RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

实现 SCADA 安全性为什么是一场攻坚战？

Amol Sarwate
Qualys Inc.

RSA CONFERENCE CHINA 2012
RSA信息安全大会2012

会议 ID： MN-2005
会议级别：中级

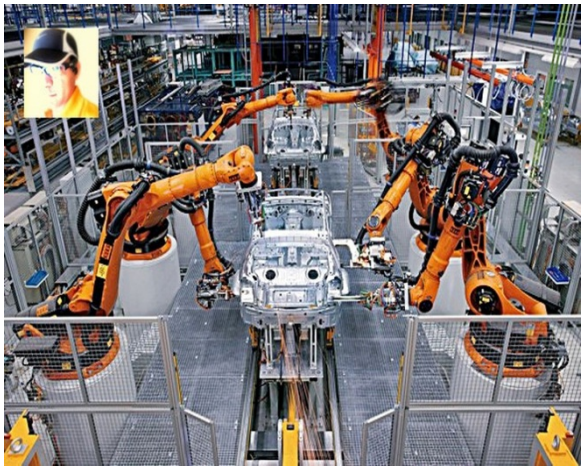
议程

- SCADA 基础知识
- 威胁（位置、原因和方式）
- 挑战
- 提议
- ScadaScan 工具

什么是 SCADA 系统？








事故

输油管道故障

http://www.ntsb.gov/doclib/safetystudies/SS0502.pdf

电力故障

http://www.nerc.com/docs/docs/blackout/Status_Report_081104.pdf

其他事故

http://en.wikipedia.org/wiki/List_of_industrial_disasters

恶意破坏

恶意破坏者破坏绝缘装置

http://www.bpa.gov/corporate/BPAnews/archive/2002/NewsRelease.cfm?ReleaseNo=297

内部人员

满腹怨言的员工

http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

