

APPLIED RESEARCH AT BCIT



RESEARCH • DEVELOPMENT • SOLUTIONS

Myths and Facts Behind Cyber Security of Industrial Control

Eric Byres, P.Eng.
eric_byres@bcit.ca

John Kay, P. Eng.
jkay@udl.com

Joel Carter
jcarter@bcit.ca



www.tc.bcit.ca



Background

- BCIT Industrial Incident Database
 - Tracks network security incidents that directly impact industrial control operations.
- BCIT Internet Engineering Lab
 - Conducts security tests on control system products and designs.

Incident Information	
IncidentID	DE004
Event Date	2/9/1988
Title	PLC Password Change
Description	An unauthorized employee changes the password in a PLC belong to a different department via the PLC network.
Incident Type	Disgruntled Employee
Report Date	3/28/2002
Report Source	Company Engineer
Entry Author	Eric Byres
Report Reliability	Confirmed
Network System	Control System
Company	
Industry	Pub and Paper
Impact	Shut down of PLC to clear memory and reload program
Impact(\$\$)	\$0.00
Location	BC, Canada
Investigation	
Recommendations	
Following Work	





Five Myths of Industrial Security

- The Control System is Safe if We Don't Connect to the Internet
- We Need to Focus on those Terrorists
- The Bad Guys are all on the Internet
- The IT Department Looks After Process Security
- Hackers Don't Understand SCADA/PLCs



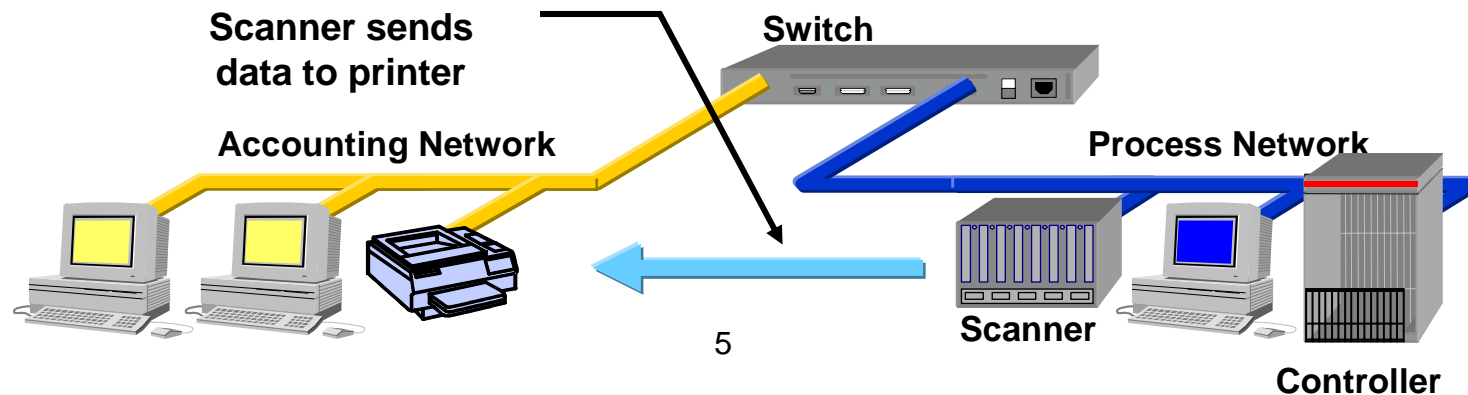
Myth #1: The Control System is Safe if We Don't Connect to the Internet

- **Audit Results:** Major paper company war dials its lines looking for modems with PCAnywhere.
- Average monthly results:
 - 20,000 numbers tested.
 - 975 Modems located (most known and secured).
 - 3 new unsecured modems located.



