SCADA Security

ASHIT V DALAL, CISA,CISM, CGEIT, CRISC, CPSA

ISACA MUMBAI CHAPTER

NOVEMBER 19, 2016

DISCLAIMER #1

- The slides in the presentation are my personal views and are based on actual experience and the publicly available information and not the views of or binding on my current or past organizations in any way….
- The presentation is purely for education, awareness and training and should not be used for any commercial or business benefits.

Topics

- Critical Infrastructure & SCADA
- Introduction to SCADA / ICS
- SCADA / ICS Architecture
- Key Security Considerations and Challenges
- SCADA / ICS Standards

What is Critical Infrastructure ?

- Energy : Oil & Gas and Power & Utilities
- Healthcare & Pharmaceuticals
- Aerospace and Defense
- Banking and Financial Services
- Refinery, Chemicals and Petrochemicals
- Food and Agriculture
- Transportation

Interdependency in Critical Infrastructure

- The (U.S.) Critical Infrastructure is often referred to as a “System of systems” because of the interdependencies that exist between its various industrial sectors as well as interconnections between business partners.
- Critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies.
- An incident in one infrastructure can directly and indirectly affect other infrastructures through cascading and escalating failures.

(Source: NIST 800-82)

So, have there been any hacks into SCADA systems?

- Numerous - Demonstrations of Vulnerabilities by Security System Suppliers
- Unknown - “Friendly Hacks” into Energy and Transportation Systems by Federal Government Agencies to Assess Vulnerabilities
- Fewer than ten incidents in systems, which are related to or connected to SCADA systems or have been in systems in other industries, e.g. a railway SCADA system in Asia
- One, definite, and very well known hack into a wastewater SCADA system…*just enough to show that it can happen...*
- *Sniper attack on PG & E substation in California in April 2013*

So, have there been any hacks into SCADA systems?

'Sewage' hacker jailed
8th May 2002 - News.com.au

A COMPUTER hacker who avenged his rejection for a council job by deliberately allowing sewage to run into public parks and creeks on Queensland's Sunshine Coast was jailed for two years today.

In March last year, up to one million litres of raw sewage flowed into the grounds of the Hyatt Regency Resort at Coolum and nearby Pacific Paradise, where it ended up in a stormwater drain.

The Maroochydore District Court heard that 49-year-old Vitek Boden was a "disgruntled" former employee of the company that installed a computerised sewerage system for Maroochy Shire Council.

He applied for a job with the council but was rejected and later hacked into the council's sewage control computers, using radio transmissions to alter pump station operations.

The court was told on April 23 last year, police pulled Boden over in his car less than one hour after one of the sabotage attempts on the system.

They found a variety of electronic equipment, including a two-way radio and a computer with programs for hacking into the council's sewerage pumping stations.

A copy of the hard disk on Boden's laptop showed that it had been used at the same times as pump malfunctions.

Environmental Protection Agency (EPA) investigations manager Janelle Bryant today welcomed the court's decision, saying that damaging the environment was a criminal act and would be prosecuted accordingly.

"Vitek Boden's actions were premeditated and systematic, causing significant harm to an area enjoyed by young families and other members of the public," Ms Bryant said.

"Marine life died, the creek water turned black and the stench was unbearable for residents," she said.

Boden, of Springwood in Brisbane, was sentenced to two years jail after being found guilty on 46 counts of computer hacking and two counts of stealing.

He was also sentenced to 12 months jail to be served concurrently for wilfully causing serious environmental harm. *-AAP*

Attack on PG & E Substation in California:

Shortly after midnight on April 16, 2013, some people snuck up on PG&E's substation in Metcalf, California. They cut fiber-optic AT&T phone lines, shutting off service to nearby neighborhoods. They also fired more than 100 rounds of .30-caliber rifle ammunition into the radiators of 17 electricity transformers. Thousands of gallons of oil leaked, causing electronics to overheat and shut down.

PG&E engineers were able to reroute power, but it was a struggle to keep the power on during the attack.

The assault lasted only 19 minutes, but it caused US$15 million in damage. It also became a harsh wake-up call for energy providers, who have since become obsessed with the physical security of their remote power stations.

Thousands of gallons of Transformer oil went inside the Sewer resulting into a Ground water and Stormwater issues and Environmental Concerns. US EPA is expected to levy a hefty fine of more that USD 100 Million due to this.

PG&E alone has pledged to spend $100 million to improve security at its facilities. Also, it and AT&T (T, Tech30) have each announced separate $250,000 rewards to catch the attackers.

DHS believes that this was the work of an insider most likely a disgruntled employee or a contractor.

Other Known SCADA Security Incidents:

Davis-Besse :

In August 2003, the Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours. In addition, the plant's process computer failed, and it took about six hours for it to become available again. Slammer reportedly also affected communications on the control networks of at least five other utilities by propagating so quickly that control system traffic was blocked.

