公安部第三研究所
The Third Research Institute Of Ministry Of Public Security

国家网络与信息系统
安全产品质量监督检验中心

工业控制设备漏洞与对策

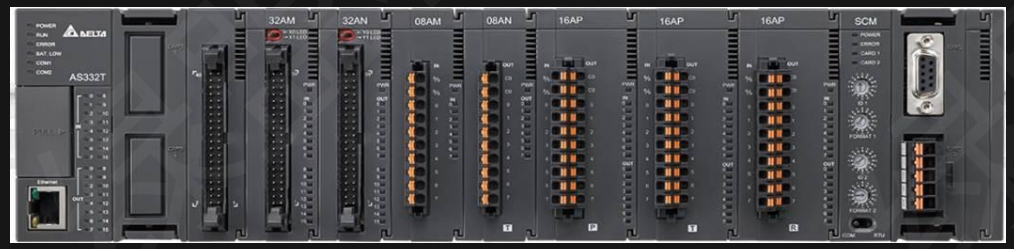
公安部第三研究所
国家网络与信息系统安全产品质量监督检验中心
邹春明

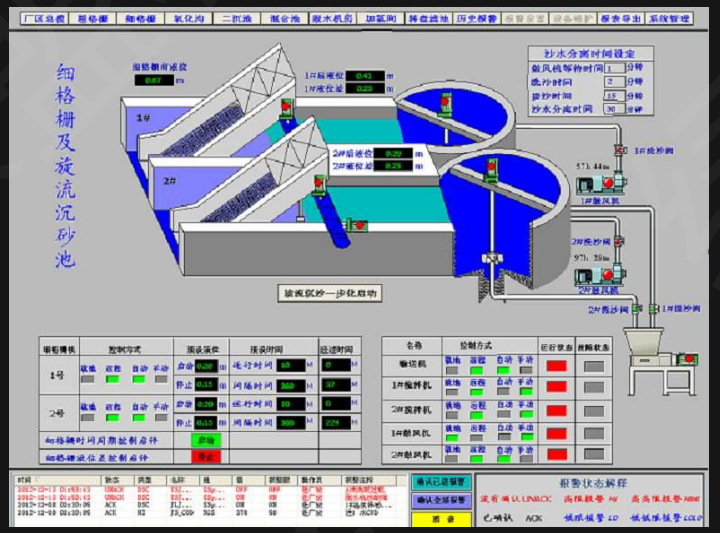
NSFOCUS

概述

工业控制设备：

- 硬件：PLC、DCS、RTU、现场执行设备
- 软件：固件、上位机软件





概述

工控设备安全

功能安全（Safety）：

保证系统或设备执行正确的功能，当失效或故障发生时，设备和系统仍需保持安全条件或者进入到安全状态。

信息安全（Security）：

保证信息的可用性、完整性、保密性，防范非授权的窃取、破坏。

概述

工业控制设备漏洞及脆弱性主要方面：

- 固件方面
- 工控协议方面
- 上位机软件方面
- 硬件方面
- 配置管理方面

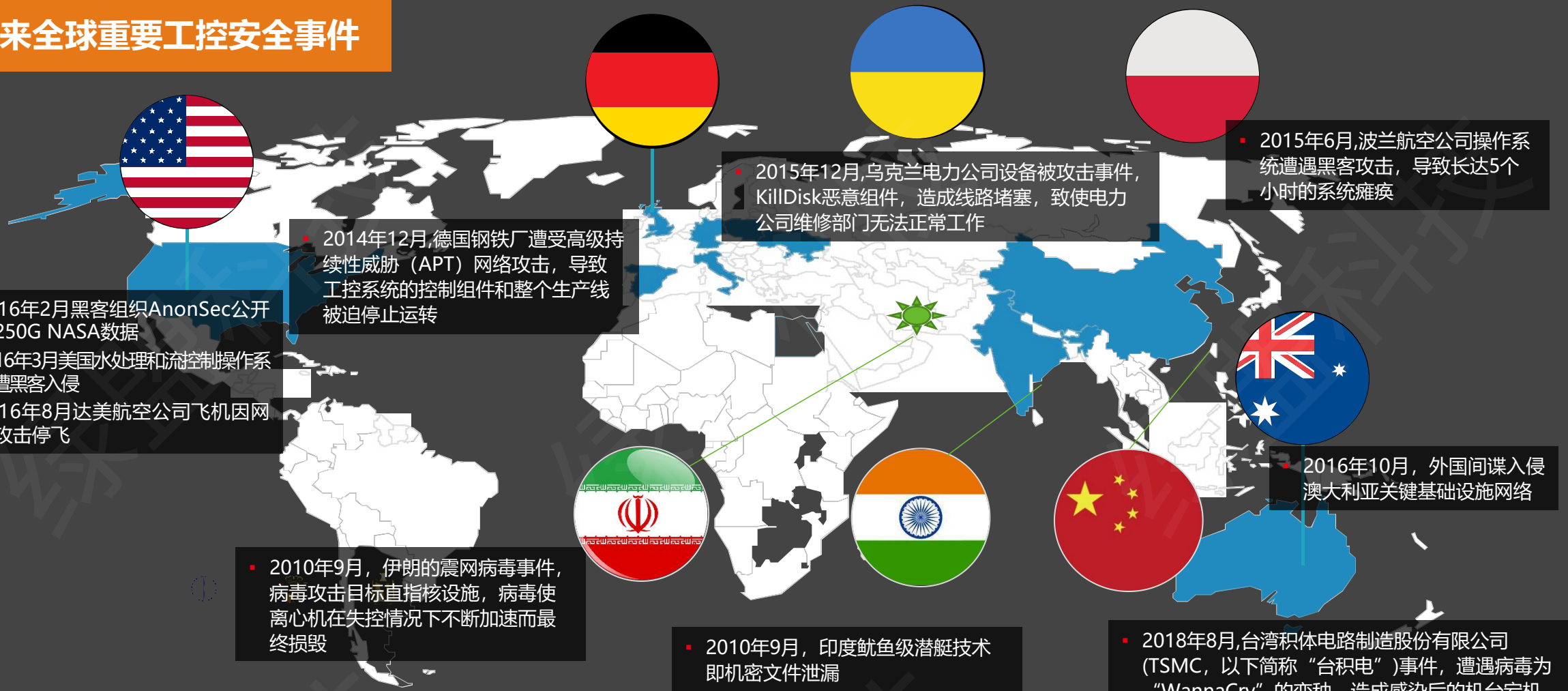
概述

漏洞标题	危害级别	点击数	评论	关注	时间
ABB Telephone Gateway TG/S和Bu...	高	138	0	0	2020-04-23
ABB Telephone Gateway TG/S和Bu...	中	72	0	0	2020-04-23
ABB Telephone Gateway TG/S和Bu...	高	76	0	0	2020-04-23
ABB Telephone Gateway TG/S和Bu...	中	71	0	0	2020-04-23
ABB System 800xA Base授权问题漏...	高	160	0	0	2020-04-23
ABB System 800xA Information M...	高	70	0	0	2020-04-23
