Issues of Access Control for Ancillary Equipment

Rodney R. Porter

Argonne National Laboratory
Intense Pulsed Neutron Source

Once security procedures and safety systems have been implemented, one is still left with the question, "Who should be able to do what, when?" This becomes even more important with the increased access allowed by the World Wide Web. Traditional answers include trusting the user, "hiding" advanced features, and only supporting those commands that everyone needs. Permission-based solutions allow for greater flexibility, but with a substantial increase in time needed for configuration and management. I will examine the benefits and problems with these differing solutions as IPNS looks to find answers to allow us to move forward and better serve our user community.

Introduction:

Background

Traditional Solutions

1. Trusting the User
2. Hiding Advanced Features
3. Supporting a Limited Set of Commands

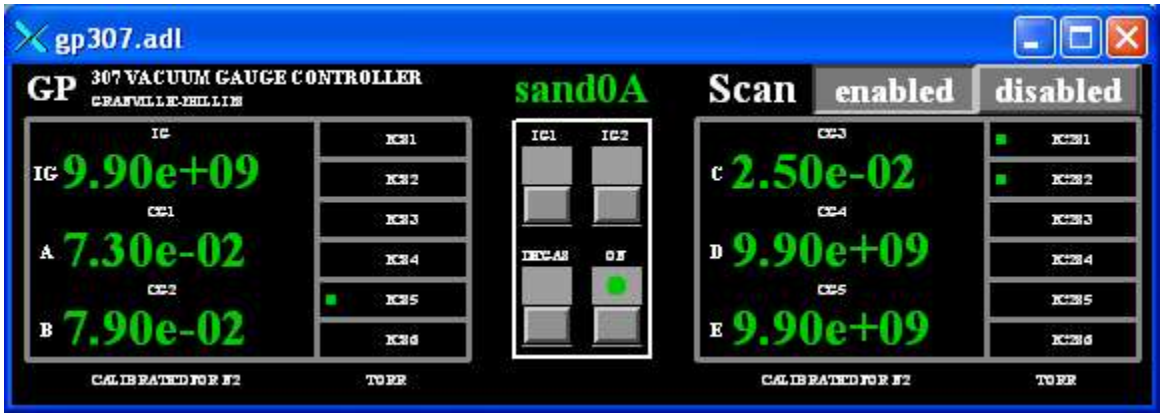
Permission-Based Solutions

1. Individual Accounts
2. Enable/Disable Access

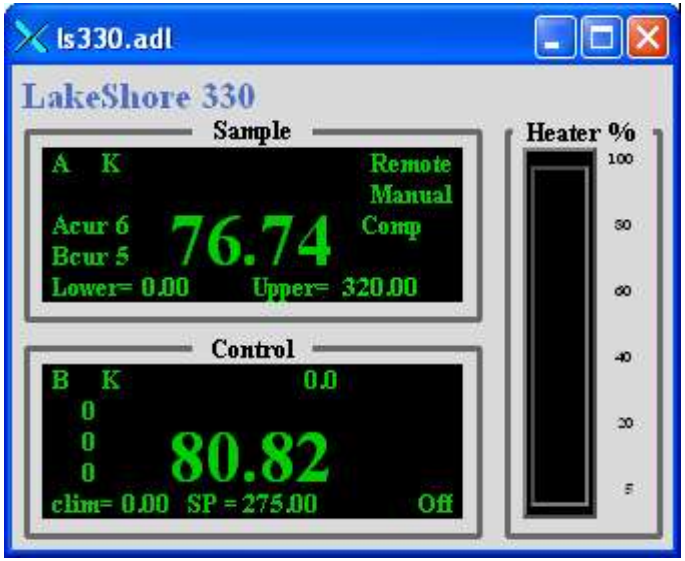
Combined Solutions

Conclusions

Background: What is Ancillary Equipment?



- Vacuum
- Sample Environment
- Beam Conditioning
- Motors



- Equipment that Controls or Monitors the Condition of the Experiment

Background: The Problem

- **Changes in the set-up of equipment that adversely affect the quality or quantity of data**
  - Longer times between runs
  - Increased work load for support staff
  - No data
  - Bad data
- **This is not a new problem!**

Solutions:

Traditional Solutions: Solutions in this category are traditional because they have been proven to work, at least in some cases, and are a part of almost any solution.