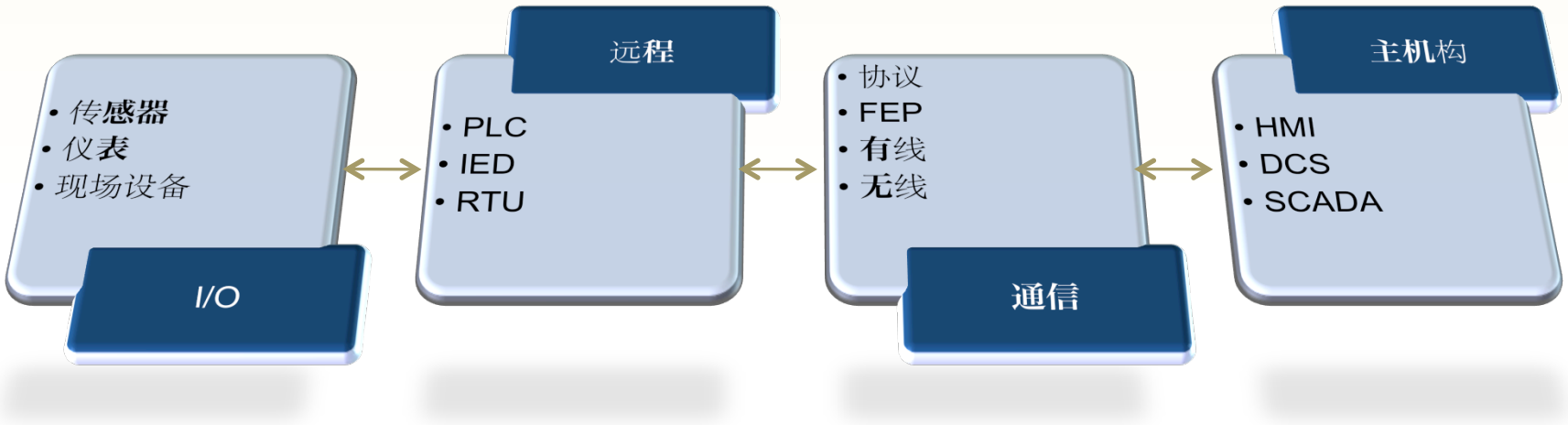
APT

（高级持久威胁）

恐怖行动或间谍活动

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

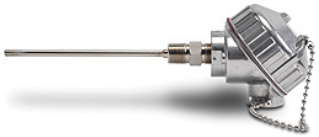
基本配置

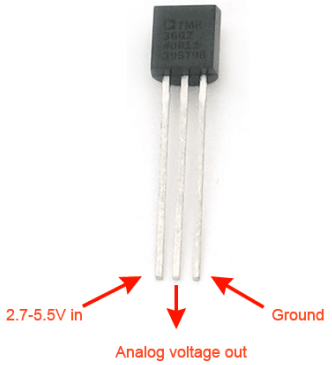


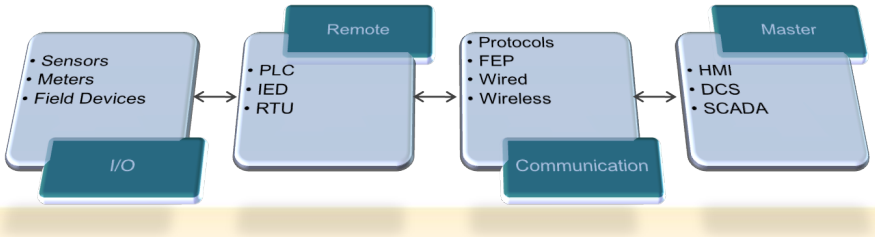
现场 控制中心

收集

将光、温度、压力或流量等参数转换为**模拟信号**





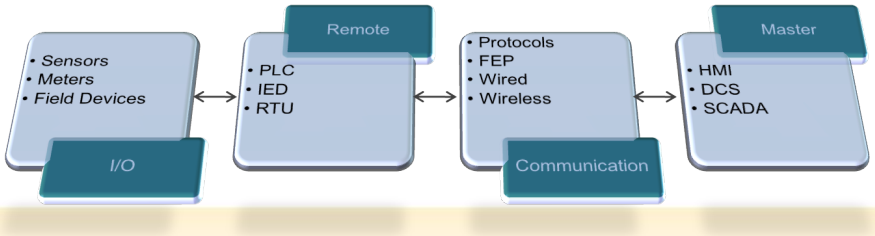


QUALYS®

转换

将模拟**和不**连续**的**测**量**值转换为**数字信息**



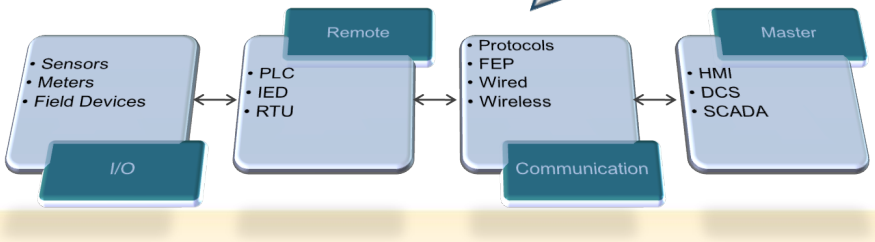



通信

前端处理器 (FEP) 和协议
有线或无线通信

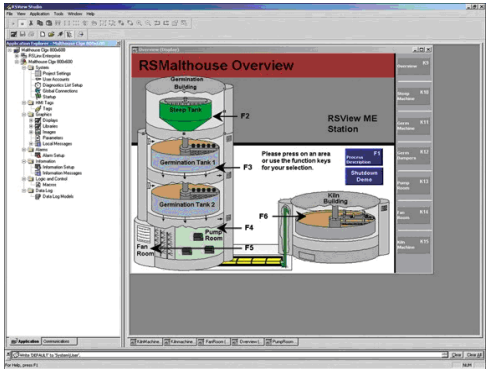


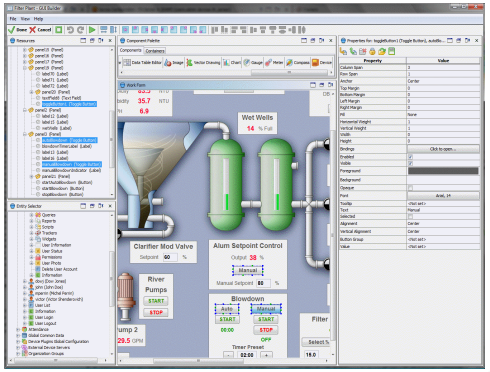
Modbus	DNP 3	OPC
ICCP	ControlNet	BBC 7200
ANSI X3.28	DCP 1	Gedac 7020
DeviceNet	DH+	ProfiBus
Tejas	TRE	UCA

