构筑网络安全防御纵深
护航电力工控网络安全

中国长江电力股份有限公司
张家治

长江电力：三峡集团控股的公司，负责6座水电站的运营管理。

愿景：做世界水电行业的引领者

中国最大的
电力上市公司

全球最大的
水电上市公司

葛洲坝电站：“万里长江第一坝“，位于长江干流中游西陵峡出口，是三峡电站的反调节水库。奠基于七十年代初，竣工于八十年代末，是华中地区的枢纽电站和重要电源点。

一、电力工控网络安全面临的形势

二、电力工控网络安全的防护策略

三、电力工控网络安全发展的展望

一、电力工控网络安全面临的形势

电力系统重要性

电力是工业的命脉，是国民经济的第一基础产业，对促进国民经济的发展和社会进步有着重要作用，关系到国家经济安全、社会的稳定、人们的日常生活。

楼上楼下，电灯电话

电力系统是敌对国家间攻击的首要目标

攻击面广、影响范围大、经济损失大、

对社会秩序的重大破坏

------看不见硝烟的战场

电力行业典型网络攻击案例

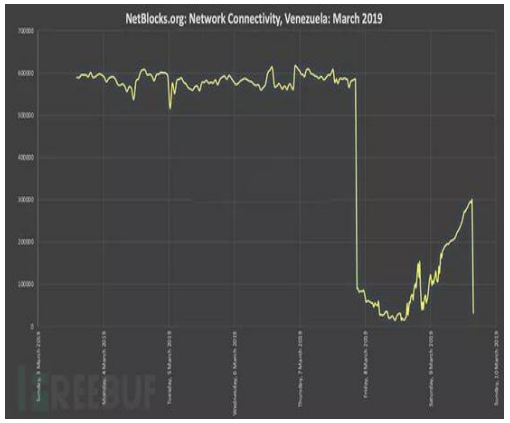
➢ 伊朗震网

2010 年 6 月，一个名为 Stuxnet 处于休眠状态的病毒潜伏在伊朗的铀浓缩设施网络中，Stuxnet 在位于纳坦兹的离心机中被激活，控制了30%的纳坦兹设施的计算机，致使伊朗暂时关闭了核设施和核电厂，震网病毒感染了全球超过20万台电脑，摧毁了伊朗浓缩铀工厂五分之一的离心机。

➢ 乌克兰大停电

2015年12月23日，乌克兰电网遭网络攻击，受影响家庭70万户，这是有史以来首次导致大规模停电的网络攻击。以BlackEnergy等相关恶意代码为主要攻击工具，以邮件发送恶意代码载荷为最终攻击的直接突破入口，最后达成长时间停电并制造社会混乱的具有信息战水准的网络攻击事件。

➢ 委内瑞拉大停电



2019年3月7日，委内瑞拉发生全国范围的大规模停电，全国18个州电力供应中断，仅有5个州幸免，停电给委内瑞拉带来了重大损失，全国交通瘫痪，地铁系统关闭，医院手术中断，所有通讯线路中断，航班无法正常起降。

➢ 纽约大停电

2019年7月，纽约停电4个小时

黑客闯入了纽约市三十多个变电站的控制中心，并对控制中心进行信息战破坏，导致了纽约全城大约4个小时的停电。这是几十年来的第一次大规模停电造成混乱。

几起攻击的共同点：利用先进的计算机及网络技术对电力工控系统进行控制和破坏。

习总书记的网络安全观

习近平总书记指出，没有网络安全就没有国家安全，没有信息化建设就没有现代化。建设网络强国，要有自己的技术，过硬的技术；要有丰富全面的信息服务，繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济。作为支撑信息化建设的网络基础设施，网络安全是其中的核心。

电力工控网络现状

- **工业化、信息化两化融合**
- **云大物移智**
- **智能电网建设 “一次设备智能化，二次设备网络化”**

在互联互通、纵向集成等新的生产模式下，关键基础设施正逐渐暴露于互联网中，工控系统下的安全问题逐渐显现，包括软件隐患、网络边界隐患、环境和硬件隐患、网络安全协议问题、操作系统补丁更新不及时问题、不安全的远程访问等。

