Managing Proficy iFix SCADA Nodes and iClient in Technical Division at Fermilab

What is iFix:

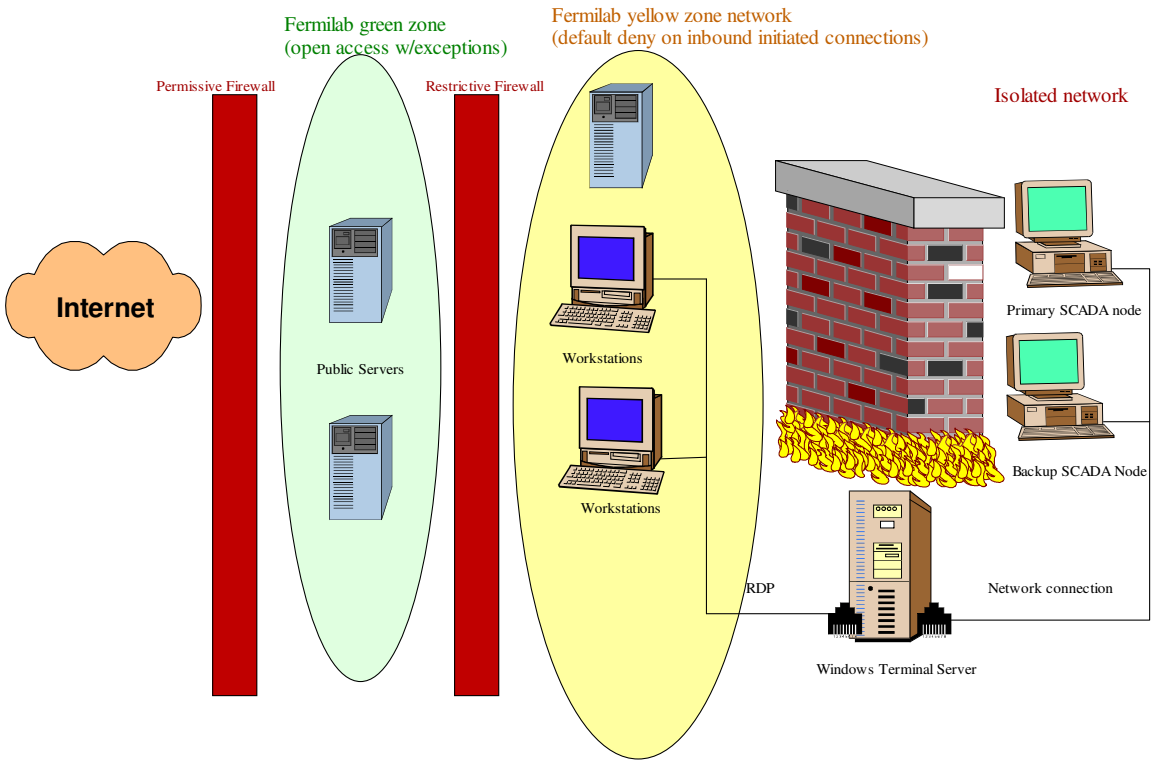
Proficy HMI/SCADA – iFIX from GE Fanuc Intelligent Platforms is a wild used supervisory monitoring and control software. It provides real time information management and SCADA solution that is open, flexible and scalable. It includes visualizations, control engine, a powerful built in historian.

Topics:

1. Network Configuration for iFix SCADAs and Windows Terminal Server
2. Remote Access/Control using MS Terminal Server and iFix iClient
3. Implement iFix security & Windows File Protection
4. Console logon with domain captive accounts (and lock out policy)
5. Patching and Anti-virus mechanisms
6. Fault tolerance
7. Disaster recovery

1. Network configuration for iFix SCADAs and Windows Terminal Server -1

Network Architecture:



1. Network configuration for iFix SCADAs and Windows Terminal Server-2

CISCO ASA Firewall separates TD DAQ/refrigerator network from Fermi public network. There are firewall rules to allow Fermilab's DNS, WINS, WSUS, Symantec Anti-Virus, and SMS Servers. All SCADA nodes are in a private network. The Windows Terminal Server has dual network cards*: one connects to the yellow zone of Fermilab public network (default deny on inbound initiated connections), the other connects to the isolated private network. Users run iFix from workstations in the yellow zone through an RDP session on the terminal server.

