中国华能
CHINA HUANENG

发电行业工控系统信息安全现状

工业控制系统信息安全技术国家工程实验室第三次理事会演讲

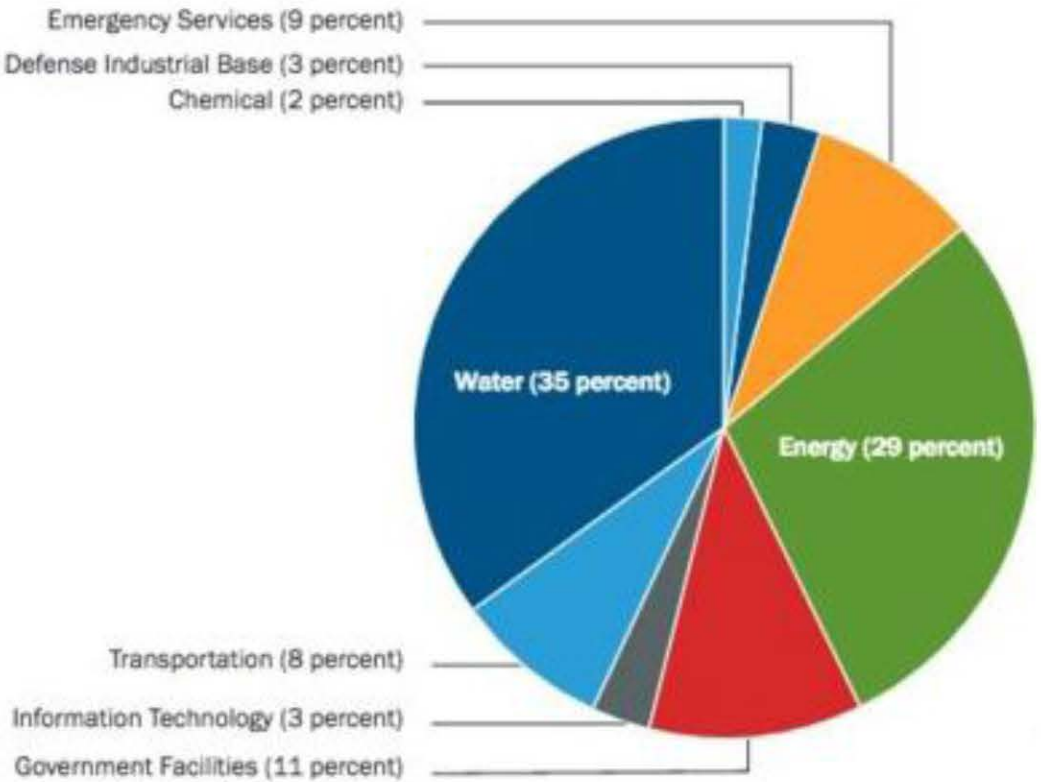
华能集团信息中心 郭森

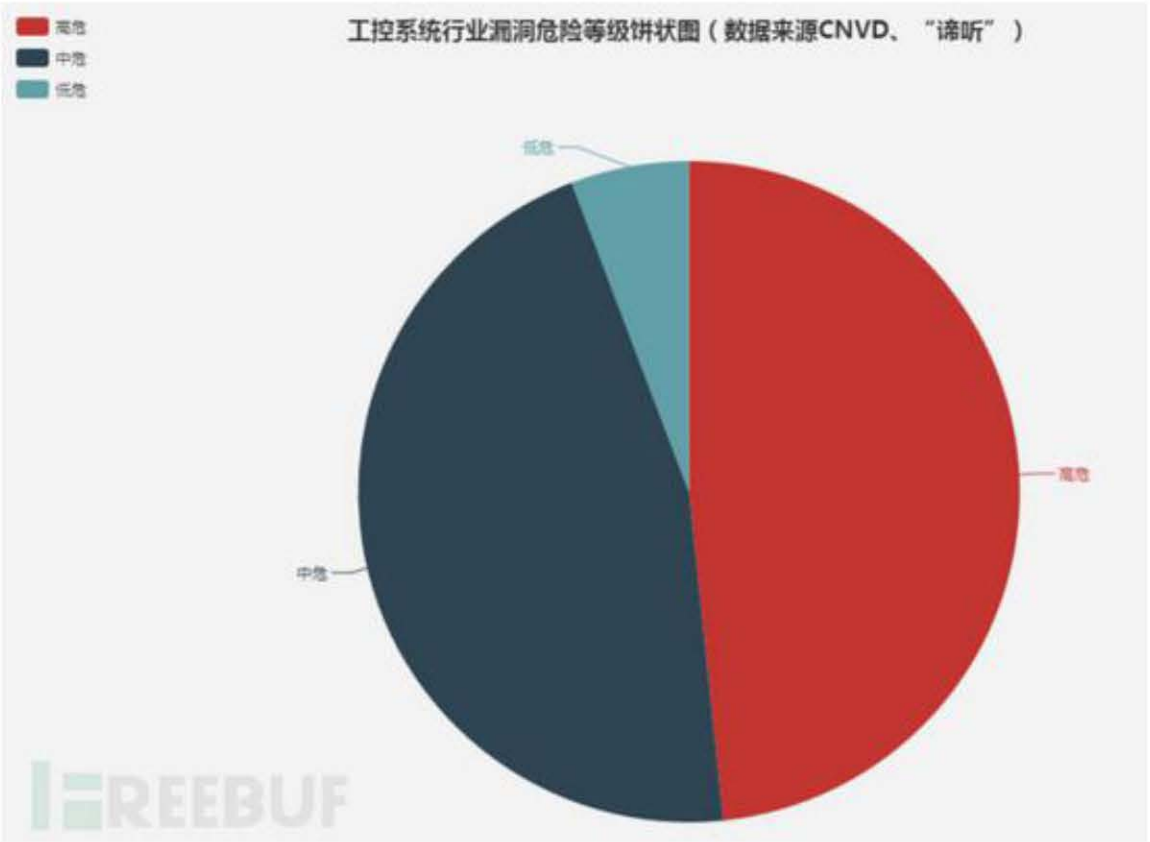
2018.6.29

电力行业的特殊性

- 是国民经济重要基础产业
- 生产过程关联性强
- 具有很强的规模性
- 技术和资金密集型行业
- 对于安全的要求更高
  - 生产安全
  - 信息安全
  - 人身安全

电力工控安全的重要性

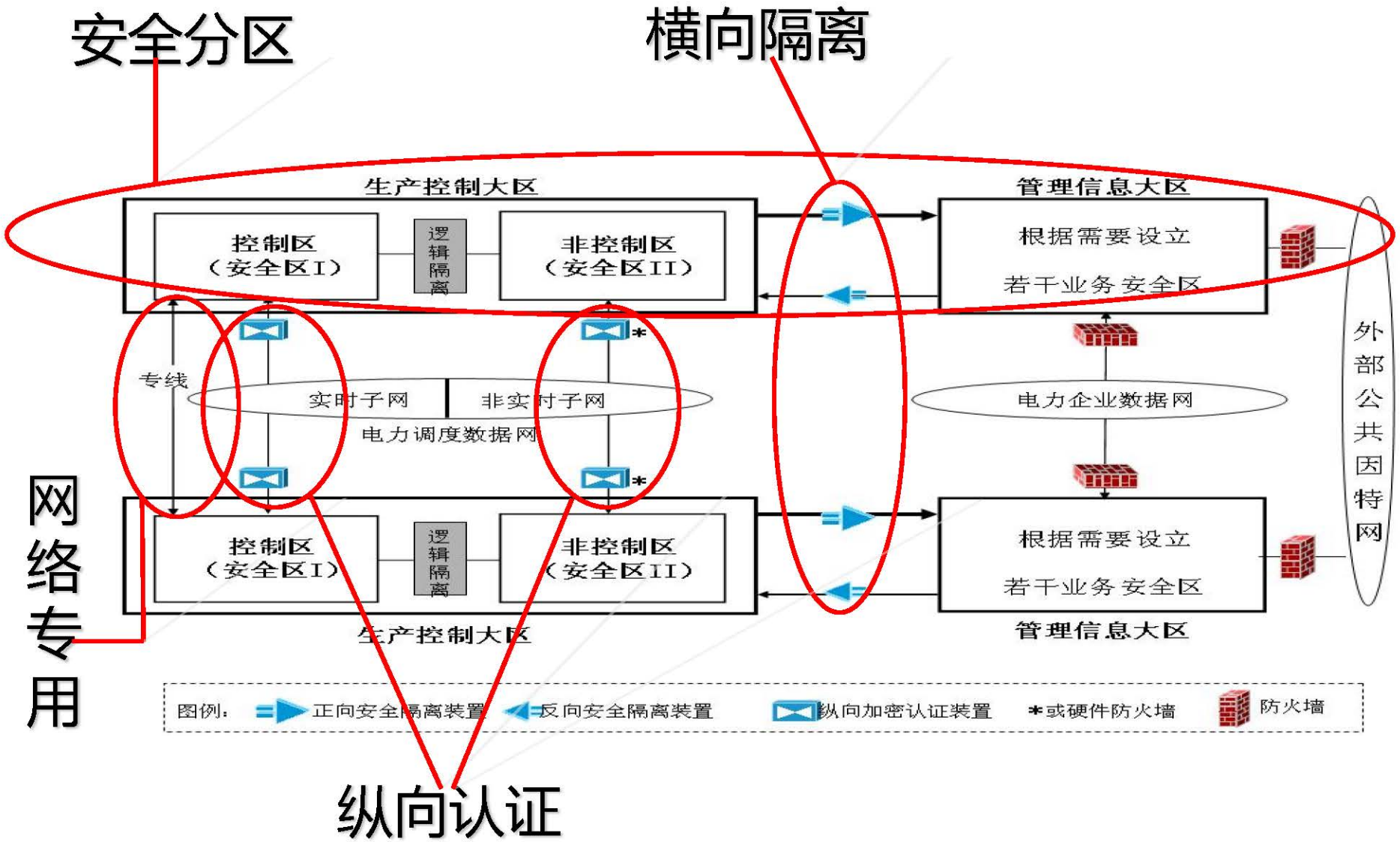

Emergency Services (9 percent)
Defense Industrial Base (3 percent)
Chemical (2 percent)
Water (35 percent)
Energy (29 percent)
Transportation (8 percent)
Information Technology (3 percent)
Government Facilities (11 percent)