网络是一把双刃剑，在提高我们生产效率的同时，也可能产生巨大的破坏。但我们不能因噎废食，要直面问题，稳步发展，做好网络安全工作。

二、电力工控网络安全的防护策略

电力工控网络防护与传统IT安全的不同点

安全优先级：

- 工控系统网络安全焦点问题是生产过程稳定可靠，强调的是可用性，不能停产，不能发生生产安全事故
- 工控系统网络通讯协议不同，大量的工控系统采用私有协议。要求实时高效，多采用明文通信.
- 系统运行环境不同，工控系统运行环境相对落后，对系统稳定性要求高。
- 工控系统安全优先级为可用性>完整性>机密性，传统IT系统的优先级由机密性>完整性>可用性。

安全防护特点：

- 工控网络通常不允许直接连接互联网，不具备及时更新病毒库的条件。
- 工业控制系统通常不允许在生产运行期间进行系统升级。
- 病毒误杀在工业控制系统中可能产生致命的后果。
- 为防止网络中断对生产造成的影响，工控网络安全设备更多的是监视、报警、分析；而传统的IT安全设备可采取断网等措施，阻断威胁更有效。

电力工控网络面临的主要威胁

便携笔记本	USB移动存储	远程维护
内部员工	WLAN无线连接	网络入侵

……

电力工控网络防护策略

作为企业来讲，网络安全防护，重点在防护，决定了这是一场防御战。敌人在何方，何时发动何种攻击，我们无从知晓。

我们能做的就是，练就金刚不坏之身。任凭风吹浪打,我自岿然不动。

2018年-2019年，我们和天融信一起制定并实施了《葛洲坝电站电力工控安全防护方案》

特点：实现了电力工控系统全方位、立体、多层次的纵深防御

政策指导

《中华人民共和国网络安全法》

《中华人民共和国密码法》

《关键信息基础设施安全保护条例》（征求意见稿）

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

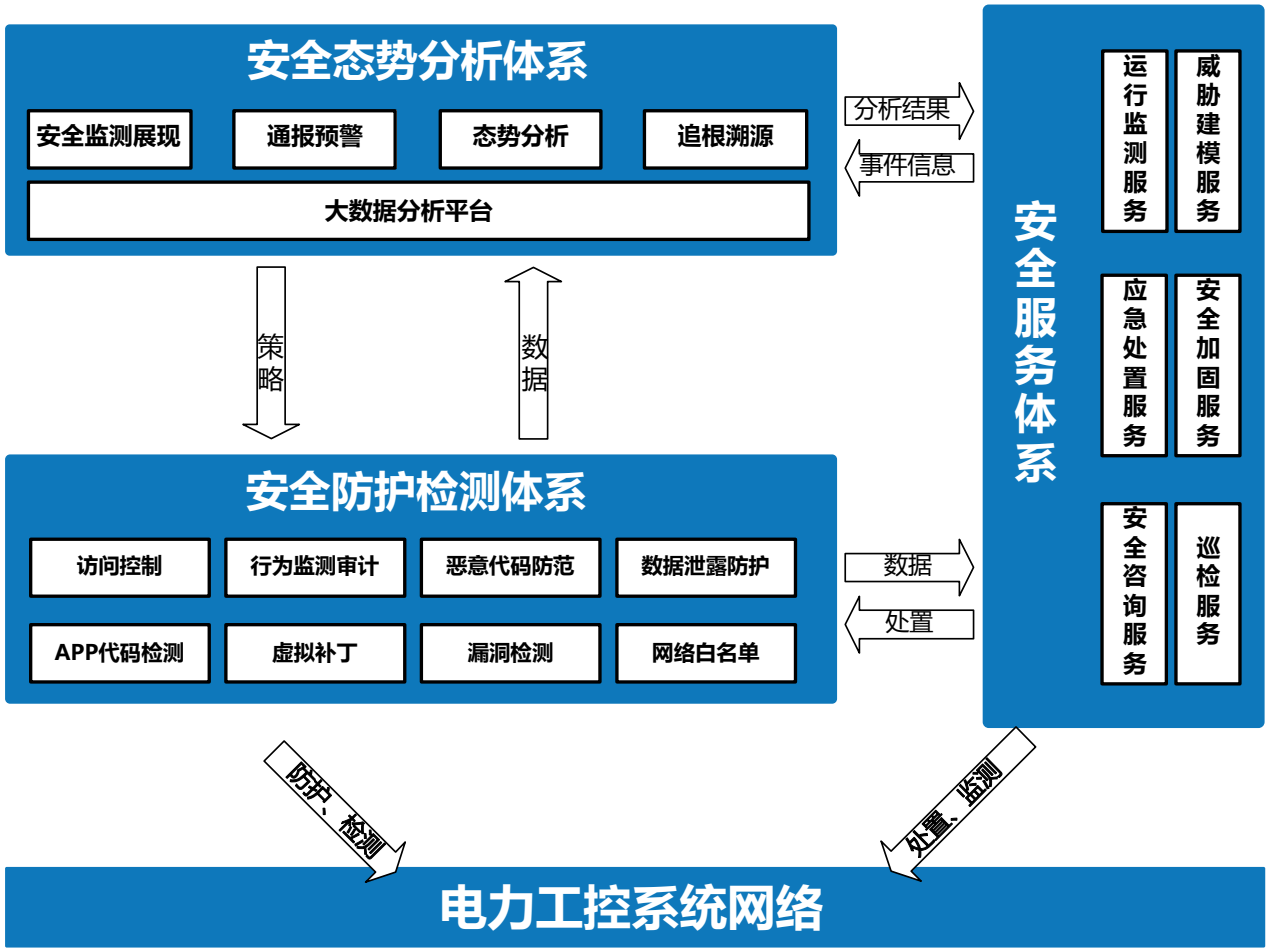
《电力监控系统安全防护规定》(发改委2014第14号令)

