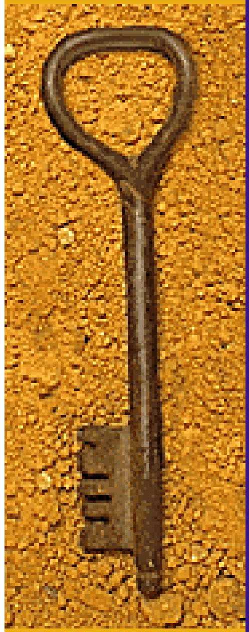
Vulnerabilities & Incident Response in Control Systems

Dale Peterson

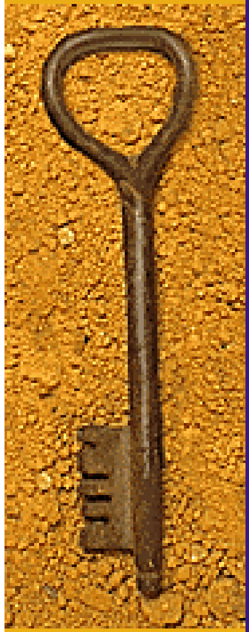
Digital Bond, Inc.

peterson@digitalbond.com



Digital Bond

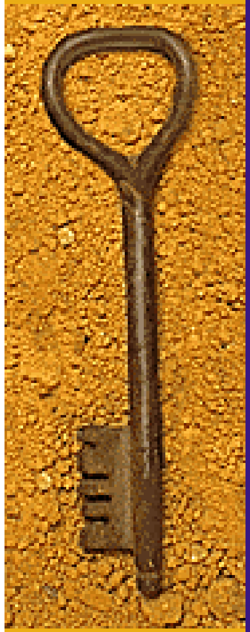
- Control System Security Practice
  - Research and Consulting
- Available on Digital Bond Site
  - IDS Signatures for Control System Protocols
  - Nessus SCADA Plugins
  - SCADA PLC Honeynet
  - Blog, SCADApedia, White Papers, Podcasts
  - SCADA Security Scientific Symposium (S4)



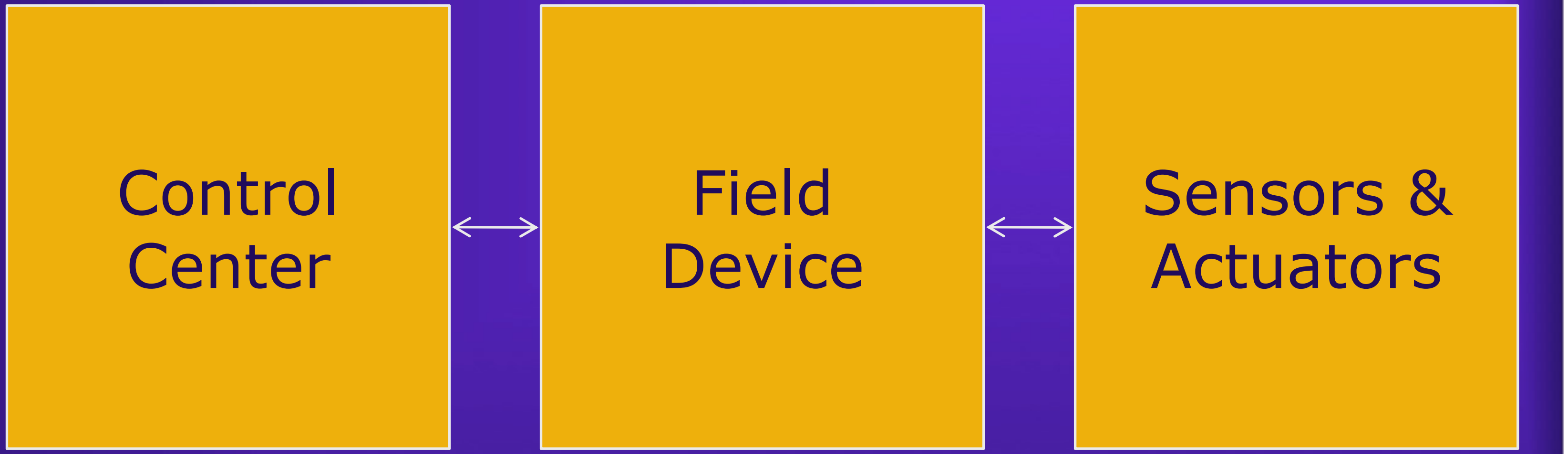
Control Systems

- Monitor and control physical processes
  - SCADA: Supervisory Control and Data Acquisition (WAN)
    - Oil Pipelines, Trains, Electric Transmission
  - DCS: Distributed Control System (LAN)
    - Manufacturing, Power Generation, Refinery
  - Very similar technologies

