Presentation for the

2005 Tri-service infrastructure systems conference

Remote Operation System, Kaskaskia Dam Design, Certification, & Accreditation

by

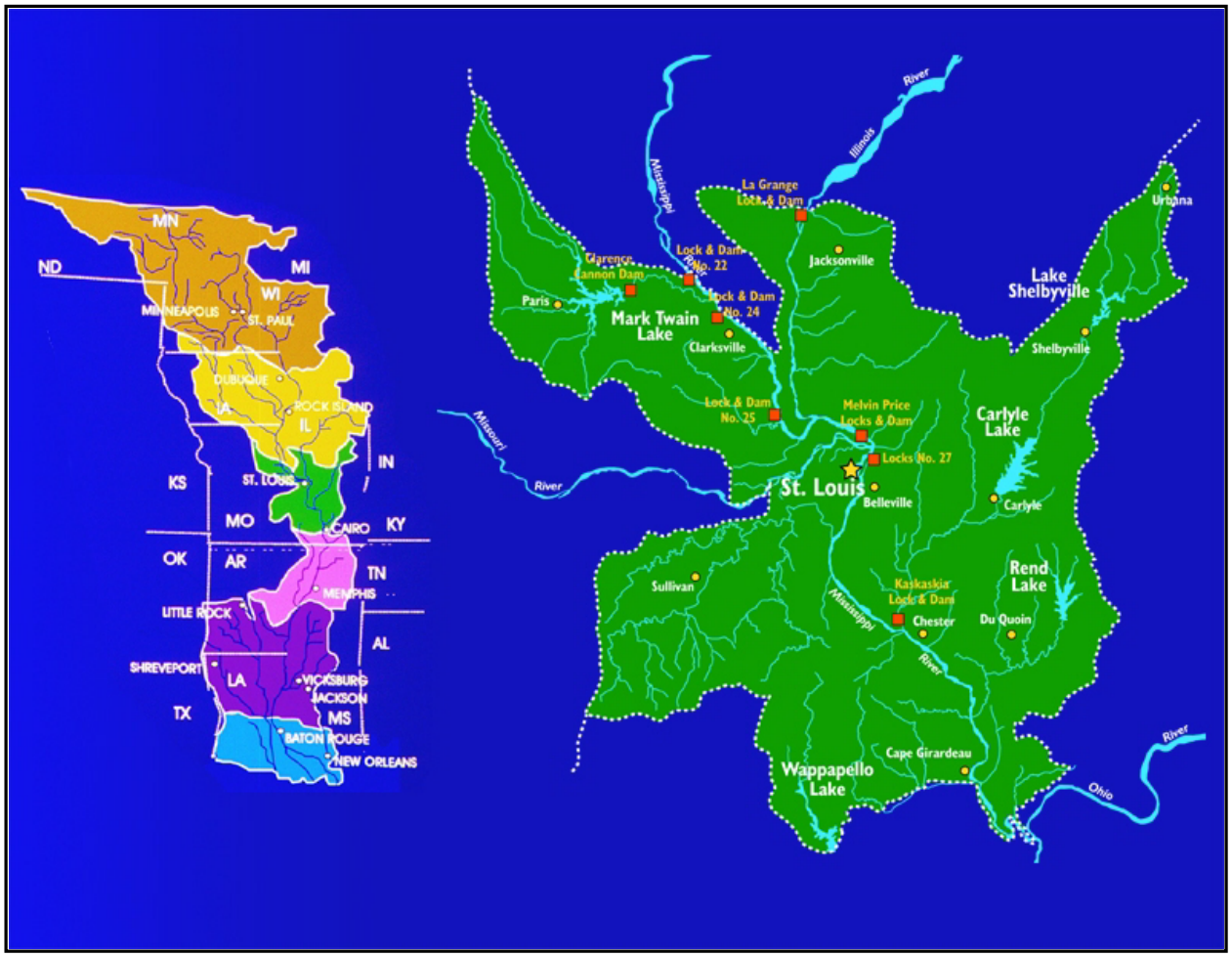
Shane M. Nieukirk, P.E.

Electrical Engineer, St. Louis District

August , 2004

US Army Corps
of Engineers®
Mississippi Valley Division
Mississippi River Commission

St. Louis District



- 10 rivers
- 5 lock & dam sites
- 5 Corps lakes
- 720 miles of levees
- 92 flood control systems
- 416 miles of navigable channel
- 70 pumping plants
- 162 recreation areas
- 1 hydropower project

Primary Missions

- Navigation
- Flood Damage Reduction
- Environmental
- Hydropower
- Water Supply
- Readiness
- Recreation
- Regulatory
- FUSRAP
- Interagency/International Support

Agenda

- Overview/Background
- System Design & Architecture
- System Accreditation & Certification

Kaskaskia Lock and Dam

US Army Corps of Engineers®
Mississippi Valley Division
Mississippi River Commission

Kaskaskia Navigation Project

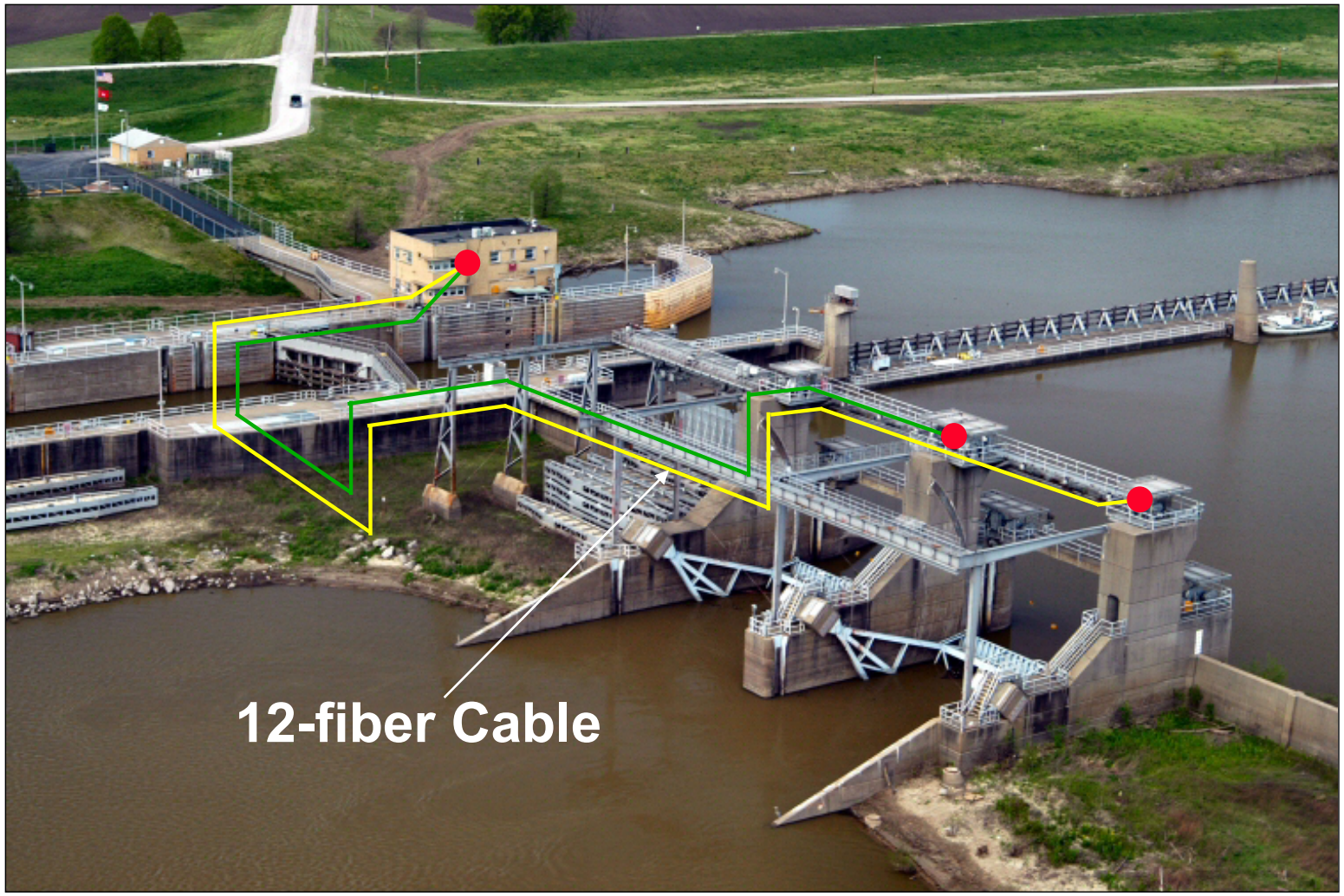
- Constructed in 1974
- Located approximately 60 miles south of St. Louis
- Pool provides 36 miles of navigation channel on the Kaskaskia River
- Supports commercial navigation for grain and industry
- Provides water supply to several communities
- Project includes:
  - 600’ x 84’ Lock Chamber
  - Two 60’ Tainter Gates

Remote Operation System

- The FY04 budget for the project was $2.4M. The initial FY05 budget was $392k.
- Operations Division requested the design of a system to control the pool in the event 24/7 operation of the project could not be maintained.
- System was designed by Engineering Division at a cost of $30,000. Startup and EDC totaled another $29,500.
- Electrical enclosures were fabricated locally at a cost of $51,150.
- Installation of enclosures, conduit, cable, & CCTV was under a separate contract at a cost of $123,525.

