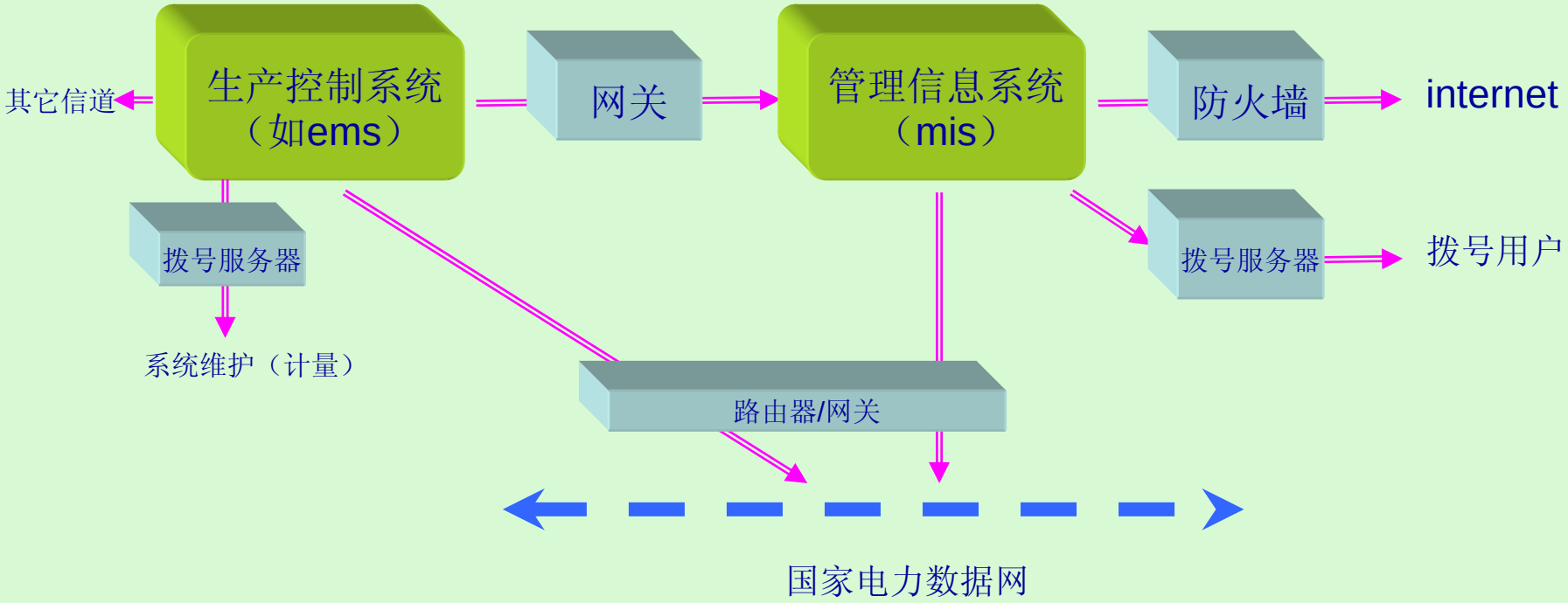
电力系统

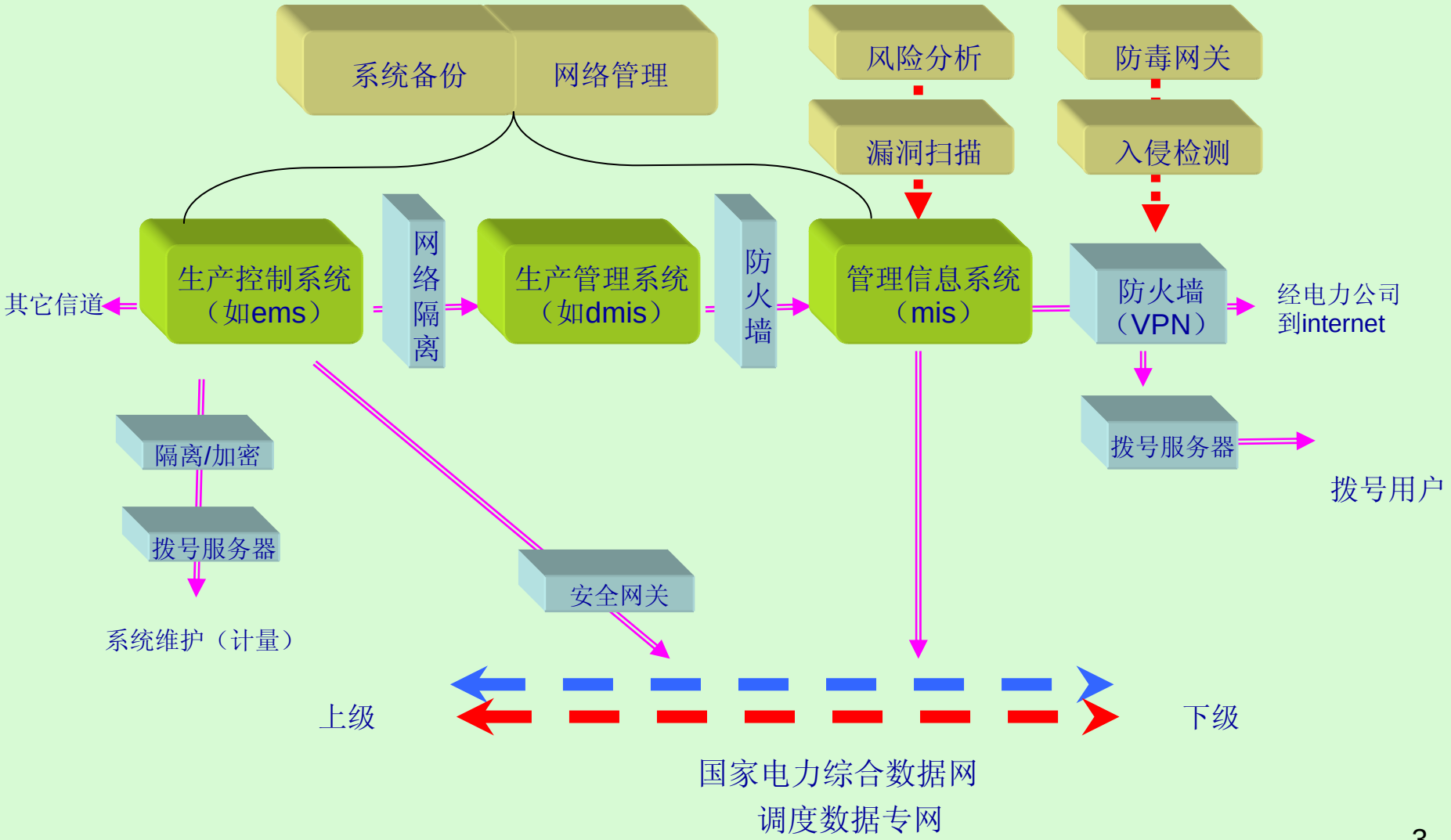
专用网络隔离设备

电力系统网络结构

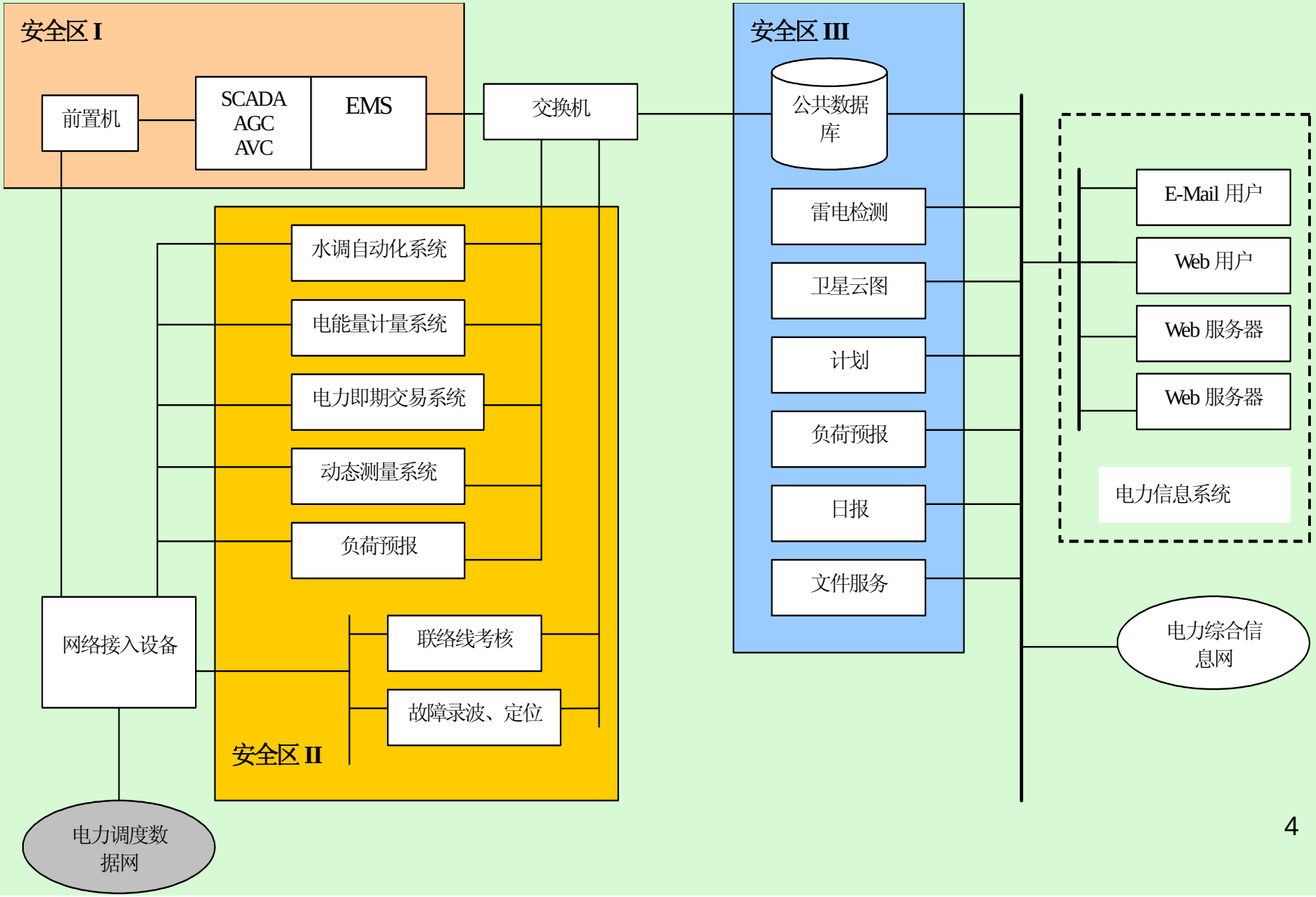
1、目前数据网络在电力系统中的应用日益广泛，已经成为不可或缺的基础设施。
2、国家电力数据网同时承载着实时准实时控制业务及管理信息业务，但安全级别较低、实时性要求较低的业务与安全级别较高、实时性要求高的业务在一起混用。
2、不同安全等级别的系统没有隔离措施，特别缺乏生产控制系统与其他信息系统的有效隔离，以及建立电力系统的安全防护体系。