Get Out of the Data Center - - Wear a Hard Hat



Simplified Control System



Control Center

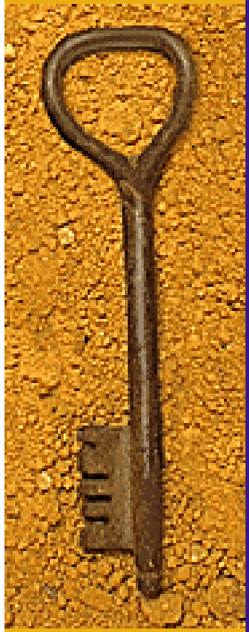
Field Device

Sensors & Actuators

Realtime Servers
Historians
Operator Stations

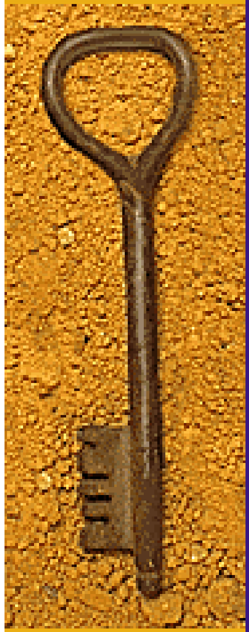
PLC’s
RTU’s
IED’s

Flowmeters
Gates and Valves



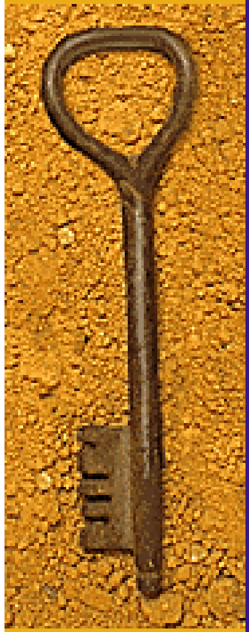
RESPECT

- ♦ Control Systems lag IT and IT Security by at least 5 years, but …
  - – They control very complex processes with 10,000+ or even 100,000+ points
  - – Timing is extremely important, 4 ms typical
  - – Huge automation, one or two operators can run an entire plant, pipeline, water treatment, train
  - – Highly reliable, 24 x 7 x 365 for years
    - No downtime in many control systems
    - Failure can cost lives or huge economic damage



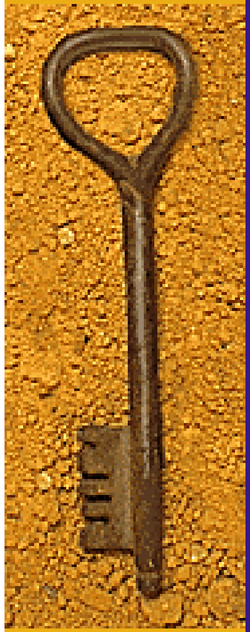
Why No Cyber Security?

- ♦ Control systems were truly isolated
  - – Serial protocols designed for control systems
    - 4-20 mA, still represent maybe 80%
  - – No Ethernet, IP or TCP/UDP
  - – Difficult to reach or attack the system without a physical connection to the network
  - – Even with connection requires specialized tools and a lot of control system knowledge



What Changed?

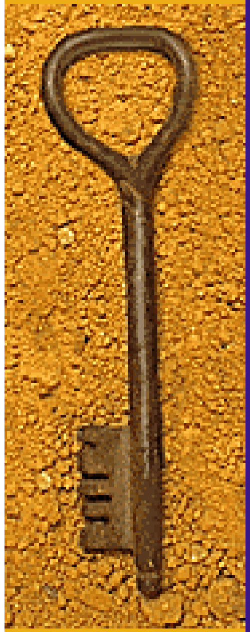
- 90’s the PC invaded the control center
  - Customers demanded it
  - Vendors enjoyed leveraging Windows
  - Ethernet NIC’s and LAN’s were deployed
  - Enter the IP stack and routing
- Next “SCADA” data was sent to enterprise
  - Valid business reasons
  - No thought of security implications



Field Devices

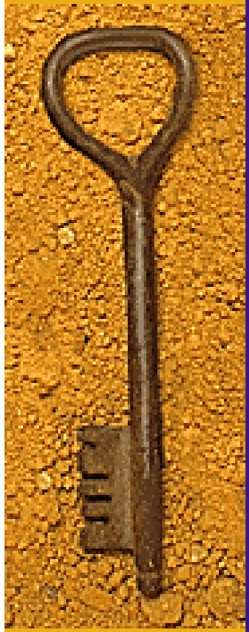
- ♦ Field devices add Ethernet interface
  - – Lower cost, ubiquitous, higher data rate
  - – Non deterministic, no guaranteed performance
- ♦ Approach 1: Industrial Ethernet
  - – Token approach over Ethernet
- ♦ Approach 2: True Ethernet
  - – Protocol encapsulated in TCP/UDP packet

