

根基不牢，地动山摇

——全国联网电力系统安全态势评估

何跃鹰 (hyy@cert.org.cn)

工业互联网安全应急响应中心/国家互联网应急中心

网络安全应急技术国家工程实验室

工控安全应急技术工信部重点实验室



提纲



一

背景

二

技术路线

三

资产暴露分析

四

漏洞风险分析

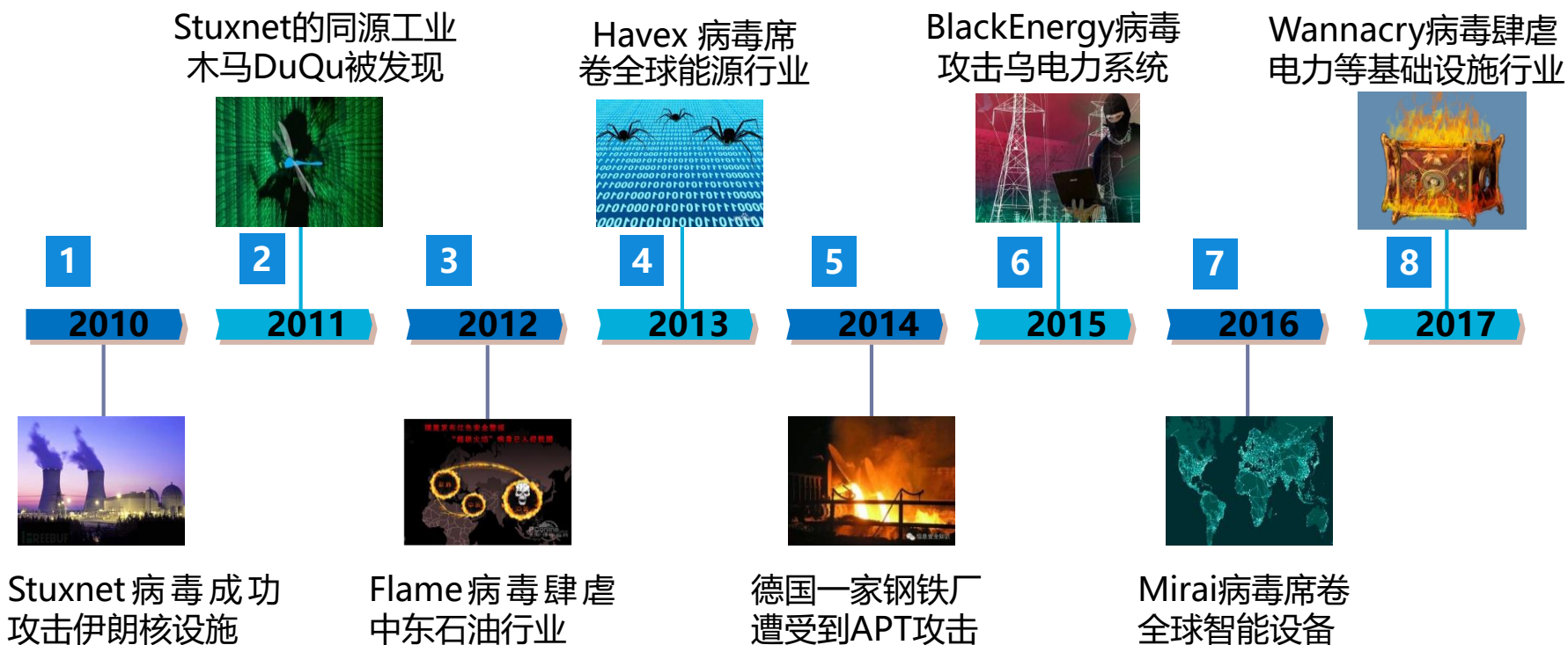
五

安全监测分析

六

安全态势评估

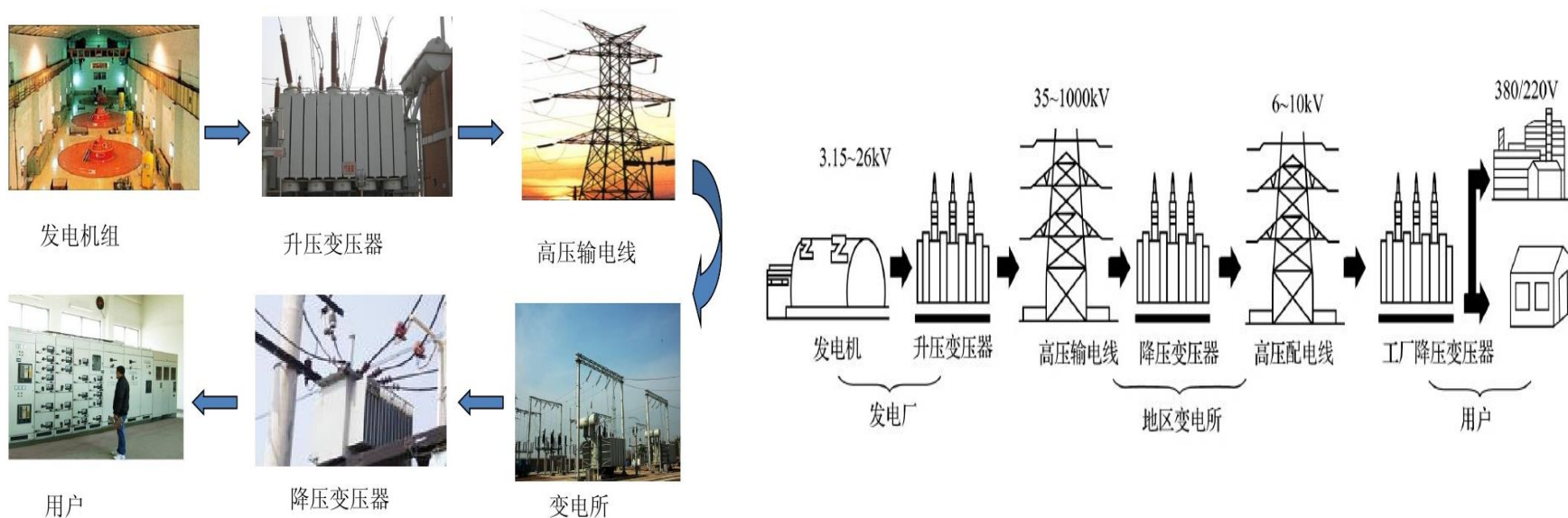
一、背景——电力系统网络安全形势



从最早的“震网”事件到去年Wannacry病毒事件，世界范围内针对工控系统的网络攻击事件愈演愈烈，**电力系统**作为关键基础设施中的基础设施，已成为**网络攻击的重点目标**。