Myth #2: We Need to Focus on Those Terrorists

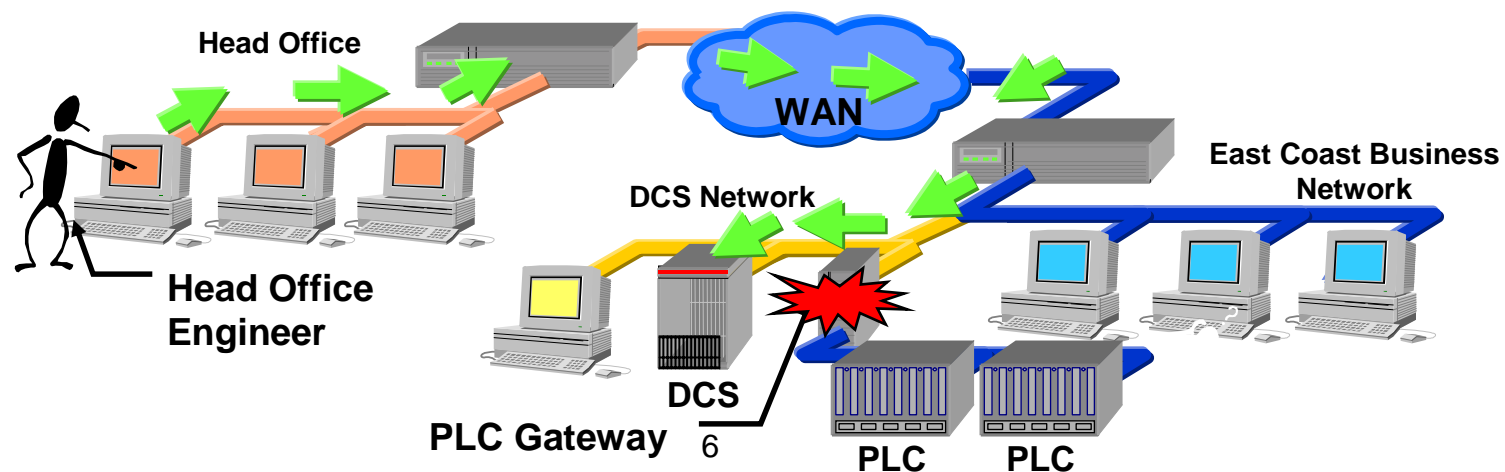
- Paper Machine Profile Controller Case History:
 - Controller & Scanners use TCP/IP to communicate.
 - Printer in admin gets same address as controller.
 - Scanners try to talk to printer instead of controller.





Myth #3: The Bad Guys are all on the Internet

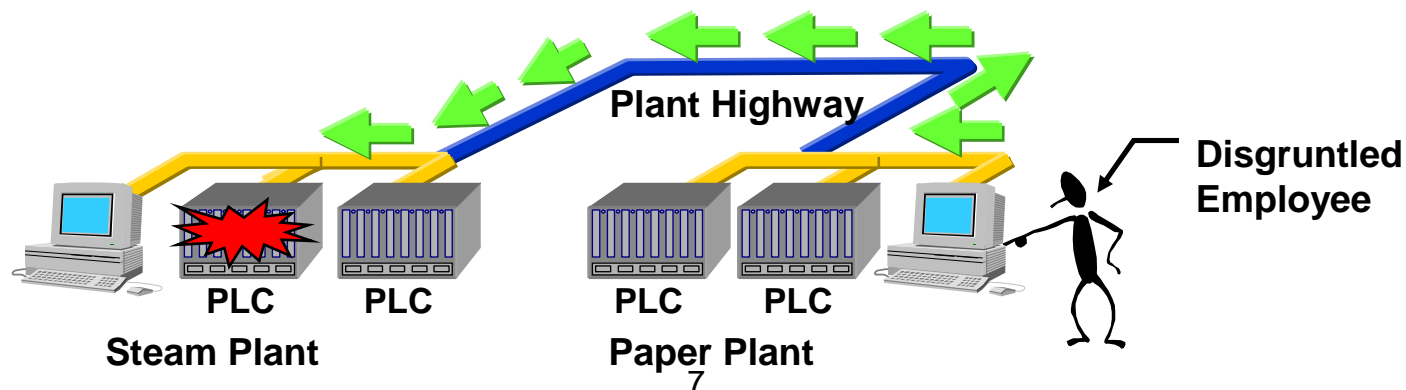
- **Incident:** Engineer loads program onto a DCS graphics station to send data to head office.
- New task overloads DCS/PLC gateways and operators lose control of plant motors.