工控系统行业漏洞危险等级饼状图（数据来源CNVD、“谛听”）
高危
中危
低危
FREEBUF

电力行业历来重视安全生产

- 遵循国家标准
- 结合行业特点
- 行业测评队伍
- 各行业中领先

电力行业的十六字方针

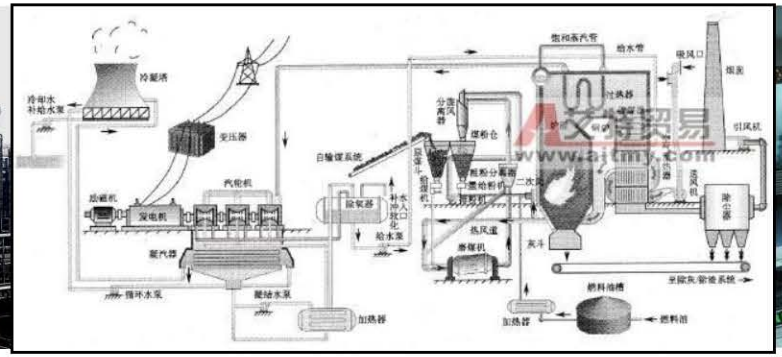

安全分区
横向隔离
生产控制大区
控制区
（安全区I）
逻辑隔离
非控制区
（安全区II）
管理信息大区
根据需要设立
若干业务安全区
外部公共因特网
专线
实时子网
非实时子网
电力调度数据网
电力企业数据网
网络专用
控制区
（安全区I）
逻辑隔离
非控制区
（安全区II）
根据需要设立
若干业务安全区
生产控制大区
管理信息大区
图例：
正向安全隔离装置
反向安全隔离装置
纵向加密认证装置
*或硬件防火墙
防火墙
纵向认证

目录

目录

工控系统安全问题和现状

- 工业控制系统（ICS）是多种类型控制系统的总称，包括：
  - 监控与数据采集（SCADA）
  - 分布式控制系统（DCS）
  - 过程控制系统（PCS）
  - 可编程逻辑控制器（PLC）
  - 应急停车系统（ESD）
  - 安全仪表系统（SIS）
  - 其他自动化控制系统



工控系统安全问题和现状

- 工控系统在能源、交通、水利、城市公用设施行业等国家关键基础设施发挥着“大脑”和“神经中枢”的作用，是保障基础设施安全稳定和高效运行的核心装备和技术

IT的需求

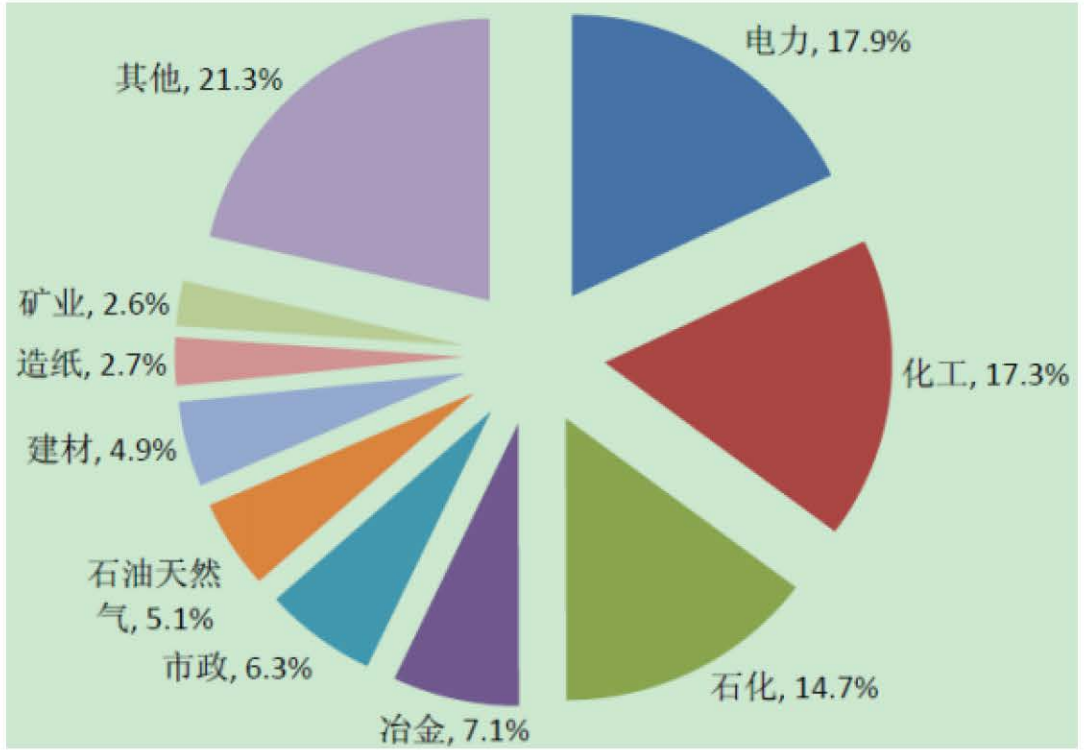
- 高吞吐量
- 标准统一的通信协议
- 设备部署在本地，易于访问
- 设备生命周期为3-5年

VS

ICS的需求

- 实时通信
- 不允许重启
- 人和控制过程安全
- 加入安全后不影响控制流程
- 通信协议多种多样
- 设备不易访问
- 设备生命周期为15-20年

工控系统安全问题和现状



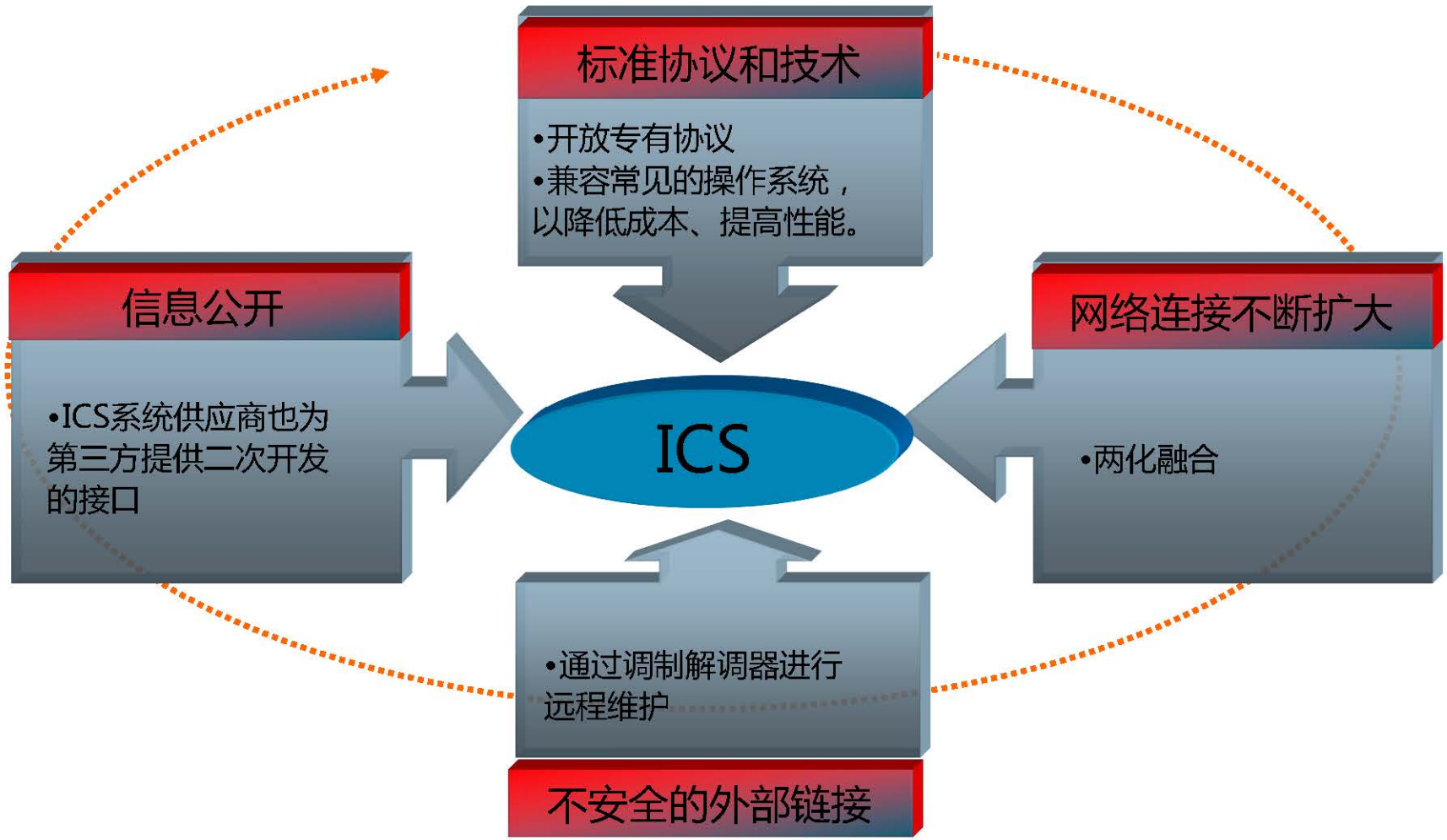
长期垄断全世界流程工业
集散控制系统（DCS）
主要有四家公司

霍尼韦尔 Honeywell 美国
横河 Yokogawa 日本
艾默生 Emerson 美国
西门子 Siemens 德国

1995年之前完全依赖进口
2007年之前大型系统完全依赖进口

安全策略不统一，行业特点差异大。

导致工业控制系统脆弱性的主要原因



十六字方针:
安全分区
网络专用
横向隔离
纵向认证

十六字方针
面临新的挑战

工控系统安全问题和现状

二滩水电厂装机6X550MW，2000年10月13日，500KV二滩—普提—洪沟一回线路检修，二滩水电厂1-4机组运行，5、6号机组停运。11:30机组总处理1014MW，突然计算机监控系统操作员站和返回屏无任何实时数据显示，计算机监控系统死机。
二滩水电厂计算机监控系统供应商为ABB公司。1999年，二滩水电厂开发了一套MIS系统，在没有任何网络安全措施的情况下，将MIS系统直接接入计算机监控系统。MIS系统接入后，计算机监控系统曾出现过系统过载情况。