一、背景——电力系统的联网风险

电力行业是国民经济发展中最重要的基础能源产业，可以划分为**发电、供电两大系统**和**发电、变电、输电、配电、用电五大环节**。



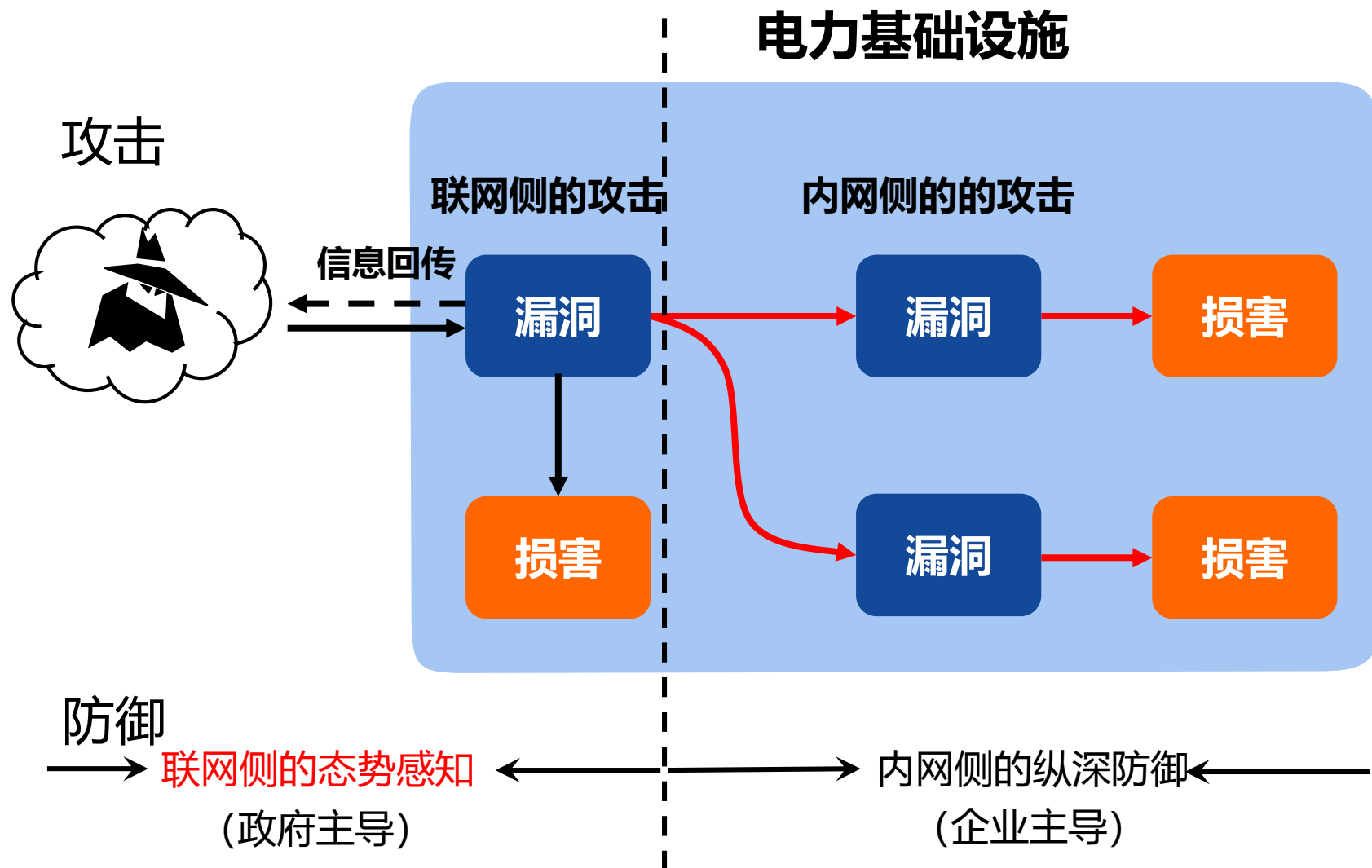
当前，随着电力系统的信息网络从“大型、封闭”网络**逐渐转换成**“**超大型、半封闭**”网络，可能引发联网安全风险。

一、背景——联网电力系统可能成为优先攻击目标

	震网 (Stuxnet)	黑色能量 (BlackEnergy)
攻击目标	伊朗核设施	乌克兰发电站 (电力系统)
联网与否	隔离, 非联网	直接或间接联网
目标属性	军工, 高度警戒	民用, 重点防护
攻击源	美国政府	黑客组织 (俄政府背景)
攻击方法	USB摆渡、自动扩展	协同攻击、远程操控
核心部件	HMI、PLC	HMI、PLC
攻击成本	超高、长时间谋划	相对较低, 常规方式
攻击效果	精确攻击、定向清除	大面积瘫痪

联网电力系统可能成为攻击者**优先选择的**电力基础设施**攻击目标**!