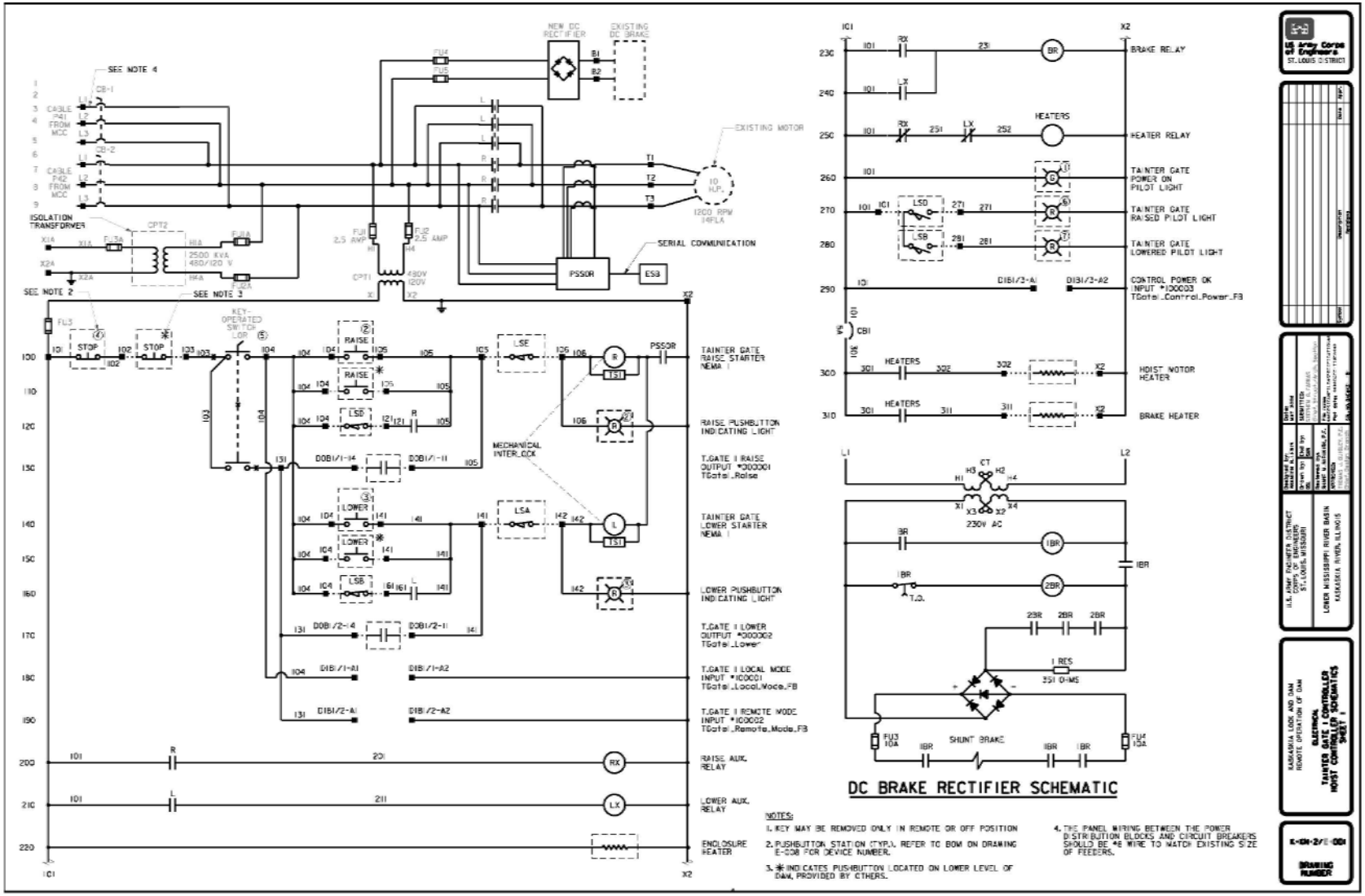
US Army Corps
of Engineers®
Mississippi Valley Division
Mississippi River Commission

Kaskaskia Navigation Project



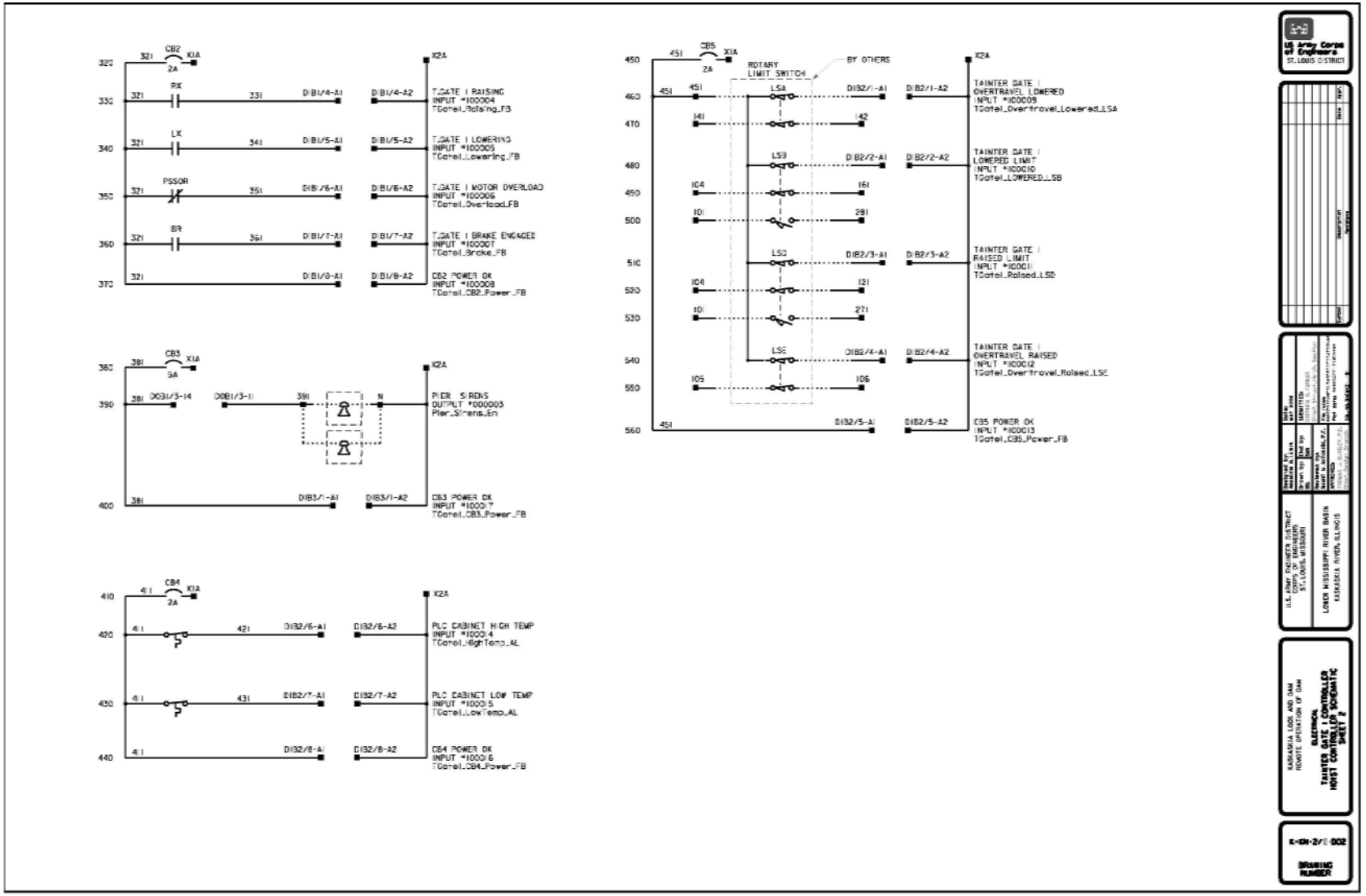
US Army Corps of Engineers®
Mississippi Valley Division
Mississippi River Commission

