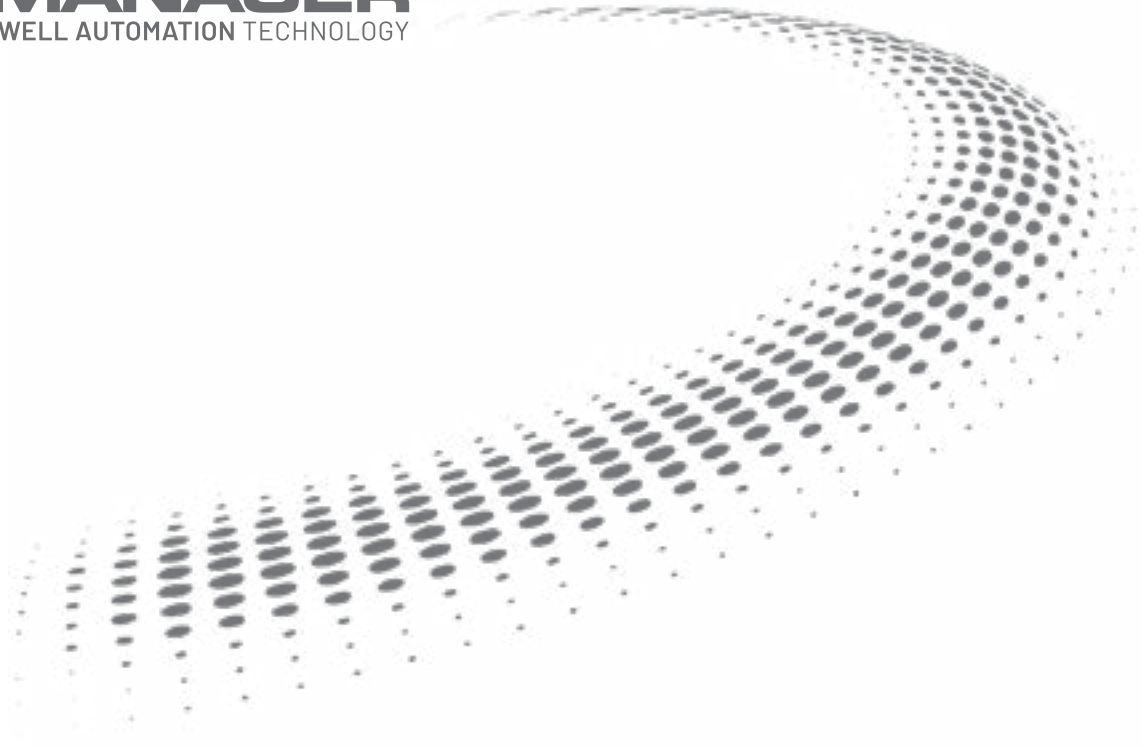




THINMANAGER[®]
A ROCKWELL AUTOMATION TECHNOLOGY



LEARNING PAPERS: NERC Compliance

The North American Electric Reliability Corporation, or NERC, has a series of standards that apply to the electricity generation business. This article shows some of the ThinManager features that can help comply with the NERC Reliability Standards.

See www.nerc.com for details on the standards.

Critical Infrastructure Protection (CIP)

- Thin Client Architecture
 - No Hard disks that retain data if the unit is stolen
 - No Flash or USB drives to prevent Trojan Horse attacks from USB devices
 - Centralized Processing can be moved to a secure area
- AppLink limits access to specific applications
- Relevance User Services (formerly TermSecure) provides additional control over access to applications and operator stations
- Event Logs
- Scheduled Reports
- Event Notification by E-mail
- ThinManager Security Groups to control ThinManager access through Windows group membership

Emergency Preparedness and Operations (EOP)

- Automatic Failover and Instant Failover of terminal servers that don't require operator initiation
- Redundancy of ThinManagers
- Event Logging
- Scheduled Reports
- Scheduled Configuration Backup
- Easy Terminal Replacement
 - Near zero configuration
 - Many hardware choices

Facilities Design, Connections, and Maintenance (FAC)

- Multi-functional operator stations
 - MultiMonitor to increase the operator desktop
 - MultiSession to run multiple applications
 - SmartSession load balancing of terminal servers
 - Tiling to allow viewing of multiple sessions at once

Interchange Scheduling and Coordination (INT)

Interconnection Reliability Operations and Coordination (IRO)

- Client shadow from within ThinManager
- Terminal to Terminal shadowing
- MultiMonitor to increase the operator desktop
- MultiSession to run multiple applications

Modeling, Data, and Analysis (MOD)

Nuclear (NUC)

Personnel Performance, Training, and Qualifications (PER)

- Access during training can be controlled with ThinManager
 - AppLink limits access to specific applications
 - Relevance User Services (formerly TermSecure) provides additional control over application deployment
 - Shadowing of terminals and operator stations, either interactive or view-only
 - ThinManager Security Groups to control ThinManager access through Windows group membership

Protection and Control (PRC)

- Thin Client Architecture
 - No Hard disks that retain data if stolen
 - No Flash or USB drives to prevent Trojan Horse attacks from USB devices
 - Centralized Processing can be moved to a secure area
- AppLink limits access to specific applications
- Relevance User Services (formerly TermSecure) provides additional control over access to applications and operator stations
- MultiMonitor to increase the operator desktop
- MultiSession to run multiple applications
- ThinManager Security Groups to control ThinManager access through Windows group membership

Transmission Operations (TOP)

Transmission Planning (TPL)

Voltage and Reactive (VAR)