Myth #4: The IT Department Looks After Process Security

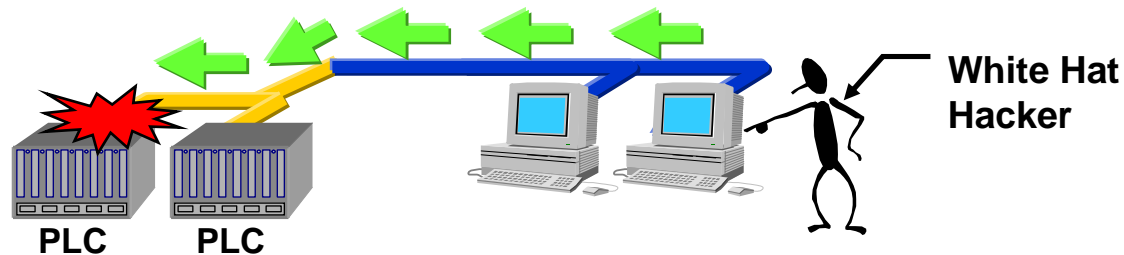
- **Security Incident:** Employee attacks PLC in another plant area over PLC highway.
- Password changed to obscenity, blocking legitimate maintenance and forcing process shutdown.





Myth #5: Hackers Don't Understand SCADA or PLCs

- **Internal Testing:** “White Hat” hacker with no knowledge of PLCs manages to block all communication from PLC within 1 hour of discovering device.





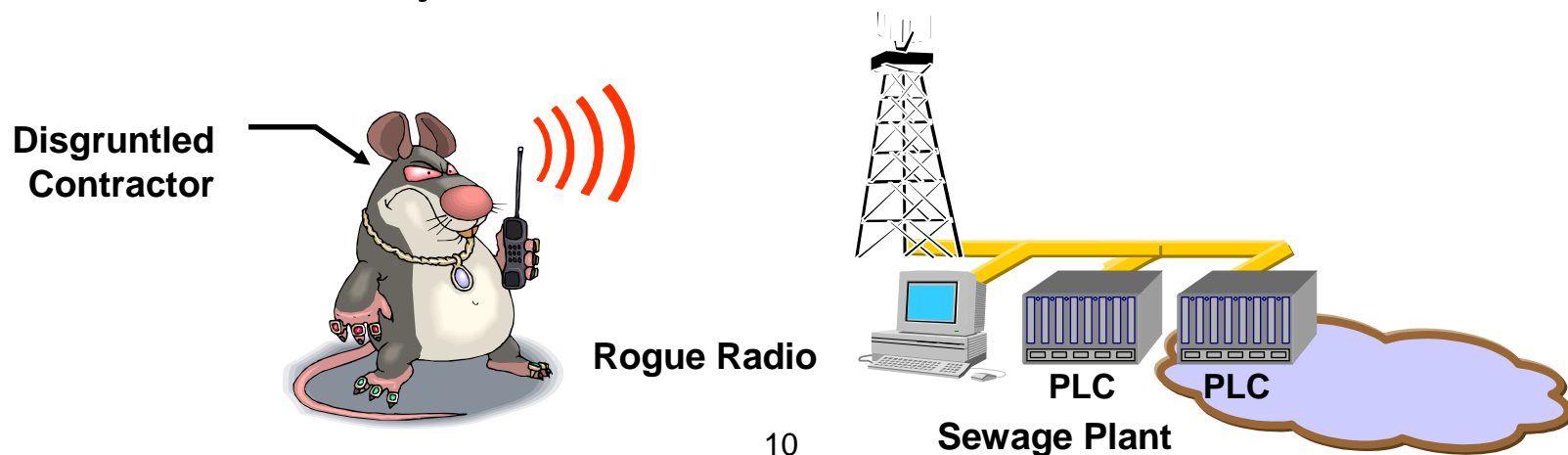
Combining Them All: The Maroochy Sewage Spill

- On October 31, 2001 Vitek Boden was convicted of:
 - 26 counts of willfully using a computer to cause damage
 - 1 count of causing serious environment harm
- The facts of the case:
 - Vitek worked for the contractor involved in the installation of Maroochy Shire sewage treatment plant.
 - Vitek left the contractor in December 1999 and approached the shire for employment. He was refused.
 - Between Jan and Apr 2000 the sewage system experienced 47 unexplainable faults, causing millions of liters of sewage to be spilled.