Tainter Gate Hoist Controller

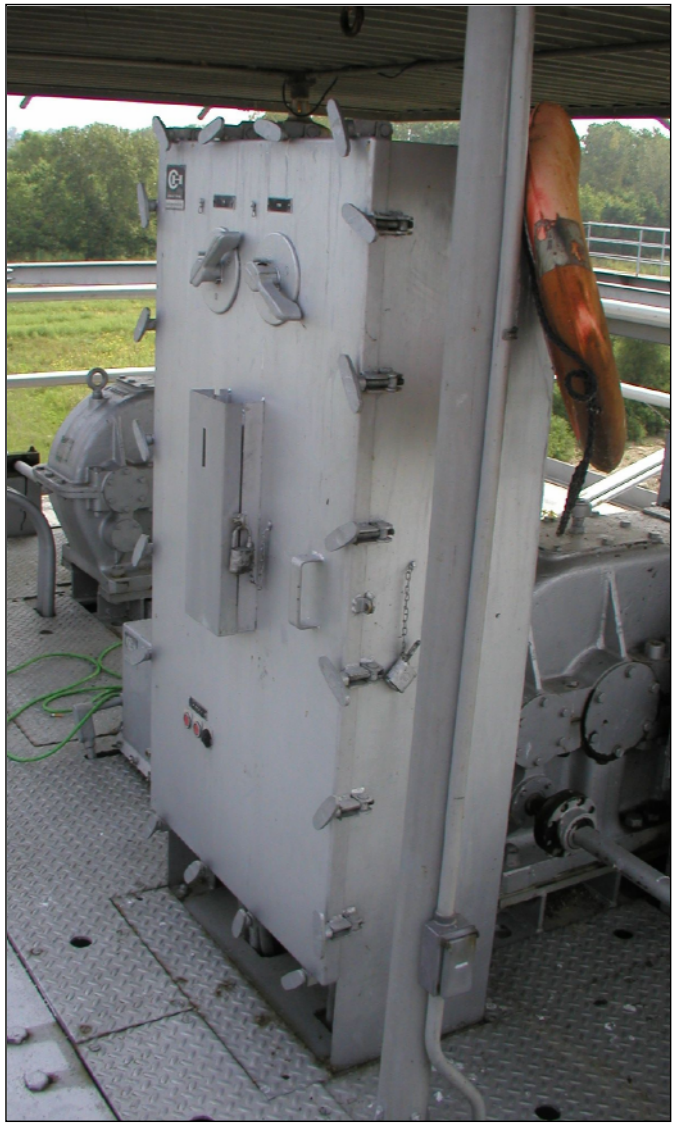


One Corps Serving the Armed Forces and the Nation

Tainter Gate Hoist Controller

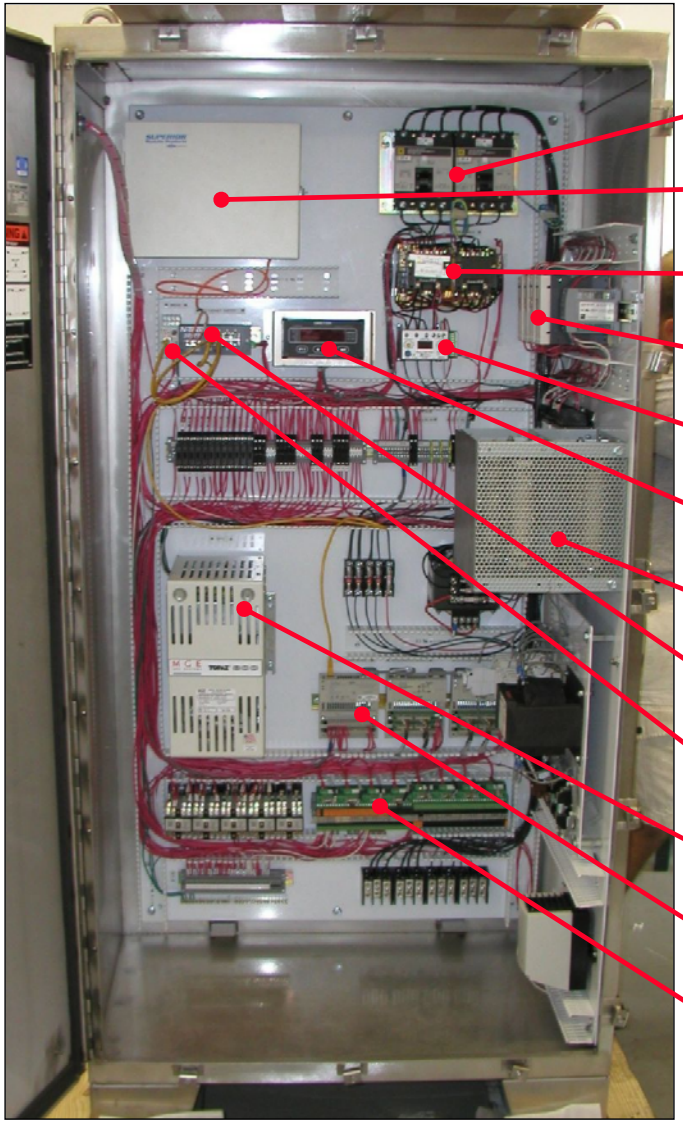


Tainter Gate Hoist Controller



- Two Tainter Gate Hoist Controllers and an Ethernet Switch Enclosure were fabricated in a panel shop
  - Greater control over equipment delivered
  - Greater oversight of fabrication
  - Tested by the Government
- Enclosures were installed under a separate contract

Tainter Gate Hoist Controller

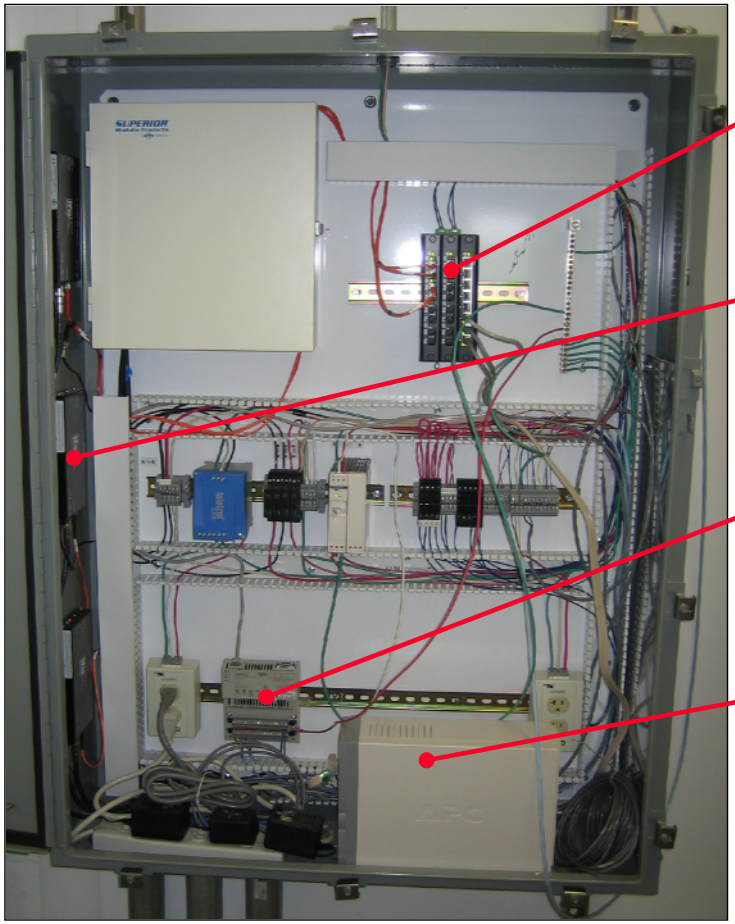


- Mech. Interlock Circuit Breaker
- Fiber Optic Interconnect
- Reversing Starter
- Power Supplies
- Solid-State Motor Overload
- Resolver Interface Module
- DC Brake Rectifier
- Industrial Ethernet Switch
- Ethernet-Serial Bridge
- Isolation Transformer
- Schneider Momentum PLC
- Isolation Relays

Tainter Gate Hoist Controller

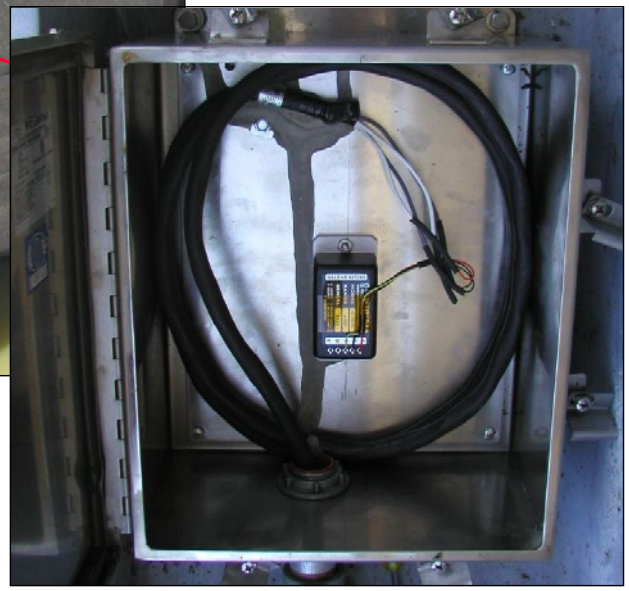
- Local controls provided in a separate enclosure on the side of the controller
- Includes a keyed Local-Off-Remote selector switch
- Key cannot be removed while in Local mode (also cannot close enclosure with key in place)S

Ethernet Switch Enclosure



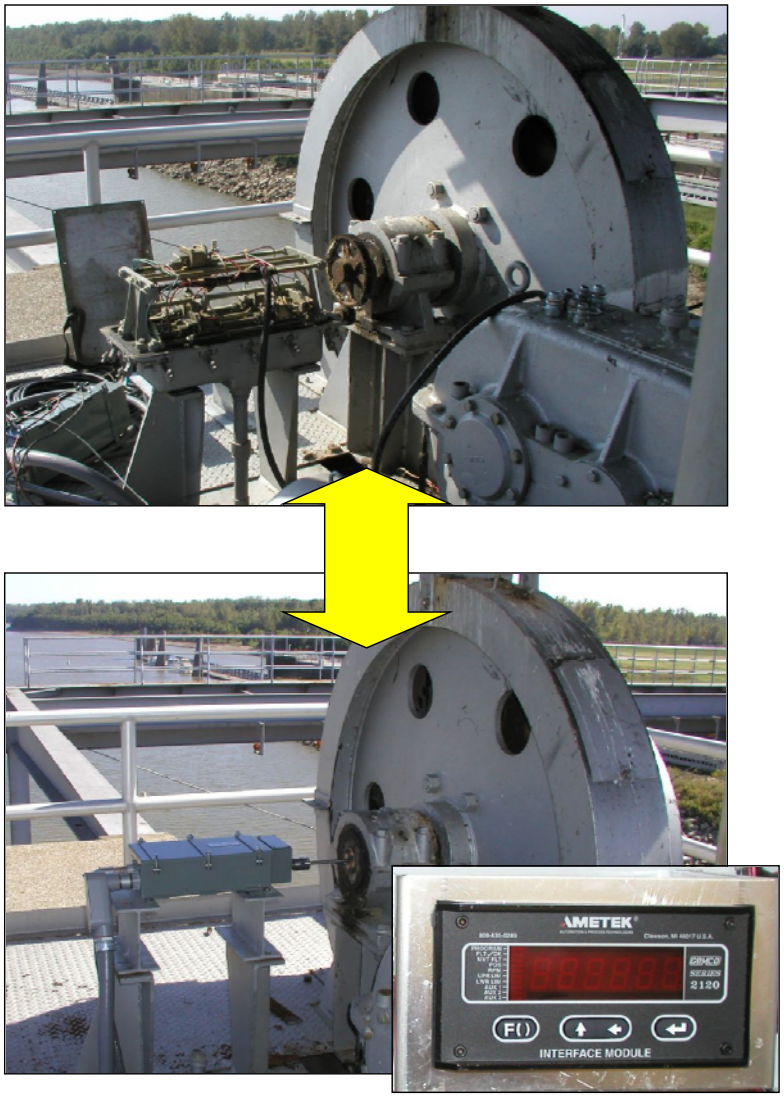
- Provides Ethernet connectivity to the PLCs on the dam
- Enclosure houses the F/O transceivers for the CCTV cameras
- A Momentum PLC processor was added for water levels
- Uninterruptible power supply

Tainter Gate Position



- Inclinometer measures angle of upper strut
- Linear feet of opening is calculated using trigonometry

Tainter Gate Limit Switch



- Original traveling nut limit switch was replaced by a rotary cam limit switch (Gemco 1980R)
- Includes integral gear reduction and resolver for hoist position. Requires interface module for a 4-20mA input to PLC
- The 1980 was used in lieu of the 1997 to avoid the cost of the incremental control. This feature was implemented in the PLC

Water Level Sensing

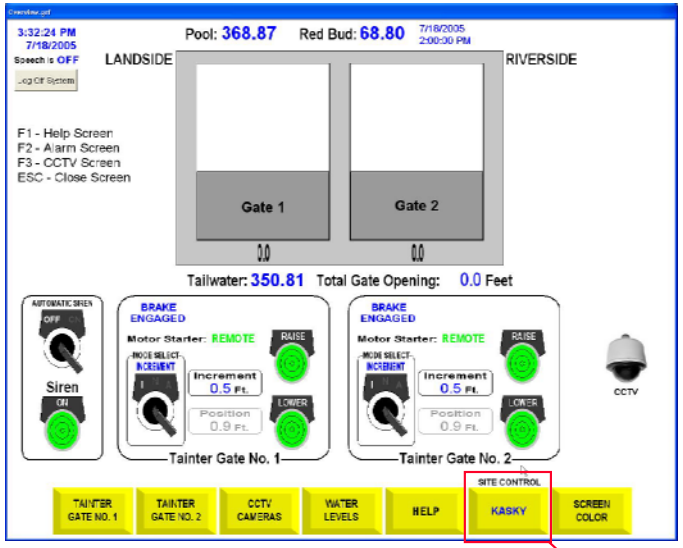
- In a effort to save money dedicated sensors were not installed
- Original approach was to access all levels across the network
- Because the network data was received by satellite and was not real-time, a PLC was added to interface with Water Control's float gages
- Pool and tailwater levels are analog inputs from shaft encoder
- Other river stage data is accessed from a database across the network