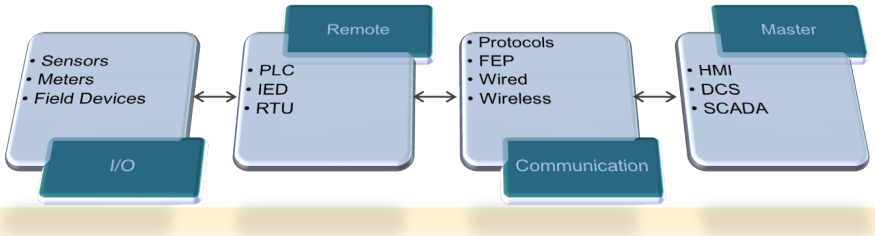


显示和控制

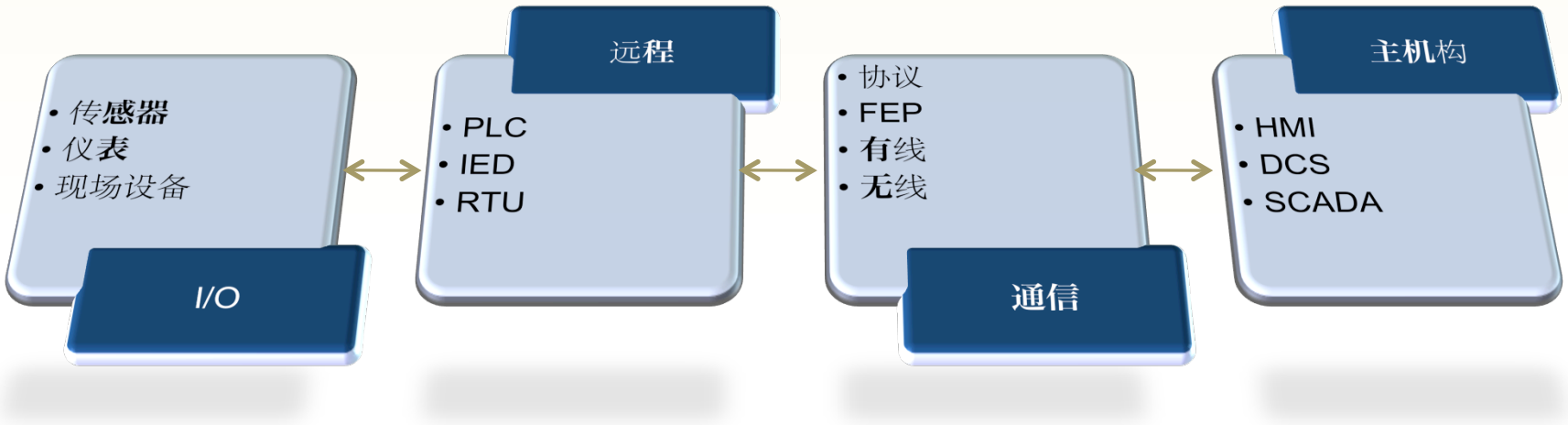
使用人机界面 (HMI) 控制、监视**和**报警

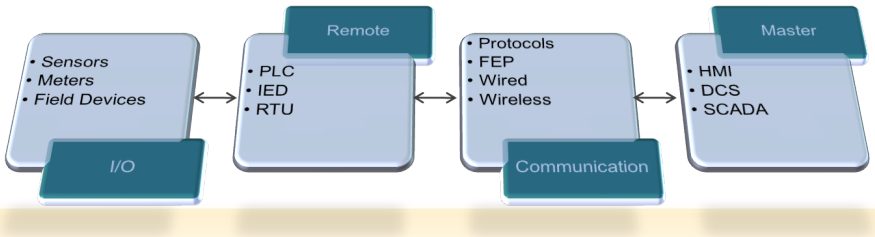




