火龙果·整理
uml.org.cn

企业安全风险与防护

2010年12月于昆明. 中国

火龙果·整理
uml.org.cn

主要内容

- 电网安全威胁分析
- 智能电网安全防护方案
- 南网十大安全风险与防护方案

2009 IBM X-Force® 威胁趋势与风险分析报告：-- 在信息系统的每个层面都存在漏洞、攻击威胁

Application and Process

- 6,601 new vulnerabilities were discovered in 2009, an **11%** decrease over 2008, largely due to declines in SQL injection and Active X vulnerability disclosures.
- **49%** of all vulnerabilities are Web application vulnerabilities.
- **52%** of all vulnerabilities disclosed had no vendor-supplied patches available at the end of 2009.

Data and Information

- PDF-related vulnerabilities have far surpassed those affecting Office documents.
- Vast majority of Web-based exploitation centered around Web exploit toolkits in contrast to purpose-built lone sources.
- US continues as the top hoster of malicious Web links.

Network, Server, and End Point

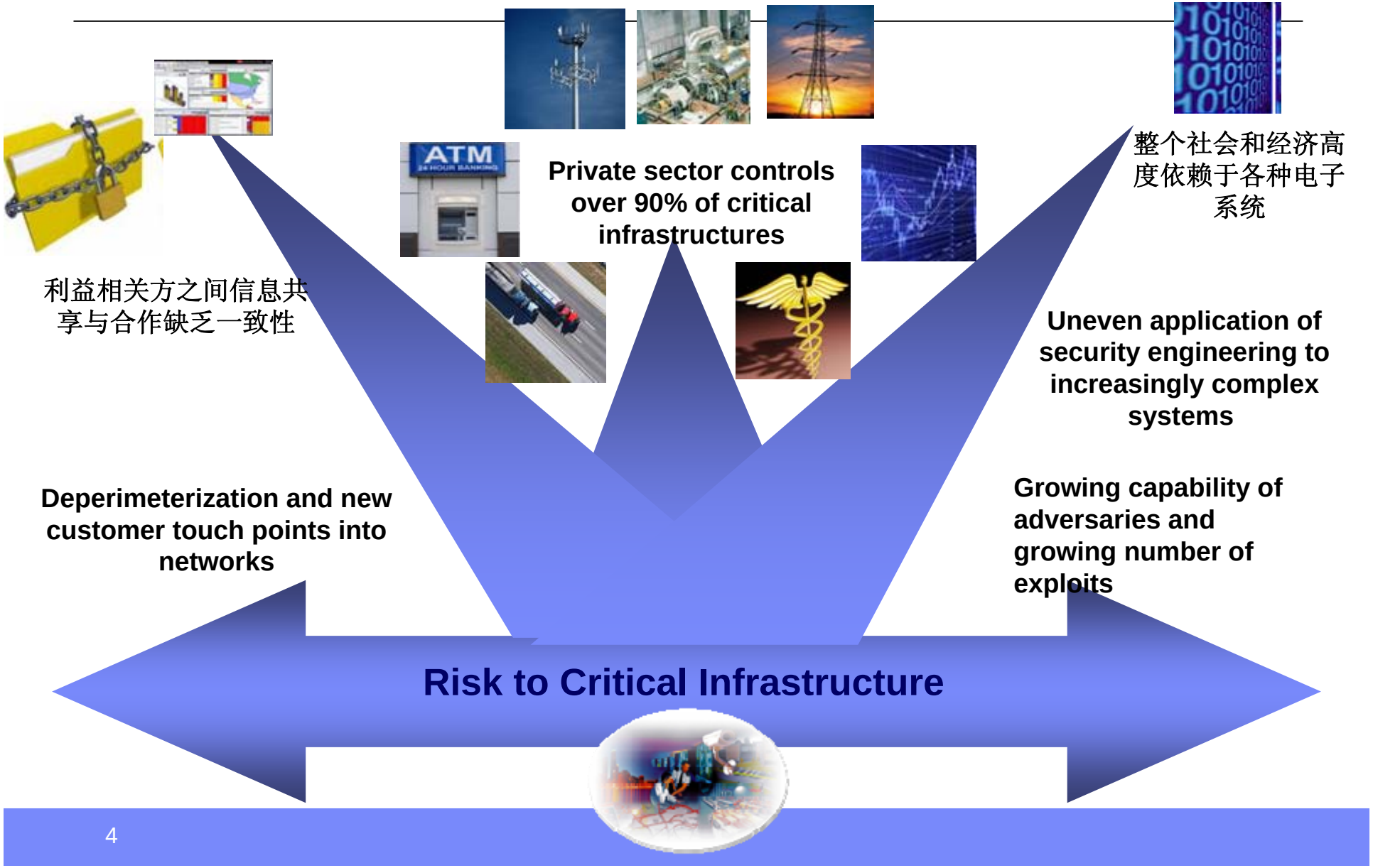
- 7.5 percent of the Internet is considered “socially” unacceptable, unwanted, or flat out malicious.
- New malicious Web links increased by **345%** compared to 2008.

People and Identity

- Majority of spam **(80%)** is still classified as URL spam—spam messages that include URLs that a person clicks to view the spam contents.
- Amount of URL spam using well-known and trusted domain names continue to increase.
- **60.9%** of phishing is targeted at the finance industry, **20.4%** targeted at government organizations.

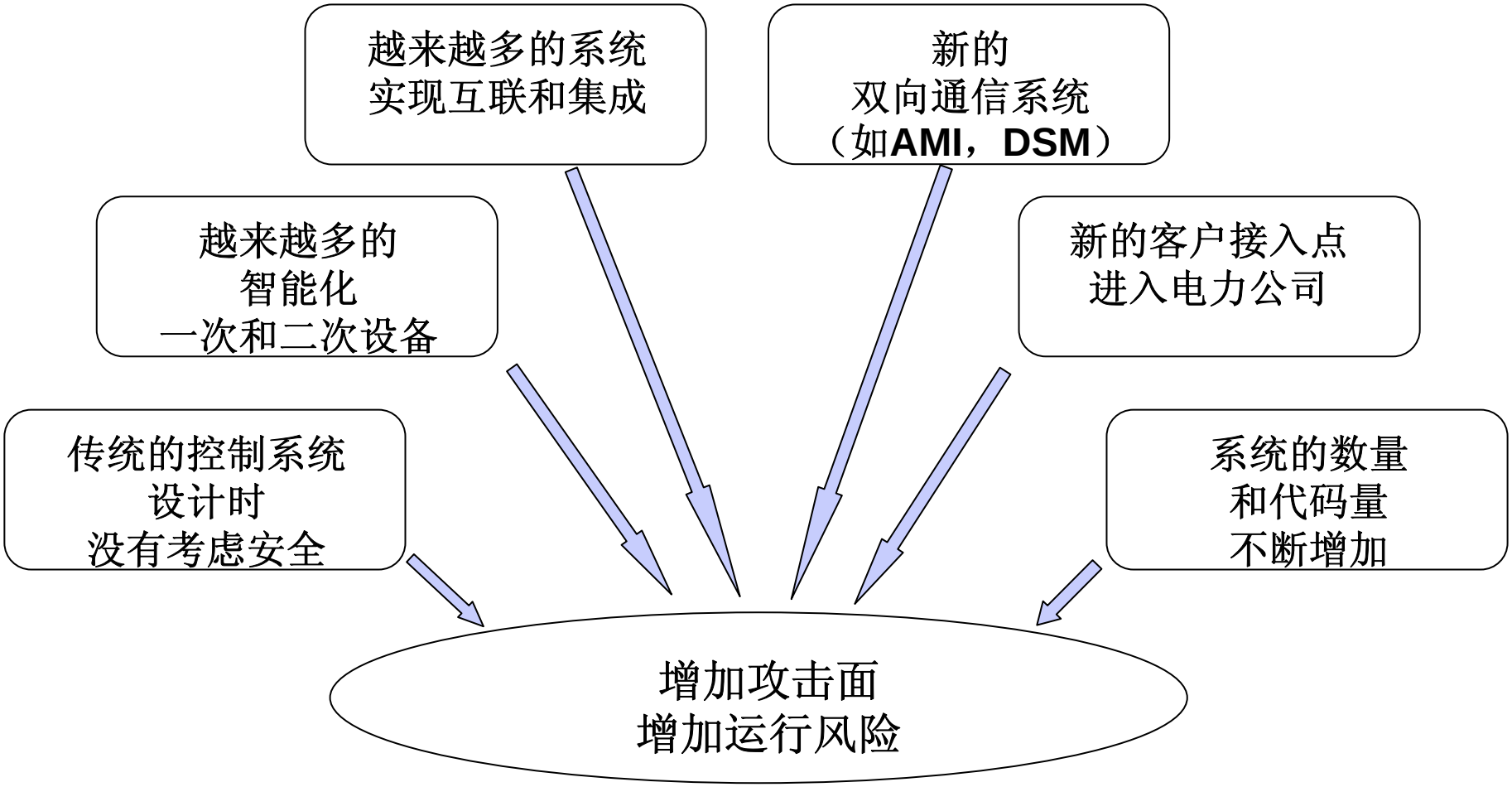
火龙果 · 整理
uml.org.cn

影响智能电网体系结构安全性的各种因素

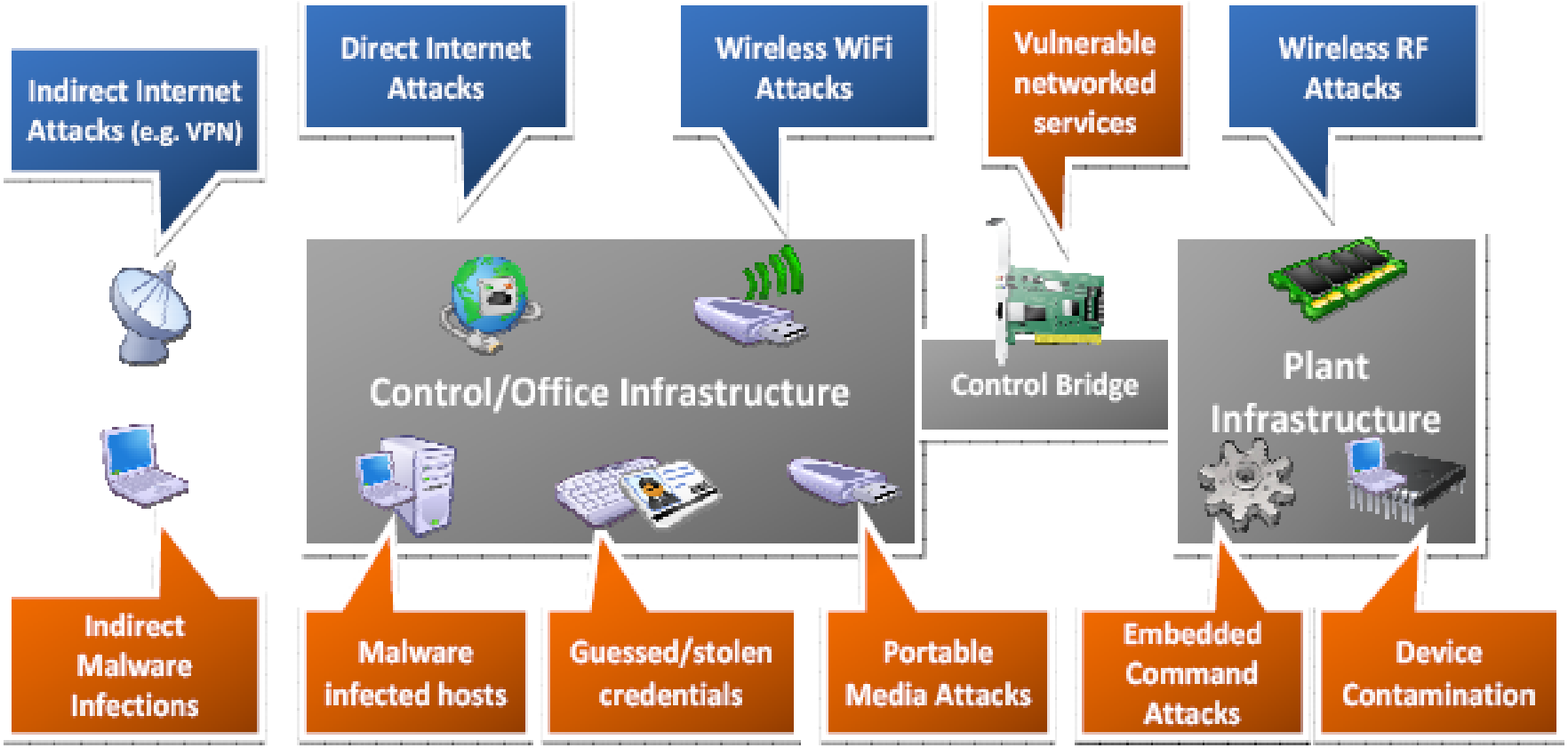


火龙果·整理
uml.org.cn

对数据和信息的依赖使电网面临的信息安全风险大大增加，表现在通信协议、访问控制、传输、业务流程等各个方面



在复杂的电网IT环境中也存在很多的攻击形式



火龙果·整理
uml.org.cn

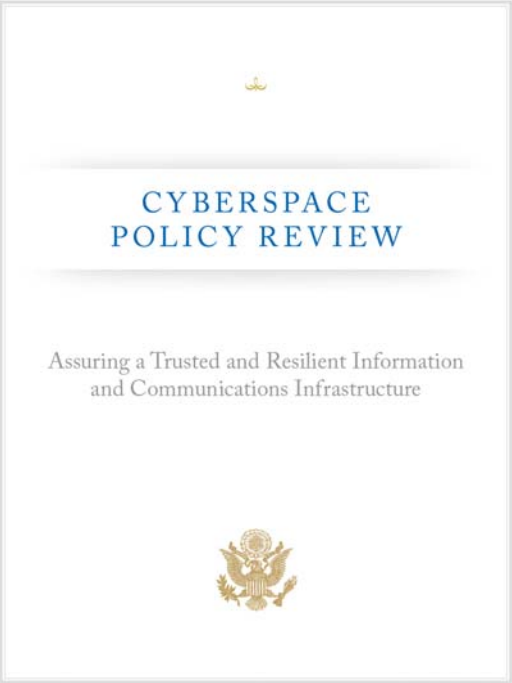
网络攻击不仅会破坏信息和数据，甚至会直接威胁电网设备

- 近些年美国发生的一些针对电网的攻击事件
  - 2001年，黑客侵入了加州ISO，负责监视全州大部分地区的电力传输网。攻击途经加利福尼亚和俄克拉荷马州。
  - 2003年1月，俄亥俄州Davis-Besse核电厂安全监测系统由于Slammer蠕虫病毒而离线5个小时。
  - 2003年10月，19岁的Aaron Caffrey入侵休斯敦港网络。这被认为第一个被广泛报道的对美国重要基础设施的攻击。
  - 2005年3月，电力行业的信息安全顾问在报告中说，黑客已经把美国电网作为目标，并已进入了美国公用事业的电子控制系统。在少数情况下，这些入侵“造成了影响“。
  - 2009年4月，华尔街日报指出有黑客侵入了美国的电网并留下了后门程序，可以让他们破坏电网服务。