系统总体防护结构



三层四分区原则



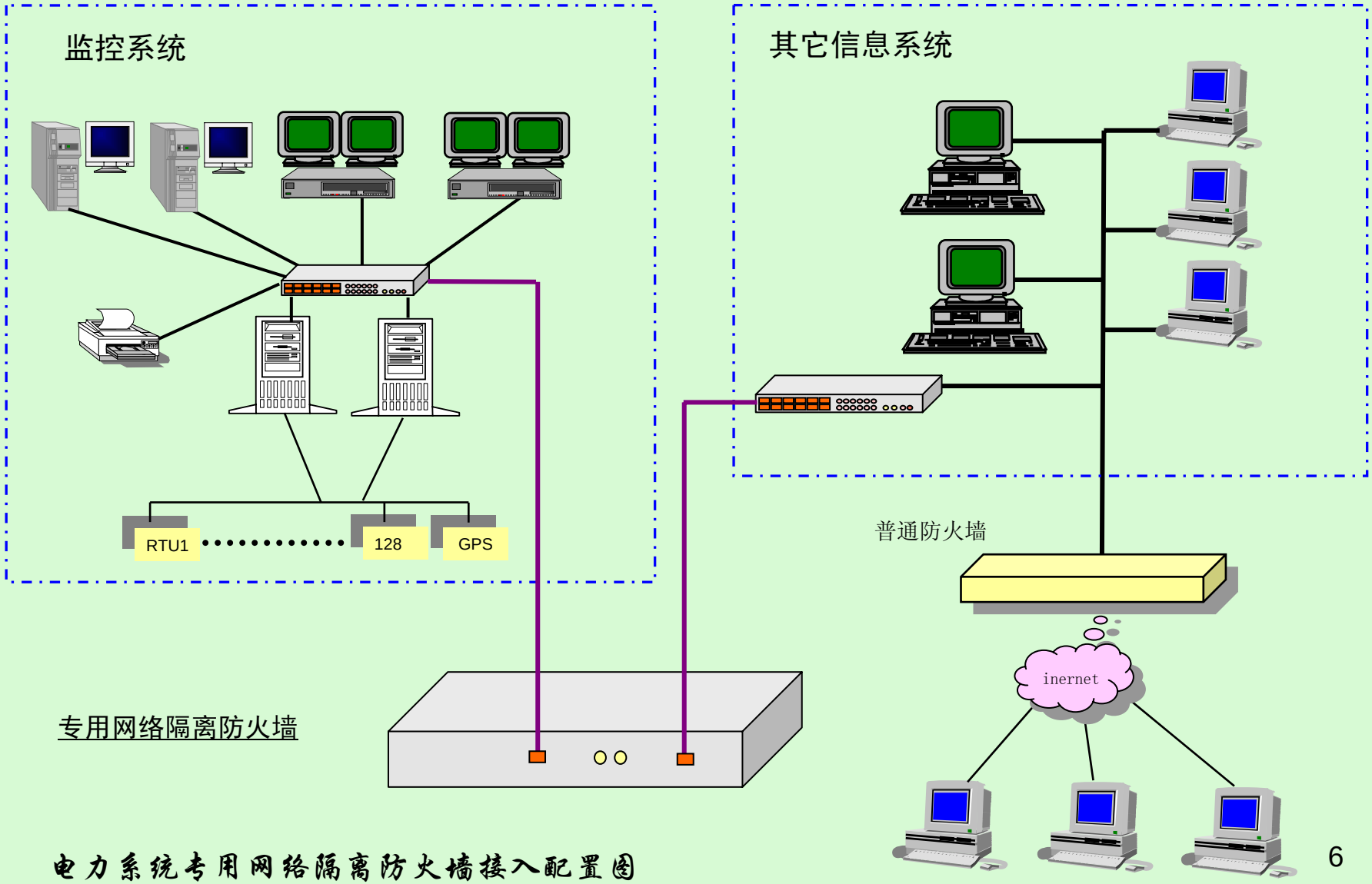
安全防护原则

基本原则　　安全等级较高的系统不受安全等级较低系统的影响

具体原则

1) 系统性原则（木桶原理）；
2) 简单性原则；
3) 实时、连续、安全相统一的原则；
4) 需求、风险、代价相平衡的原则；
5) 实用与先进相结合的原则；
6) 方便与安全相统一的原则；
7) 全面防护、突出重点的原则；
8) 分层分区、强化边界的原则；
9) 整体规划、分步实施的原则；
10) 责任到人，分级管理，联合防护的原则

使用场合



电力系统专用网络隔离防火墙接入配置图

设计目标

设计基本目标：

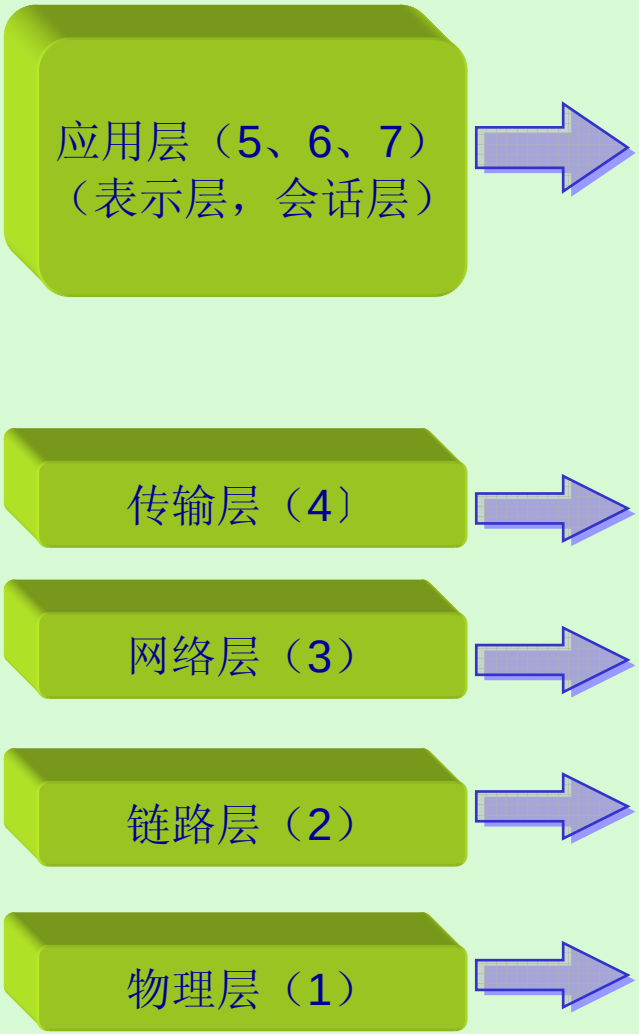
1. 作为一个中心“控制点”，集中管理监控系统的安全；
2. 屏蔽非法请求，防止跨权限访问，并产生安全报警；

装置具体目标：

1. 无IP地址，透明监听方式
2. 具有单向连接请求、单向数据传输
3. 带应用层标记数据传输的控制能力
4. 网络地址转换（NAT）的功能，实现内网地址屏蔽
5. MAC/IP地址、协议、端口过滤功能
6. 单向数据控制，单向连接控制
7. 防止穿透性TCP联接，具有应用层解析功能

网络协议分层

七层网络协议



文件传输，电子邮件，文件服务，虚拟终端	TFTP，HTTP，FTP，SMTP，DNS，Telnet …
数据格式化，代码转换，数据加密	
解除或建立与别的接点的联系	
透明传送报文，提供端对端的通信链路建立、维护、管理	TCP，UDP
为数据包选择路由、分组传送、流量控制	ICMP ，IP，RIP，OSPF
传输有地址的帧以及错误检测功能	ARP，RARP， SLIP，CSLIP，PPP，MTU
在物理媒体上传输数据，尽可能屏蔽物理介质及设备的差异	ISO2110，IEEE802.3