《电力监控系统安全防护总体方案》（国能安全〔2015〕36号）

《电力监控系统网络安全防护导则》（GB/T 36572-2018）

《电力信息系统安全检查规范》（GB/T 36047-2018）

防护框架



安全防护检测体系

安全防护检测体系包含网络中的安全防护设备、管理设备、感知设备等，防护、检测范围覆盖工业互联网体系结构，对各个层面分别提供对应的安全能力。

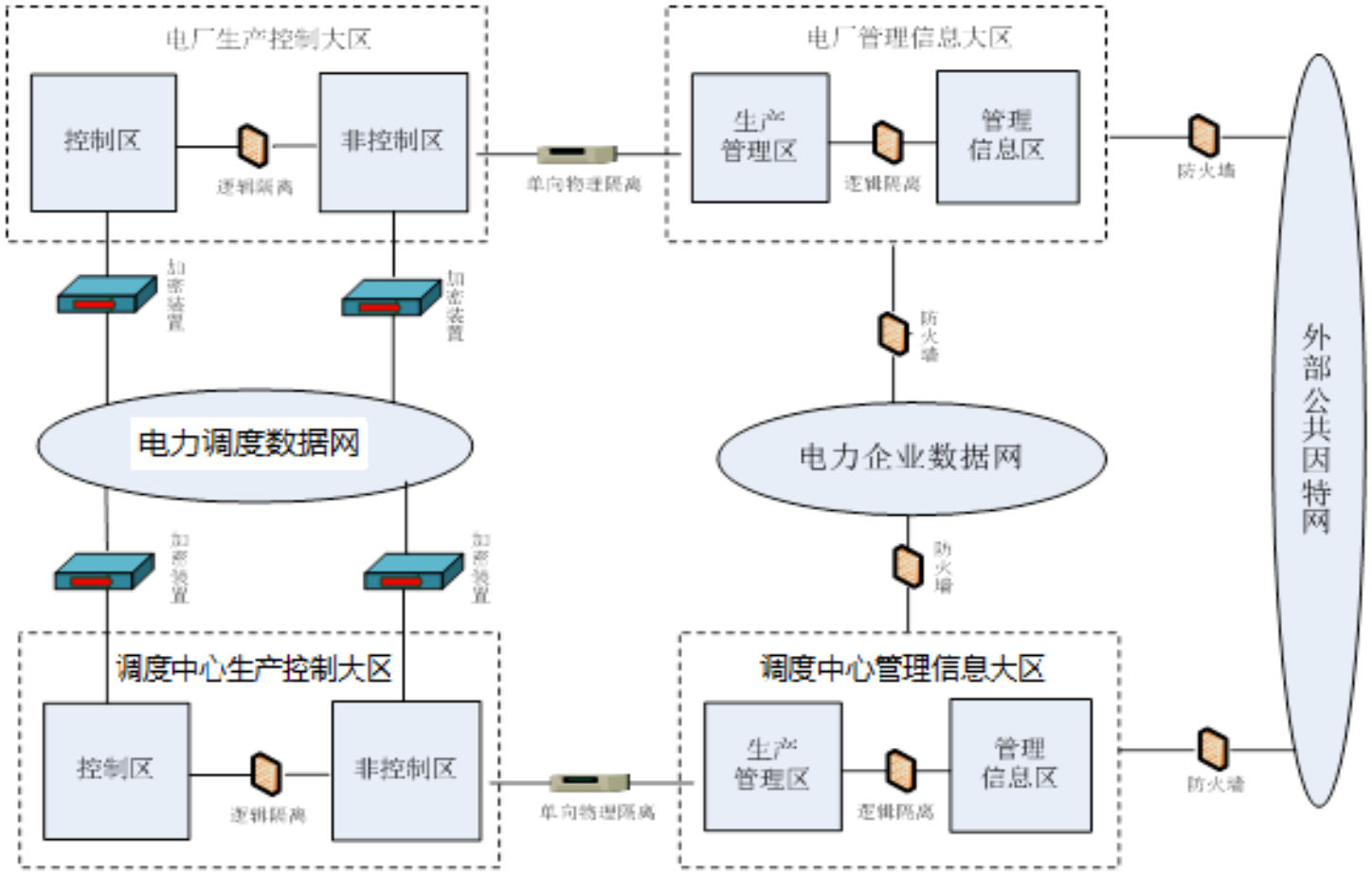
安全态势分析体系

安全态势分析体系作为工业互联网安全防护的“大脑”，承担安全信息分析及统计的的作用，并对其他体系提供信息的支持。