一、背景——针对电力基础设施进阶式网络攻击的防御策略



提纲



一

背景

二

技术路线

三

资产暴露分析

四

漏洞风险分析

五

安全监测分析

六

安全态势评估

二、技术路线

国家层面全面准确评估展现全国**联网电力系统安全态势**

全面准确掌握国内电力系统**暴露状况和安全隐患**
全网监测针对我国联网电力系统的**网络攻击行为**

主动探测与漏洞识别

国家互联网
基础平台和数据资源

流量监测与威胁检测

国家电力基础设施安全保障业务需求

提纲



一

背景

二

技术路线

三

资产暴露分析

四

漏洞风险分析

五

安全监测分析

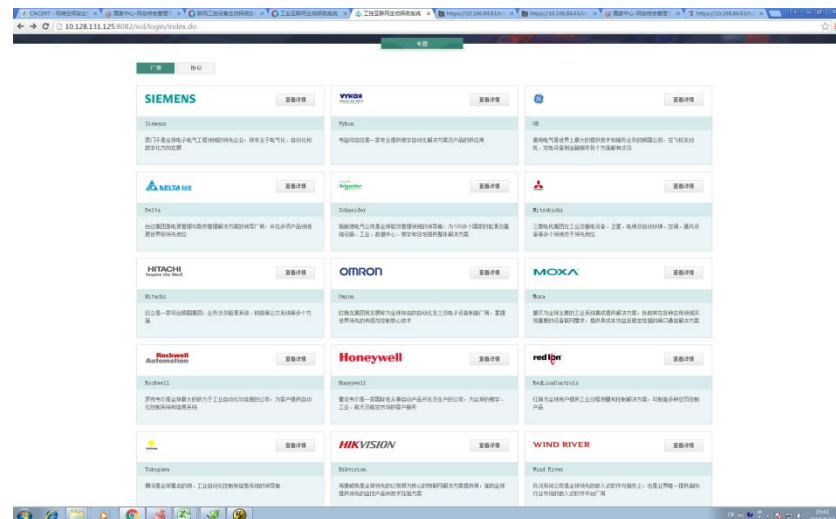
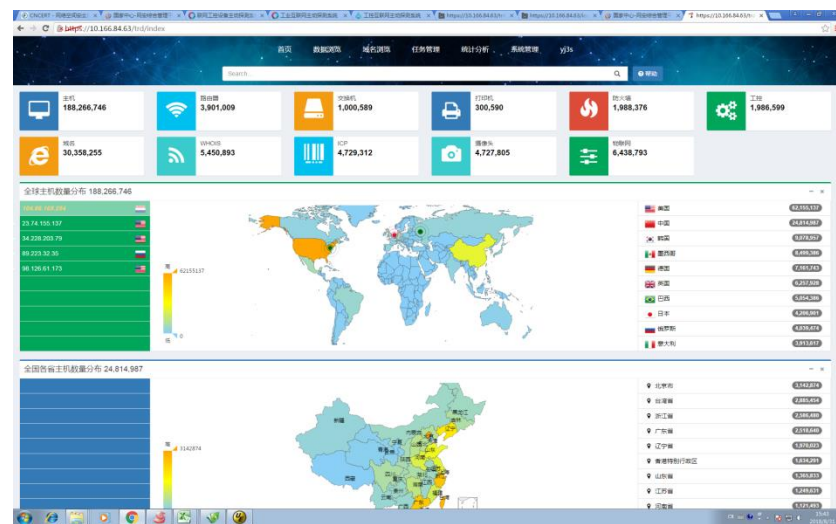
六

安全态势评估

三、资产暴露分析——联网设备探测发现系统

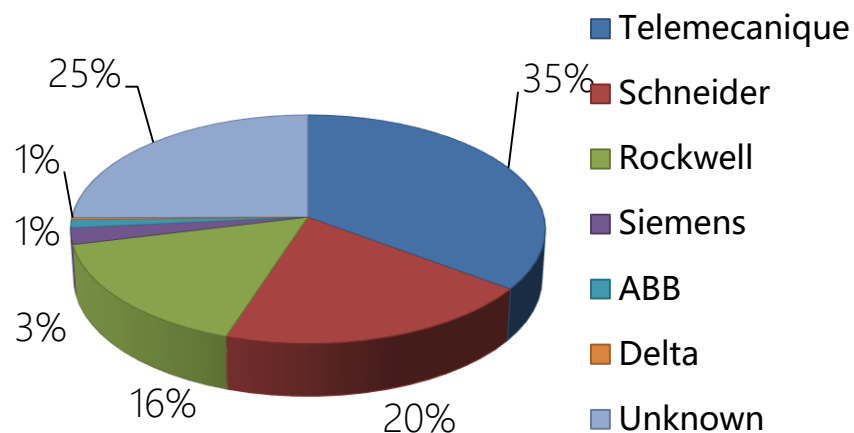
特点1：由于防护手段的升级，当前“Shodan”、“ZoomEye”等主流主动探测系统普遍存在的“易被感知、被反制”的缺陷，本系统利用“基于全局流量对准的IP复用技术”，系统实现可仿冒任意源IP对目标实施探测并不被防护设备所感知，实现了探测行为的“高隐蔽性”

特点2：当前探测系统大多存在“探测深度不够、存在探测盲区”的缺陷，本系统利用“基于互联网流量的扫描规则获取与验证技术”，从关口流量中快速获取各类扫描规则，做到“人无我有、人有我优”，并通过通联行为发现隐藏较深的联网工控设备及系统