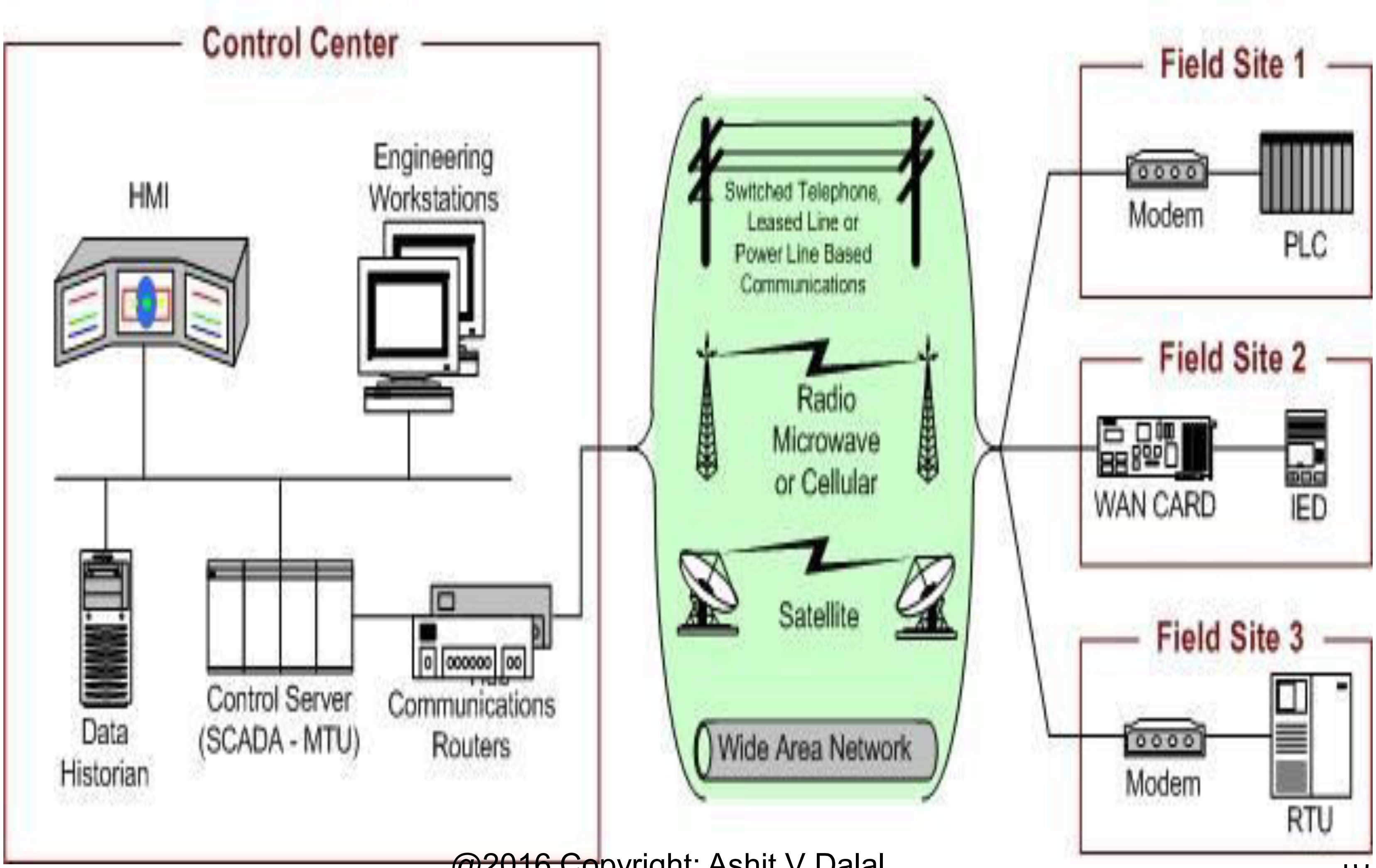
Northeast Power Blackout:

In August 2003, failure of the alarm processor in First Energy's SCADA system prevented control room operators from having adequate *situational awareness* of critical operational changes to the electrical grid. Additionally, effective reliability oversight was prevented when the state estimator at the Midwest Independent System Operator failed due to incomplete information on topology changes, preventing contingency analysis. Several key 345kV transmission lines in Northern Ohio trip due to contact with trees. This eventually initiates cascading overloads of additional 345 kV and 138 kV lines, leading to an uncontrolled cascading failure of the grid. 61,800 MW load is lost as 508 generating units at 265 power plants trip.

