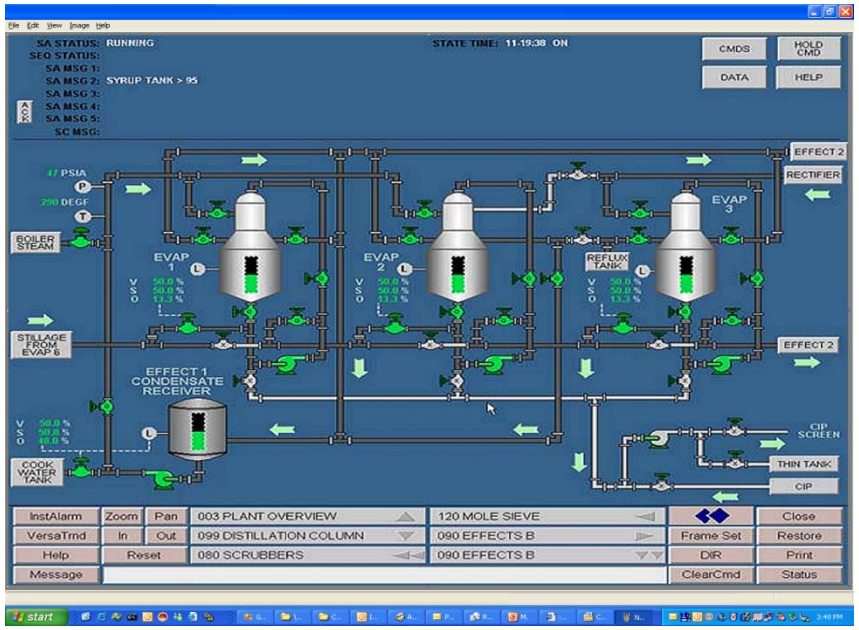
Implementation of Operator Authentication Processes on an Enterprise Level

Mark Heard
Eastman Chemical Company

Presenter

- Mark Heard, Eastman Chemical Company
  - Control System Engineer
  - Experience with several kinds of automation systems, especially networking with other plant systems
  - General interest in security and admin issues for MCS
- Work on Eastman Cybersecurity teams
  - Process Control Network Security, 2003-
  - Network Segmentation, 2004-
  - Cybersecurity Vulnerability Assessment, 2005-
  - Process Automation Systems Authentication, 2006-
  - Systems Integrity, 2008-
- Working with ISA, ChemITC (formerly CIDX) since 2002

Brief History of Control System Security



In The Good Old Days…

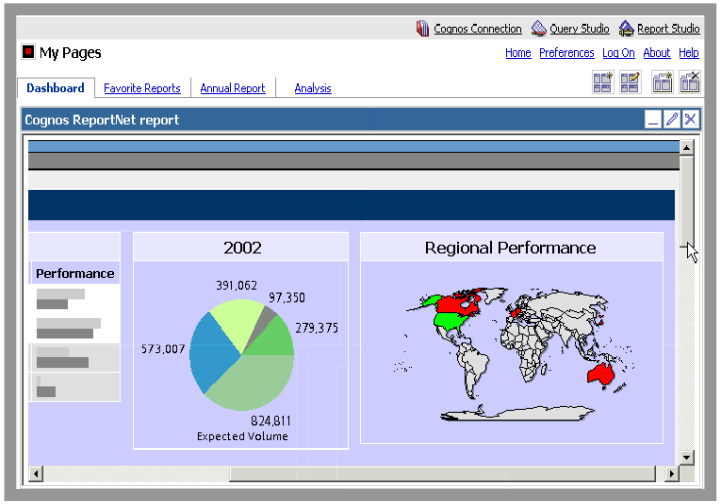
- Proprietary or VAX/VMS O/S
- Dedicated Operator Workstations
- Physical Key Access Controls
  - Operator/Supervisor/Engineer
  - Easily shared
  - Hard to duplicate
  - Obvious if lost or stolen