TCP首部

TCP传输原理

TCP协议在IP协议之上。TCP协议为其上的应用层提供了一种可靠传输服务。这种服务的特点是通过积极确认和重发送方式，提供、可靠、全双工、流式和无结构传输。

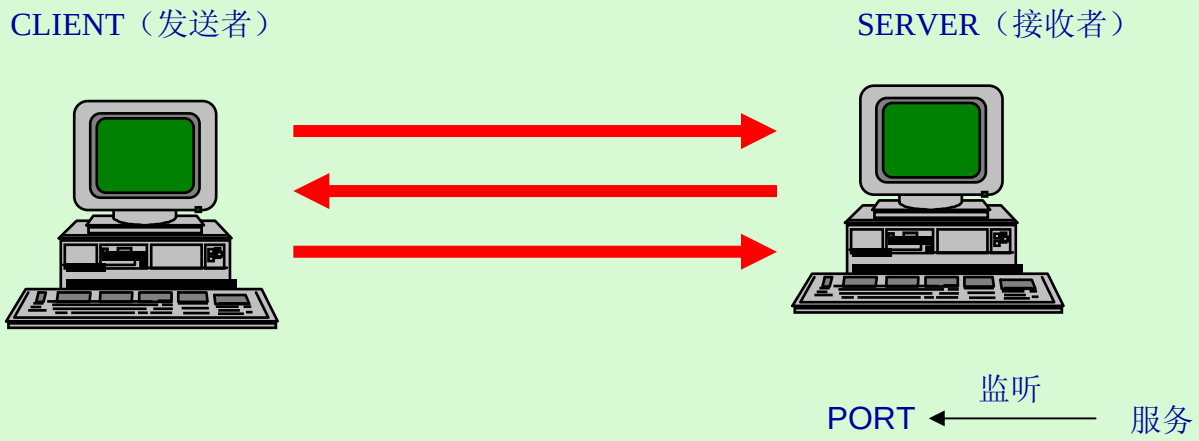
<table>
<tr><td colspan="10">32bit</td></tr>
<tr><td colspan="5">源端口</td><td colspan="5">目的端口</td></tr>
<tr><td colspan="10">序列号</td></tr>
<tr><td colspan="10">确认号</td></tr>
<tr><td>数据偏移</td><td>保留</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="2">窗口</td></tr>
<tr><td colspan="5">校验和</td><td colspan="5">紧急指针</td></tr>
</table>

发起连接　　SYN=1 ACK=0

重连　　RST=1

保留　　应用程序　　加戳

C/S交互过程

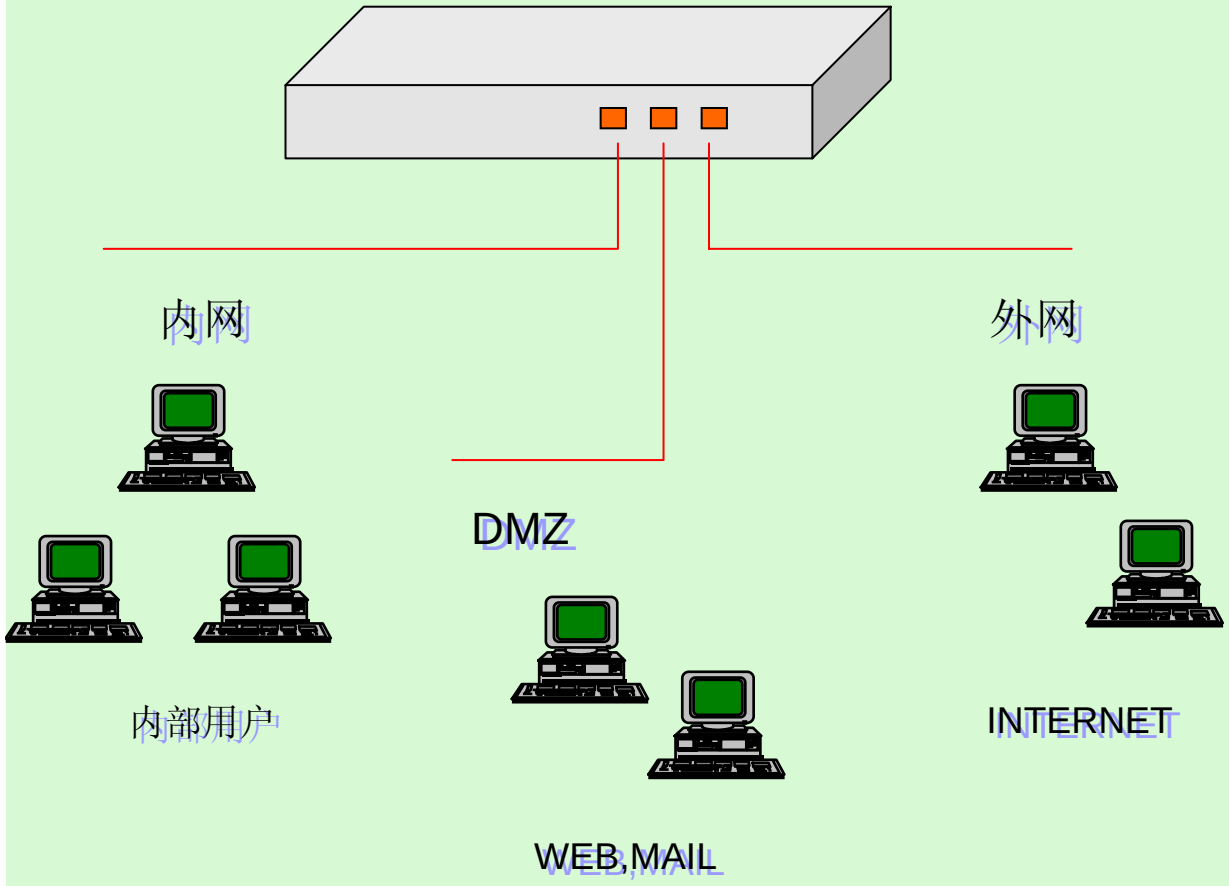


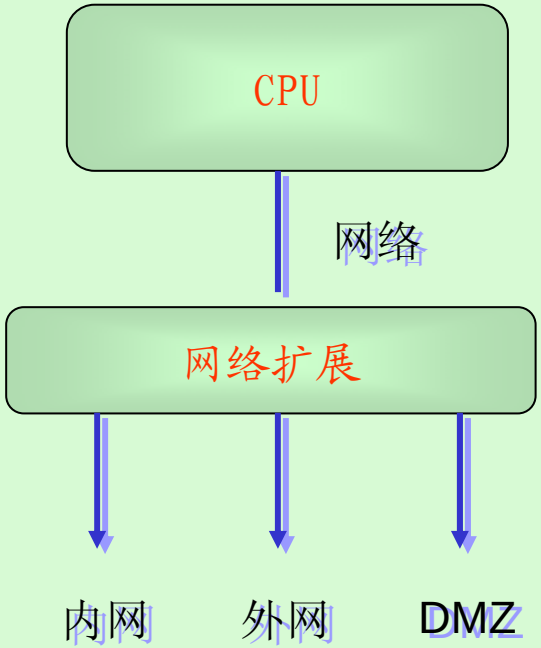
TCP协议使用一个三次握手来建立一个TCP连接的。

1. 握手过程的第一个段的代码位设置为SYN，序列号为x，表示开始一次握手。
2. 接收方收到这个段后，向发送者回发一个段。代码位设置为SYN和ACK，序列号设置为y，确认序列号设置为x+1。
3. 发送者在收到这个段后，知道就可以进行TCP数据发送了，于是，它又向接收者发送一个ACK段，表示，双方的连接已经建立。

