SCADA Security and Terrorism: We're not crying wolf.

RG & DM

INTERNET | SECURITY | SYSTEMS®

Agenda

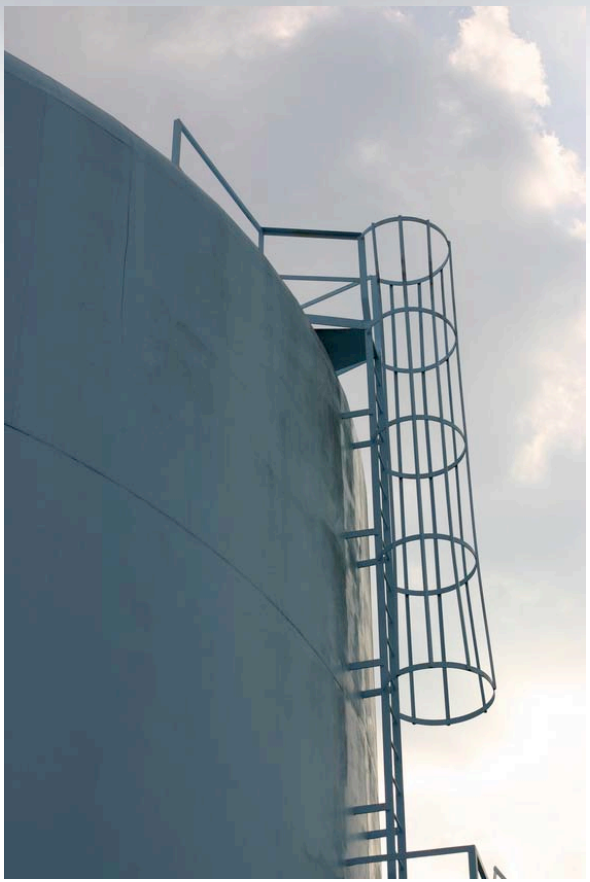
- **Introduction to the problem**
  - Rumors and claims that have achieved press
- **Our own experiences over the last 5 years**
  - New data to add to the debate
  - Hard data we stand behind
  - We can confirm some of those claims in the press
  - NAMES HAVE BEEN CHANGED TO PROTECT THE INNOCENT
- **Conclusion**
  - There is neither cause to **panic** nor cause to **ignore** the issue
  - Our own experience penetrating systems leads us to believe that it should be **taken seriously**.

What is SCADA?

- **Press buzzword to discuss cyberterrorism**
  - “control” systems is better term
  - “Supervisory Control and Data Acquisition”
- **Monitor and control industrial systems**
  - Oil and Gas
  - Air traffic and railways
  - Power generation and transmission
  - Water management
  - Manufacturing
- **Defined by threat**
  - Massive power blackout
  - Oil refinery explosion
  - Waste mixed in with drinking water

What is SCADA and control systems?

- The power your home
- The water in your home
- Where the water goes from your home
- The traffic lights on the way to the office
- The commuter train controls
- The air conditioning system in your office building
- The phone system to your home



What are the stories so far

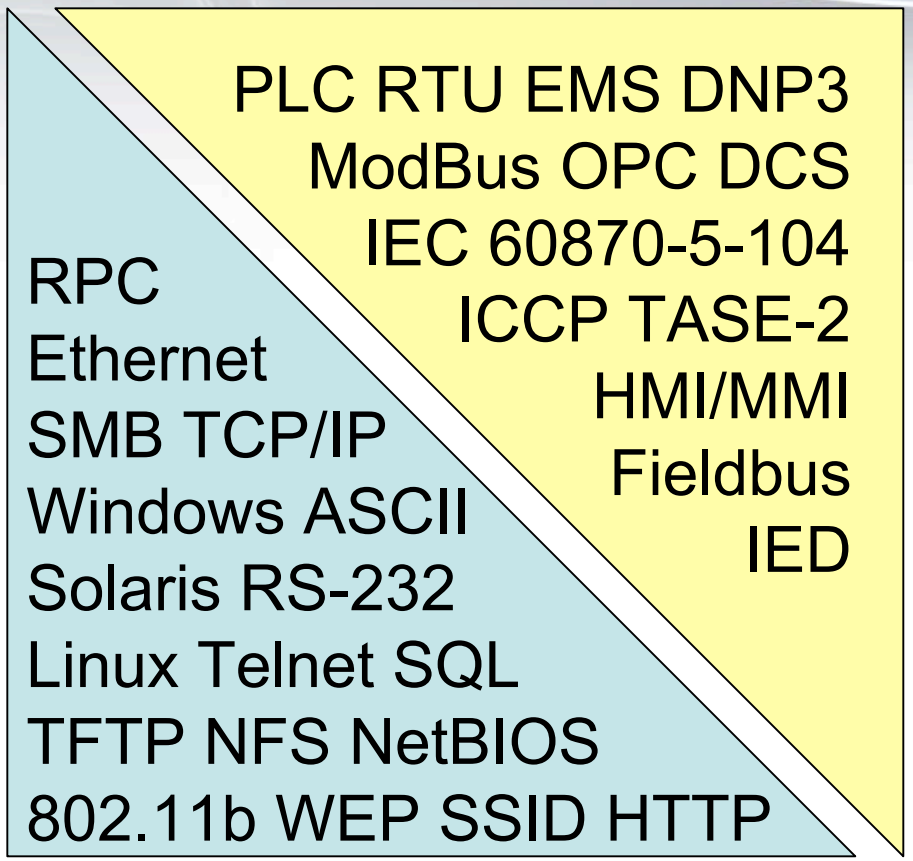
- **Warnings of doom by famous people**
  - Richard Clark, former cybersecurity czar and terrorism expert
    - Claims that mock intrusion scenarios have always succeeded.
    - Accuses industry of spending more on coffee than security.
  - Howard Schmidt, former cybersecurity czar and business expert
- **Well-known incidents**
  - Computers and manuals seized in Al Qaeda training camps full of SCADA information related to dams and related structures.
  - Ohio Davis-Besse Nuclear power plant safety monitoring system was offline for 5-hours due to Slammer Worm in January 2003.
  - In 2000, former employee Vitek Boden release a million liters of water into the coastal waters of Queensland, Australia.
  - In 2003, the east coast of America experienced a blackout, while not the cause, many of the related systems were infected by the Blaster worm
  - In 1992, former Chevron employee disabled it's emergency alert system in 22 states, which wasn't discovered until an emergency happened that needed alerting.
  - In 1997, a teenager breaks into NYNEX and cuts off Worcester Airport in Massachusetts for 6 hours, affecting both air and ground communications.
  - In the action to liberate Kosovo, NATO used information warfare techniques against the Serbs, Russian hackers attacked NATO computers, Chinese hackers (in response to accidental U.S. bombing of Chinese embassy) attacked United States computers.
  - In 2000, the Russian government announced that hackers succeeded in gaining control of the world's largest natural gas pipeline network (owned by Gazprom).
  - In 2005, Hurricane Katrina affected a few refineries in the southern coast of the United States, affecting gasoline prices world-wide.