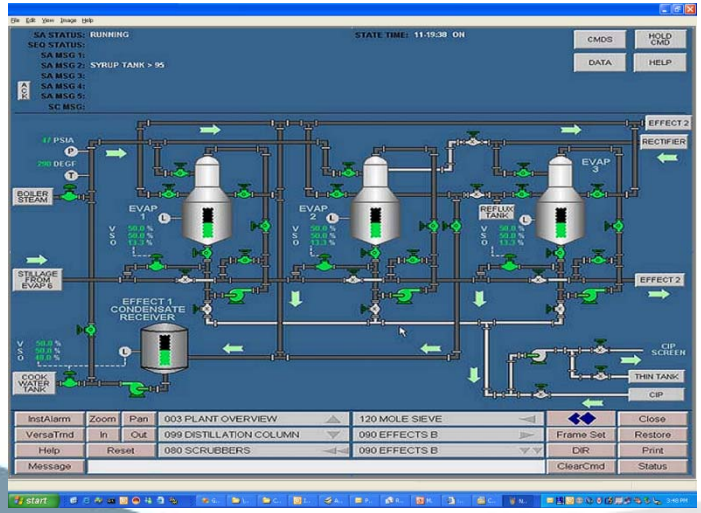
Make way for Windows!

- Inexpensive standardized hardware
- UserID/Password Access Control
- Group Accounts
  - Maintain process visibility & control
  - Diminished access control
  - Loss of accountability

EASTMAN

CIA and AIC Security Models





- For Information Systems
  - Confidentiality is #1
  - Integrity is #2
  - Availability is #3
- For Control Systems
  - Availability is #1
  - Integrity is #2
  - Confidentiality is #3
- All Systems Must Protect
  - People
  - Property
  - Information

EASTMAN

Corporate Team Formed

- Assessment of DCS Security by I/T based Auditors revealed a potential risk
- Team formed to address the risk
  - Combination of DCS and I/T backgrounds on team
- **Charge from Executive Team**
  - Address Control Room Operator Authentication
    - Is It Possible?
    - Is There 1 Optimal Solution?
    - What is the Cost?
    - Lead Instead of Wait and See
- **Process Control Systems Involved**
  - Honeywell TDC, TPS, Experion
  - NovaTech D/3
  - Emerson WDPF, Ovation, DeltaV

Challenges

- Different Hardware/Software Configurations for Each DCS Vendor
- Proprietary Input Devices
- Security Model Delivered by DCS Vendors
- Segmented Networks
- Ease of Use vs Security
- High Availability, Robustness
- Implementation

Review of DCS Vendor Security Models

- Find out what was in place and what is planned
- Most Vendors are waiting for Customer Demand
- Industry "Best Practice" guidance recommends waiting on Vendor developed solutions
- Catch 22 Scenario

Authentication Requirements

- **Musts:**
  - Authenticates process control system operators by Eastman domain UserID and Password.
  - Runs without a network connection in cached credentials mode (automatic).
  - Verifies user authorization before allowing interaction with the process control system.
  - Supports emergency unlock (login bypass) with notification to designated system administrators.
  - Process control displays remain visible at all times (transparent).

Authentication Requirements (Continued)

- **Musts**
  - Can only be configured, disabled or stopped by authorized administrators.
  - Uses standard Windows domain authentication (Eastman network UserID's and Passwords).
- **High Priority Needs:**
  - Logs all user authentication and authorization activity.
  - Locks out user again after a predetermined period of user inactivity.
  - Supports remote administration and reporting through remote registry/event-log connection

Authentication Requirements (Continued)

