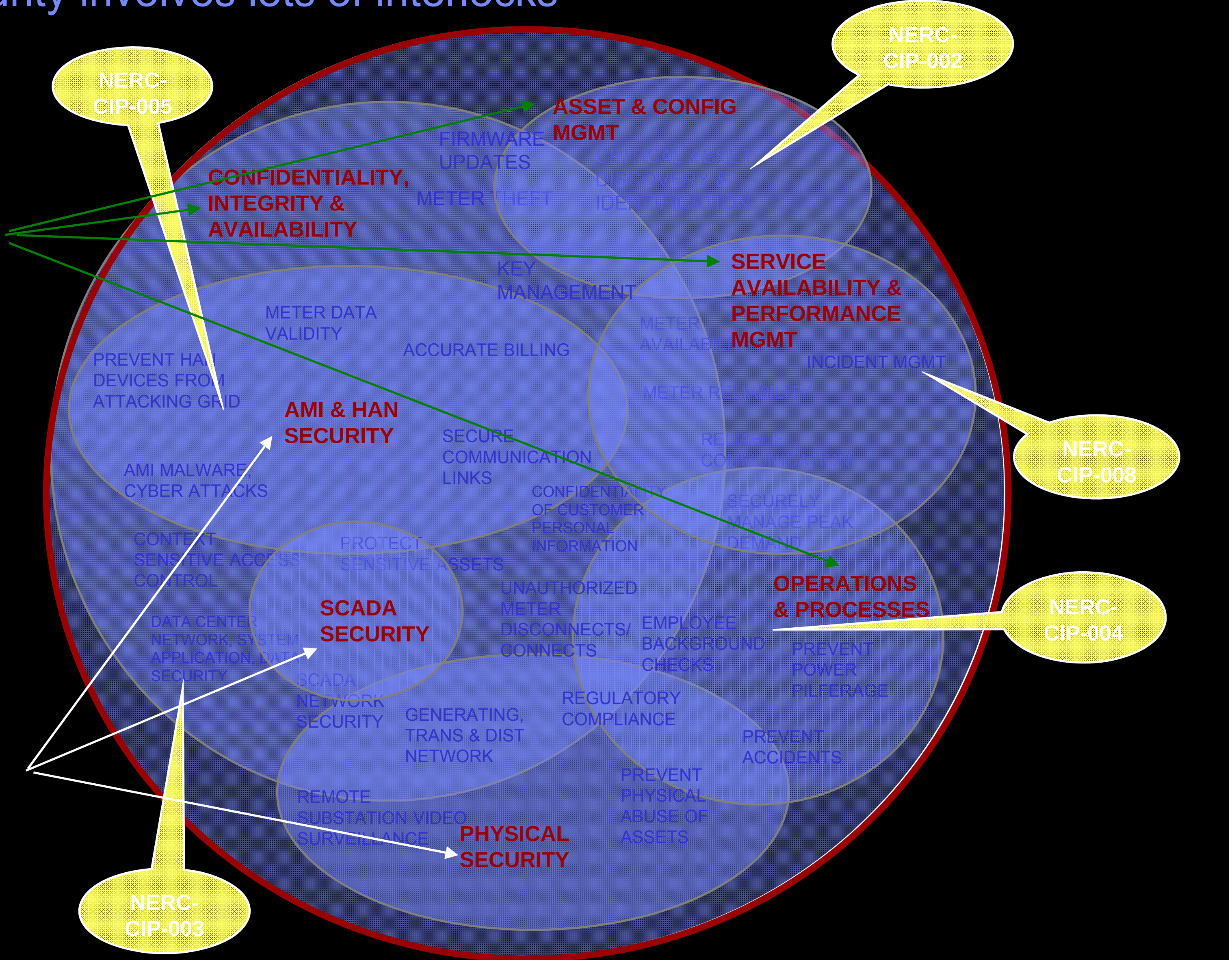
Meter to Collection Engine

Meter

Home Area Networks

Distributed Generation

End to End Security involves lots of interlocks*

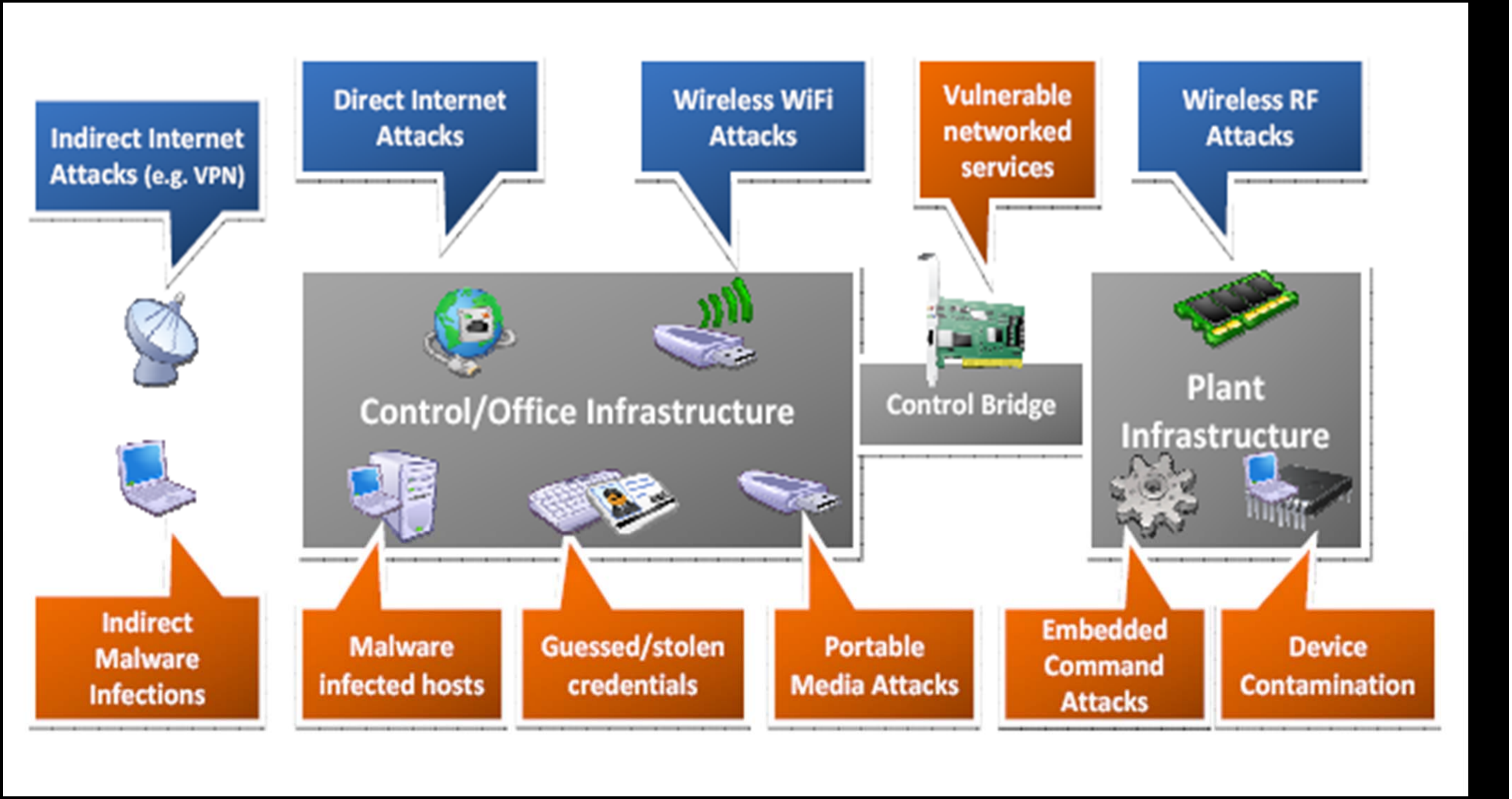

NERC-CIP-005
NERC-CIP-002
NERC-CIP-008
NERC-CIP-004
NERC-CIP-003
ASSET & CONFIG MGMT
FIRMWARE UPDATES
CRITICAL ASSET DISCOVERY & IDENTIFICATION
METER THEFT
CONFIDENTIALITY, INTEGRITY & AVAILABILITY
KEY MANAGEMENT
SERVICE AVAILABILITY & PERFORMANCE MGMT
METER AVAILABILITY
INCIDENT MGMT
METER RELIABILITY
RELIABLE COMMUNICATION
METER DATA VALIDITY
ACCURATE BILLING
PREVENT HAN DEVICES FROM ATTACKING GRID
AMI & HAN SECURITY
SECURE COMMUNICATION LINKS
AMI MALWARE, CYBER ATTACKS
CONFIDENTIALITY OF CUSTOMER PERSONAL INFORMATION
SECURELY MANAGE PEAK DEMAND
CONTEXT SENSITIVE ACCESS CONTROL
PROTECT SENSITIVE ASSETS
OPERATIONS & PROCESSES
SCADA SECURITY
UNAUTHORIZED METER DISCONNECTS/ CONNECTS
EMPLOYEE BACKGROUND CHECKS
DATA CENTER NETWORK, SYSTEM, APPLICATION, DATA SECURITY
PREVENT POWER PILFERAGE
SCADA NETWORK SECURITY