- 真实的威胁
  - 2007年，美国爱达荷州国家实验室的研究人员进行了一项实验，通过网络攻击造成了发电机的自毁。

火龙果 · 整理
uml.org.cn

为此，美国制定了信息安全政策



...在美国部署新的智能电网技术时，联邦政府必须确保安全标准的制定和采用，以免给对手可乘之机，穿透这些系统或进行大规模袭击。

到2013年北美电力公司的年度智能电网信息安全开支将超过7.5亿美元

- EISA 2007
- NERC CIP Standards
- NIST Interoperability Standards
- Enterprise Security Policy

- *攻击 –*
- *窃听*
- *破解*
- *拒绝服务攻击*
- *破坏*
- *恶意软件安装*
- *重新配置*
- *重放*
- *社会工程*
- *欺骗*
- *流量分析*

火龙果·整理
uml.org.cn

同时，NIST成立了智能电网信息安全协调工作组（ CSCTG ）

- 超过270个成员，来自于政府、学术界和行业界
- 已经建立了几个工作组，包括：
  - 漏洞级别分析
  - 自下而上的评估
  - 隐私权
  - 标准评估
  - 高阶需求
  - 开发功能性架构
  - 研究与开发
- 最终成果
  - 一个推荐的智能电网信息安全需求集
- 今后的活动...
  - 加密和密钥管理
  - 参与开发智能电网信息安全合格评定战略

并且制定了智能电网信息安全的相关标准

支持许多不同的智能电网应用系统的每一个接口都需要标准。同样，数据网络和信息安全也需要标准。

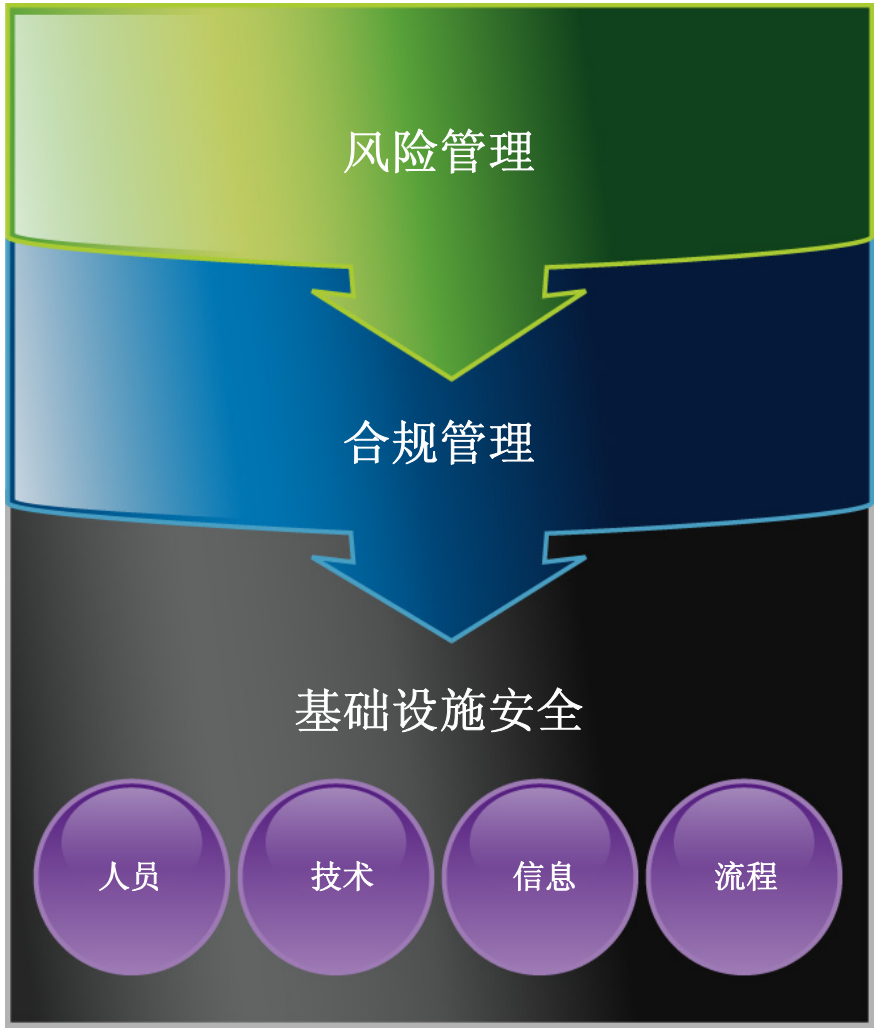
- 已经有超过46个智能电网信息安全的相关标准，涉及的国际组织包括：IEC，IEEE，NIST，W3c，NERC，ISO/IEC，IETF等。
- 安全要求涉及智能电网的一个或多个方面
  - 与智能电网直接相关的
    - NERC CIP 002-009, *Cyber Security*
    - IEEE 1686, *IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities*
    - AMI-SEC *System Security Requirements*
    - OpenHAN SRS
    - IEC 62351, *Power System Control and Associated Communications - Data and Communication Security*, Parts 1-8
  - 与控制系统密切相关的
    - ANSI/ISA-99, *Manufacturing and Control Systems Security*, Parts 1 and 2
    - NIST SP800-53, *Recommended Security Controls for Federal Information Systems*
    - NIST SP800-82, *DRAFT Guide to Industrial Control Systems (ICS) Security*
    - DHS Procurement Language for Control Systems
    - ISA SP100, *Wireless Standards*

火龙果·整理
uml.org.cn

主要内容

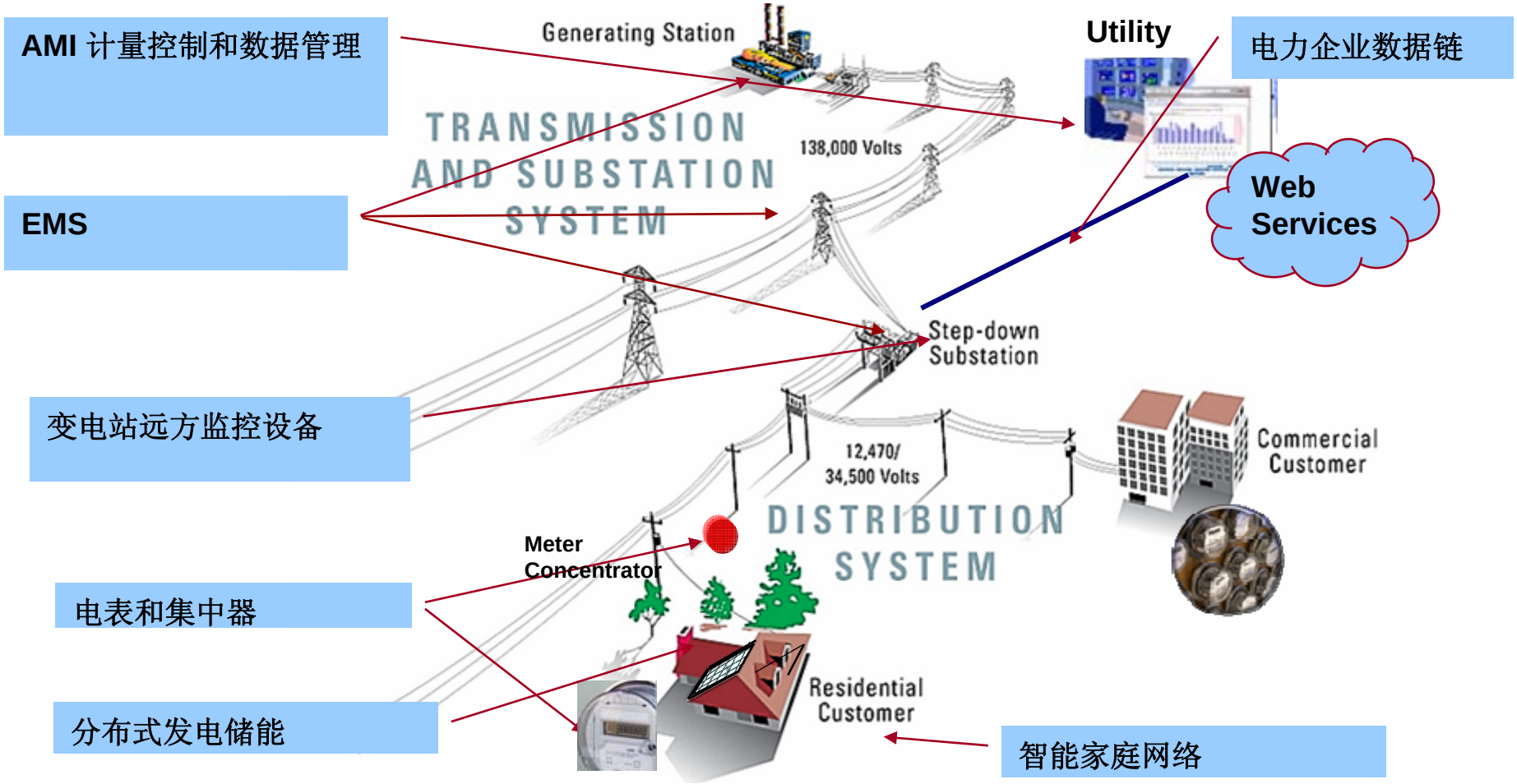
- 电网安全威胁分析
- 智能电网安全防护方案
- 南网十大安全风险与防护方案

对电力公司来说，信息安全的要求来自三个方面



- 保护企业
  - 知识产权
  - 客户信用记录
  - 内部/ IT的运营
- 法规要求
  - 电监会5号令
  - NERC-CIP, FERC, PCI…
- 保护智能电网
  - 保护控制系统（如SCADA）
  - 传感器和设备，网络和基础设施

智能电网安全管理跨越整个供应链

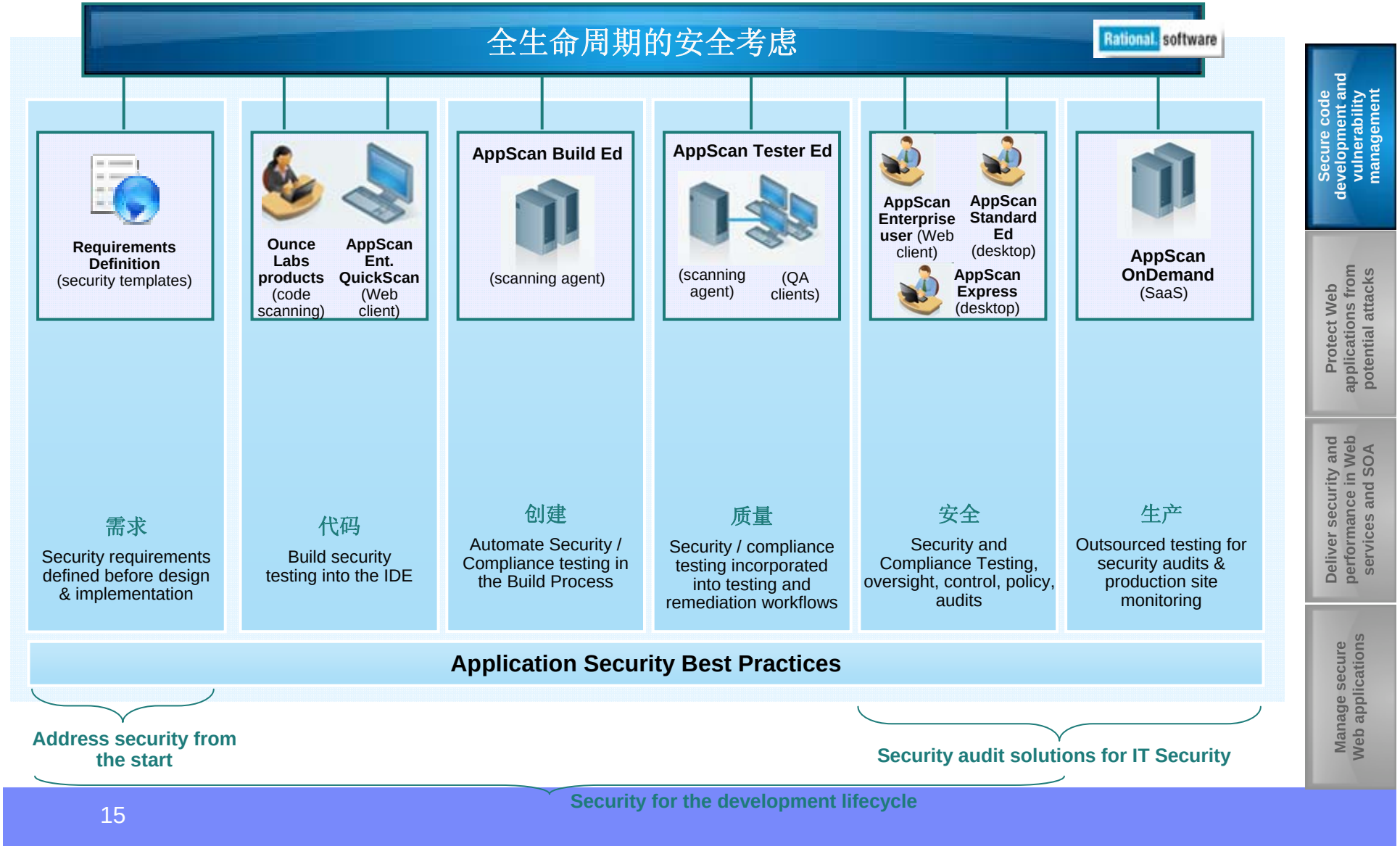


AMI系统安全防护建议

Advanced Meter Infrastructure (AMI) / Smart Meter Security Considerations

火龙果 · 整理
uml.org.cn

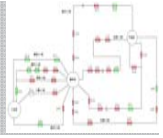
AMI安全防护应当贯穿产品和应用系统的整个生命周期，从需求、设计、开发、部署到运行