Closed Circuit Television

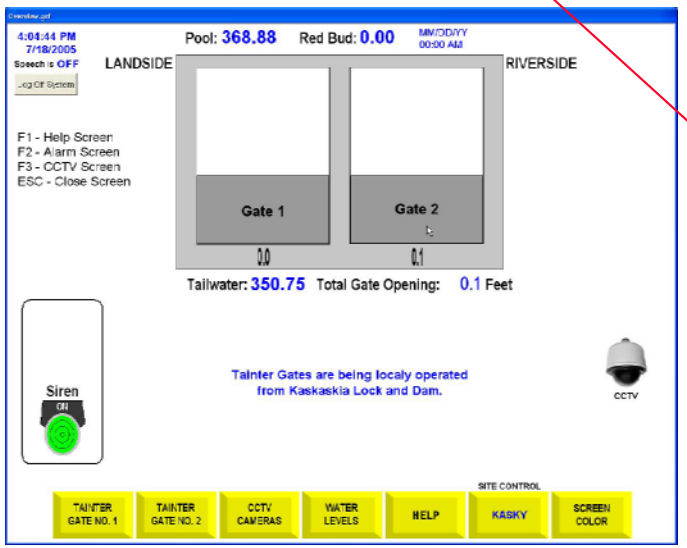
- Two cameras provide coverage of the pool, gate, and staff gage
- One downstream camera provides coverage behind the tainter gates and downstream of the dam
- Cameras are accessible across the network via a digital video recorder
- DVR is accessed using Internet Explorer or client software

Human Machine Interface

Local

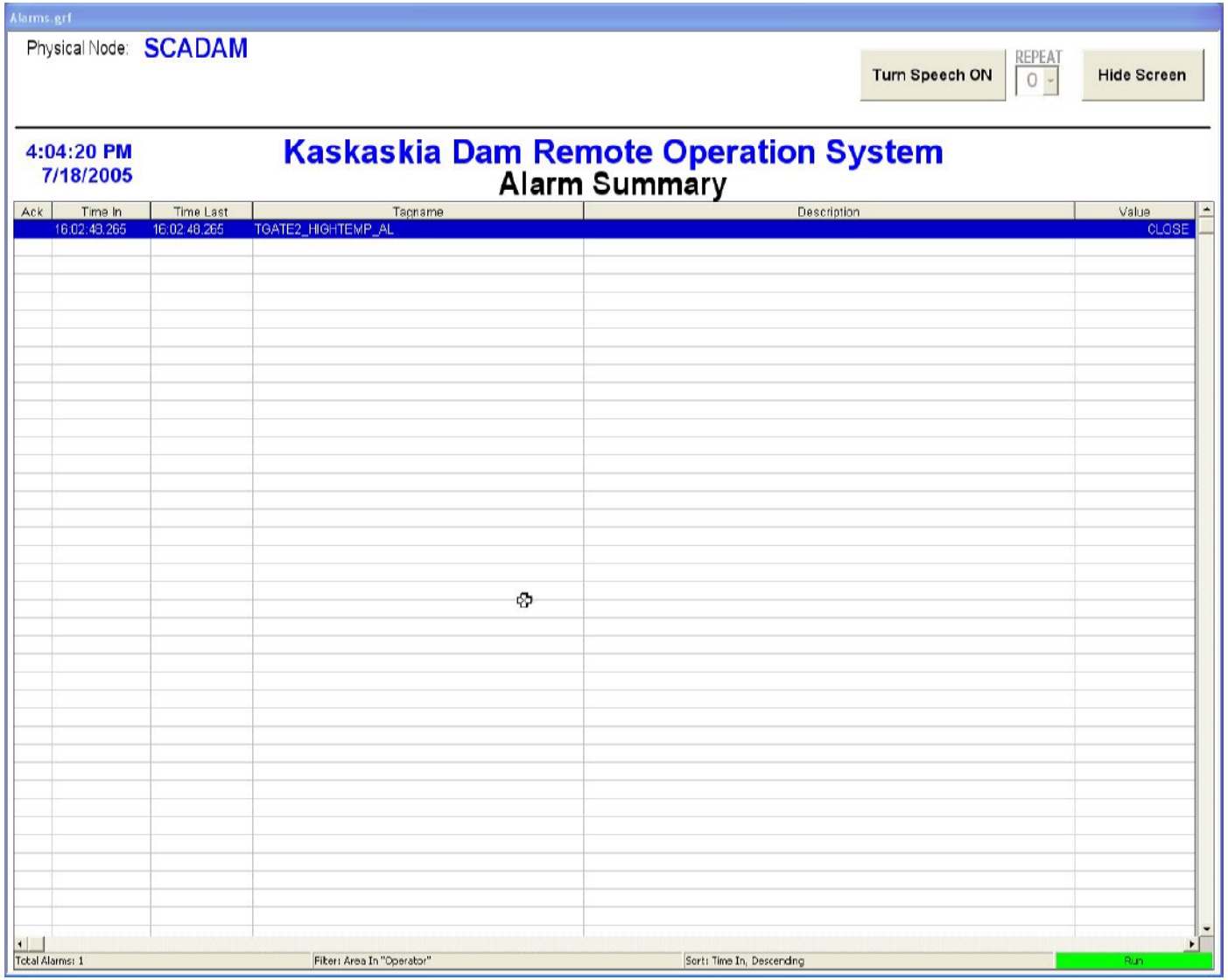


Remote

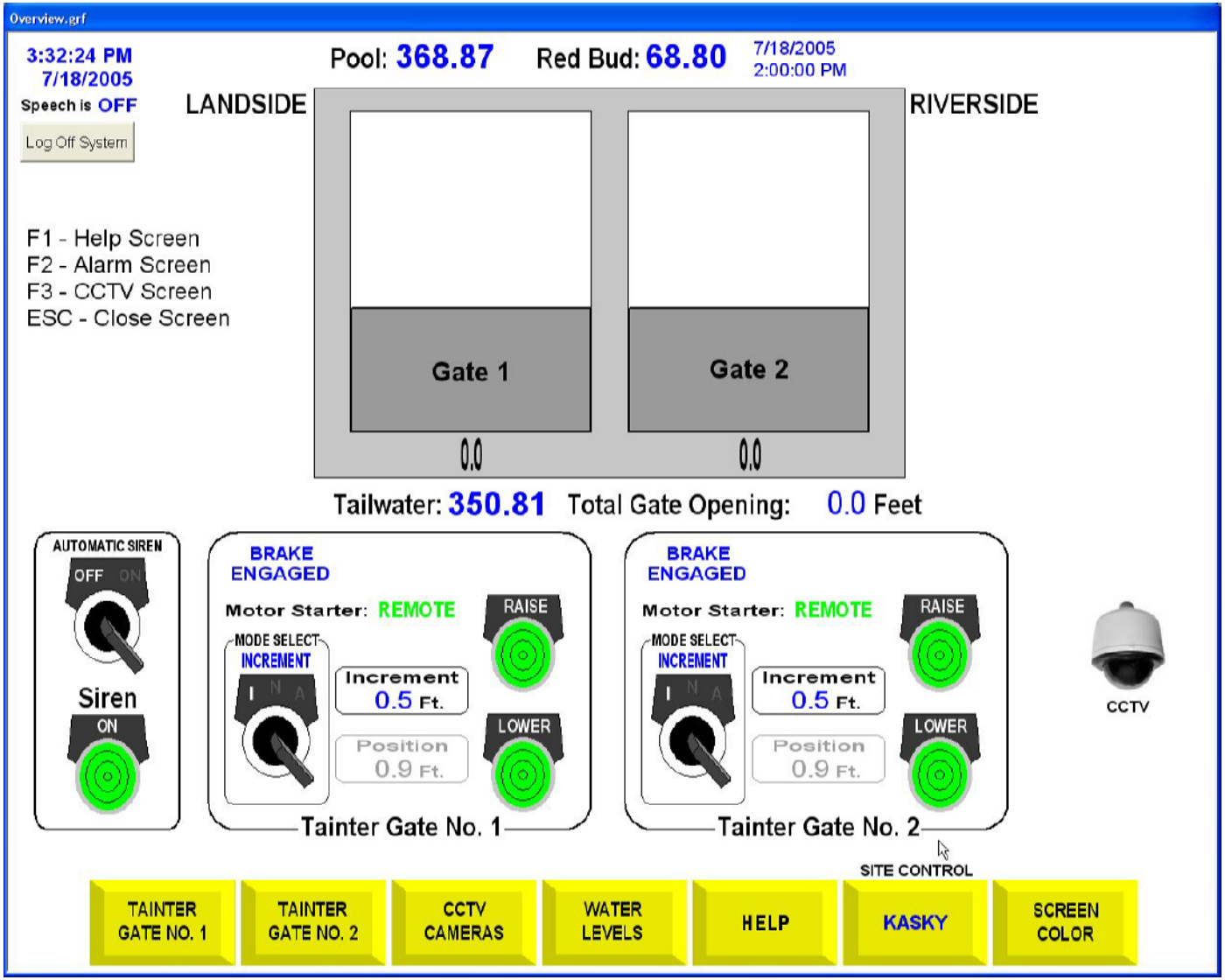


- iFIX by GE Fanuc
- A single application is used between both the local and remote locations
- Each location is stand alone (SCADA node) communicating to each PLC
- Both locations cannot control the dam at the same time. This is controlled by the local site