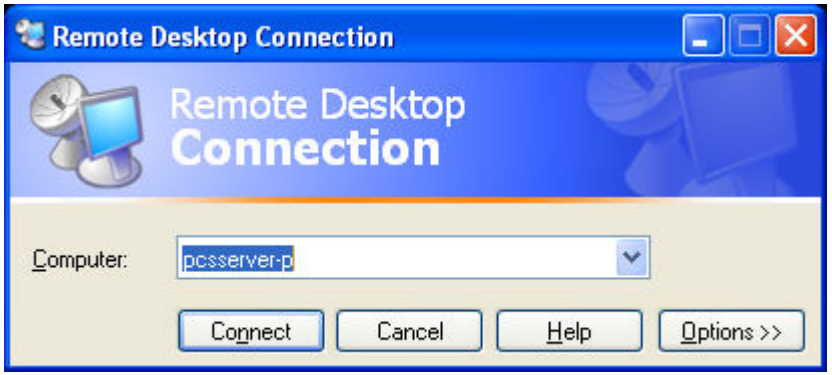
*This system does not route between these networks.

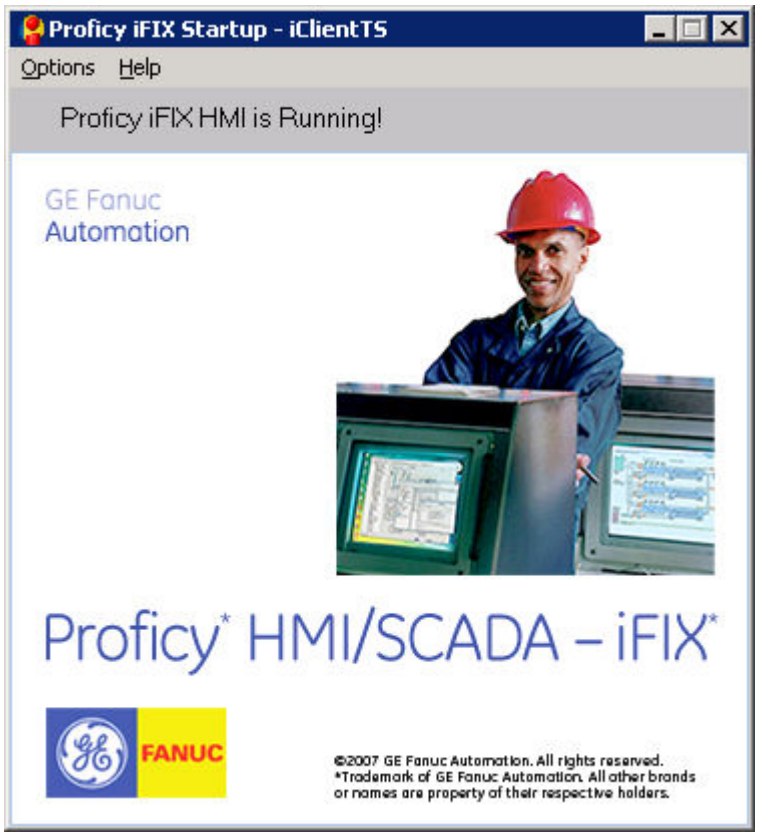
2. Remote Access/Control using MS Terminal Server and iFix iClient -1

Using Terminal Services with iFix provides:

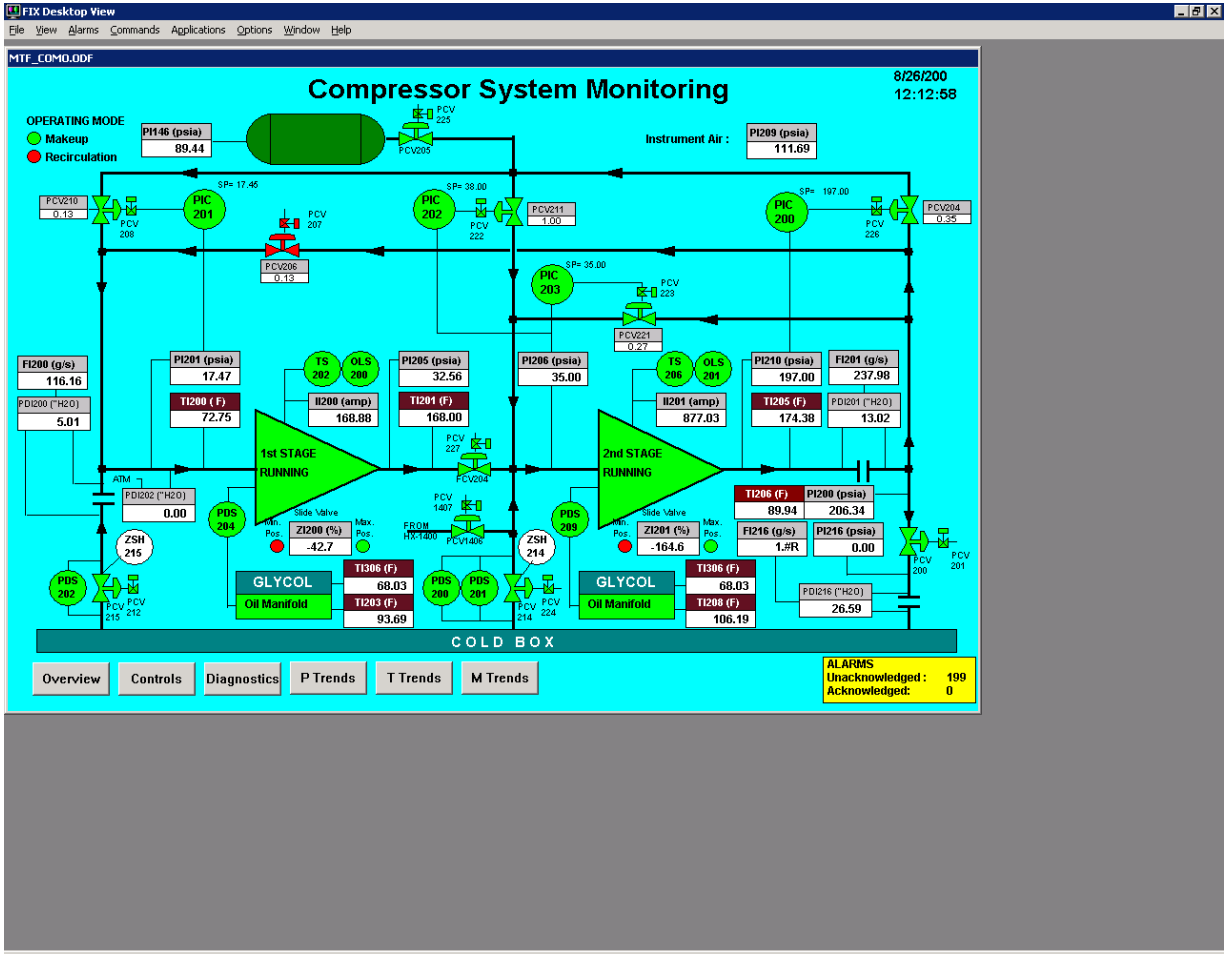
- Ease of maintenance: You can install one copy of iFix onto the server, allowing multiple users to run clients from the server (licenses are much cheaper).
- Share pictures and historical data: Each user accesses the same set of pictures and historical data.
- Remote access: From client, users can RDP to the server to run iFix.
- Security: Data between the iFix Terminal Server and client session is encrypted.
- Meanwhile by using host base firewall or third party firewall on the server, the RDP port, Windows file and printing sharing and iFix program can be only accessed from certain IP addresses.
- Specialized environments: Terminal Services allows you to tightly control user accounts. Users can be limited to run iFix only after he logs in. When he exits iFix, he logs off windows too. He does not have access to Windows desktop.

2. Remote Access/Control using MS Terminal Server and iFix iClient -2





2. Remote Access/Control using MS Terminal Server and iFix iClient -3



3. Implement iFix security & Windows File Protection -1

We categorized our users into three groups: developers, operators and viewers.

Controlled access to files: Each user is configured to run iFix iClient in his own environment.

Developers have their unique directories except for NLS(language support) and Base path. Developers can design and test pictures, dynamo sets and Global color tables in their own directories before they deploy them. They have Write permission to the common picture folder.

Operators and views can have their own user preference files saved in their own profile. They have permission read only permission to the shared folders.