多款Siemens产品资源管理错误漏洞...	高	406	0	0	2020-04-15
多款Siemens产品资源管理错误漏洞...	高	234	0	0	2020-04-15
Synergy Systems & Solutions HU...	中	47	0	0	2020-04-08
Synergy Systems & Solutions HU...	中	43	0	0	2020-04-08
Synergy Systems & Solutions HU...	高	46	0	0	2020-04-08
Synergy Systems & Solutions HU...	高	49	0	0	2020-04-08
GE CIMPLICITY权限提升漏洞	高	335	0	0	2020-04-08
Advantech WebAccess访问控制错误...	中	398	0	0	2020-04-02
Phoenix Contact PC WORX SRT权限...	高	740	0	0	2020-03-30
Advantech WebAccess缓冲区溢出漏...	高	790	0	0	2020-03-27
Moxa EDS-G516E缓冲区溢出漏洞	中	691	0	0	2020-03-27
3S-Smart Software Solutions CO...	中	101	0	0	2020-03-26
3S-Smart Software Solutions CO...	中	512	0	0	2020-03-26
WAGO PFC 200资源管理错误漏洞	中	841	0	0	2020-03-24

1 2 3 4 5 6 7 8 9 10 .. 127 下页 共 2524 条

概述

近年来全球重要工控安全事件



- 2016年2月黑客组织AnonSec公开约250G NASA数据
- 2016年3月美国水处理和流控制操作系统遭黑客入侵
- 2016年8月达美航空公司飞机因网络攻击停飞