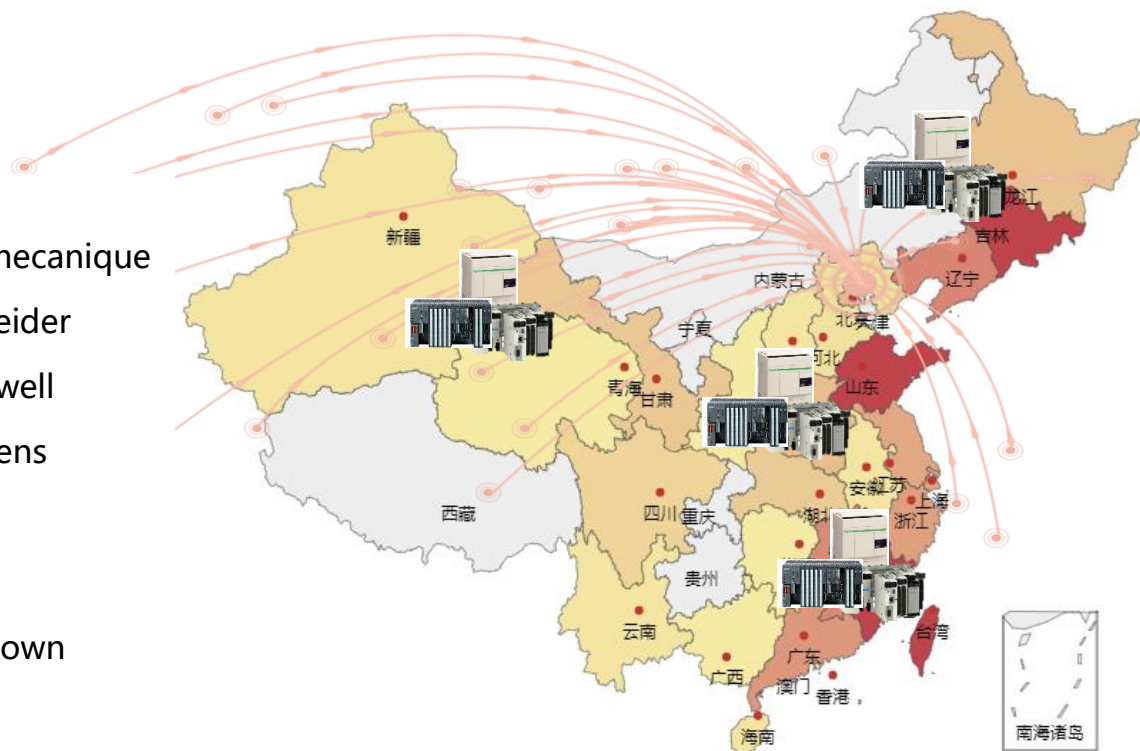


三、资产暴露分析——电力行业设备资产暴露情况

探测发现全国范围内使用IEC104、IEC103、IEC101、IEC92、IEC-MMS、Modbus、EtherNet/IP等协议的**联网电力设备556个**，主要分布在东部沿海地区，涉及到大量施耐德、罗克韦尔等企业生产的电力相关产品。



暴露电力设备涉及的生产厂商



暴露电力设备的全国分布图

三、资产暴露分析——电力行业Web资产暴露情况

探测发现暴露在公网的**传统电力WEB资产523个**，其中政府监管平台79个、电力企业相关平台406个、用电管理系统6个以及云平台32个，**北京、长三角和珠三角**地区暴露最多；发现**新能源智能电站及部分WEB资产59个**，主要分布在我国**西部地区**。

传统电力																											新能源					
政府监管平台					电力企业相关平台																	用电平台		云平台					电站与WEB			
需求侧管理平台	能源管理系统	能源监督平台	电力业务许可平台	其他	企业内部管理系统	充电桩管理系统	企业服务平台	企业邮件系统	能源监控系统	风电场监测系统	电能管理系统	企业信息管理系统	能源管理系统	变电站管理系统	用电管理系统	光伏电站监控系统	工程管理平台	电表充值系统	供电巡检管理系统	企业MIS系统	特变电源管理系统	气象环境监测系统	其他	能耗检测系统	用电管理网上查询系统	发电机组云控平台	光伏电站智能管理系统	电力智能云管理系统	企业能源管理云平台	充电云平台	其他	生产管理系统
22	14	27	4	14	48	38	28	26	25	18	17	17	15	14	11	8	6	5	4	4	4	3	115	3	3	1	10	2	5	7	14	59