GENERATING, TRANS & DIST NETWORK
REGULATORY COMPLIANCE
PREVENT ACCIDENTS
PREVENT PHYSICAL ABUSE OF ASSETS
REMOTE SUBSTATION VIDEO SURVEILLANCE
PHYSICAL SECURITY

* Not all intersections and NERC-CIP directives shown

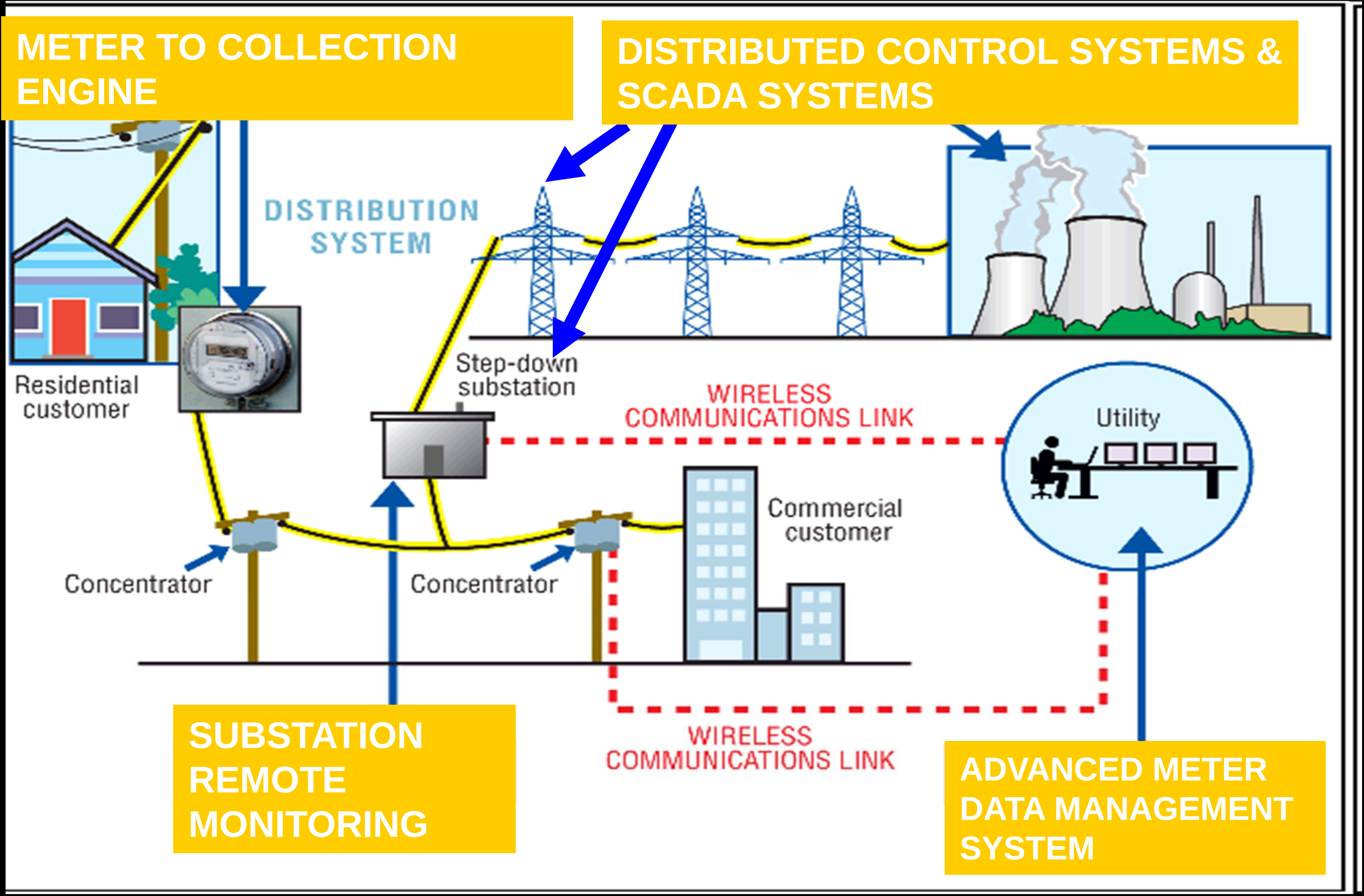
Smart Grid Threats- Some examples

Threat Category	Mitigation Strategy	Possible Remediation
Unauthorized or accidental disclosure of information	Encryption, access control, security policy enforcement	Trust domain-based secure messaging
Unauthorized or accidental modification of information	Authentication, tamper detection, security policy enforcement	Software-based attestation
Unauthorized or accidental destruction of information	Access control, authentication, security policy enforcement	Trust domain-based secure messaging
Non-Delivery or Miss-Delivery	High availability & resiliency, authentication, security policy enforcement	Resilient multi-path overlay routing
Denial or degradation of service	High availability & resiliency	Resilient multi-path overlay routing