- 2014年12月,德国钢铁厂遭受高级持续性威胁（APT）网络攻击，导致工控系统的控制组件和整个生产线被迫停止运转

- 2015年12月,乌克兰电力公司设备被攻击事件，KillDisk恶意组件，造成线路堵塞，致使电力公司维修部门无法正常工作

- 2015年6月,波兰航空公司操作系统遭遇黑客攻击，导致长达5个小时的系统瘫痪

- 2016年10月，外国间谍入侵澳大利亚关键基础设施网络

- 2010年9月，伊朗的震网病毒事件，病毒攻击目标直指核设施，病毒使离心机在失控情况下不断加速而最终损毁

- 2010年9月，印度鲉鱼级潜艇技术即机密文件泄漏

- 2018年8月,台湾积体电路制造股份有限公司(TSMC，以下简称“台积电”)事件，遭遇病毒为“WannaCry”的变种，造成感染后的机台宕机或是重复开机，生产线停摆

固件方面

固件方面主要安全漏洞：

- 通用服务方面：

主要漏洞：HTTP、FTP、SNMP、TELNET、SSH等服务程序存在安全漏洞；应用程序逻辑漏洞（如HTTP）

产生原因：组件版本过低、应用程序编程缺陷

应对措施：升级补丁；关闭非必要服务（设备自身、边界访问控制设备）；安全的编程+严格的测试

固件方面

固件方面主要安全漏洞：

- 协议栈方面：

  主要漏洞：协议健壮性问题，导致短时失去响应甚至宕机

  产生原因：校验机制不完善

  应对措施：以白名单方式对所有的请求进行校验，不符合协议规约的请求包一律丢弃

固件方面

固件方面主要安全漏洞：

- 补丁升级：

  主要漏洞：伪造、植入恶意程序的升级包

  产生原因：缺少升级包文件的完整性、真实性校验机制

  应对措施：对升级包文件进行签名，升级时验签

固件方面

固件方面主要安全漏洞：

- 其他方面：

主要漏洞：鉴别信息硬编码、缓冲区溢出、敏感信息（组态程序）明文存储、代码质量安全/缺陷等

产生原因：编程缺陷、白盒测试不充分

应对措施：加强人工代码审核、完善代码白盒测试