What are the counter-stories so far?

- **Nobody has every been killed by a cyberterrorist**
  - "Unless people are injured, there is also less drama and emotional appeal." – Dorothy Denning
- **Despite the fact that both hackers and terrorists scare the public, what cyberterrorists could actually do (ground airplanes, power blacks, minor explosion in oil refinery) would not scare them nearly as much as 9/11.**
- **Many stories are "juiced up" to scare people**
  - Blaster did not cause the north-east power outage
  - Many stories of "teenage geniuses" gaining control of things are often exaggerated.
  - Yes, Al Qaeda had SCADA information, but nothing indicated an actual plan.
  - Companies do spend more on security than coffee (in my personal experience)
- **Many predictions have so far been wrong**
  - Tech research firm IDC named 2003 the year of cyberterrorism, predicting that a major cyberterrorism event would bring the Internet to its knees for a day or two.
- **They are trained to cope with emergencies**
  - They practice for all sorts of problems, from floods to earthquakes to hurricanes

SCADA is daunting, but our existing knowledge is adequate

Just this is sufficient



This helps, and it's all on the Internet

INTERNET | SECURITY | SYSTEMS®

How does SCADA work?

- **Multi-tier systems**
- **Physical measurement/control endpoints**
  - "RTU," "PLC"
  - Measure voltage, adjust valve, flip switch
- **Intermediate processing**
  - Normally based on commercial 3rd party OSes
    - VMS, Unix, Windows, Linux
- **Human interfaces**
  - Windows GUIs, for example
- **Communication infrastructure**
  - A variety of transport mediums
    - Analog, serial, Internet, radio, wi-fi

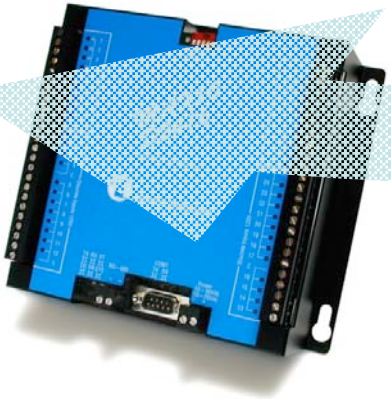
Protocols

- **The heart of a SCADA system - communication protocols**
- **Raw data protocols**
  - Examples: “modbus,” “DNP3”
  - Designed for serial/radio links, but can also be tunneled over Internet
  - Reads data (such as measuring voltage, pressure, fluid flow)
  - Sends alerts (when something breaks)
  - Send commands in other direction (flip a switch)
- **High-level data protocols**
  - Examples: “ICCP,” “OPC”
  - Designed to send bulk data and commands between various applications/databases
  - Designed to provide info for humans
  - ***They often bridge between the office-network and the control-network***