Many Attack Vectors Exist Across Complex Utility Infrastructure Environments



Smart Grid security solution points



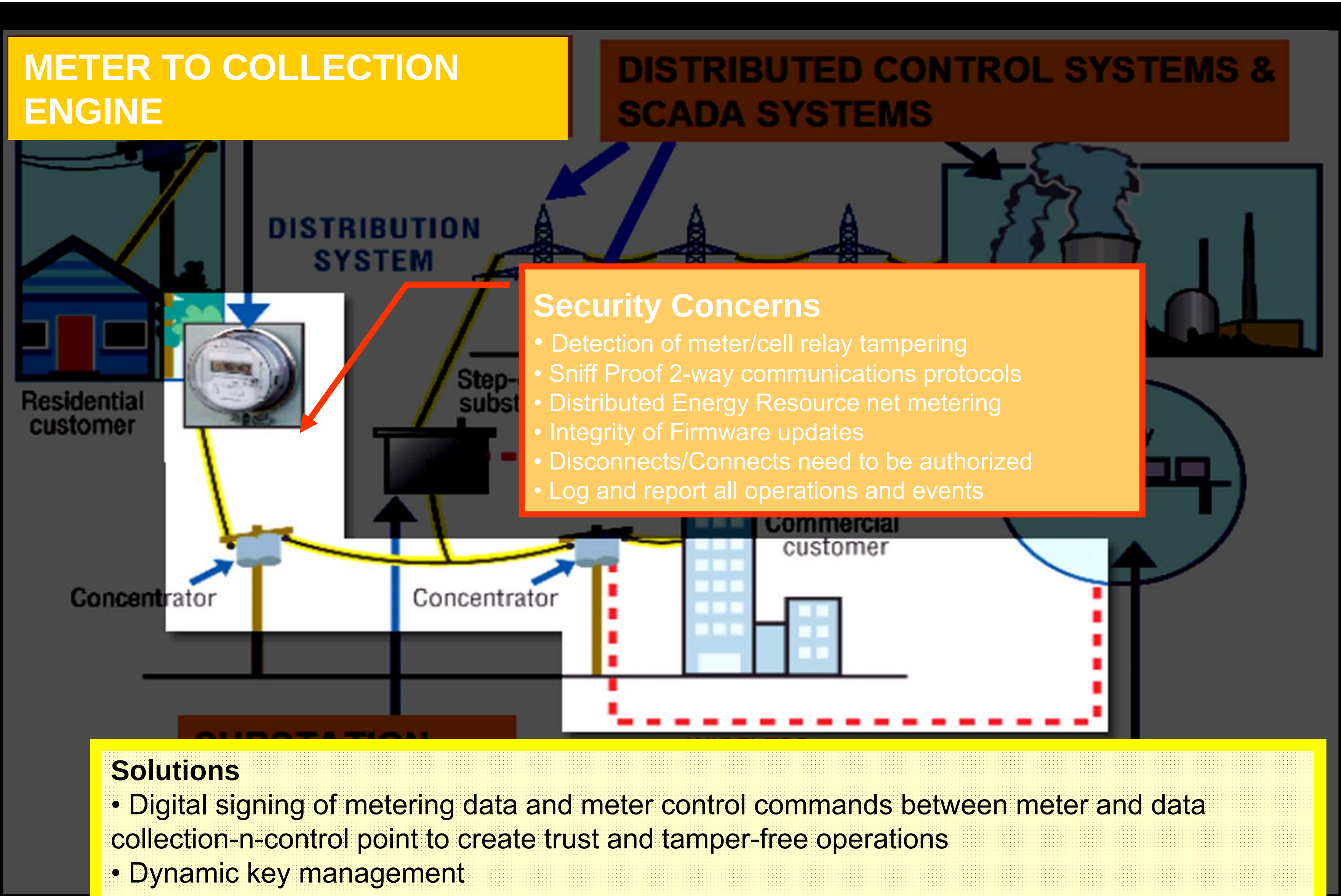
METER TO COLLECTION ENGINE

DISTRIBUTED CONTROL SYSTEMS & SCADA SYSTEMS

SUBSTATION REMOTE MONITORING

ADVANCED METER DATA MANAGEMENT SYSTEM

METER TO COLLECTION ENGINE

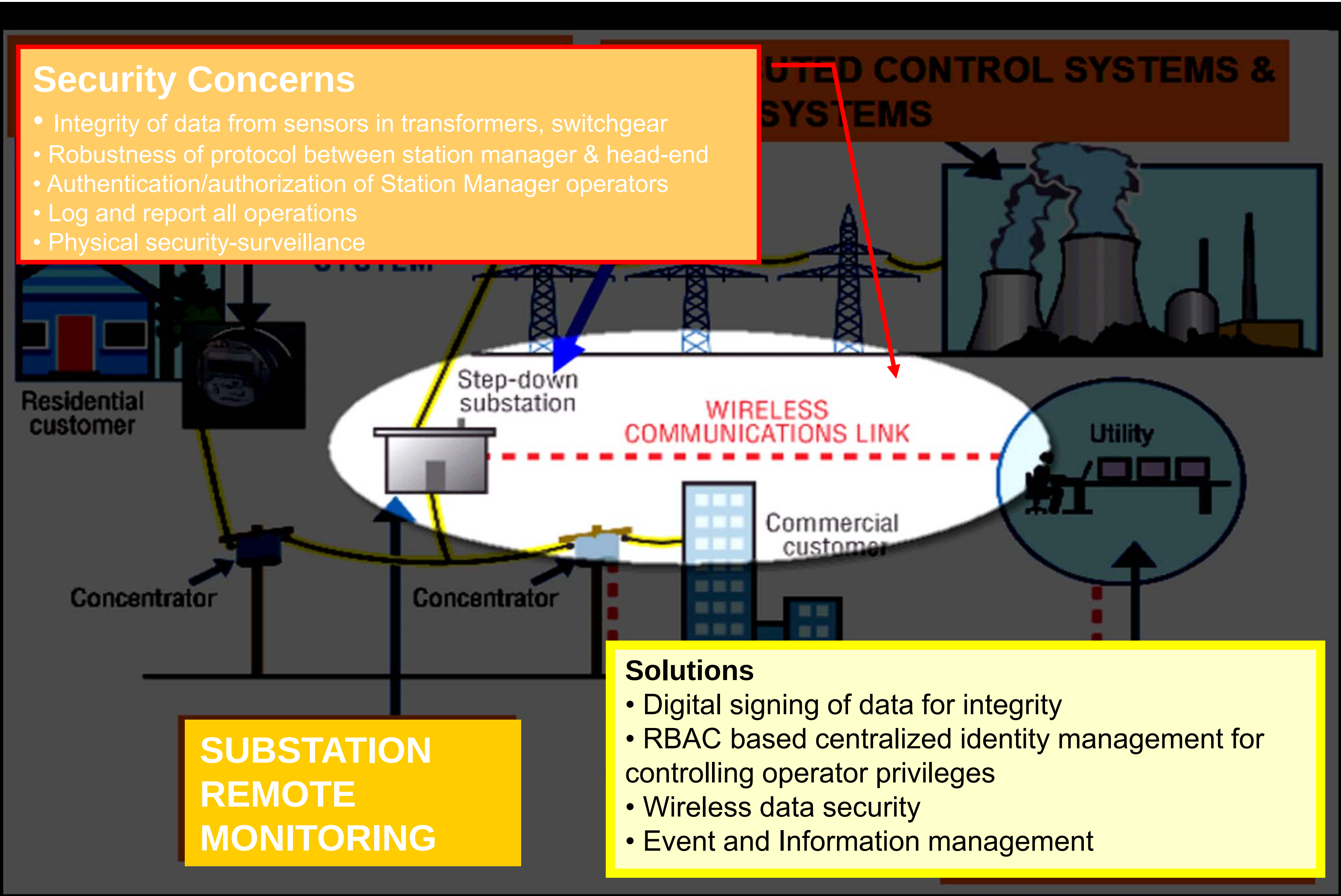


Security Concerns

- Detection of meter/cell relay tampering
- Sniff Proof 2-way communications protocols
- Distributed Energy Resource net metering
- Integrity of Firmware updates
- Disconnects/Connects need to be authorized
- Log and report all operations and events

Solutions

- Digital signing of metering data and meter control commands between meter and data collection-n-control point to create trust and tamper-free operations
- Dynamic key management
- Security Event and Information Management