火龙果 · 整理
uml.org.cn

AMI安全防护分为如下几个关键步骤

目标	A fundamental objectives of AMM security
策略和路程	A fundamental rethink of business strategy and security
安全规范和标准	Alignment of corporate security polices with Smart Grid Security; evaluation and adoption of emerging standards
安全架构	A well-defined architecture that is all encompassing
安全评估	A focused look at all aspects of risk
安全测试	Comprehensive component and system level testing
实施	Comprehensive security solution implementation



①安全防护的目标

- 安全：抵御外部攻击
- 保密：信息的私密性
- 集成：数据的集成能力
- 可用：对授权的用户，提供可靠的服务

火龙果·整理
uml.org.cn

①安全防护的目标：安全体系成熟度

成熟度等级	读取控制策略	动态密钥管理	安全运行控制	远方安全升级	加密对称私钥	分片防火墙
5	X	X	X	X	X	X
4		X	X	X	X	X
3		X	X	X	X	X
2			X	X	X	X
1				X	X	X
0						X
* Maturity increases 0 to 5						

Source: Gartner (December 2007)

Based on Gartner's Maturity Level 5 and a security "Best Practices" approach, Oncor's AMS Security Architecture Framework has the ability to address the maturing ANSI C12.22 and ZigBee standards, while meeting/exceeding other emerging security standards (e.g., AMI-SEC).

②安全防护体系策略

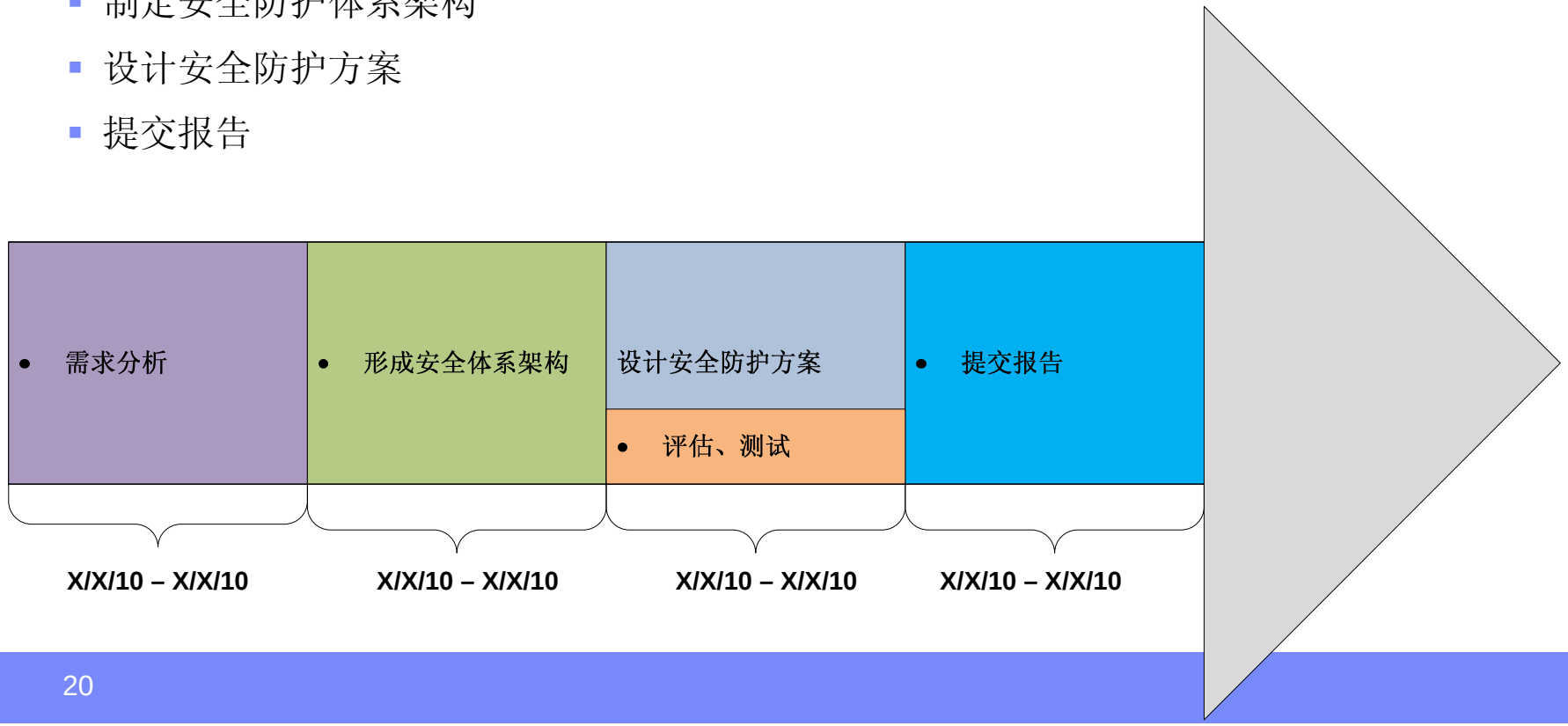
- 了解用户需求
- 安全法规
- 数据流
- 安全标准和规程
- 安全原则
- 安全服务
- 监管,风险和遵从
- 整体方案和部分点的方案
- 实施计划
- 支持

火龙果·整理
uml.org.cn

②安全防护体系路线

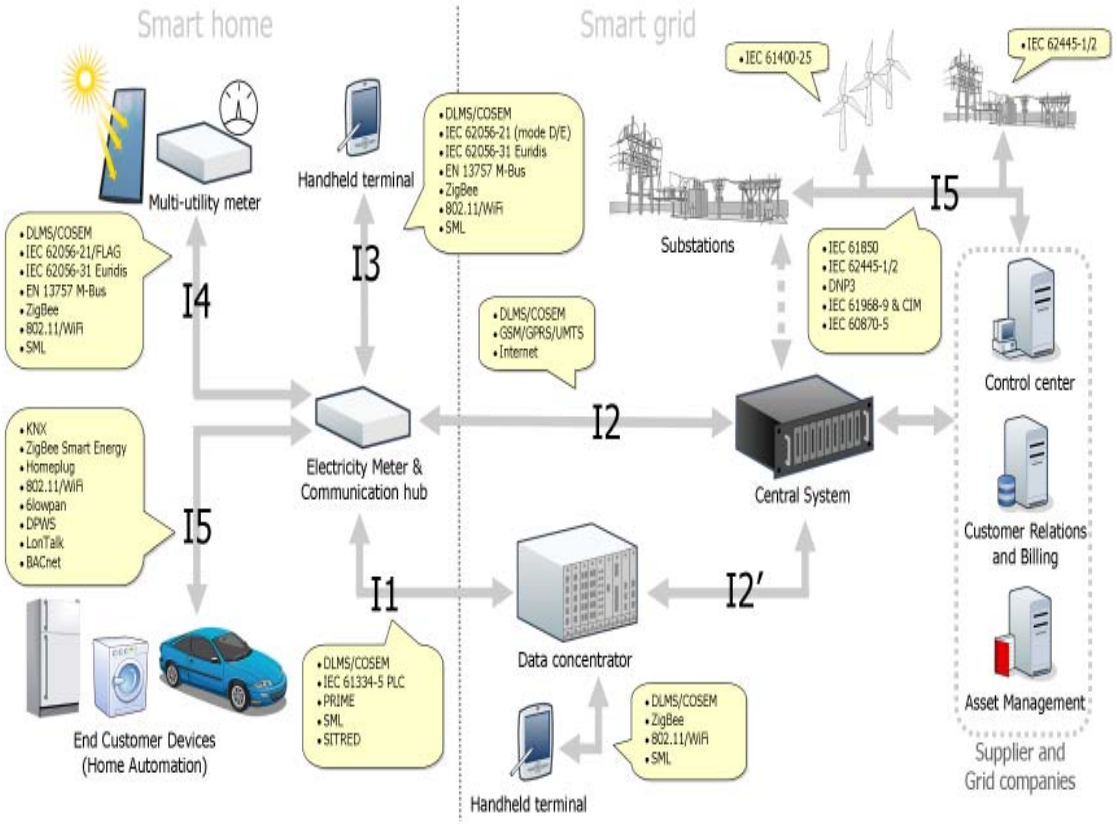
安全防护执行路线分为四个阶段：

- 需求分析：确定安全防护体系的目标，分析现有系统和计量自动化安全防护的成熟度模型
- 制定安全防护体系架构
- 设计安全防护方案
- 提交报告



③最终形成电网公司的安全规范和标准

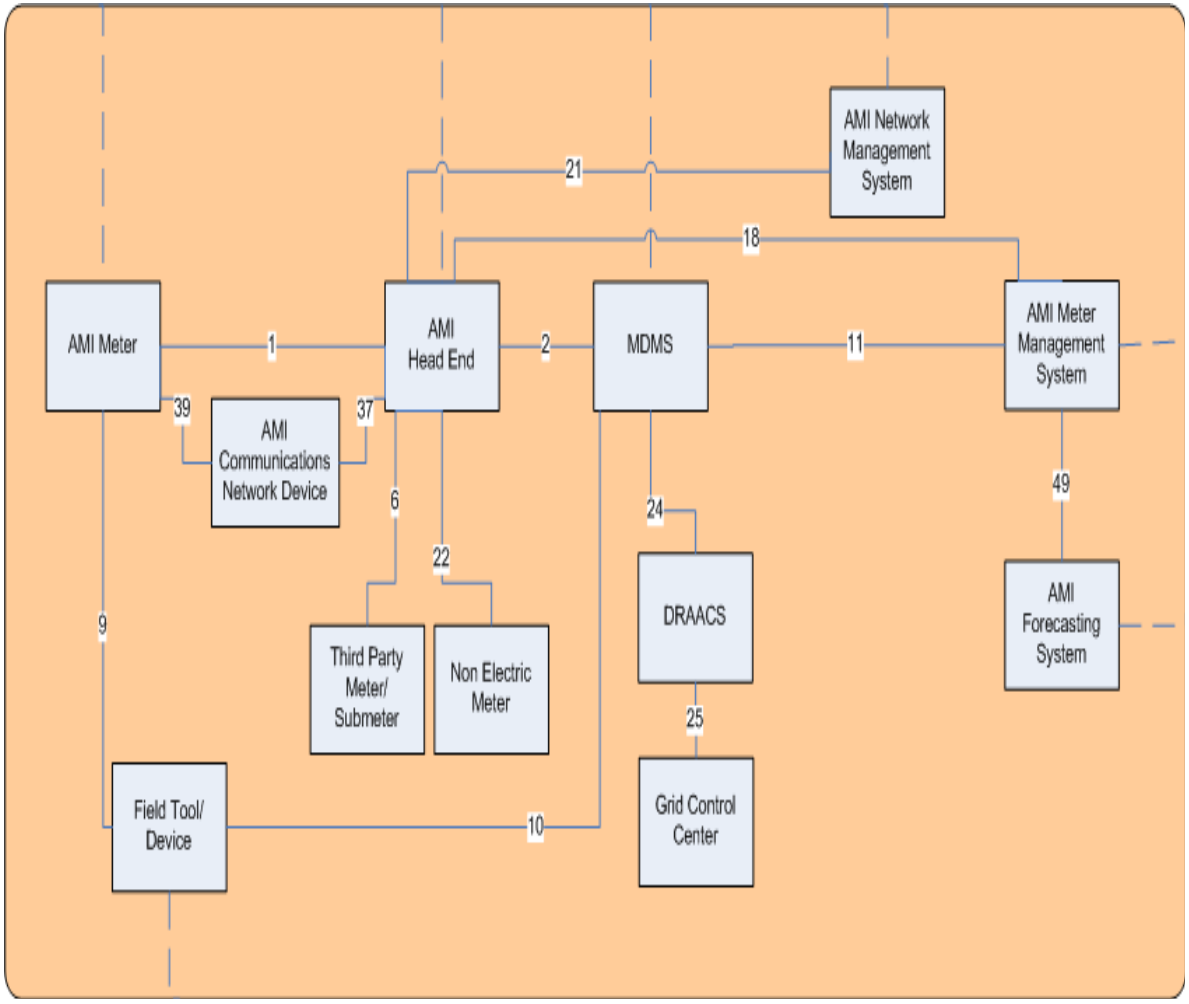
- 遵循的标准
- 公司的IT政策
- 公司的IT标准
- 新的政策和标准
- 业务安全等级
- 架构安全等级
- 运行安全等级
- 执行
- ……