3. Implement iFix security & Windows File Protection -2

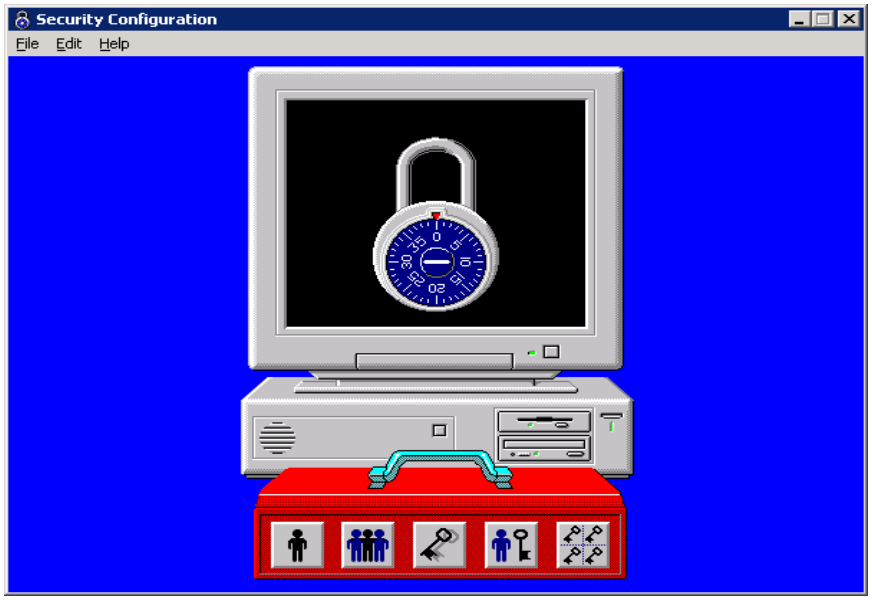
- ├──ALM
- ├──APP
- ├──Config Files Backup
- ├──DEVKTDOC
- ├──HELP
- ├──HTR
- ├──HTRDATA
- │ ├──SCADA00
- ├──LOCAL
- ├──LOGON
- ├──MANAGER
- ├──NLS
- ├──PDB
- ├──PIC (common folder)
- ├──PROJECTS
- │ ├──DEV
- │ │ ├──huangy
- │ │ │ ├──ALM
- │ │ │ ├──APP
- │ │ │ │ └──CustomUserDir
- │ │ │ ├──HTR
- │ │ │ ├──HTRDATA
- │ │ │ ├──LOCAL
- │ │ │ ├──PDB
- │ │ │ ├──PIC
- │ │ │ ├──RCC
- │ │ │ └──RCM
- │ │ ├──OPS
- │ │ │ ├──rsward
- │ │ │ │ ├──ALM
- │ │ │ │ ├──HTR
- │ │ │ │ └──LOCAL
- │ │ └──viewers
- │ │ └──hess
- │ │ ├──ALM
- │ │ ├──HTR
- │ │ └──LOCAL
- ├──RCC
- ├──RCM
- ├──Resources
- ├──SIMS
- ├──SOUNDS
- └──XLSTART

3. Implement iFix security & Windows File Protection -3

Implement iFix application security:

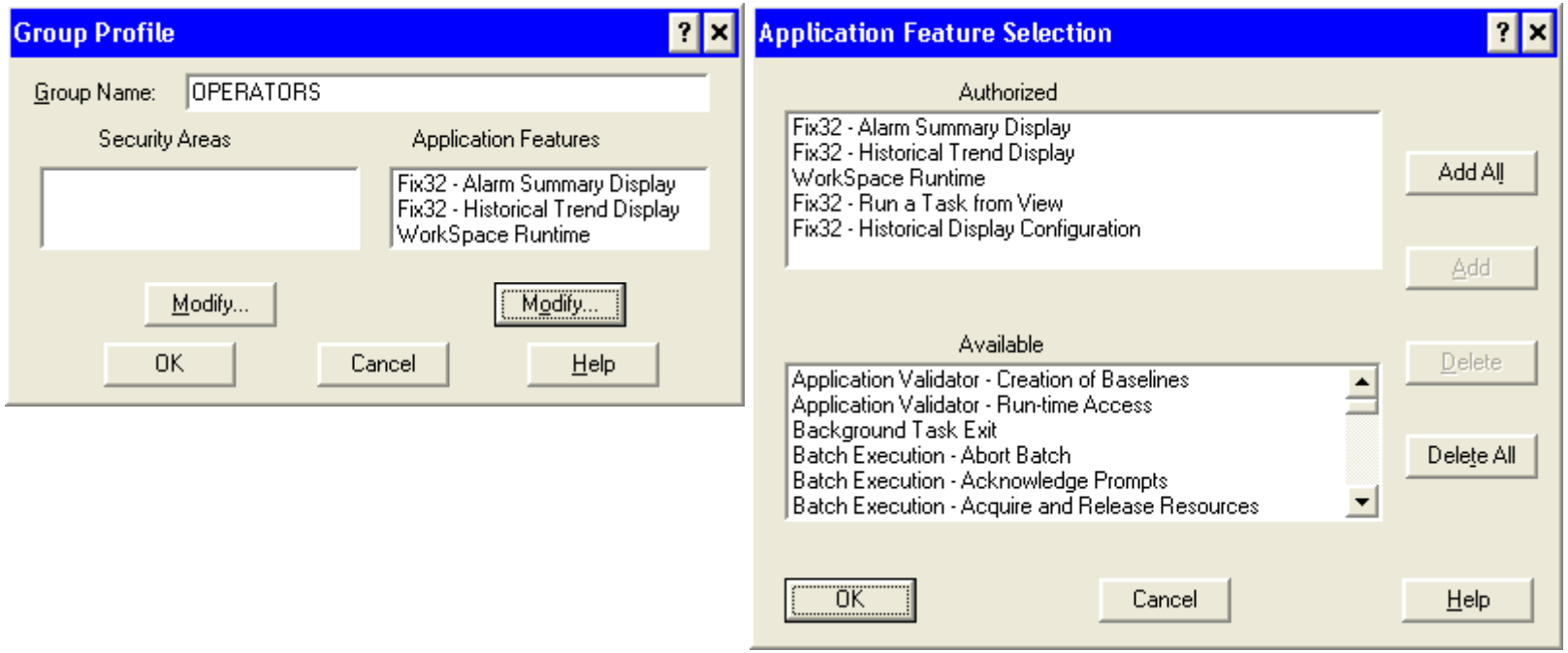
iFix security is a User based security system. We added Windows domain users to iFix users and groups to assign specific rights.