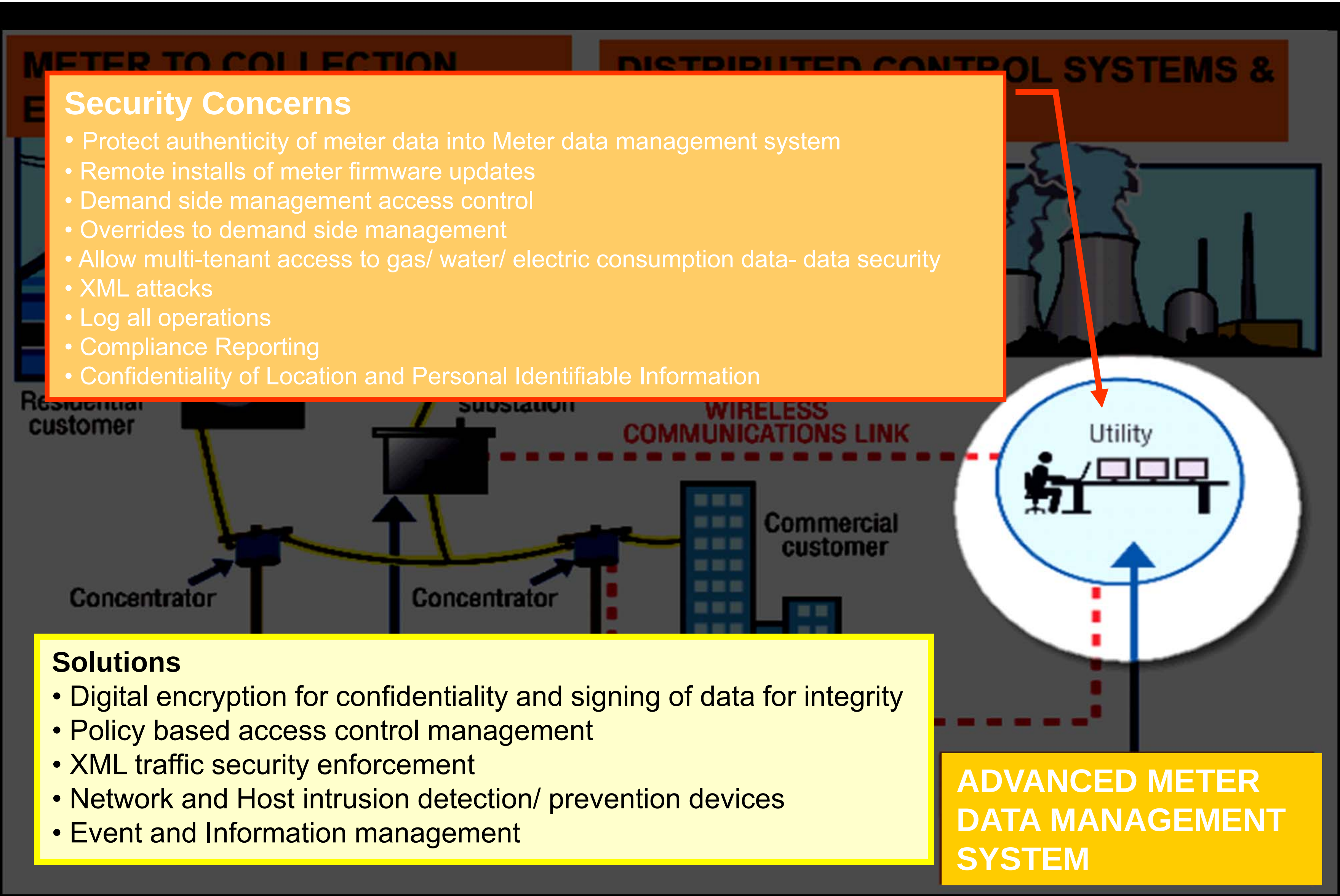
Security Concerns

- Integrity of data from sensors in transformers, switchgear
- Robustness of protocol between station manager & head-end
- Authentication/authorization of Station Manager operators
- Log and report all operations
- Physical security-surveillance

Solutions

- Digital signing of data for integrity
- RBAC based centralized identity management for controlling operator privileges
- Wireless data security
- Event and Information management

SUBSTATION REMOTE MONITORING



Security Concerns

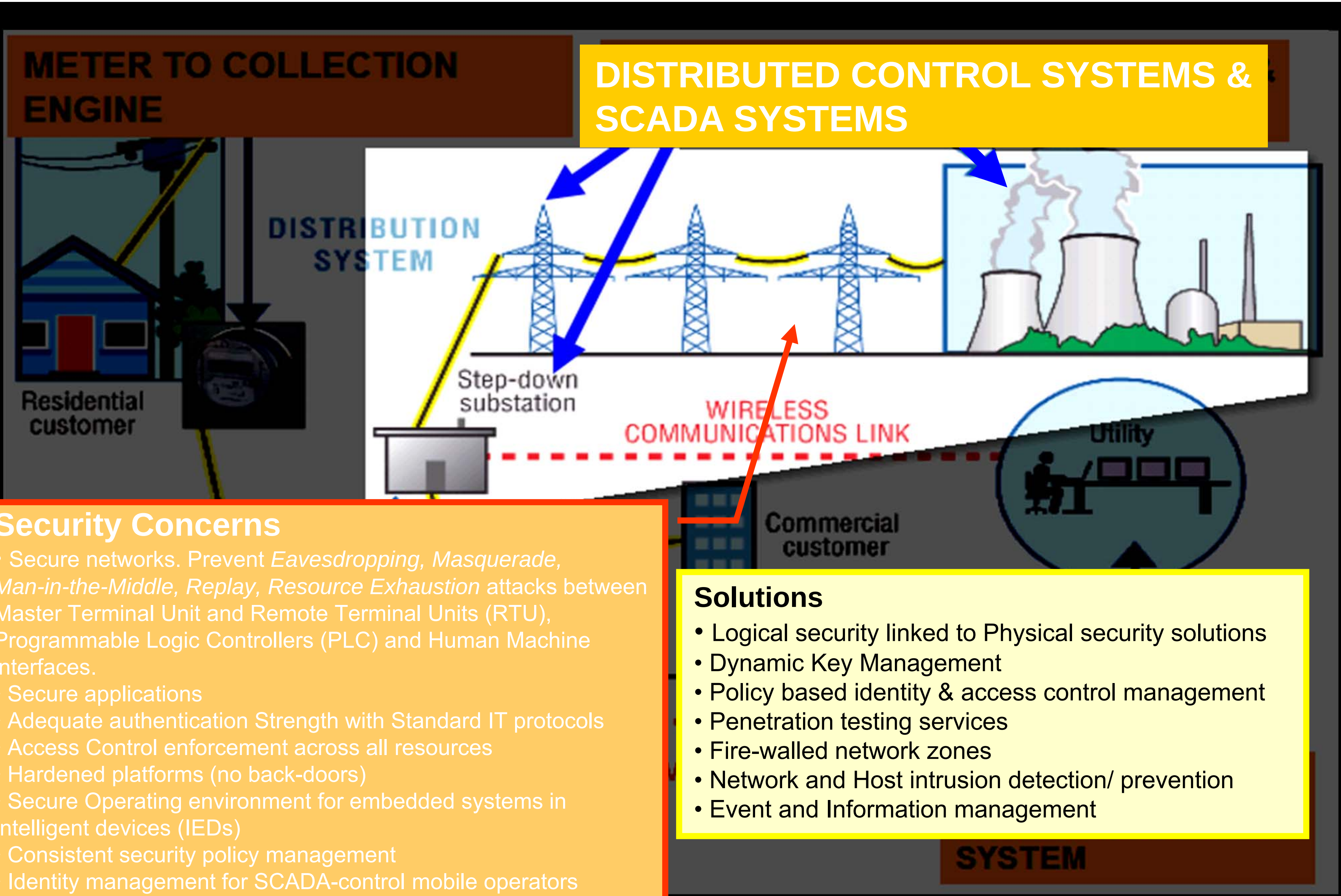
- Protect authenticity of meter data into Meter data management system
- Remote installs of meter firmware updates
- Demand side management access control
- Overrides to demand side management
- Allow multi-tenant access to gas/ water/ electric consumption data- data security
- XML attacks
- Log all operations
- Compliance Reporting
- Confidentiality of Location and Personal Identifiable Information

Solutions

- Digital encryption for confidentiality and signing of data for integrity
- Policy based access control management
- XML traffic security enforcement
- Network and Host intrusion detection/ prevention devices
- Event and Information management

ADVANCED METER DATA MANAGEMENT SYSTEM

DISTRIBUTED CONTROL SYSTEMS & SCADA SYSTEMS



Security Concerns

- Secure networks. Prevent *Eavesdropping, Masquerade, Man-in-the-Middle, Replay, Resource Exhaustion* attacks between Master Terminal Unit and Remote Terminal Units (RTU), Programmable Logic Controllers (PLC) and Human Machine interfaces.
- Secure applications
- Adequate authentication Strength with Standard IT protocols
- Access Control enforcement across all resources
- Hardened platforms (no back-doors)
- Secure Operating environment for embedded systems in Intelligent devices (IEDs)
- Consistent security policy management
- Identity management for SCADA-control mobile operators
- Physical security
- Content aware access control
- High performance