安全服务体系

安全服务体系包含运行监测中心、应急响应团队以及整体安全管理执行机构。

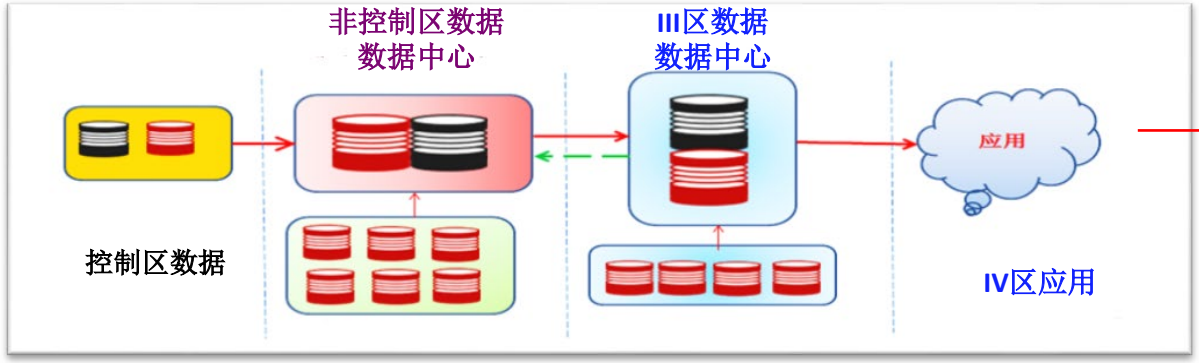
防护策略：　安全分区，网络专用，横向隔离，纵向认证

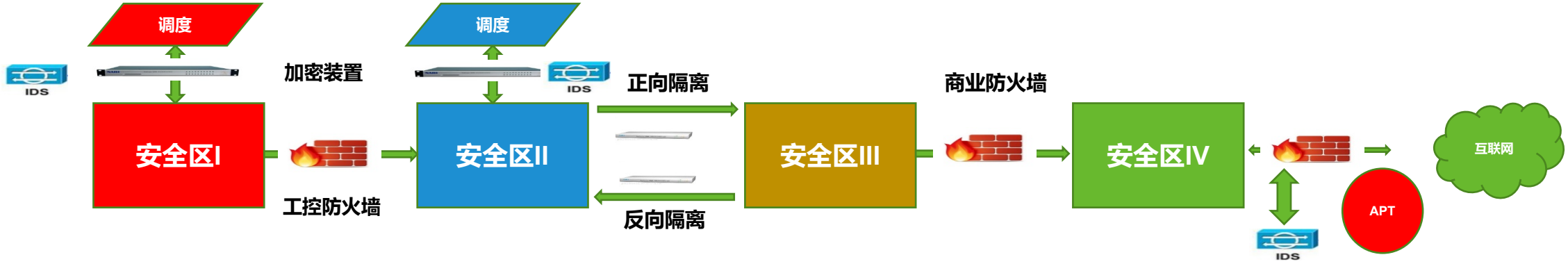


电力工控网络防护策略

边界防护

- 隔离装置
- 加密装置
- IDS
- 防火墙





电力工控网络防护策略

本体防护

系统加固：核心服务器、边界服务器进行系统加固，安装操作系统加固软件，同时对操作系统、应用系统的服务、用户、权限、端口等采取最小化策略。