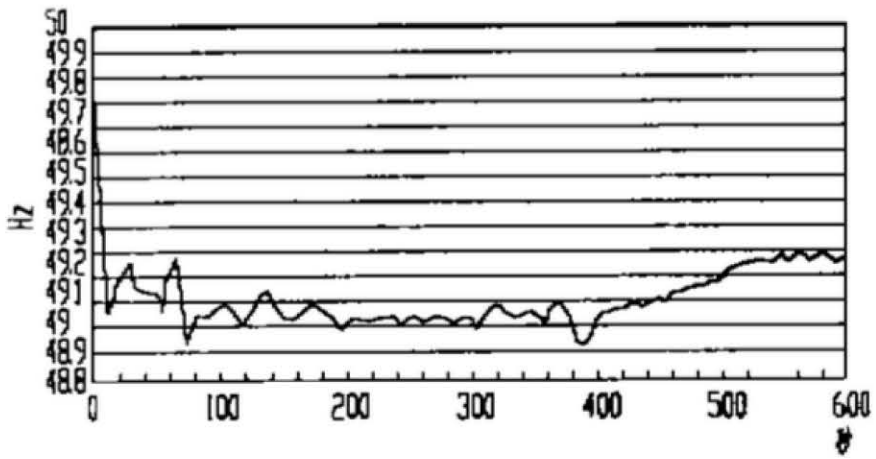


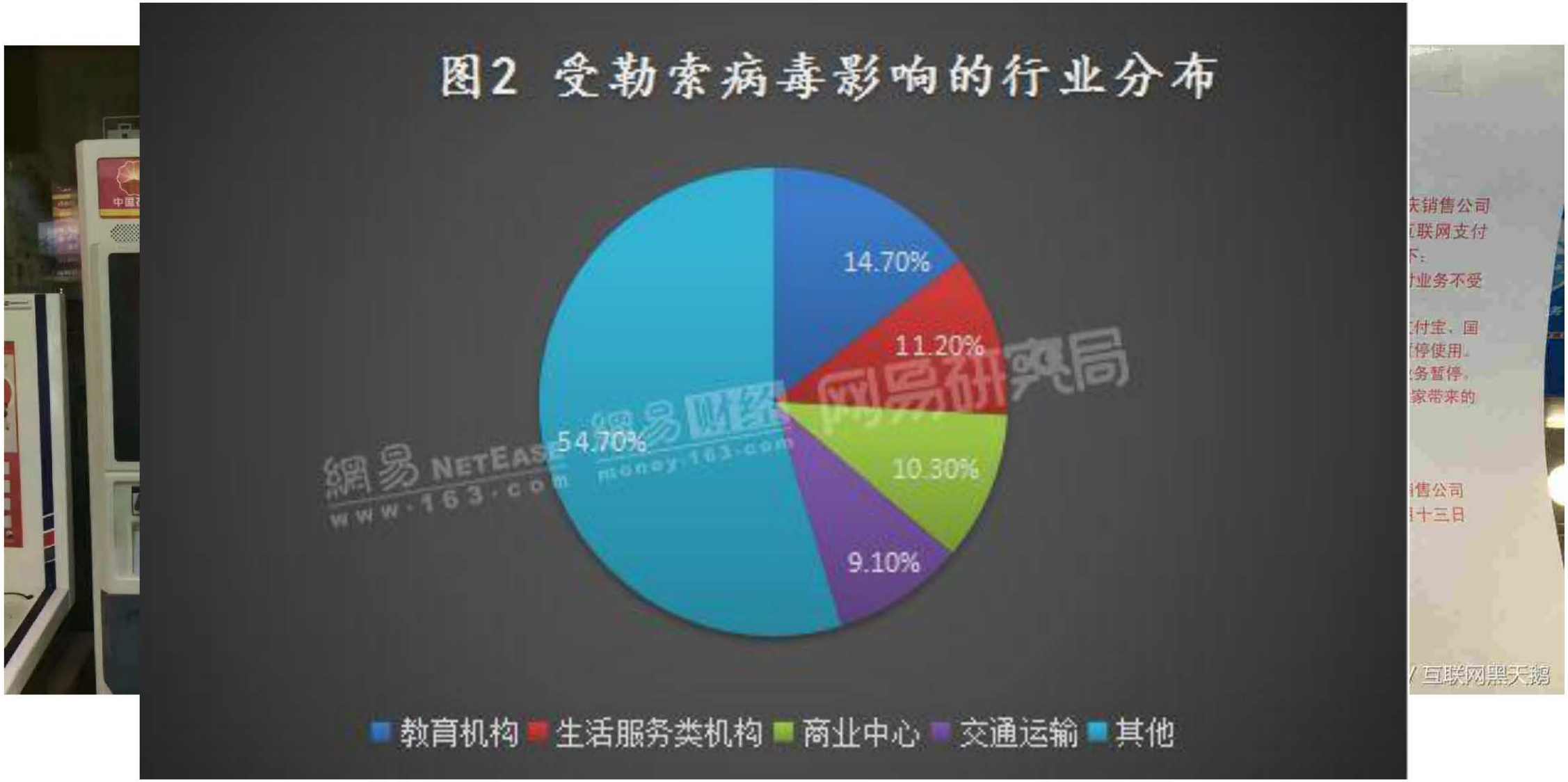
图 1　二滩水电厂"10.13"事故系统频率变化曲线

工控系统安全问题和现状

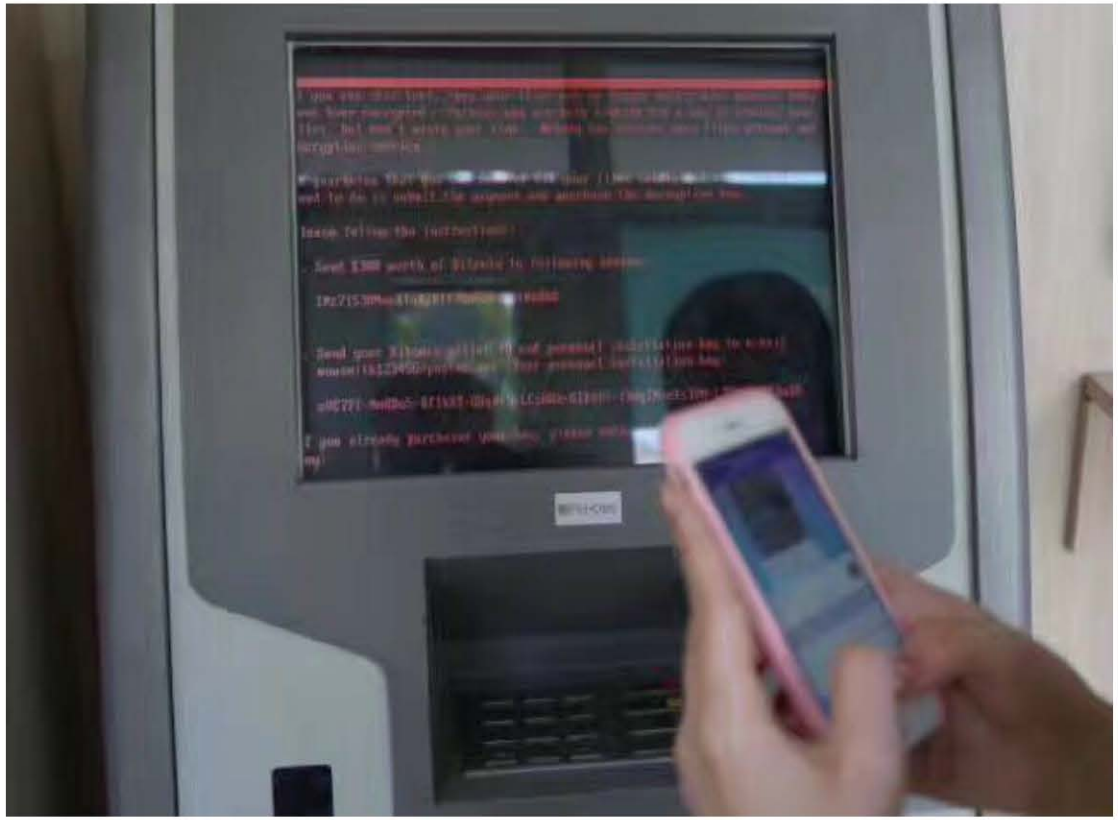
2010年

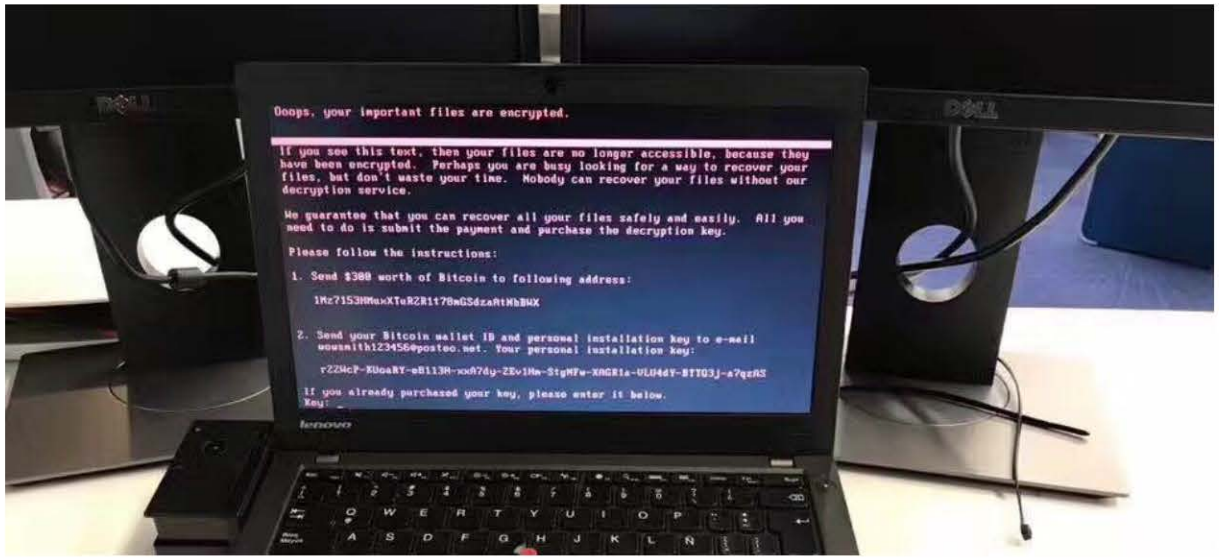
2016年

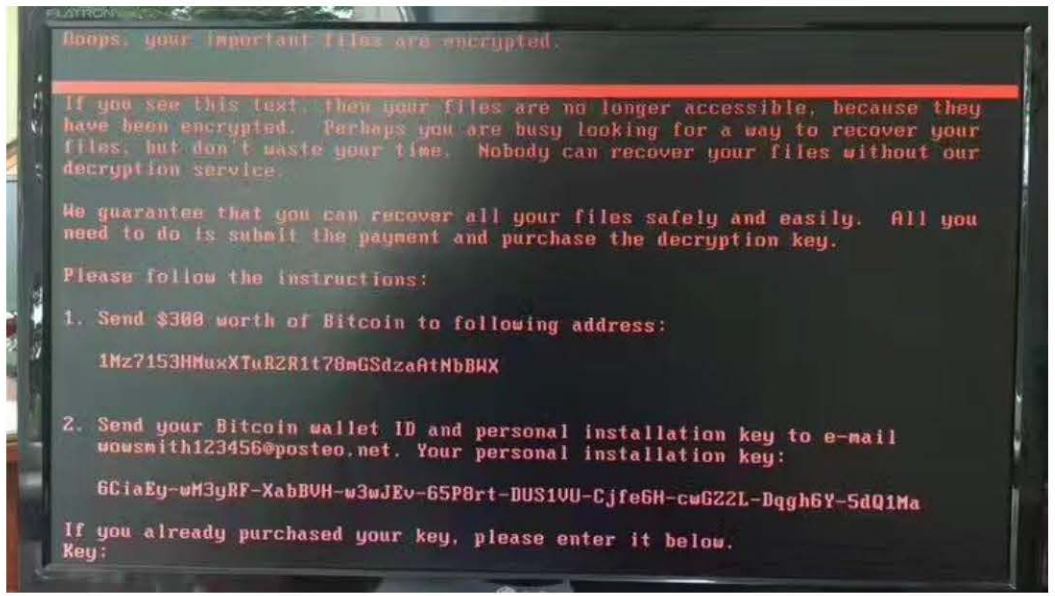
工控系统安全问题和现状



2017年6月乌克兰







北京时间 6月27 日 21:00消息，乌克兰境内包括国家储蓄银行(Oschadbank)、Privatbank 银行在内的几家银行机构、 电力公司 KyivEnergo 、国家邮政（UkrPoshta）遭受“未知病毒”大规模网络攻击。

2016年我国互联网网络安全态势

9.7万个木马和僵尸网络控制服务器控制了我国境内**1699万余**台主机

1Gbps以上DDoS攻击事件日均**452**起

通过自主捕获和厂商交换获得移动互联网恶意程序数量**205万余**个

恶意APP事件**8910**起

通用软硬件漏洞**10822**个(国家信息安全漏洞共享平台收录)，其中高危漏洞数量高达**4146**个(占38.3%)

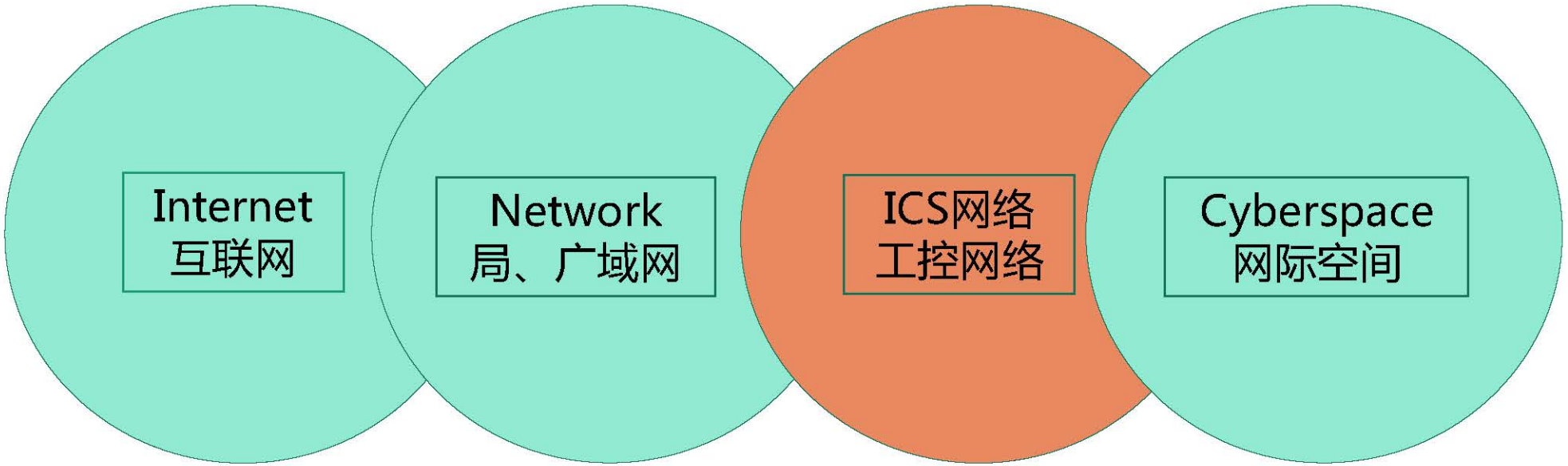