– First, enable user based security in Security Configuration



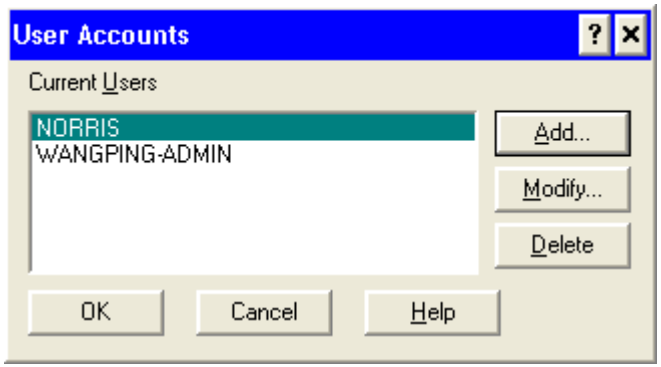
3. Implement iFix security & Windows File Protection - 4

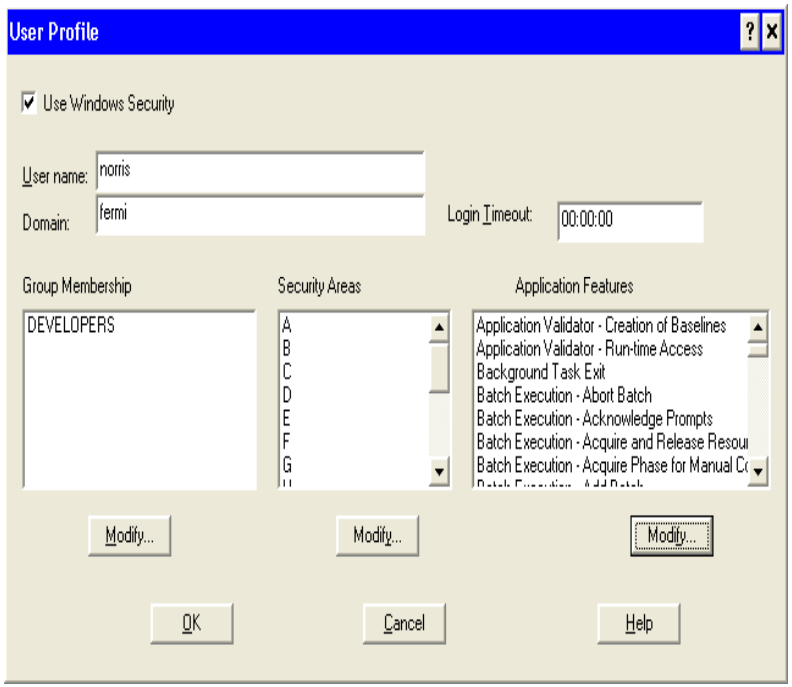
- Second, add group accounts, assign access to the Security Areas and Applications.