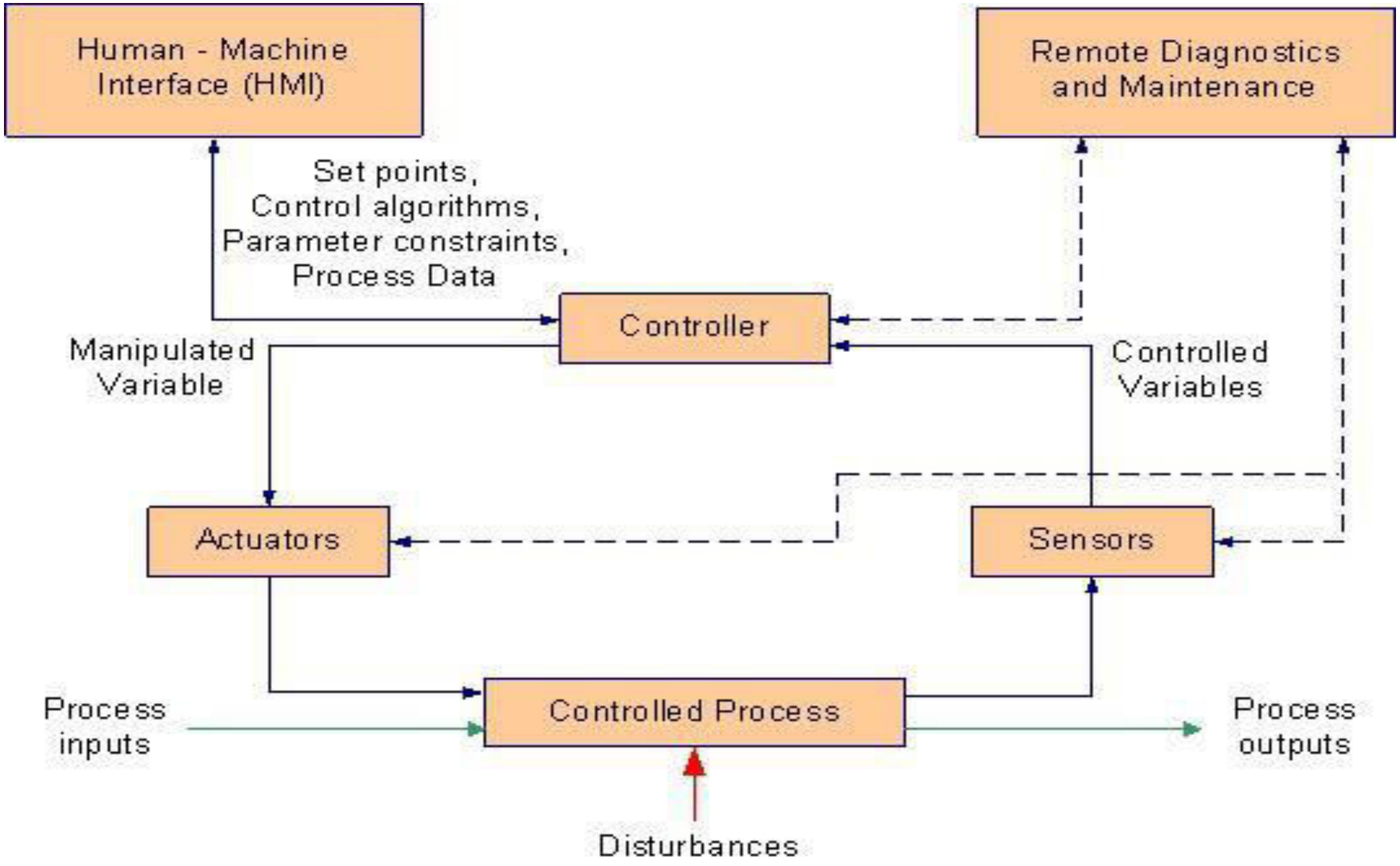
Zotob Worm:

In August 2005, a round of Internet worm infections knocked 13 of DaimlerChrysler's U.S. automobile manufacturing plants offline for almost an hour, stranding workers as infected Microsoft Windows systems were patched. Plants in Illinois, Indiana, Wisconsin, Ohio, Delaware, and Michigan were knocked offline. While the worm affected primarily Windows 2000 systems, it also affected some early versions of Windows XP. Symptoms include the repeated shutdown and rebooting of a computer. Zotob and its variations caused computer outages at heavy-equipment maker Caterpillar Inc., aircraft-maker Boeing, and several large U.S. news organizations.

Typical SCADA Architecture



Typical SCADA Operation



SCADA TERMINOLOGY

SCADA TERMINOLOGY :

Control Server: The control server hosts the DCS or PLC supervisory control software that is designed to communicate with lower -level control devices. The control server accesses subordinate control modules over an ICS network.

SCADA Server or Master Terminal Unit (MTU): The SCADA Server is the device that acts as the master in a SCADA system. Remote terminal units and PLC devices (as described below) located at remote field sites usually act as slaves.

Remote Terminal Unit (RTU): The RTU, also called a remote telemetry unit, is special purpose data acquisition and control unit designed to support SCADA remote stations. RTUs are field devices often equipped with wireless radio interfaces to support remote situations where wire-based communications are unavailable. Sometimes PLCs are implemented as field devices to serve as RTUs; in this case, the PLC is often referred to as an RTU.

Programmable Logic Controller (PLC) : The PLC is a small industrial computer originally designed to perform the logic functions executed by electrical hardware (relays, drum switches, and mechanical timer/counters) . PLCs have evolved into controllers with the capability of controlling complex processes, and they are used substantially in SCADA systems and DCSs. Other controllers used at the field level are process controllers and RTUs; they provide the same control as PLCs but are designed for specific control applications. In SCADA environments, PLCs are often used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.