通用防火墙的隔离方式1

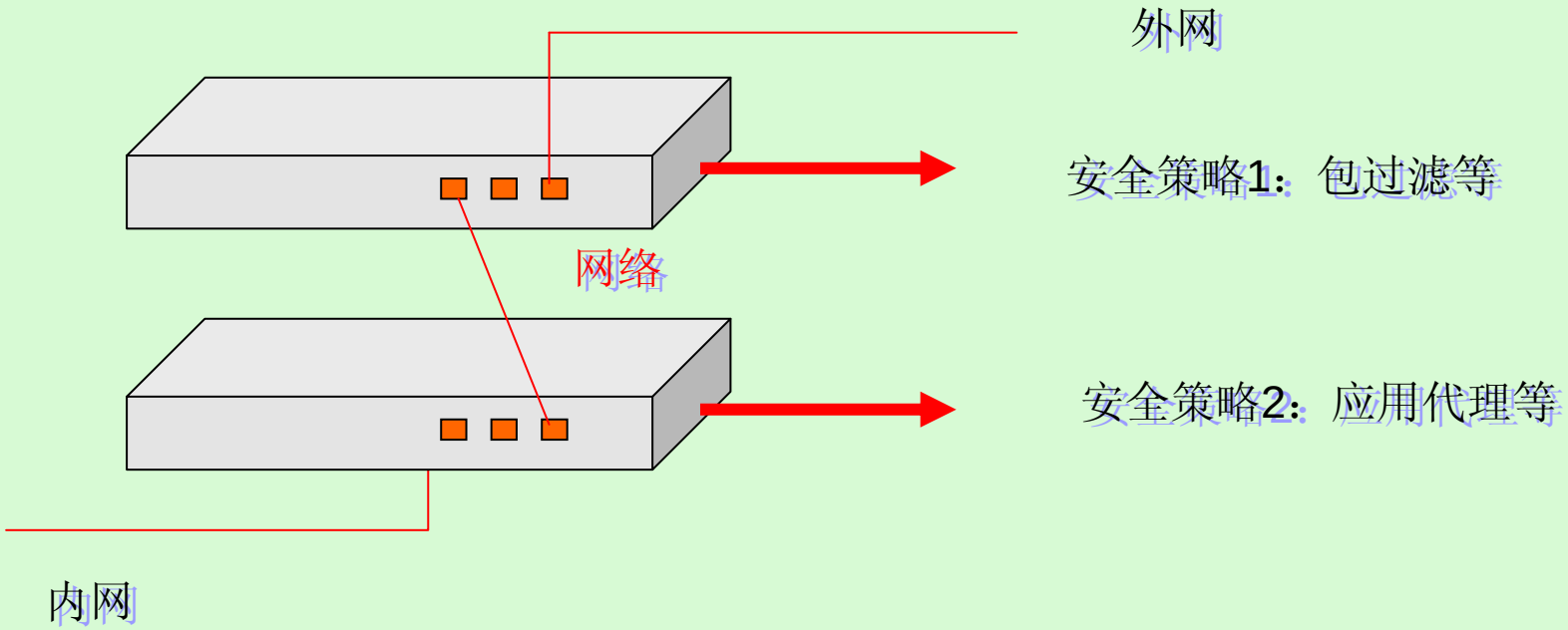
基本方式





通用防火墙的隔离方式2

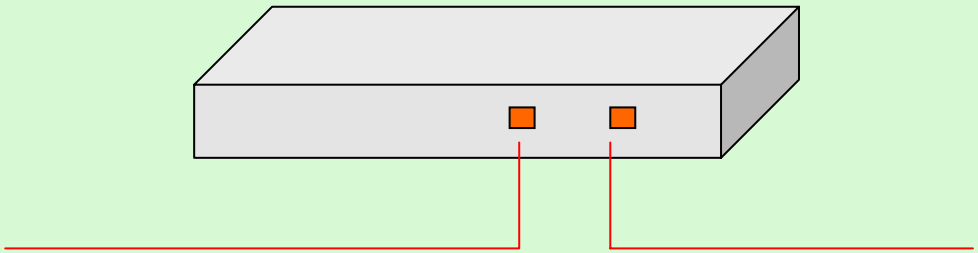
双机方式

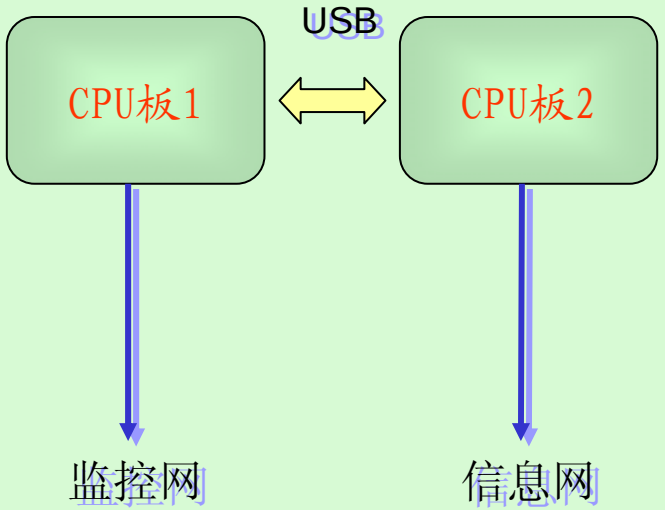


装置硬件结构

1. 非intel系列双处理器
2. 内部非网连接

有效隔离





CPU:GX, POWERPC
连接： USB、双端RAM
非网络驱动

Hrsoft®

装置自身安全

1. 掌握所有硬件板级设计
2. 采用开放源码的嵌入式Linux操作系统为基础的加固操作系统
3. 大量网络安全源程序供使用
4. 掌握所有底层驱动程序源码
5. 取消或修改所有的网络服务
6. 外加安全套件使Linux操作系统安全等级由C2级升为B2级