火龙果 · 整理
uml.org.cn

④安全防护体系架构

- 安全设计原则和目标
- 安全架构概述
- 安全分区概述
- 子系统和模块
- 安全架构路线
- 高等级解决方案设计
- 详细设计
- 身份读取管理
- 安全遵从管理
- 安全政策监管管理
- SOA 安全服务
- 消息管理
- 数据中心的安全



⑤安全防护体系的风险评估

- 开发威胁
- 认证资产
- 评估威胁
- 评估资产漏洞
- 计算风险
- 确定影响
- 测定
- 执行
- 剩余风险管理

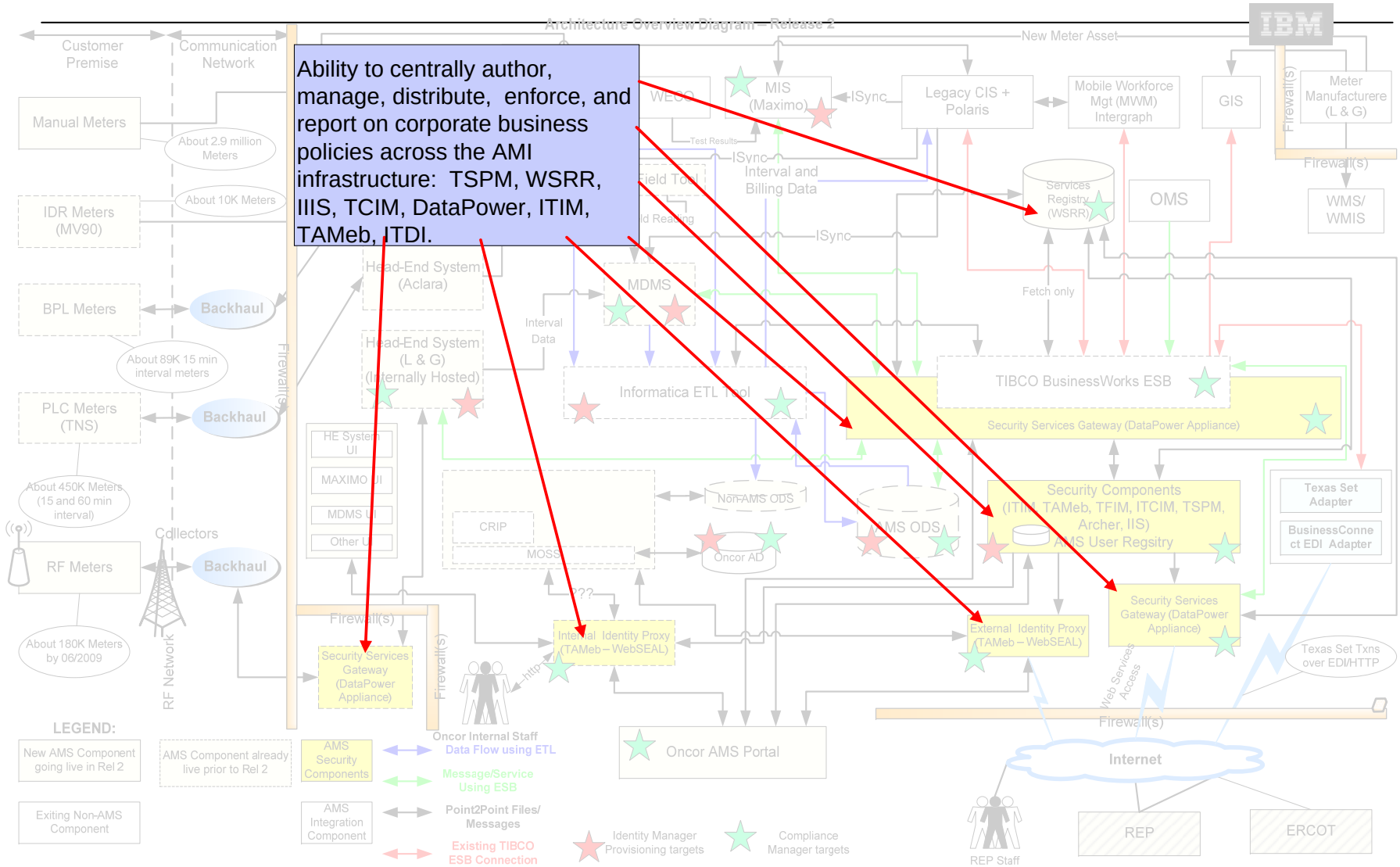
Information Gathering	▪ Review environment ▪ Types of systems ▪ Timing requirements ▪ Locations ▪ Security requirements
Network Analysis	▪ Gain understanding of network architecture and systems in place ▪ Identify security issues related to the network architecture ▪ Identify security issues based on observed network components and network traffic
Network Vulnerability Analysis	▪ Identify interconnections with other networks – Intranets, wireless, dialup ▪ Identify vulnerabilities in devices ▪ Identify vulnerabilities in applications
System Vulnerability Analysis	▪ Identify vulnerabilities in devices ▪ Identify system configuration and procedural vulnerabilities such as weak passwords, virus protection, patch management, system logging, etc.
Application Vulnerability Analysis	▪ Identify vulnerabilities in SCADA application components
Vulnerability Identification/Validation	▪ Review all data from automated tools and, where possible, check systems to verify identified vulnerabilities

⑥安全防护体系的测试

- 开发安全测试计划
  - 漏洞测试
  - 应用漏洞评估
  - 网络测试
  - 模块级测试
  - 应用源代码的审查
  - 物理安全测试
- 鉴定漏洞测试之后的行为
- 开发可纠正计划
- 执行