全年通报安全漏洞事件**24246**起

17.8万个针对我国境内网站的仿冒页面

（数据来源：国家互联网应急中心，《2016年我国互联网网络安全态势综述》）

目录

《网络安全法》的实施



《网络安全法》的“网络” 所涵盖的内容

《网络安全法》的实施

- 有关概念
  - 网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统
  - 网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力

- 有关概念
  - 网络运营者，是指网络的所有者、管理者和网络服务提供者
  - 网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据
  - 个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等

《网络安全法》的实施





第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

《网络安全法》的实施

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查

《网络安全法》的实施

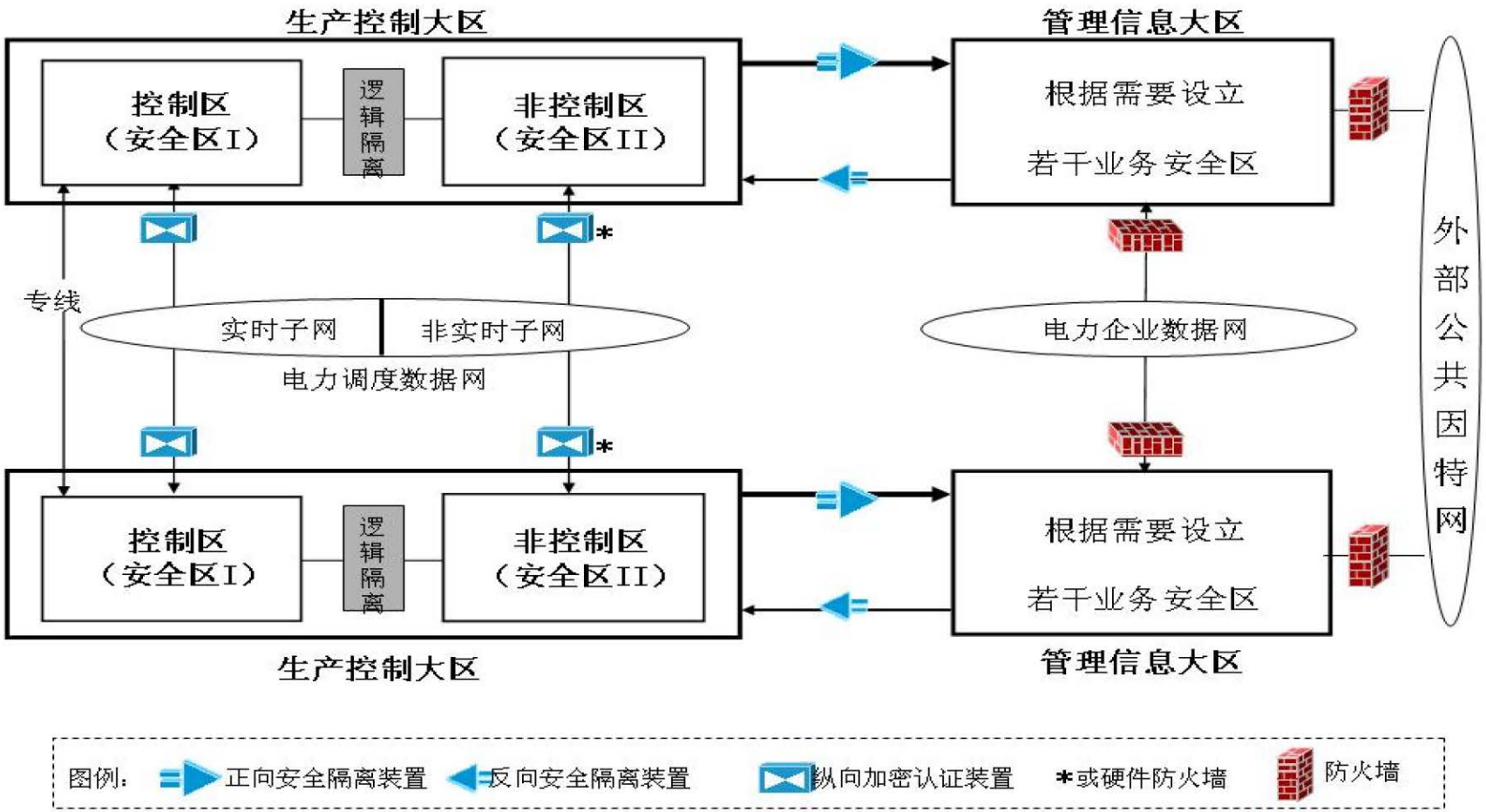
第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门