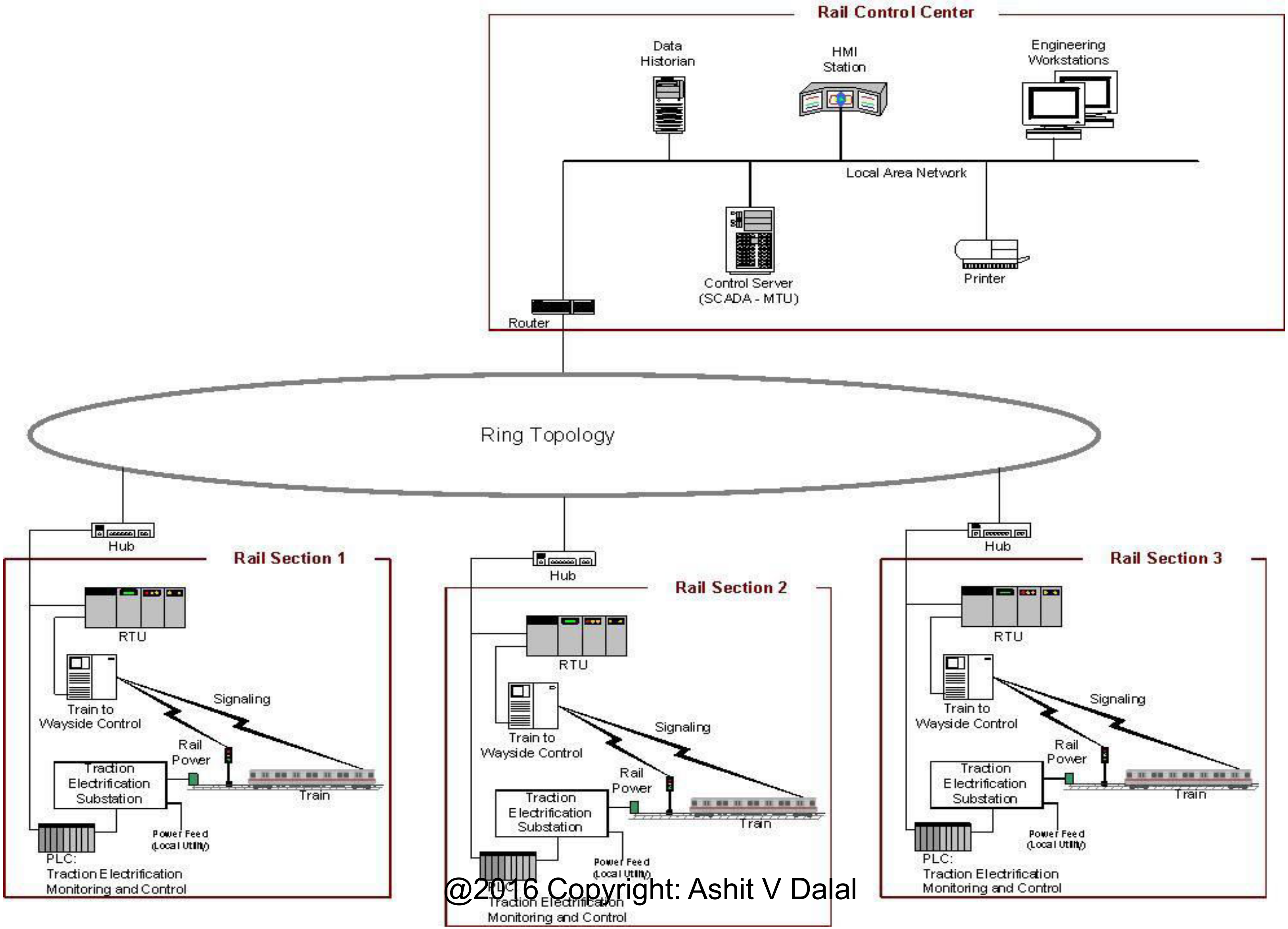
Intelligent Electronic Devices (IED).: An IED is a “smart” sensor/actuator containing the intelligence required to acquire data, communicate to other devices, and perform local processing and control. An IED could combine an analog input sensor, analog output, low-level control capabilities, a communication system, and program memory in one device. The use of IEDs in SCADA and DCS systems allows for automatic control at the local level.

Human-Machine Interface (HMI): The HMI is software and hardware that allows human operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency. The HMI also allows a control engineer or operator to configure set points or control algorithms and parameters in the controller. The HMI also displays process status information, historical information, reports, and other information to operators, administrators, managers, business partners, and other authorized users. The location, platform, and interface may vary a great deal. For example, an HMI could be a dedicated platform in the control center, a laptop on a wireless LAN, or a browser on any system connected to the Internet.

Data Historian: The data historian is a centralized database for logging all process information within an ICS. Information stored in this database can be accessed to support various analyses, from statistical process control to enterprise level planning**.**

Input /Output (IO) Server: The IO server is a control component responsible for collecting, buffering and providing access to process information from control sub-components such as PLCs, RTUs and IEDs. An IO server can reside on the control server or on a separate computer platform. IO servers are also used for interfacing third-party control components, such as an HMI and a control server.