. Implement iFix security & Windows File Protection - 5

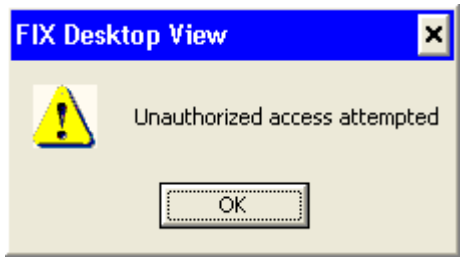
Then, add Windows domain users to iFix:





. Implement iFix security & Windows File Protection - 5

If the user tries to access a security area or open one of iFix application or a database block that he does not have privilege, he will be rejected. iFix security system creates a text file to log activities. The file is located in the alarms subdirectory with the naming convention: yymmdd.log.



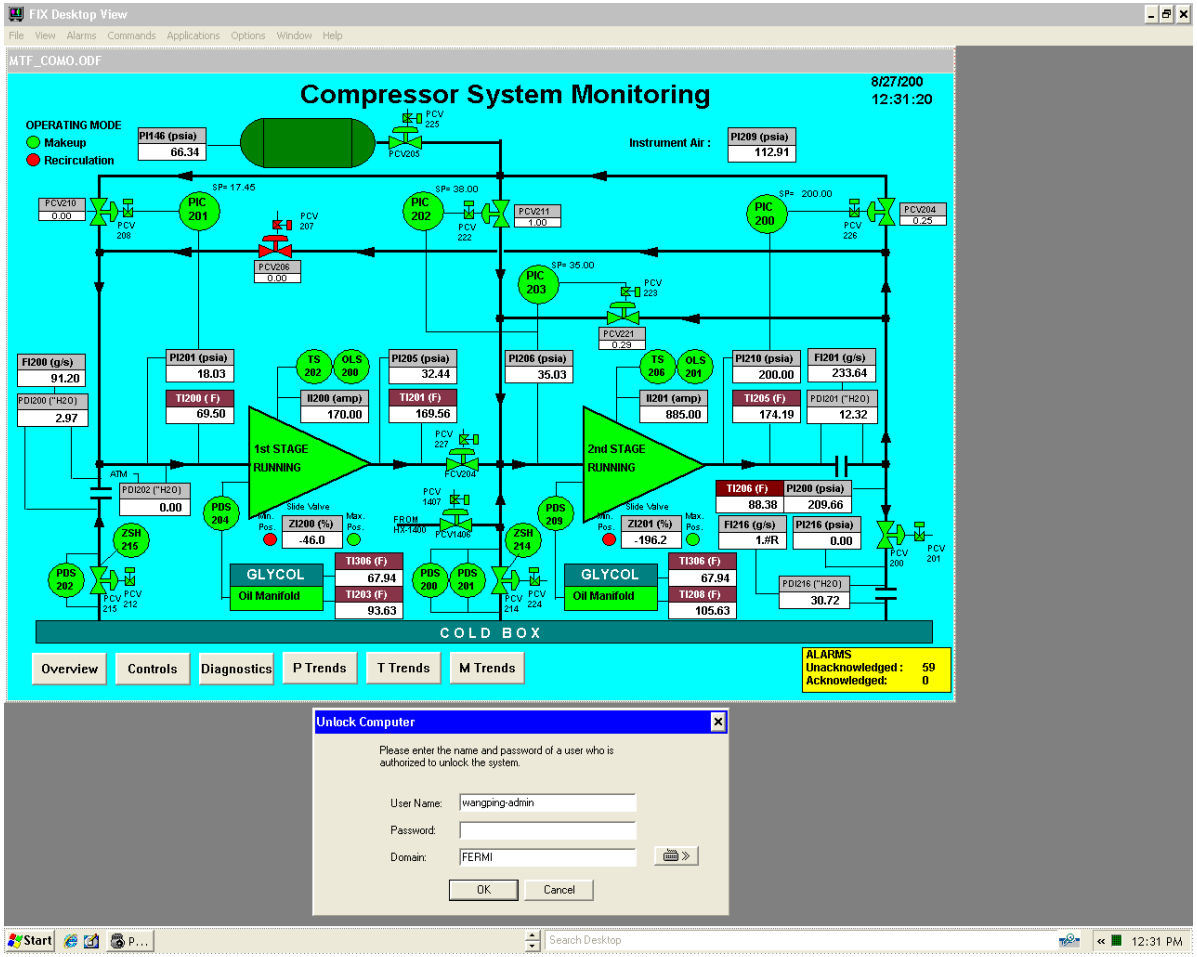
4. Console logon with domain captive accounts and lock out policy-1

We're using domain captive accounts to log in at the console of SCADA nodes and the terminal server.