国家发改委2014第14号令，能源局2015第36号《电力监控系统安全防护规定》

第一章 总则
第二章 技术管理
第三章 安全管理
第四章 保密管理
第五章 监督管理
第六章 附 则

1．《电力监控系统安全防护总体方案》
2．《省级以上调度中心监控系统安全防护方案》
3．《地、县级调度中心监控系统安全防护方案》
4．《变电站监控系统安全防护方案》
5．《发电厂监控系统安全防护方案》
6．《配电监控系统安全防护方案》

电力监控系统安全防护的基本方针



十六字方针:
安全分区
网络专用
横向隔离
纵向认证

十六字方针
面临新的挑战

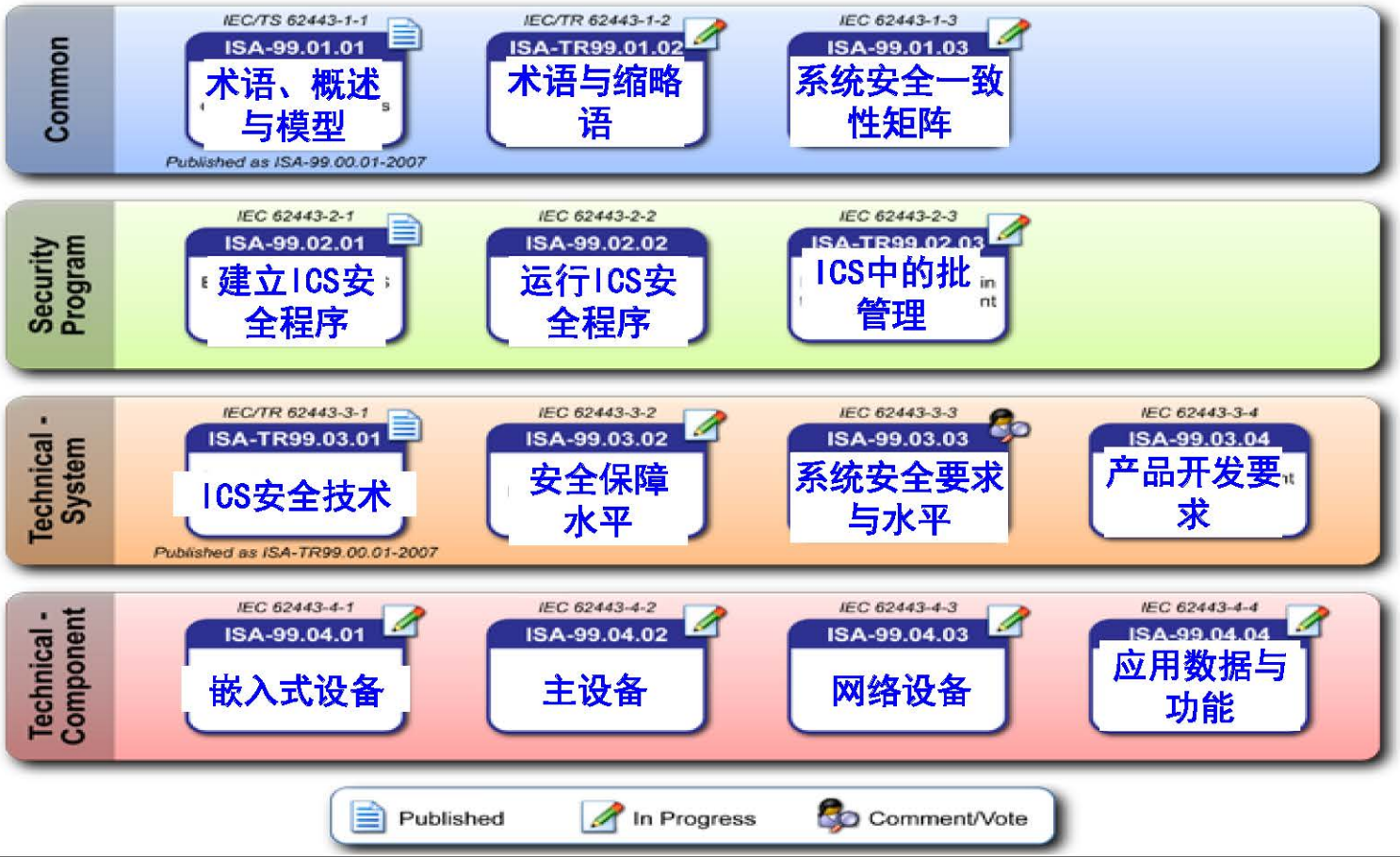
国外信息安全标准-IEC

ICS评估安全标准

ICS程序安全标准

ICS系统安全标准

ICS组件安全标准



我们国家目前还没有完整的工控安全标准体系

标准名称	制定者	内容概要	特点分析
IEC 62443系列《工业过程测量、控制和自动化 网络与系统信息安全》	IEC/TC65/WG10 与 ISA99 联合工作组	定义一个通用的、最小要求集以达到各级SALS安全保障需求。可指导工控系统集成商、产品提供商和服务提供商对他们的产品和服务进行安全性评估。	目前仅出台3份标准，主要是基础标准、策略和规程标准

工控安全相关的标准（制定中）

序号	标准名称	牵头单位
1	工业控制系统网络监测安全技术要求和测试评价方法	电子四院
2	工业控制系统网络漏洞检测技术要求	匡恩
3	工业控制网络安全隔离与信息交换系统安全技术要求	公安部三所
4	工业控制系统产品信息安全技术要求	中国信息安全测评中心
5	工业网络审计产品安全技术要求	公安部三所
6	工业控制系统风险评估实施指南	国家信息技术安全研究中心
7	工业控制系统安全分级指南	江南天安
8	工业控制系统安全防护技术要求和测试评价方法	三零卫士
9	工业控制系统测控终端安全要求	中国电力科学研究院
10	工业控制系统安全检查指南	中国信息安全测评中心
11	工业控制系统安全管理基本要求	电子四院
12	工业控制系统安全控制应用指南	国家信息技术安全研究中心
13	安全可控信息系统 电力系统安全指标体系	中国电力科学研究院
14	《信息安全技术等级保护基本要求》	
15	《信息安全技术 信息系统等级保护工业控制系统安全设计技术指南》	电子六所牵头
16	《信息安全技术 信息系统等级保护物联网安全设计技术指南》	电信研究院
17	《信息安全技术 信息系统安全等级保护基本要求物联网要求》	公安部一所
18	《信息安全技术 信息系统安全等级保护基本要求工业控制系统要求》	浙江大学 （电子六所参与）
19	《信息安全技术 信息系统安全等级保护测评要求工业控制系统要求》	能源局 （电子六所参与）
20	《信息安全技术 信息系统等级保护安全设计技术云计算指南》	阿里巴巴牵头
21	《智能制造综合标准化试验验证项目 “功能安全和工业信息安全标准研究和验证平台建设》	仪综所 （电子六所参与）
22	城市轨道交通系统信息安全技术体系建设规范	启明星辰、北京地铁设计院
23	城市轨道交通工业控制系统信息安全技术要求	启明星辰、北京地铁设计院
24	铁路站（场）局域网无线安全接入暂行技术要求制	铁总，启明星辰

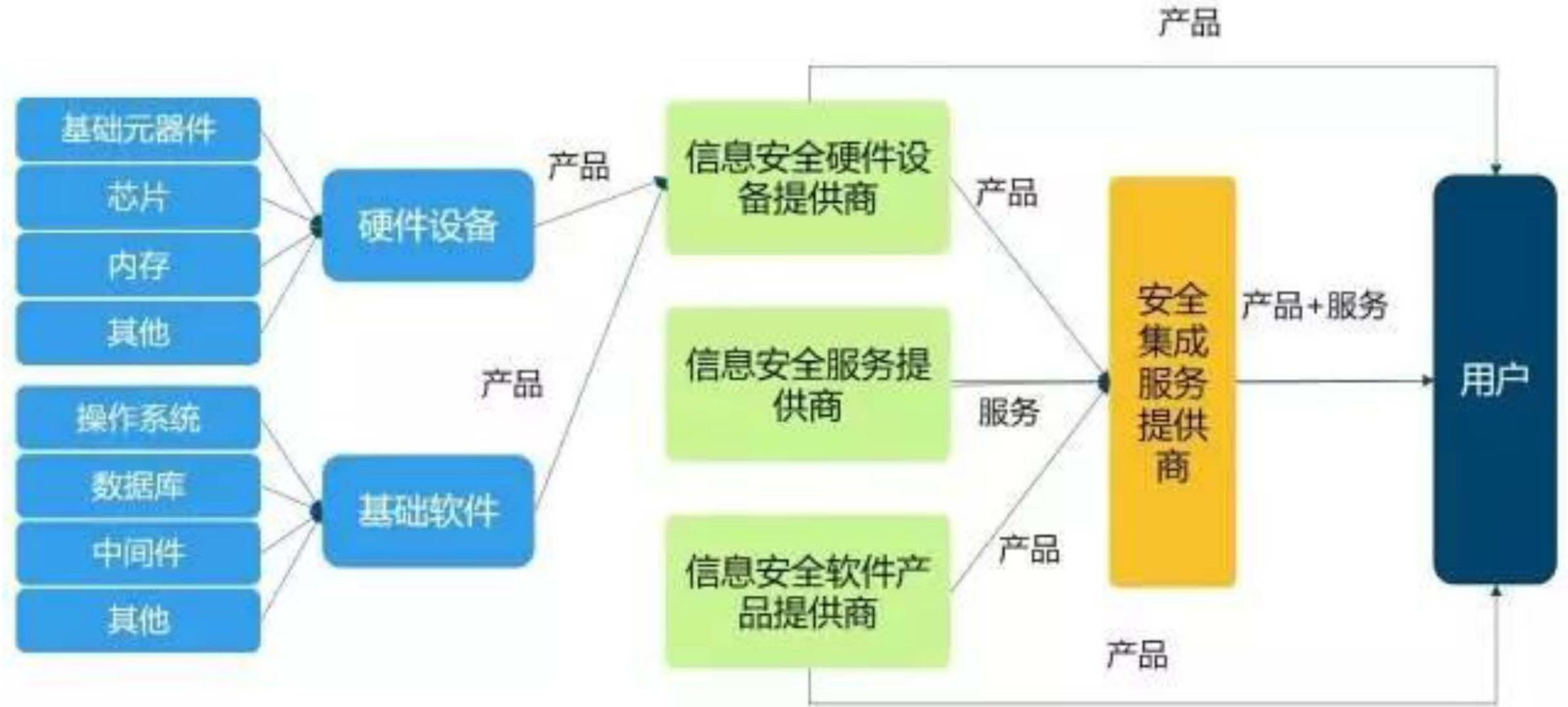
目录

能源局2015第36号《电力监控系统安全防护规定》

- 安全加固要求（增加了对主机与网络设备的加固要求）
- 边界防护问题（控制大区增加了入侵检测要求）
- 应用安全控制（对重要业务系统登录及访问进行控制，加强安全机制）
- 安全审计（控制大区增加了安全审计要求）
- 专用安全产品管理（增加了保密要求，关闭工控产品远程链接功能）
- 备份与容灾（增加了异地备份要求）
- 恶意代码防范（增加了恶意代码防范要求）