提纲



一

背景

二

技术路线

三

资产暴露分析

四

漏洞风险分析

五

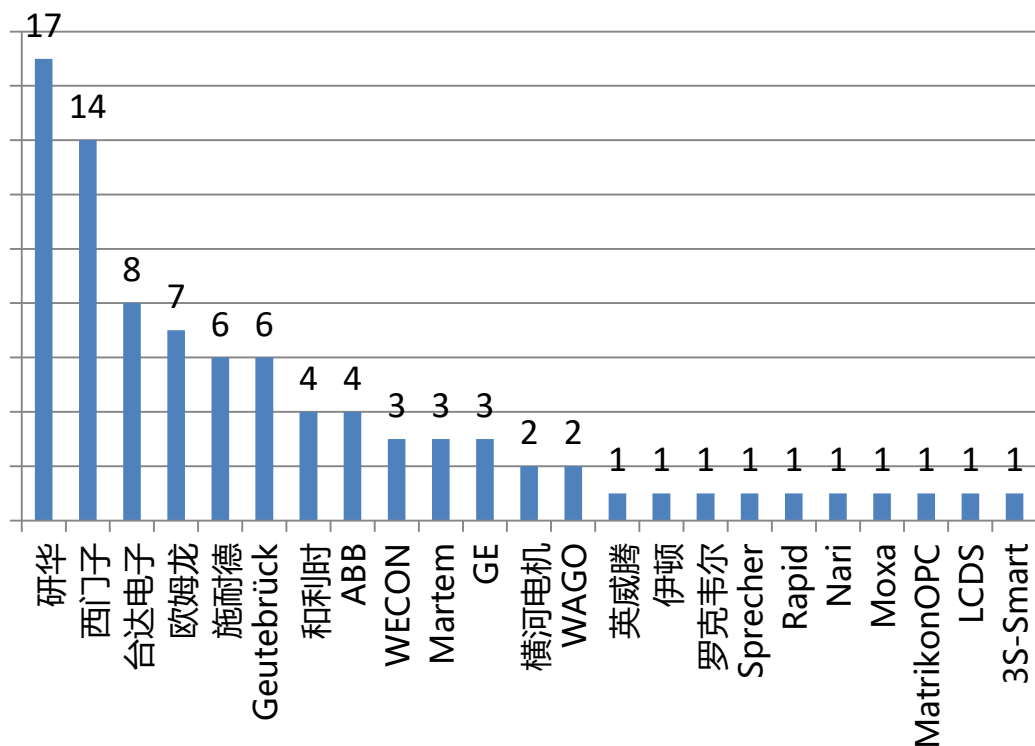
安全监测分析

六

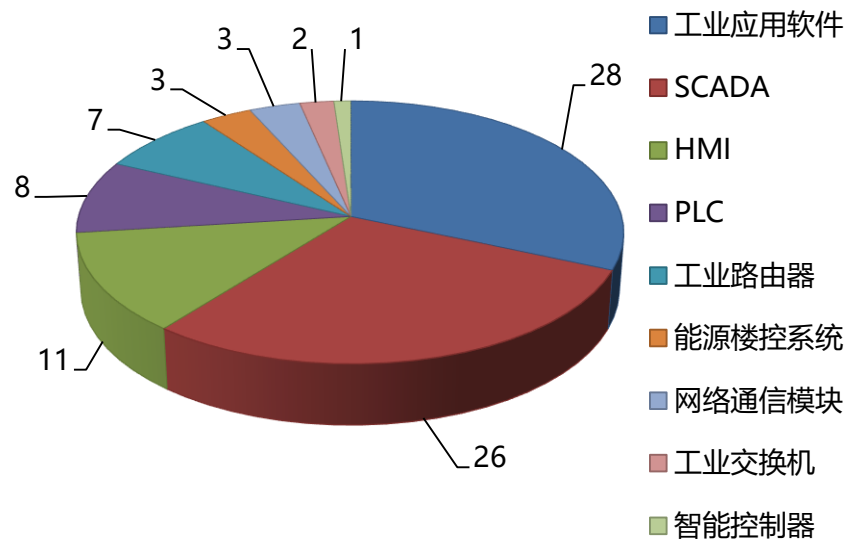
安全态势评估

四、漏洞风险分析——CNVD能源电力行业产品漏洞收录情况

CNVD收录大量能源电力行业相关产品漏洞，例如今年上半年新增收录89条，这些漏洞影响到包括研华、欧姆龙、台达等多家厂商，涉及到SCADA系统、可编程逻辑控制器、HMI等多种类型的软硬件产品和服务。



漏洞涉及厂商



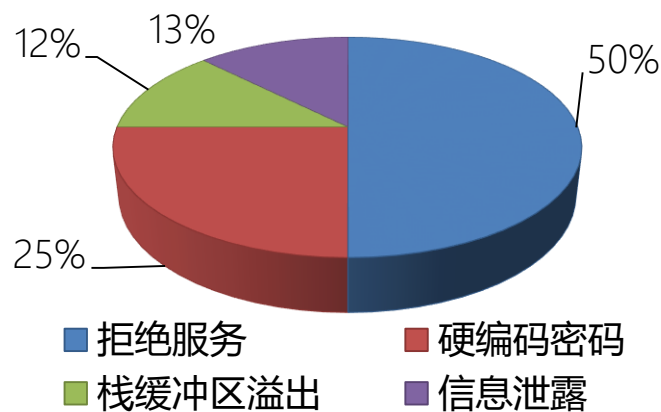
漏洞涉及产品类型

四、漏洞风险分析——暴露电力设备资产的漏洞巡检情况

将CNVD漏洞数据库与暴露设备的基本信息进行比对，即发现部分型号的联网电力设备存在拒绝服务、硬编码密码等安全漏洞，主要涉及西门子、施耐德生产的可编程控制器（PLC）产品。

暴露设备的漏洞列表

厂商	产品型号	漏洞编号	等级
西门子	S7-400	CNVD-2012-4031	高危
		CNVD-2016-12695	中危
		CNVD-2016-12694	中危
		CNVD-2017-06153	中危
		CNVD-2017-06151	中危
		CNVD-2018-06025	中危
		CNVD-2012-4032	高危
施耐德	BMX NOE 0100	CNVD-2011-5607	高危
		CNVD-2015-08446	高危
施耐德	BMX P34 2020	CNVD-2011-5607	高危
		CNVD-2015-08446	高危
施耐德	TSXETY4103	CNVD-2011-5607	高危
西门子	S7-200	CNVD-2017-06153	中危
		CNVD-2017-06151	中危
施耐德	TM221CE16R	CNVD-2017-05014	高危
		CNVD-2017-05011	中危

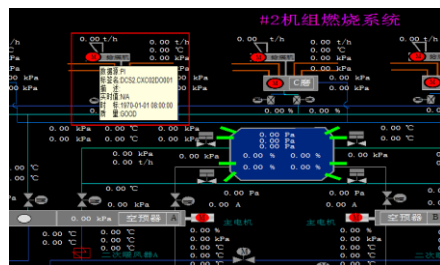
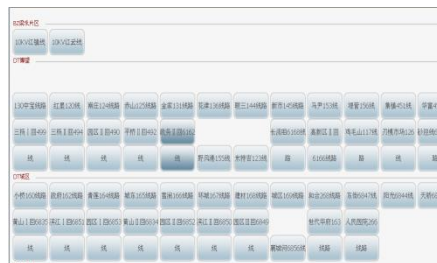


暴露设备的漏洞类型

四、漏洞风险分析——暴露电力Web资产的漏洞巡检情况

抽取了200个暴露的电力WEB资产，其中生产管理类系统127个，生产监控类系统73个。通过远程安全巡检，发现超过10%的系统存在明显的安全问题，易被入侵：

- 21个系统存在严重安全漏洞隐患，生产监控类16个，生产管理类5个
- 主要涉及弱口令、SQL注入、远程代码执行和逻辑错误四大类漏洞



序号	用户名	密码	权限
139080	李记(巴中)		禁用
181337	范长(开县)		禁用
139568	李队长(保靖)		禁用
138819	李队长(巴中)		禁用
136982	李队长(巴中)		禁用
135005	范队长(开县)		禁用
139653	李队长(开县)		禁用
183269	李队长(开县)		禁用