Captive account is a domain account that is restricted to be used on one specific machine and password can be shared within a group. Generally it is used when several users are involved in continuous measurements during day.

We're using transparent screen saver to lock the screen after 15 minutes of idle time for these captive accounts. This allows users to keep monitoring the screen while the keyboard is locked.

4. Console logon with domain captive accounts and lock out policy-2



5. Patching and Anti-virus mechanisms -1

- Patching:

  Starting from July 2007, All Windows systems in Fermi domain were migrated to a new central Windows patching facility --- Fermi WSUS server.

  All TD Windows systems are categorized into three WSUS member groups at Fermilab:

  - Td-pilot-testers-kiosks: machines to test monthly patches
  - General: users desktops
  - Manual: DAQ systems and servers

  iFix SCADA nodes and the terminal server are in the manual group.

  If a reboot is required for patching, the deadline to reboot the members in “manual” group is postponed to the day when Microsoft releases next month patches (2^nd Tuesday of each month). This gives users more days to reboot the systems.

  *Any user can install the patch -- simply ‘double-click’ on the shield in the tray to start installation.

  * Fermi Computing Security group may consider accelerating patch rollout than normal. They may give a shorter period of deadline. In this case CIS will send a reminder to DAQ users before the deadline.

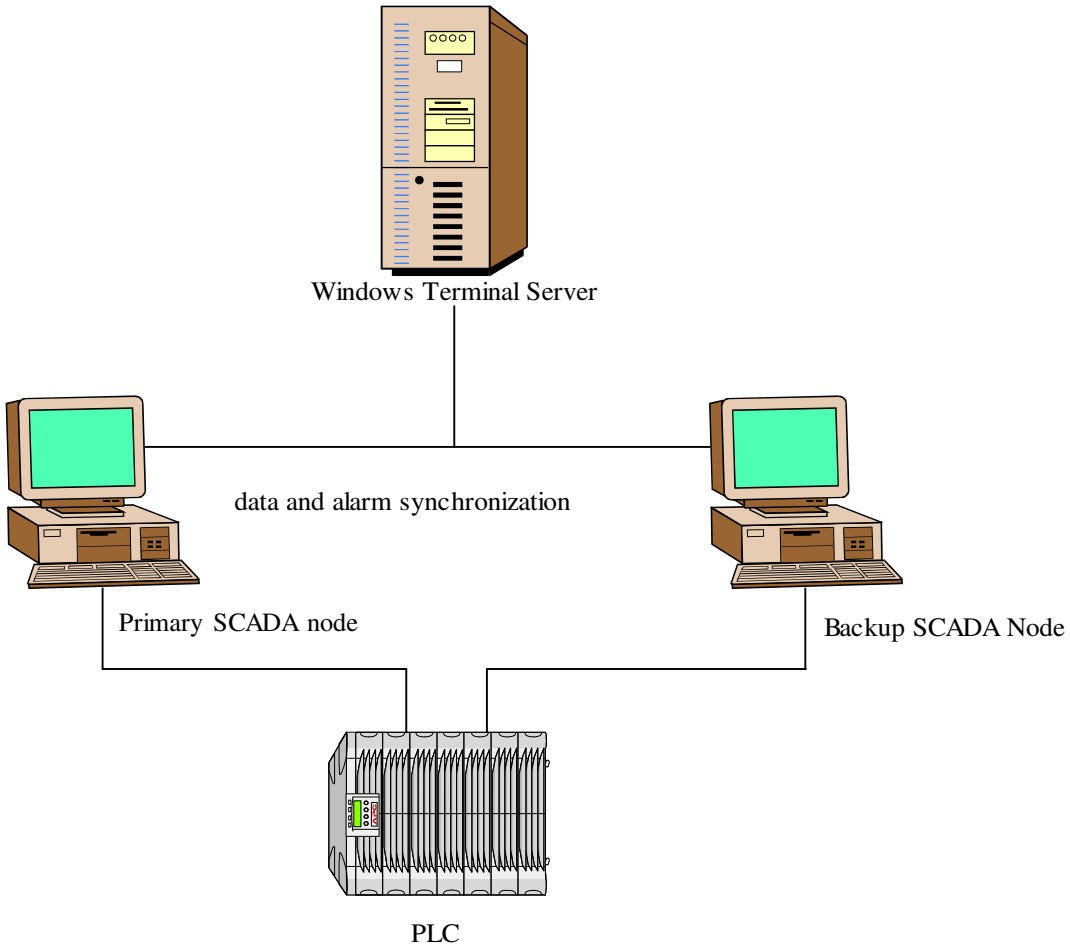
5. Patching and Anti-virus mechanisms -2

