The background is a stylized, low-poly illustration of a dam and its surroundings. The dam is a long, white structure with a central spillway, set against a backdrop of rolling hills in shades of blue, green, and brown. The water in the reservoir is a light blue. The overall style is modern and graphic.

“Unifying Dam Safety and Security”

FERC Workshop February 15 – 18, 2005

Session 4

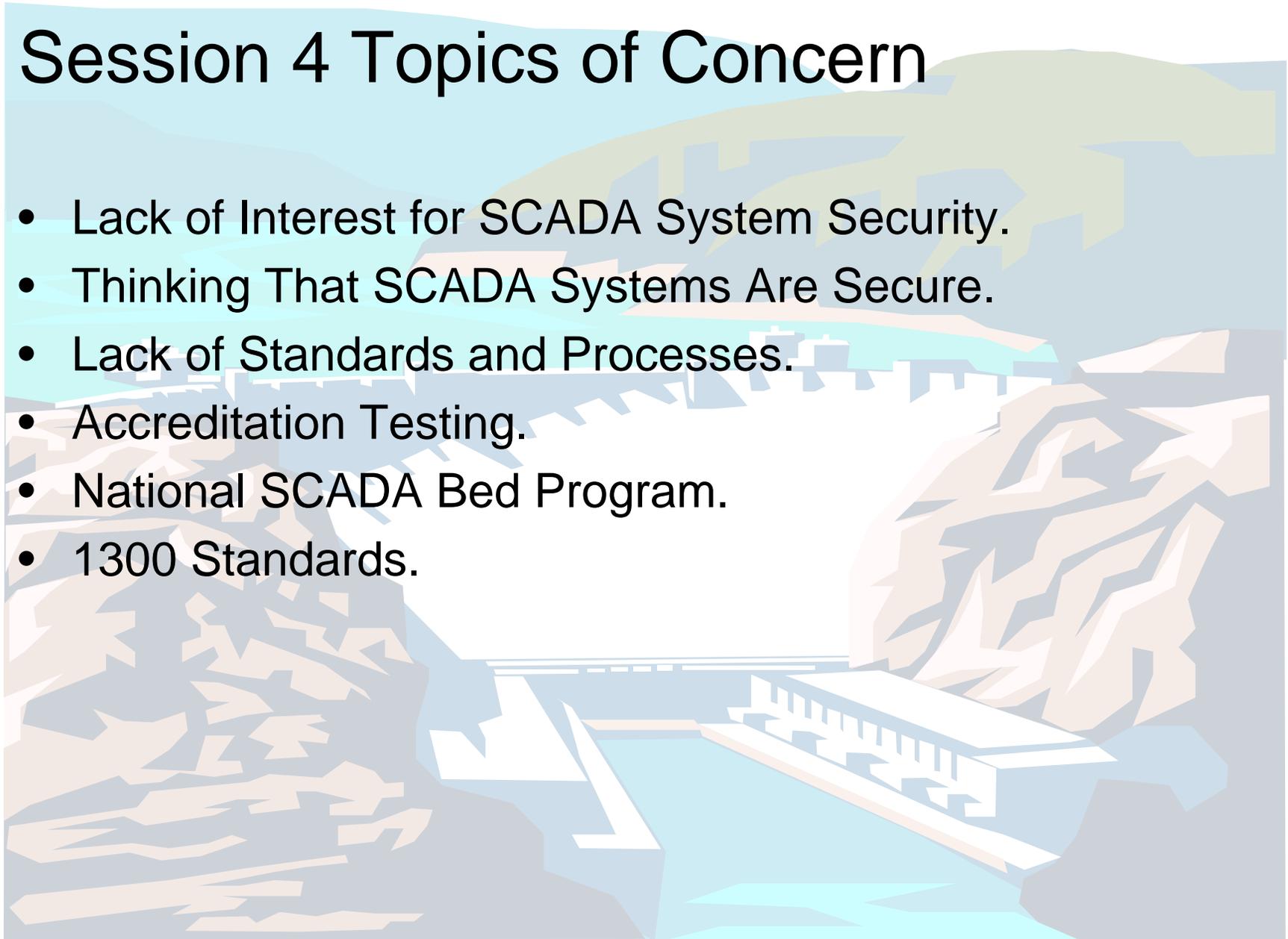
“SCADA Issues and IT”

Panel Members: Tom Flowers, CenterPoint Energy
Steve Jones, Placer County Water Agency
Bruce Lonnecker, Bureau of Reclamation
Jack Seibel, Portland General Electric Company

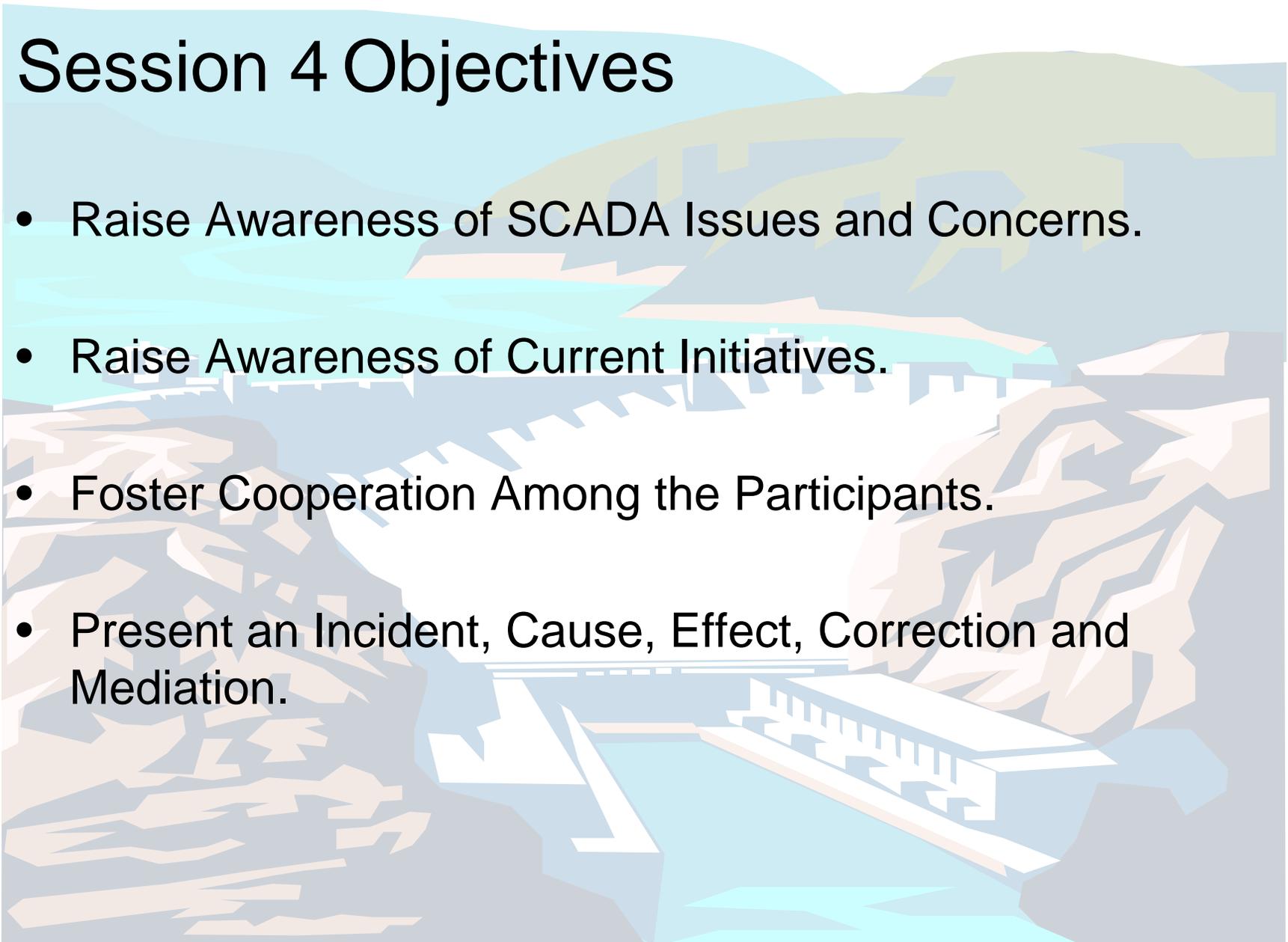
Moderator: Al Hancock, Xcel Energy Corporation