Solutions

- Logical security linked to Physical security solutions
- Dynamic Key Management
- Policy based identity & access control management
- Penetration testing services
- Fire-walled network zones
- Network and Host intrusion detection/ prevention
- Event and Information management

What E&U Companies need for Smart Grid Security

□ Products and processes that address NERC-CIP requirements*
□ Standards based Industry Framework approach

□ NERC-CIP compliance report generation tools*
□ Consulting services tailored for E&U industry
□ Policy management at the business, architectural and operational levels*

□ Trusted platforms and networks
□ Secure operating environments for Embedded Systems & Intelligent Devices
□ High performance hardware cryptographic modules

□ Intrusion detection & protection systems for preemptive threat mitigation*
□ Network, Application & Data security SW products*
 – supported by research
 – meet independent certifications
□ Application Security Vulnerability Testing tools*

□ Penetration Testing services
□ Identity & Access Management services
□ Managed Security services to help monitor and remedy networks
□ Research teams that study and publish emerging threats and exploits

□ Command centers for event management and control*
□ Critical Cyber Asset identification and management tools*
□ Security Incident & Problem Management process automation*

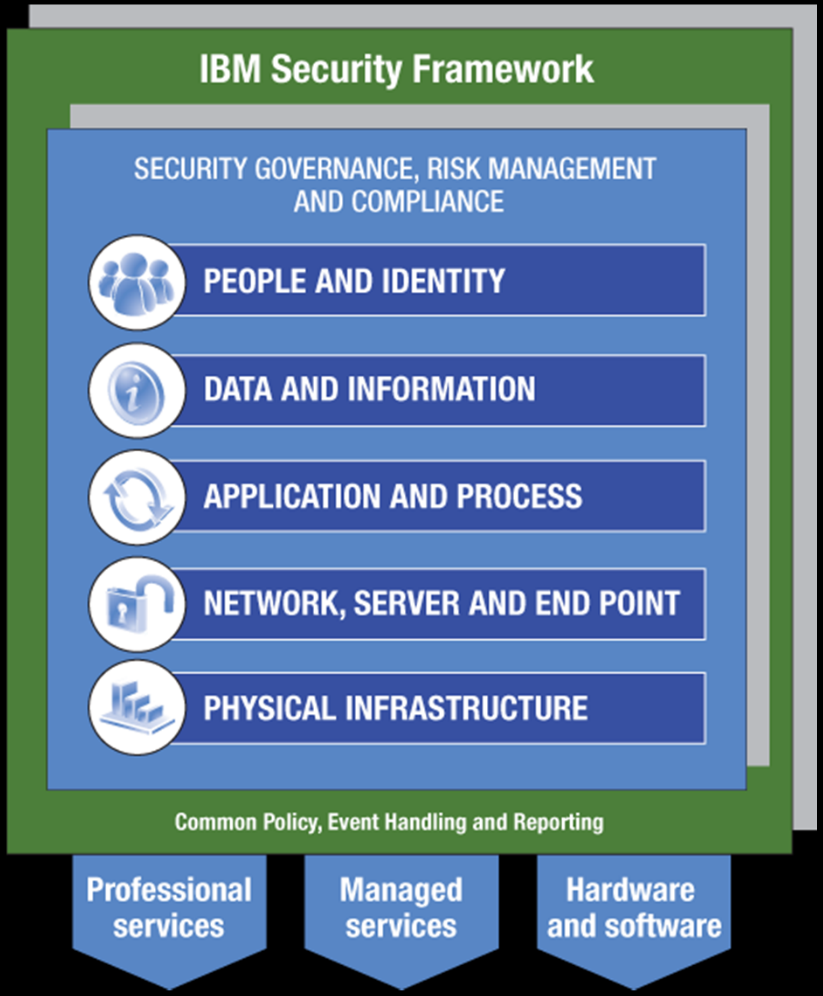
*** Items that help meet NERC-CIP requirements**

Worldwide standards equivalent to NERC-CIP
***UK**: The Center for Protection of National Infrastructure: http://www.cpni.gov.uk/*
***EU**: European Network and Information Security Agency: http://www.enisa.europa.eu/pages/About_ENISA.htm*

Take a holistic approach to cyber security

Built to meet four key requirements:

- **Provide *Assurance***
- **Enable *Intelligence***
- **Automate *Process***
- **Improve *Resilience***



End-to-End Security Perspective

The DOE has published a list of standards as part of the **Smart Grid Interoperability Standards Framework**

➢ Security at the Information Technology standards level
(ISO 27001:27005, ISO 15408)

➢ Security at the Bulk Power System Protection level
(NERC-CIP 001 – NERC CIP 009*, NIST Special Publication (SP) 800-53,
NIST SP 800-82)

➢ Security at the Industrial Control System (SCADA) level
(IEC 62443, IEC 62351 Parts 1-8 and NIST 800-82)

➢ Security relevant to the IEC 61850 substation architecture components Intelligent Electronic Devices - IEDs and Remote Terminal Unit - RTUs
(IEEE 1686-2007)

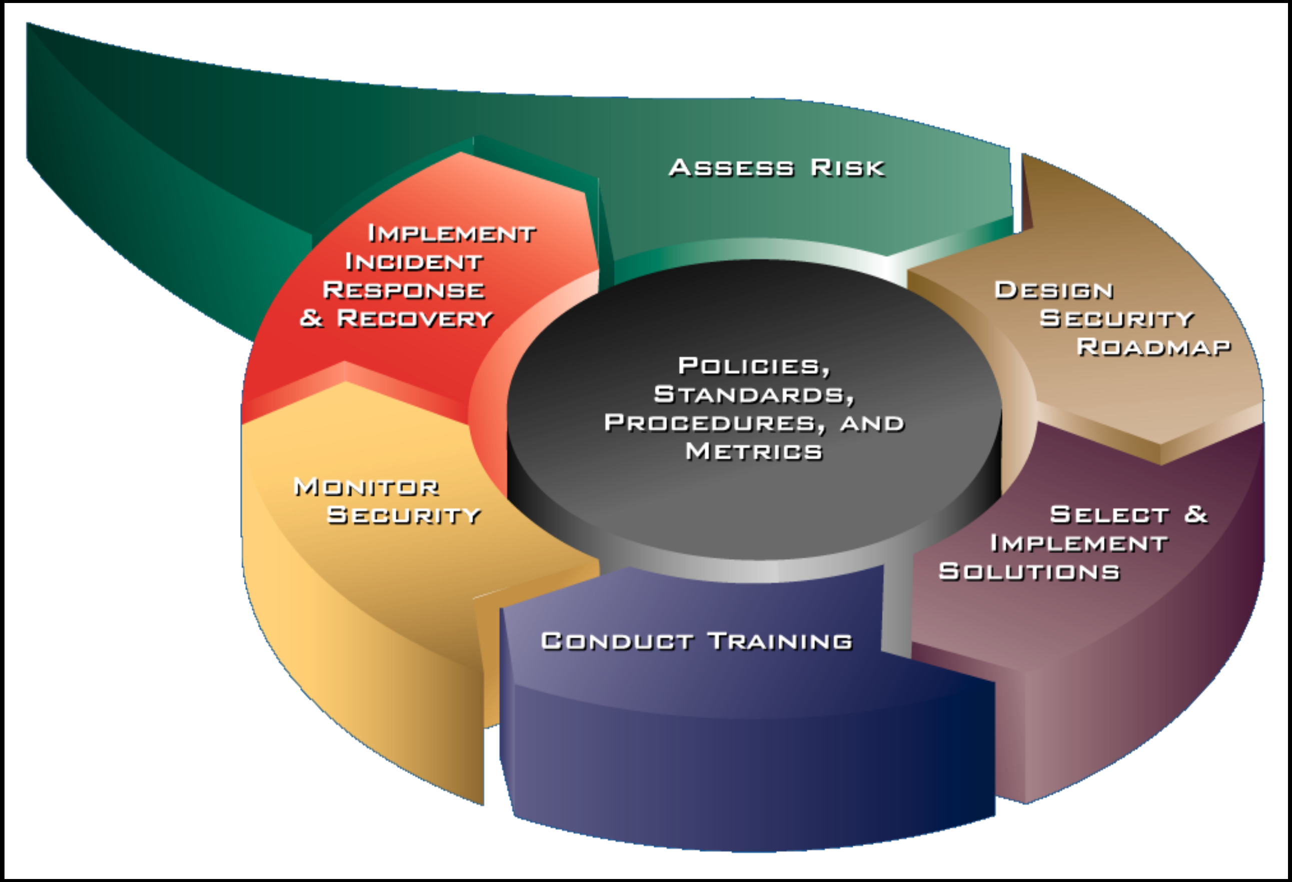
➢ Security for the Advanced Metering Infrastructure level (AMI-SEC System Security)