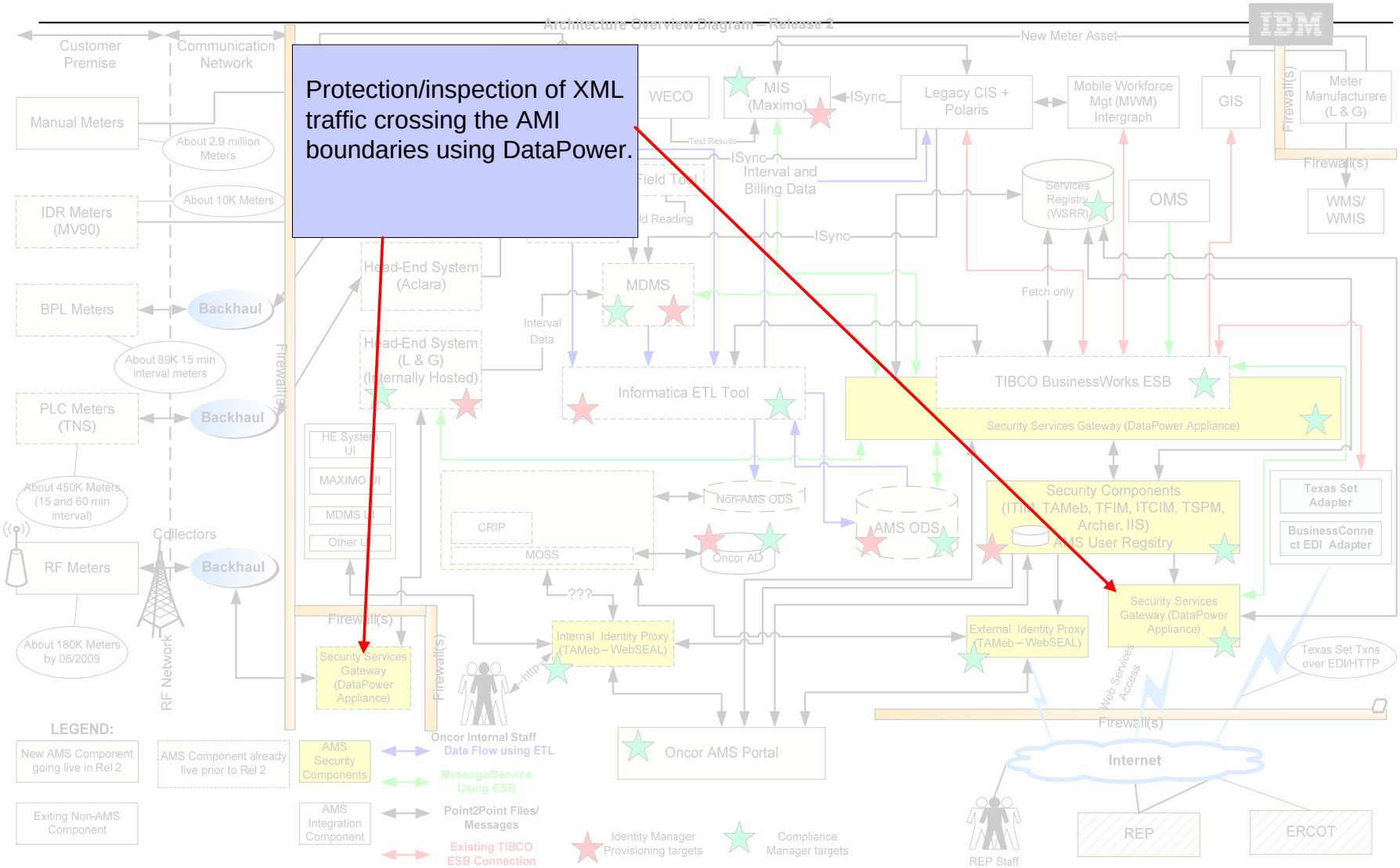
火龙果 · 整理
uml.org.cn

AMI 安全技术方案设计#1 – Policies & Compliance



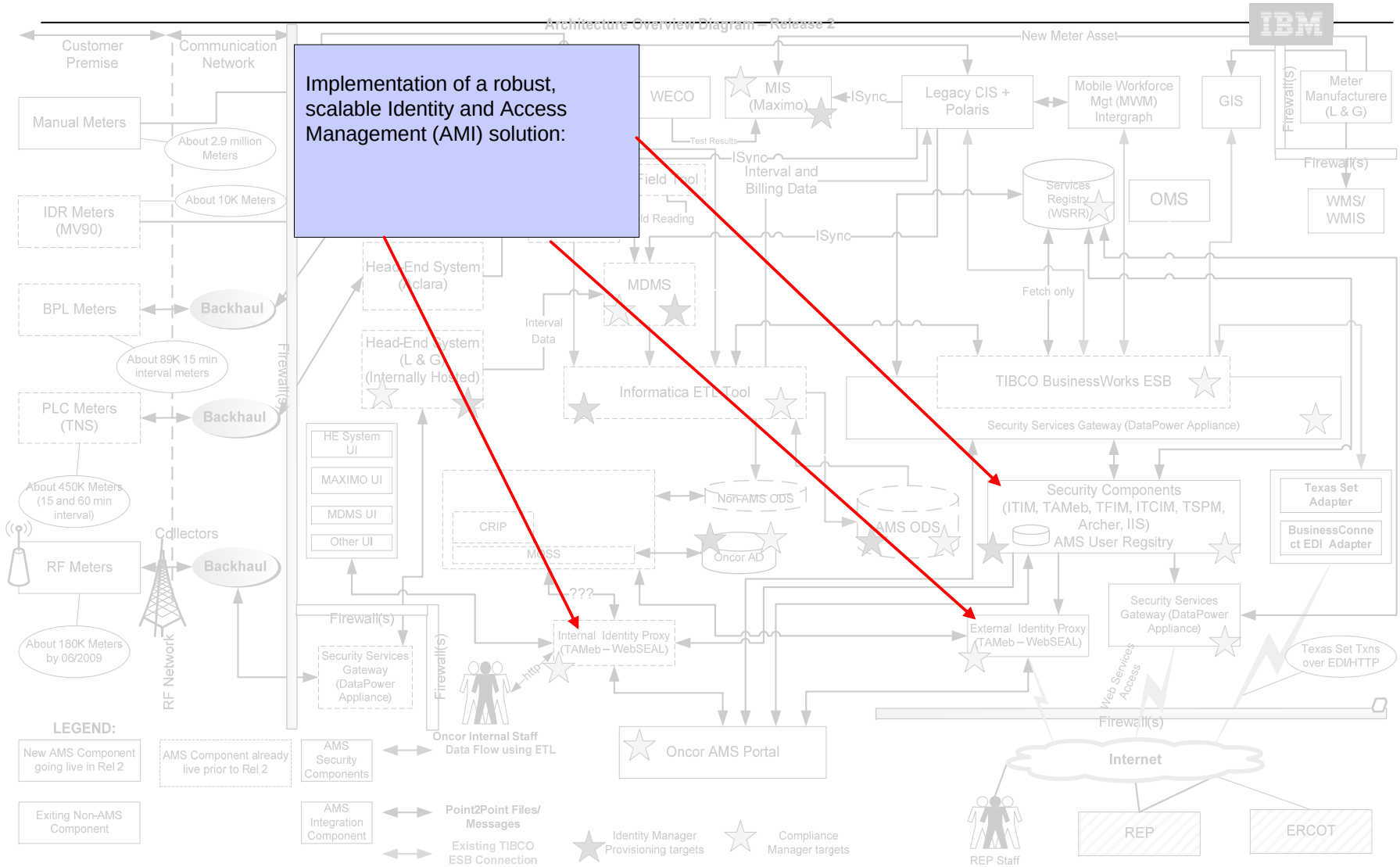
火龙果 · 整理
uml.org.cn

AMI 安全技术方案设计#2 - Messaging



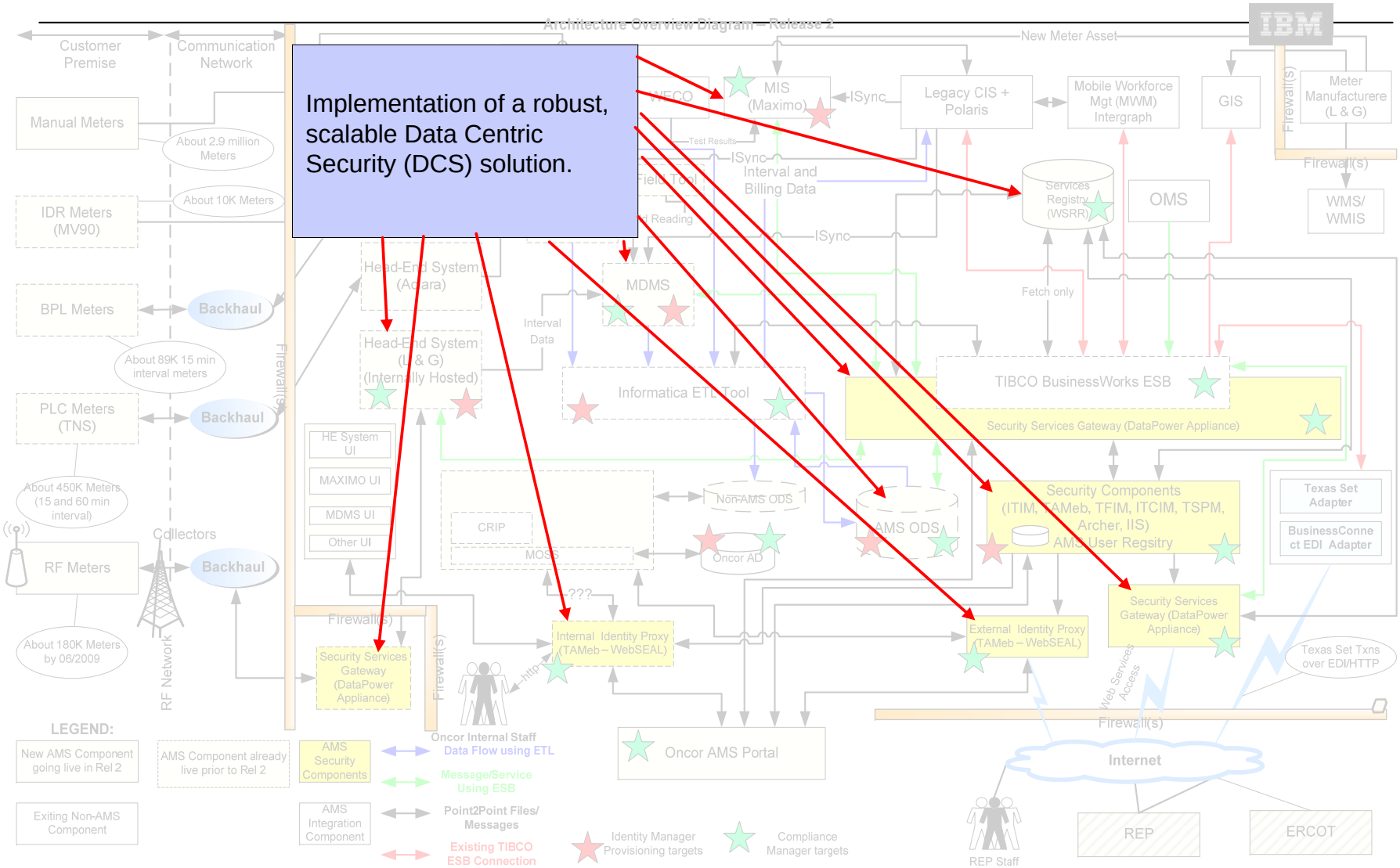
火龙果 · 整理
uml.org.cn

AMI 安全技术方案设计#3 – Identity & Access Management



火龙果 · 整理
uml.org.cn

AMI 安全技术方案设计#4 – Data Centric Security



AMI 安全防护建议汇总

The AMI space as a whole is relatively immature and as a result comprehensive security standards have yet to be developed and accepted security methods embraced by the AMI product vendors. As these standards continue to evolve and mature, there may be a need to expand or contract the overall security solution to accommodate new, and perhaps unknown requirements.

Potential Future Changes

Expansion/Contraction of the AMI Security Solution

- XML interrogation and protection
- Removal of the need for XML protection crossing some AMI boundaries
- Scaling the Identity Management (IdM) system to accommodate end customers
- Expanding the security infrastructure beyond AMI specific resources
- Assist in building Federations with business partners, based on open standards such as SAML, Liberty, WS Federation
- Expand user authentication to the new technologies such as Microsoft Card Space and Open Source Info Card.

火龙果 · 整理
uml.org.cn

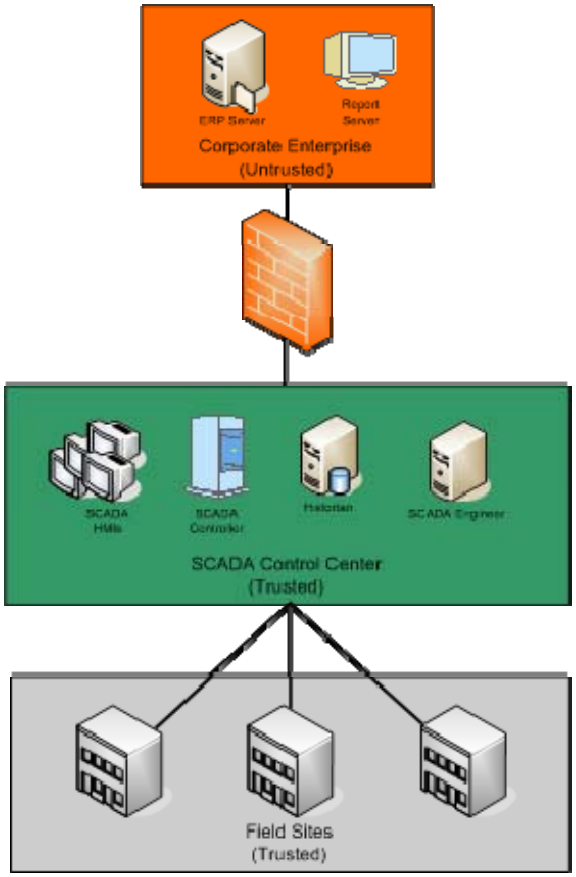
SCADA安全防护建议

Supervisory Control and Data Acquisition (SCADA) Network Security Considerations

火龙果 · 整理
uml.org.cn

SCADA 技术部件构成

- Field Devices
  - RTU – Remote Terminal Unit
  - PLC – Programmable Logic Controller
  - IED – Integrated Electronic Device
  - PAC – Programmable Automation Controller
- Fieldbus Protocols
  - Modbus
  - DNP3
  - DeviceNet
- SCADA Control Center
  - HMI – Human Machine Interface
  - SCADA Controller – Real time processing
  - Historian – database of events
  - Control Center Protocols
    - OPC
    - ICCP – Inter Control Center Protocol
- Communication Technologies
  - Serial connections (hardwire & dial-up)
  - Ethernet & TCP/IP / Wireless
  - RF & Microwave
  - Cell: CDMA



火龙果·整理
uml.org.cn

已经出现的安全事件

Since 2000, there has been a 10-fold increase in the number of successful cyber attacks against SCADA systems at power generation, petroleum production and nuclear plants and water treatment facilities.

- Pennsylvania Water Treatment Plant
  - A hacker exploited employee laptops, tunneling into the network through remote access applications
  - The hacker installed a virus and spyware and ultimately used the plant's computer system to distribute emails and pirated software
- Australian Sewage Release
  - Utilized unsecured wireless communications to regain access to the system after quitting his job
- California System Operator Hack
  - Attackers, possibly from China, gained access to one of the computer networks that has hierarchical control over a number of PCS networks

SCADA面临的安全威胁

- Directed Threats
  - Industrial Sabotage
    - Disgruntled employees
    - Competing vendors
  - Coordinated Terrorist Threat
    - Physical + Cyber Attack
  - Internal and External Hackers
- Indirect Threats
  - Operator Error
    - Minor human errors can have disastrous effects
  - Viruses

导致SCADA不安全的因素

1. Ran on proprietary hardware using proprietary protocols
   - Initially designed to maximize functionality, with little attention paid to security
   - Physical security the most important aspect
2. Migrated to standard operating systems (Windows/Unix)
   - Windows is now the primary platform for SCADA vendors
3. Migrated to standard networking protocols (IP)
   - Opens SCADA systems up to well known, existing exploits
   - Eliminates need to learn proprietary techniques
4. Tried to improve efficiencies by connecting their corp systems (ie billing) directly to their PCS networks
   - Opens critical SCADA systems to external attackers

火龙果·整理
uml.org.cn

需要从不同层面考虑SCADA系统面临的安全问题（Must Be Approached with Different Mindset）

- **Availability/reliability** of systems most important security aspect for SCADA
- Availability and Integrity concerns due to:
  - Sparse networks, spreading over large geographic regions
  - Termination by sensors of limited intelligence rather than general-purpose workstations
  - Components often communicate to the master station on a report-by-exception basis, or a polled basis, rather than as peers
  - No data authentication
  - Human security presence is not possible at all sensor sites

最需要关注的安全问题

- IBM's Perspective
  - Weak protocols leave systems vulnerable
  - Standardized technologies make systems more vulnerable
    - Patches may not be able to be applied
    - No OS Hardening of the devices leaves them open to standard hacking attacks
  - Insufficient network segmentation does not provide protection within the SCADA trusted network
    - Almost all communication is deemed "trusted" and unencrypted
  - Limited security logging, and almost no protection systems
  - Limited cyber security policies exist for SCADA, and users are not trained on the risks

火龙果·整理
uml.org.cn

建议的方法-Phase 1: Establish

- Network segmentation an easy first step
  - Utilize DMZs to isolate networks of different trust levels
    - Never allow traffic from trusted network directly to/from the untrusted networks
    - Support vendor access on separate DMZ
    - Deny all, only allow what is explicitly allowed
    - Utilize FW logs to watch for malicious traffic
  - Intrusion Prevention Systems (IPS) provides lots of advantages for internal segmentation
    - Layer 2 bridging does not require changes in IP addresses
    - Fails open at the hardware layer to ensure network availability
    - Can add real-time protection for known attacks/virus before they spread

火龙果·整理
uml.org.cn

建议的方法- Phase 1: Establish

- Implement existing best practice technologies
  - Harden OS to minimize attack vectors
    - Disable unnecessary ports
    - Ensure strong authentication
      - Microsoft Active Directory (with SCADA Application Integration)
      - Utilize smart cards for physical and logical access
      - Minimize shared accounts/weak passwords
    - Develop an appropriate patch process
      - Vendor acceptance
      - Internal testing
      - Phased rollout (HMIs -> SCADA Servers)
  - Utilize A/V systems on Windows platforms
    - Vendor approval
    - Real-time checks without system scans
    - Automate A/V updates to less critical systems (HMI), manual updates on critical servers

火龙果·整理
uml.org.cn

建议的方法- Phase 1: Establish

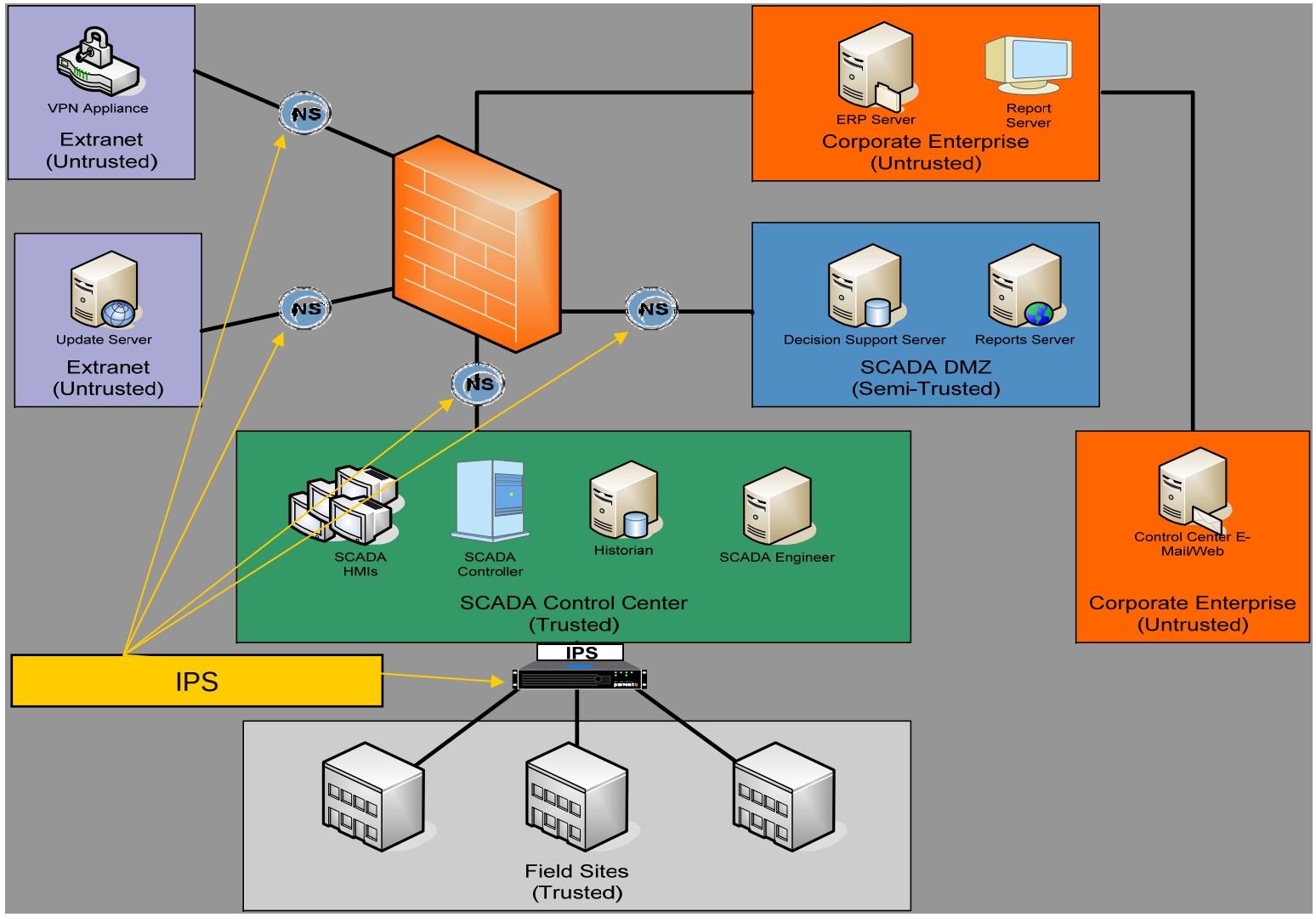
- IPS can be used to provide additional layers of security
  - Virtual Patch Concept
    - IPS will block malicious traffic from attacks for patches that can't be applied
      - Simulation mode can identify malicious traffic without blocking
    - Provide a window of time to test and apply vendor patches
  - IPS can be used to detect malicious traffic on multiple segments
    - Provide protection for remote access points
    - Provide application level protection for traffic that is authorized by the firewall
    - Real-time alerting provides additional levels of logging
- Utilize all levels of logging for incident analysis
  - Firewall and router logs
  - OS level logging for user level activity
  - SCADA application logs for abnormal activity