Session 4 Topics of Concern

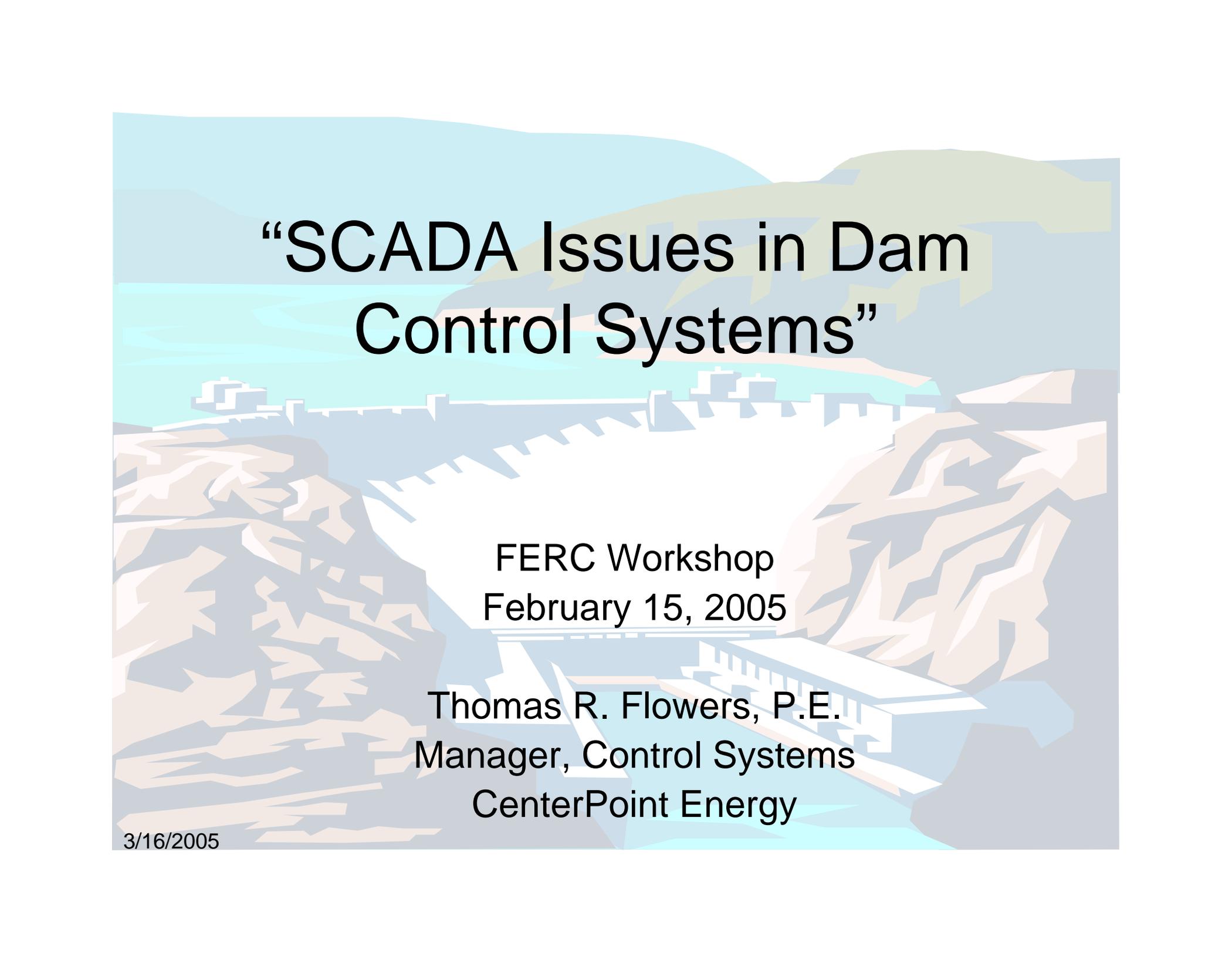
- Lack of Interest for SCADA System Security.
- Thinking That SCADA Systems Are Secure.
- Lack of Standards and Processes.
- Accreditation Testing.
- National SCADA Bed Program.
- 1300 Standards.



Session 4 Objectives



- Raise Awareness of SCADA Issues and Concerns.
- Raise Awareness of Current Initiatives.
- Foster Cooperation Among the Participants.
- Present an Incident, Cause, Effect, Correction and Mediation.



“SCADA Issues in Dam Control Systems”

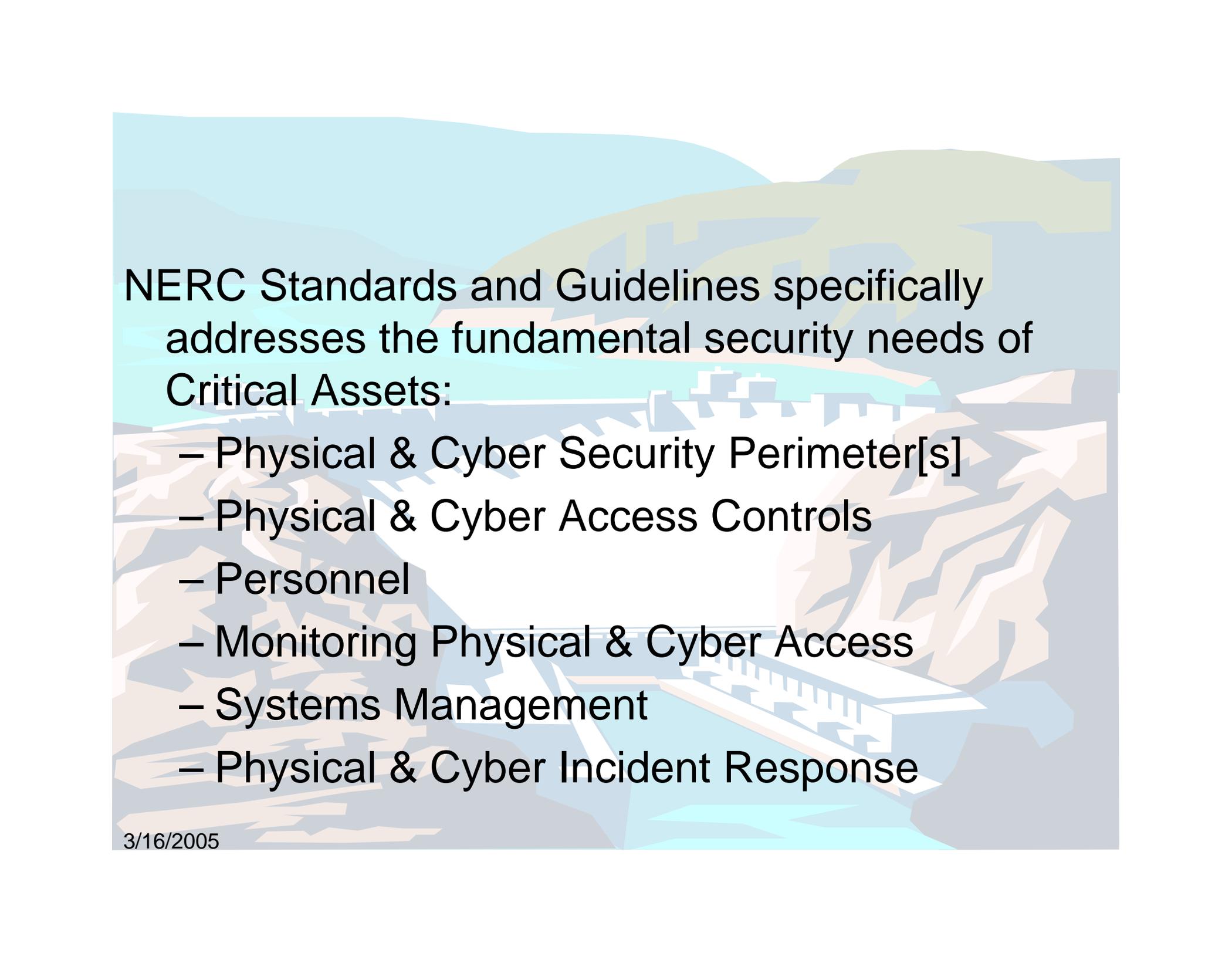
FERC Workshop
February 15, 2005

Thomas R. Flowers, P.E.
Manager, Control Systems
CenterPoint Energy

3/16/2005

NERC CIPC Role

Provide Guidance when considering the cyber and physical security/reliability at control facilities with a focus on practical methods using existing technology and proven processes.



