

网络及信息安全技术研讨会

电力二次系统安全防护

李毅松

国家电力调度通信中心

2005-03-03 广西

提纲



一、概况

二、总体方案

三、安全管理

四、结语

GW

中国发电量和装机容量现居世界第二位

350

300

250

200

150

100

50

0

建国初期：发电量第25位

装机容量第21位

2002年 均已跃居第 2位

美

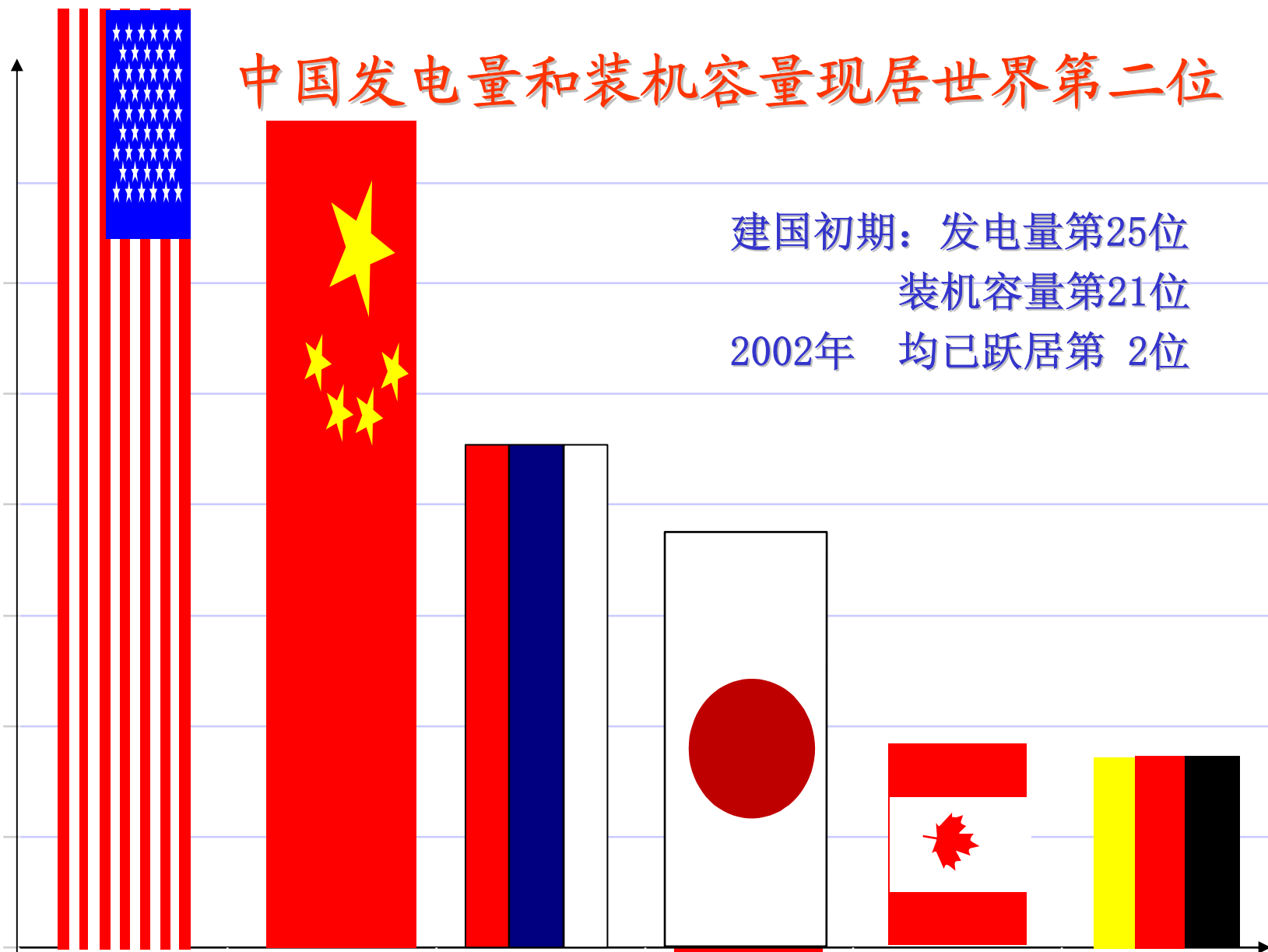
中

俄

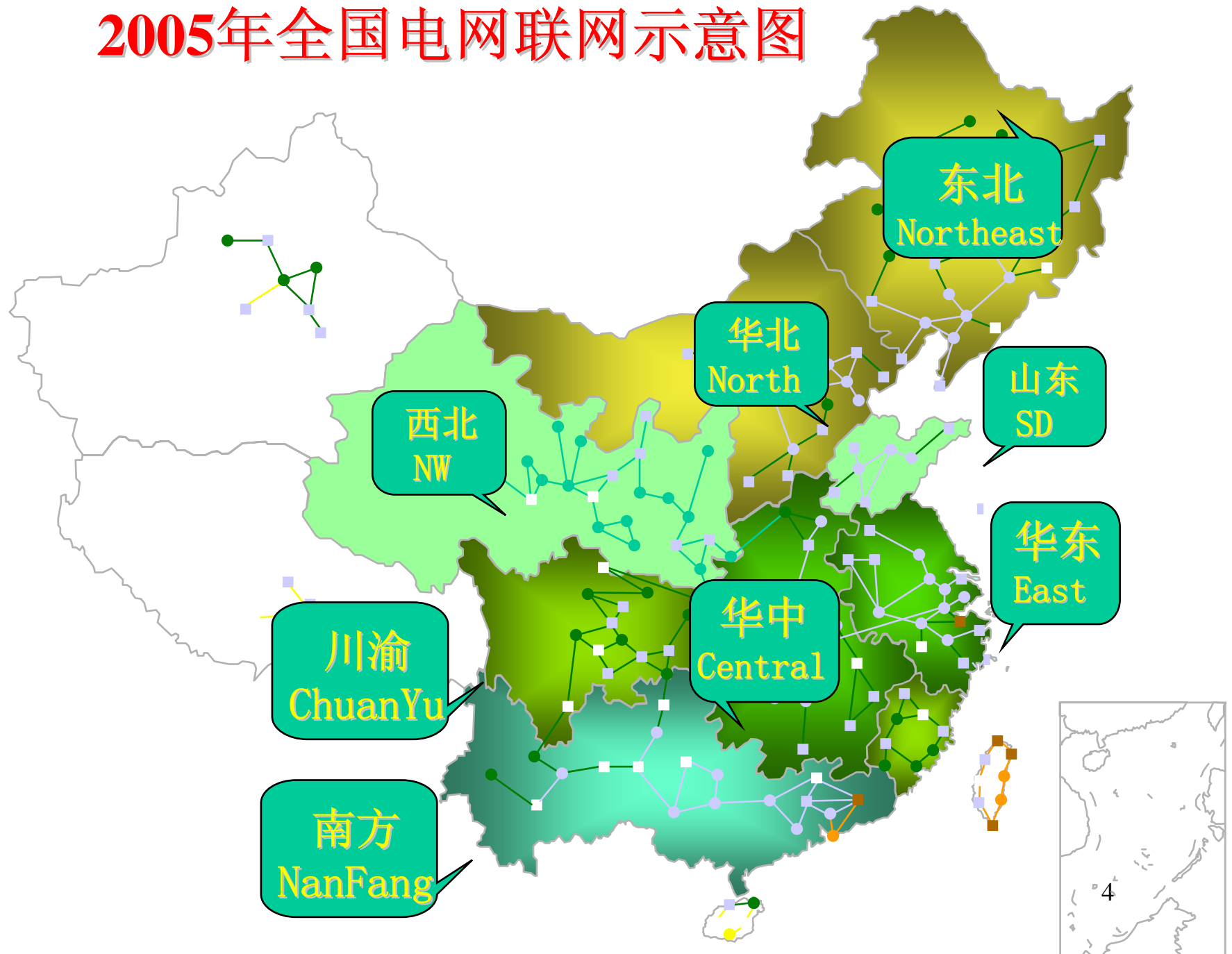
日

加

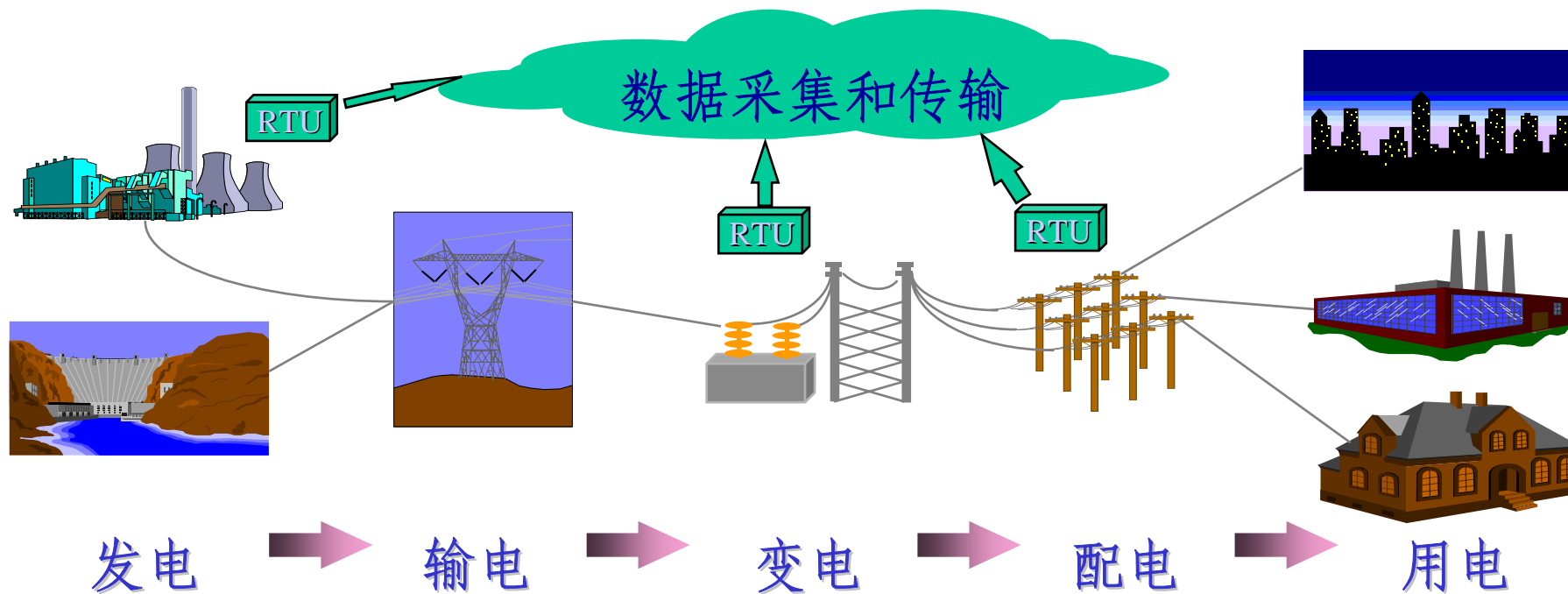
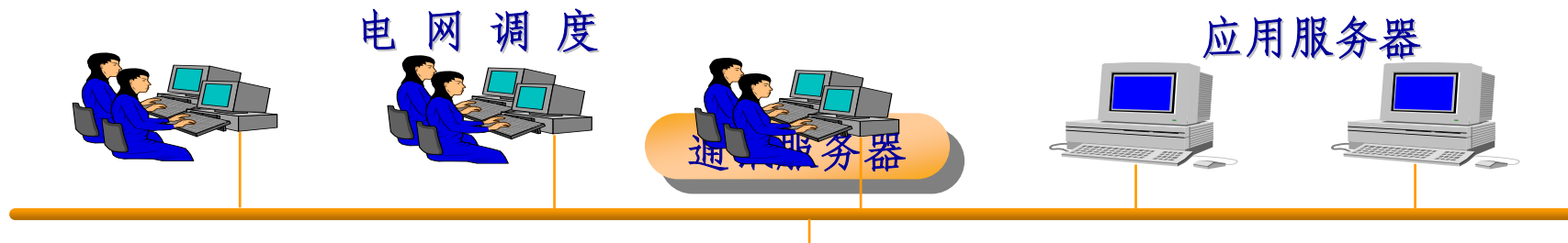
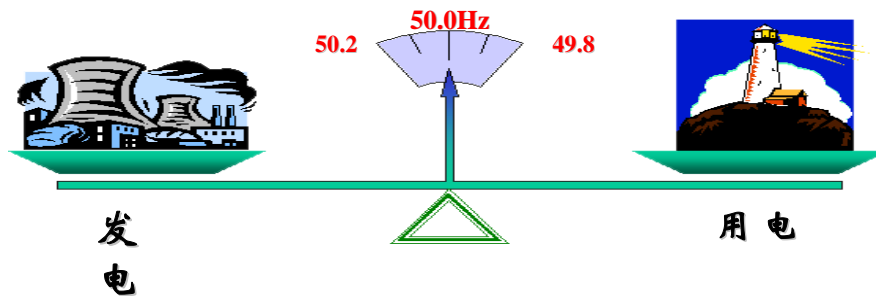
德