火龙果·整理
uml.org.cn

建议的方法- Phase 1: Establish

- Outsource areas not part of your core skill set
  - Managed Security Service Providers
    - Can be done without compromising trust of SCADA network
    - Can provide correlation of multiple layers of security
      - Firewall
      - IDS
      - IPS
  - Development of the SCADA Data Dictionary
    - A tool that normalizes events from SCADA/DCS application logs
    - Allows a MSS provider to tie the patterns to a common set of security events
    - Integrates documentation for each event

建议的 SCADA 系统架构



建议的方法- Phase 2: Educate

- Raise security awareness internally and with third-party vendors
  - End-users are the weakest link
- Reiterate importance of policies to employees
- Utilize OS hardening procedures to ensure vulnerabilities are not reintroduced into the environment

建议的方法- Phase 3: Enforce

- Utilize automated scanning software to maintain system compliance
  - Work in coordination with SCADA engineers
  - Heavier scans on less critical systems
  - Leverage redundancy to ensure no system down time
- Conduct reoccurring security assessments
  - External and internal
  - Network and application levels
  - Use results to constantly reevaluate risk assessment goals

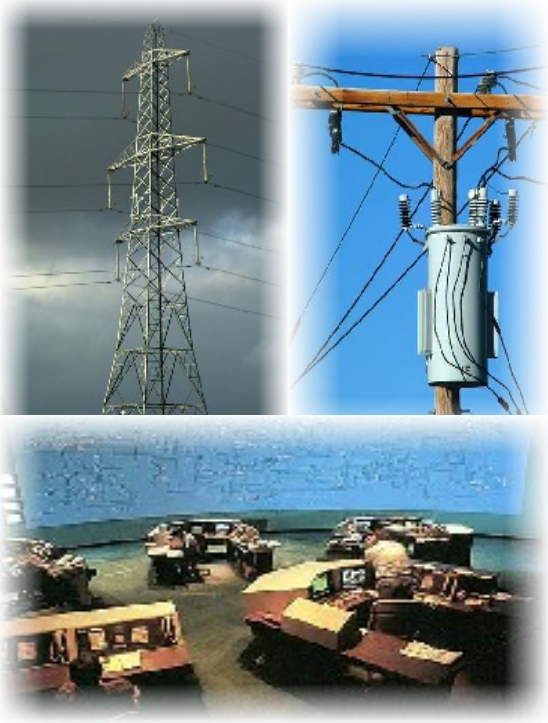
建议的方法- Phase 4: Evaluate

- Audit processes to ensure compliance
  - Ensure continued compliance with government regulations
- Measure return-on-investment

火龙果 · 整理
uml.org.cn

SCADA安全防护经验分享

- Conducted comprehensive SCADA Security Risk Assessments for a variety of companies
  - Both national and international experience
    - Completed 15-20 unique security assessments over the last 5 years
    - 2 year project assessing the largest electrical power utility in America
- Unmatched Assessment, and Remediation experience in all aspects of the industry including:
  - Transmission and Distribution Systems
  - Nuclear, Fossil, and Hydro Generation Plants
  - Nuclear Reactor Protection and Industry Control Systems (ICS)
  - Several Types of Distributed Control Systems (DCS), Energy Management System (EMS), SCADA, and Process Control Systems
  - Hydro-automation Systems
  - Physical Security Systems
  - Data and Telecommunications Networks
- Integrated SCADA protocol specific IDS/IPS signatures
  - DNP3 & Modbus
- **Certified SCADA Security Architects**

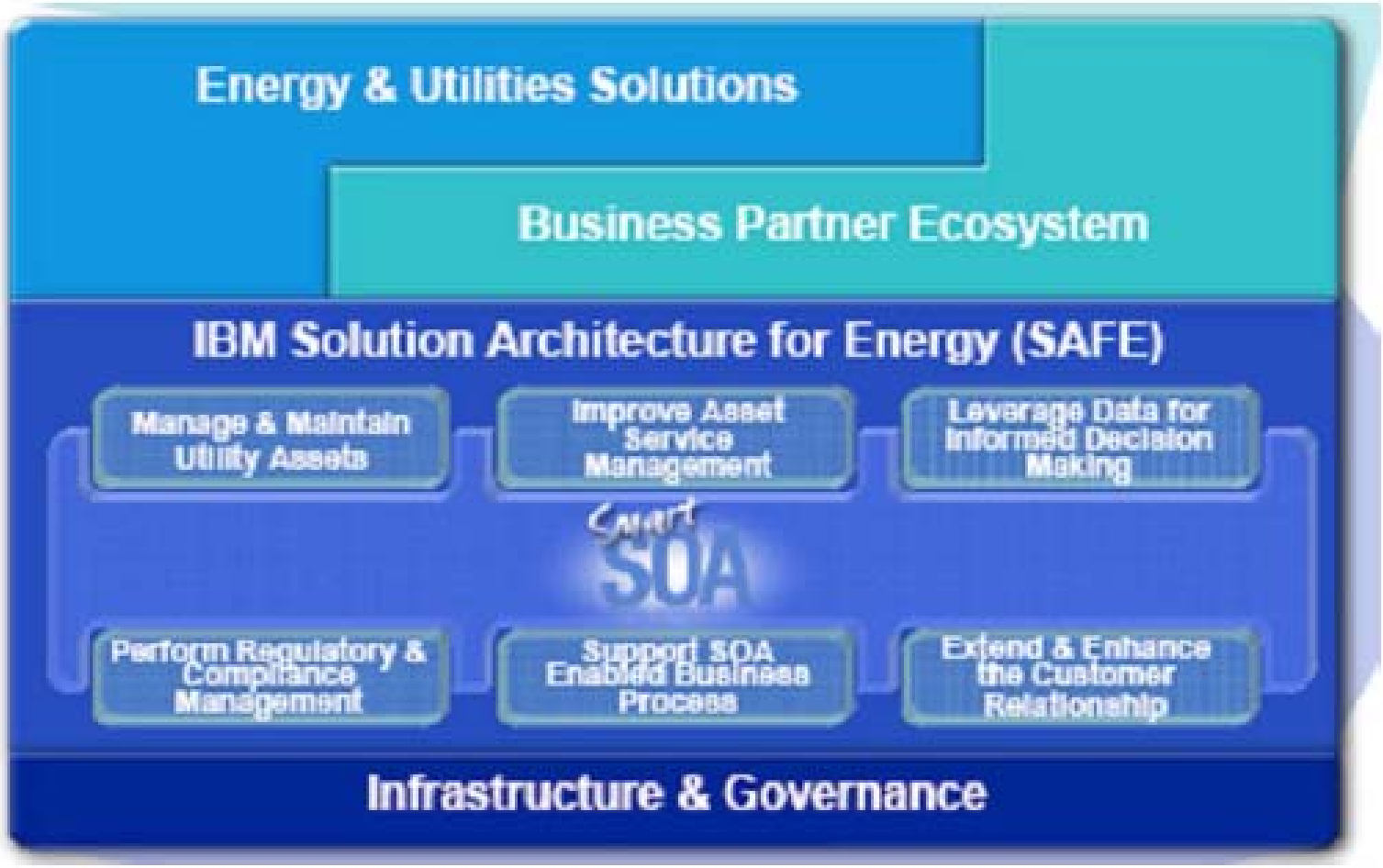


火龙果 · 整理
uml.org.cn

Solution Architecture for Energy (SAFE) Security Considerations

火龙果 · 整理
uml.org.cn

IBM Solution Architecture for Energy (SAFE)



火龙果 · 整理
uml.org.cn

SAFE Highlights

- Based on Service-Oriented Architecture (SOA) that allows the utility to build and extend new services to customers easily and cost effectively through the efficient flow of information across the enterprise.
- Provides business applications and services securely interoperating with business partners, suppliers, regulators and utility customers, keeping in mind the confidentiality, integrity and accountability and privacy of data exchanged.
- The security design and operational mechanisms allow for centralized identity, access, policy and entitlement management.
- The solution includes security event handling and compliance management systems.