NERC Standards and Guidelines specifically addresses the fundamental security needs of Critical Assets:

- Physical & Cyber Security Perimeter[s]
- Physical & Cyber Access Controls
- Personnel
- Monitoring Physical & Cyber Access
- Systems Management
- Physical & Cyber Incident Response

NERC Security Guidelines

- Vulnerability & Risk Assessment
- Threat Response
- Physical Security – General
- Physical Security – Substations
- Risk Management
- Access Controls

NERC Security Guidelines

- Employment Background Screening
- Securing Process Control Systems
- Threat & Incident Reporting
- Control System Connectivity (2005)
- Information Security – Encryption (2005)
- Risk Assessment Methodologies (2005)*

Schedule for CIP-002-1_{thru} CIP-009-1

1/17 - 2/17	Post Draft 2 for a 30-day comment period (abbreviated period).
2/2	Conduct a Webcast for the Registered Ballot Body
2/18 - 3/15	Resolve comments on Draft 2 and prepare Draft 3.
3/15 - 4/30	Post draft 3 for a 45-day comment period
5/1 - 5/31	Resolve comments on Draft 3 and prepare final draft
6/1 - 6/30	Post final draft for 30-day review prior to ballot
7/1 - 7/31	Hold two rounds of balloting (includes time to respond to first ballots cast with negative comments.)
8/1 - 8/31	Post for 30 days prior to BOT adoption into the compliance program (assuming a positive vote by the ballot pool)

3/16/2005

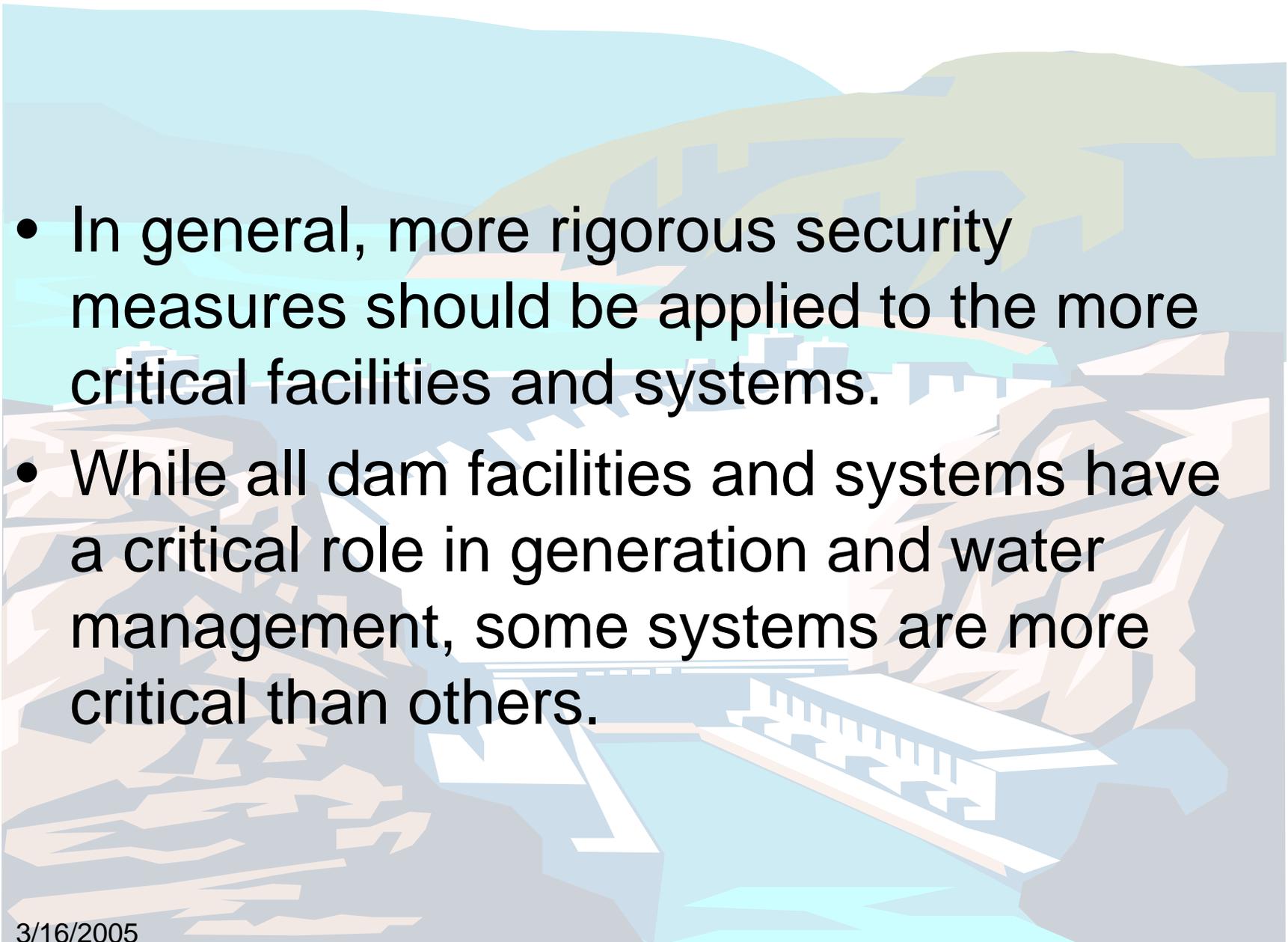


“The most effective Control System security profiles utilize physical access solutions to enhance cyber security and cyber solutions to enhance physical security.”

3/16/2005

Definition – Critical Asset

Those facilities, systems, and equipment which, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.

- 
- In general, more rigorous security measures should be applied to the more critical facilities and systems.
 - While all dam facilities and systems have a critical role in generation and water management, some systems are more critical than others.

The First Step

“The single most important element of your dam Control System security profile must be your Critical Infrastructure Protection Policy. However, the first step in the process is a Gap Analysis.”

The Most Common Mistake

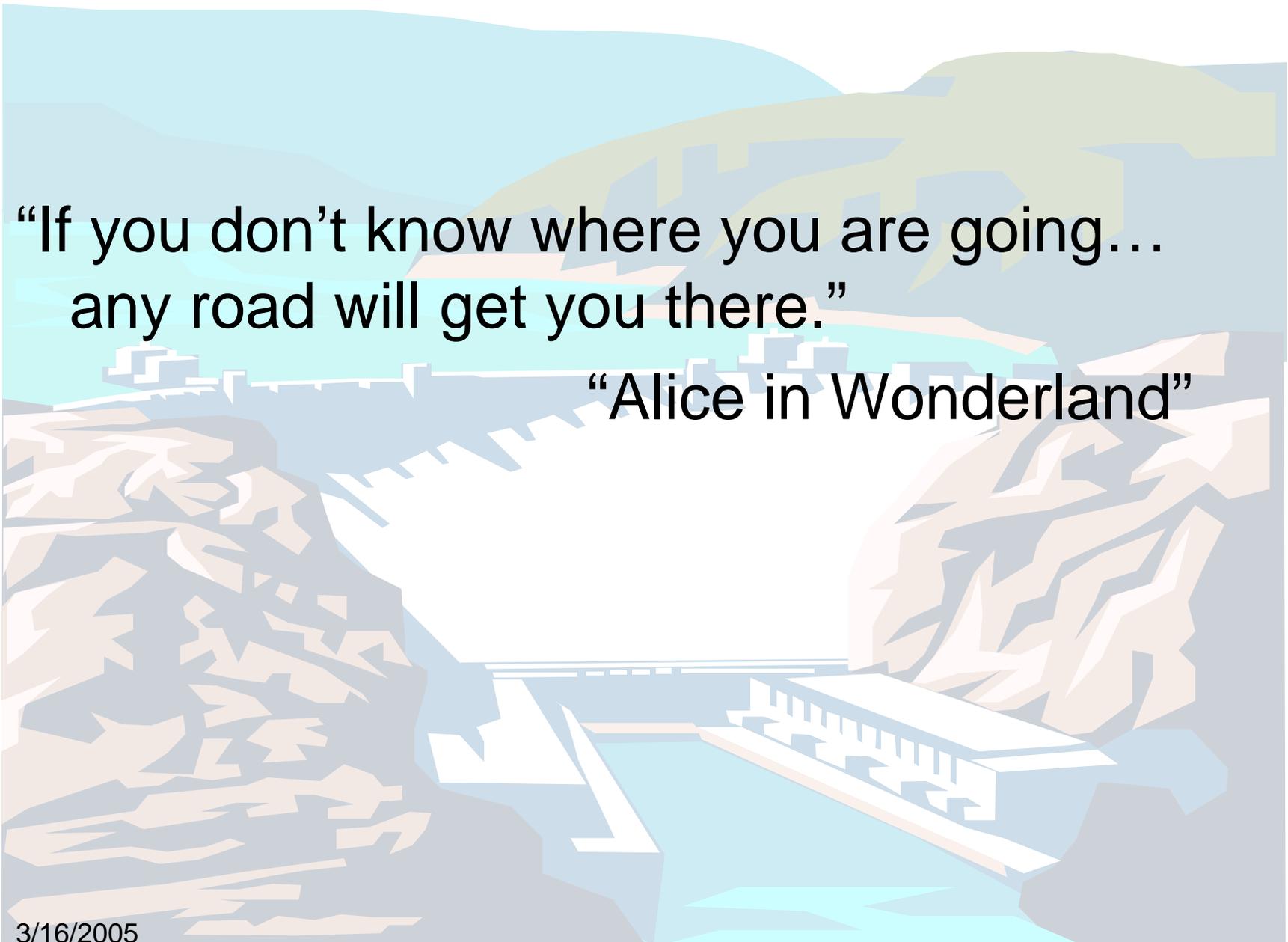
“While threats and vulnerabilities make the news... mitigating the consequences increases reliability.”