提纲



一

背景

二

技术路线

三

资产暴露分析

四

漏洞风险分析

五

安全监测分析

六

安全态势评估

五、安全监测分析——安全威胁监测系统

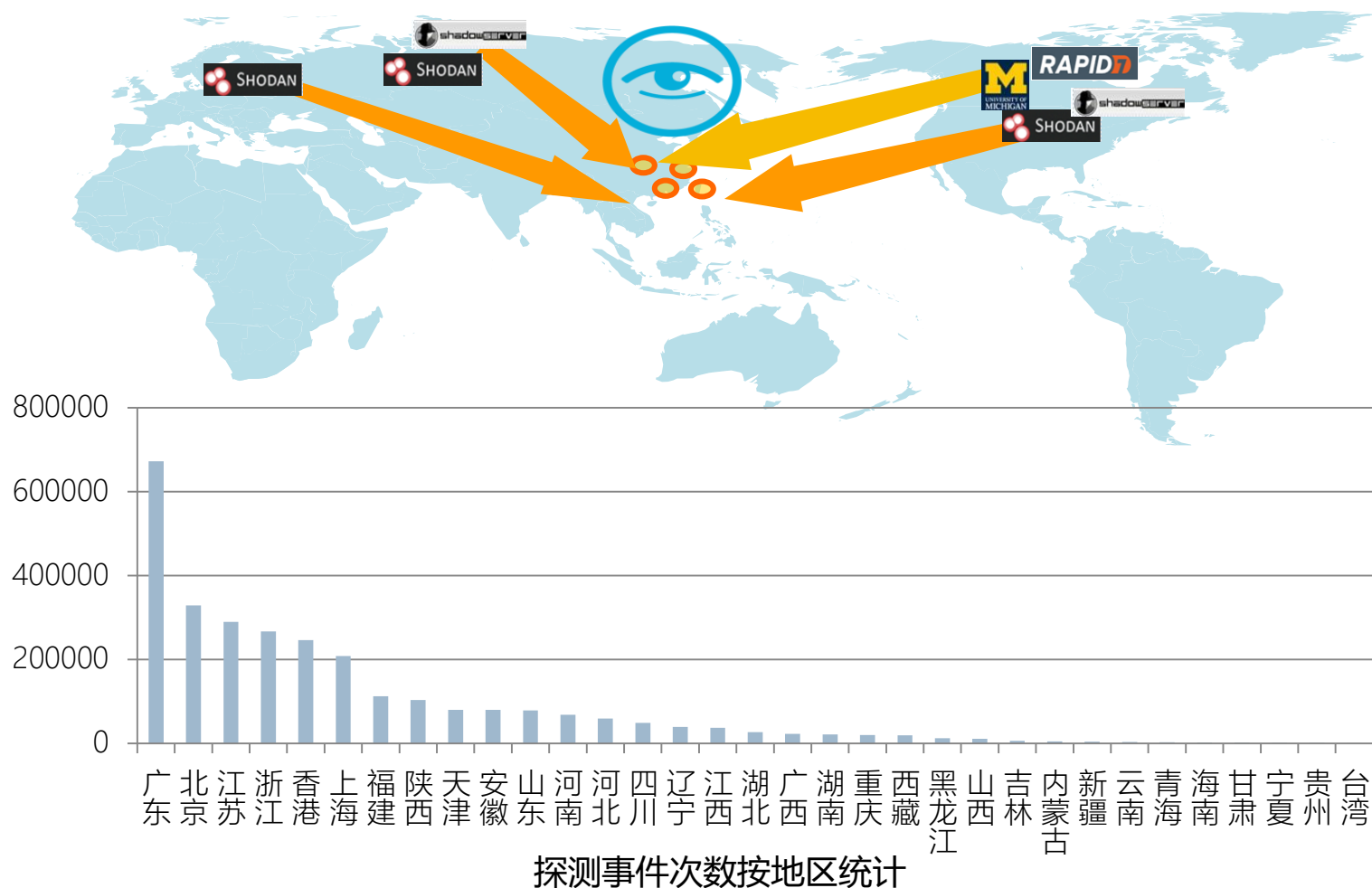
已实现国内独有的网络空间工业网络安全威胁监测系统，具有以下特点：

- **范围大**：本系统实现了对互联网关键节点的全流量全时段监测覆盖
- **协议广**：支持对**50余种主流工控通信协议**的解析，进而实现了**数百种主流工控产品**的发现识别
- **响应快**：对扫描探测、木马注入、拒绝服务等网络恶意行为，实时监测和快速检测



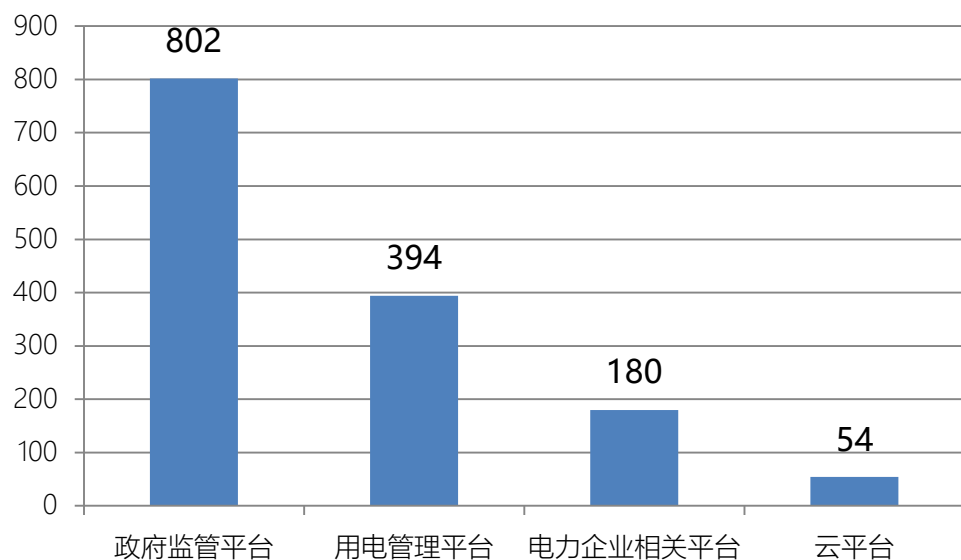
五、安全监测分析——跨境端口探测情况

2018年上半年，累计监测到来自境外Shadowserver、Shodan等重点探测组织全球数百个探测节点的IEC-104、Modbus等电力协议相关的端口探测事件**2880316**起。

