

典型行业工控安全案例解析

目录/CONTENTS

01 工控系统常见安全问题及政策法规

02 电力发电行业典型案例解析

03 石油石化行业典型案例解析

04 市政燃气行业典型案例解析

01

工控系统常见安全问题及政策标准

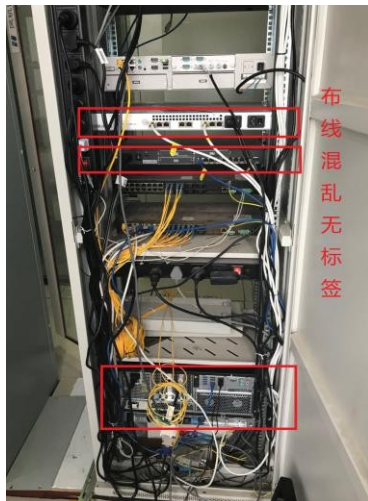
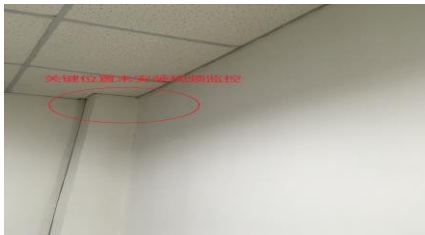
安全现状

政策标准

安全现状

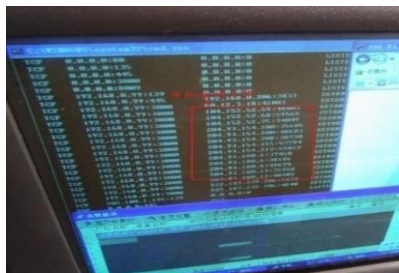
■ 机房建设不合规

机房安全建设不合规：如门禁系统、视频监控
系统、防盗报警系统、防火系统的缺失，不符
合相关标准的物理安全要求。



■ 存在违规外联现象

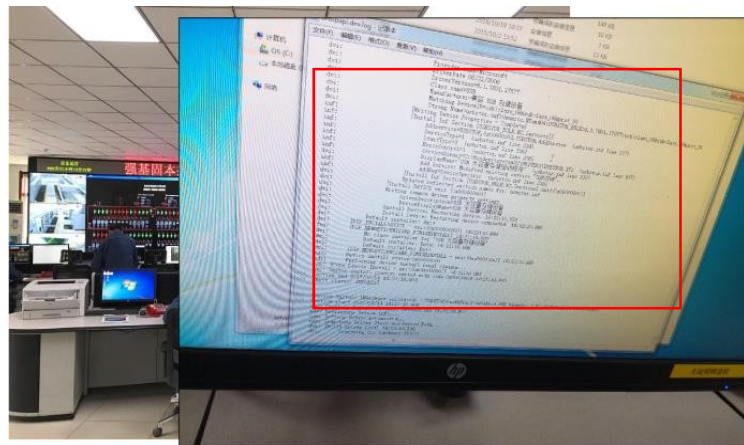
网络通信存在诸多安全隐患：如为了方便运维
管理，违规保留了远程维护通道，安全检查时就
将通道临时关闭，规避安全检查；将重要的生
产管理服务器违规接入互联网，服务器有频繁
的境外IP访问；网络安全设备形同虚设，策
略不正确甚至没有开启任何策略。



安全现状

主机安全问题突出

上位机安全隐患突出：如安装非工作软件、操作系统老旧且容易遭受病毒感染、操作系统安全配置缺失、移动存储介质非法使用等。



策略

- 密码必须符合复杂性要求
- 密码长度最小值
- 密码最短使用期限
- 密码最长使用期限
- 强制密码历史
- 用可还原的加密来储存密码

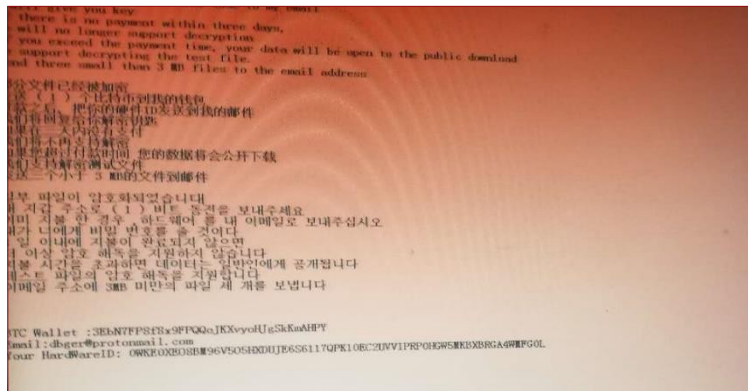
安全设置

- 已禁用
- 0 个字符
- 0 天
- 42 天
- 0 个记住的密码
- 已禁用

安全现状

病毒肆虐

长期以来，病毒问题是困扰工业控制系统主机的一个棘手问题，从大名鼎鼎的震网病毒到2015年岁末的BlackEnergy，从WannaCry到Satan，这些如鬼魅般游荡在工业控制系统网络中的杀手总是伺机而动



安全现状

- 在众多用户现场发现，重要工业控制设备前端无任何安全防护设备，冒用、篡改等攻击行为都将会直接作用于关键控制设备。



现场控制设备无防护



现场控制设备无防护

安全现状

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：
<https://d.book118.com/898051135024006061>