“Don’t dwell on ‘how’ someone might exploit a vulnerability... focus on ‘if’ they do, what are the consequences, and what can you do to prevent or mitigate the impact.”

The SCADA Paradox

“Situational awareness is center of the SCADA universe and it comes only from consistent and coherent data acquisition.”

“Focus your cyber and physical security hardening efforts on maintaining reliable situational awareness.”



“If you don’t know where you are going...
any road will get you there.”

“Alice in Wonderland”

3/16/2005

Internet Links

- *Security Guidelines for the Electric Sector*
<http://www.esisac.com/library-guidelines.htm>
- *Urgent Action Cyber Security Standard*, NERC, August 13, 2003
<http://www.esisac.com/library-guidelines.htm>
- *An Approach to Action for the Electricity Sector, Version 1*, NERC, June 2001,
<http://www.esisac.com/library-other.htm>
- *Threat Alert Levels and Physical Response Guidelines*, NERC, October 2002,
<http://www.esisac.com/library-guidelines.htm>

Contact

A stylized, low-poly illustration of a dam and its surrounding environment. The dam is a long, white structure with a spillway on the left side, situated in a valley. The water behind the dam is a light blue color. The surrounding landscape consists of brown and tan rocky terrain on the left and right sides, and green hills in the background under a light blue sky.

Thomas R. Flowers, P.E.
Manager, Control Systems Division
CenterPoint Energy
Phone: (713) 207-2122
Email: tom.flowers@centerpointenergy.com

3/16/2005

SCADA System Security Investigation and Documentation at the Bureau of Reclamation

Panel Member: Bruce Lonnecker,
IT System C&A Project Manager
Bureau of Reclamation

Panel Session: Session 4 - SCADA Issues

What is SCADA?

- Supervisory Control And Data Acquisition (AKA DCS or Process Control System)
- Computer-based network system that collects, displays and/or stores information from data collection equipment and sensors to support the control and automated operation of equipment, devices and systems.

What is SCADA?

(and is it IT?)

- Typically has these minimum components:
 - Master control station(s)
 - Servers and other ITComponents
 - HMI
 - Remote Terminal Units (RTUs)
 - Gather data
 - Transmit control signals
 - Network and communication system
 - Microwave
 - Leased telephone line
 - LANs and WANs
 - Internet

Why the concern for SCADA security?

- Typically SCADA must be available at all times for system control and monitoring. Manual control is slow and expensive and monitoring without SCADA is incomplete.
- If connected, compromise from anywhere through the WAN, LAN or Internet may be possible and the system controlled to cause system or plant damage or personnel injury.

Why the concern for SCADA security?

- If the SCADA is connected to other SCADA systems, compromise of one may affect another.
- If the SCADA controls a broad system like a power transmission system, compromise could start or foster a cascading (blackout) problem, affecting national security and organizational embarrassment.

How can SCADA security be evaluated?

- Follow NIST, FIPS, Trade Org. guidance
- For Reclamation, Certification and Accreditation is a documented process of evaluating
 - Threats
 - Vulnerabilities
 - Consequences

to determine Risks ($R=T \times V \times C$), scheduling remediation, and accepting (management) remaining risks.

Minimum evaluation:

- Describe the SCADA system – Essential step
 - Purpose
 - System diagram and IT component listing
 - Communication protocol
 - Communication paths
 - HAR
 - microwave
 - Personnel responsibilities
 - Criticality to business function

Minimum evaluation:

- Assess Risks – The MOST important step
 - Determine THREATS
 - Environmental
 - Weather related
 - Man made
 - External
 - » Terrorist
 - » Viruses and worms
 - Internal
 - » Organizational
 - » Malicious and non-malicious

Minimum evaluation:

- Assess Risks – The MOST important stem
 - Determine VULNERABILITIES to threats
 - Physical
 - Control room access
 - Control cable protection
 - IT-based
 - Routable protocols
 - Unnecessarily open ports
 - Unnecessary services
 - Connections
 - » Internet
 - » Dial-up

Minimum evaluation:

- Assess Risks – The MOST important step
 - Determine CONSEQUENCES of system failure
 - Confidential information
 - Operating information
 - Privacy
 - Integrity of information
 - False readings
 - Availability of system
 - For business function
 - For economical operation

Minimum evaluation:

- Assess Risks – The MOST important step
 - Determine each risk by combining each component, Threat, Vulnerability, and Consequence:

$$R = T \times V \times C$$

Note that a low value for any component brings the risk down to that value. For example, if there is negligible consequence of a weakness being exploited, the risk to the system is also negligible.

Minimum evaluation:

- Develop (or review) System Security Plan
 - Describes how system is to be operated and maintained to ensure security
 - Management controls
 - Separation of management duties
 - Background checks
 - Upgrade and replacement planning
 - Operational controls
 - Identification and authorization
 - Auditing
 - Technical controls
 - Patching procedures and virus protection
 - Backup procedures

Minimum evaluation:

- Formal Testing of Security Controls
AKA Security Test and Evaluation (ST&E)
 - Should be performed by a trained, independent agent
 - Involves review of:
 - Risk Assessment
 - System Security Plan
 - Includes technical testing including
 - System inspection
 - Port and service scans, Patch checks

Minimum evaluation:

- Risk Mitigation Plan
 - List vulnerabilities and associated risks
 - Determine if the risks are serious enough to mitigate or if they can be accepted
 - Might include schedule for mitigation and estimated costs

Minimum evaluation:

- Assignment of Responsibility (Reclamation calls it Certification and Accreditation)
 - A certifying manager signs a form saying the system has been evaluated and certifies that the documentation accurately describes the system and vulnerabilities.
 - A accrediting manager authorizes the system to operate and takes responsibility for secure operation.

Additional Document:

- Contingency Plan
 - Should list who can be called on to solve problems with system operation.
 - Work phones
 - Cell phones
 - Home phones
 - Should describe where to find replacement equipment and backup data
 - Should describe how to restore system to operational capability
 - Should be tested on a regular basis and improved.

Costs:

- Depends on complexity of system
- Depends on level of detail and documentation desired
- We have seen complete assessments cost as much as \$500,000 and as little as \$20,000. Developing a System Description and a Risk Assessment could cost as little as one week's time and could give management an idea as to whether it is necessary to proceed.
- We have seen assessments that took 4 months and some that took 3 weeks.
- Can be done in-house or by contractor. The break point might be at 4 to 7 systems.

Questions:

- Do your facilities have SCADA systems?
- Do you know if they are secure?
- Does management know the risks to the SCADA system?
- Can you afford to loose the system for as much as a week or month? – economic trade off of evaluation and remediation vs. contingency operation during repairs.
- Will CC, NERC, EPA or DHS require evaluation grid, distribution and plant control security?