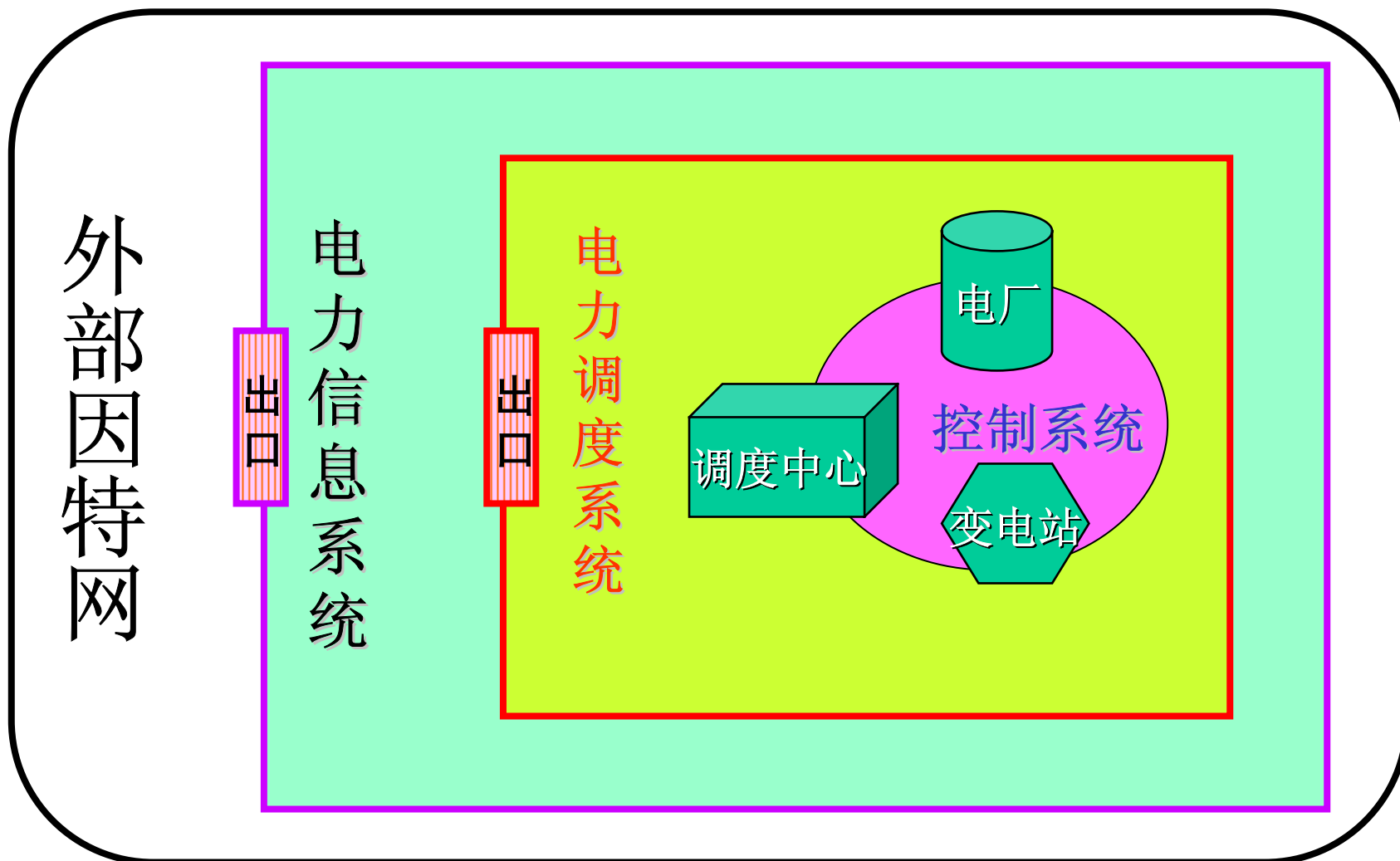
2005年全国电网联网示意图



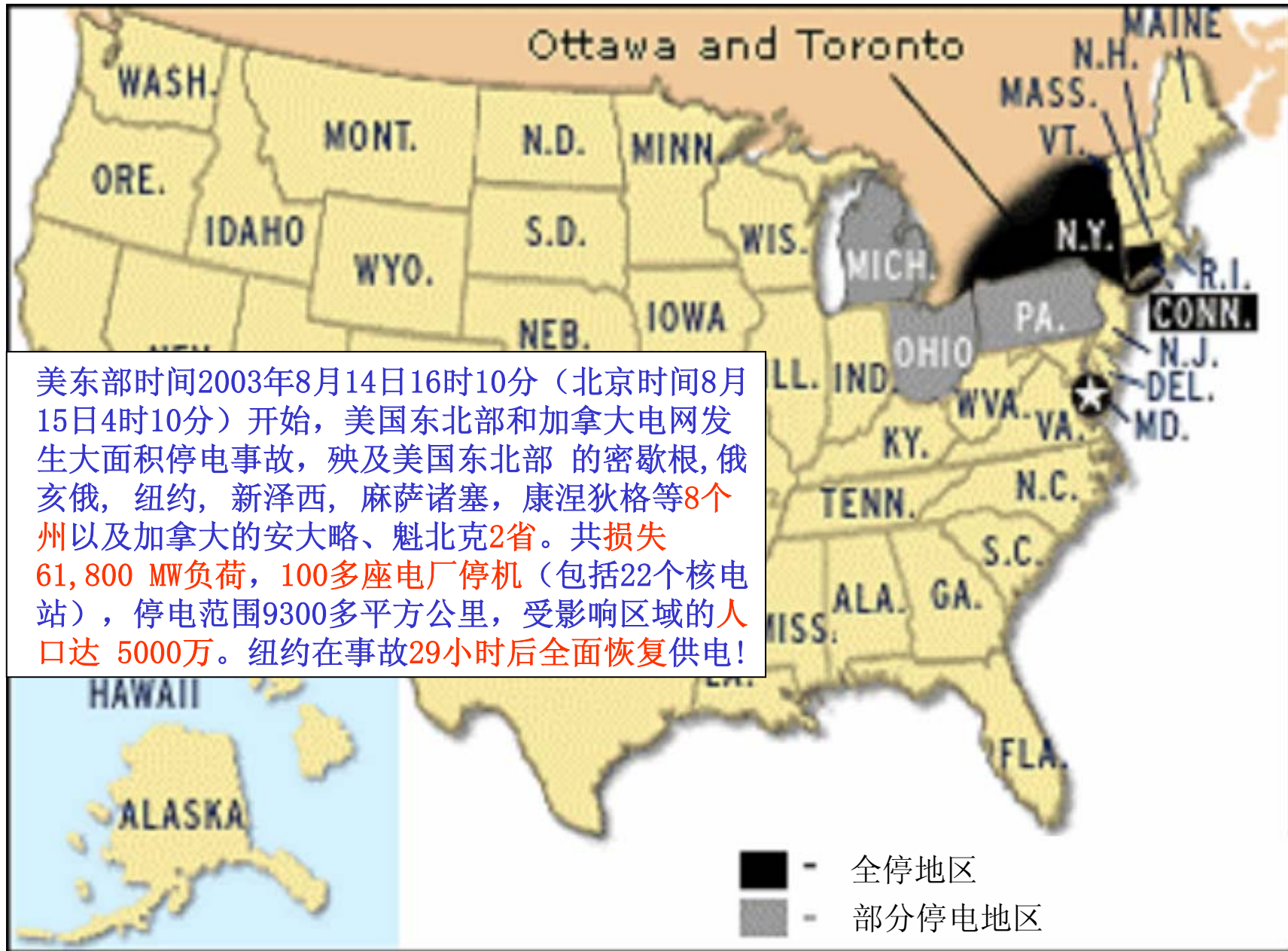
电力二次系统示意图



电力系统安全防护总体结构示意图



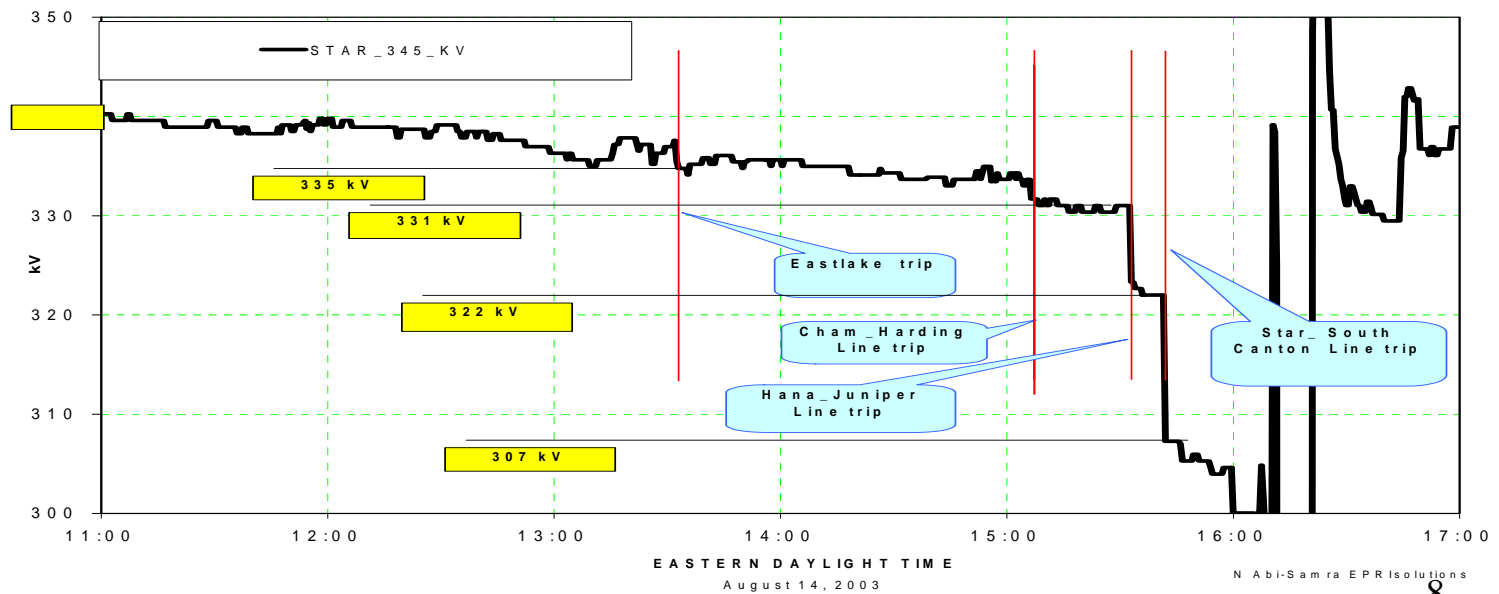
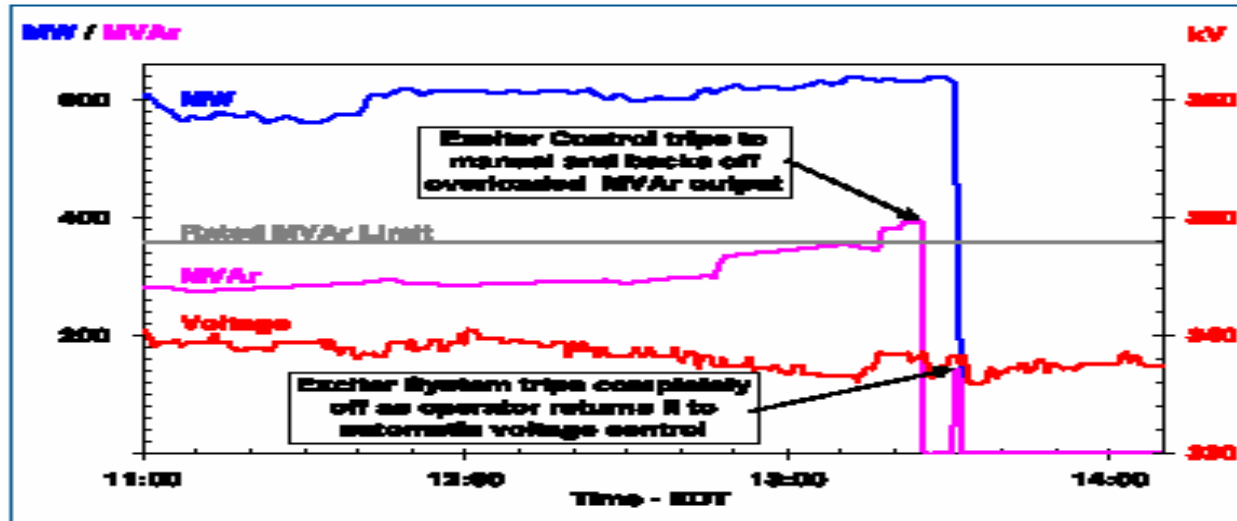
美加2003-8-14大停电事故



