- 工业控制网络安全误区
- 误区一、Control Systems aren't Vulnerable to Hackers or Viruses

（控制系统对黑客或病毒来说不是那么脆弱）

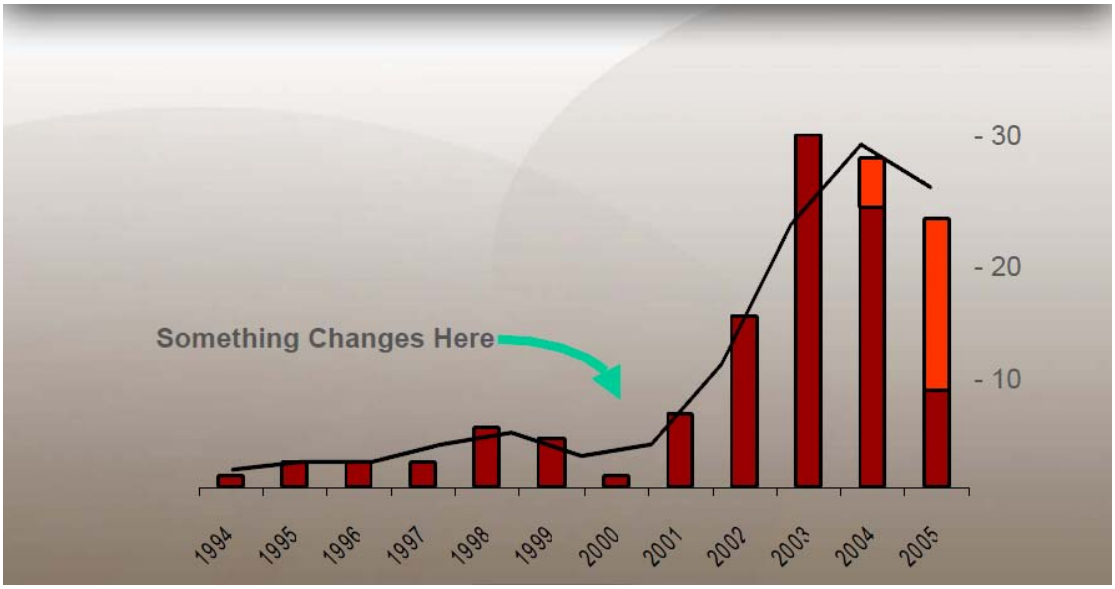
佳士拿汽车工厂事件 - 多个地点受影响

- 2005 年 8 月 13 日美国的佳士拿汽车工厂被一个简单的电脑病毒关闭了。
  - 尽管公司网络与互联网之间已安装了专业防火墙，病毒依然能进入了工厂的控制系统（可能是通过一台笔记本电脑）。
  - 一旦进入了控制系统,病毒就能够在几秒钟之内从一个車间感染到另一个車间。
- 大约 50,000 流水线工人因此要暂停工作在这期间。
- 该事故的原因是什么？就是一个叫 **Zotob** 的蠕虫病毒经过第二通道进入了网络。
- 估计损失影响为 1,400 万美元。

美国 Browns Ferry 核工厂的“安全”事件 ：

- 2006 年 8 月因反应堆在‘高功率、低流量条件’的危险情况下, Browns Ferry 核电厂所有人员不得不全部撤离。
- 控制循环水系统的冗余驱动器失效了，原因是控制网络上“过量交通”的缘故。
- 可能是两种不同供应商的控制产品产生了通讯过荷现像。
- 该事故的原因是什么？不当和过度的交通在控制网络上。
- 核电厂因此停机 2 天,估计损失的费用约 60 万美元。
- **水处理入侵, Harrisburg, PA**
- 2006 年 10 月一部被感染的笔记本电脑(维修用的),黑客入侵了在美国宾夕法尼亚州的哈里斯堡水处理厂的计算机系统 。
- 被攻破的笔记本电脑是通过互联网，然后与一个 VPN 连接作为切入点用来安装病毒和间谍软件在这工厂 SCADA 系统的 PC 里。
- 虽然进攻目标似乎並没有在水的质量上，但此事如果没有被发现的话，恶意软件随时可以干扰了工厂的业务 。
- 误区二、Nothing Much Has changed (so we are Safe)

