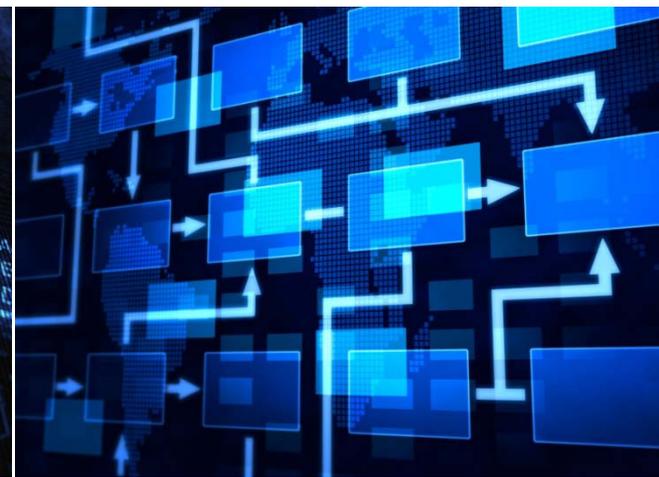




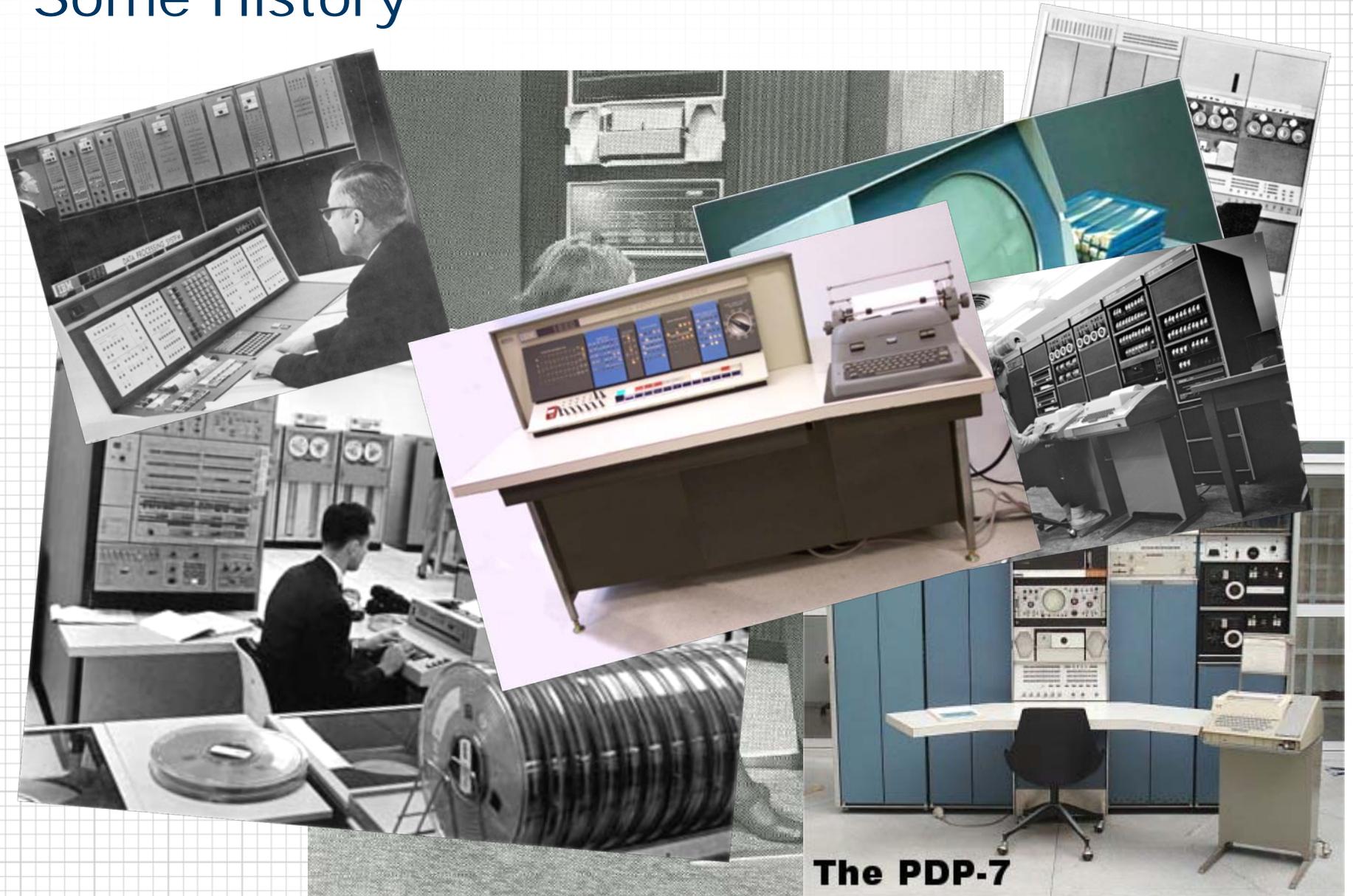
Security and Configuration Consoles and Other Physical/Virtual Communication Ports