美东部时间2003年8月14日16时10分（北京时间8月15日4时10分）开始，美国东北部和加拿大电网发生大面积停电事故，殃及美国东北部的密歇根，俄亥俄，纽约，新泽西，麻萨诸塞，康涅狄格等8个州以及加拿大的安大略、魁北克2省。共损失61,800 MW负荷，100多座电厂停机（包括22个核电站），停电范围9300多平方公里，受影响区域的人口达5000万。纽约在事故29小时后全面恢复供电！

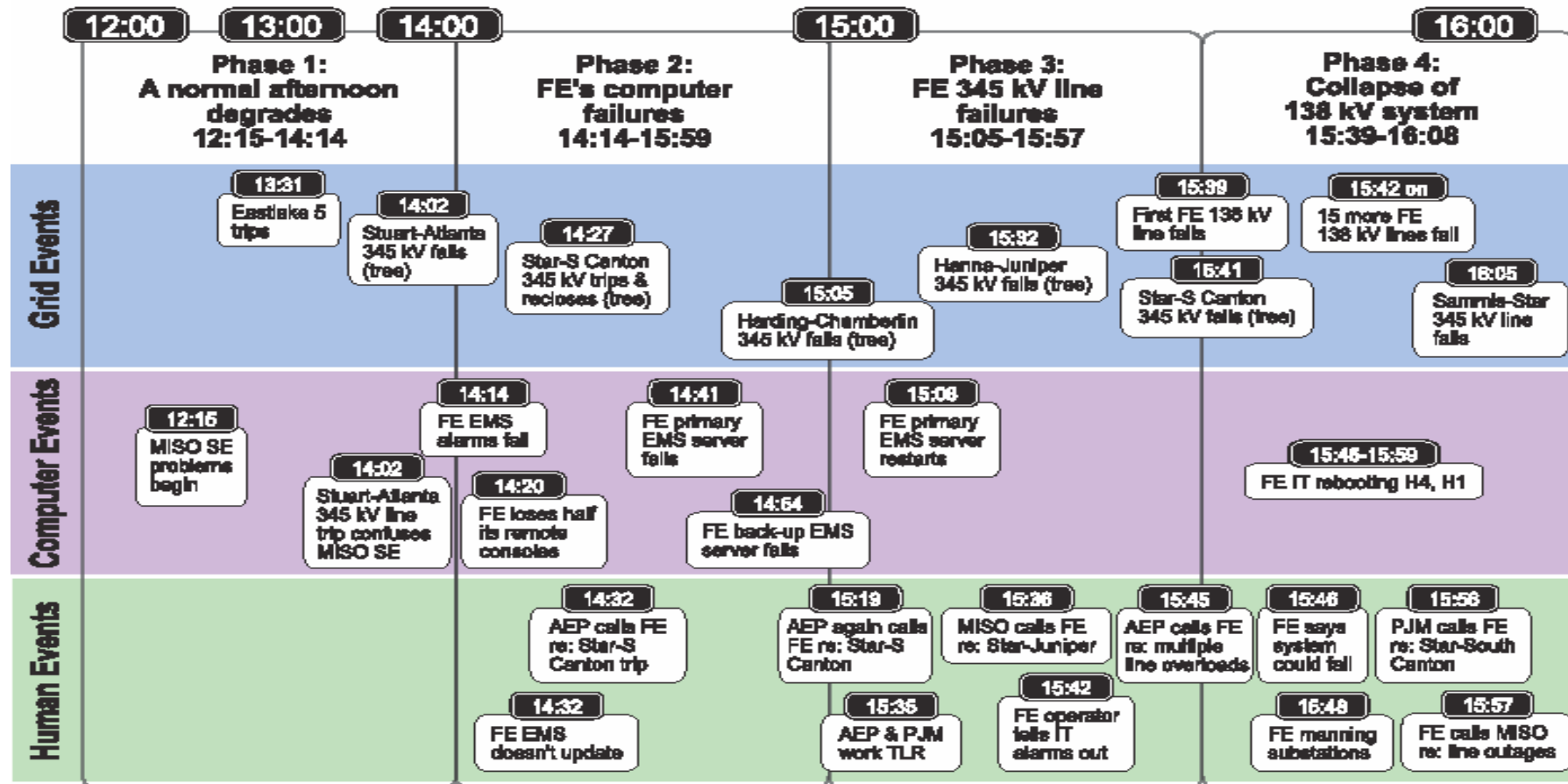
美加8.14事故电压崩溃过程

Figure 3.5. MW and MVar Output from Eastlake Unit 5 on August 14



美加8.14事故顺序事件分类分析

Figure 4.1. Timeline: Start of the Blackout in Ohio



The existence of both internal and external links from SCADA systems to other systems introduced vulnerabilities. At this time, however, preliminary analysis of information derived from interviews with operators provides no evidence indicating exploitation of these vulnerabilities before or during the outage.

我国电力二次系统安全问题

2000年10月13日，四川二滩水电厂控制系统收到异常信号停机，7秒甩出力**89万**，川渝电网几乎瓦解。

2001年10月1日，银山公司生产的故障录波装置出现“时间逻辑炸弹”，全国共**146套**。

2003年12月30日，龙泉、政平、鹅城换流站控制系统发现病毒，外国技术人员在系统调试中用笔记本电脑上网所致。

电力二次系统安全防护的重点

电网调度系统安全防护的目标是抵御病毒、黑客等通过各种形式发起的恶意破坏和攻击，尤其是集团式攻击，重点保护电力实时闭环监控系统及调度数据网络的安全，防止由此引起电力系统事故，从而保障电力系统的安全稳定运行，保证国家重要基础设施的安全，要从国家安全战略的高度充分认识电力安全防护的重大意义。