（目前为止没有什么事情发生，所以我们是安全的）



2001 年之前特点

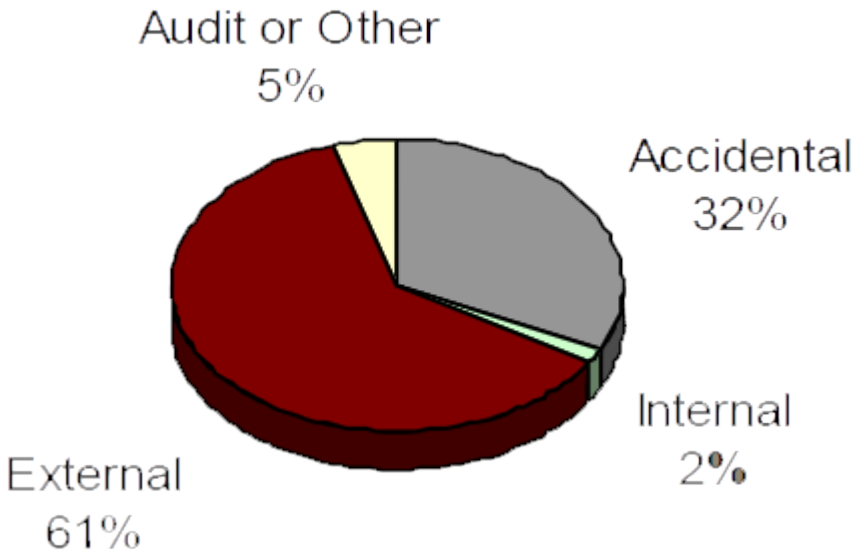
敌对事件为主要原因:

- 不合适的雇用活动
- 不满意的雇用员工
- 偶然事件

2001 年之后特点分析：

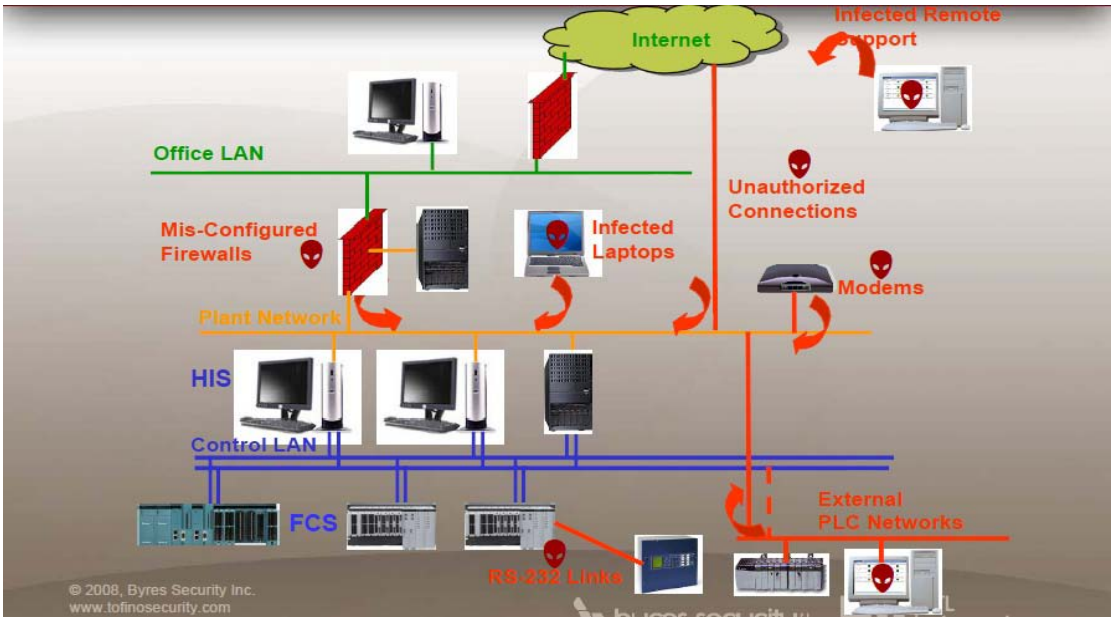
大部分为外部攻击:

- 系统突破
- 病毒/特洛伊/蠕虫
- 拒绝服务（DOS)
- 阴谋破坏



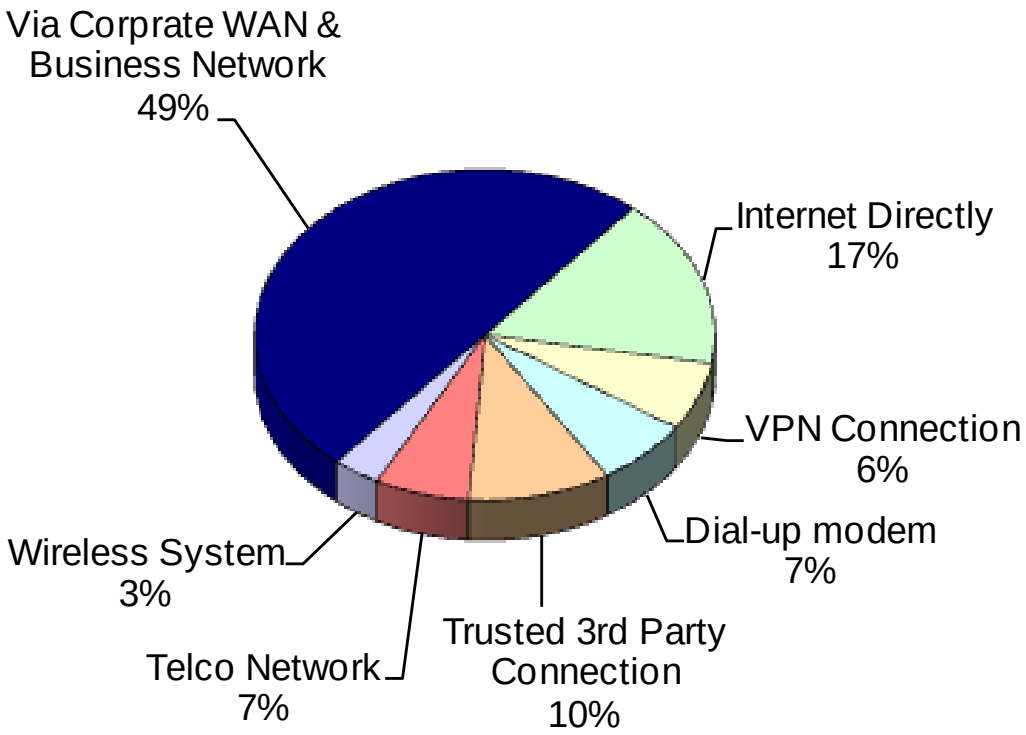
- 误区三、The SCADA System is Safe Because We Don’t Connect to the Internet

（我们的控制系统没连因特网，所以控制系统很安全）



连接到 WANS 和 MES

- 直接从因特网
- 被信任的第三方
- 连接到 PC 网的笔记本电脑



通过对 37 个来自金融、能源、电信、多媒体、自动化和安全公司的防火墙的调查：

大约 80%的防火墙允许内部规则的任意服务和不安全的登录，这是一个重大错误

防火墙组态错误定量研究

Avishai Wool ， IEEE Computer Magazine

IEEE Computer Society, June 2004

- 误区四、Hackers Don’t Understand SCADA/PLC/DCS

（黑客不懂 SCADA/PLC/DCS）

- ***Brum2600 Blackhat Conference:***

“事情开始变得有趣了…讨论议题就像是讨论‘用玻璃杯装着的水是多么的安全’，英国水资源管理部门讨论一次用无线电射频系统来控制的系统故障分析，这种系统可以被滥用、擅自试用和轻易地破坏”

Source: The Register, October 20, 2003

- **Talk #16: SCADA 系统暴露出很多问题，在这些系统或者子系统上的信息攻击可以通过远程登录或者同时多重登录实现，本议题侧重于今天日益增多的 SCADA 系统的结构和攻击分析及一般的 SCADA 通讯协议分析**

Source: Toorcon 2005 Website