信息安全产品结构及分类

信息安全产业链


基础元器件
芯片
内存
其他
硬件设备
操作系统
数据库
中间件
其他
基础软件
产品
产品
信息安全硬件设备提供商
信息安全服务提供商
信息安全软件产品提供商
产品
服务
产品
安全集成服务提供商
产品+服务
用户
产品
产品

目录

网络安全威胁是“鼠”，工业安全生产是“器”

网络安全威胁是“鼠”，工业安全生产是“器”

●●●●○ 中国联通 08:18 93%
返回 关闭 江西丰城电厂事...
手机凤凰网 资讯频道

江西丰城电厂事故续：9人涉玩忽职守和行贿罪被捕(图)

2016-12-25 19:50 江西网络广播电视台 T大

华中能源监管局电力安全监管处处长张志祥等人涉嫌玩忽职守罪被逮捕

江西丰城电厂事故伤者正接受治疗(图) 打开

●●●●● 中国联通 4G 16:45 48%
返回 湖北通报当阳市电厂...
返回 国内快讯

湖北通报当阳市电厂致22死爆炸事故:14人被追责

2017-06-02 08:48:31 人气：177

中新社武汉6月1日电(马芙蓉 王有哲)湖北省政府新闻办6月1日召开新闻发布会，通报当阳市重大高压蒸汽管道裂爆事故调查处理情况。经调查认定，这是一起生产安全责任事故。

去年8月11日，当阳市马店矸石发电有限责任公司热电联产项目在试生产过程中，2号锅炉高压主蒸汽管道上的“一体焊接式长径喷嘴”(企业命名的产品名称，是一种差压式流量计，以下简称“事故喷嘴”)裂爆，造成22人死亡，4人重伤，直接经济损失约2313万元(人民币，下同)。

首页 历史 我的 发布

●●●●○ 中国联通 08:24 95%
返回 国家能源局对国家电...
中国青年网

国家能源局对国家电网公司开展安全监管约谈

2017-05-17 19:27 中国新闻网 A+

中新网5月17日电 据国家能源局网站消息，近期，国家电网公司连续发生多起安全事故，安全生产工作有滑坡倾向。为督促企业落实安全生产主体责任，提高安全生产水平，5月17日，国家能源局依据有关规定对国家电网公司开展了安全监管约谈。

●●●●○ 中国联通 06:52 92%
返回 光伏們

存在重大隐患，山东43座光伏、风电电站被强制断网

2017-03-31 王超 光伏們

在过去一年，山东能源监管办对当地的风电、光伏电站进行多次现场核查，并要求相关电站就相核查出来的问题进行整改。经过数月时间过后，43个光伏、风电电站存在重大隐患且未整改，山东电力调度控制中心已在2017年3月28日下午起，将这些新

网络安全威胁是“鼠”，工业安全生产是“器”

家庭储备药品越多越安全	只要对症，用药不必因人而异	药越贵越好，剂量越大病好得越快	互为禁忌的药品同时服用	盲从广告
网络安全设备并非越多越好	专门的防护设备也需要结合系统情况	价格不是网络安全设备优劣的标志	相同和复合功能设备的选用要谨慎	忽悠（fool you）