Combining Them All: The Maroochy Sewage Spill

- On April 23, 2000 Vitek was arrested with stolen radio equipment, controller programming software on a laptop and a fully operational controller.
- Vitek is now in jail...





Some Conclusions for Industrial Cyber Security

- Types of Incidents
- Sources of Incidents
- Dependence on IT Department Security
- Vulnerability of PLC/DCS Systems



Types of Incidents

- Cyber incidents can have a variety of causes. In rough order of severity:
 - Audit
 - Accidental
 - Non-malicious intrusion
 - Malicious intrusion



Sources of Incidents

- Serious security incidents can be caused by well intentioned employees.
- 60% - 70% of all industrial security breaches are carried out by insiders.



Sources of Incidents

- Infiltration can occur from many other sources besides Internet connections:
 - Desktop modems
 - Wireless networks
 - Laptop computers
 - Trusted vendor connections



Dependence on IT Department Security

- Process control departments tend to defer responsibilities for security to the IT department.
- Most IT departments' primary responsibility is to prevent external threats through firewall and account management.
- IT departments are generally unfamiliar with process reliability issues, equipment or industrial protocols.



Vulnerability of PLC/DCS/SCADA Systems

- Hackers don't need to understand a system to wreck it.
- Most control systems rely heavily on Microsoft Windows (which is well understood by hackers).
- Most PLC/DCS/SCADA systems have poor security designs and weak protection.



Plugging the Holes

- Audit the Process Systems
- Policy Development
- Architecture Development
- Intrusion Detection Systems
- Exception Tracking
- Incident Response Plans



Step #1: Audit the Process Systems

- It is critical to understand the state of cyber security of the process control systems.
- Not the same focus as IT security audit.
- Testing is not without risk - It is important that technical audits be performed following a plan and by individuals technically knowledgeable on the process and control systems.



Step #2: Policy Development

- Develop security policy for control systems.
 - Statement of the goals, responsibilities and accepted behaviors required to maintain a secure process environment.
 - Should be technology and architecture independent
- The security policy outlines what you want to achieve, not how to do it.



Step #3: Architecture Development

- Typically involves creating a multi-level network with firewalls between the layers.
- Simple architecture might be to divide the plant into two levels.
 - All inter-network and interlayer traffic flows through the firewall.
 - Provides a single point of control to manage all network traffic.



Step #4:

Intrusion Detection Systems

- The firewall is the lock on the door - not the burglar alarm.
- Networks require intrusion detection systems (IDS) to monitor traffic and identify unintended or malicious activity.
- Process control traffic patterns tend to be very consistent so simple traffic matrices can be enough to start.



Step #5: Exception Tracking

- A layered security model is very strong if it is implemented as designed without exception. Unfortunately, we all know there will be exceptions.
- For example, control vendor may connect into a PLC via a modem to for tech support.
- Requires a system of recording of exceptions and ensuring that they are being secured by other means.



Step #6: Incident Response Plan

- Develop an incident response plan for security incidents.
 - Define process to deal with incidents in advance.
 - Establish a Security Response Team
- The Security Response Team is a central resource and provides testing, guidance and solutions in the event a serious incident is reported.



Worlds in Collision...

- Industry is currently experiencing massive changes as new network technologies blend into process control.
- The commercial IT industry sees security as both a opportunity and a serious hurdle to growth.



Worlds in Collision...

- The industrial controls world needs to recognize that cyber security is important or it will risk paying a steep price:
 - Lost production
 - Inappropriate legislation
 - Environmental damage
 - Loss of life
- Industrial cyber-security is a critical safety issue.



Acknowledgements

■ Special thanks to:

- Spirent Communications for donating a SmartBits 6000B traffic generator to test PLC stability.
- Universal Dynamics Ltd. for use of their industrial cyber security audit case histories.





Video – Status of Industrial Cyber Security Standards and Research

**Eric Byres,
Manager - BCIT Internet Engineering Lab**