提纲

一、概况



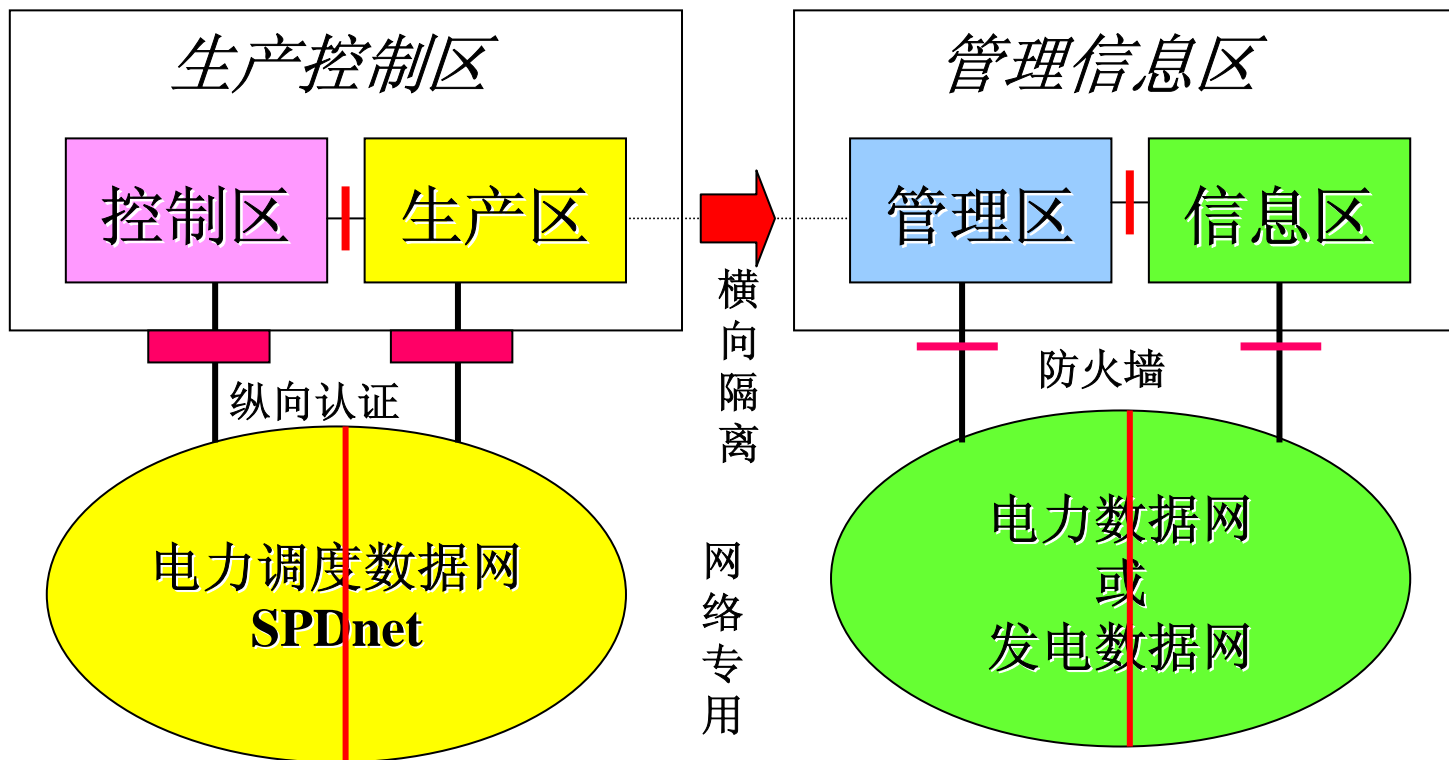
二、总体方案

三、安全管理

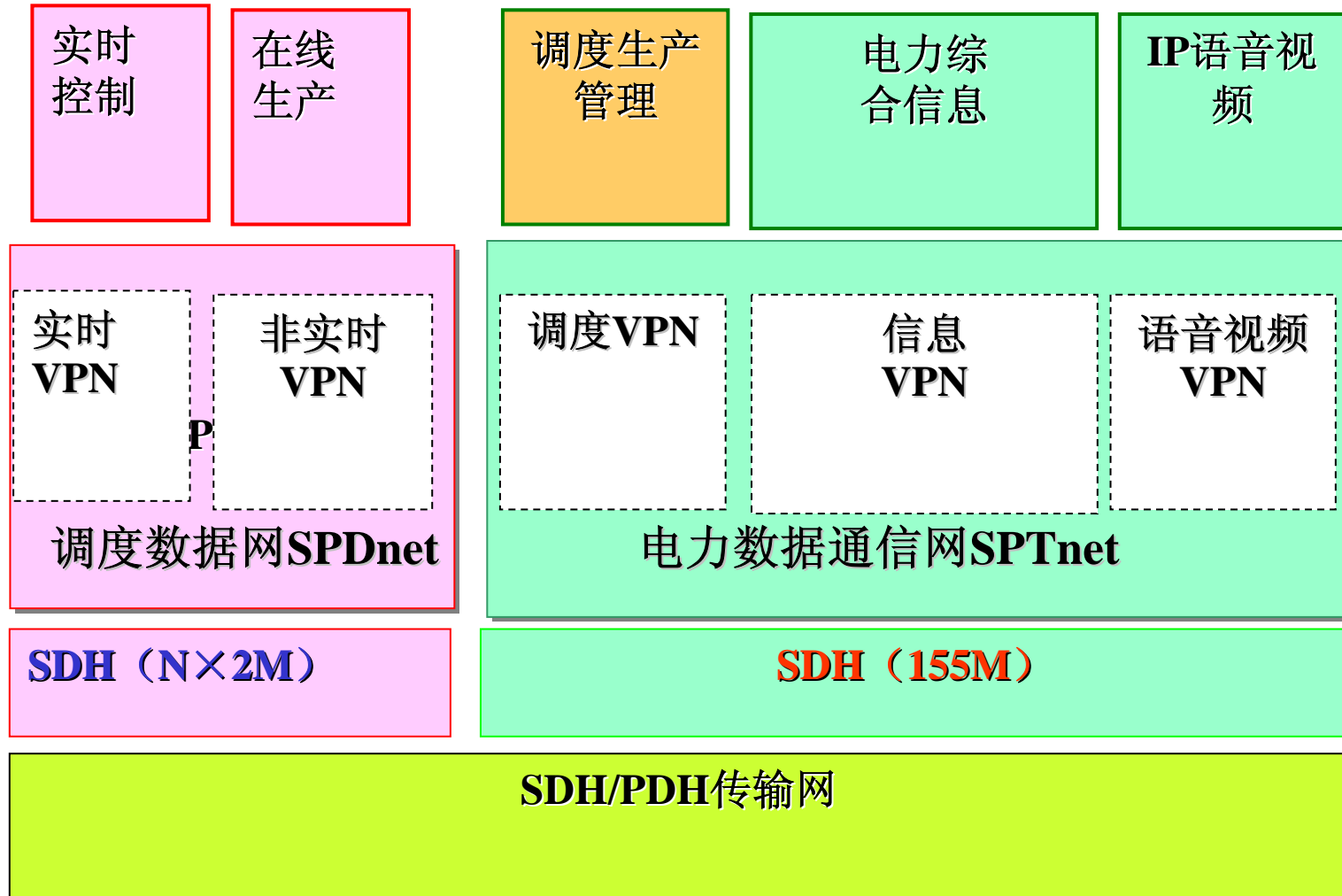
四、结语

电力二次系统安全防护总体策略

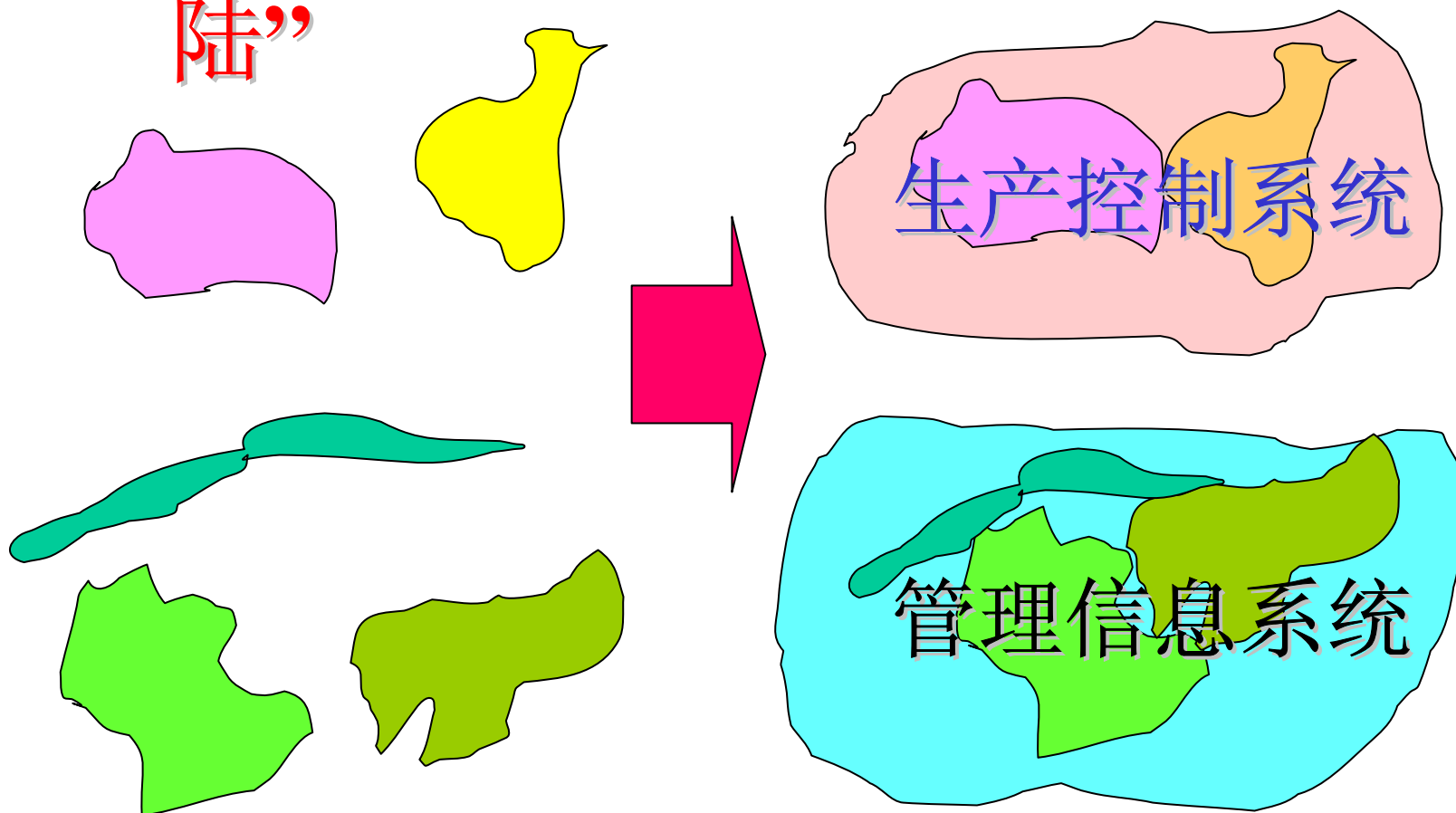
安全分区



电力数据通信网络业务关系



从“信息孤岛”到“安全大陆”