Questions:

- Do you have a security assessment process available?
- Do you have operational agreements with other SCADA systems that are connected to yours?
- Do you have connections to the LAN, WAN, or Internet?
- Do you have outside vendors servicing your SCADA?
- Do outside vendors have security credentials?

Questions:

- Have your SCADA administrators and operators had background checks?
- Do your SCADA security managers audit operations regularly to ensure that only authorized operations are performed by authorized persons?
- Is your SCADA system aging? Are replacement components and software upgrades available?
- Are you dependant on a single person for maintenance of the system?

Are Hydro Control Systems Vulnerable?

Unifying Dam Safety and Security
Fort Worth Workshop – February 2005

Jacob Seibel, PE
Compliance Specialist
Portland General Electric Co.

Are Hydro Control Systems Vulnerable?

To a Greater or Lesser Extent, all Control Systems are Vulnerable

- Some Items Subject to Failure?
- What Can Cause Failures?
- How Do You Know?
- How to Correct?
- PGE's experience.

Are Hydro Control Systems Vulnerable?

- What are some of the items that fail:
 - Hardware
Instruments, Sensors, Control Devices
 - Communications
Hard Wire, Wireless
 - Software
Man Machine Interface (MMI)
Control Devices

Are Hydro Control Systems Vulnerable?

- What Can Cause These Failures:
 - Natural Events such as Flood, Fire, Wind, Ice
 - Damage or Destroy Hardware
 - Disrupt Communications
 - Temporary Loss of Physical Access
 - Manmade events
 - Accidents
 - Logic/Wiring Mistakes
 - Motor Vehicles (Autos, Trucks, Cranes, Airplanes)
 - Intentional acts
 - Vandalism and Sabotage

Are Hydro Control Systems Vulnerable?

- How do you know the extent your systems are vulnerable :
 - Review the Design
 - Know the Maintenance History
Component Failure History
 - Are Contingency Procedures and Operator Training Adequate

Are Hydro Control Systems Vulnerable?

■ PGE's Experience:

- Original Design
- Penetration Assessment

Are Hydro Control Systems Vulnerable?

- PGE's Original Design (mid 90s). The system is:
 - Proven Vendors and Proven Technology
 - Local area PLC Based
 - Local MMI interface if communications lost
 - No connections to Corporate LAN
 - Programming done by PGE employees using non-proprietary software
 - Password protected. Restricted number of Modems – double password protected.
 - Operations Procedures and Training Address Abnormal Events including control failures

Are Hydro Control Systems Vulnerable?

- Penetration Assessment (2002)
 - Sponsored By Corporate IT
 - Why?
 - Findings:
Although The Designers and Technicians Thought our Hydro Control Systems were “Bulletproof”, the Consultant Found Items That Needed to be Fixed.

Are Hydro Control Systems Vulnerable?

- Questions?

Ralston Afterbay Dam

Incident

August 5, 2004







Placer County Water Agency
Oxbow Powerhouse / Ralston Afterbay
Station Power

Backup Generator
@ Afterbay



Transfer
Switch

Oxbow 208/120 Station Bus

52-2

52-1

Ralston A Bay
Station Bus

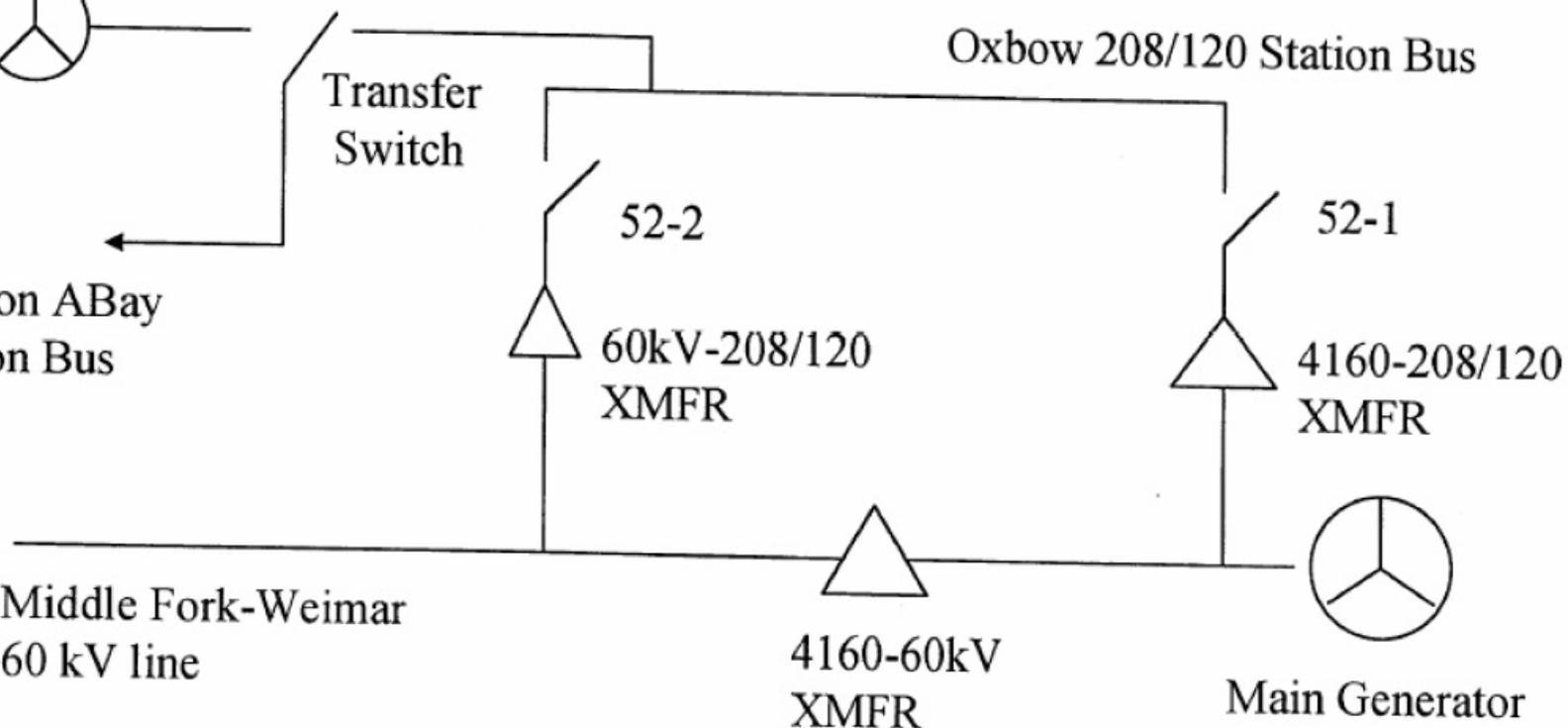
60kV-208/120
XMFR

4160-208/120
XMFR

Middle Fork-Weimar
60 kV line

4160-60kV
XMFR

Main Generator



1-24-00
AP 117300
SP 117500
2-15-00 * AP 117500
SA 117500
AP 117500
SP 117500



- DISPLAY OPTIONS
- 00-LEVEL
 - 01-SET POINT
 - 02-NO. 1 RESPONSE TIME
 - 03-DEADBAND
 - 04-RESET PERIOD
 - 05-NO. 1 MAX RUN TIME
 - 06-LOW ALARM
 - 07-HIGH ALARM
 - 08-LAST COMMAND
 - 09-AVERAGE LEVEL
 - 10-COUNTDOWN
 - 11
 - 12-NO. 2 RESPONSE TIME
 - 13-ACTIVE GATE
 - 14-ALARM CODE
 - 15-NO. 2 MAX RUN TIME
 - 16-GATE NO. 1
 - 17-GATE NO. 2
 - 18-DIFFERENCE
 - 19-DIFFERENCE SET