我国信息安全行业市场规模

数据来源：智研咨询《2017-2022年中国信息安全行业市场分析预测及投资前景分析报告》

目录

治病用药的三个关键因素

治病用药的三个关键因素

关注药效

关注副作用

关注服用方法

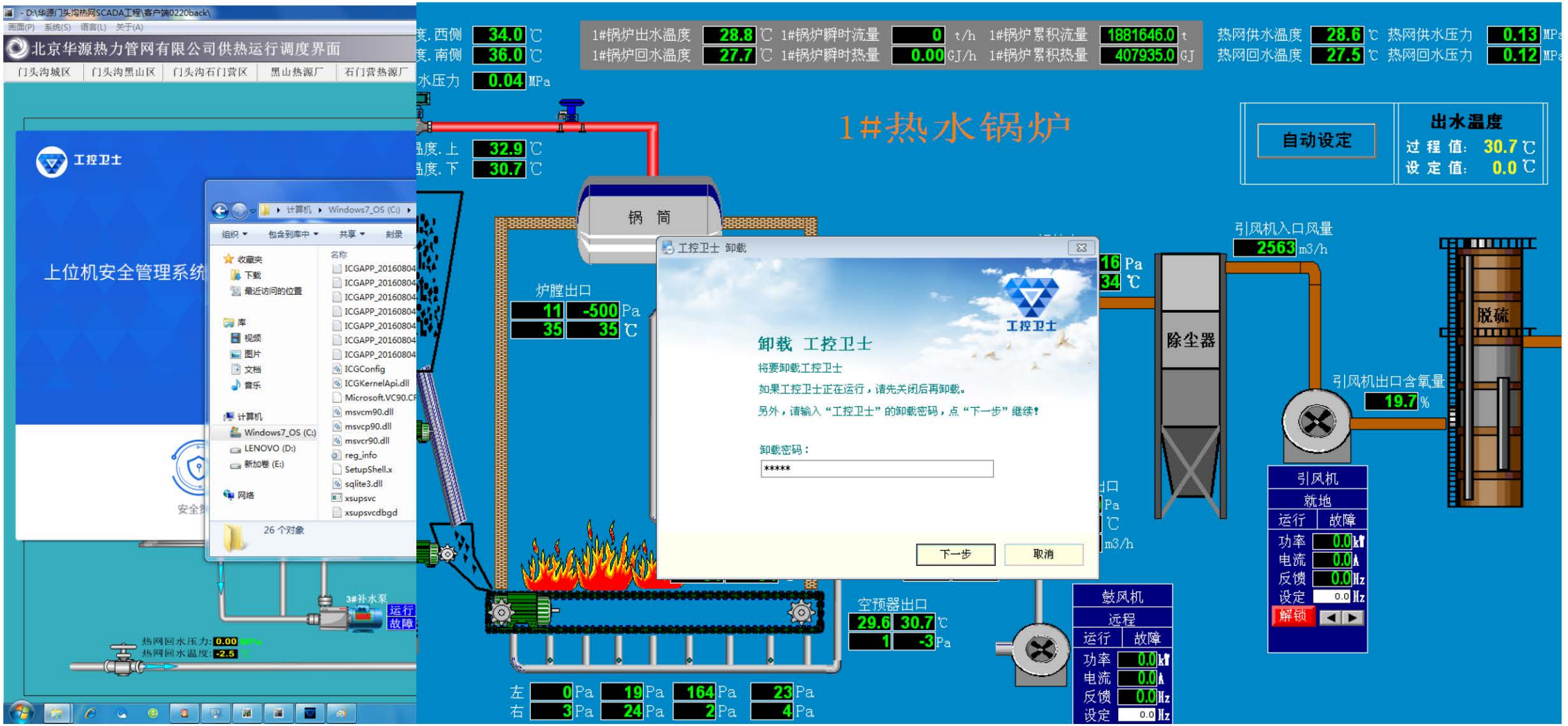
我们需要什么？

工业控制系统信息安全实验基地

工业控制系统信息安全实验基地

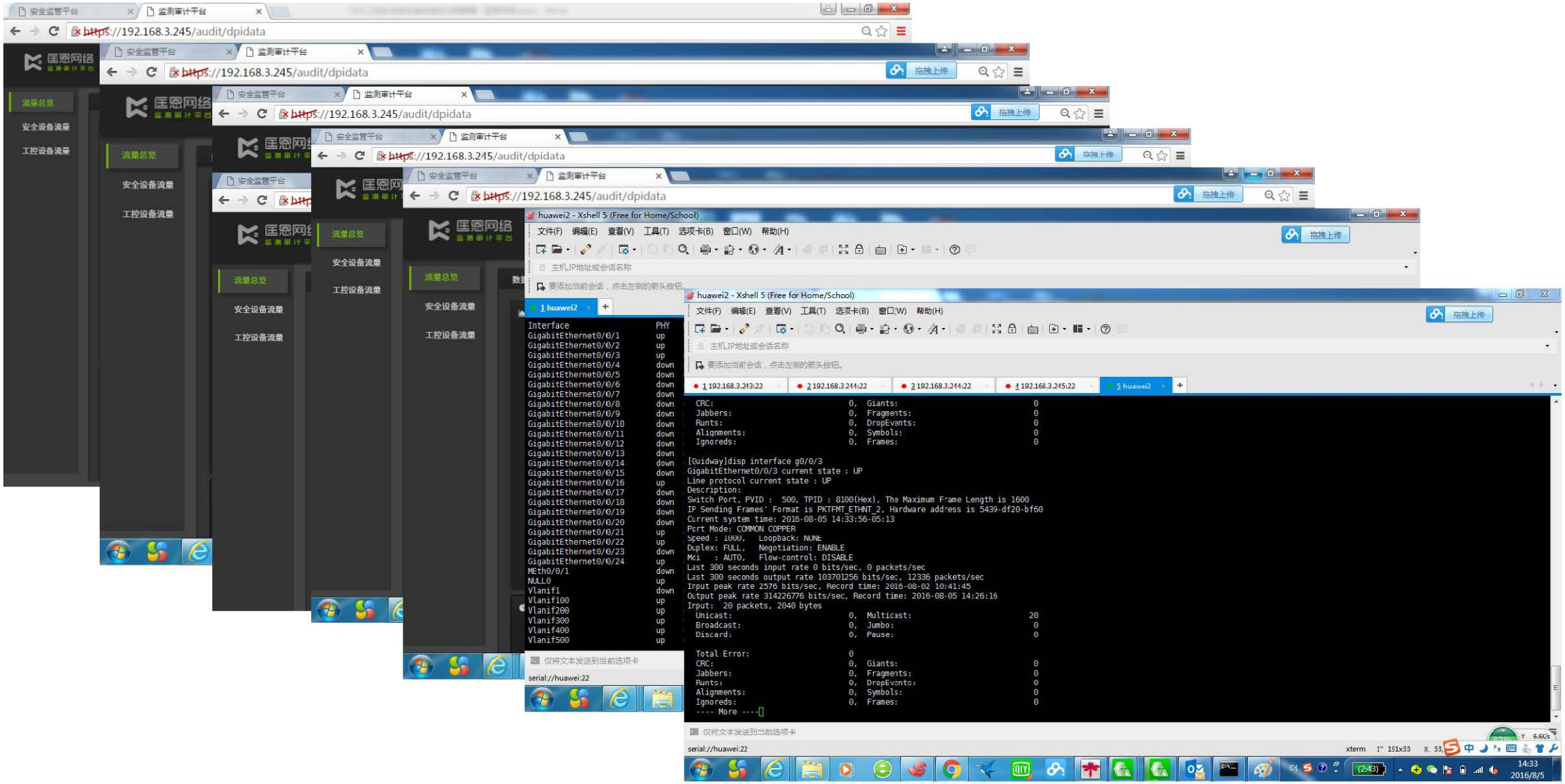
工业控制系统信息安全实验基地

工业控制系统信息安全实验基地

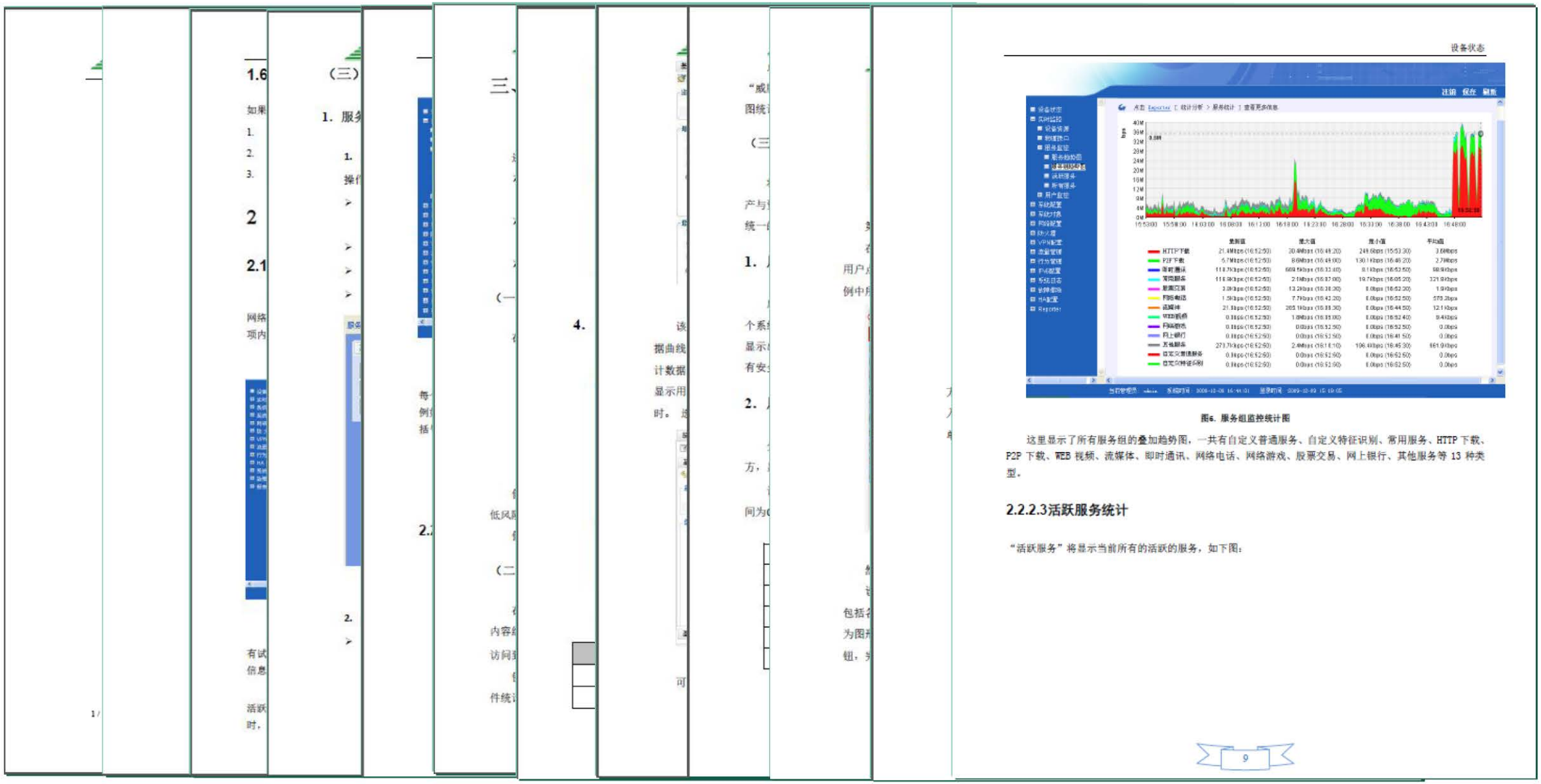


工业控制系统信息安全实验基地

工业控制系统信息安全实验基地



工业控制系统信息安全实验基地



设备状态

图6. 服务组监控统计图

这里显示了所有服务组的叠加趋势图，一共有自定义普通服务、自定义特征识别、常用服务、HTTP 下载、P2P 下载、WEB 视频、流媒体、即时通讯、网络电话、网络游戏、股票交易、网上银行、其他服务等 13 种类型。

2.2.2.3活跃服务统计

“活跃服务”将显示当前所有的活跃的服务，如下图：

目录

技术上降低“脆弱性”，制度上降低“威胁”

当前火电厂控制系统信息安全工作策略探讨

原创 2017-05-31 侯子良

CAA发电自动化

【摘要】：本文从火电厂控制系统特点出发，指出控制系统信息安全防护与互联网系统信息防护应具有不同安全工作策略，并对当前控制系统供应侧和应用侧两个信息安全战场互相协调和促进进行了探讨。最后，作者还对控制大区和管理大区隔离问题以及DCS信息安

一、我国工业控制系统信息安全发展态势

从2011年底起，国家各部委发布了一系列关于工业控制系统信息安全的文件，把工控信息安全列为“事关经济发展、社会稳定和国家安全”的重要战略，受到国家层面的高度重视。

当前面临的困难是：

1、从事安全信息产业的公司大多不太熟悉特点各异的各行业工控系统，有时还不免把工控系统视作一个互联网信息系统去思考和防护；

2、而从事工控系统应用行业的人们大多还来不及了解信息安全技术，主导制订本行业的相关标准和本行业控制系统信息安全的工作策略，并推动两支力量的紧密配合。

技术上降低“脆弱性”，制度上降低“威胁”

当前火电厂控制系统信息安全工作策略探讨

原创 2017-05-31 侯子良

CAA发电自动化

【摘要】：本文从火电厂控制系统特点出发，指出控制系统信息安全防护与互联网系统信息防护应具有不同安全工作策略，并对当前控制系统供应侧和应用侧两个信息安全战场互相协调和促进进行了探讨。最后，作者还对控制大区和管理大区隔离问题以及DCS信息安

二、 从工控系统特点出发正确制订信息安全发展策略

对于一般互联网信息系统，分布地域极广，接触人员多而杂，因此信息安全策略重点，除了在适当地点采取一些防火墙等隔离措施外，主要提高自身健壮性，以及查杀病毒等措施。

对于工控系统，特别是火电厂控制系统，它与外部互联网联系较少，分布地域有限，接触人员较少。

因此，对火电厂可以也应该首先把重点放在为控制系统营造一个良好环境上。也就是说，尽可能与充斥病毒和恶意攻击的源泉隔离，包括从互联网进来的外部风险入侵，以及企业内外人员从内部的直接风险入侵。

前者可采取电力行业中证明行之有效的硬件网络单向传输装置（单向物理隔离装置）等技术手段；后者则主要通过加强目前电厂内比较忽视和薄弱的信息安全管理措施。火电厂控制系统采取这种信息安全策略可以达到事半功倍的效果。

技术上降低“脆弱性”，制度上降低“威胁”

当前火电厂控制系统信息安全工作策略探讨

原创 2017-05-31 侯子良

CAA发电自动化

【摘要】：本文从火电厂控制系统特点出发，指出控制系统信息安全防护与互联网系统信息防护应具有不同安全工作策略，并对当前控制系统供应侧和应用侧两个信息安全战场互相协调和促进进行了探讨。最后，作者还对控制大区和管理大区隔离问题以及DCS信息安