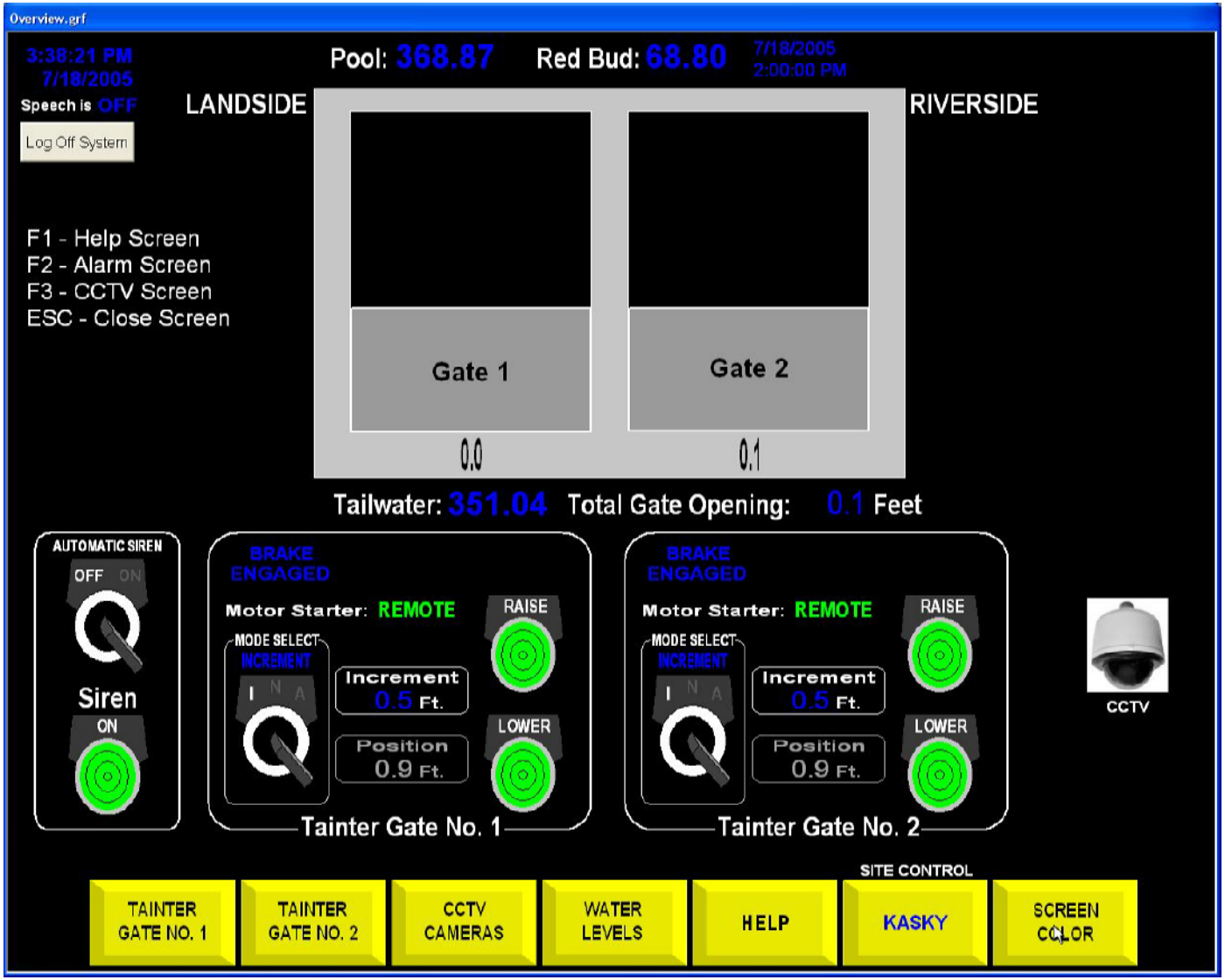
Human Machine Interface



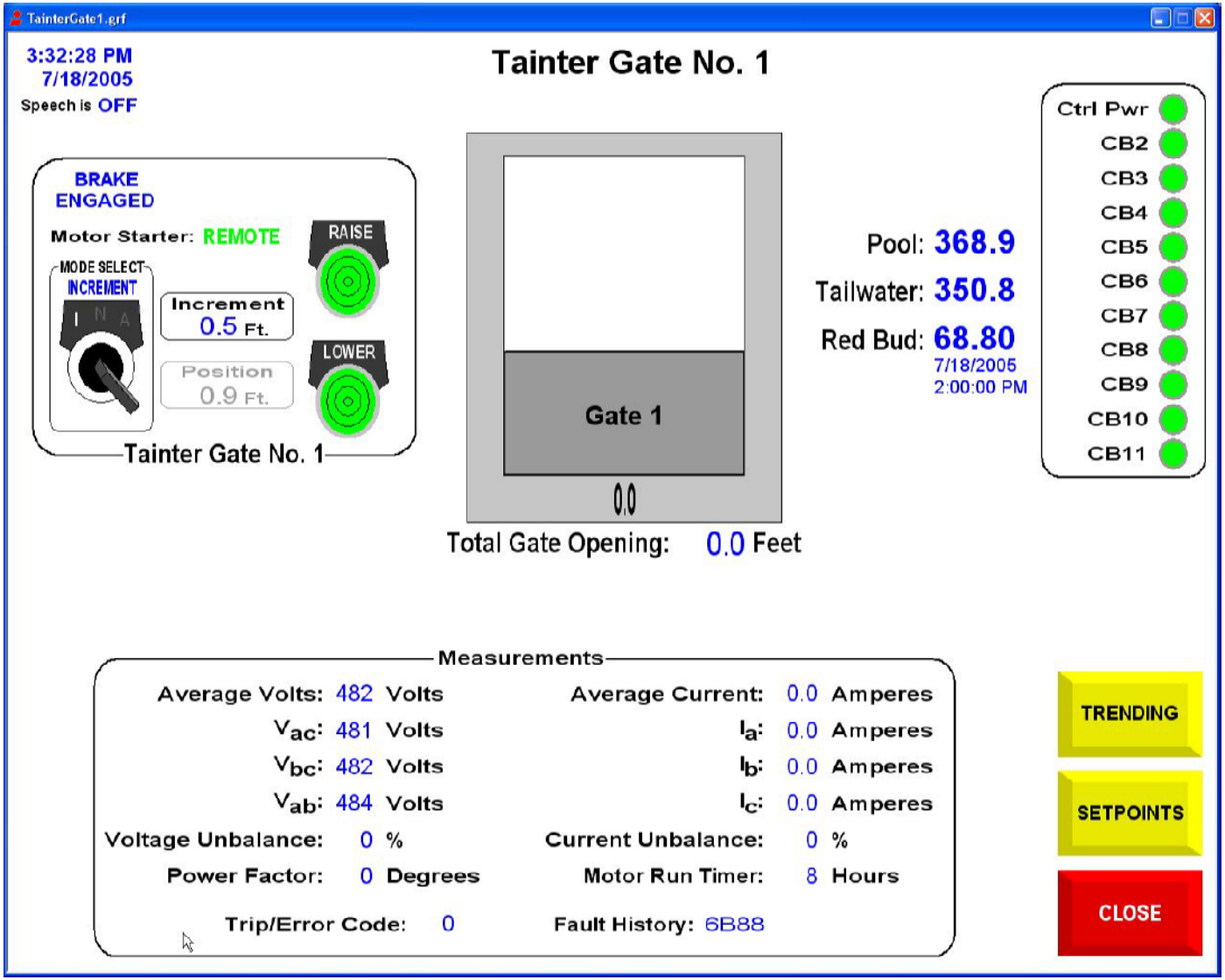
Human Machine Interface



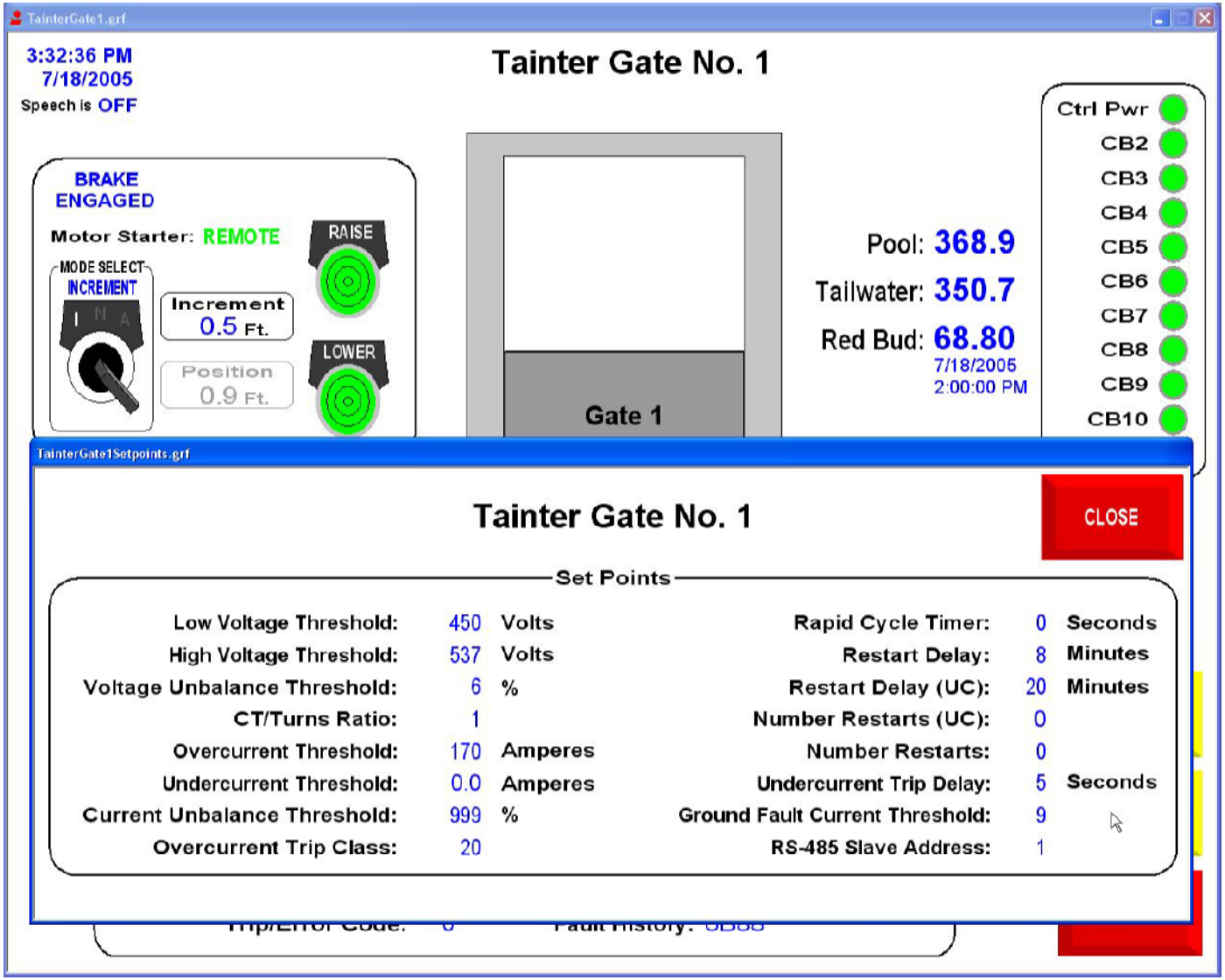
Human Machine Interface



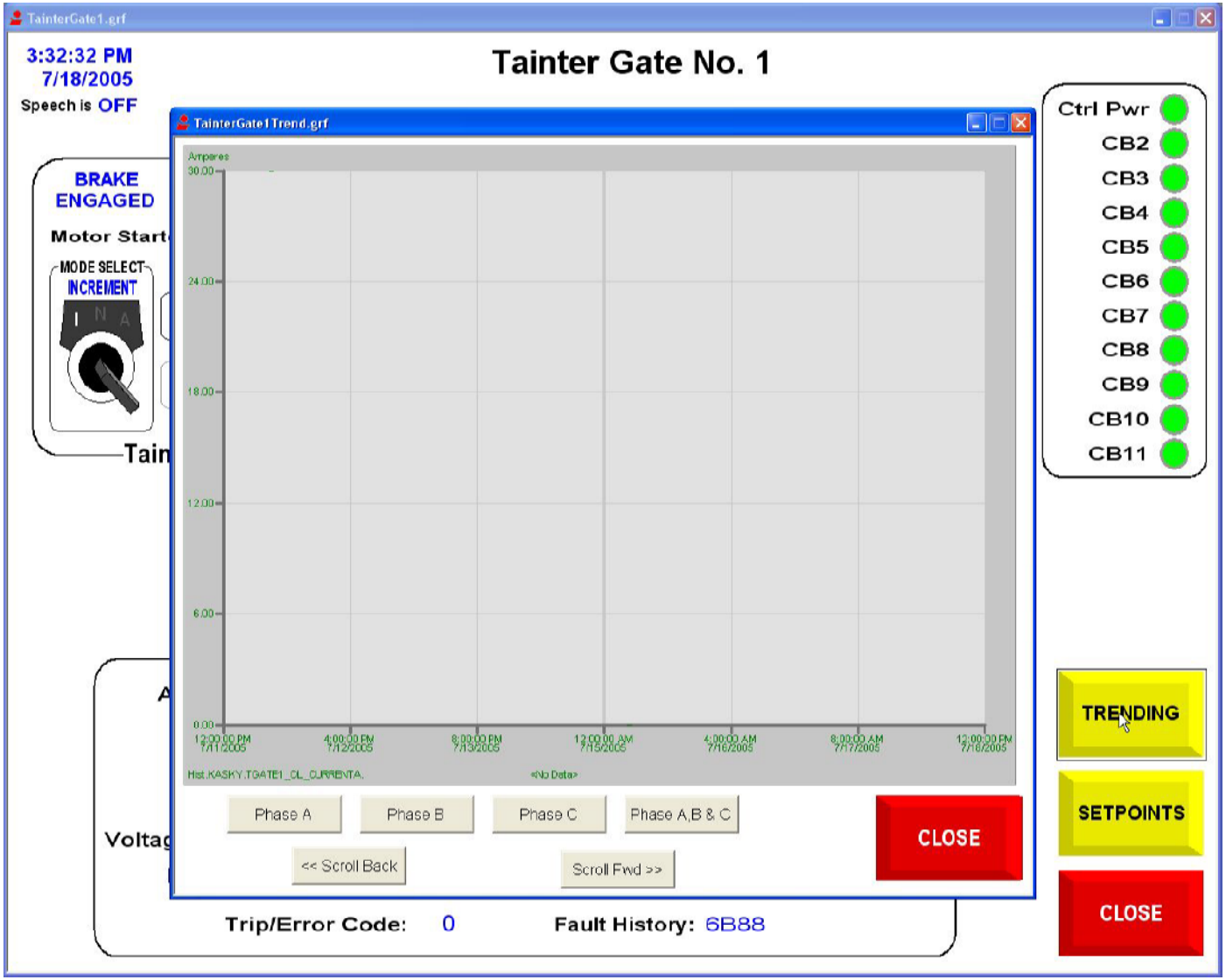
Human Machine Interface



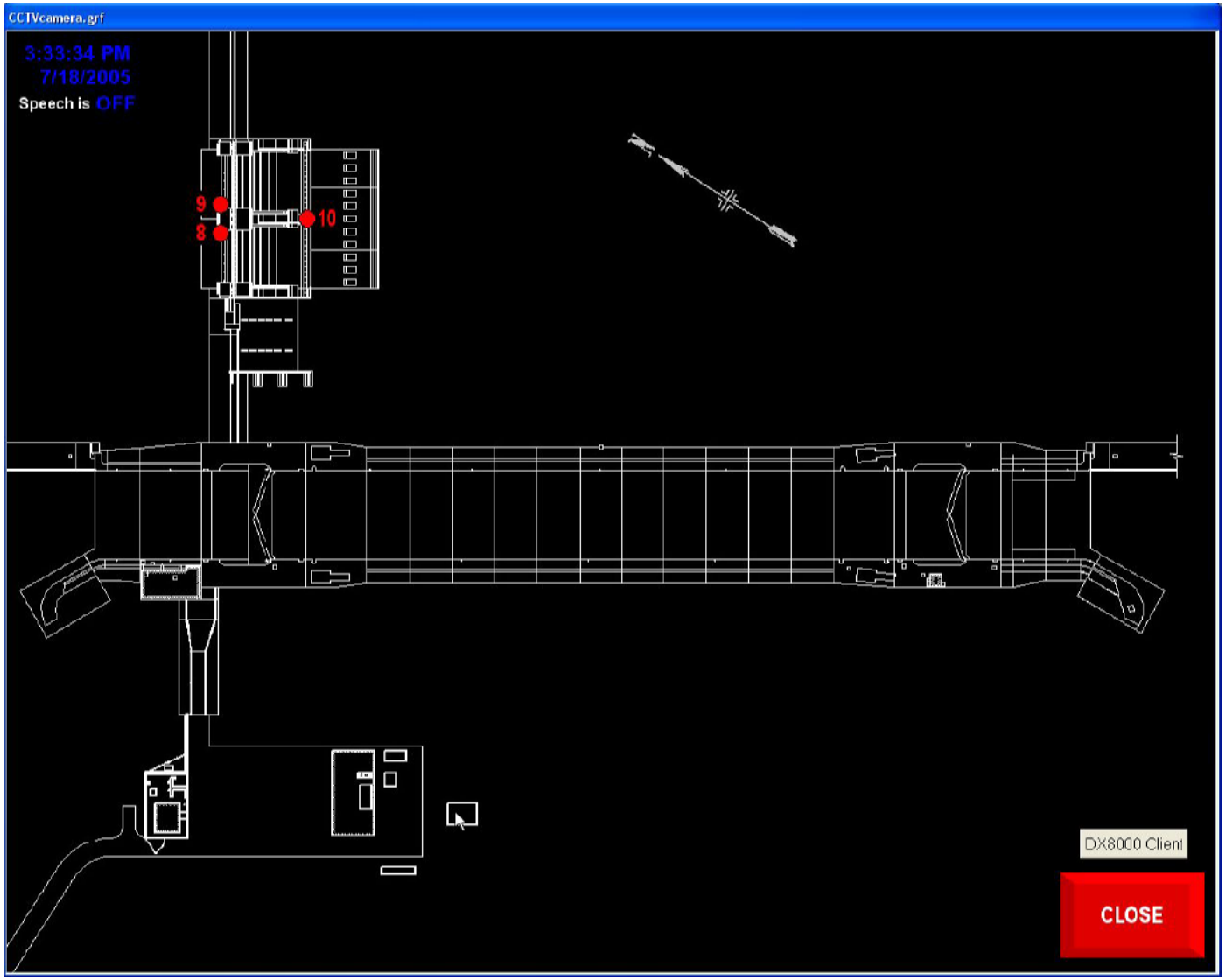
Human Machine Interface