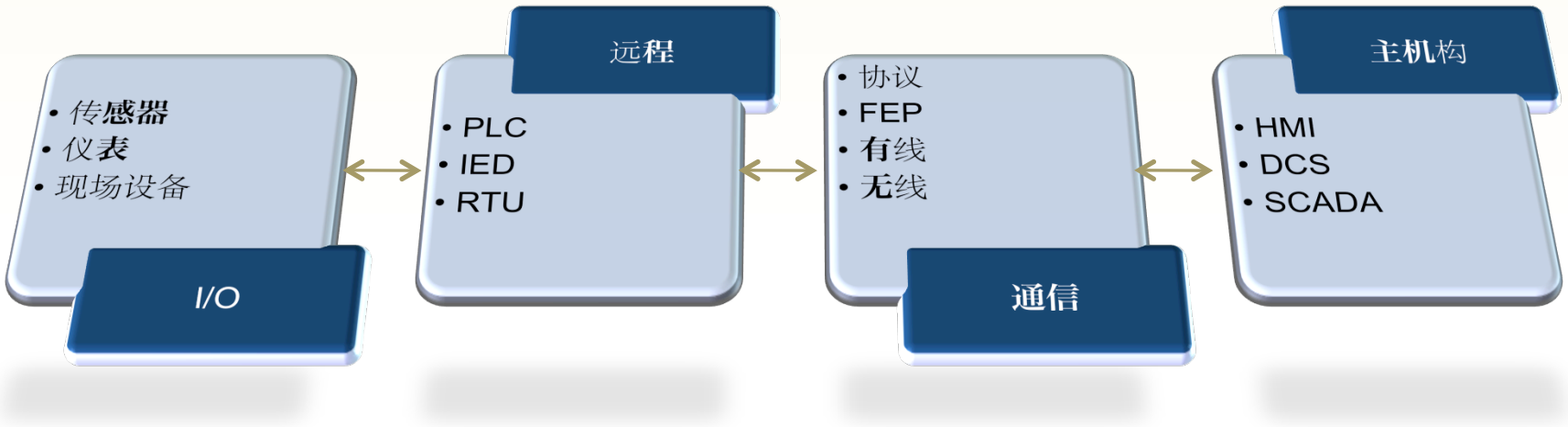


威胁？


• 传感器
• 仪表
• 现场设备
I/O
远程
• PLC
• IED
• RTU
• 协议
• FEP
• 有线
• 无线
通信
主机构
• HMI
• DCS
• SCADA