三、火电厂控制系统供应侧和应用侧两个信息安全战场的不同策略及相关协调

火电厂控制系统，主要是DCS，不仅是保证功能安全的基础，也是提高自身健壮性，确保信息安全的关键。

•DCS供应侧，注重增量的市场：

在DCS供应侧提高自身健壮性，并通过验收测收，确保系统信息安全有许多明显的优点。它可以非常协调的融入信息安全策略，可以离线进行危险性较大的渗透性测试等。

DCS供应侧在提高信息安全方面积累的经验和措施，培养起来的队伍，也将有助于现有电厂DCS的测试评估，以及安全加固等直接升级服务或指导服务。

技术上降低“脆弱性”，制度上降低“威胁”

当前火电厂控制系统信息安全工作策略探讨

原创 2017-05-31 侯子良

CAA发电自动化

【摘要】：本文从火电厂控制系统特点出发，指出控制系统信息安全防护与互联网系统信息防护应具有不同安全工作策略，并对当前控制系统供应侧和应用侧两个信息安全战场互相协调和促进进行了探讨。最后，作者还对控制大区和管理大区隔离问题以及DCS信息安

•火电厂DCS应用侧，是当前最紧迫面临现实信息安全风险：

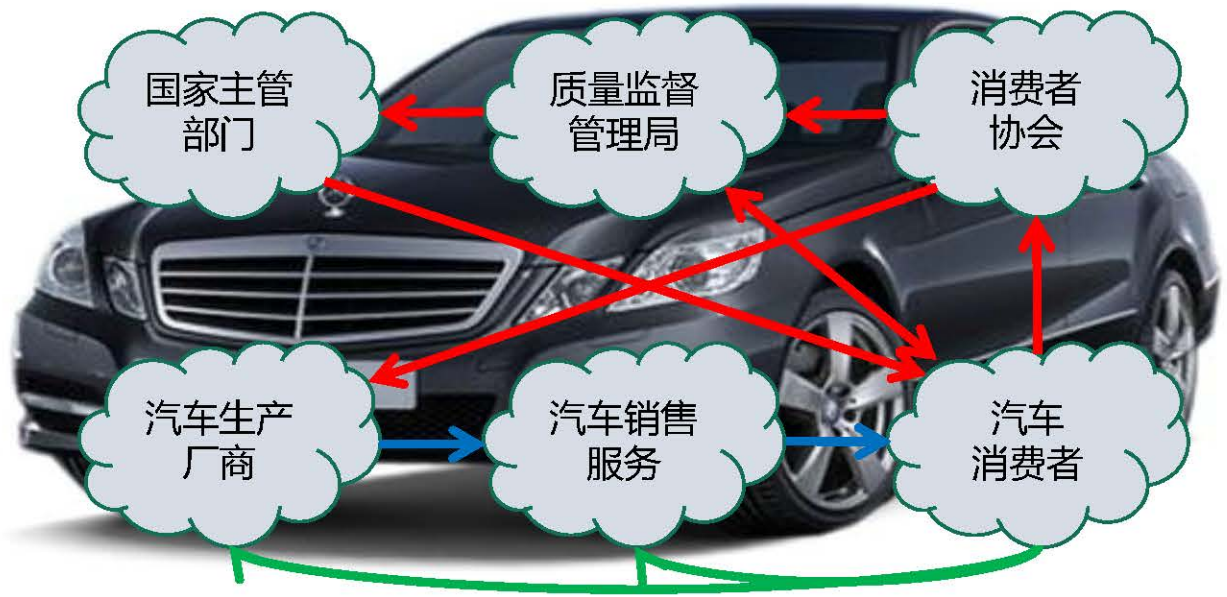
1．应迅速全面开展下列两方面工作

1）全面核查DCS与SIS及互联网间是否真正贯彻落实了发改委2014年14号令和国家能源局2015年36号文附件中关于配置单向物理隔离的规定，没有加装必须尽快配置，已配置的要检查是否符合要求。

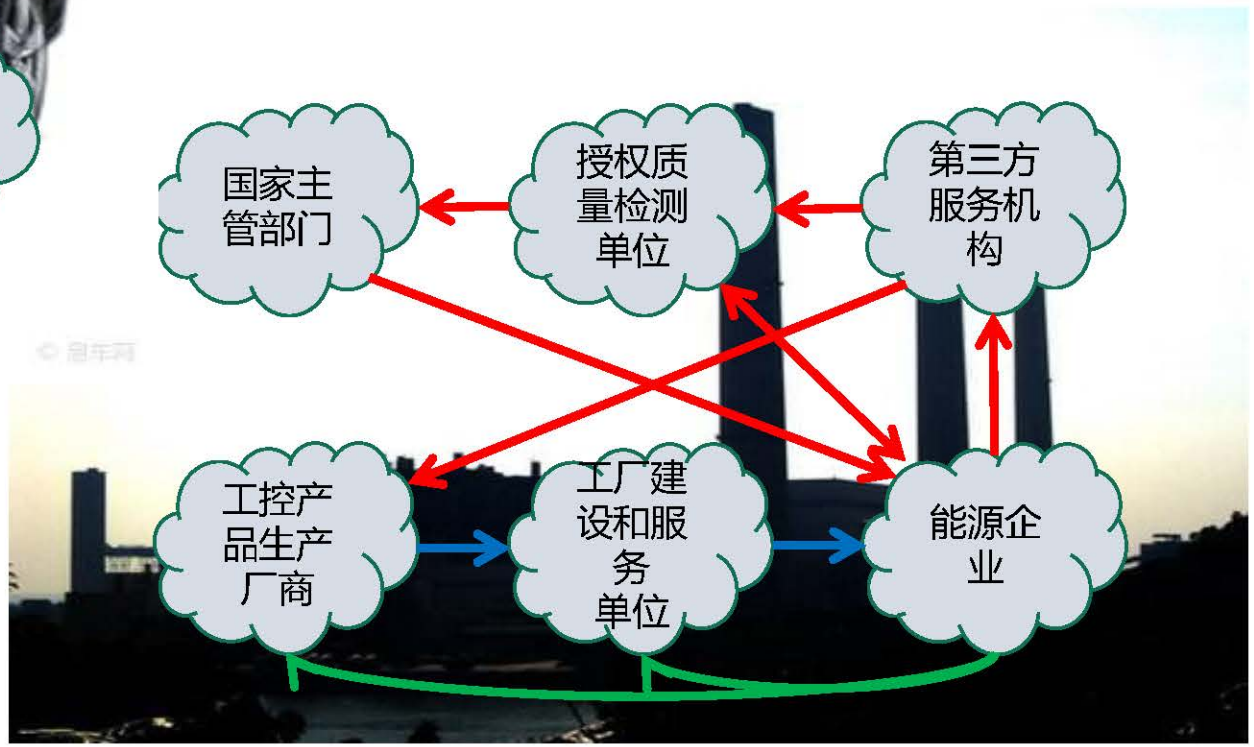
2）迅速按照《工业控制系统信息安全防护指南》加强内部安全管理，杜绝内部和外部人员非法接近操作、介入或在现场总线及其它接入系统上偷挂攻击设备等，并适度开展一些风险较小的安全测评项目。

2.通过试点，逐步开展对已运DCS进行较为深入的安全测评，适度增加信息安全技术措施，待取得经验后，再组织力量全面推广，把我国火电厂控制系统信息安全提高到一个新的水平。为此，建议针对国内火电厂应用的各种型号的DCS品牌出发，各大电力集团互相协调，统筹规划，选择十个左右试点电厂，由应用单位上级领导组织，国家级或重点的测评机构、实验室技术指导，相关DCS供应商、优秀信息安全产品生产商以及电厂负责DCS的工程师一起成立试点小组。

技术上降低“脆弱性”，制度上降低“威胁”



汽车成熟的安全生产价值链

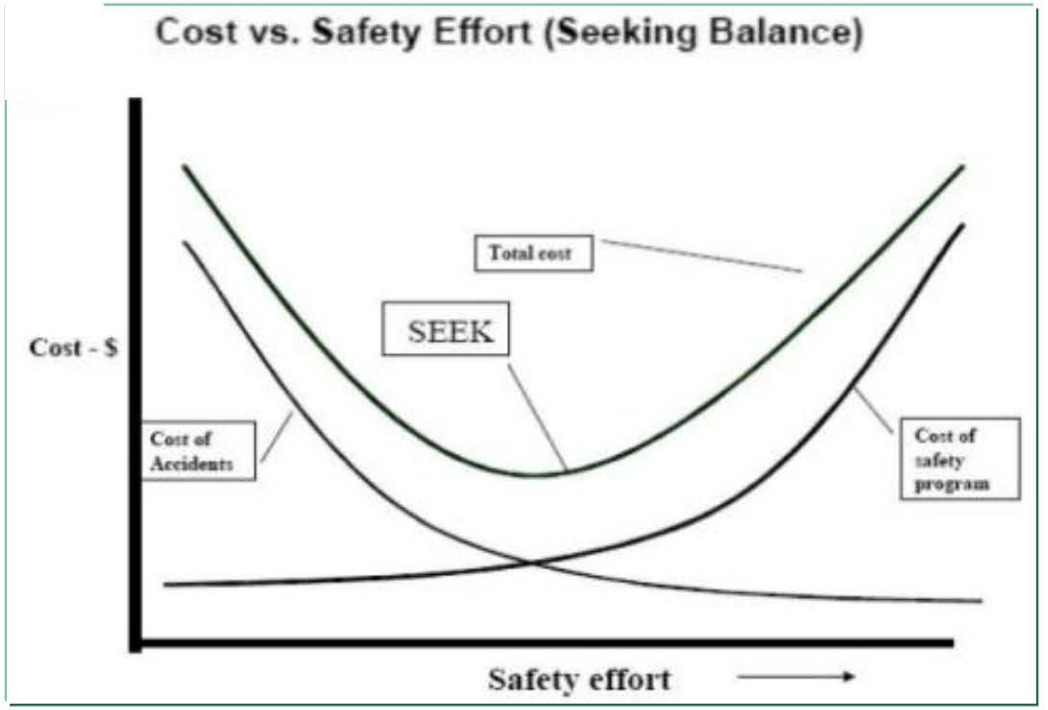


工控安全生产价值链的建立

技术上降低“脆弱性”，制度上降低“威胁”

风险=威胁 X 脆弱性

投资与风险控制适度



中国华能
CHINA HUANENG

谢谢！

郭森

北京 西城