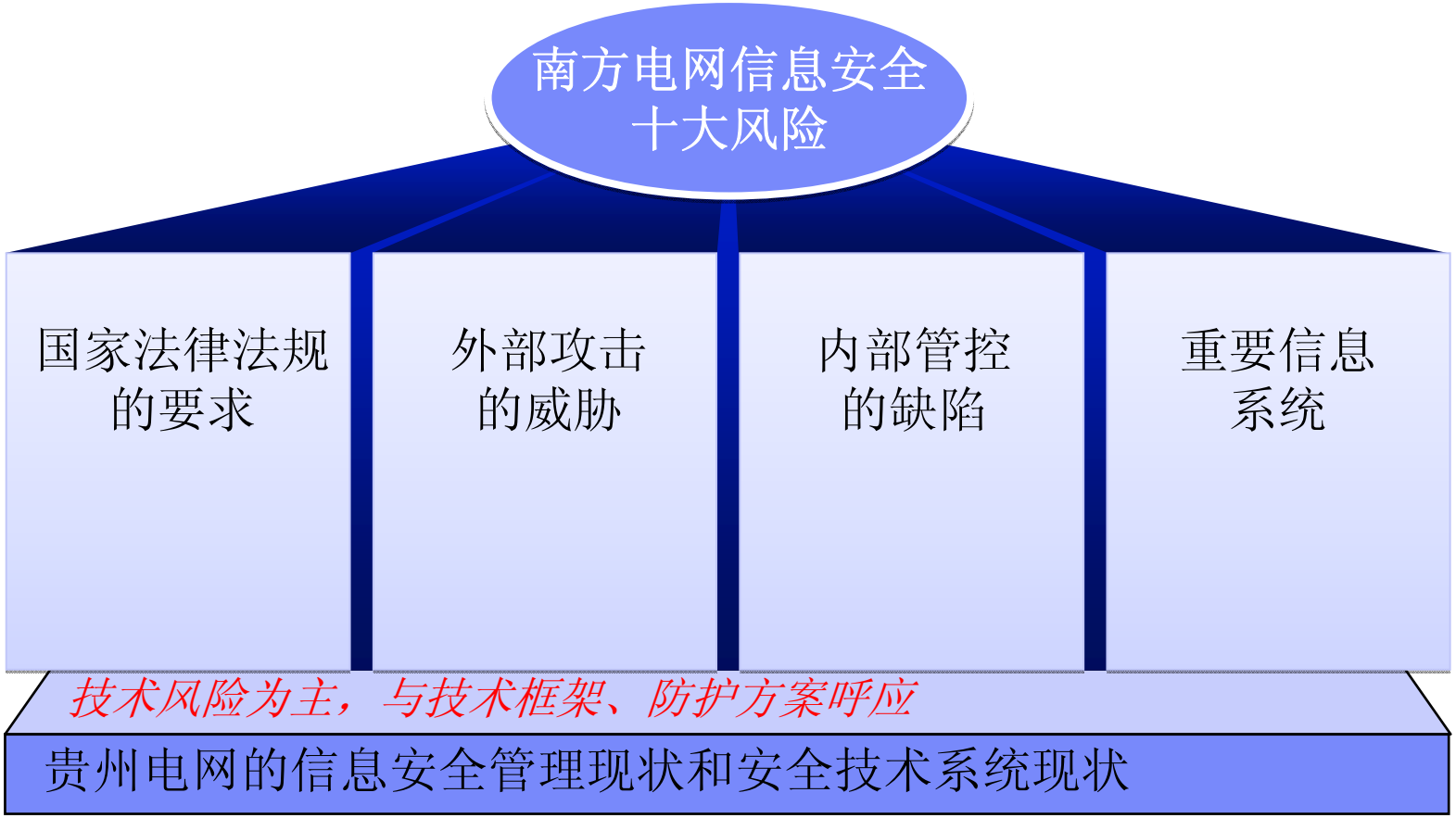
火龙果·整理
uml.org.cn

主要内容

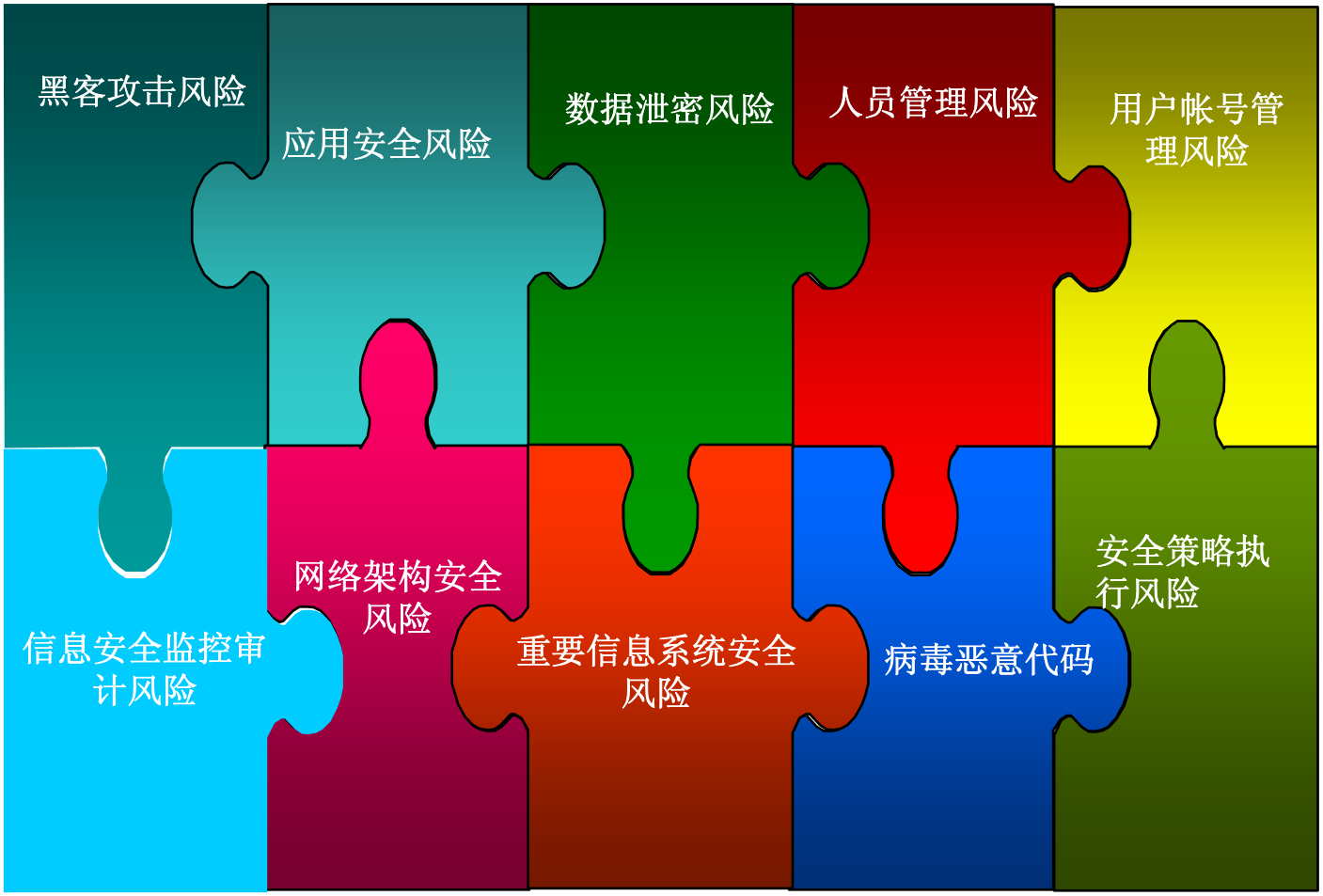
- 电网安全威胁分析
- 智能电网安全防护方案
- 南网十大安全风险与防护方案

火龙果·整理
uml.org.cn

南方电网信息安全十大风险－背景与思路



南方电网信息安全十大风险



火龙果·整理
uml.org.cn

南方电网信息安全十大风险报告架构

十大风险概述

序号	风险名称	风险描述	风险分析	应对策略与效果
1	黑客攻击风险	✓黑客危害包括：企业形象损失，机密信息泄漏，服务中断，财务损失，业务系统被非授权控制等	✓缺乏有效的安全保护措施 ✓缺乏有效的运维与监控措施 ✓人员的安全意识不足	✓建立完善的安全技术体系 ✓建立各种有效的监控审计系统 ✓对内部人员进行安全意识培训，与内部人员、第三方签订保密协议 ✓建立有效的灾备系统
2	应用安全风险	✓信息安全攻击大都发生在 Web 应用层面上，大多数的 Web 站点都存在漏洞，易受攻击 ✓电监会、南方电网总部和其他安全测评机构组织的数次安全评估中发现应用系统存在造成严重危害的安全问题	✓没有对应用系统开发进行约束和规范 ✓缺乏代码缺陷的检查工具和专业人才 ✓运维阶段缺乏持续的应用安全检测加固防护手段	✓建立应用安全管理规范 ✓采用应用安全防护技术，通过 Web 应用防火墙实现在线防护，通过应用安全评估系统帮助检查代码安全隐患 ✓培养内部应用安全评估人员 ✓加强对应用安全的考核要求
3	数据泄密风险	✓数据泄密造成的损失难以估量 ✓数据泄密事件在各行各业频繁发生	✓存储介质管理不善或维修失密 ✓内部人员无意泄密 ✓内部人员有意（恶意）泄密 ✓内部文档权限失控失密 ✓对外信息发布失控失密	✓梳理敏感数据，并做好敏感数据的存储和传输加密 ✓加强员工信息安全保密意识 ✓加强控制和审计移动存储介质的使用 ✓加强网络准入管理工作 ✓建立健全网络行为监控系统

十大风险详述

2 南方电网信息安全 10 大风险详述

- 2.1 黑客攻击风险
  - 2.1.1 风险描述
  - 2.1.2 风险分析
  - 2.1.3 应对策略与效果
- 2.2 应用安全风险
  - 2.2.1 风险描述
  - 2.2.2 风险分析
  - 2.2.3 应对策略和效果
- 2.3 数据泄密风险
  - 2.3.1 风险描述
  - 2.3.2 风险分析
  - 2.3.3 应对策略和效果
- 2.4 人员管理风险
  - 2.4.1 风险描述
  - 2.4.2 风险分析
  - 2.4.3 应对策略和效果

十大风险—— 数据泄密风险

- 数据泄密造成的损失难以估量
- 数据泄密事件在各行各业频繁发生

风险分析

- 存储介质管理不善或维修失密
- 内部人员无意泄密
- 内部人员有意（恶意）泄密
- 内部文档权限失控失密
- 对外信息发布失控失密

应对策略与效果

- ✓ 梳理敏感数据，并做好敏感数据的存储和传输加密
- ✓ 加强员工信息安全保密意识
- ✓ 加强控制和审计移动存储介质的使用
- ✓ 加强网络准入管理工作
- ✓ 建立健全网络行为监控系统

53

案例1：企业数据泄密经典案例分导—— 富士康PK比亚迪

案例背景

2006年6月，富士康在国内起诉比亚迪侵犯商业秘密，索赔500万。
2007年6月富士康在香港起诉比亚迪，索赔650万。
同年10月，富士康变更当事人后重新起诉。
07年12月，北京市高级人民法院鉴定，比亚迪获取的相关文件，确有大量文件构成非公知信息，能给企业带来经济价值。富士康新闻发言人童文欣当时对结果满意。
在比亚迪被起诉的过程中，比亚迪一直在进行手机业务的分拆上市工作，并在07年底上市。
07年的财报显示，比亚迪手机整机代工的比例为33%，元件为67%，整机代工同比增长3400%。

2008年9月，巴菲特附属公司战略入股比亚迪，用18亿港元收购比亚迪总股本的10%。
08年财报显示，两家公司都受到环境影响利润下滑。富士康利润同比下滑83.22%至1.21亿美元，而比亚迪也下滑了三成为7.65亿元，但其手机整机代工业务占比上升超过四成。
比亚迪电子在2008年财报中表示，针对富士康2007年提起的诉讼，比亚迪在2008年6月申请搁置法律程序，但该申请被驳回。比亚迪表示正在就判决寻求法律意见。这也是比亚迪对整个诉讼案件最后的对外意见。
在前不久举行的富士康股东会上，董事长陈伟良表示，比亚迪是一间与深圳政府有密切关系的公司，令诉讼处理的速度有被拖缓之嫌。现时富士康已在香港提起民事提出诉讼，法院已受理案件，希望下半年可以正式开审。
2009年4月，巴菲特接受美国《财富》杂志访问时，盛赞比亚迪总裁王传福是“爱迪生与杰克·韦尔奇的综合体”。
2009年5月，鸿海集团总裁郭台铭炮轰巴菲特，认为巴菲特不应投资偷窃商业机密的比亚迪。
之后，说服巴菲特投资的Hathaway副董事长芒格表示，他对比亚迪公司和领导人王传福毫无疑虑。。。。。

案例1：分析

富士康科技集团

富铭字【2008】016号

尊敬的贾庆林主席：

您好！

富士康科技集团虽然是最大的台商，却是在大
在深圳开办的第一家企业不过百十来人，如今已扩
达700多亿美元。可以说，没有中国政府对台商企
的今天。对此，台铭时刻铭记在心，并一直努力通
一。如今，国民党在台湾选举中已大获全胜，这为
合作创造了条件，台铭对此甚感欣慰。

但令人遗憾的是，富士康在大陆也受到了不公
限公司侵犯商业秘密一案未能得到公正处理。

富士康生产手机的商业秘密，是经过多年摸索
其核心技术是花费4100万美元购买的，成本之大
士康的商业秘密进行手机生产。由于不费分文，因
订单，几年来给富士康造成了数十亿元的经济损失
比亚迪涉嫌侵犯商业秘密罪，此案被称为中国知识

1/2

富士康科技集团

富字【2008】054号

尊敬的陈云林主任：

您好！现将我司控告比亚迪单位犯罪进展情况汇报如下，望予以帮助。

深圳市公安局宝安分局于3月12日决定立案侦查比亚迪涉嫌侵犯商业秘密后，我司于17日要求该局立即拘留犯罪嫌疑人王传福、夏佐全。18日晚，深圳市公安局通知我司决定拘留夏佐全，但同时表示按现有证据、依法律规定，离拘留还有一定距离。只是考虑到案件的重要性，才决定拘留夏佐全。王传福与夏佐全不在一个层次上，还不能拘留。

我司认为深圳市公安局意见错误，遂致函李锋书记予以反驳。考虑到深圳市政府，特别是贵办都有希望双方和解的意愿，我司在函中同时指出，如果4月1日前王传福承认侵犯商业秘密的事实，向我司道歉并愿意赔偿，我司保证在达成和解协议后撤销一切刑事控告和民事诉讼（见附件一）。令人遗憾的是，比亚迪至今仍认为其没有侵权。

我司认为，比亚迪的态度在很大程度上取决于深圳市公安局的态度。在深圳市公安局认为王传福不是犯罪嫌疑人，尤其是不认真收集证据的情况下，比亚迪是不可能认错的。而要转变深圳市公安局的观