- **Needs**:
  - Logs all user control system activity tagged with the UserID

Honeywell's Sign-on Manager was the best fit to most of our requirements

Group Account Transparency Enabler

GATE

Accountability

Access Control

Audit Trails

Transparency

Ease of Use

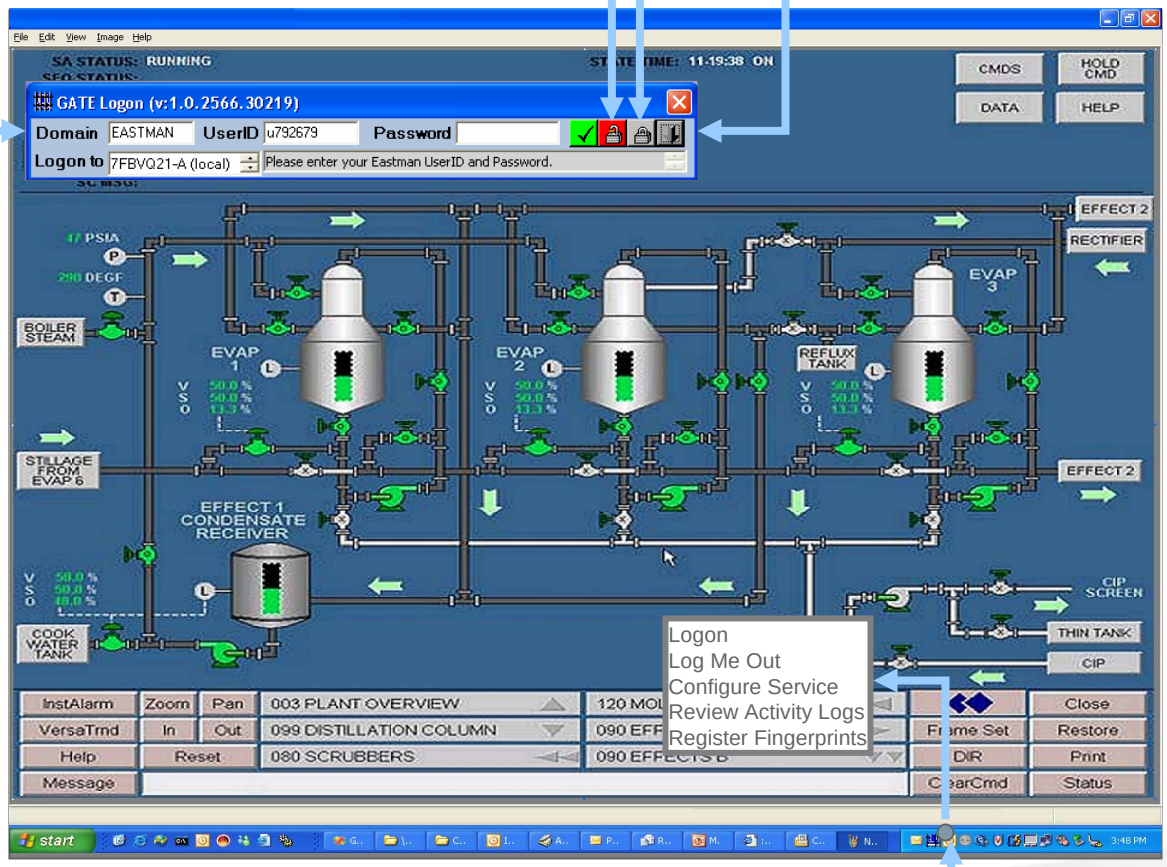
GATE Operator Authentication Interface

Logoff Current User

Emergency Unlock

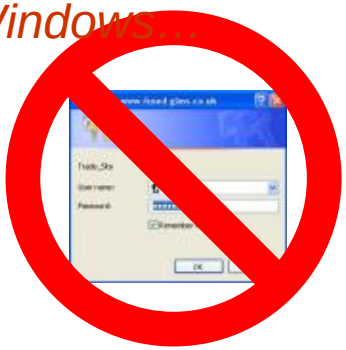
Hide Login Form

Operator Authentication (Domain Login)

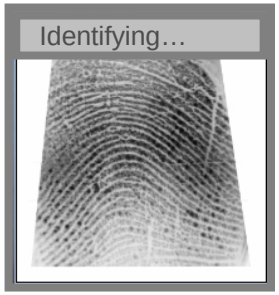


Service Configuration & Login History Review

We could just make everyone logon to Windows…



Not a popular option!

