



“互联网+”时代下 工业控制系统网络安全

工业和信息化部电子科学技术情报研究所

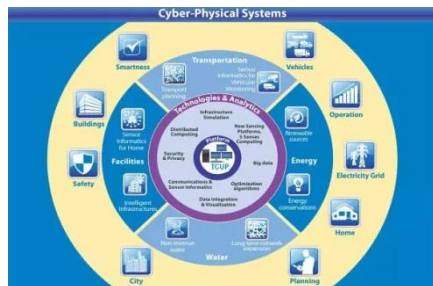
郭 娴 博士

2015年5月14日

无处不在的“互联网+”



工业互联网



信息物理系统



物联网



智慧城市

工业控制系统网络互联的利与弊

- 提高生产力
- 提升创新能力
- 减少工业能源与资源消耗
- 助力产业模式转型升级

。 。 。



诱发一系列网络安全问题





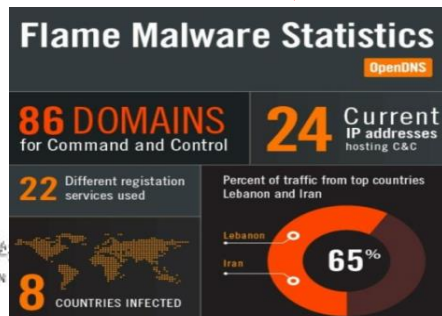
钢铁厂



ICS-ALERT-14-281-01A

BlackEnergy

正在影响工业控制系统网络



工业控制系统网络安全事件危害严重

环境污染



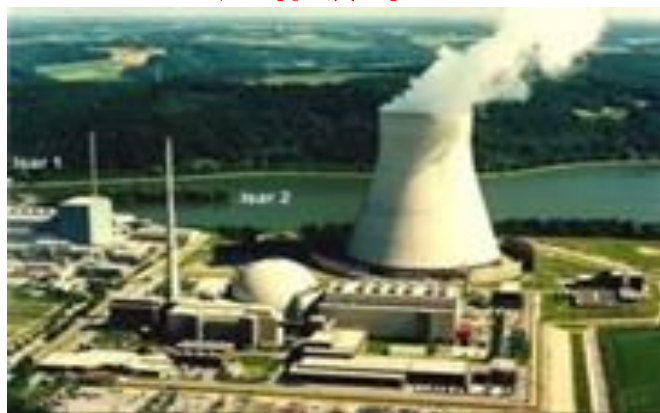
澳大利亚马卢奇污水处理厂
非法入侵事件

经济损失



德国钢铁厂遭遇网络安全攻击

战略破坏



伊朗布什尔核电站遭到“震网”病毒攻击

信息泄露



中东能源行业遭遇“Flame”病毒攻击

工业控制系统网络安全关乎国家安全

Danger!

国家
安全
风险



网络部队



黑客

工业控
制系统
网络安
全



极端势力



工业控制系统防护情况：“门户洞开”

访问控制形同虚设

重要数据明文传输

公网映射“掩耳盗铃”