1/2

练习

1、分组通过网络搜索本事件的相关报道或分析，归纳还原事件真相

2、分组讨论该案例中企业隐私所包含的内容与启示

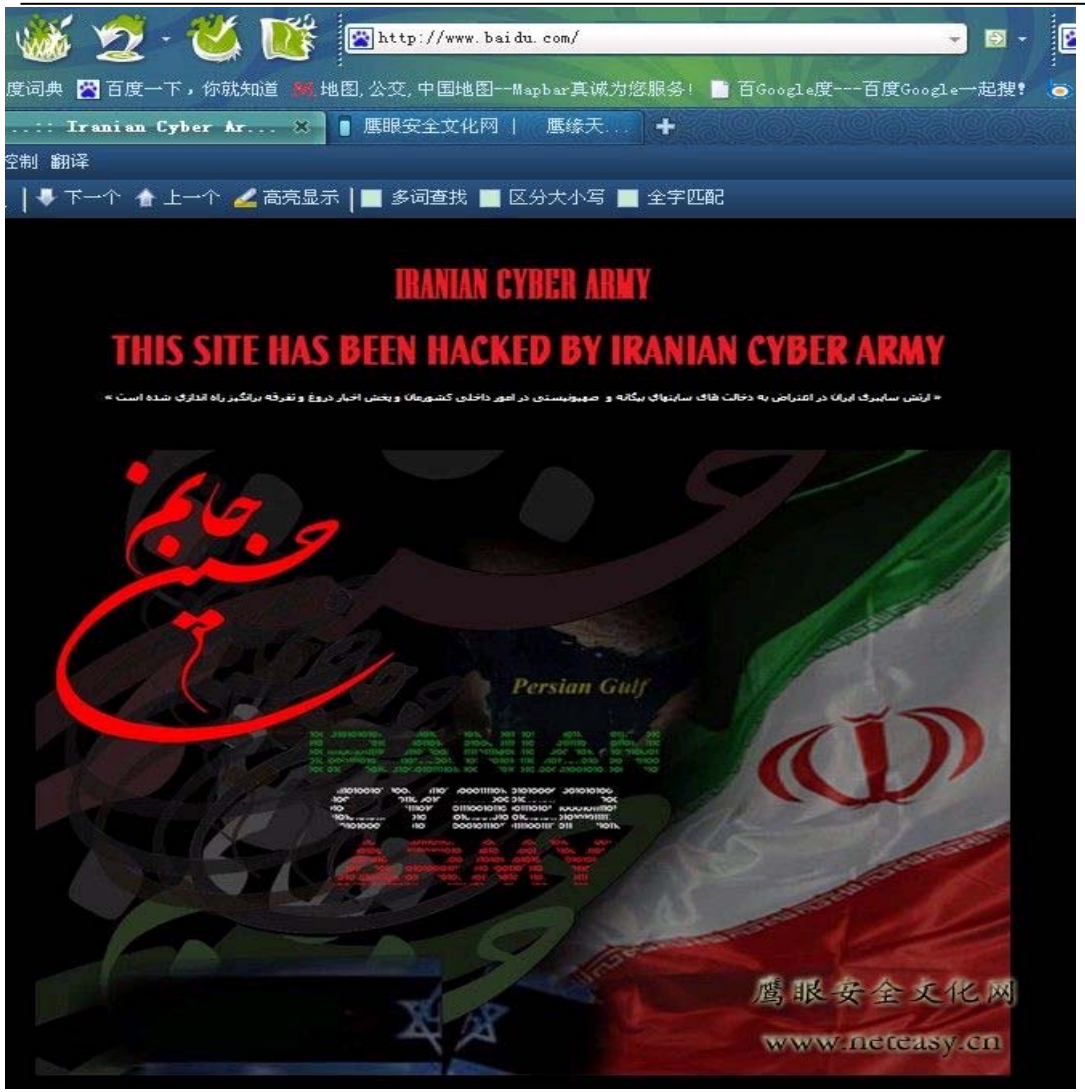
案例2：企业数据安全-营销黑白道

- 美国迪士尼乐园的每一位游客都拥有一个以自己为主角的“剧组”，在客人到达时，甚至在到达以前，他的“剧情”就已经安排好了。“剧组成员”就会根据客人的需求，通过各种预订渠道帮客人安排行程：就餐、打高尔夫、参观主题公园以及每一项具体活动。“把客人的信息，如姓名、到达日期等输入客户管理系统数据库，然后据此建立针对不同客户而定制的欢迎信，以及行程单。”迪士尼乐园的管理者意识到，成千上万的游客来到迪士尼乐园，目的是为了获得一场“终极体验”，因而，迪士尼乐园的首要目标是让游客梦想成真，并且吸引他们成为回头客。

- 全球著名的客户沟通管理解决方案供应商Group1Software进入中国后，即与上海电信和深圳电信展开合作，推出个性化账单。每个用户拿到的话费账单都不相同，如果客户是女性，账单的色调就更加女性化；如果年龄较大，字号就明显大一些。这还不是全部，长话频繁的用户，账单上往往会出现更省钱的长话套餐广告；经常出差的用户，则会看到机票加套餐的广告，甚至是出差目的地的旅游资讯。

- 在美国，Group1Software的合作伙伴——美国运通卡原来单纯地通过账单发送的广告信息得到的平均响应率仅为0.24%，因为广告往往与接收者无关。而通过个性化账单账单发送的有针对性的营销信息平均响应率提高到0.93%，其中酒店对账单的广告响应率从0.02%跃升为0.57%，提高了2750%。 个性化账单的背后，有着一系列复杂的后台操作，个人信息与个人消费特征的匹配，之后再与企业的服务形成一一对应，这不是斥资千万就立即能实现，美国运通卡在此方面已经探索了10年之久。

案例3：隐私营销学的新趋势-社会工程学与互联网情报分析案例



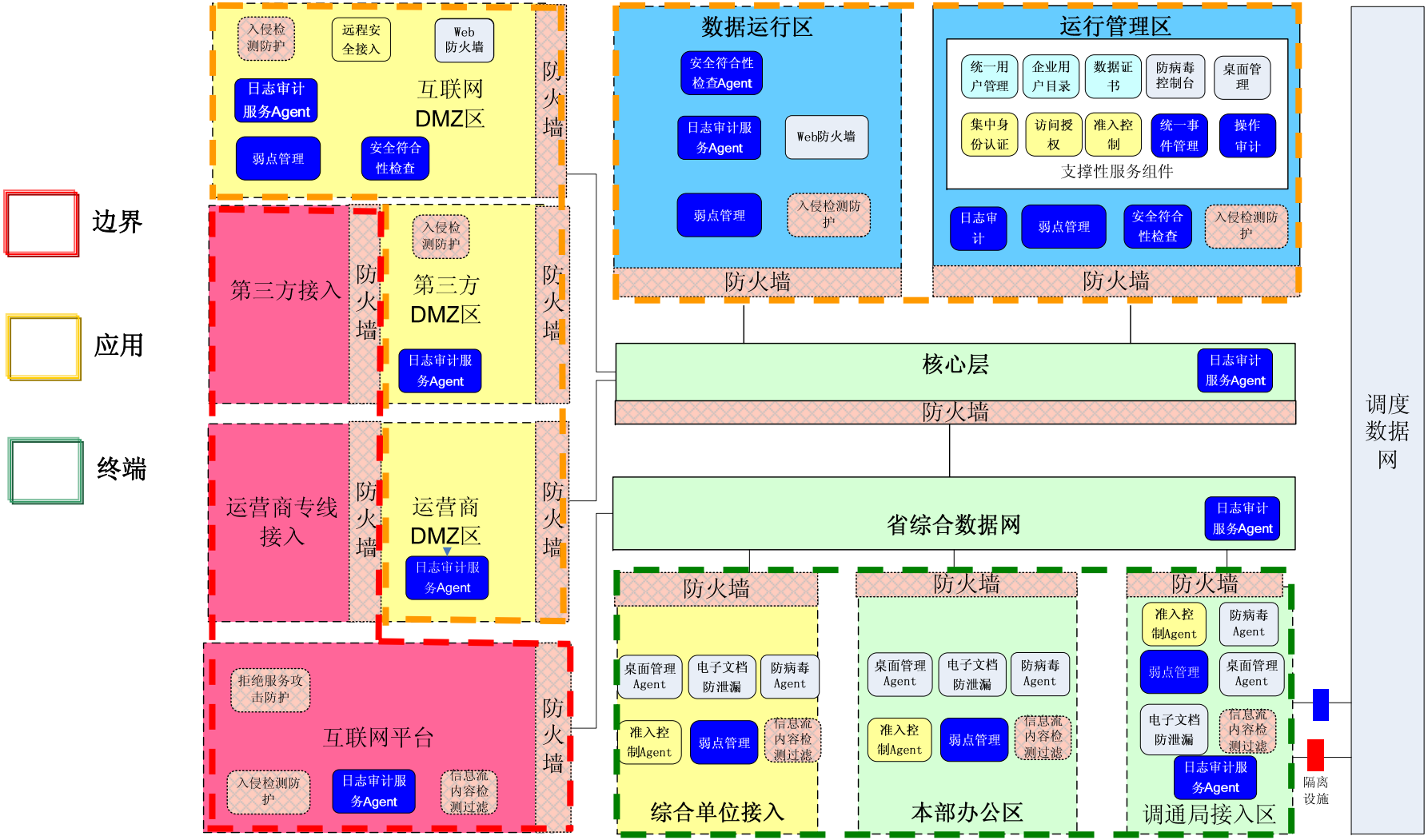
百度被黑真相与互联网社会工程学的分析练习：

背景：2010年1月12日上午6点左右起，全球最大中文搜索引擎百度突然出现大规模无法访问，主要表现为跳转到一雅虎出错页面、伊朗网军图片，出现“天外符号”等，范围涉及四川、福建、江苏、吉林、浙江、北京、广东等国内绝大部分省市。

这次百度大面积故障长达5个小时，也是百度2006年9月来最大一次严重断网事故，在国内外互联网界造成了重大影响

火龙果·整理
uml.org.cn

从三个方面着手南方电网的信息安全防护部署



火龙果·整理
uml.org.cn

南方电网信息安全防护部署设计原则

分区控制、整体预防
通过在各区域部署不同的安全组件，提高对整体的安全控制
全网的整体监控，及时监控任何区域发生的信息安全事件

分类保护、综合治理
通过对安全组件的部署，加强信息安全防护与控制
合理应用各种安全技术，使公司信息安全实现综合治理

管理集中化、部署标准化
规范的公司信息安全技术体系，为公司及下属各单位的信息安全防护提供指导

各单位的信息安全防护建设必须达到安全基线要求，
并按照基线管理办法强制管理。

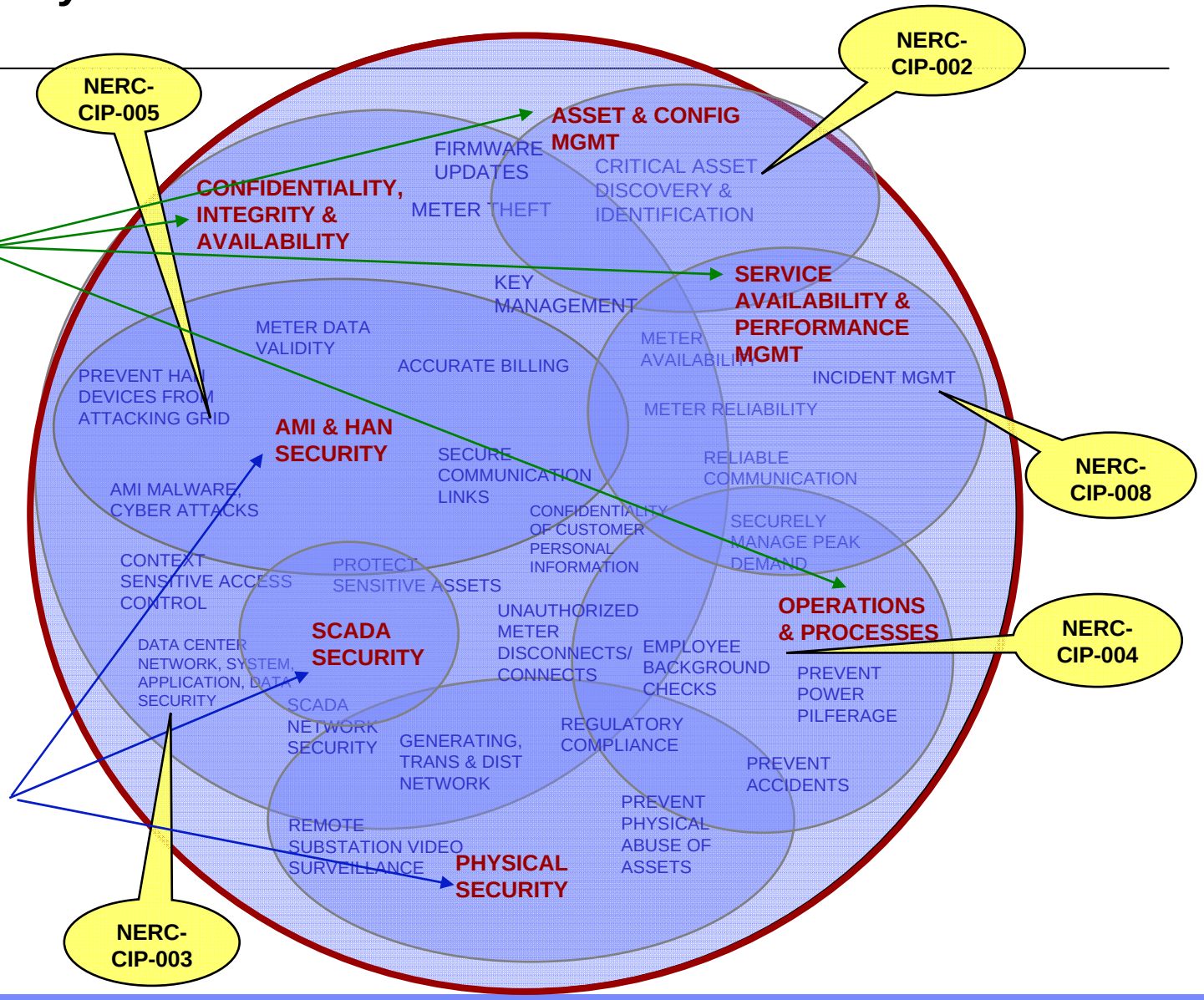
59

火龙果 · 整理
uml.org.cn

End to End Security involves lots of interlocks*

IBM has proven strengths in traditional IT security and service management …

…and is extending these strengths in integrating with Smart Grid devices and partner offerings



* Not all intersections and NERC-CIP directives shown

IBM在电力行业安全优化方面有独特的优势

- IBM是唯一拥有完整、综合信息安全解决方案的公司，包括有形安全和保密解决方案，以及符合电力行业要求的产品。
  - 能力范围涵盖所有层面，从安全芯片设计，到系统设计和开发，到安全和合规架构，到合规性验证，以及运行/建设/测试。
- IBM是唯一建立8个实验室，专门从事安全和保密产品研究与开发的公司，研究人员达15000人。
- IBM是同时拥有信息安全专家和电力行业专家的公司。IBM的电力行业专家拥有丰富的实践经验，熟悉电气设备的设计、制造、配送、运输到现场运行。
- IBM在信息安全、保密、合规方面是公认的世界领导者，仅2008年就获得超过4000项专利。
- IBM已经协助数百家公用事业公司、政府机构和其他管制行业管理最敏感、大型和复杂的安全和保密问题。
- IBM在信息安全、保密和合规领域有超过3000名经过培训、认证与经验丰富的从业人员。
- IBM是目前世界上唯一能在各个层次推动和提升电力公司信息安全能力的公司。事实上，IBM自身就是一个大范围、大规模的国际性公司，对信息安全有密集、先进和多样化的要求。

IBM广泛参与智能电网信息安全的政策和标准活动

- 15000名研究人员，开发人员和专家研究信息安全问题。
- 3000 +项安全与风险管理的专利。
- 2008年在信息安全方面的投入达15亿美元。
- 与公共/私营部门展开广泛合作。

Thank
You