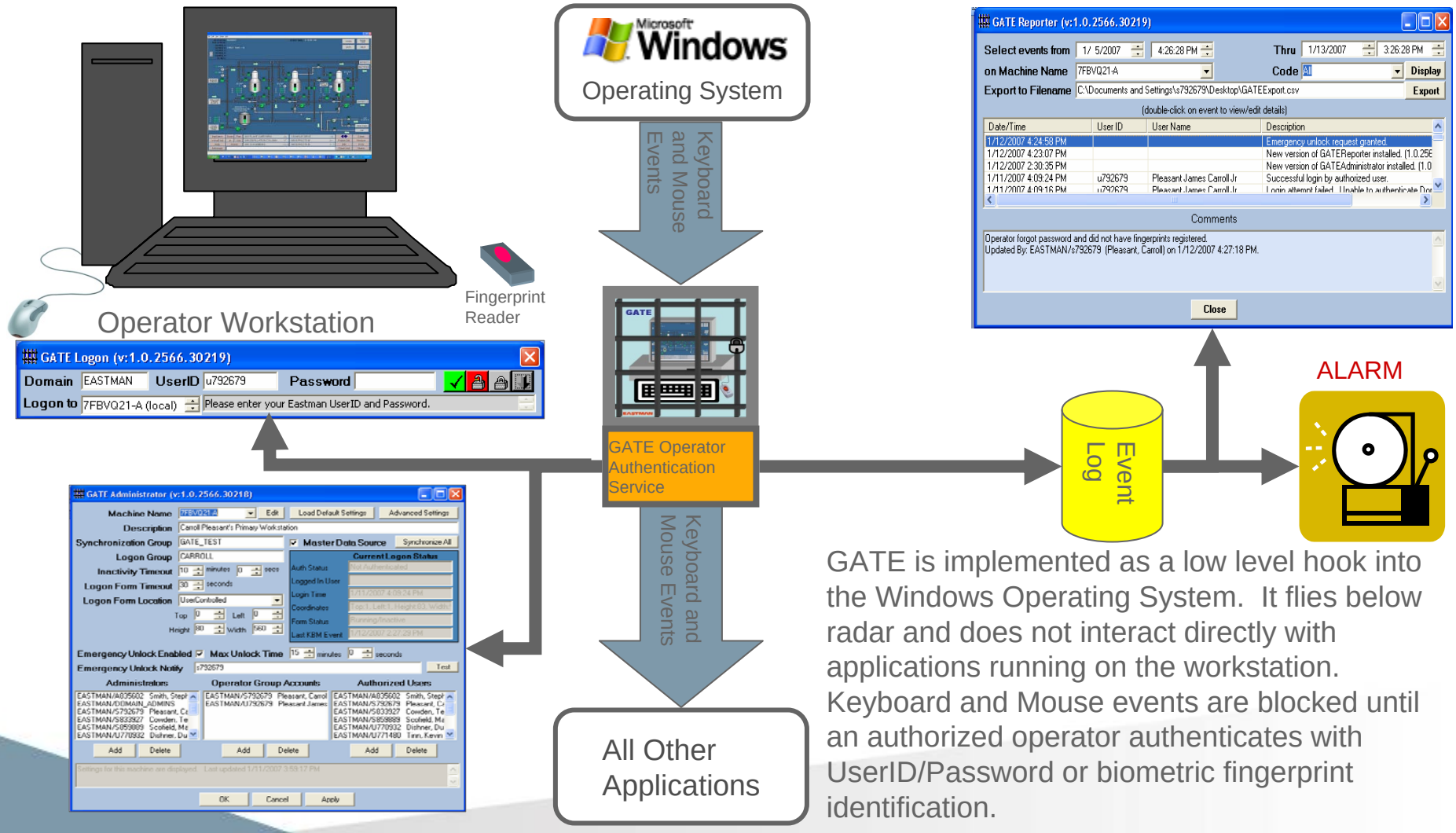


Very Cool
Very Fast
Very Easy

Operator Authentication Processes

EASTMAN

GATE Authentication Service Architecture



GATE is implemented as a low level hook into the Windows Operating System. It flies below radar and does not interact directly with applications running on the workstation. Keyboard and Mouse events are blocked until an authorized operator authenticates with UserID/Password or biometric fingerprint identification.