漏洞扫描：安全区I和安全区II分部配置一台脆弱性检测设备,采用**在线部署，离线扫描**方式。

行为管控

安全卫士：安全区I、安全区II、安全区III范围内所有操作员终端配置安全卫士，实现对操作终端的进程、文件、内存、权限等进行全面掌控，对U盘进行识别管控，防止摆渡式攻击。

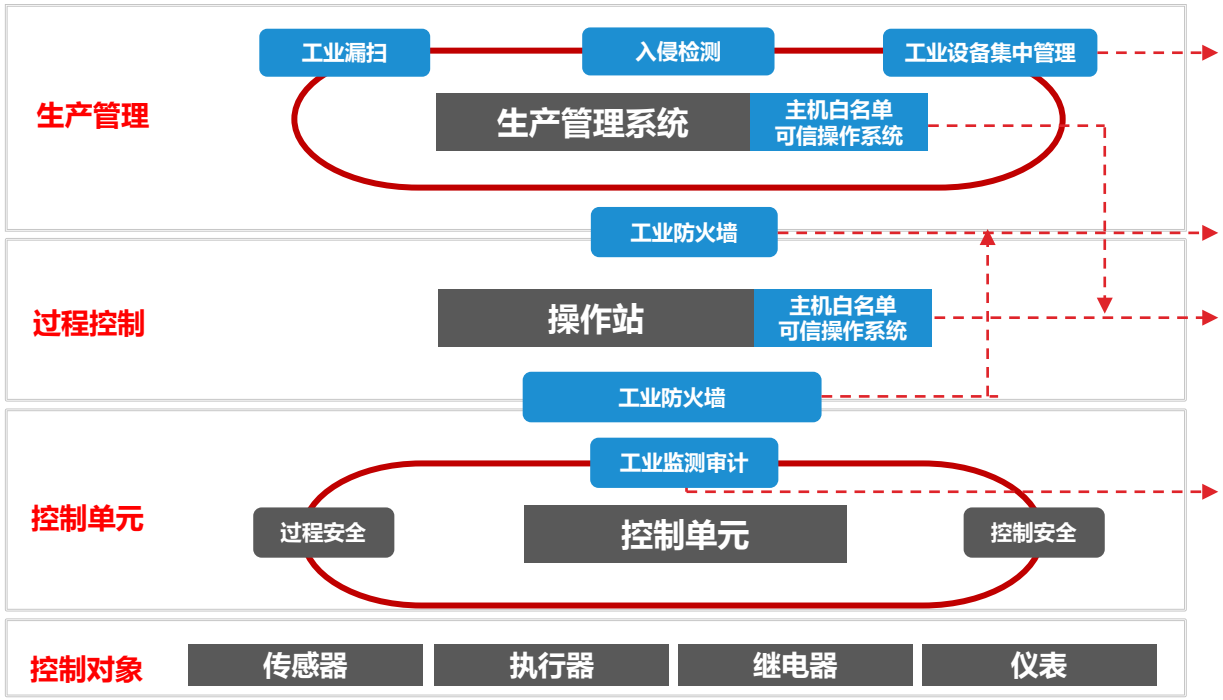
监测审计：采用软硬件一体的行为监测审计设备，实现攻击异常检测；无流量的异常检测；工控协议规约检测；重要操作行为审计；网络会话审计；原始告警报文记录；告警日志审计等。