电力调度证书服务系统

鉴于电力系统具有多年形成的安全生产管理机制和半军事化管理的五级调度体系，为非常宝贵的安全资源，而且根据电力控制系统的高可靠性和实时性、控制对象的确定性、控制环境和网络的封闭性、控制范围的有限性和分布性等特点，电力生产控制系统采用简单实用的公钥技术和认证技术，并与其他安全技术和应用系统紧密配合，构造了电力二次系统安全防护体系，而不需建立复杂昂贵的PKI和CA系统。

专家忠告： 可用公钥技术，但不用PKI
可用证书技术，但不用CA

电力调度证书的特点

全国电力调度统一建设基于公钥技术的电力调度证书服务系统，选用公钥技术和证书技术的精华，结合电力调度系统半军事化管理的特点，以数字证书的方式管理和保护密钥，使电力控制业务可以方便地使用加密和数字签名技术，保证控制数据的机密性、完整性、有效性、可靠性、实时性。

Web服务: I区禁用, II区可用安全WEB;
III区和IV区可采用;

E-MAIL服务: I区和II区禁用,
III区和IV区可采用;

拨号服务: I区和II区需采用基于
LINUX/UNIX的拨号认证服务器。

加密认证: I区和II区的关键应用采用调度证
书,

对称加密采用专用芯片。

通用安全防护技术

- 防火墙：** 实现逻辑隔离，须用国产设备；
- 防病毒：** I区和II区以离线的方式及时更新；
- 入侵检测：** 部署在区域边界；
- 备份恢复：** 定期备份，确保能够恢复；
- 主机防护：** 对关键服务器和网关进行安全配置、安全补丁、主机加固；
- 访问控制：** 采用强口令、调度证书等；
- 安全审计：** 对系统及安全设施日志等进行审计；
- 安全蜜罐：** 迷惑攻击者，收集攻击者相关信息。

其它专门开发的安全防护技术

安全告警平台：对安全区I和II中的防火墙、IDS、横向隔离装置、纵向加密认证装置、拨号认证装置等告警信息采集（syslog），自动短信告警；

安全文件交换平台：II区生产数据文件交换，用户侧无须再开发接口，简单方便；

综合数据平台：部署在安全区III，集成I、II区各应用系统的结果数据，便于大量桌面客户访问；

数据交换平台：部署在安全区II，区内各应用系统之间交换在线数据，对III区转发在线数据；

纵向装置管理平台：在线管理、测试纵向装置；

分布证书管理平台：离线分发管理调度证书。

国际标准与安全防护

IEC 61970系列标准：调度自动化系统（CIM）

IEC 61968系列标准：配电自动化系统

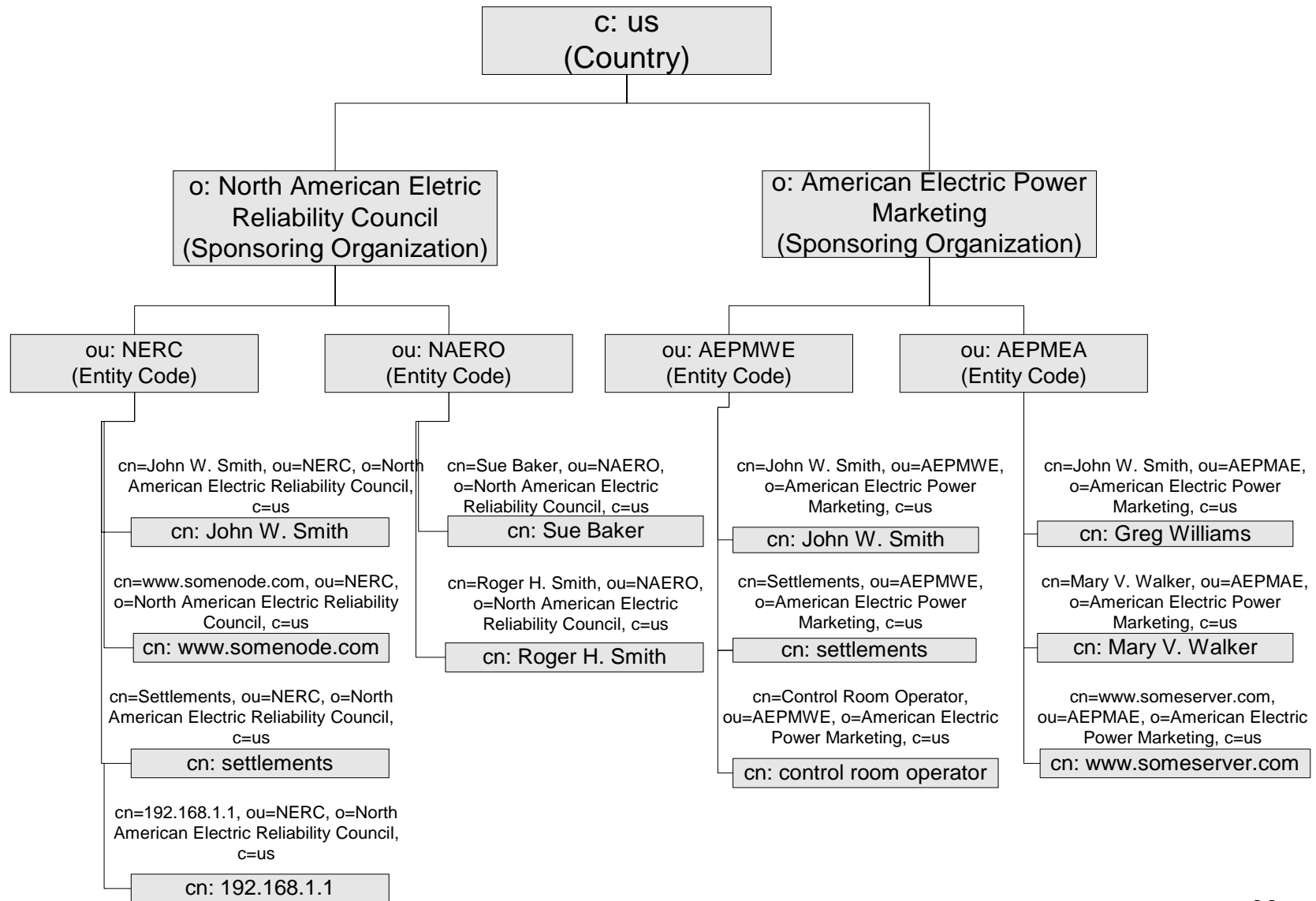
IEC 61850系列标准：变电站自动化系统

中国提出这些标准尚未采取任何安全防护措施，实施这些标准必须坚持合理划分安全区域的原则，将标准规定的功能模块恰当的置于各安全区域之中，从而实现国际标准与安全防护的有机统一。