AFTERBAY GATES 2 & 3



ALARM CODES
1-TRANSDUCER FAIL
2-SETTING OUT OF RANGE
3-NO GATE IN AUTO

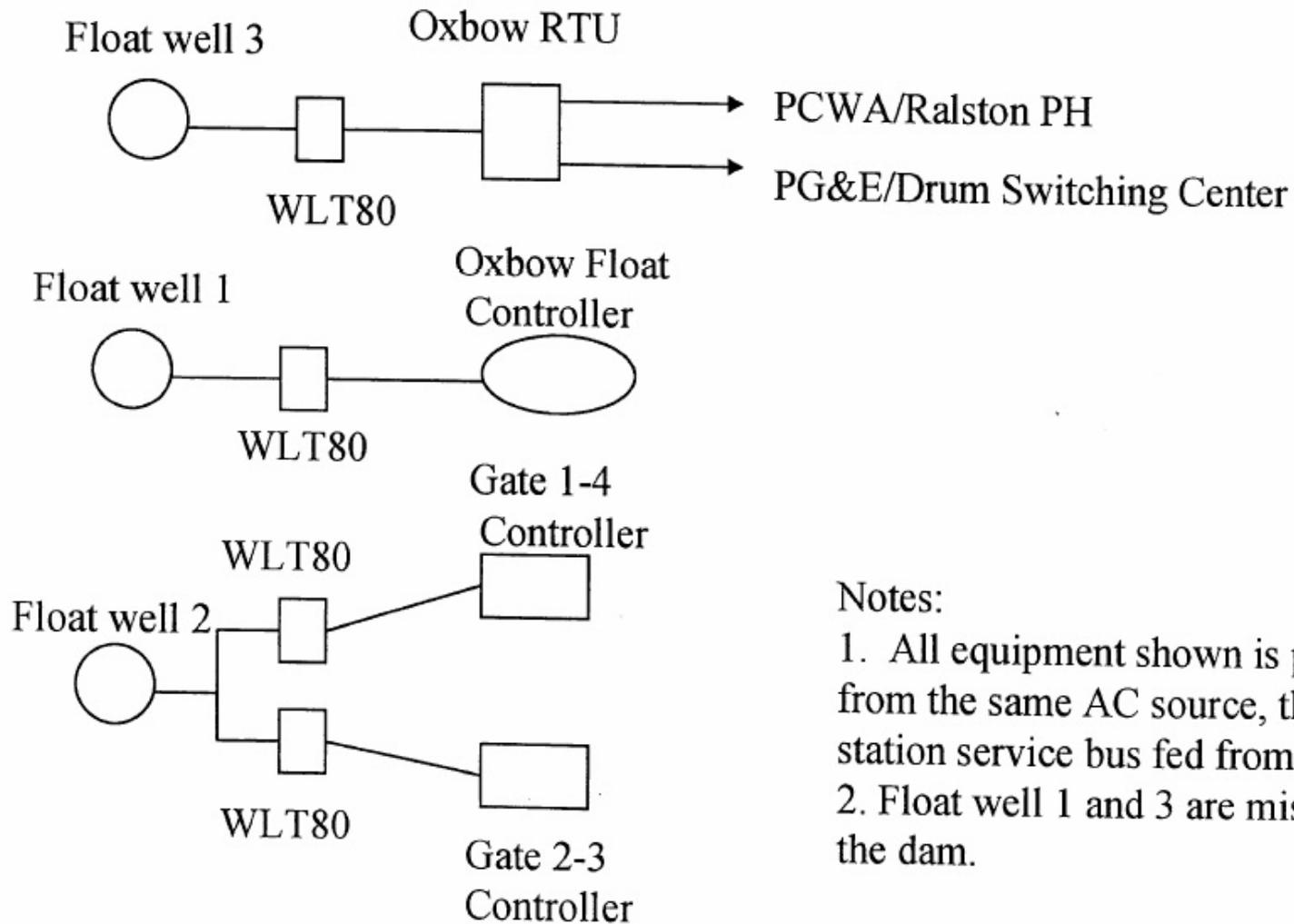
#1

NO. 2

NO. 1

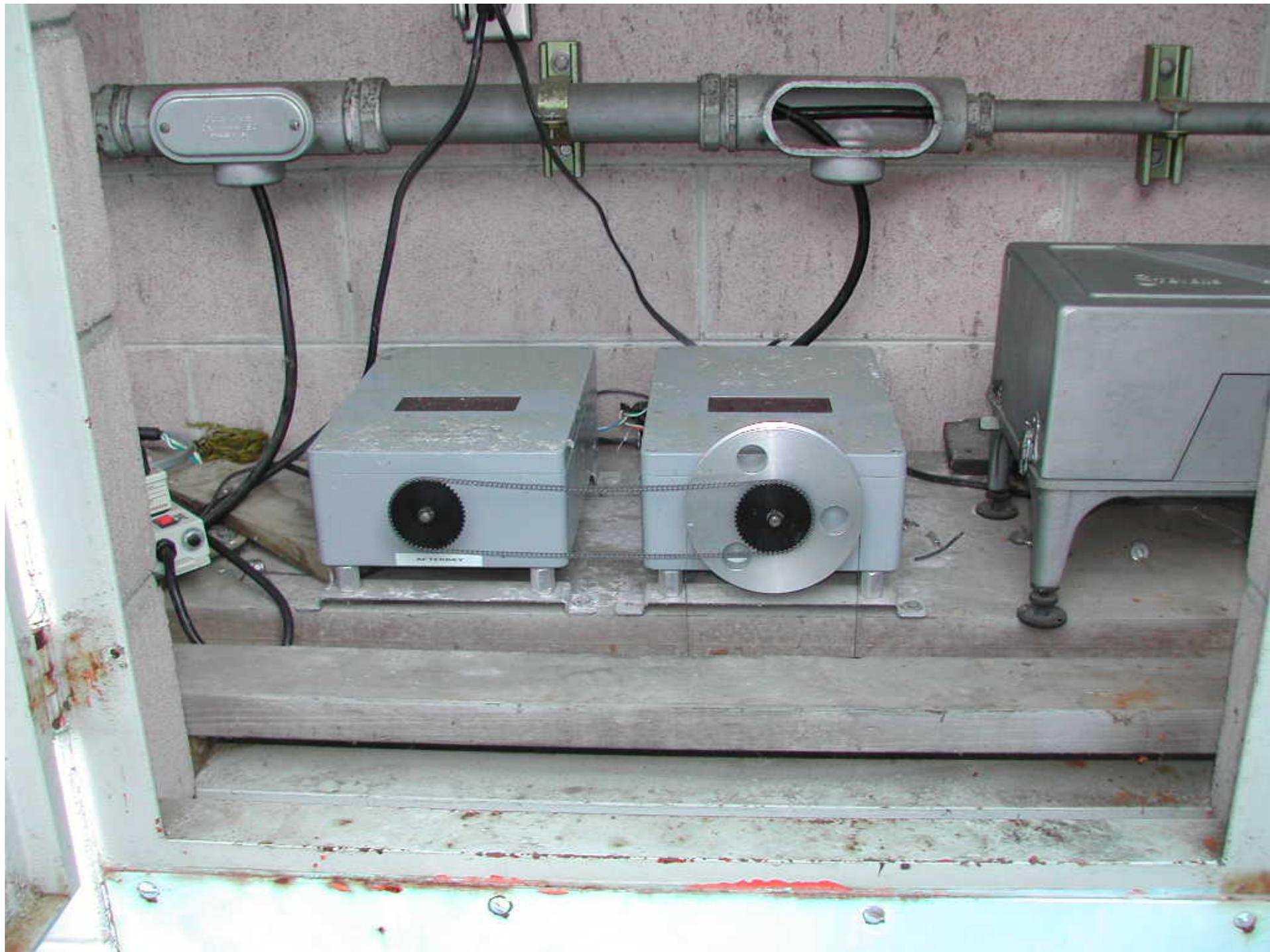
Placer County Water Agency

Ralston Afterbay Spillgate/Float Controls



Notes:

1. All equipment shown is powered by from the same AC source, the Ralston A Bay station service bus fed from the powerhouse.
2. Float well 1 and 3 are mismarked 3 and 1 at the dam.