Network Components

Human interface

OPC

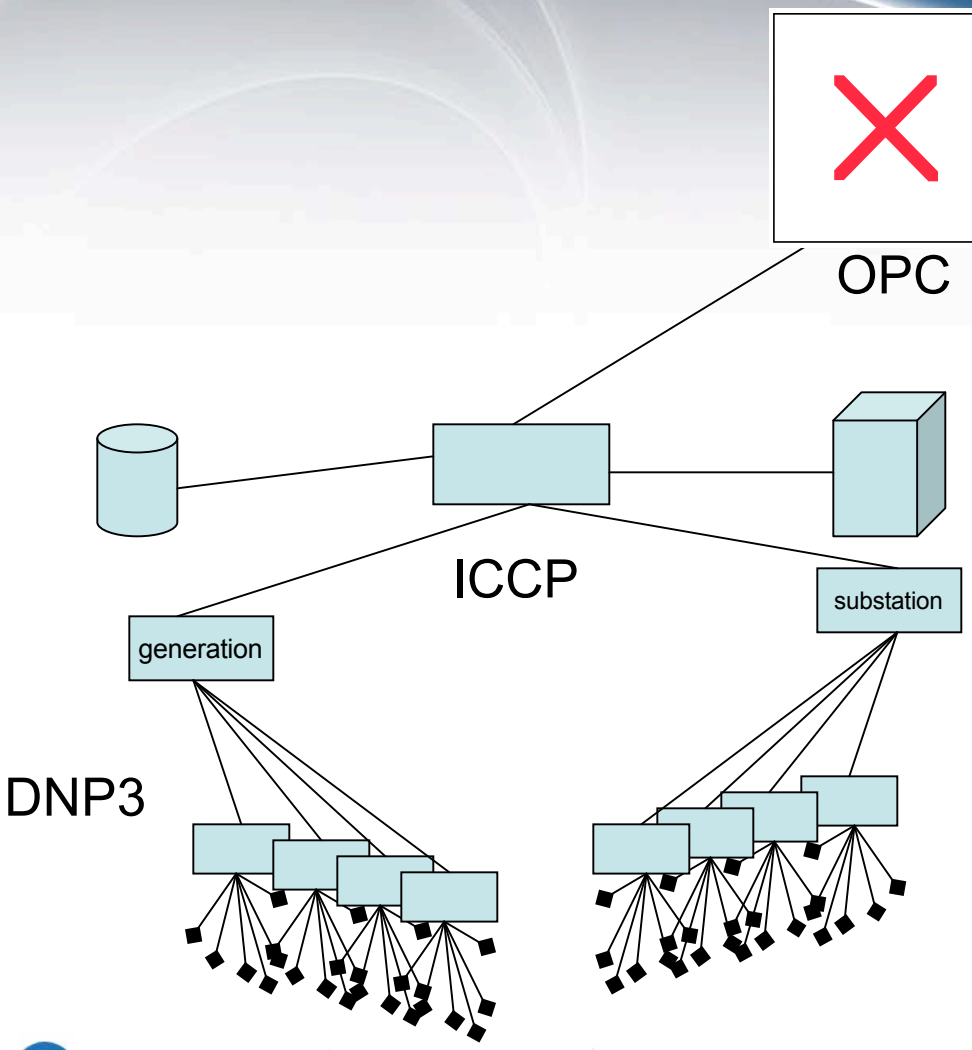


DNP3

ICCP

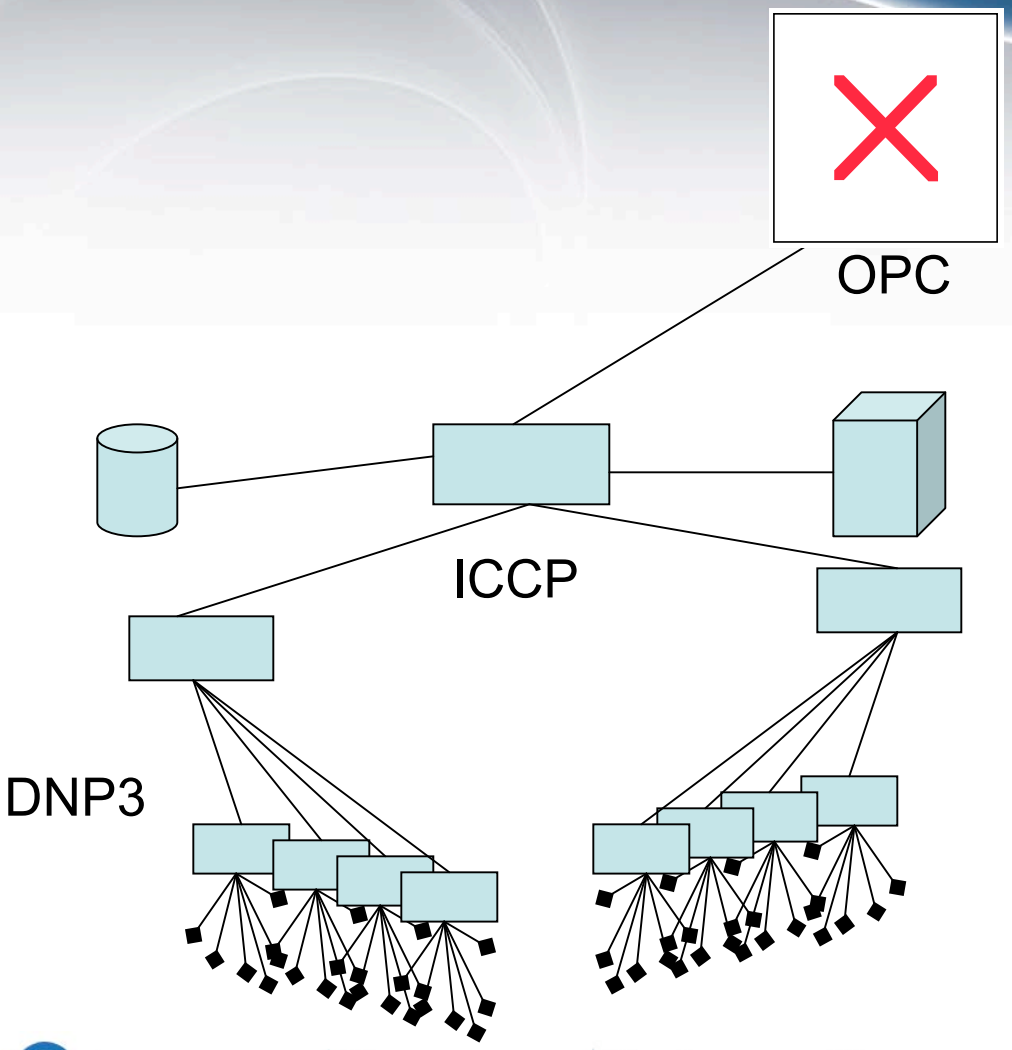
INTERNET | SECURITY | SYSTEMS®

Protocols



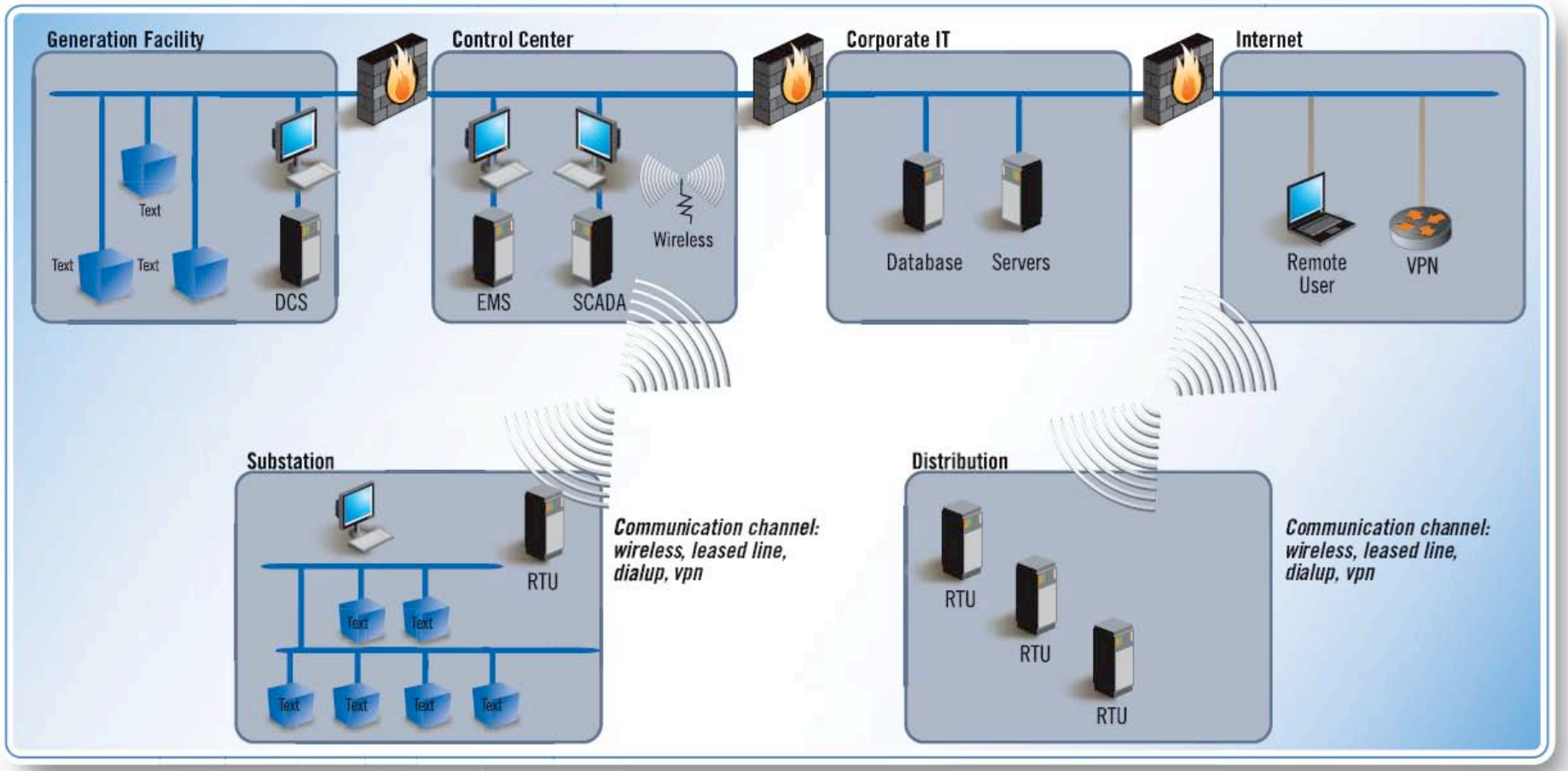
- **Data flows up to humans, commands flow down**
- **OPC**
  - Optimized for making it easy to write human applications
- **ICCP**
  - Optimized for passing bulk data around to systems like historical databases and power trading/analysis systems
- **DNP3**
  - Optimized for collecting data from simple devices