联动防御

统一管理平台：统一管理工控安全设备，提供统一策略配置，并支持集中收集日志统一分析。

信息联动：将安全日志信息上送至电网调度中心（国家电网调〔2017〕1084号文）、公司安全监管平台，进行监视分析，实现全公司、全电网的网络安全态势感知。

电力工控网络安全运营体系



STEP3:安全管理：集中管理平台（策略管理+事件管理+策略管理）

STEP3:辅助安全：漏洞扫描、入侵检测等

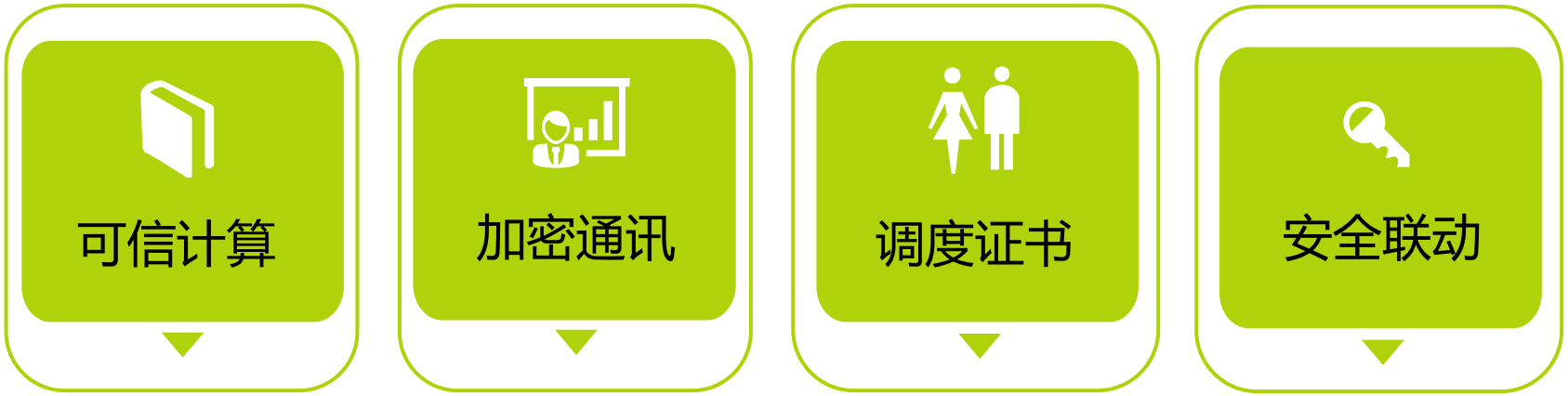
STEP1:控制区域间边界：区域隔离（基于协议还原解析的访问控制）

STEP2:计算环境：可信操作系统；主机白名单（应用）

STEP2:控制区域内部：行为监测（基于协议还原解析的行为分析）

三、电力工控网络安全发展的展望

三、电力工控网络安全发展的展望



魔高一尺道高一丈

攻击、防御相辅相成

网络安全工作中，我们要注重情报分析，拥抱技术，通力协作，不能单兵作战，才能保障网络安全。

网络安全防护，永远在路上！

THANKS

谢谢！