➢ Security for Home Area Network
(Open HAN and Zigbee)

*** Equivalent non-US standards**
In the UK: The Center for Protection of National Infrastructure: http://www.cpni.gov.uk/
In the EU: European Network and Information Security Agency: http://www.enisa.europa.eu/pages/About_ENISA.htm

Comprehensive approach focuses on the Engineering "Full Life-Cycle"

Regardless of the Smart Grid technology chosen, an integrated "Best Practices" security approach can benefit you because security becomes a continually-compliant cycle of cycles; a closed-loop-of-trust, which increases the efficiency of your overall security posture.


Assess Risk
Design Security Roadmap
Select & Implement Solutions
Conduct Training
Monitor Security
Implement Incident Response & Recovery
Policies, Standards, Procedures, and Metrics

Lessons from the Security Front

- Focus points

  - Perimeter defense alone is probably not enough
  - RF devices require additional security consideration
  - It is not just keeping the ‘bad guys’ out, it is making the internal systems less vulnerable
  - Source code security is strategic, before tactical deployment security
    - Secure development life cycle
    - Supply Chain Integrity
  - Smart Grid is a System of Systems
    - Reliability could be compromised by inadequate design without external sabotage
  - Interoperability may decrease security in the wrong architecture
  - Security often goes out the window during an emergency
  - Smart Meters can be a weak entry point
  - Resiliency is key

Lessons from the Security Front

- Points of View
  - Security is risk management
  - Security overlaps reliability
  - TCP/IP does not mean connected to the Internet, but is often interpreted that way
  - Security is part of the phase one design or don't bother with the project
  - Projects have schedules and budgets – hackers have no such constraints – thus periodic testing is required
    - Security is a process, not a project
  - Do not overlook physical security and think only of cyber
  - Fault containment is not just a power concept

Lessons from the Security Front

- Technology Implications
  - Some IP enabled devices can benefit from IT systems management techniques
  - Correlating suspicious activity from all inputs is part of the detection methodology
  - Chain rule – security is only as strong as the weakest link
  - Aspects of security involve privacy issues

Lessons from the Security Front

- Technology Implications
  - If it has a computer in it, then the security of it must be evaluated
  - Identify agency to certify “secure for smart grid”
  - Platforms must be secure too, not just components
  - Air gaps are important – please balance convenience with security
  - Other industries have tackled similar issues
  - Airplane is unstable but has good control system
  - Utilities should test devices for functionality and scalability
    - Maintenance ports in devices can be missed in utility evaluation
  - Difficult to define cyber security metrology
    - It is not the engineer’s fault if the bridge is blown up
    - Avoid law of externalities – sloppy security is OK because consequences laid on someone else
  - Standards for interoperability do not imply security
  - What does/should your vendor disclose about security ?

Evolution of Electric Utility Risks

PAST HARD-WIRED CONTROL

- Most controls are “hard wired” AND require manual intervention
- Lesser public availability of RF devices
- Little capability for damage to or financial benefit from RF attacks
- Cost-plus charging – “If we need it, we’ll do it! If we can’t do it, we’ll buy it!”
- Clear regulatory and financial landscape

PRESENT SCADA / RF ENABLED

- Financial pressure to reduce staffing;
- Computerization and RF control become common
- Project excellence not always followed by outstanding security operations
- SCADA hacking can cause damage to neighborhoods and equipment
- Uncertain regulatory, audit, and liability landscape

NEAR FUTURE SMART GRID / RF PERVASIVE

- Control inside-the-home of all appliances
- Wide use of 802.x, ZigBee, X10 methodologies
- Uncertain Software Provenance, Packages
- Increased organized crime / terrorist focus
- Potential for damage to, and “net” theft by everyone
- Revenue/Risk asymmetry for each customer
- RF transition to IP and OS “Monoculture”
- Increased public and regulatory scrutiny

Security Concerns in Advanced Metering Control and Data Management

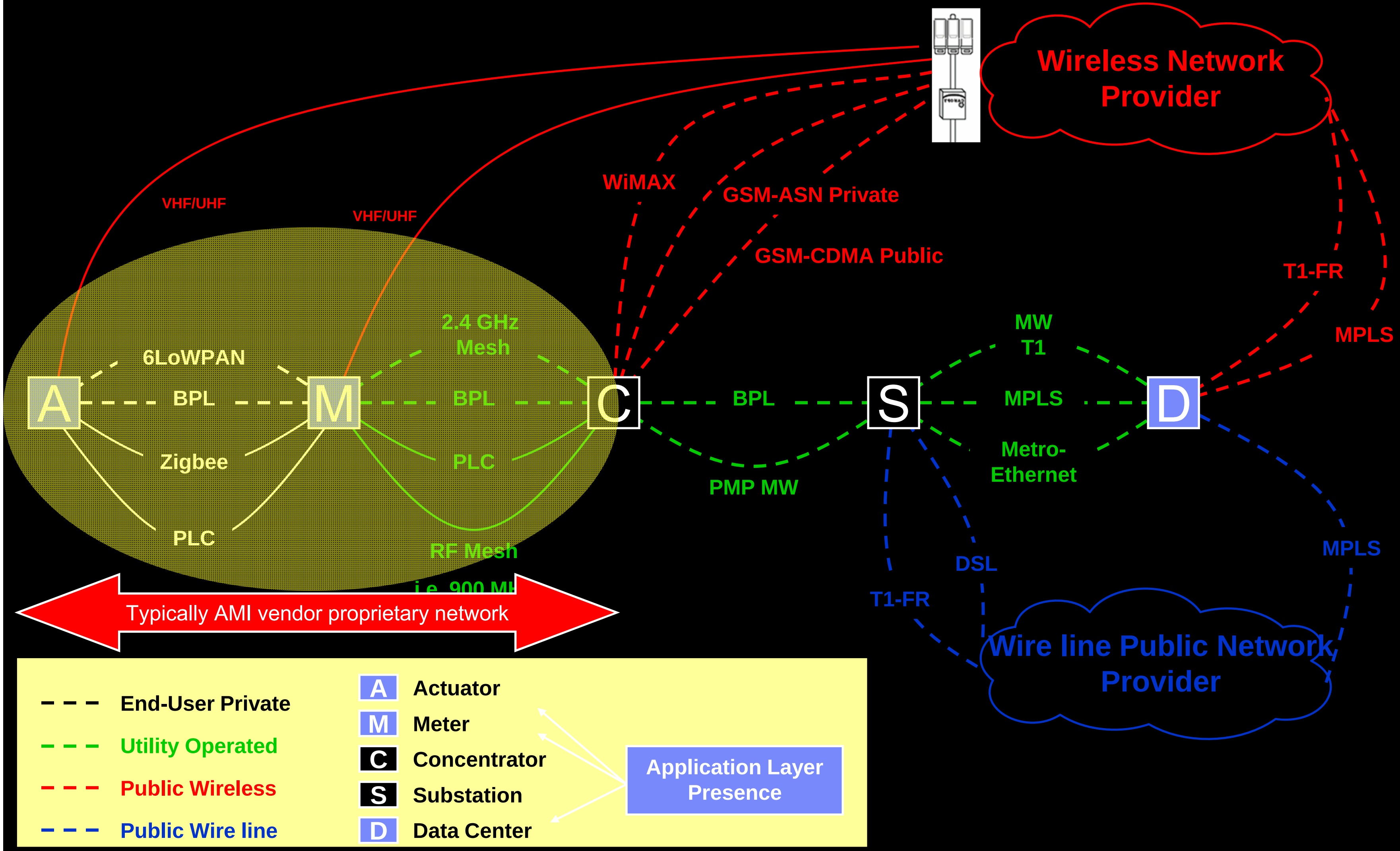
Category	Security Concerns
Billing	▪Integrity of meter data ▪Availability of meter data to contracting utilities (B2B infrastructure)
Distribution	▪Efficient and accurate unplanned and planned outage detection ▪Load control – reliability of connect/disconnect service
System	▪Integrity of end to end infrastructure ▪Integrity of tamper indication notifications ▪Enforce access control of customer equipment (HAN)
Installation (lifecycle)	▪Integrity of meter firmware updates; resistance to malicious tampering
Customer	▪Confidentiality of Personal Identification Information Data ▪Customer access control to account management applications ▪Availability of customer payment data and usage balances