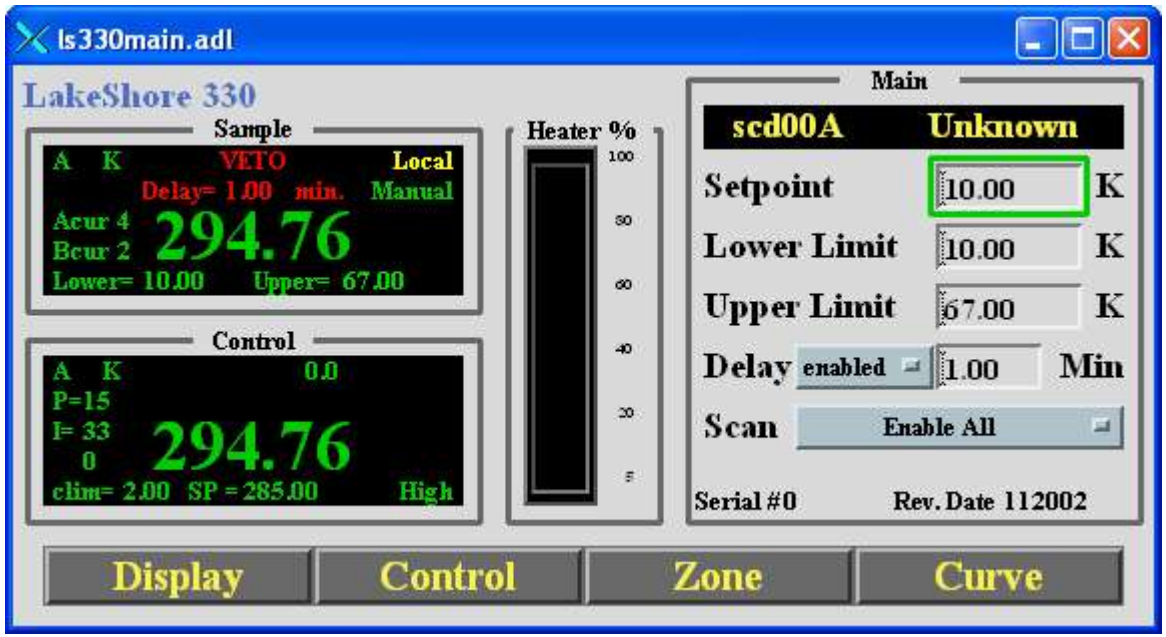
1. Trust the User
2. Hide Advanced Features
3. Support a Limited Set of Commands

Permission-Based Solutions: Solutions in this category use some form of authentication to determine who has access to individual features.

1. Individual Accounts
2. Enable/Disable Access

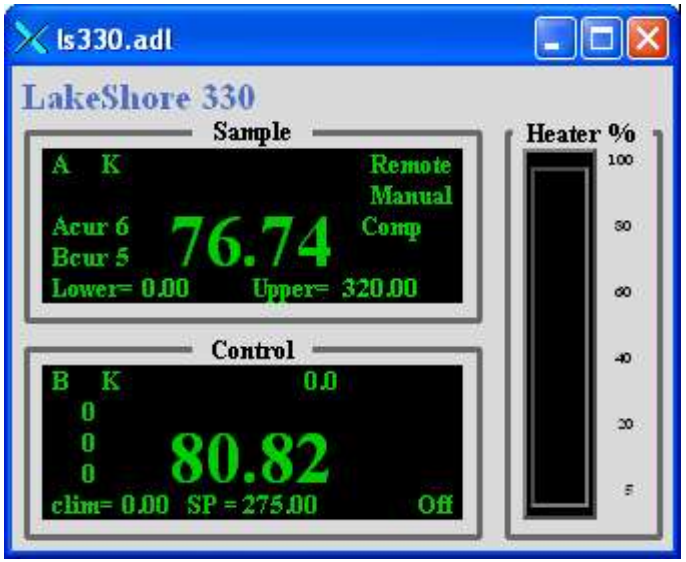
Traditional Solutions: Trust the User

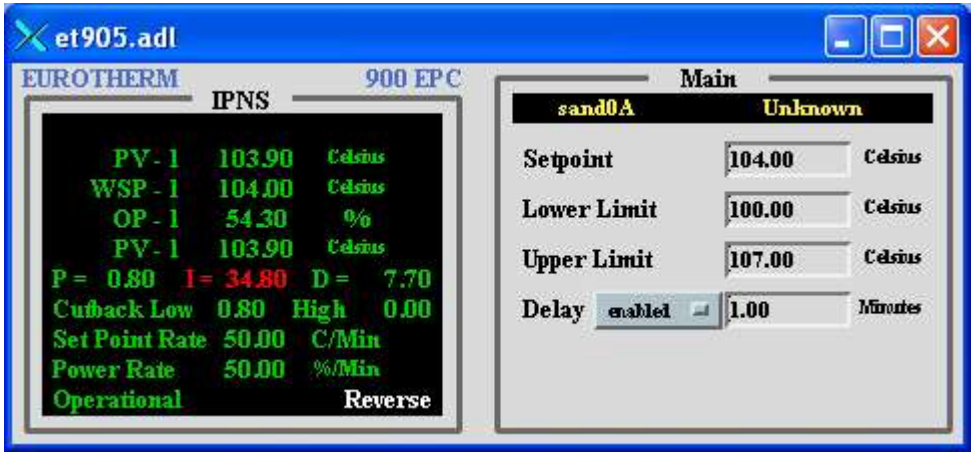
- **Benefits:**
  - Simple
  - Known Implementation
  - Proven Track Record
- **Problems:**
  - Operator Error
  - "I can fix this."
- **Examples:**
  - Instrument Training
  - LakeShore 330 Front Panel not locked out
  - Do not use these commands
  - Confirmation Window