Security

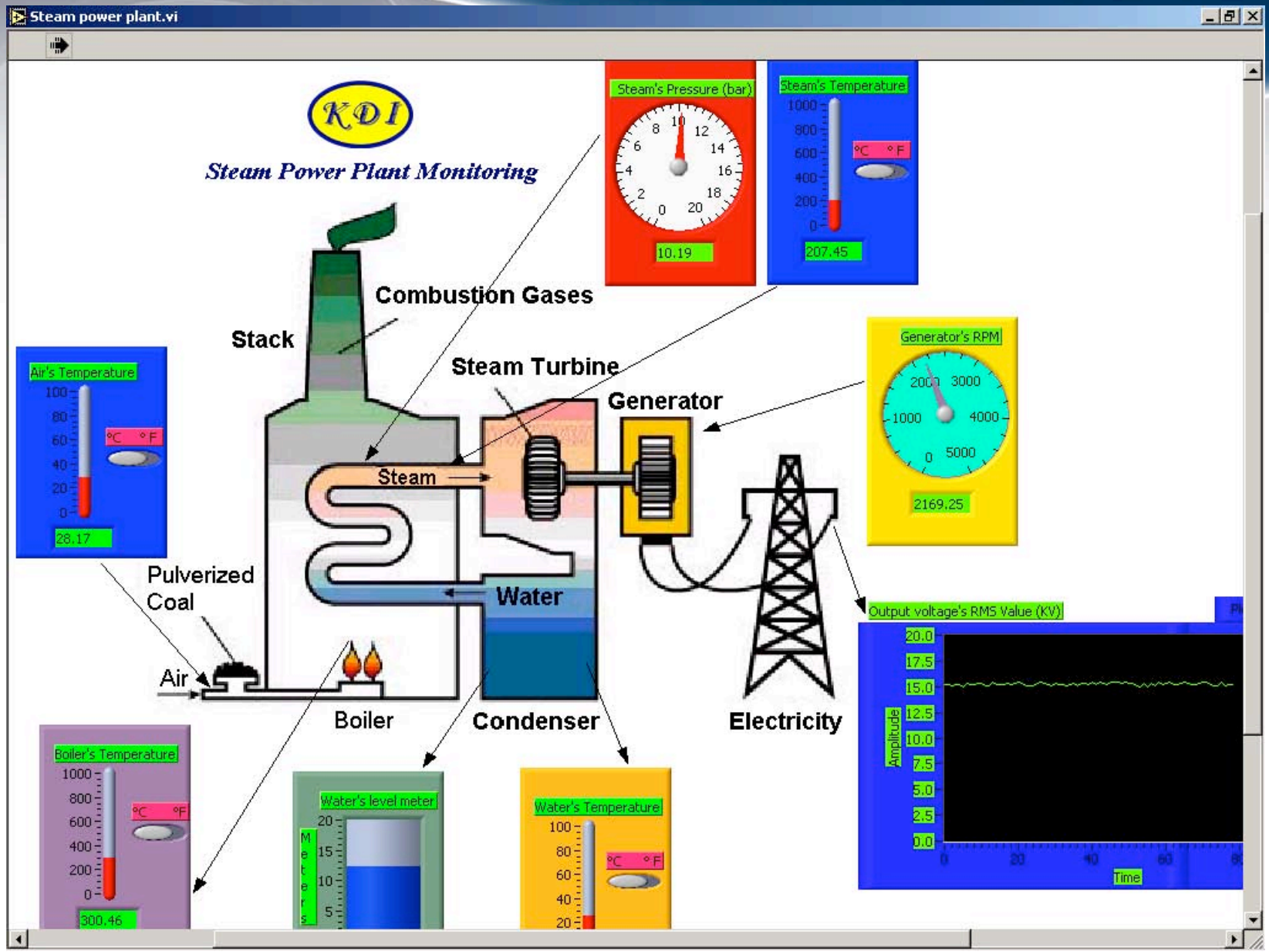


- **Where is the human located?**
  - Does she have access to the Internet?
- **Bulk data, who gets access to it?**
  - Partners?
  - Office computers?
- **Where is the authentication in this network?**
  - Which of my 300 humans can monitor/control more than 10,000 devices in the network
- **Where do firewalls go?**
  - …and impact the delay in the network causing response to happen too late?