Human Machine Interface

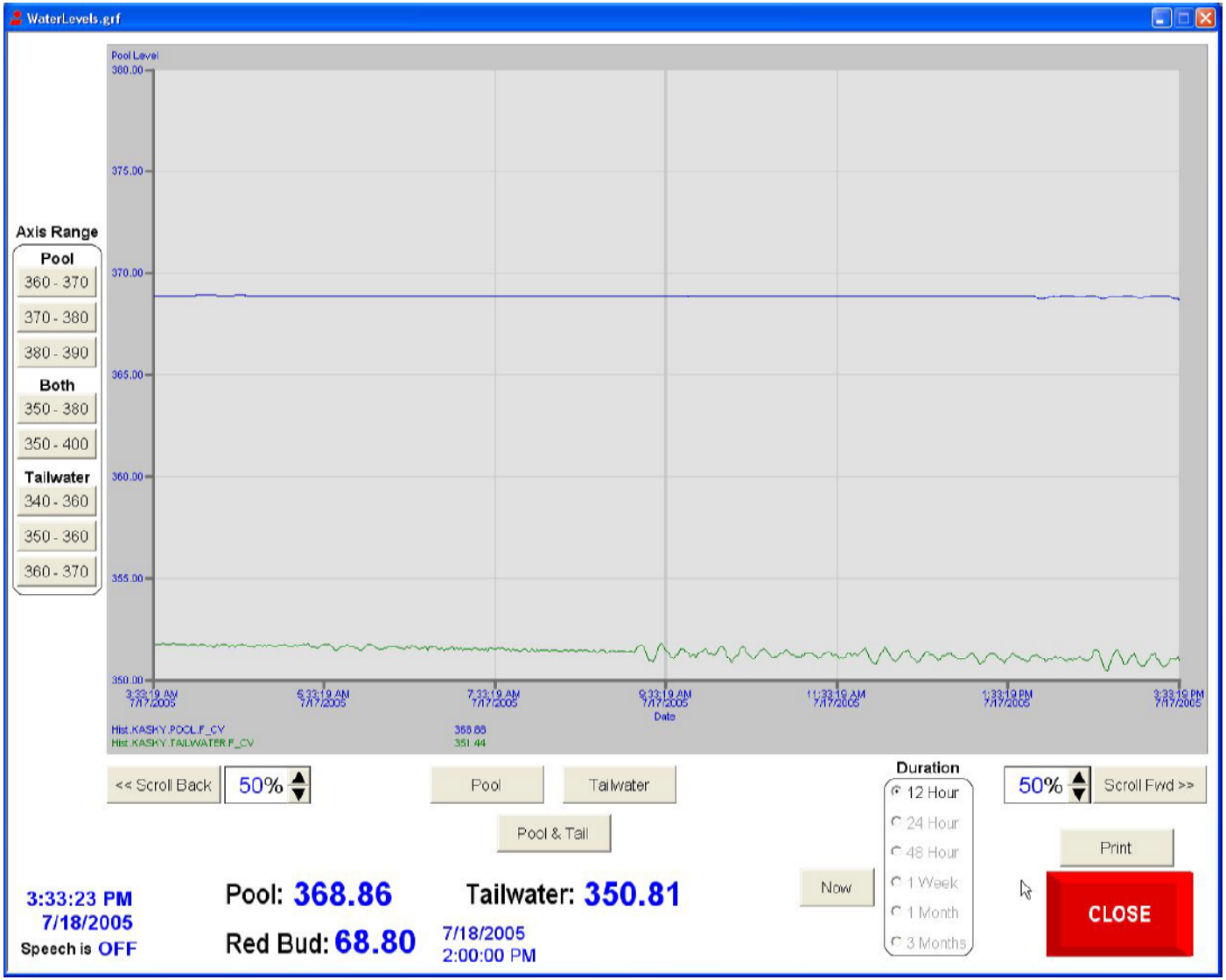


Human Machine Interface

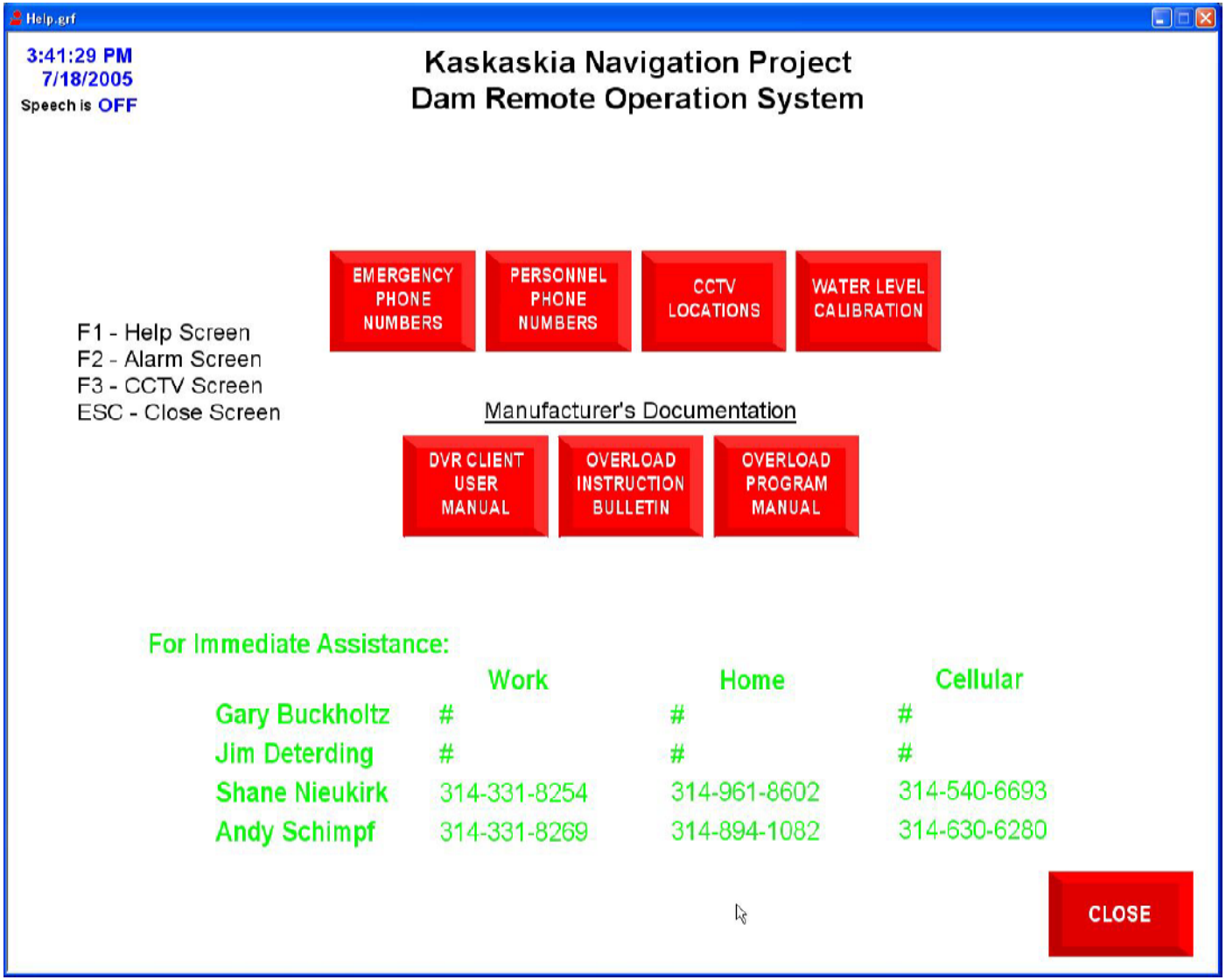


Human Machine Interface

Human Machine Interface

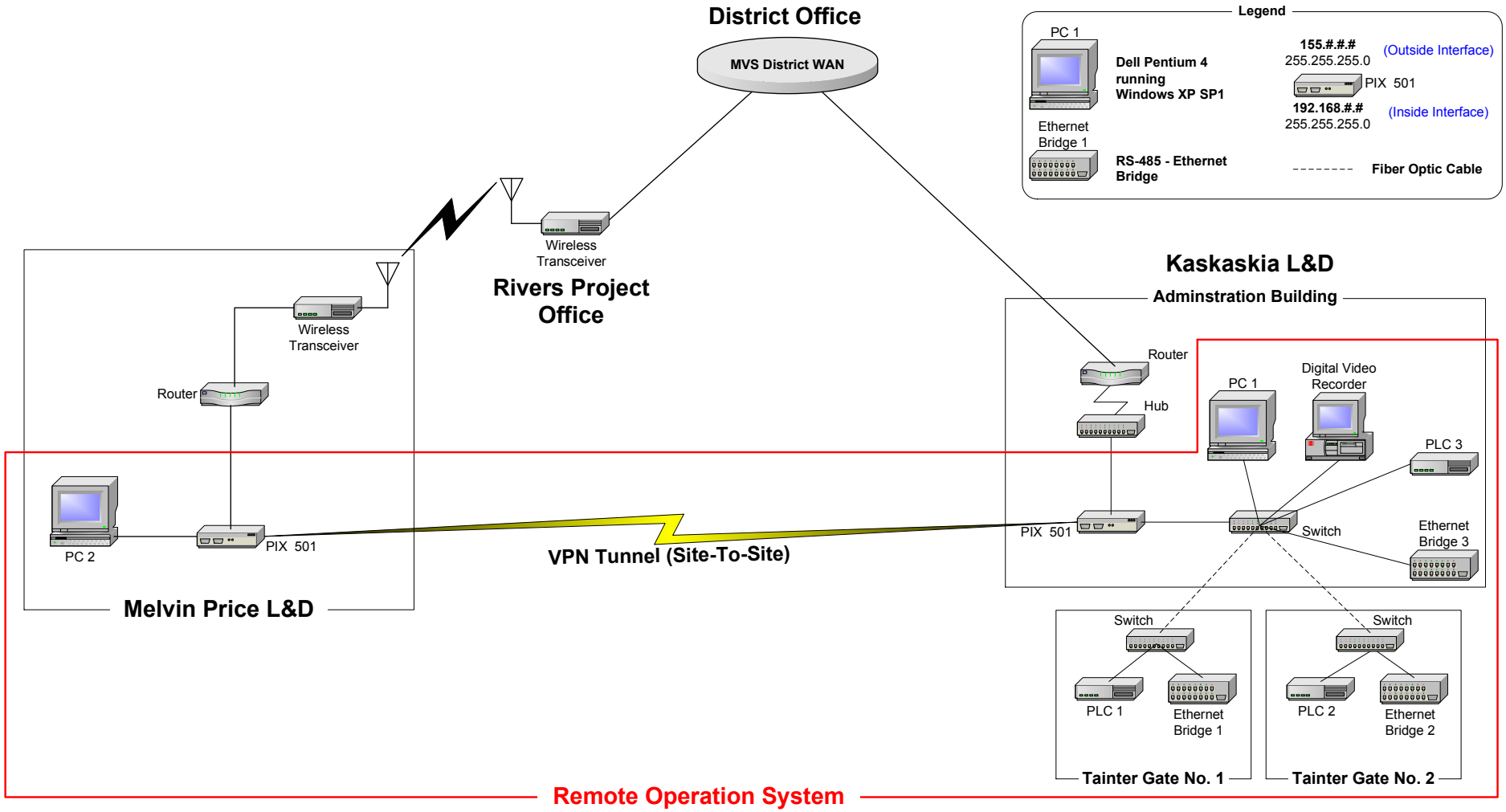


Human Machine Interface



US Army Corps of Engineers®
Mississippi Valley Division
Mississippi River Commission

Network Diagram