工业控制系统在线监测能力建设迫在眉睫

有多少数量的工业控制系统暴露在互联网中？

有哪些行业的工业控制系统暴露在互联网中？

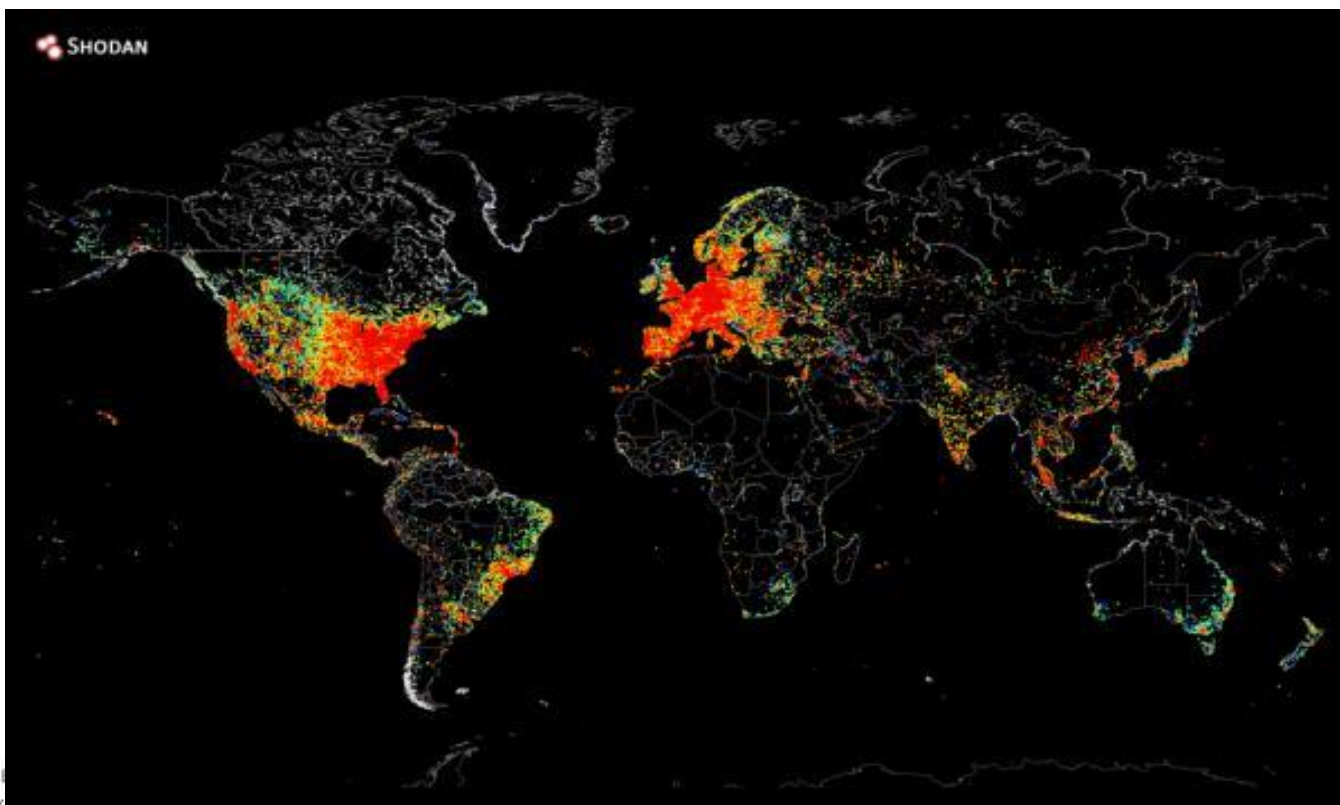
有哪些地区的工业控制系统暴露在互联网中？

暴露在互联网的工业控制系统有什么安全风险？



美国已形成工业控制系统在线监测能力

美国国土安全部通过Project Shine项目搜索暴露在互联网上的关键信息基础设施，自2012年4月起，已经收集了全球范围内超过220万条数据，并确定其中7200个为美国关键信息基础设施。



工业控制系统在线监测情况

Shodan Exploits Scanhub Maps Blog Membership

SHODAN 6ES7 country:CN Search

Home Search Directory Data Analytics/ Exports Developer Center Labs

+ Add to Directory

Services
[Siemens S7](#)
[SNMP](#)

Top Cities
[Shenyang](#)
[Nanjing](#)
[Nanchang](#)