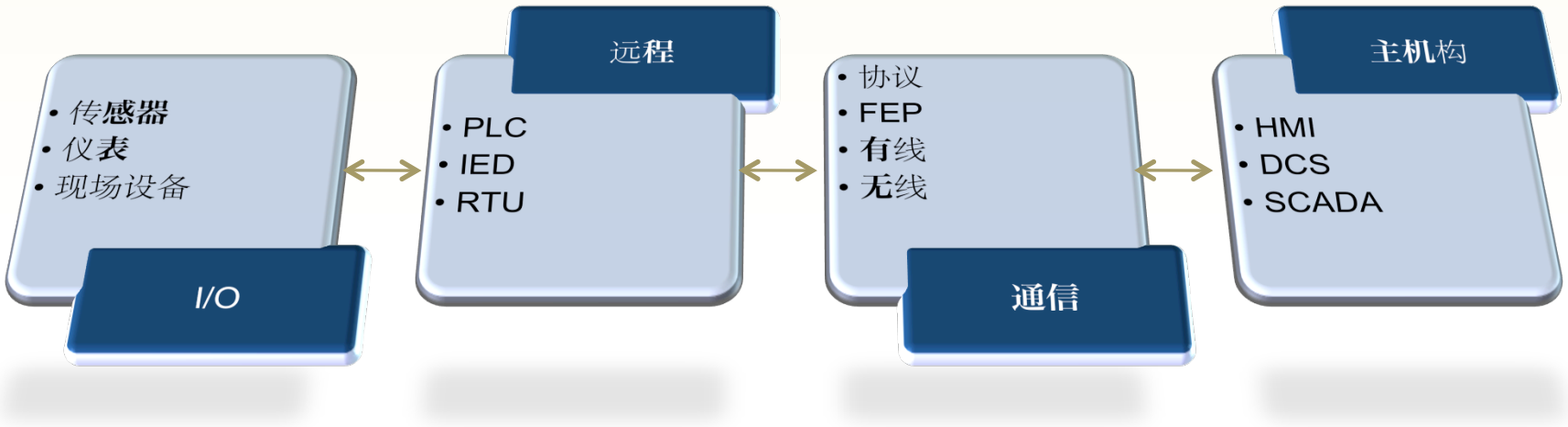

• Sensors
• Meters
• Field Devices
I/O
Remote
• PLC
• IED
• RTU
• Protocols
• FEP
• Wired
• Wireless
Communication
Master
• HMI
• DCS
• SCADA

io 和远程



- **需要物理**访问
- 现场设备**通常不包含流程信息**
- **缺少流程信息会**导**致无**谓**的中断**

通信



- 更改 FEP 输出
  哪个是 HMI 输入
- 协议威胁

ScadaScan (示例)

```
C:\SCADA>perl scadascan.pl

Usage: scada_scan.pl [-m|-d] (-r|-t) target_IP
Options:
        -m : Modbus bruteforce slave ID
        -r : Rate at which Modbus packets are sent.
             1 = fastest, 5 = slowest. Possible values 1 to 5
        -d : Scan for DNP 3.0 TCP
        -t : Read timeout in seconds.
```

```
C:\SCADA>perl scadascan.pl -m 10.40.1.182

Working on 10.40.1.182.......................... Modbus unit ID 28 found
```