Clyde Poole, CISSP
Chief Security Officer
TDi Technologies, Inc.

ConsoleWorks®



Some History



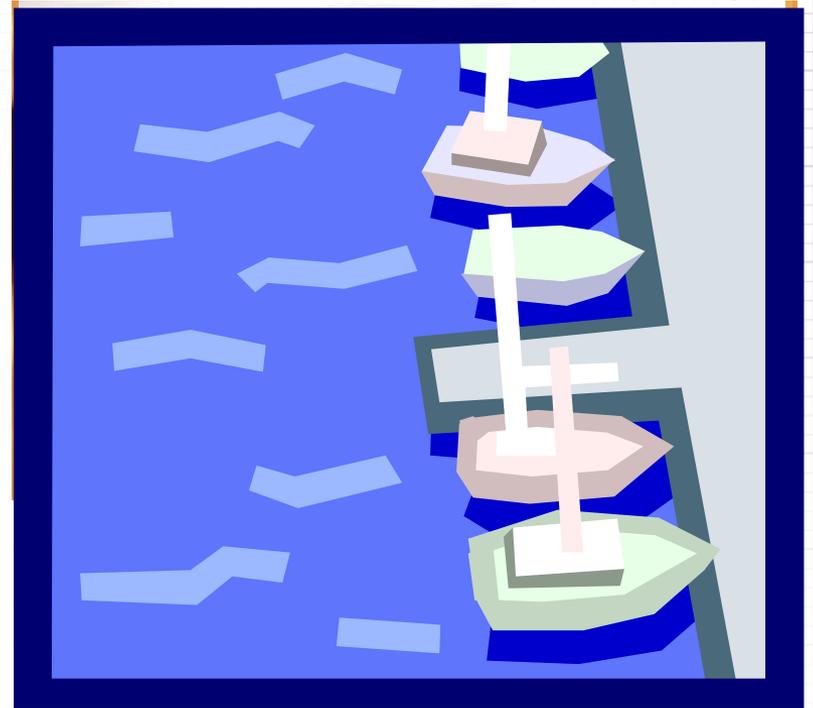
The PDP-7

And Then We Junked the Console Devices



What is a "Port"?

- Network/IP Port
- Serial Port
- Console Port
- Configuration Port
- USB Port
- Virtual or Physical?