SCADA – Railway Monitoring & Control System


Rail Control Center
Data Historian
HMI Station
Engineering Workstations
Local Area Network
Control Server (SCADA - MTU)
Printer
Router
Ring Topology
Hub
Rail Section 1
RTU
Train to Wayside Control
Signaling
Rail Power
Traction Electrification Substation
Train
Power Feed (Local Utility)
PLC: Traction Electrification Monitoring and Control
Hub
Rail Section 2
RTU
Train to Wayside Control
Signaling
Rail Power
Traction Electrification Substation
Train
Power Feed (Local Utility)
PLC: Traction Electrification Monitoring and Control
Hub
Rail Section 3
RTU
Train to Wayside Control
Signaling
Rail Power
Traction Electrification Substation
Train
Power Feed (Local Utility)
PLC: Traction Electrification Monitoring and Control

Alarming Best Practices for Vulnerable Areas

- Define alarm points sparingly - otherwise operators can be overloaded
- Use alarm management e.g. sort by process unit or zone to avoid overload
- Eliminate nuisance alarms - *the alarm system should never lose credibility with operators!*
- Back up with local audit trail/alarm history in the RTU

Chlorine Storage System with Alarm, Sensors, cameras and water Deluge System

Alarming Best Practices for Vulnerable Areas

Operating Procedures must include:

- Scheduling of site visits
- Requirement that site workers inform operators when they arrive and leave.
- Logging of all site visits as events (record keeping is very important!)
- Reactions to alarms including acknowledging, disabling and resetting them.

Advanced Alarm Techniques

- Rate of change e.g. pressure drop - sometimes, limit alarms are too late or miss the actual problem
- Sanity check or process mismatch, e.g. influent pumps are on but settling basin is full
- Ratio alarm, e.g. chlorine feed rate vs. water flow

Key Recommendations for enhancing SCADA Security

- Identify, minimize, and secure all network connections to the SCADA / ICS.

- Segment SCADA from Corporate IT Network through a series of Firewalls / Air gaps to prevent direct connectivity between two systems

- Harden the ICS and supporting systems by disabling unnecessary services, ports, and protocols; enable available security features; and implement robust configuration management practices.

- Continually monitor and assess the security of the ICS, networks, and interconnections.

- Implement a risk-based defense-in-depth approach to securing ICS systems and networks.

- Manage the human—clearly identify requirements for ICS;
  - establish expectations for performance;
  - hold individuals accountable for their performance;
  - establish security policies;
  - and provide ICS security training for all operators and administrators.

Some well-known SCADA Security Standards

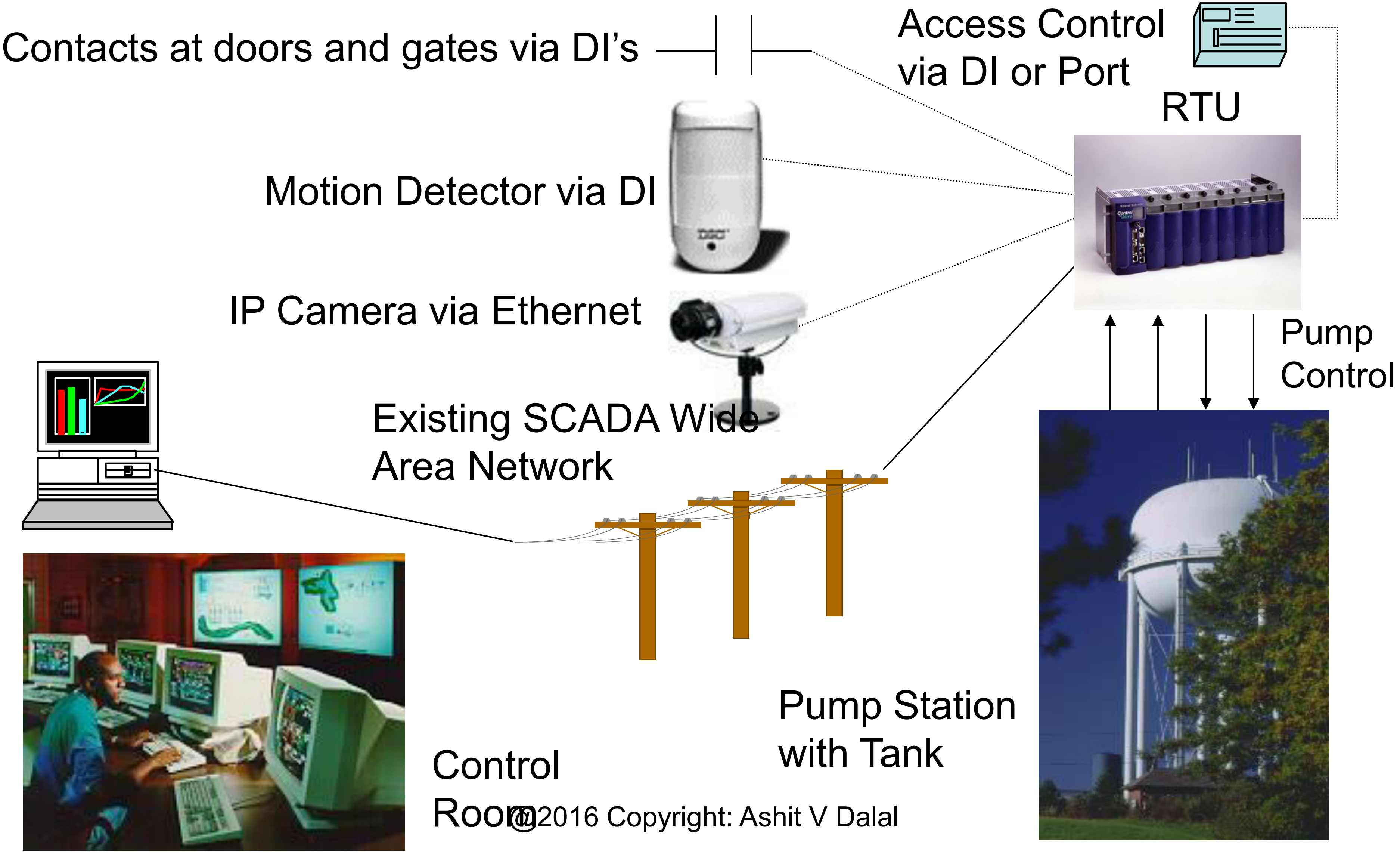
- NERC-CIP (Power & Utilities)
- CFATS (Chemical Facility Anti-Terrorism Standard) or 6 CFR Part 27
- NIST 800-82
- ISA 99
- AGA 12