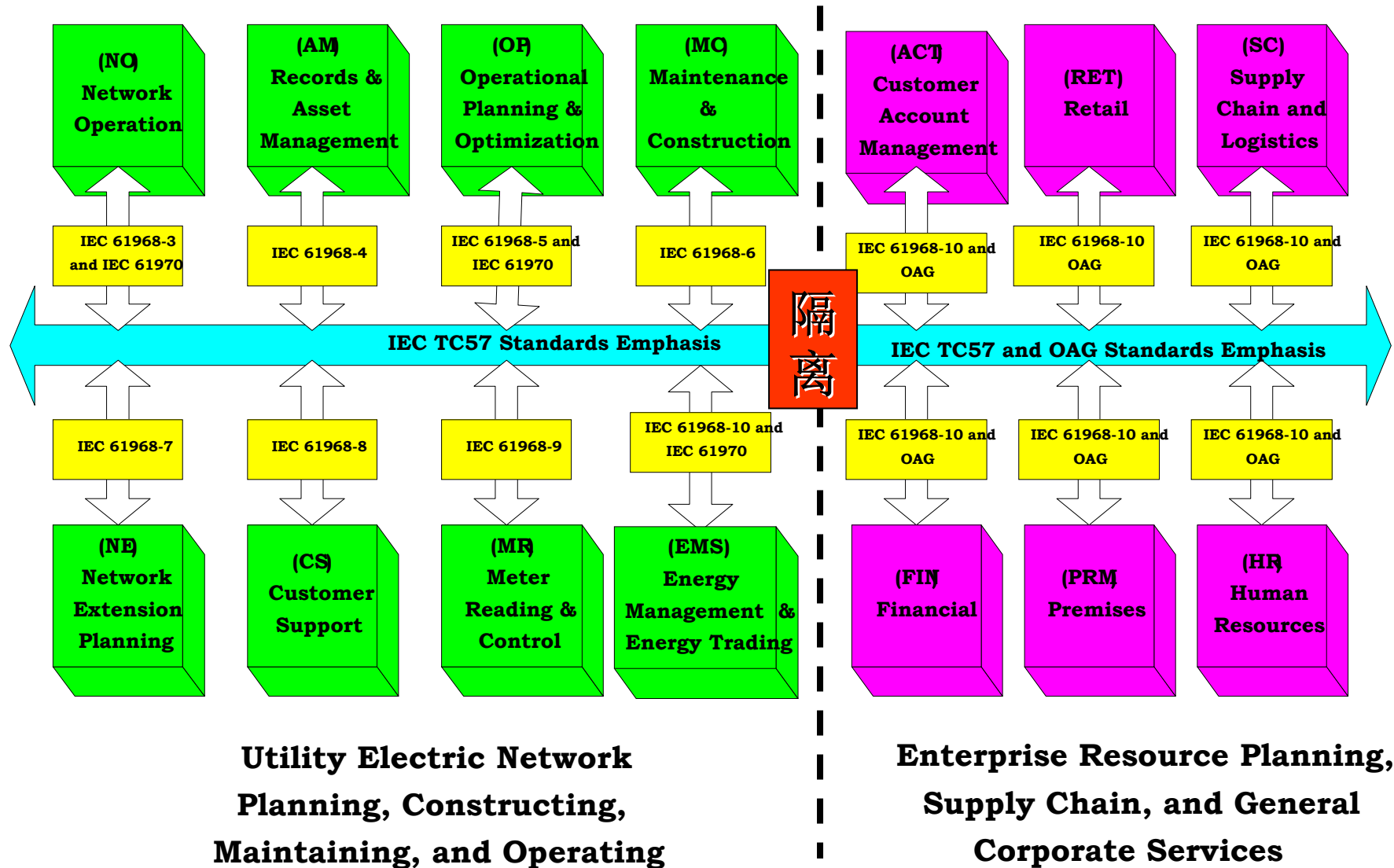
TC57 WG15 提出以传输层安全（TLS）为主的草案

美国能源管制委员会（FERC）提出PKI的e-MARC草案

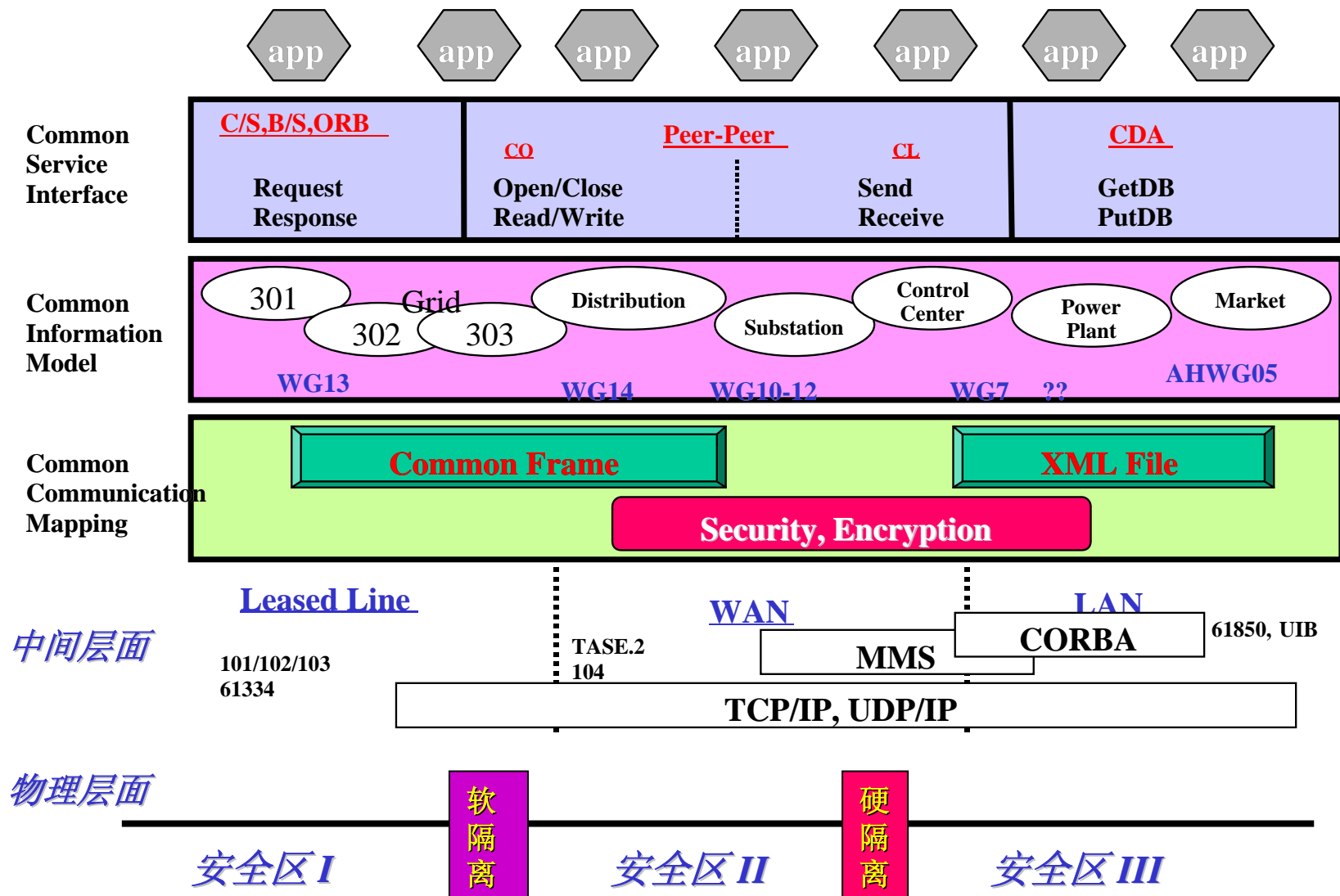
US Certificate Policy for Energy Market Access and Reliability Certificates (e-MARC)



配电自动化系统理想配置示意图

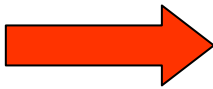


电力系统数据通信协议体系



提纲

- 一、概况
- 二、总体方案
- 三、安全管理
- 四、结语



三分技术 七分管理：安全管理措施

- 人员管理
- 权限管理
- 访问控制管理
- 设备及子系统的维护管理
- 恶意代码（病毒及木马等）的防护
- 安全审计管理
- 数据及系统的备份管理
- 用户口令及数字证书的管理
- 应急处理
- 联合防护

建立完善的安全管理组织机构

- 建立完善的安全分级负责制
- 明确各级的人员的安全职责
 - 各调度机构、发电厂、变电站的主要负责人为该单位所管辖的电力二次系统的安全防护第一责任人
 - 各调度机构、发电厂、变电站指定专人负责管理本单位所属电力二次系统的公共安全设施
 - 对于各个电力二次专业应用系统指定专人负责该系统的安全管理
 - 指定专人负责管理本单位或本部门的电力二次系统的数字证书管理系统

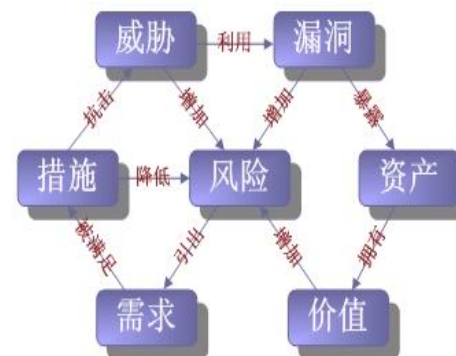
工程实施的安全管理

- 新建电力二次系统工程的设计方案必须符合国家、行业的有关安全防护的标准、法规、法令、规定等；
- 电力二次系统各相关设备及系统的供应商必须承诺：所提供的设备及系统中不包含任何安全隐患，并承担由此引起的连带责任，终生有效；
- 电力二次系统的安全防护方案必须经过上级主管单位的审查、批准，完工后必须通过上级有关部门验收。

安全设备及应用系统接入管理

- 在所有电力二次专业系统的安全区 I 及安全区 II 中的任何工作站、服务器均严格禁止以各种方式开通与互联网的连接；
- 接入电力二次系统的安全区 I 及安全区 II 中的安全产品必须使用国产产品并经过国家有关安全部门或电力有关部门的认证。