Physical “plugs” or connectors

- Physical Access is a Security Risk
 - Password Recovery mechanisms
 - Use your own cable
- Labels that say “Do Not Use” are red flags
- Disabling Sometimes Prevents Future Configuration Changes
- Often Required in Emergencies
- Detecting Use or Tampering is Important

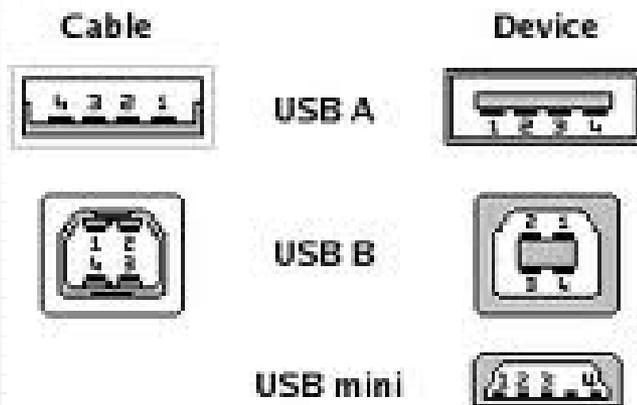
Console Ports

- Physical, Network, or Virtual
- Last Gasp Messages
- Often Protected by “default” usernames and passwords
- Network Enabled
 - iLO
 - ALOM
 - ILOM
 - DRAC
 - HMC



USB Ports

- Needed for Keyboards etc
- Auto-Play a Huge Security Risk
- Detection of Use is good Security
- Misused by Employees to “charge” personal devices



Ports Not Monitored

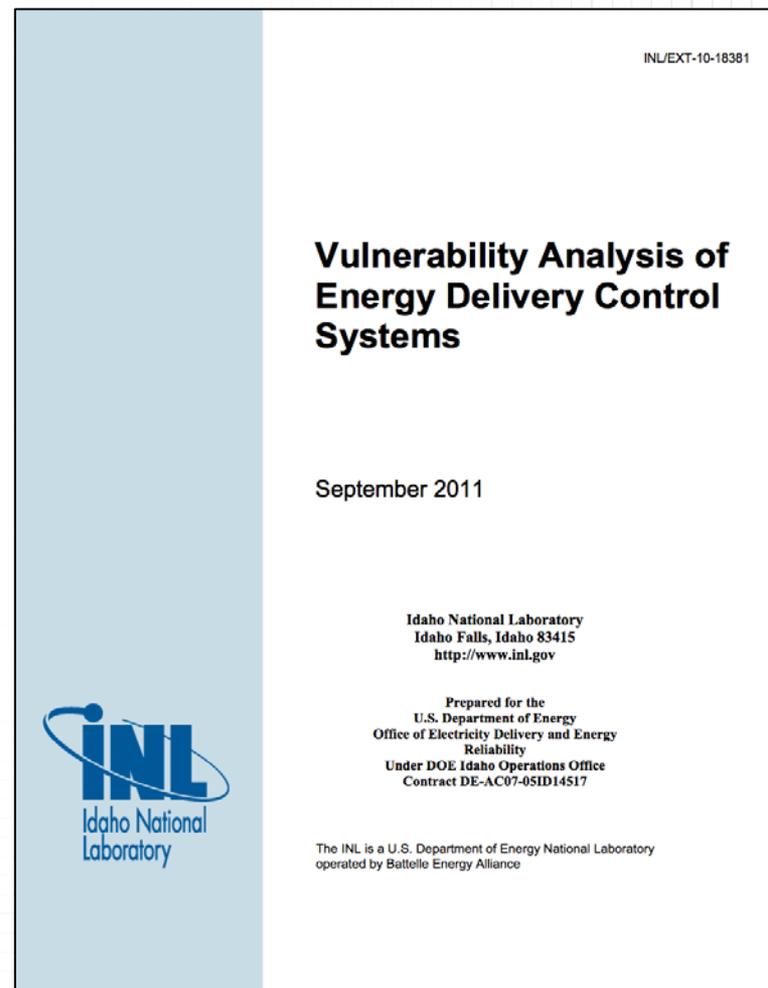
- Physical, virtual and logical console ports seldom monitored
- Clear Text protocols often used
- Web Based configuration interfaces hard to log

Terminal and Console Servers

- Used for management of systems with serial consoles
- Many are very old
- Default Usernames and Password
- No authentication of connection to consoles
- Telnet protocol predominant