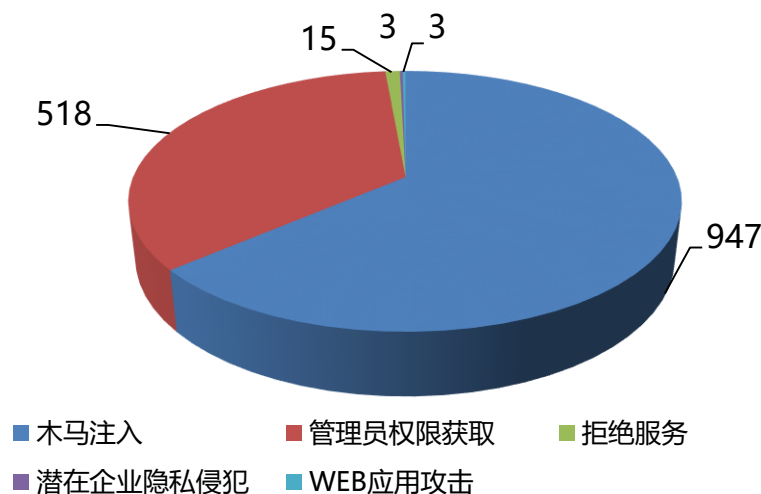


五、安全监测分析——跨境网络攻击抽样监测情况

抽取84个暴露在公网的典型WEB电力监控管理平台进行了为期1周的全流量监测，发现木马注入、管理员权限获取、拒绝服务等类型攻击共计1486次，涉及平台数量43个，占抽样监测平台总数的51.2%。