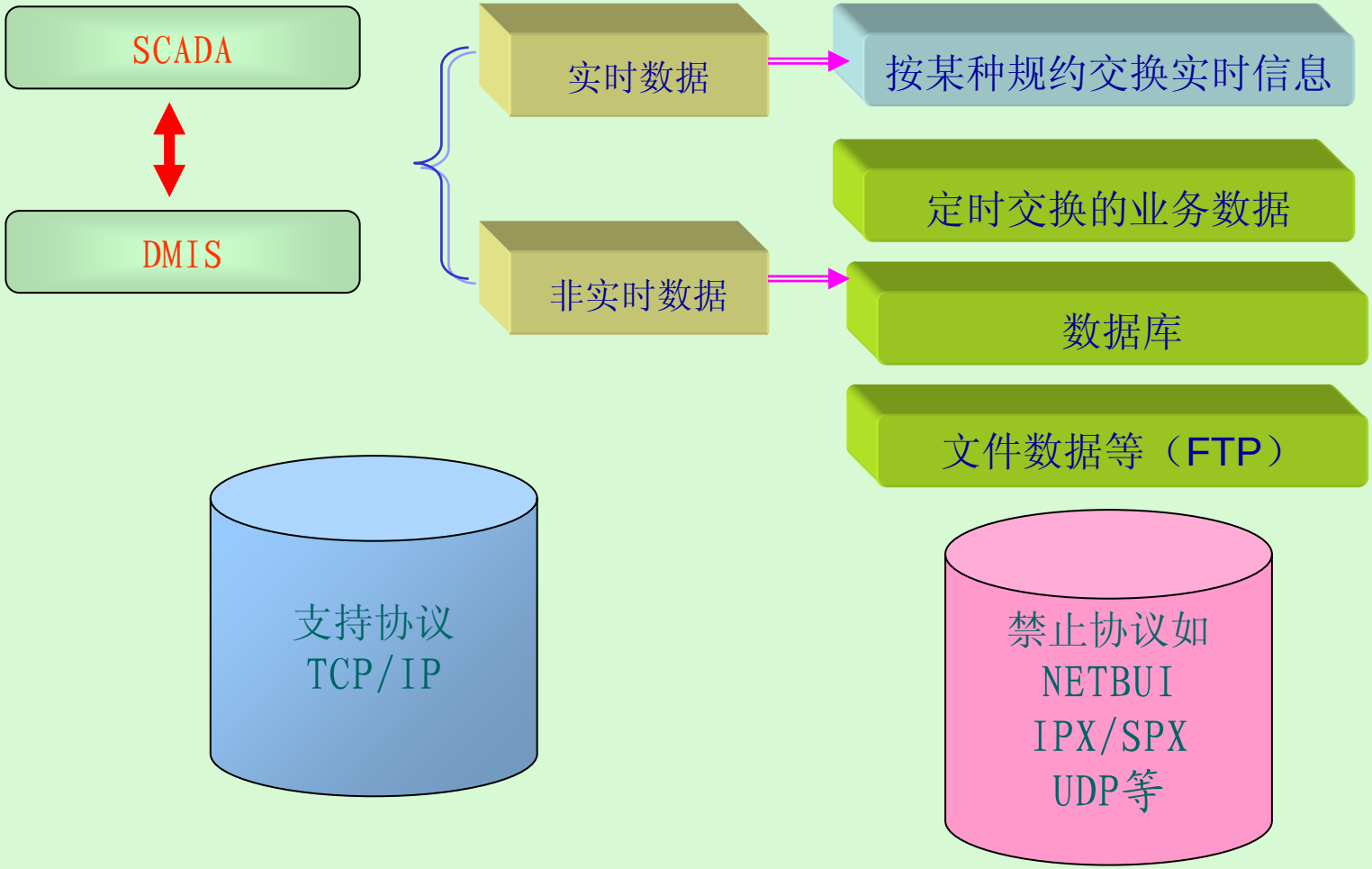
安全操作系统

1. 取消危险的系统调用；
2. 限制命令执行权限；
3. 取消IP转发功能；
4. 检查每个分组的接口；
5. 取消动态路由功能；
6. 取消所有的网络服务；
7. 完成操作系统大量精简；

服务	状态
rsh、rlogin、rexec	删除
telnet	删除
Finger	删除
Tftp	删除
systat、netstat	删除
Rwhod	删除
rwalld*	删除
ftp	删除
ident(auth)	删除
Printer	删除
Ingreslock	删除
Linuxconf	删除
Sendmail	删除
named(DNS)	删除
www(httpd)	删除
pop3&imap	删除
talk&ntalk*	删除
chargen*	删除