敬畏每一行代码

工控协议方面

工控协议方面主要安全缺陷：

工控协议特点：不支持身份认证、无加密措施；具有应用层的完整性校验措施。

- 数据包重放攻击：

主要缺陷：数据包重放攻击、实现对工控设备的启停、点位控制等

产生原因：无身份验证措施、会话安全措施不足

应对措施：增加身份认证措施、增加会话序列号/随机数/时间戳等；限制会话的IP/MAC地址

上位机软件方面

上位机软件方面主要安全缺陷：

- 传统软件的信息安全问题：

  主要缺陷：身份鉴别机制缺陷（上位机本地验证）、访问控制绕过、敏感信息明文存储等

  产生原因：编程缺陷

  应对措施：加强人工代码审核、完善代码白盒测试；对上位机操作系统进行强加固

上位机软件方面

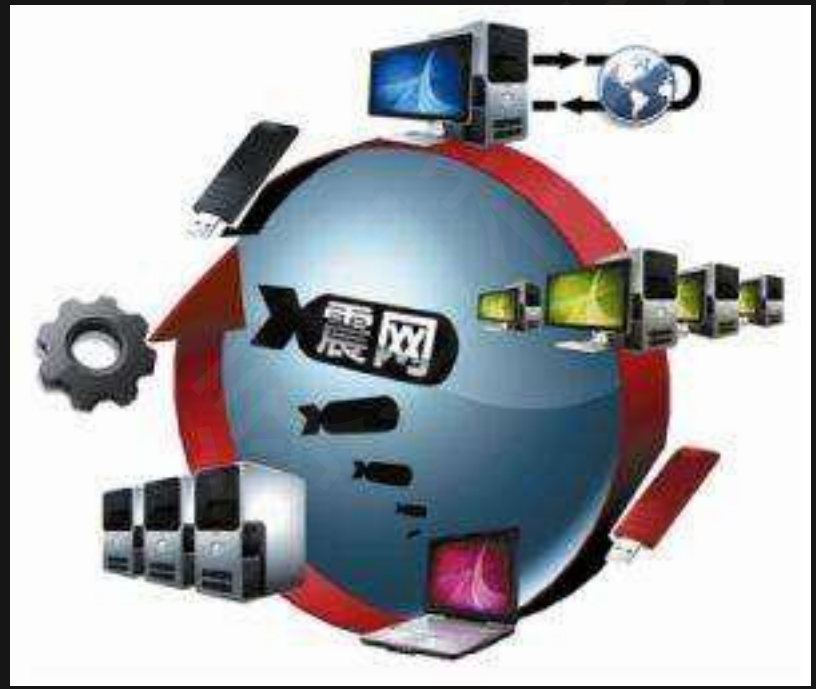
上位机软件方面主要安全缺陷：

- 可执行文件篡改：

  主要缺陷：可对可执行文件（包括DLL文件）等进行篡改

  产生原因：缺少文件签名及验证机制

  应对措施：对重要文件进行签名，调用时验证；主机白名单产品防护

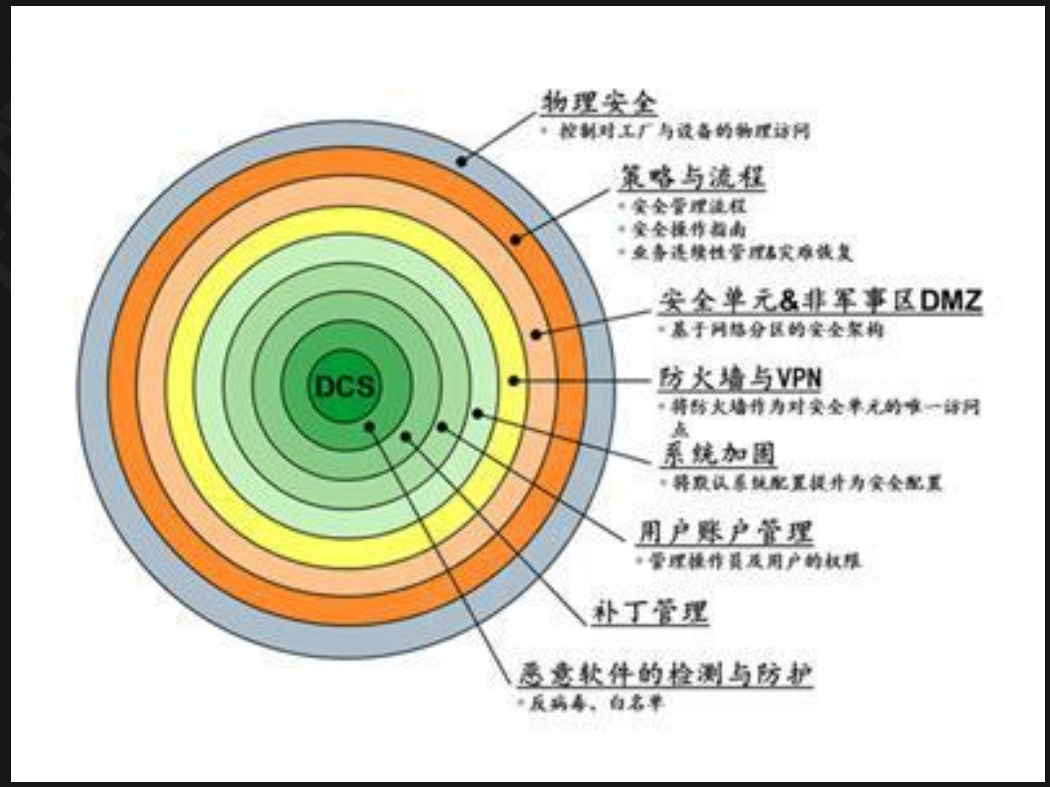


工控设备漏洞特点


05
一旦被利用，后果非常严重
04
固有的安全问题难于短期内得到解决
03
漏洞修复严重依赖设备厂商
02
漏洞修复周期长
01
安全漏洞普通存在

系统层面的漏洞防御


物理安全防护
多层次边界防护
全面的审计监控
严格的主机防护
细致的安全管理
充分的安全测试
纵深防御


物理安全
策略与流程
安全单元&非军事区DMZ
防火墙与VPN
系统加固
用户账户管理
补丁管理
恶意软件的检测与防护
DCS

谢谢！

公安部第三研究所
The Third Research Institute Of Ministry Of Public Security

MSTL
国家网络与信息系统
安全产品质量监督检验中心

NSFOCUS