Selector Switch Setting	Function	Setting for Gates 2 & 3 Controller	Setting for Gates 1 & 4 Controller
0	Reservoir forebay elevation, feet	n/a	n/a
1	Setpoint (reservoir elevation controller will seek to maintain), feet	1177.11	1177.61
2	Gates 2 & 1 response times, respectively, seconds	41.8	39
3	Deadband, feet	0.15	0.15
4	Reset period, seconds (The time interval between successive control actions.)	603	601
5	Gates 2 & 1 maximum run times, respectively, seconds (the duration of a control action)	30	30
6	Low level alarm, feet	1173.02	1174.3
7	High level alarm, feet	1176.01	1176.01
8	Last command length, seconds	30	30
9	Average water level	1171.24	1171.23
10	Next command countdown	countdown	countdown
11	Blank		
12	Gates 3 & 4 response times, respectively, seconds	42	41
13	Active gate	1	1
14	Malfunction code	0	0
15	Gates 3 & 4 maximum run times, respectively, seconds	30	30
16	Gates 2 & 1 positions, respectively	0.3	0.3
17	Gates 3 & 4 positions, respectively	0.3	0.3
18	Gate difference	0.2	0.2
19	Difference setpoint, percent	12.5	10.5

- CONNECTION DIAGRAM -

SEQUENCE CONTROLLER
W/RX TELEMETRY
REF DWG 94-121

SWITCH MUST BE
CLOSED TO INDICATE
AUTO CONTROL

GATE #1
IN AUTO

GATE #2
IN AUTO

FSK TONE 2125HZ

FSK TONE 2125HZ

GATE #2 POSITION 4-20MA

GATE #1 POSITION 4-20MA

PRIMARY
WATER LEVEL

SECONDARY
WATER LEVEL

TRANSDUCERS
REF DWG 72-977

GATE #2
CONTROLS

GATE #1
CONTROLS

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15

- 1
- 2
- 3

- 1
- 2
- 3
- 4
- 5
- 6
- 7

H } POWER
N } IN
G } 120VAC



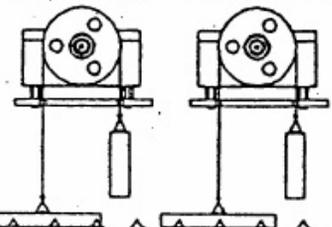
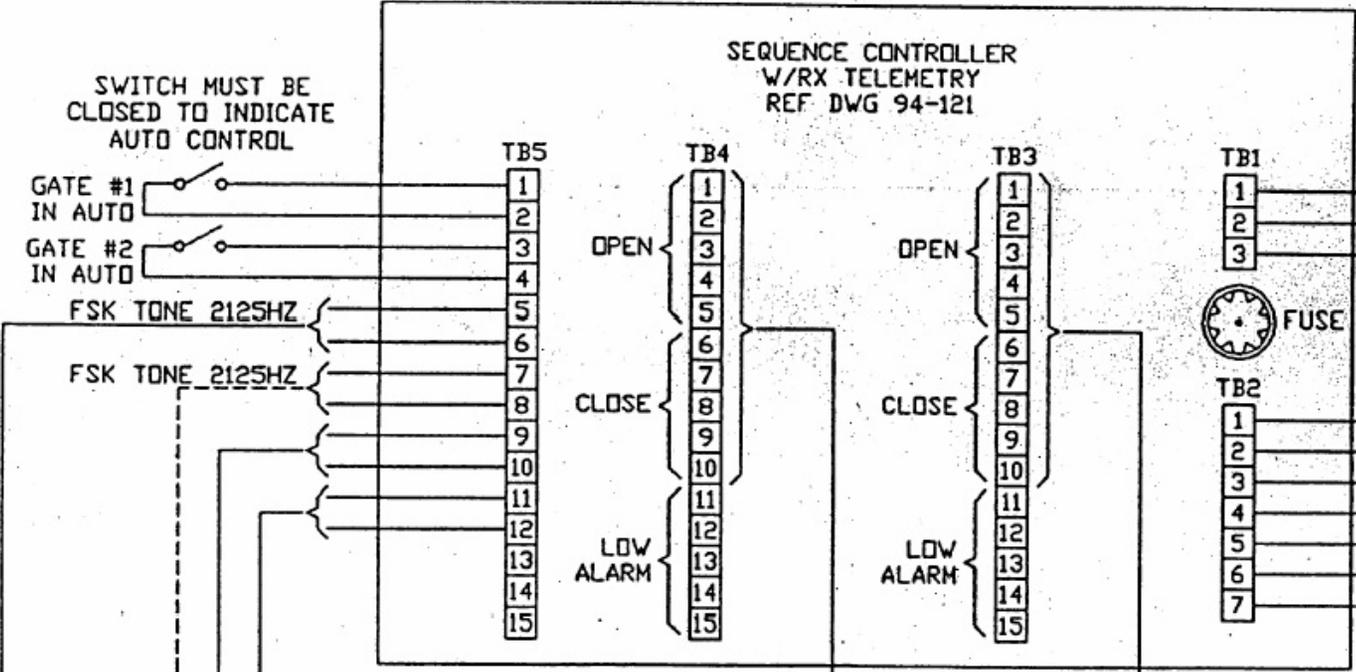
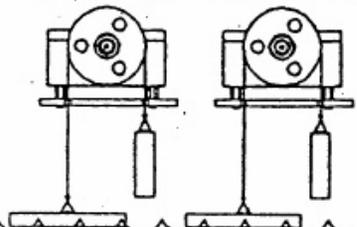
0-10V
COMMON
0-1MA
COMPUTER
FAIL
SYSTEM
ALARM