Traditional Solutions: Hide Advanced Features

- **Benefits:**
  - Reduces Operator Error
- **Problems:**
  - Advanced Features not Readily Available
  - People Learn Where Features are Hidden





Traditional Solutions: Support a Limited Set of Commands

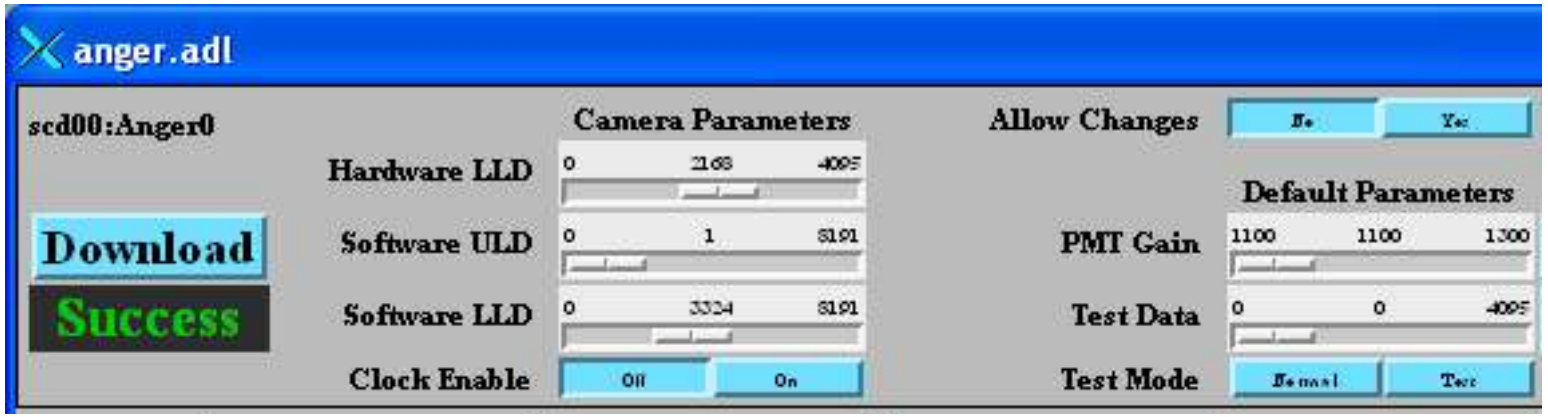
- **Benefits:**
  - Simple
  - Reduces Development Effort
- **Problems:**
  - Increased Operations Effort
  - Configurations Not Available for Control or Monitoring

Permission-Based Solutions: Individual Accounts

- **Benefits:**
  - Follows Security Implementation
  - Extremely Flexible
- **Problems:**
  - Increased development effort to automate as much as possible
  - Increased management effort to route appropriate information
  - Increased operations effort to set up individual permissions
- **Compromise:**
  - One user account with changing password

Permission-Based Solutions: Enable/Disable Access

- **Benefits:**
  - Prevents Operator Error
  - Limits Access to Advanced Features
  - The Ability to Enable/Disable Access Can Be Disabled
- **Problems:**
  - Increased development effort
  - Access can be left enabled



Combined Solution:

- **Trust The User**

  The user is trained to run the experiment, and to call the support staff if there is a problem. Confirmation windows are used for changes in parameters that would veto data.

- **Hide Advanced Features**

  Advanced features are located on related screens, available, but not normally visible. Disabled features are not visible or available.

- **Only Support Needed Commands**

  Only commands for operation and set-up are supported.

- **Access Based on Account/Computer**

  Access is limited to the instrument and user computer, with account access limited by level of knowledge/training/responsibility. The instrument account on the instrument computer has full access, with the instrument account on the user computer having only limited access.

- **Access Enabled/Disabled By Some Accounts/Computers**

  Advanced features are enabled on the instrument account on the instrument computer and can be enabled by accounts with appropriate access.

Conclusions:

- The user must be trusted to the extent of their training
- Advanced features should be hidden
- Only necessary commands should be supported
- Access should be based on account and computer
- The Instrument Responsible should be able to enable or disable access for users