Applications using Security integrated with SCADA

Video Security Application

- Implemented in a **Control**Wave RTU
- Camera images are stored securely in **Control**Wave flash memory.
- Provides pre and post-event image storage to capture full event.
- Supports one or multiple cameras for wide vulnerable area coverage.
- Pre-configured User Defined Function Block eliminates custom programming.
- Used in conjunction with process control logic.
- OpenBSI utility automatically recovers and displays video images.
- Compatible with TCP/IP and existing BSAP networks.

Typical Application



Contacts at doors and gates via DI's

Access Control via DI or Port

RTU

Motion Detector via DI

IP Camera via Ethernet

Pump Control

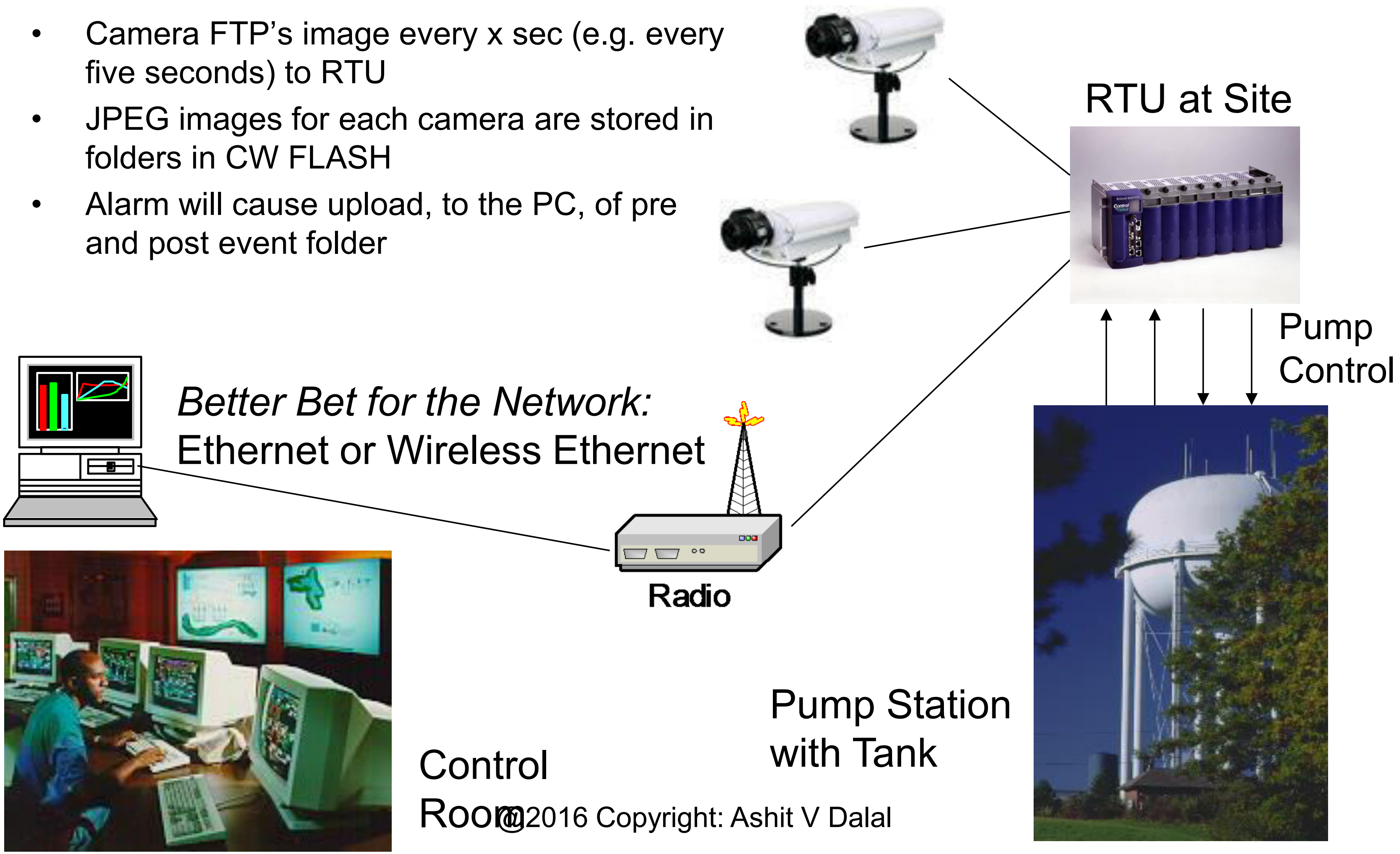
Existing SCADA Wide Area Network

Pump Station with Tank

Control Room

Video Sequence

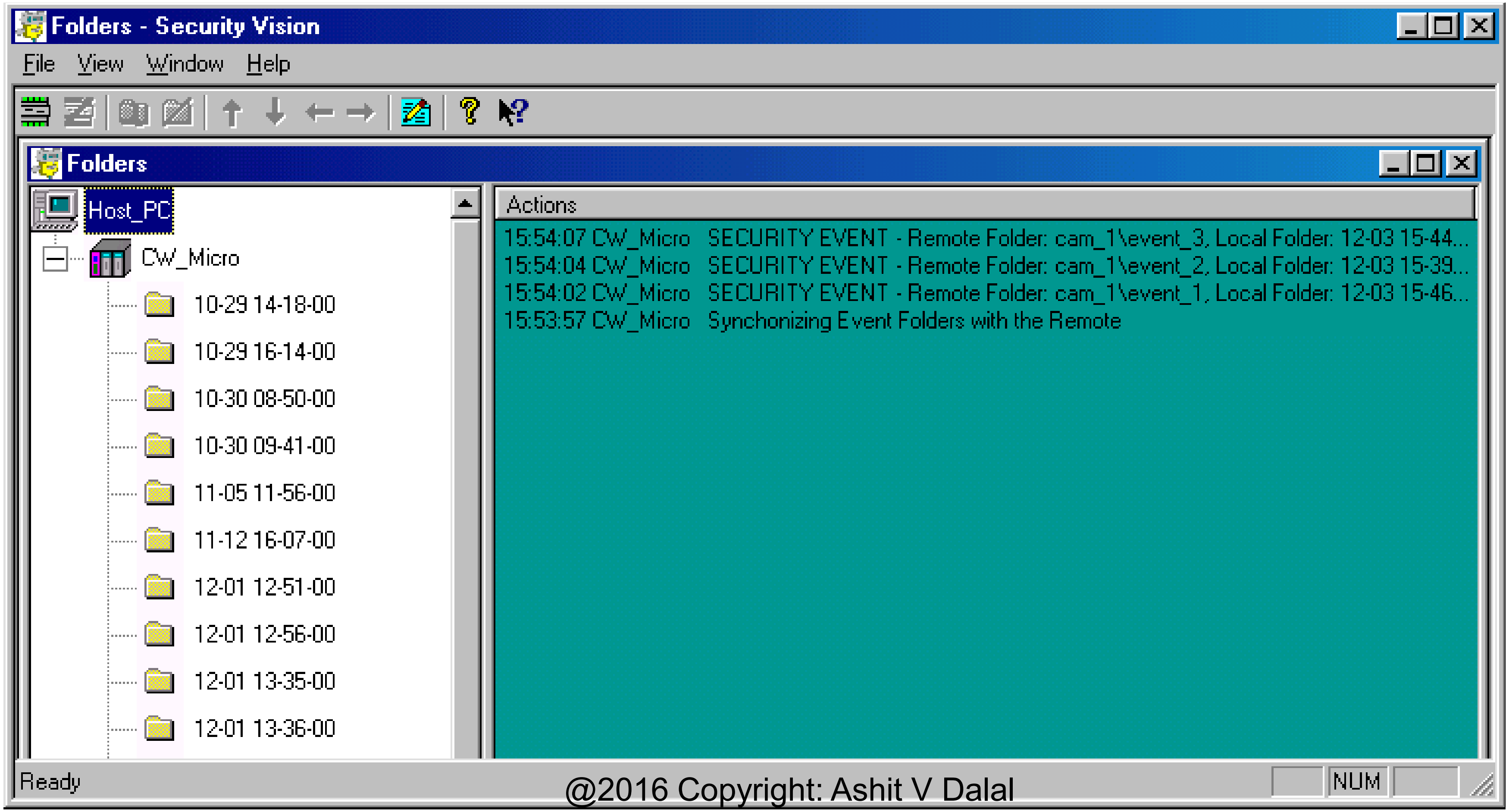
- Camera FTP’s image every x sec (e.g. every five seconds) to RTU
- JPEG images for each camera are stored in folders in CW FLASH
- Alarm will cause upload, to the PC, of pre and post event folder