Advice for the Security Conscious

- Defense in depth can mean more attack surfaces
- There is no security balance – always commoditization of hacking tools, creating a perpetual state of tension
- Don’t forget the human attack vectors
  - Misinformation given to operators
  - Irresponsible disclosure by testers
- Security standards can be the enemy of situational awareness
  - Target dies with all boxes checked
  - Want culture of security, not culture of compliance
  - Pioneers take the arrows
  - Gardeners should not be surprised by weeds in their garden
- Amateurs attack algorithms, professionals attack key management

Issues and Trends – Multiple Ways to Reach End Points

The Smart Grid of the future will be a network of networks



– – –	End-User Private	A	Actuator
– – –	Utility Operated	M	Meter
– – –	Public Wireless	C	Concentrator
– – –	Public Wire line	S	Substation
		D	Data Center

Application Layer Presence

© 2010 IBM Corporation

Threats of Interest

- Local Attacks (physically at the device)
  - Software Modification / Substitution / Addition
  - Hardware Modification / Substitution / Addition
  - Data Modification / Substitution / Addition (e.g., Bit twiddling, memory-based attacks)
  - Denial of service
  - Covert Channel
  - Side Channel
  - Traffic flow analysis

- Remote Attacks (Trying to break in from anywhere in the internet)
  - Software Modification (Injection, Buffer overflow, …)
    - persistent modification
    - runtime modification
  - Denial of service

- Network Based Attacks (breaking in from the “local” network)
  - Eaves dropping (breach of confidentiality)
  - Man-in-middle (read and change messages)
  - Message Forgery
  - Message Replay
  - Traffic analysis
  - Protocol-Based Denial of Service Attack

Secure Endpoints

- **Authentication:** Ensures endpoints and systems are mutually authenticated
- **Data Integrity & Confidentiality**: Ensures data is untampered and visible only to intended recipient
- **Endpoint security awareness:** Software Integrity Attestation provides assurance that endpoint has not been tampered with

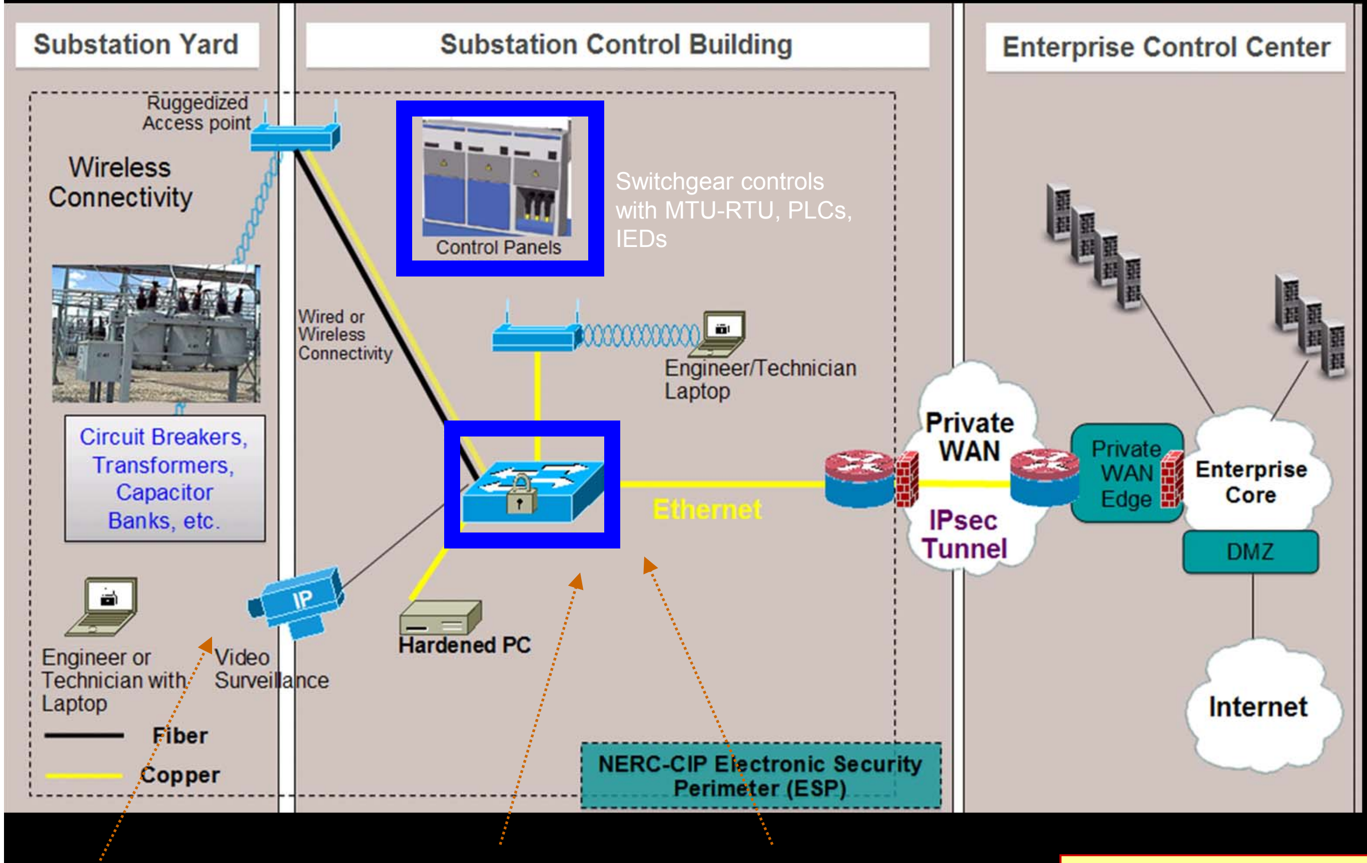
Integrated SW platform

- Integrated software offers unified and consistent security and asset management platform

Hardware protection

- Physical attack protection
- Side-channel attack protection
- Tamper detection, response protection
- Software compromise detection
- Secure sensor identification

Smart Grid: Substation Architecture
Cyber and Physical Security


Substation Yard
Substation Control Building
Enterprise Control Center
Ruggedized Access point
Wireless Connectivity
Control Panels
Switchgear controls with MTU-RTU, PLCs, IEDs
Wired or Wireless Connectivity
Engineer/Technician Laptop
Circuit Breakers, Transformers, Capacitor Banks, etc.
Ethernet
Private WAN
IPsec Tunnel
Private WAN Edge
Enterprise Core
DMZ
Internet
IP
Engineer or Technician with Laptop
Video Surveillance
Hardened PC
Fiber
Copper
NERC-CIP Electronic Security Perimeter (ESP)