- Anti-Virus:

  The lab has taken steps to lessen the number of attacks by blocking offsite NetBIOS probes, scanning all incoming email for viruses, and providing anti-virus software on all the major windows fileservers on site. Fermi domain member systems are required to participate in the existing infrastructure. Users benefit by having their systems updated to current Virus signatures almost instantly when the vendor provides new updates. The Computing Division/Anti-virus support group is responsible to send threat warnings to OU administrators and primary system admin, and also trigger network blocking event when necessary. The TD Computing helpdesk designee is responsible for tracking these warning messages. If Windows system folders on the machine are infected, normally we will have the disk wiped and the system reloaded.

6. Fault tolerance -1:

Redundancy Architecture:

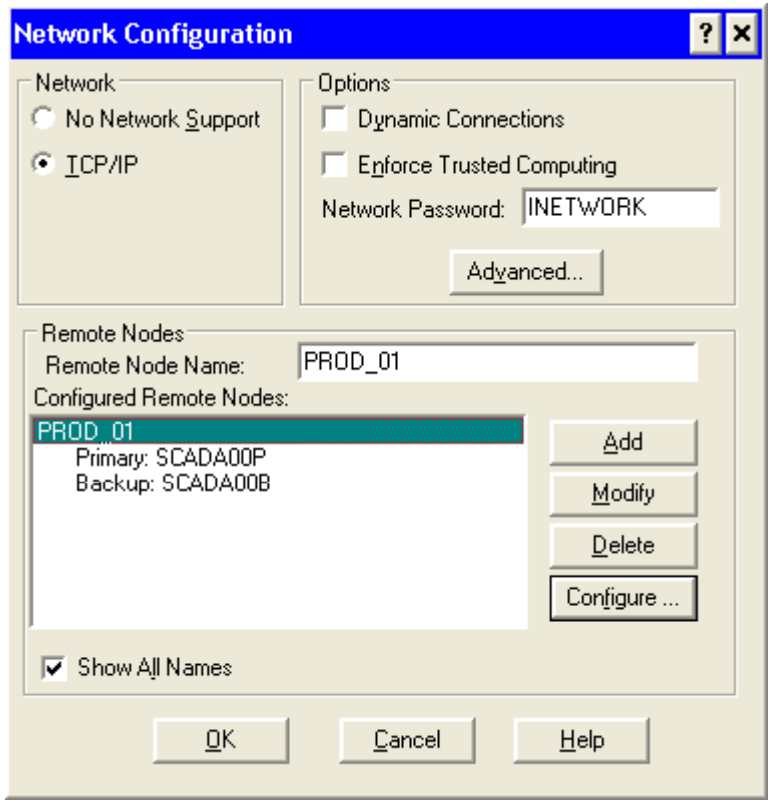


6. Fault tolerance -2:

- Two iFix SCADA servers have identical database loaded and maintained.
- They have identical I/O driver configurations.
- They connect to the same I/O devices.
- The SCUs are configured for alarm synchronization

On the terminal server, the Logical Node name is referenced instead of a physical node name. The logical name is used in data links, VBA scripts, scheduler and animations.

6. Fault tolerance -3:



On each SCADA node, you need to specify the name of its partner SCADA node.

At startup, the terminal server establishes and maintains sessions with both primary and backup SCADA nodes. It obtains data from the primary one while two SCADA nodes always maintain sessions with each other for synchronization. Whenever there is a failure on the primary, the terminal server automatically switches to the backup. At the client side, users do not experience any failure.

7. Disaster Recovery:

- Since the SCADA nodes are in the isolated network and there is no backup server available in this network, we're using the Windows Backup Utility on these windows systems to back up the file systems and save the backup file on the terminal server which is in turn backed up by TD backup server on the public network (via the dual NICs on Terminal Server).
- We're using Symantec Ghost to create images of the SCADA node system disks once per week. The restore from the image files takes only 20-30 minutes.
- Since Symantec Ghost only supports Windows workstation restoring from image files, we're currently using R-Image Drive to create image files for the terminal server. The restore of the TS from the image files takes about 2-3 hours.