System Description & Functionality

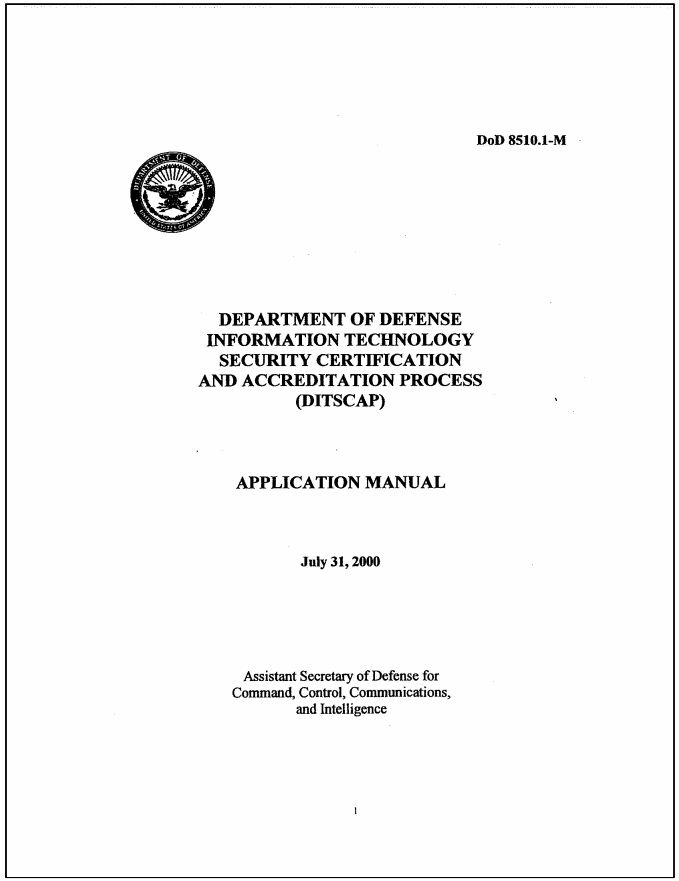
- Operators login using local user accounts
- Passwords are updated manually. Distributed using encrypted email with CAC
- Patches and updates to be installed manually using PCAnywhere
- Access to VPN firewall using local user accounts (including extended authentication)