数据类型及通信协议

装置隔离及连通数据分析

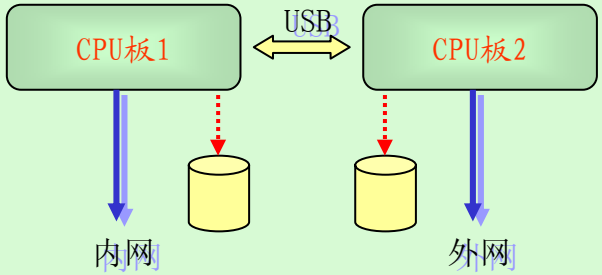


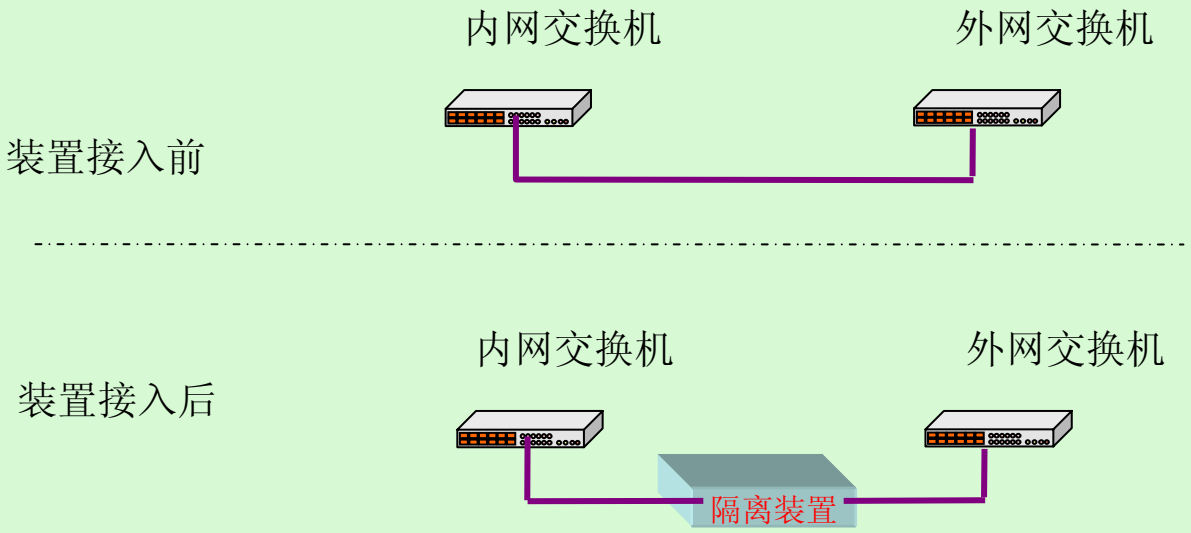
基本防护措施

1. 具有MAC/IP地址绑定
2. 协议（TCP）
3. 端口(非特权端口)过滤

无IP地址透明监听

无IP地址，透明监听方式、便于实施





无穿透性TCP/IP连接

1. ARP、ICMP用特殊的机制完成
2. TCP握手连接由装置控制

   通过tcp代理的方式建立连接

单向连接请求

1、只允许由内网向外网络发起连接，完成数据交互。

2、连接建立后可双向交换数据

3、对单位时间连接数及数据包个数可设定限制。

双向网络地址转换

1. 内网地址经隔离装置进行网络地址转换（NAT），实现内网地址屏蔽
2. 外网地址经隔离装置同期进行网络地址转换（NAT）及端口重定向

应用层标记

1.提供不同的操作系统API调用函数，设置IP报头保留位

2.针对装置转换标记

3.符合标记内容的数据方可通过

应用层流监控

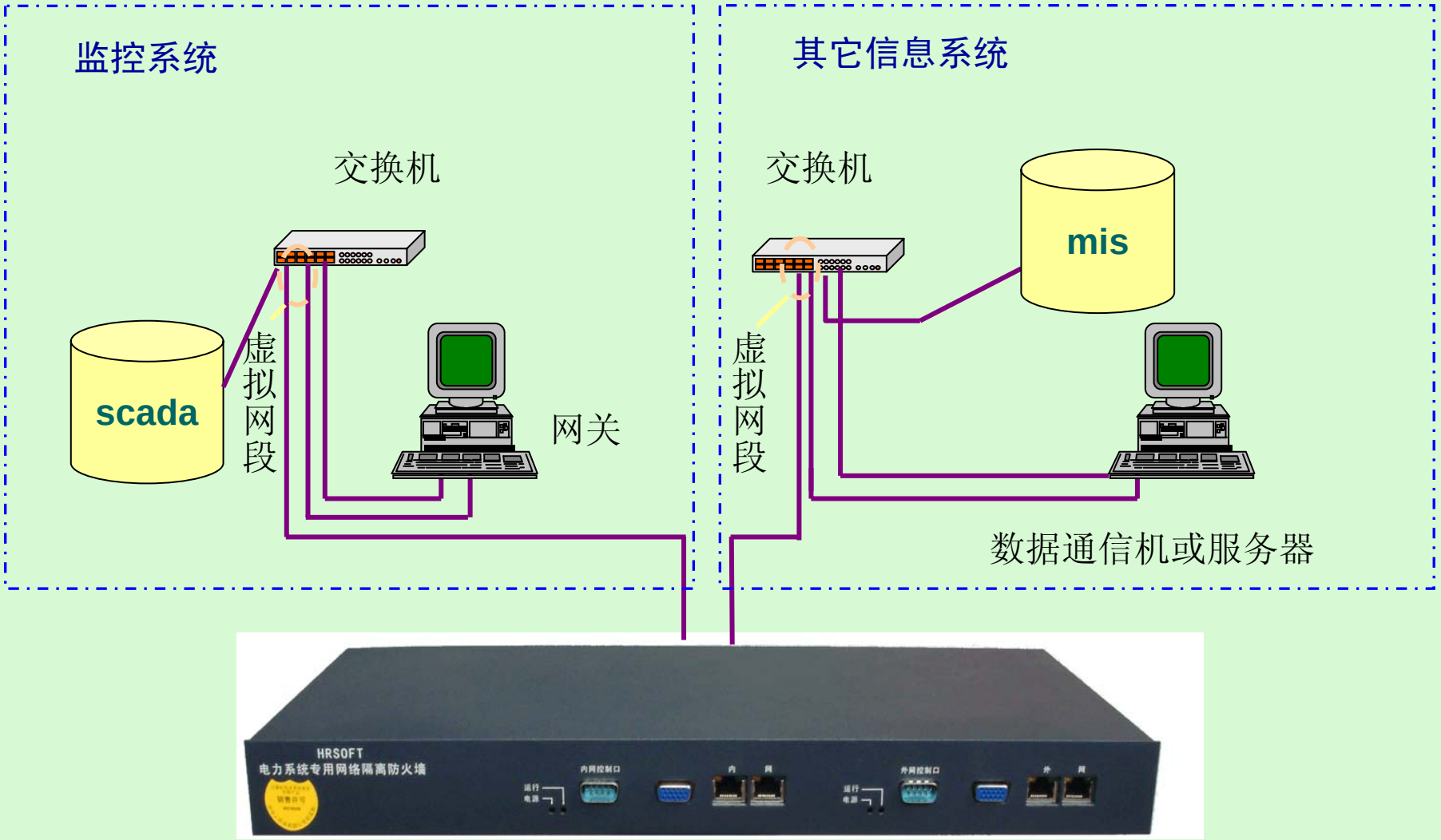
1.应用层规约：

电力部应用层传输协议

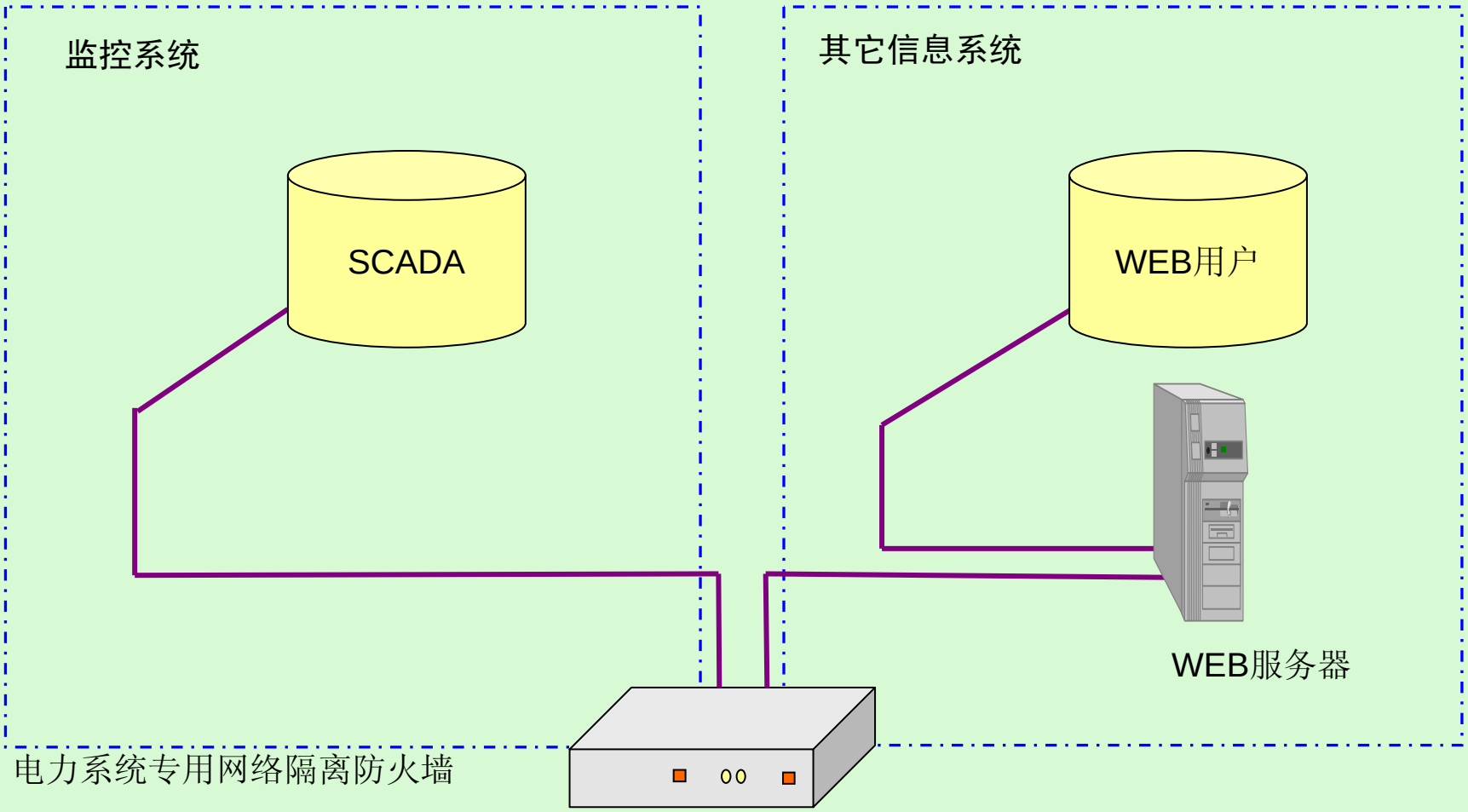
IEC60870-5-104等规约

