

电力能源领域工业互联网 信息安全平台

上海市电站自动化
实验室

随着工业信息化的快速发展，在极大提高工业生产效率的同时，也暴露了工控系统的弱点。2010年攻击伊朗布什尔核电站的“震网”病毒被认为是全球首个投入实战的网络“超级武器”。



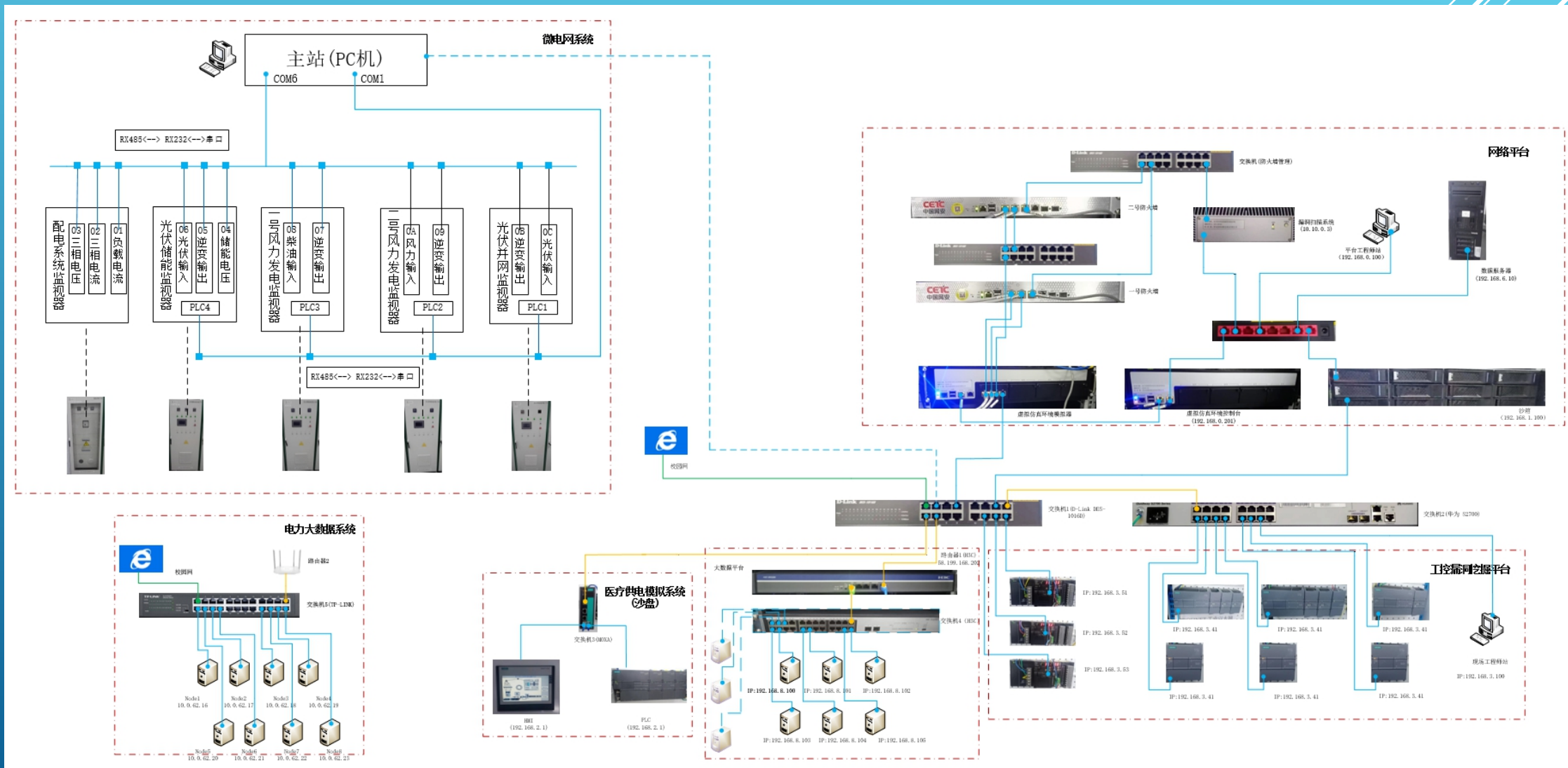
电力能源领域工业互联网 信息安全平台

上海市电站自动化
实验室



电力能源领域工业互联网 信息安全平台

上海市电站自动化
实验室



实验室网络拓扑图

模糊测试

Fuzzing test

上海市电站自动化
实验室

因为工控设备的特殊性，传统IT的漏洞挖掘办法并不能适用。因此使用模糊测试对工控系统的健壮性进行测试。



模糊测试(fuzz testing, fuzzing)是一种软件测试技术。其核心思想是将自动或半自动生成的随机数据输入到一个程序中,并监视程序异常,以发现可能的程序错误,比如内存泄漏。模糊测试常常用于检测软件或计算机系统的安全漏洞。



名称	等级	影响产品	厂商
Modbus Slave缓冲区溢出	中	V7.0.0	modbustools
组态王堆溢出	高	V6.5.3	亚控
KingView栈溢出	高	V6.5.3	亚控
Modbus解析器拒绝服务	中	V2.4.0	Wireshark
Profinet解析器拒绝服务	中	V2.4.0	Wireshark
M340 PLC加密问题	高		施耐德
M340 PLC网络配置漏洞	高		施耐德
Unity Pro XL缓冲区溢出	高	V11.0	施耐德
M340 PLC逻辑崩溃	高		施耐德

截止2019年11月21日，披露的工控系统行业漏洞数量为**302**个。
 课题组挖掘漏洞：**9**个。挖掘对象均为国内外知名工控网络产品制造厂家。
 漏洞类型主要为**高、中级漏洞**。

漏洞反馈及信息确认

发件人：漏洞管理处vul... <vulpro@itsec.gov.cn>

时 间：2019年12月30日 15:43:47 (星期一)

收件人：jeloy@shu.edu.cn

您好：

经验证，您提交的漏洞危害等级情况如下。CNNVD将于近期通过官方网站（<http://www.cnnvd.org.cn>）发布以下漏洞信息，请于2020年1月10日前确认信息是否需要修改，并反馈至本邮件。

提交日期	漏洞名称	危害等级	漏洞编号	漏洞来源
2019/11/19	UnityPro拒绝服务漏洞	低危	CNNVD-201911-1586	上海大学机电工程与自动化学院付敬奇 易慕白 沈仁亮 曹一帆

如有问题，请联系010-82341017

国家信息安全漏洞库（CNNVD）