安全风险评估



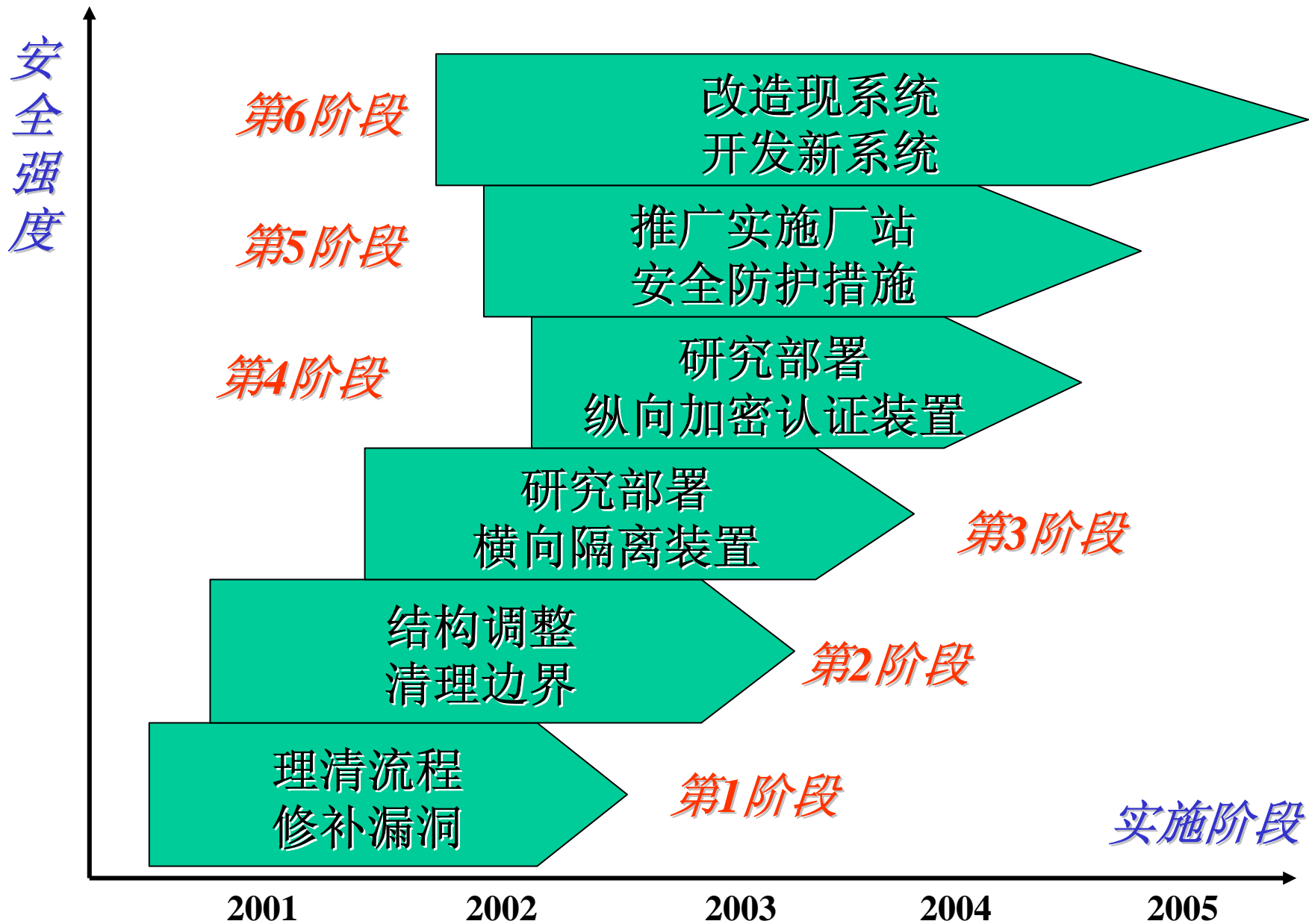
存在问题：

- 1) 社会上一些安全评估单位工作不规范，反而造成安全漏洞。
- 2) 缺乏方便实用的安全评估工具。
- 3) 目前电力系统的信息安全评估方面的技术力量还有待进一步加强，尤其是地调、县调、电厂。

主要措

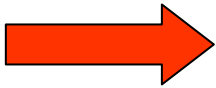
施电力调度系统的风险评估今后将作为一项经常性的工作，不定期地在各个电力调度系统中开展，主要依靠电力系统自身的技术力量，有选择地从外单位引入技术支持。

将安全风险评估作为安全管理的基础工作，纳入安全生产评价体系，主管部门统一指导、统一规范。重点培养、充分依靠系统内部安全专业服务队伍，强调各级电力企业的自我评估。

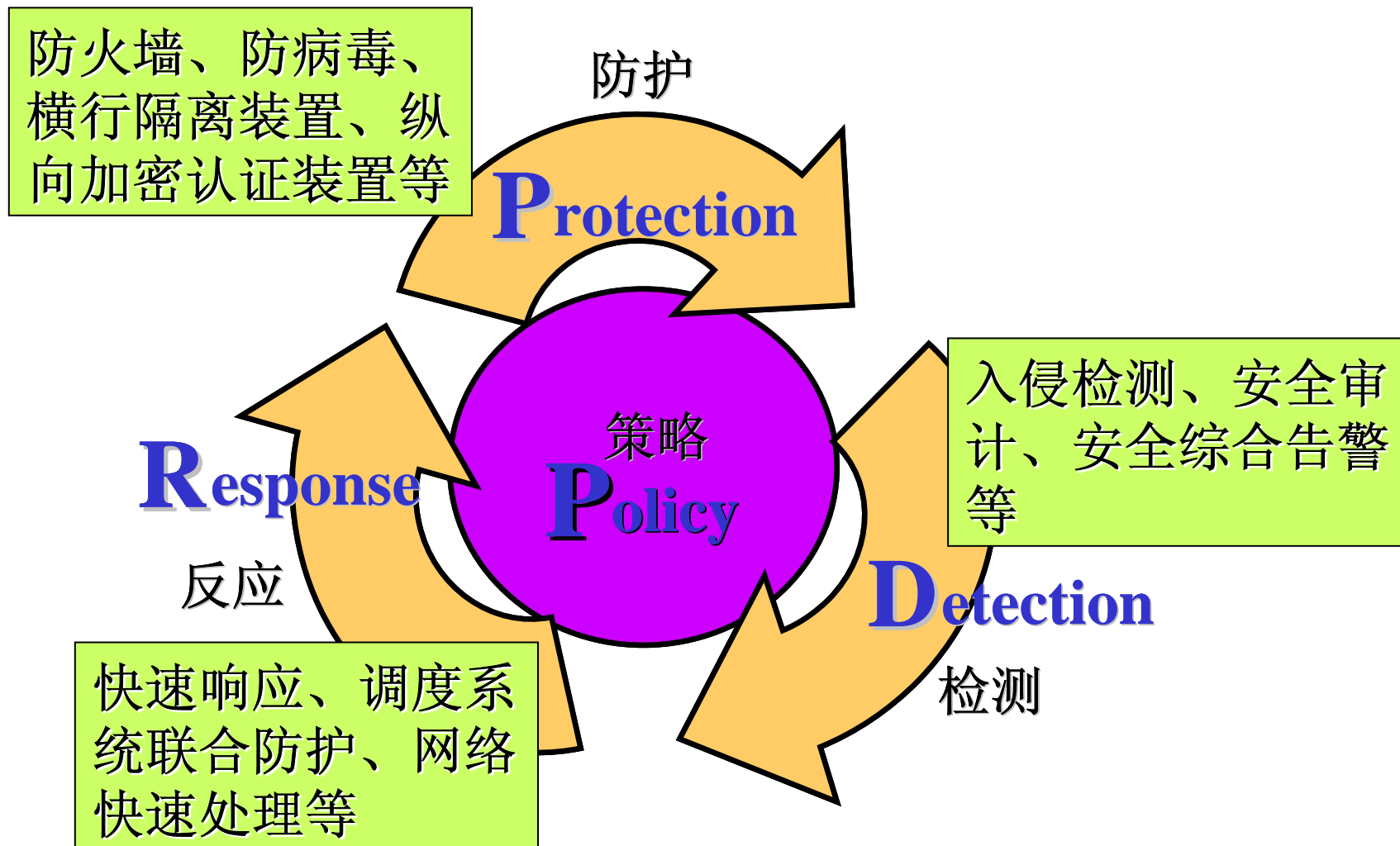


提纲

- 一、概况
- 二、总体方案
- 三、安全管理
- 四、结语



安全防护 永无止境



谢谢大家