2. 对应用层数据流格式、校验进行监控，关闭不符合格式的数据流

细化接入方案



scada web安全重构



安全重构的难点

1. 监控系统与MIS系统连接方向及程序的修正
2. WEB 放置隔离装置外
3. 数据库及文件同步复制的方式
4. 复制数据的载体容量、速度、可靠性

隔离装置的速度问题

连接速度

8 Mbits　　90 Mbits

1、实时数据（yc/yx）

10000 YC 10000 YX

600K bits

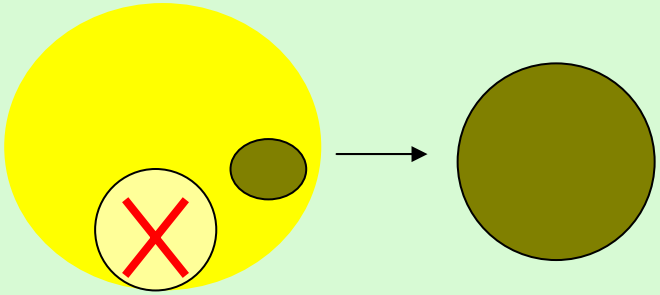
2、非实时数据（数据库、文件、计划值）

突发流量，但不经常

与通用防火墙的区别

通用防火墙

网络隔离装置



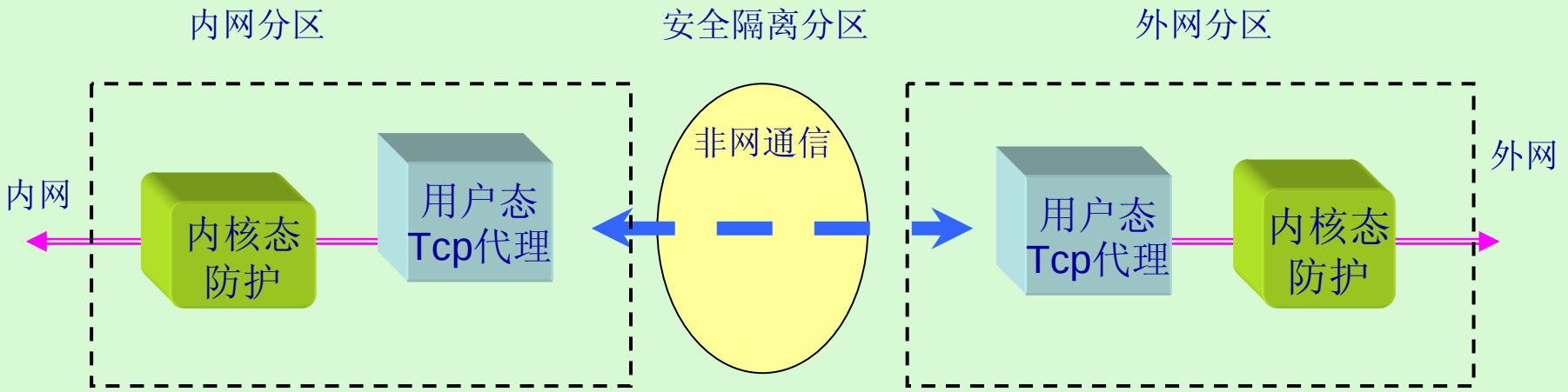
\+ 强度 + 电力系统的特点

项目	通用防火墙	网络隔离装置
设计目标	安全、通用	安全、实时、可靠、专用
隔离强度	强	特强
适用电力特殊要求	无	专业特点定制

1、不通过网络管理，不通过web方式设置参数
2、设置必须当地断电方可生效
3、双cpu非网络方式通信
4、单向控制发起连接
5、结合电力系统规约及应用层标记

Hrsoft®

分层立体防护



其中：1、内核态防护作简单的包过滤等基本策略
2、用户态Tcp代理介绍，可以防止等攻击，比并且可以监视tcp层数据内容等。
3、安全隔离分区的电气信号锁定。

谢谢！