111.75.189.5
China Telecom JIANGXI
Added on 26.05.2014
Nanchang
Details

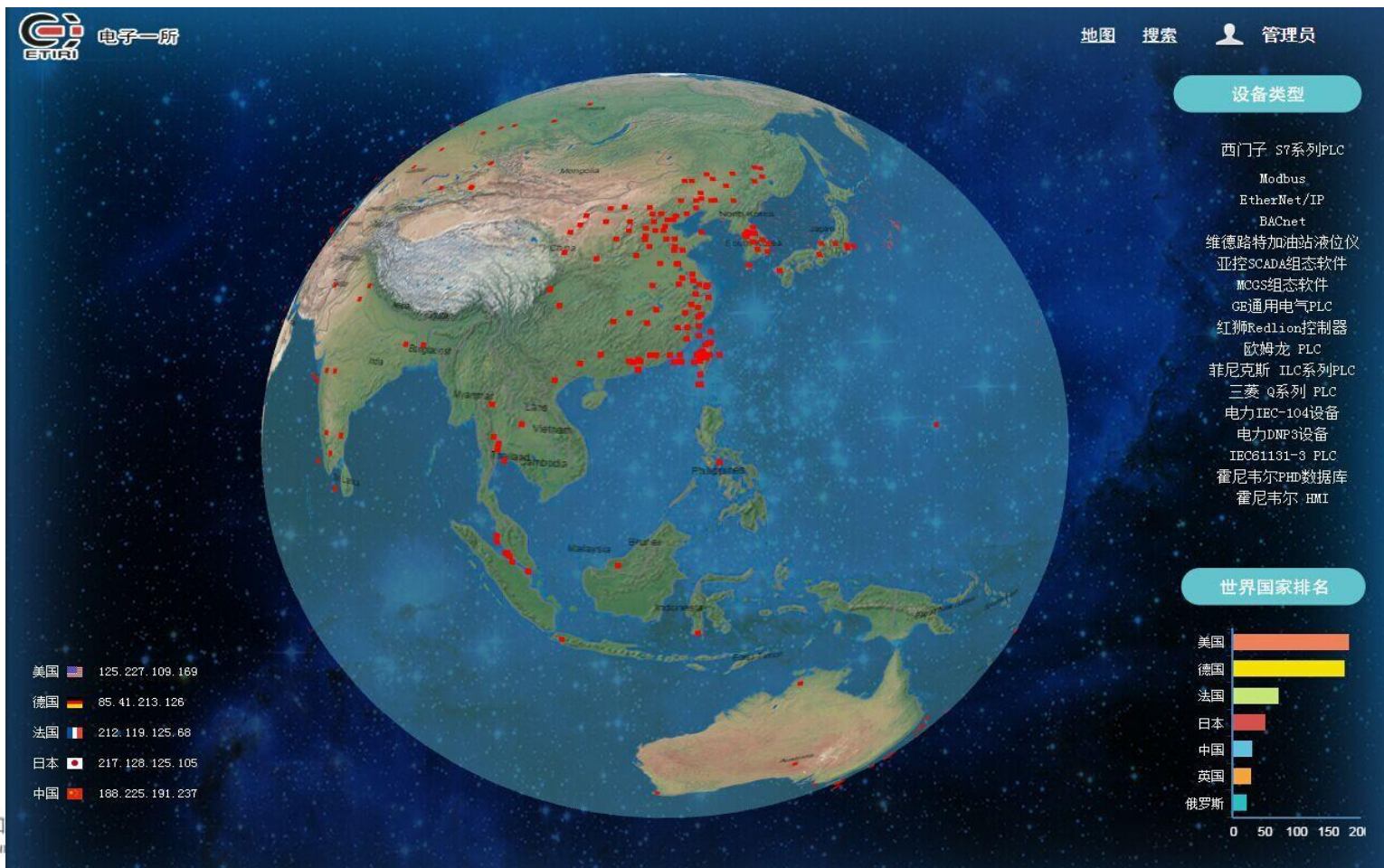
Copyright: Original Siemens Equipment
PLC name: 1_Untha
Module type: CPU 315-2 DP
Unknown (129): Boot Loader A
Module: **6ES7** 315-2AH14-0AB0 v.0.2
Basic Firmware: v.3.0.3
Module name: CPU 315-2 DP
Serial number of module: S C-B1WC06992011
Plant identification:
Basic Hardware: **6ES7** 315-2AH14-0AB0 v.0.2

113.224.72.183
China Unicom Liaoning
Added on 05.05.2014
Shenyang
Details

Siemens, SIMATIC S7, CPU-1200, **6ES7** 214-1AG31-0XB0, HW: 1, FW: V.3.0.2, SZVE2YH0100458

重要控制系统在线监测平台

2013年初，电子科学技术情报研究所开始开展重要控制系统在线搜索监测工作，逐步建设了重要控制系统在线监测平台，现已初步形成了对重要工业控制系统的在线监测能力。



重要控制系统在线监测平台

【监测数据动态化展示】



重要控制系统在线监测平台

【监测平台搜索引擎】



重要控制系统在线监测平台

【监测平台产品硬件化】



重要控制系统在线监测平台

【平台监测对象】

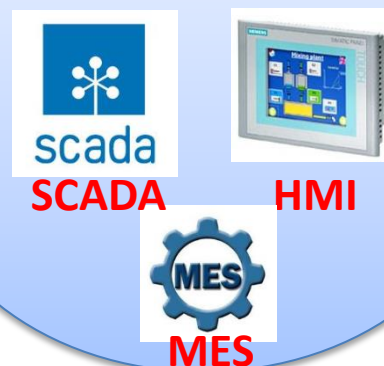
工业控制设备



系统主机及服务器



应用软件



智能设备



工业网络设备



重要控制系统在线监测平台

【平台研究成果】

- 已收集包括西门子、施耐德、三菱、AB、和利时、GE、欧姆龙等在内的国内外主流工业控制设备和组态软件的网络指纹特征，覆盖了**17**种主流工控专有协议和**20**种工控专用网络端口
- 已发现超过**700**个连接在我国互联网上的重要控制系统，涉及市政供水供热、能源、污水处理、水利等关键信息基础设施领域
- 已发现超过**30万**个连接在我国互联网上的视频监控设备，广泛分布于银行、学校、工厂、交通等关键监控区域

重要控制系统在线监测平台

【实现功能】

- 掌握国内外工业控制系统及设备的基础信息、分布情况和发展趋势
- 提高重要工业控制系统网络安全风险的“可发现”能力
- 帮助关键基础设施运营单位提高工业控制系统网络安全防护能力
- 提供工业控制系统网络安全监测与感知预警支撑



案例展示



监测实例1：安全监控系统



监测实例2：市政供水控制系统



监测实例3：市政供热控制系统



监测实例4：市政供气控制系统



监测实例5：水利涵闸控制系统



监测实例6：污水处理控制系统



监测实例7：电力控制系统