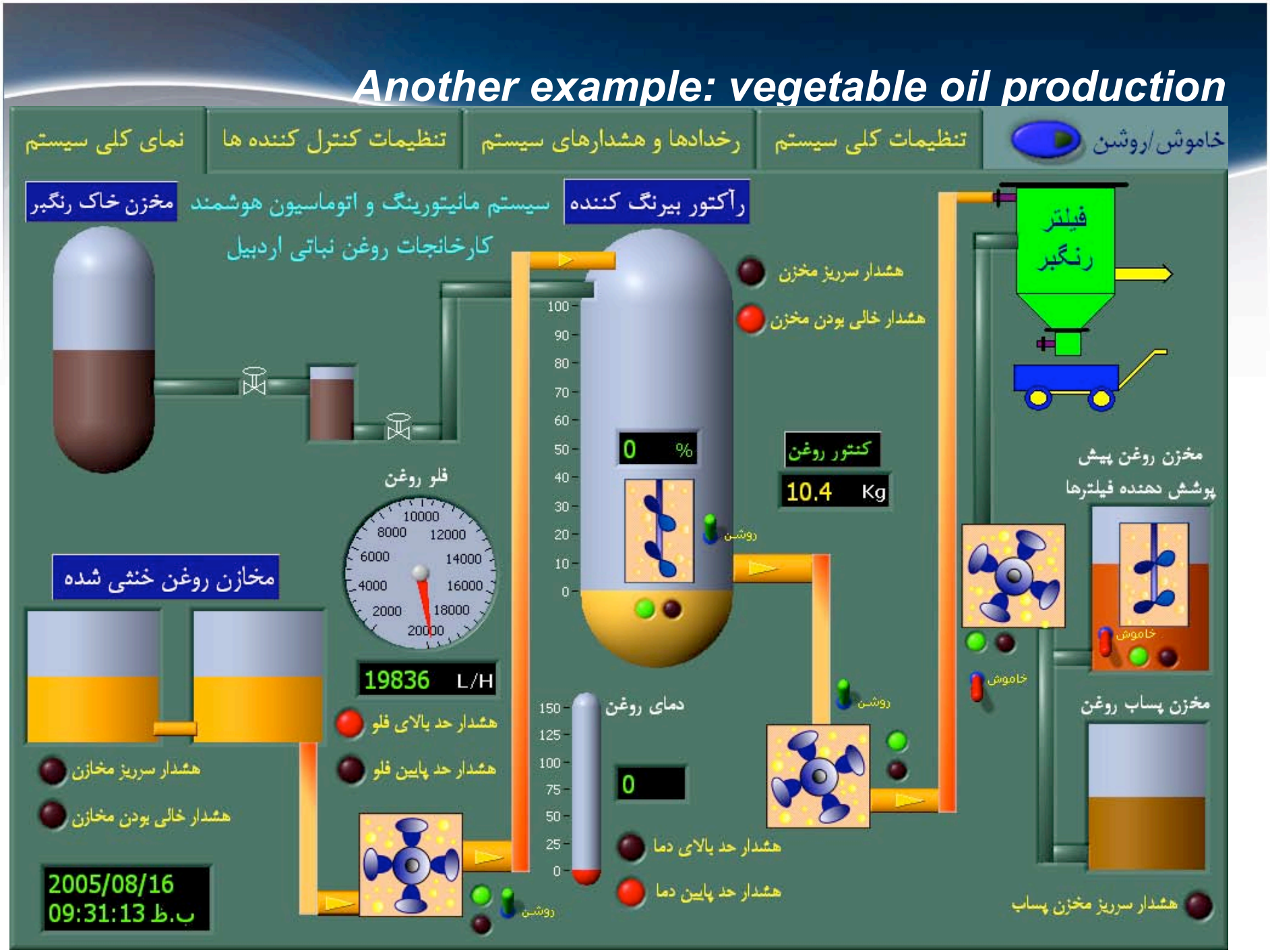
Another view of that network



Typical example of user-interface



Another example: vegetable oil production



OPC – Runs without authentication

- **In their own words:**
  - "Blaster" worm exposed the problem with DCOM
  - So Microsoft SP2 turned off "anonymous" by default for DCOM
  - This breaks SCADA systems because they don't have logins
    - No security
    - X-Force research: looks like OPC problem has lots of buffer-overflows in it, but since everyone uses it with no authentication anyway, it's pointless researching them.
    - Go to http://www.opcfoundation.org/, download trial software, test the authentication, binary review their code

Using OPC via DCOM with Microsoft Windows XP Service Pack 2

OPC FOUNDATION

6. Edit the Limits for Access and Launch
   a. Access Permissions – **`Edit Limits...`**
      You need to check the Remote Access box for the user labeled `ANONYMOUS LOGIN` in this dialog.

Problems with SCADA

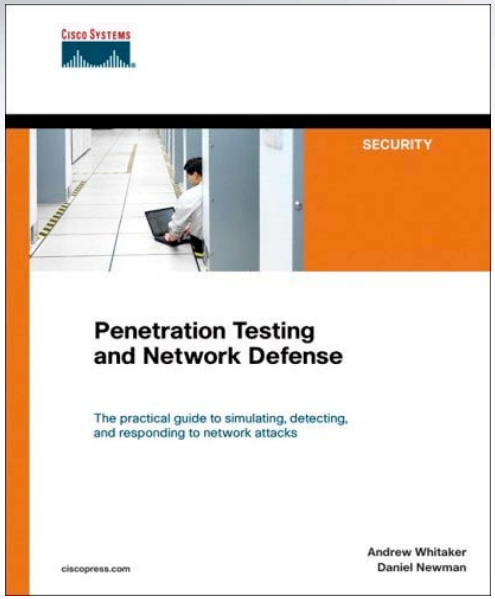
- **Lesson #1**
  - SCADA = no authentication
  - What is the “identity” of an automated system?
    - How would policies such as “change your password monthly” be applied to automated systems that are supposed to run unattended for years?
  - How do you manage rights for each person?
    - Which, of the thousands of possibilities, can they can monitor/control?
- **Lesson #2**
  - SCADA = no patching
  - Systems have never needed security patches in the past
    - Old: install a system, replace it in 5 years
    - New: install a system, patch it every month
  - The gulf between the old and the new is too wide

Problems with SCADA

- **Lesson #3**
  - SCADA = industry in denial about how much they are connected to the Internet
  - Belief: not interconnected at all
  - Reality: numerous uncontrolled interconnects
  - Reality: even networks that are separate frequently get connected via links or simple things like roaming notebooks

Cyberterrorism Threat Analysis

- **Our experience**
  - "You can go to the store and buy a book on pen-testing that will give you all the knowledge you need to cause a widespread power blackout."
    - We can create 0-day exploits, but we've never used them in SCADA pen-tests
    - Instead, we've used "old-school" techniques such as port-scanning and password-guessing



ISS Cyberterrorism Threat Analysis

- **Who?**
  - Al Qaeda?
    - We have no visibility into this
    - We guess it's not a near-term threat
    - We know hackers are notoriously hard to organize/direct by such an organization
    - We guess they would rather blow something up
  - Individuals?
    - We have a lot of visibility into this
      - Example: when we posted our first whitepaper on SCADA, the majority of downloads were from the Arab world
    - We know hacking skills are prevalent everywhere
      - Example: author of Zotob was Muslim (though a normal person, not an extremist)
    - It's not just religious fanatics, it's any individual who wants to quarrel with us, including our own citizens
      - Example: Timothy McVeigh followed a recipe for building fertilizer bombs
      - Example: Animal-rights activists, eco-extremists.