HQ Guidance for SCADA Systems

- No formal guidance concerning the connection of SCADA systems to the network exists
- As a result of a briefing given to HQ's Information Assurance Section, informal guidelines were developed
- Questions concerning the guidelines resulted in a "cease and desist" order for the Information Assurance Program Manager
- HQ directed the St. Louis District to certify and accreditate the Remote Operation System using DITSCAP prior to placing it online

DoD Information Technology Certification and Accreditation Process (DITSCAP)

- DITSCAP is defined by DoD Instruction 5200.40
- Developed to meet the requirements of DoD Directive 5200.28. This includes:
  - Stand-alone PCs
  - Connected Systems
  - Networks
- Instructions for the process are provided in DoD Manual 8510.1-M



DoD 8510.1-M

DEPARTMENT OF DEFENSE
INFORMATION TECHNOLOGY
SECURITY CERTIFICATION
AND ACCREDITATION PROCESS
(DITSCAP)

APPLICATION MANUAL

July 31, 2000

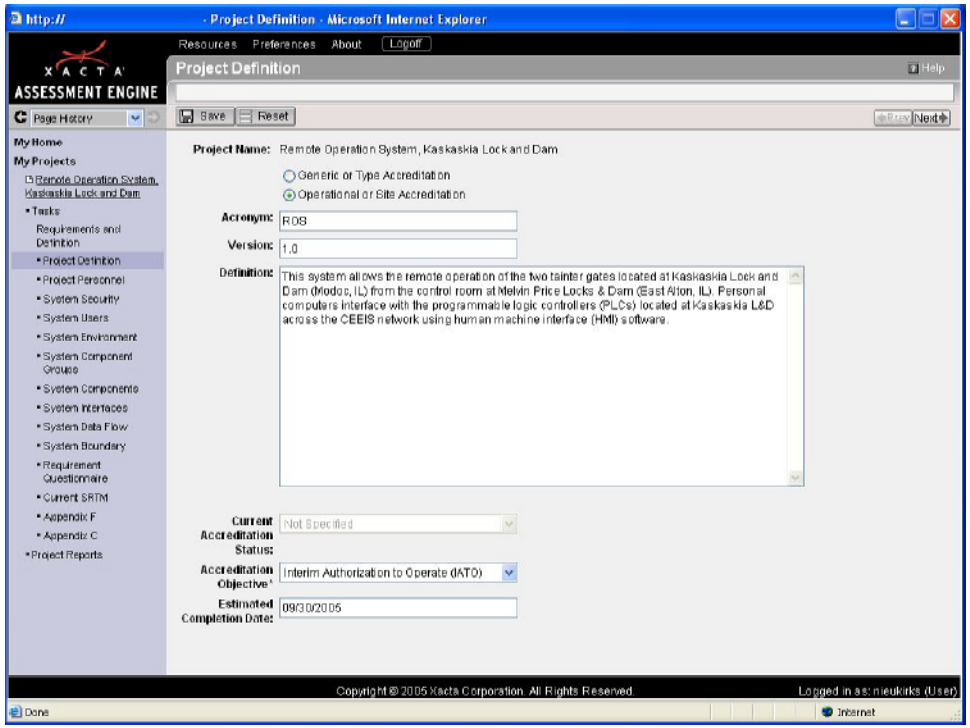
Assistant Secretary of Defense for
Command, Control, Communications,
and Intelligence

DoD Information Technology Certification and Accreditation Process (DITSCAP)

- DITSCAP uses a single document approach collecting all of the information into the Systems Security Authorization Agreement (SSAA).
- The SSAA is a formal agreement among the Designated Approval Authority (DAA), Certifying Authority (CA), Program Manager, and User Representatives.
- To aid in the development of the SSAA, HQ has directed that all new DITSCAPs use the Xacta tool.
- Xacta is a web-based application that assures SSAA consistency across USACE.

Xacta Information Assurance Manager

- Accessed using Internet Explorer
- The tool is administrated by Mr. William Barnett of HQ (contractor)
- Access is granted after completing a user request form
- To access the tool, all pop-up blockers and outside toolbars (Google) must be turned off



Systems Security Authorization Agreement

- **Characteristics of the SSAA:**
  - Describes operating environments and threats
  - Describes the system security architecture
  - Identifies required hardware, firmware, software, etc.
  - Establishes the C&A boundary
  - Documents all requirements necessary for accreditation
  - Documents the DITSCAP plan including test plans and procedures, certification results, and residual risk
  - Forms the baseline security configuration document
- **DITSCAP includes four phases**
- **Each phase is comprised of "activities" which are broken down further into "tasks"**

DoD Information Technology Certification and Accreditation Process (DITSCAP)

- **DITSCAP Phases:**
  - **Phase 1, Definition**
    - **Verify system mission, environment, and architecture. Identify threats. Define level of effort and team members.**
  - **Phase 2, Verification**
    - **Document compliance of system with security requirements.**
  - **Phase 3, Validation**
    - **Assure system environment and configuration provides acceptable level of risk.**
  - **Phase 4, Post Accreditation**
    - **Monitor systems management, configuration, and changes to the operational and threat environment to assure acceptable level of risk is preserved.**

DITSCAP – Phase 1, Definition

- **Activities**
  - **Preparation, Registration, and Negotiation**
- **Tasks (12)**
  1. **Review Documentation**
  2. **Prepare the System and Functional Description, System Identification**
  3. **Register the System (Define the C&A Team)**
     - **Designated Approval Authority (DAA) has final approval of the SSAA. The DAA is often the District Engineer**
     - **Certifying Authority (CA) identifies security requirements**
     - **Information Security Systems Officer (ISSO) insures system is accurately documented**
     - **Program Manager defines the system and security architecture and supports DITSCAP tailoring**

DITSCAP – Phase 1, Definition

- **Tasks (12)**
  4. Prepare Environment and Threat Description
  5. Determine System Security Requirements
  6. Prepare System Architecture Description (hardware, software…)
  7. Identify the C&A Organizations and Resources Req'd
  8. Tailor DITSCAP and Prepare Plan (Certification Level)
  9. Draft the SSAA
  10. Conduct Certification Requirements Review
  11. Establish Agreement on Level of Effort and Schedule
  12. Approve Phase 1 SSAA

DITSCAP – Phase 1, Definition

- **Roles**
  - **DAA – Continuously review the system for compliance with the SSAA.**
  - **CA & Certification Team**
    - **Support the DAA**
    - **Review threat description**
    - **Identify security requirements**
  - **PM**
    - **Initiate dialogue with the DAA, Certifier, and User Rep.**
    - **Define system schedule & budget**
    - **Define system & security architecture**
  - **User Representative – defines requirements of the system and end users**
  - **All support DITSCAP tailoring and Certification Level**

DITSCAP – Phase 2, Verification

- **Activities**
  - **SSAA Refinement, System Development and Integration, Initial Certification Analysis, Assess Analysis Results**
- **Tasks (7)**
  1. **System Architecture Analysis**
  2. **Software, Hardware, and Firmware Analysis**
  3. **Network Connection Rule Compliance Analysis**
  4. **Integrity Analysis of Integrated Products**
  5. **Life-Cycle Management Analysis**
  6. **Security Requirements Validation Procedures**
  7. **Vulnerability Assessment**

DITSCAP – Phase 2, Verification

- **Roles**
  - **DAA – Continuously review the system for compliance with the SSAA.**
  - **CA & Certification Team**
    - **Conduct Phase 2 certification analysis tasks**
    - **Identify and assess system vulnerabilities**
    - **Report certification results to the DAA & PM**
    - **Integrate changes into the SSAA**
  - **PM**
    - **Develop system or system modifications**
    - **Support certification efforts**
    - **Modify system to reduce or eliminate vulnerabilities.**

DITSCAP – Phase 3, Validation

- **Activities**
  - **SSAA Refinement, Certification Evaluation of the Integrated System, Recommendation to DAA, DAA Accreditation Decision**
- **Tasks (8)**
  1. **Security Test and Evaluation**
  2. **Penetration Testing**
  3. **TEMPEST and RED-BLACK Evaluation**
  4. **COMSEC Compliance Evaluation**
  5. **System Management Analysis**
  6. **Site Accreditation Survey**
  7. **Contingency Plan Evaluation**
  8. **Risk Management Review**

DITSCAP – Phase 3, Validation

- **Roles**
  - **DAA**
    - **Continuously review the system for compliance with the SSAA**
    - **Determine if security safeguards and residual risks are acceptable**
    - **Sign the accreditation document**
  - **CA & Certification Team**
    - **Complete Phase 3 certification analysis tasks**
    - **Identify and assess system vulnerabilities**
    - **Recommend risk mitigation measures**
    - **Report certification results to the DAA & PM**
    - **Prepare final SSAA & recommendation**

DITSCAP – Phase 4, Post Accreditation

- **Activities**
  - System and Security Operation, Compliance Validation
- **Tasks (8)**
  1. SSAA Maintenance
  2. Physical, Personnel, and Management Control Review
  3. TEMPEST Evaluation
  4. COMSEC Compliance Evaluation
  5. Contingency Plan Maintenance
  6. Configuration Management
  7. Risk Management Review
  8. Compliance Validation

DITSCAP – Phase 4, Post Accreditation

- **Roles**
  - **DAA**
    - **Decide to re-accreditate, IATO, or terminate**
  - **CA & Certification Team**
    - **Normally not involved, support DAA, ISSO, and system operators**
  - **PM**
    - **Cost/Schedule**
    - **System Documentation**
  - **User Representative**
    - **Oversee system operation**
    - **Report vulnerability/security incidents**
    - **Initiate SSAA review for change in threat or system configuration**

DITSCAP – Phase 4, Post Accreditation

- **Roles**
  - **ISSO**
    - **Periodically review mission statement, operating environment, and security architecture to insure compliance with SSAA**
    - **Maintain integrity of the site environment and accredited security posture**
    - **Ensure that configuration management adheres to security policy and requirements**
    - **Initiate C&A process when reaccredidation is required**

Summary

- The system design is the easy part
- All systems are required to be accredited using DITSCAP
- DITSCAP is a long process and should not be taken lightly
- Plan adequate funding for DITSCAP

Shane M. Nieukirk, P.E.
US Army Corps of Engineers, St. Louis District
Ph: 314-331-8254 Cl: 314-540-6693
shane.m.nieukirk@mvs02.usace.army.mil