INL Report

- Prepared for the Department of Energy
- Focused on Security Vulnerabilities in DCS
- Presentation will discuss a small portion of the information contained in the report

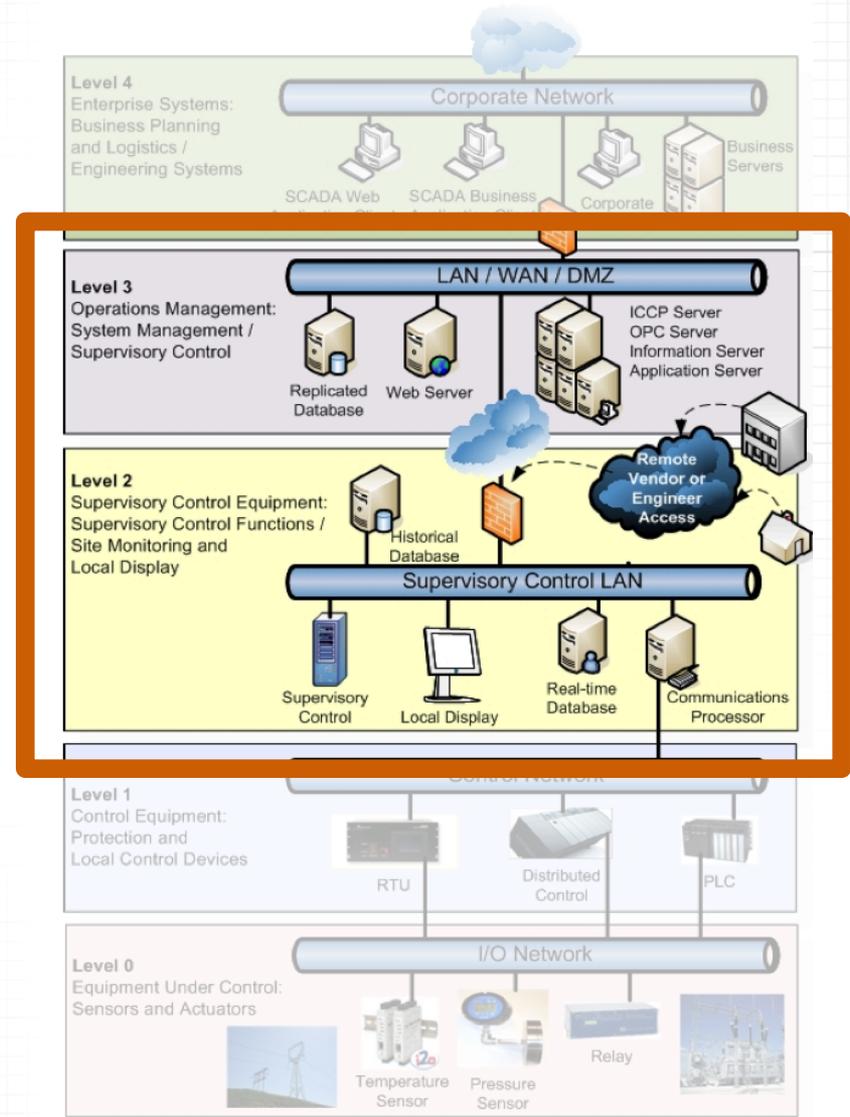


Report Findings

Level	Frequency of Observed Vulnerabilities	
1	Local or Basic Control	10%
2	Supervisory Control	45%
3	Operations Management	40%
4	Enterprise Systems	5%

85% of Observed Vulnerabilities affect

- Privileged Users
- Privileged Interfaces
- Privileged Devices



ISA SCADA architecture by functional-level reference model
 Source: Vulnerability Analysis of Energy Deliver Control System – By Idaho National Laboratory for the DOE