Better Bet for the Network:
Ethernet or Wireless Ethernet

Utility at the PC

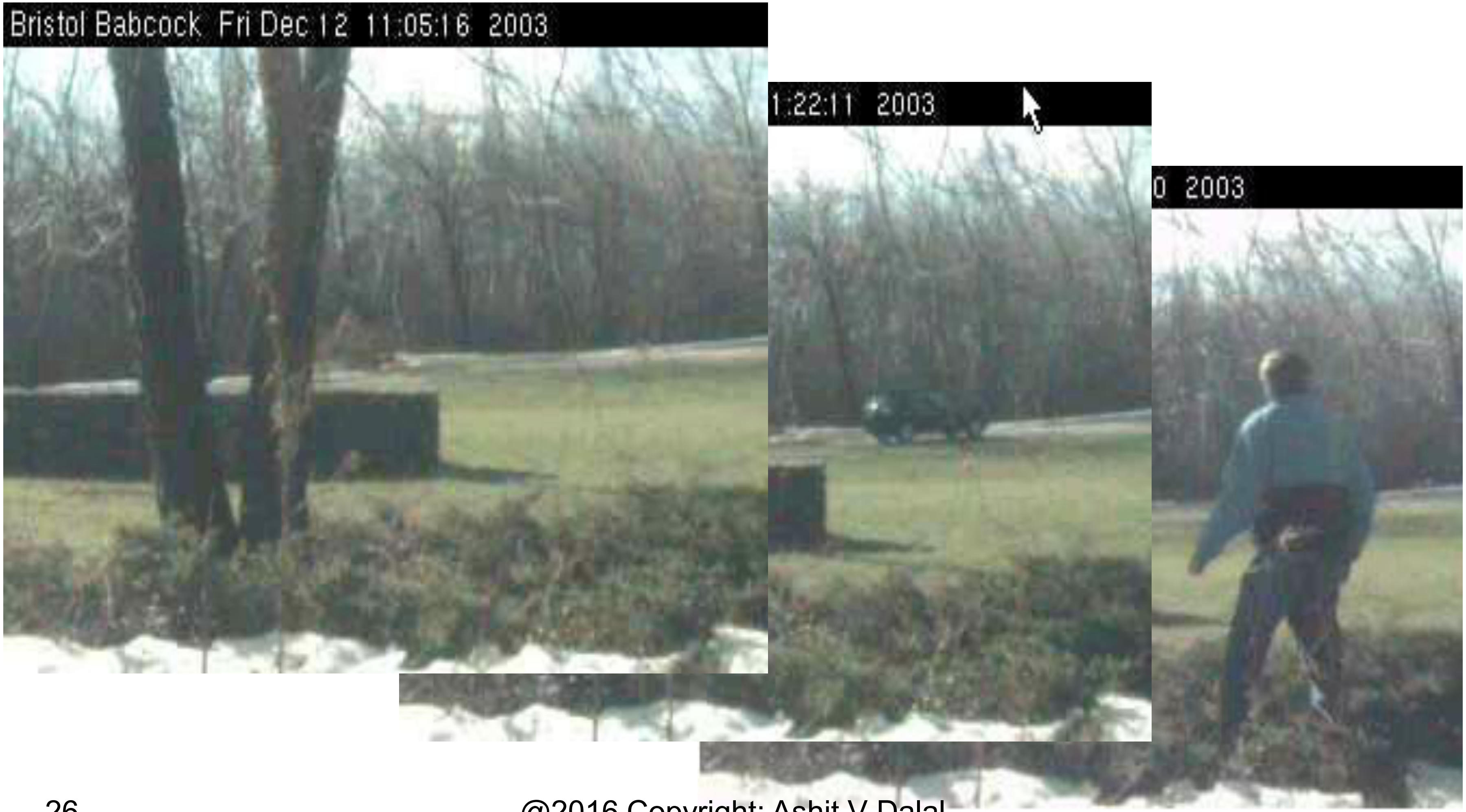
Upon receiving the time stamped event alarm notification, the entry will be added to the event list in the Security Vision window in OpenBSI.



```
15:54:07 CW_Micro   SECURITY EVENT - Remote Folder: cam_1\event_3, Local Folder: 12-03 15-44...
15:54:04 CW_Micro   SECURITY EVENT - Remote Folder: cam_1\event_2, Local Folder: 12-03 15-39...
15:54:02 CW_Micro   SECURITY EVENT - Remote Folder: cam_1\event_1, Local Folder: 12-03 15-46...
15:53:57 CW_Micro   Synchonizing Event Folders with the Remote
```

Utility at the PC

Selecting the event will initiate scrolling of the event file images.



Camera Considerations

- Numerous IP cameras and web cams are available
- Indoor or outdoor installation
- Operating temperature range
- Preferred file xfer and communication combination is FTP via Ethernet/IP
- Our experience is with Axis cameras.

Installations

- Access control and physical security for pump station associated with elevated tank in water distribution system
- Access control for gate at wastewater treatment plant
- Physical security for chemical storage
- Monitoring for chlorinator control

Any Questions?

Some References

- “SCADA and Industrial Automation Security,” http://www.scadasec.net/
- “SCADA Security Blog” http://www.digitalbond.com/SCADA_Blog/SCADA_blog.htm
- “SCADA Gospel Archives (edited archives of the SCADA mailing list)” “http://members.iinet.net.au/~ianw/archive/book1.htm
- “21 Steps to Improve the Cyber Security of SCADA Networks,” http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf
- “Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems” http://www.gao.gov/new.items/d04354.pdf
- “Myths and Facts Behind Cyber Security of Industrial Controls” http://www.pimaweb.org/conferences/april2003/MythsAndFactsBehindCyberSecurity.pdf
- Cisco’s “Integrating IT and Control System Security” http://www.scadasec.net/local/37
- modbus.org

Thank You!