SCADA Terminology & Technology

SCADA: *Supervisory Control And Data Acquisition*

MTU-RTU: *Main Terminal Unit; Remote Terminal Unit*

PLC*: Programmable Logic Controllers*

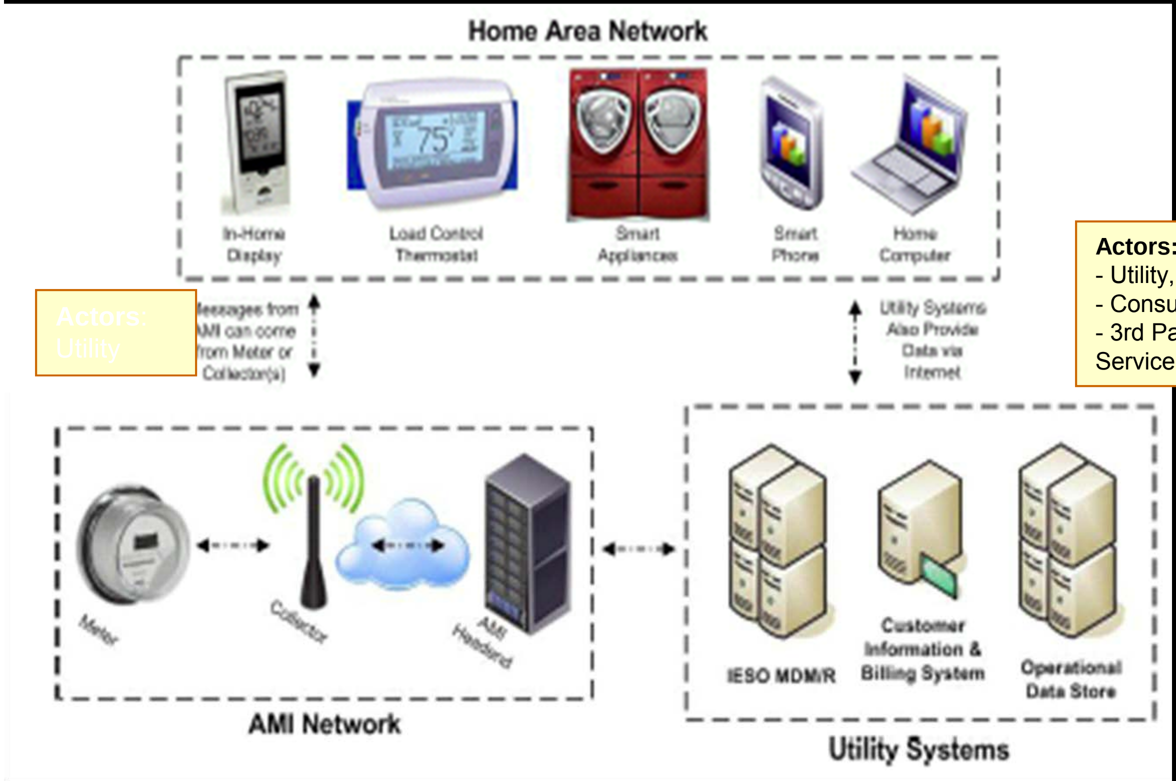
IED: *Intelligent Electronic Devices*

DNP3: *Communications Protocol between process automation components on industrial control networks*

MMI: *Machine to Machine Interface*

HMI: *Human-Machine Interface*

Smart Grid: Home Area Networks & Smart Energy Management



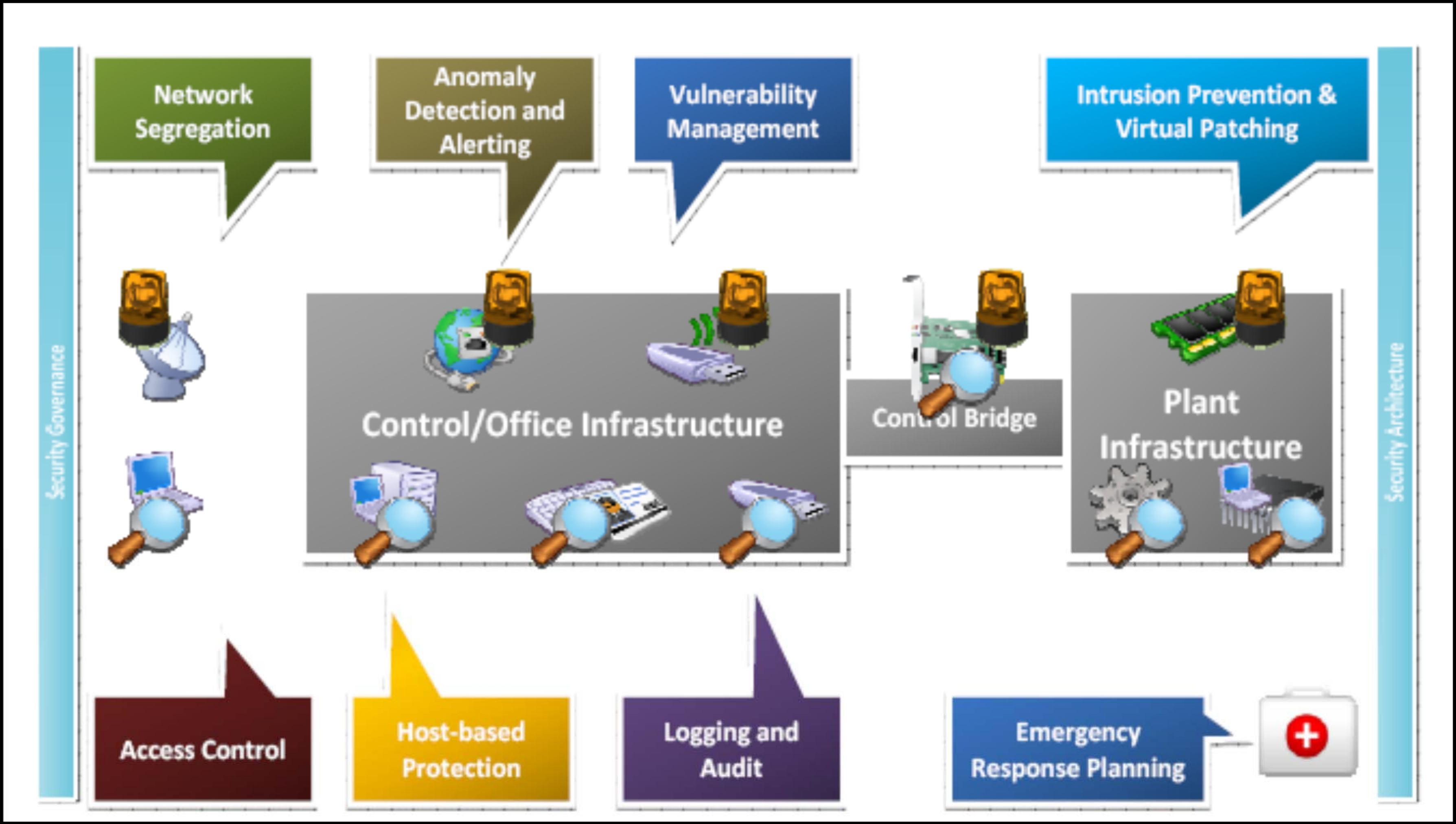
Actors:
Utility

Actors:
- Utility,
- Consumer
- 3rd Party Energy Mgmt Service Providers

HAN Terminology & Technology

Zigbee : IEEE 802.15.4 based wireless protocol adopted for home area networks
***Zigbee Smart Energy Certified Devices:** Home Devices capable of communicating with a Zigbee network coordinator and then joining that network*
***Distributed Energy Resources (DER):** Solar panels, wind farms, Electric Vehicle Batteries*
***ESP**: Energy Service Providers: New Services for smart energy management*
***ESG**: Energy Services Gateway: Customer premise equipment accessing Home area devices through the ISP or utility provided networks*

Comprehensive Protection


Security Governance
Network Segregation
Anomaly Detection and Alerting
Vulnerability Management
Intrusion Prevention & Virtual Patching
Control/Office Infrastructure
Control Bridge
Plant Infrastructure
Security Architecture
Access Control
Host-based Protection
Logging and Audit
Emergency Response Planning