Real world examples

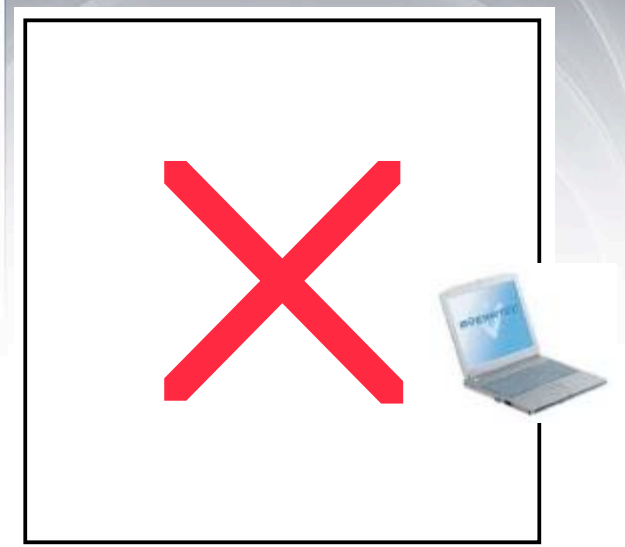
ISS Professional Services: pen-testing

- **ISS pen-testing as part of our professional services offering**
  - Standard pen-test services like many others in the industry
  - We've been contracted by many SCADA/control-systems organizations
- **"The more simple the methods, the more compelling the results"**
  - NO: 0day exploits from the ISS X-Force team
  - YES: guess simple passwords
  - YES: SQL injection
  - YES: port-scanning
  - YES: SNMP MIB walking
  - YES: anonymous FTP, SMB null sessions, Telnet no password
  - YES: old/common exploits on unpatched systems
  - YES: sniffing
  - YES: backdoors/trojans

Example #1: WiFi at power plant

- **Sitting in conference room negotiating pen-test**
  - Denial: “Why should we buy your services, we are secure so you won’t be able to break in”
- **“We have no WiFi”**
  - Turn notebook around and show that there is an open (no WEP) access point reachable from the conference room
- **“Oh, but you can’t get an IP address or anything from it”**
  - We connect, it gives us a DHCP address
- **“It’s just in the lab”**
  - We run scans and show that it’s connected to the rest of the office network
- **“The office network (where people work) is not connected to the control network (where the power plant is).”**
  - We get into Solaris system using 10 year old exploit
- **“Please stop”**
  - We had broken into a system that was on both networks and, indeed, was in direct control of something extremely sensitive and we were in danger of breaking it
- **Confirmation**
  - The skills of “average” hackers are adequate to gain access to the systems.

WiFi at power plant



lab

office

SCADA

Example #2: oil company

- **Claim: "We are secure because the oil production network is completely separate from the rest of the corporate network"**
  - Pulls out network diagram proving his case
- **Flaw #1: diagrams don't match reality**
  - It's the desired configuration, not the actual configuration.
  - The networks are interconnected at numerous points.
  - Unfortunately, most people in the company believe in the fiction.
- **Flaw #2: diagram OBVIOUSLY doesn't match reality**
  - Supercomputer that's processing oil pumping data in order to optimize extraction sits on office network
  - Pulls data from production network, sends configuration commands back to production network: therefore, the two networks MUST be interconnected at some point
  - In our experience, such data crunching systems are a key hopping point between networks.
- **Flaw #3: notebooks**
  - Production stopped at a couple of sites due to a network worm (Blaster) because somebody plugged in a notebook computer when diagnosing a problem at an oil platform. The worm quickly spread. The lost production caused million of dollars lost in revenue.
- **Flaw #4: production network has zero protection**
  - Example: once systems go into production they are never patched
  - Example: even patchable systems (consoles) have no authentication
- **Conclusion: An Internet storm could disrupt oil production like Katrina**

Example #3: Component of U.S. power grid

- **Same claim:**
  - Customer: “Backend networks are not interconnected with the Internet”
- **Same flaw: “But don’t you have power-trading websites on the Internet? Don’t those have some interconnection with the backend networks?”**
  - Customer: “yes”
- **Pen-test proved it**
  - Got in via SQL injection on website/portal
  - Established VPN-like tunnel through SQL server
  - Followed the data from system to system to the backend network, which of course was weak on authentication and patches
- **Confirmation**
  - Indeed, there was no air-gap between the backend network and the Internet
  - A hacker on the Internet could press a button and shut off the system.

Example #4: Another nation's power grid

- **Unlike United States, most nations have a single power grid and a single target**
- **Pen-test engagement used multiple vectors**
  - Via Internet
  - Via dialup
  - Via wireless
- **Again: "Office networks not interconnected to production networks"**
  - Again: false, for example the time on the production network that gets the 50/60 Hz sine wave is synchronized primarily with NTP across the Internet
- **Backend network again insecure**
  - Network equipment provided by one of the big companies
    - Example: Solaris machine with software installed and accounts already created
    - Manufacturer recommends to change passwords, but customer never does
    - Everybody in the organization logs in with same username/password in order to do things like monitor and control the power
- **Confirmation**
  - Access from the Internet to the backend network existed.
  - Sample: accessing a specially crafted (long) URL with a web-enabled phone was all that was needed to shutdown the entire grid.

Example #5: Finding targets

- **Where to start?**
  - Google
- **Vendors list their customers on their web-site**
  - Marketing: trying to impress you with well-known customers
  - Sales: detailed case-studies of how these customers have implemented their systems, which products they have
  - Availability: software is usually available on their website, hardware is often cheaply available on eBay.
- **Anecdote**
  - Customer: “We think the threat is low because outsiders know nothing about our systems”
  - Us: “Here is what we know about your systems”
  - Customer: <shocked> “How did you get that information?”
  - Us: <showed them the web-site from the vendor>
- **Confirmation**
  - Information needed to educate enemies about the systems is widely available.
- **Speculation**
  - Hackers would not need to actually target the infrastructure itself, they could instead target the suppliers.
    - Examples: Rockwell, ABB, Siemens, GE, etc.
  - *At the Abyss: An Insider's History of the Cold War*, by Thomas C. Reed
    - Claims that United States provided trojan firmware to the Soviet Union, causing a pipeline to explode in one of the biggest non-nuclear explosions the world has ever seen.