Field Devices More Accessible to Hackers



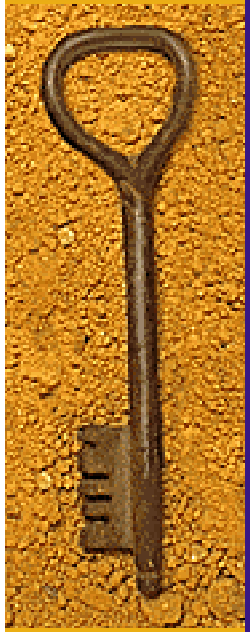
Control System Security

- Catching up after the exposure
- Network segmentation with firewalls
  - Enterprise now needs even more SCADA data
  - BUT NOT CONTROL
  - Learning DMZ’s, least privilege rulesets
- Anti-virus
- Patching - - huge issue
- Administrative controls



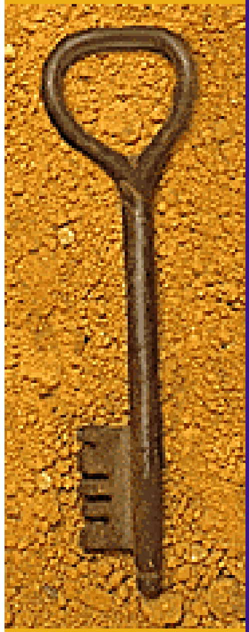
Latent Vulnerabilities

- Testing of ‘Good’ data and packets
  - Does the system work with extreme reliability?
- No testing of ‘Bad’ data or packets
  - Scans or light fuzzing will crash systems!
- Partial implementation of protocols
  - Even legal protocol messages cause crashes
  - Example: broadcast and multicast
- Build your own or buy untested stacks



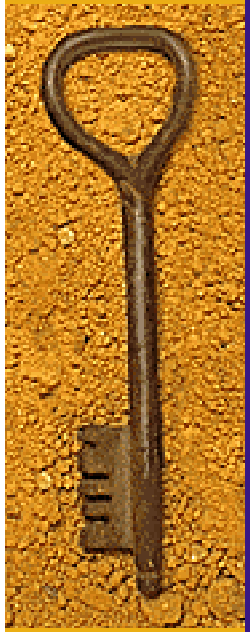
Security Development Lifecycle

- Little attention to secure coding standards and other elements of the SDL
- Poor architecture and semi-custom
  - Many patches cannot be applied
  - Detailed testing is required
- Repeat of everything you have experienced with IT applications in the last 2 decades
- Vulnerabilities are found by accident
  - Field device TCP/IP stacks
  - Control center proprietary app ports



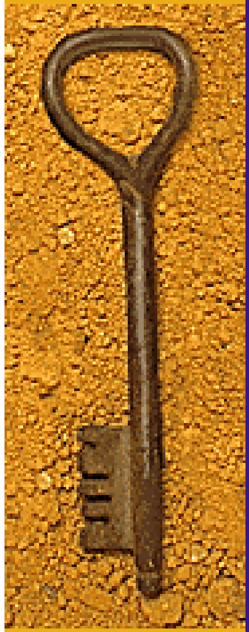
How Can You Help?

- You = FIRST and Coordination Centers
- Repeat what you did for the IT user and vendor community
  - Seriously! Have a meeting and remember what worked and repeat. (We are 5 years behind)
- Attend control system industry events
  - Educate the control system community
  - Learn and develop two-way trust
  - Most control system vulns are not reported



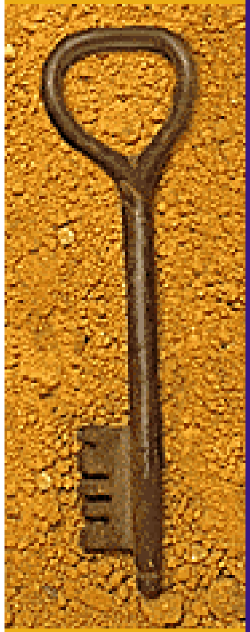
Reporting Problems

- Real World 2007/2008 Example
  - GE Fanuc vulnerabilities took 11 months to get to the right point of contact despite diligent researcher and CERT efforts
- Proactively engage the community
  - Develop points of contact for incident handling
  - Persuade the vendor to implement common vulnerability contact methods
  - Persuade users and researchers to report



Market Differences

- ♦ Geographic
  - – US approach vs. UK approach
- ♦ Market Sectors
  - – Similar technologies
  - – Different communities, protocols, vendors
  - – A single organization for critical infrastructure?



Questions?

Dale Peterson
Digital Bond, Inc.

954-384-7049
peterson@digitalbond.com