GP

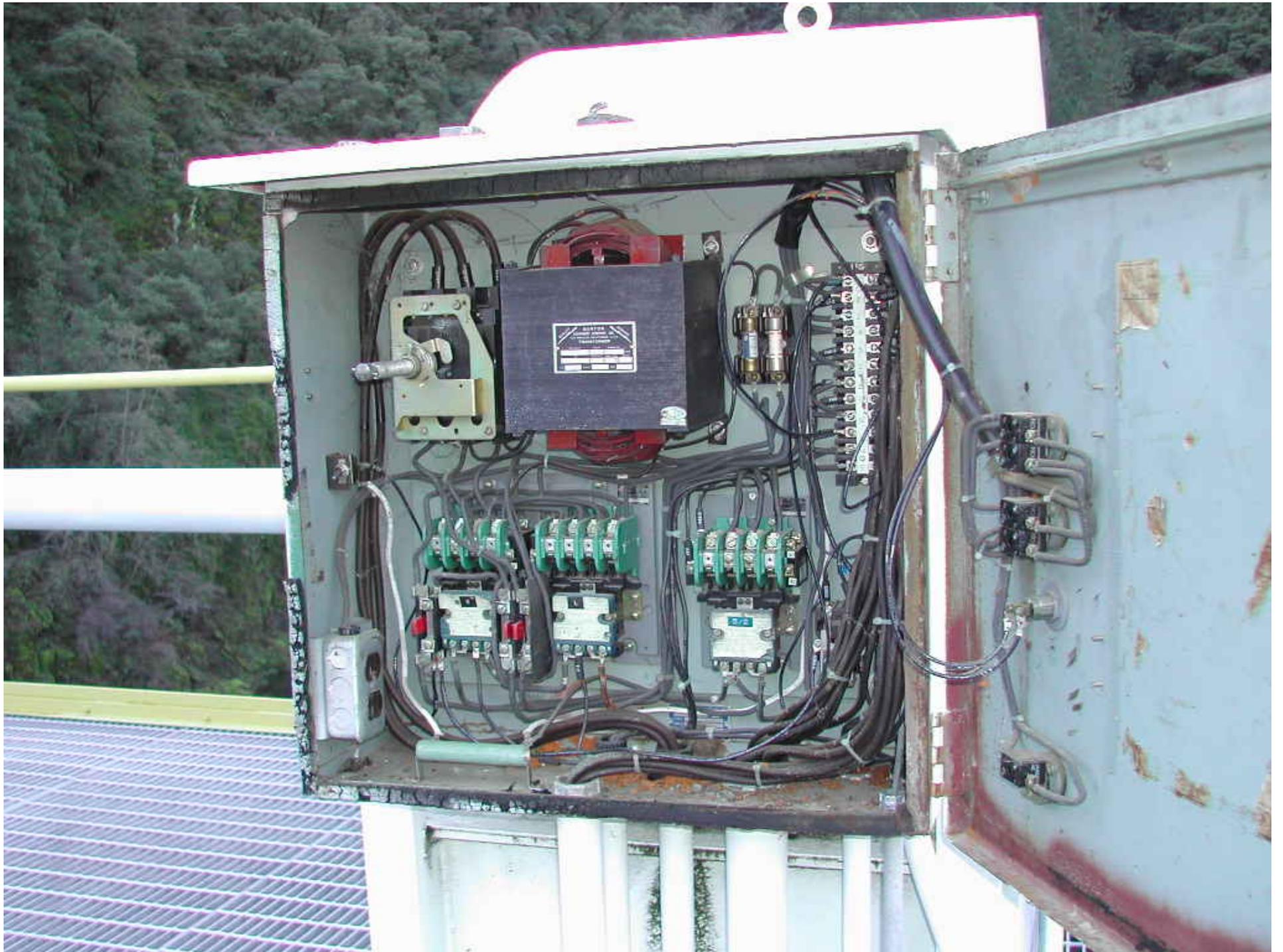
GP

GATE
#2

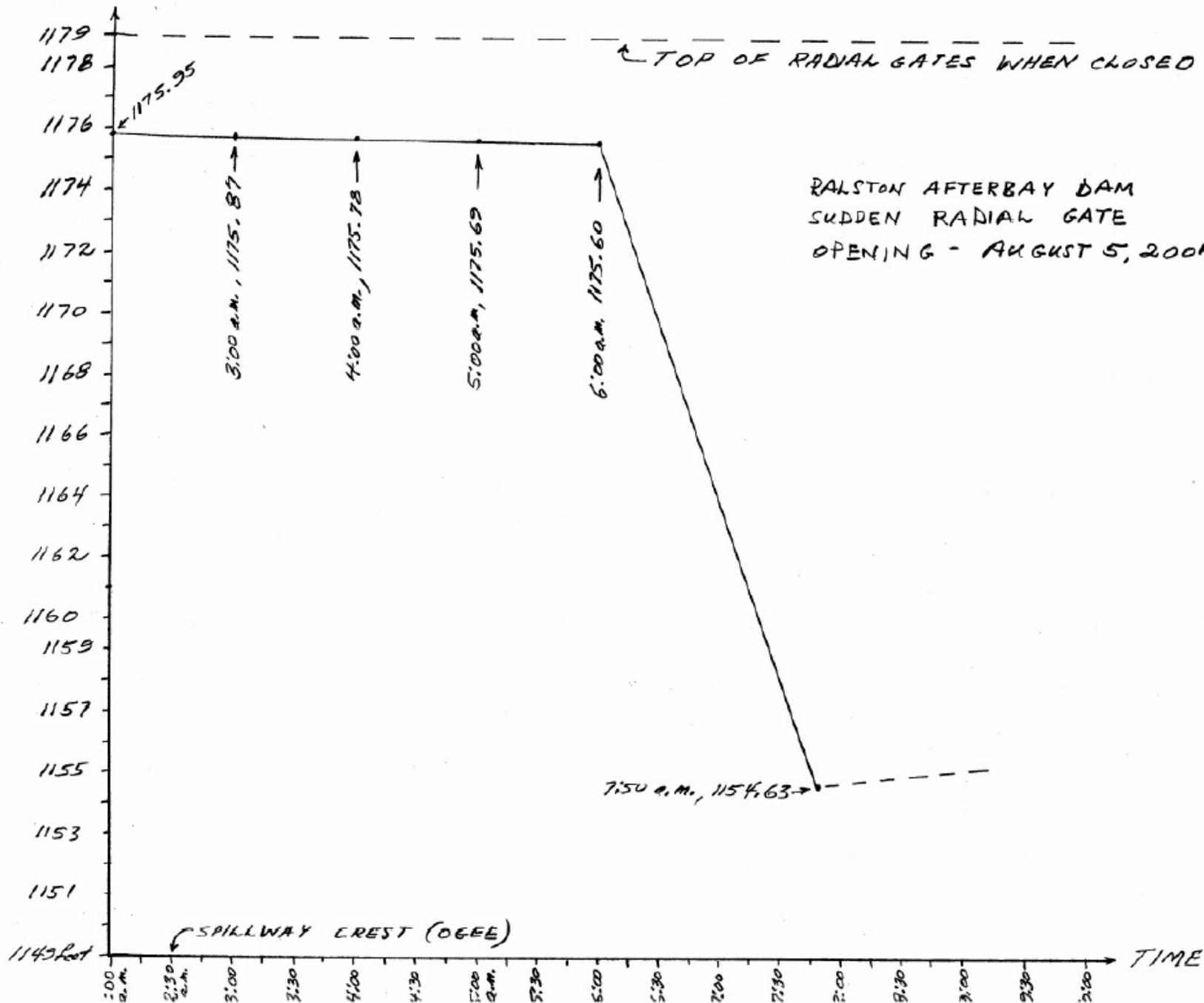
GATE
#1

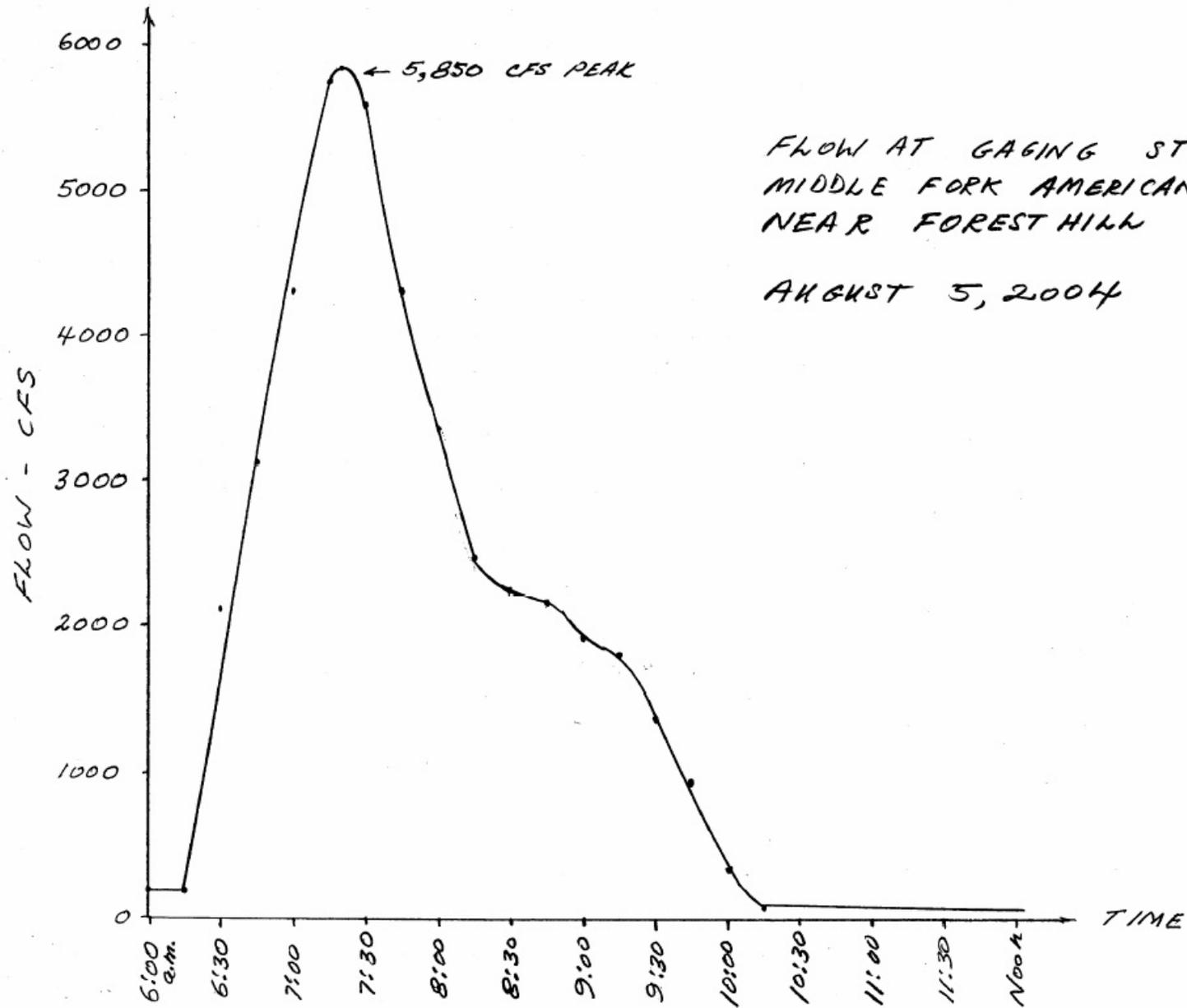






RESERVOIR ELEVATION - FEET ABOVE SEA LEVEL





FLOW AT GAGING STATION
MIDDLE FORK AMERICAN RIVER
NEAR FOREST HILL

AUGUST 5, 2004