Example #6: Finding target

- **Customer claims**
  - "SCADA too obscure for hackers"
  - "SCADA not connected to office or Internet"
- **Contents of pen-test report**
  - Listed accounts on FTP site
  - Penetrated dual-homed machine
    - Had firewall, but this machine both inside and outside the network
    - Account was same username and password
  - Found public shares on Windows file servers
  - Found intranet websites
- **Documents found**
  - Spreadsheets listing all accounts on the SCADA network (and DNS or IP addresses)
  - Maps of the network, both physical and cyber
  - Firewall policies
  - Training materials for operators of the SCADA network
  - Vendor manuals
  - Source code to major applications
  - Backup/sample configuration files for the control systems
  - Intranet search engine that made locating much of this easy
  - Word, PowerPoint, Excel, text
  - …and a listing of what they thought were things hackers could do
- **Confirmation**
  - Complete outsiders can obtain the information necessary to become experts on the system

Example #7: Sniffing (multiple targets)

- **Security assessment technique**
  - Once you find the usernames and passwords, put them into IDS as signatures
  - Watch where they trigger
  - Sniff specific applications to assess, manually search those packets for clear-text information.
- **What we have found**
  - When accounts exist, username and password information almost always sent in the clear.
  - Applies to human-to-machine applications.
  - Applies to machine-to-machine communications.
- **Confirmation**
  - Critical infrastructure communication is largely in the clear and is not encrypted.

Example #8: Physical access

- **Driving with customer through rural area**
  - Us: “What is that?”
  - Customer: “That is one of our power substations”
  - Us: “Can we take a look?”
- **What we found**
  - Door was unlocked.
  - Windows PC running in shed connected to all the equipment
  - …and connected to the Internet SCADA backbone through wireless connection and TCP/IP protocols.
- **Similar stories**
  - Petroleum customer relates how offshore platforms are unmanned and have no security, and how in one case, it was a mobile maintenance person with an infected laptop at one of those platforms that had caused an infection in the network.
- **Confirmation**
  - While physical security is strong in some areas, wide-area SCADA systems are nearly impossible to physically secure.

Example #9: Dams

- **Dams control flooding**
  - Disruption of control systems during floods can cause downstream flooding of inhabited areas.
- **Dams control water**
  - Example: release of excess water from the damn can disrupt the temperature of the water, thereby making it unsuitable for industrial uses, shutting down nearby plants.
  - Example: changes in water levels could seriously disrupt navigation and transport in the area.
- **Dams provide power**
  - Sustained power all the time
  - Peak power on-demand
  - Power storage when other systems push water back up hill
    - A release of the water can represent a huge economic loss due to the lost power
- **Confirmation**
  - We demonstrated to the customer that we had the knowledge to use the systems we penetrated to effect these outcomes.

Example #10: audit trails (multiple incidents)

- **What we found**
  - No per-user authentication: users logged in with names like “console” or “administrator” rather than “alice” or “bob”
  - This meant that activities of malicious insiders was effectively untraceable.
  - Available audit trails were usually turned off.
  - Intrusion detection systems were often not updated or regularly monitored.
- **What we reported to the customer**
  - In many cases, if an incident had occurred, there would be little or no ability to tell if it was “malicious” (caused by a human) or “accidental” (caused by accident).
  - Indeed, during our pen-tests, much of our activity was not logged.
- **Confirmation**
  - Victims may not even be aware that they have been attacked.

Example #11: modems (multiple incidents)

- **Modems**
  - Use #1: imbedded in many equipment to allow the vendor to support the product.
  - Use #2: an easy way to retrieve non-realtime data from the device.
- **Problems**
  - Most had banners. We simply googled the banners, found the manuals, and used that information to compromise the devices.
  - Devices often had default usernames/passwords that were never changed since shipped by the vendor.
  - Devices often had backdoor usernames/passwords that couldn't be changed.
  - Devices often had other tricks that could be used to bypass security
    - Example: a keystroke that would dump the 64k memory on the device, which often included the previous login session, including username/password.
- **Confirmation**
  - Forget the Internet, cyberterrorists can still attack us by war-dialing.

Example #12: core reviews

- **What we have done**
  - Cursory binary audits of implementations
  - Cursory source audits of implementations
- **What we have found**
  - Insecure coding practices
    - Trusting input from the network (e.g. ASN.1 buffer-overflows)
    - Widespread use of the known villains: strcpy(), sprintf(), etc.
  - Little or no ability for authentication or encryption
  - Clear-text
  - Difficulty in firewalling, patchings, hardening, and other security techniques.
- **Confirmation**
  - Assuming they fix everything else, they still have “vulnerabilities” to contend with.

Conclusion

- **We can confirm a lot**
  - Outsiders can gain control of the systems via cyberspace
  - This control can lead to major disruptions in the infrastruture
  - It doesn't take genius hacker skills
- **We can disprove a lot**
  - An "air-gap" between control-networks and the Internet is not the norm (we saw it only once)
  - The systems are not to complex for outsiders to understand (and we haven't even begun talking about insiders)
- **It's enough to take the problem seriously**
  - There is no need to panic
  - Yet there we shouldn't ignore the problem either