针对各类电力监控管理平台攻击事件的统计



攻击类型及攻击事件数的统计

提纲



一

背景

二

技术路线

三

资产暴露分析

四

漏洞风险分析

五

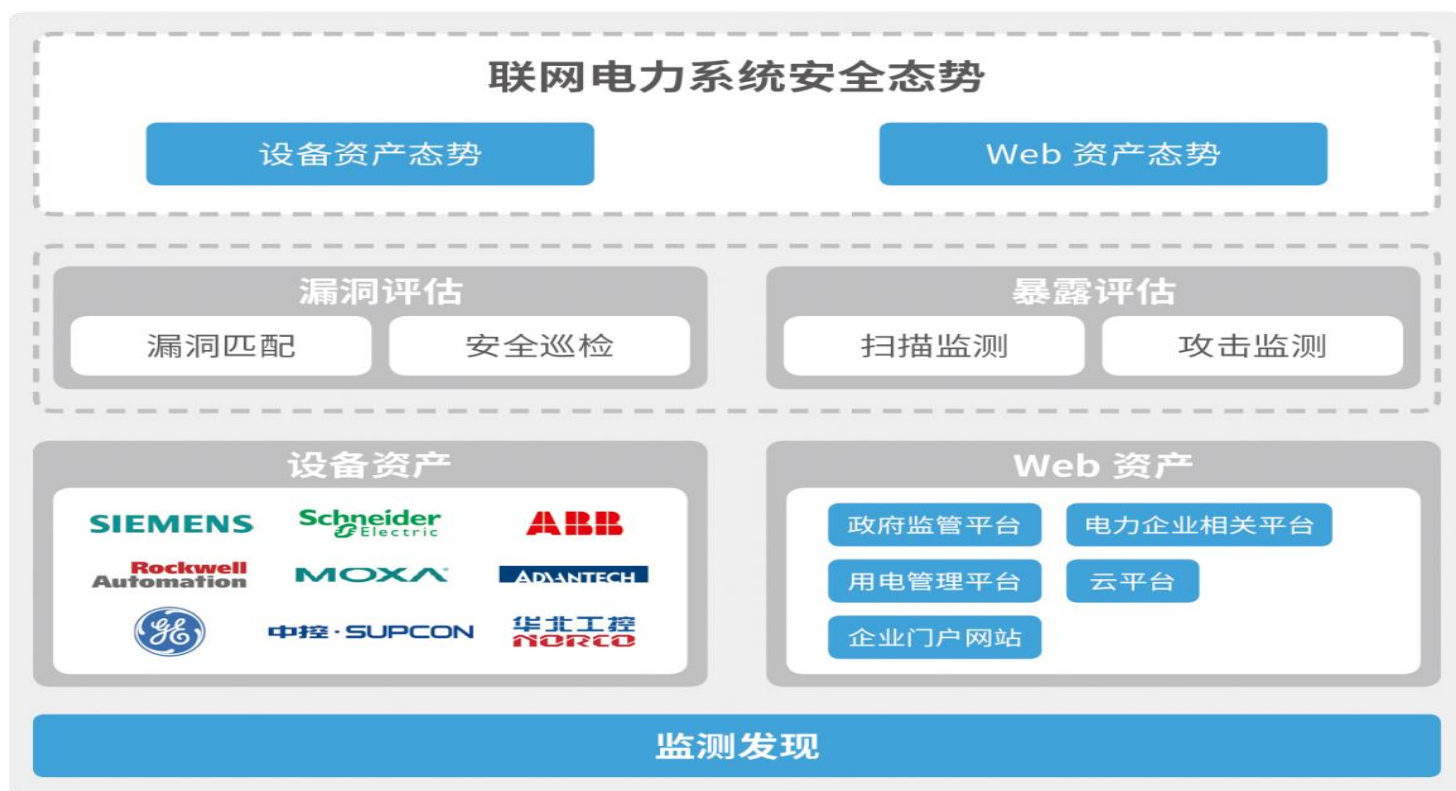
安全监测分析

六

安全态势评估

六、安全态势评估——联网电力系统网络安全态势评估体系

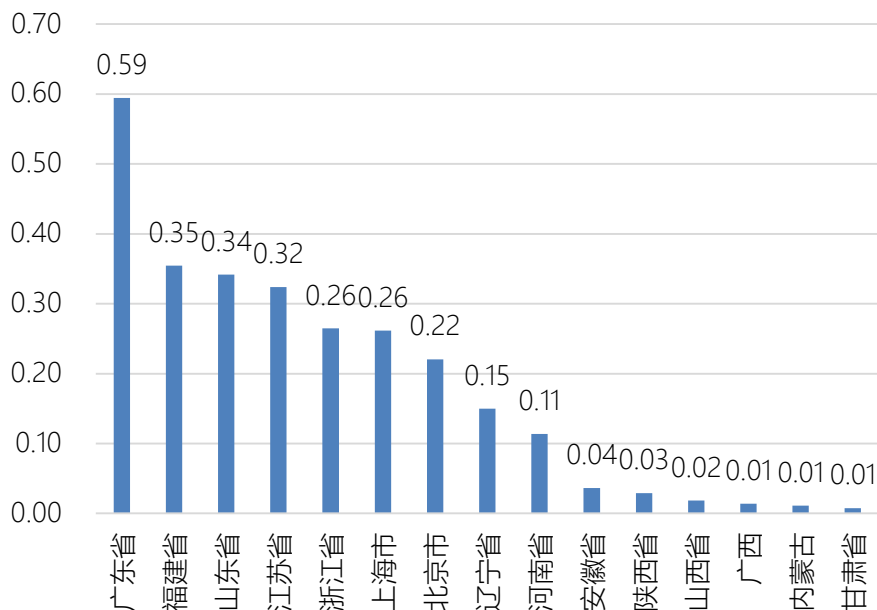
首先分别计算联网电力**设备资产安全威胁指数**和联网电力**WEB资产安全威胁指数**。两类指数计算的原理类似，计算过程中均重点考虑暴露资产的**漏洞威胁**和**暴露程度**两方面的因素。



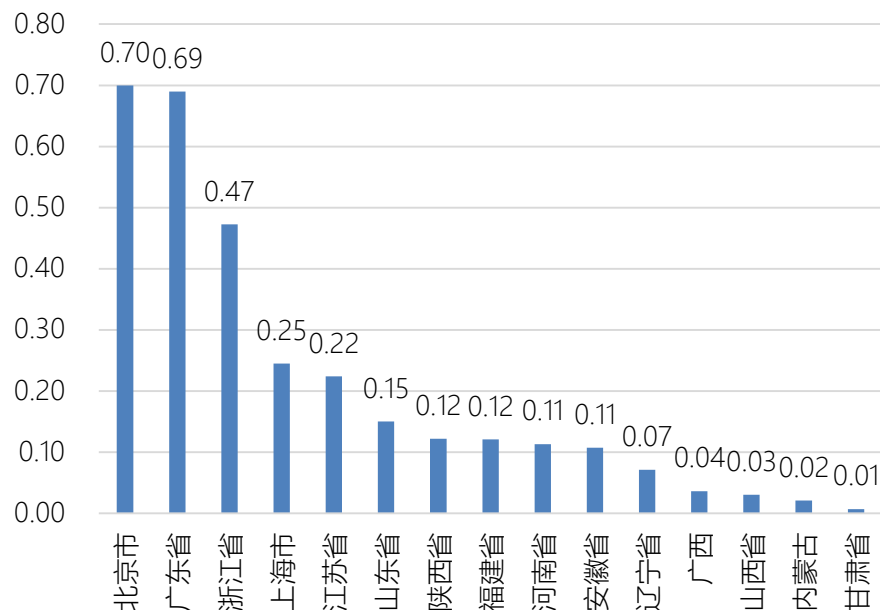
最后将设备和WEB两类威胁指数**综合加权**，进而形成联网电力系统网络安全威胁**综合评估指数及安全态势**。

六、安全态势评估——联网电力设备和Web安全威胁评估

针对发现的联网电力设备资产或Web资产，以省、自治区和直辖市作为评价对象，首先分别计算各个地区的联网资产漏洞评估指数和暴露评估指数，做归一化处理后将两者相乘即得到各个地区的联网资产安全威胁指数。



各地区联网电力设备资产安全威胁评估指数



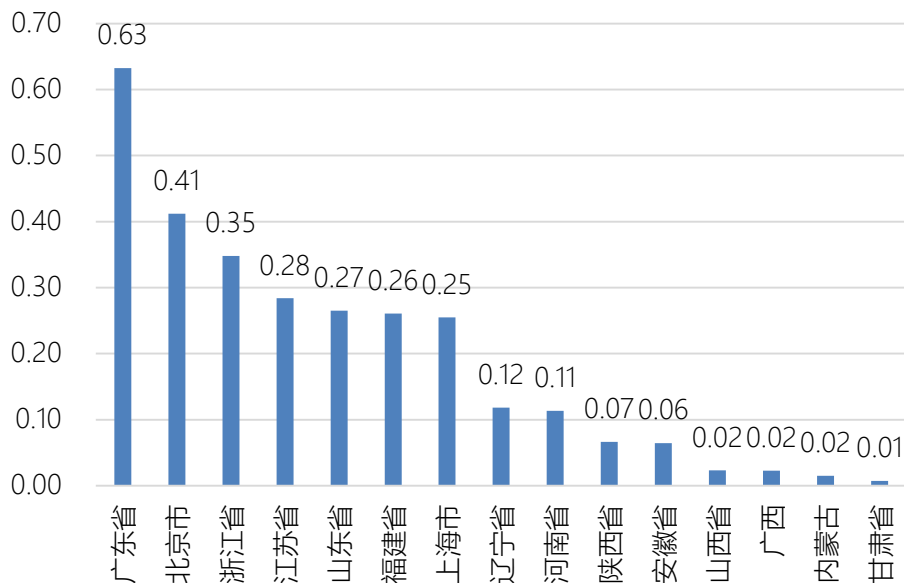
各地区联网电力WEB资产安全威胁评估指数

六、安全态势评估——全国联网电力系统网络安全态势评估

将设备和WEB两类威胁指数**综合加权**，即得到我国各个地区联网电力系统网络安全威胁综合评估指数。进一步将综合威胁指数分为**5个等级**：

优 (0-0.2)、良 (0.2-0.4)、中 (0.4-0.6)、差 (0.6-0.8)、危 (0.8-0.1)

据此得到了**全国联网电力系统综合安全态势**。



各地区联网电力系统安全威胁综合评估指数



我国联网电力系统综合安全态势

针对上述情况，已协助相关部门开展整改工作！

感谢聆听，欢迎合作！

微信公众号：工业互联网安全应急响应中心

门户网站：<https://www.ics-cert.org.cn>