Top 10 Most Critical SCADA Vulnerabilities*

Vulnerability	Impact
Unpatched Published Vulnerabilities	Most Likely Access Vector
Web Human-machine Interface (HMI) Vulnerabilities	Supervisory Control Access
Use of Vulnerable Remote Display Protocols	Supervisory Control Access
Improper Access Control (Authorization)	Access to SCADA Functionality
Improper Authentication	Access to SCADA Applications
Buffer Overflows in SCADA Services	SCADA Host Access
SCADA Data and Command Message Manipulation and Injection	Supervisory Control Access
SQL Injection	Data Historian Access
Use of Standard IT Protocols with Clear-text Authentication	SCADA Credentials Gathering
Unprotected Transport of SCADA Application Credentials	SCADA Credentials Gathering

*Based on possible consequences, impact, ability to detect, attacker awareness, frequency of attack, remediation cost, prevalence

Report Recommendations for Utility Owners

	Recommendation	Mitigation*
1	Routinely assess operating systems, applications, services, network devices, etc., for published vulnerabilities.	Apply patches as quickly as possible or restrict access to and closely monitor vulnerable systems.
2	Assess and secure servers and clients – especially when access to the physical system.	Minimize access and available functionality of Web servers and clients.
3	Minimize usage, exposure, and available functionality of remote display protocols.	Configure remote access protocols to limit access, require secure authentication, and use a trusted path.

*Can be used as a starting point for mitigating the highest risk vulnerabilities.

Report Recommendations for Utility Owners

Recommendation	Mitigation
<p>4 Lock down all applications, hosts, and networks to limit the consequences of compromise as much as possible.</p>	Redesign network layouts to take full advantage of firewalls, VPNs, etc.
	Create security zones using multiple layers, with the most critical communications occurring in the most secure and reliable layer.
	Customize IDSs for SCADA hosts and networks.
	Restrict user privileges to only those that are required to perform each person's job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege).
	Replace insecure versions of common IT services with secure versions.

Report Recommendations for Utility Owners

Recommendation		Mitigation*
5	Use proven authentication services when available. Strong authentication and encryption mechanisms should be implemented and strenuously tested.	Securely configure authentication settings and regularly audit passwords and system settings.
6	Remediate vulnerabilities in SCADA services.	Reduce the risk from vulnerable SCADA services by limiting and monitoring their access.
7	Protect SCADA databases.	Databases should be replicated out to the DMZ.

Report Recommendations for Utility Owners

Recommendation		Mitigation*
8	Use secure protocols to access SCADA components.	Uninstall or disable insecure services where possible.
		Correctly configure services to protect credentials and provide secure authentication.
		Use secure protocols to connect to SCADA components.
9	Protect user credentials and make them inaccessible to an attacker. Passwords should be securely encrypted or hashed before being stored or transmitted.	Correctly configure all applications to securely store and transfer credentials.

Report also made recommendations for SCADA vendors.



Approaches for Mitigation or Solution

- Turn off management interfaces using WEB servers
- Never use telnet, ftp, or http for the transfer of any management information
- Secure all privileged and external interfaces on physical devices
 - Serial Console Ports
 - iLO, HMC, ALOM, DRAC, etc.
 - USB
- Detect use of physical ports that are normally NOT in use

ConsoleWorks®



Approaches for Mitigation or Solution

- Override well known, default and/or shared username/passwords (require individual authentication and authorization)
- Log all privileged access to systems at the keystroke level
- Monitor, log, alarm and investigate all security events
- Use technology to assist in reviewing logs and eliminate
 - “in arrears” detection of security events
 - Data overload
- Enforce good password construction, reuse and aging
- Require multi-factor authentication
- Reduce privileges to only those required

ConsoleWorks®

Questions?



ConsoleWorks®

Contact Information

Clyde T. Poole, CISSP
Chief Security Officer and Director of Professional Services
TDi Technologies, Inc.

clyde.poole@tditechnologies.com

Corporate Information

TDi Technologies, Inc.
1600 10th Street, Suite B
Plano, Texas 75074

<http://www.tditechnologies.com/>

sales@tditechnologies.com

ConsoleWorks®