协议

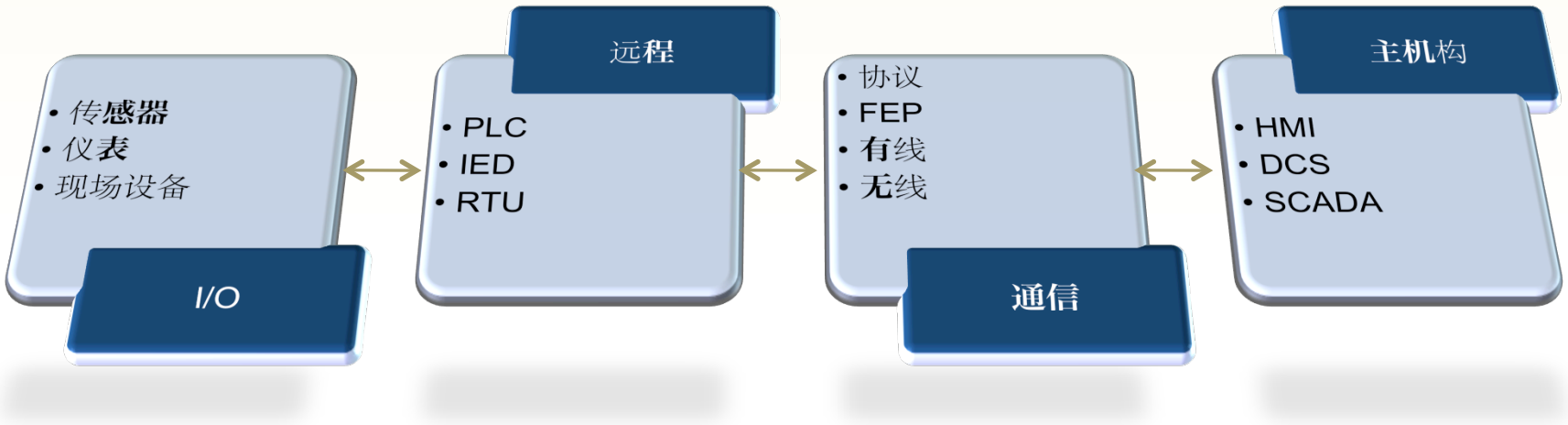
modbus 或 DNP 3 等 SCADA 协议**可提供哪些信息？**

身份验证**和授权**

Secure DNP 3.0

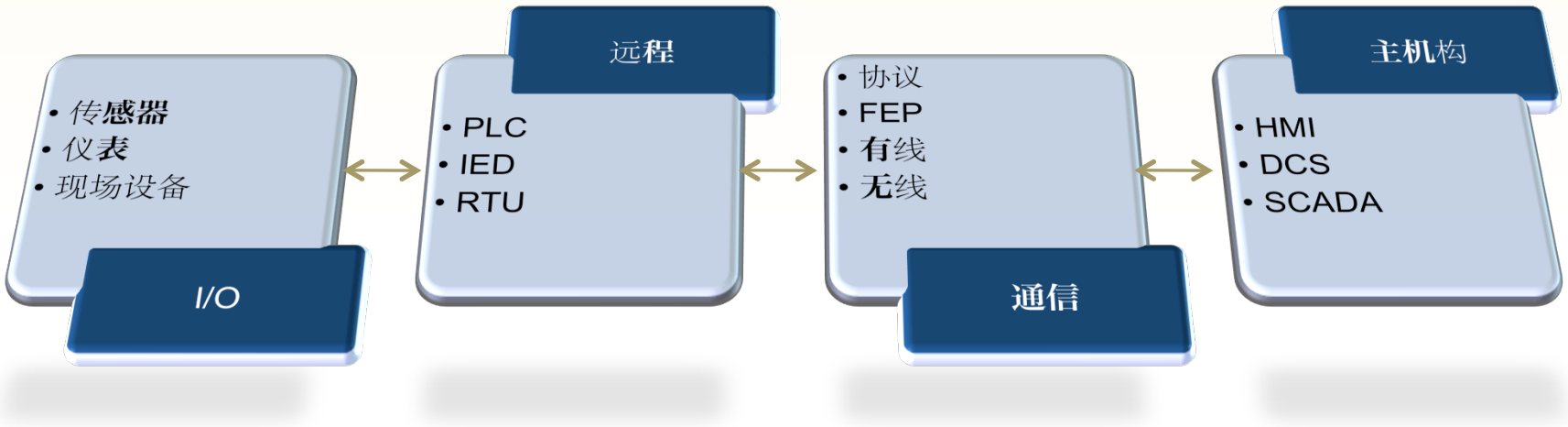
1.0 版规范已于 2007 年 2 月发布
身份验证
    初始化
    定期
    关键操作码请求
    实施细则
加密
    用于消息认证的密钥哈希 (HMAC)
密钥管理
新操作码

主机构威胁



- **控制**连**接到企**业**网**络**或互**联**网的系**统**网**络
- **无身份**验证**或每用**户**身份**验证
- **共享密**码**或默**认**密**码
- **没有密**码**更改策略**

主机构威胁



- 不进行修补
- 多年未重新启动
- 不需要的服务
- 现成的软件

挑战

- SCADA 系统生命周期很长
- 很难升级且成本高昂
- SCADA 供应商不提供有关操作系统修补程序的测试或指南
- 某些系统由 SCADA 供应商管理
- 数据历史记录和其他系统位于 SCADA 网络中
- 错误的想法 - SCADA 足够隐蔽，不会引起黑客的注意

主意

- 针对密码策略、访问控制和访问角色制定战略
- 制定软件升级和修补战略
- 建立 SCADA 测试环境
- 对 SCADA 供应商的要求：
  - 加快对操作系统修补程序的测试和审批
  - 更新、更安全的协议
- 应用 IT 网络管理和安全方面的体验
- 实施 SCADA 供应商审核和扫描

谢谢大家！

Twitter： @amolsarwate
http://code.google.com/p/scadascan/

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012