Operator Authentication Processes

EASTMAN

GATE Key Design Considerations

- **User Interface**
  - Must be almost completely ***intuitive***. Not reasonable to expect a lengthy enrollment process.
  - Must be ***fast***! Cannot get in the way during an emergency situation.
  - Must not block ***visibility*** of process control graphics.
  - Use existing EMN UserID's and Passwords. Nothing new to remember!
  - Enroll once. Use everywhere.

GATE Key Design Considerations (Continued)

- **Technology**
  - Don't monkey around with GINA and take chances with Windows ***stability***!
  - Don't make any changes to DCS vendor software. Maintain process ***isolation***! Don't plan on having 24x7, 99.999% connectivity to the corporate network. Must ***stand alone***!
  - Provide facility for remote configuration and maintenance.
  - Log everything in a place where the users cannot easily corrupt or delete the data.

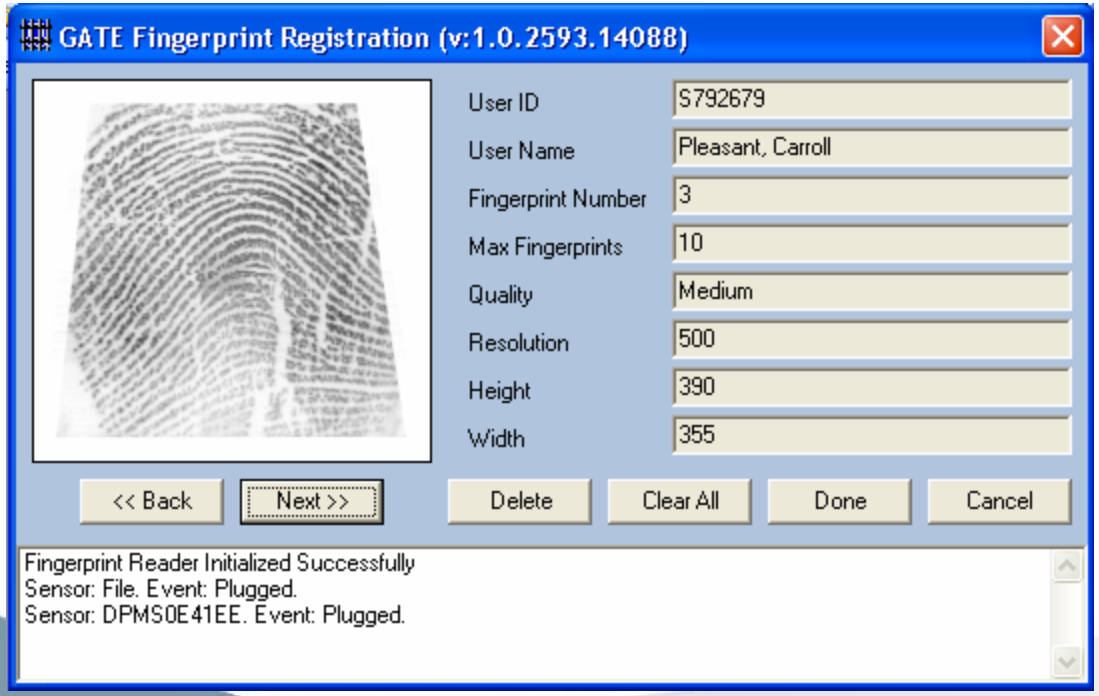
GATE Key Design Considerations (Continued)

- **Auditability**
  - Must be able to identify who had control at what time.
  - Must be able to annotate activity logs. (Management responsibility when emergency unlock is used)
  - Must be able to export logs for auditors.
  - Auditors may not have administrative rights.

GATE Failsafe Mechanisms

Software Crash	Gate fails "open" (unlocked)
Network Outage	Gate operates from locally cached data
Forgotten Password	Use the fingerprint reader or Emergency Unlock feature
Fingerprint Reader Failure	Login by UserID/Password
Software Freeze	Logon or Unlock remotely from another workstation – reboot option is always available
Data Loss/Corruption	Synchronize with data from another workstation
Can't wait for Logon!!! EMERGENCY	Click on the Emergency Unlock button twice or use Control/Alt/End hotkey.

Biometric User Registration and Authentication



Self Registration

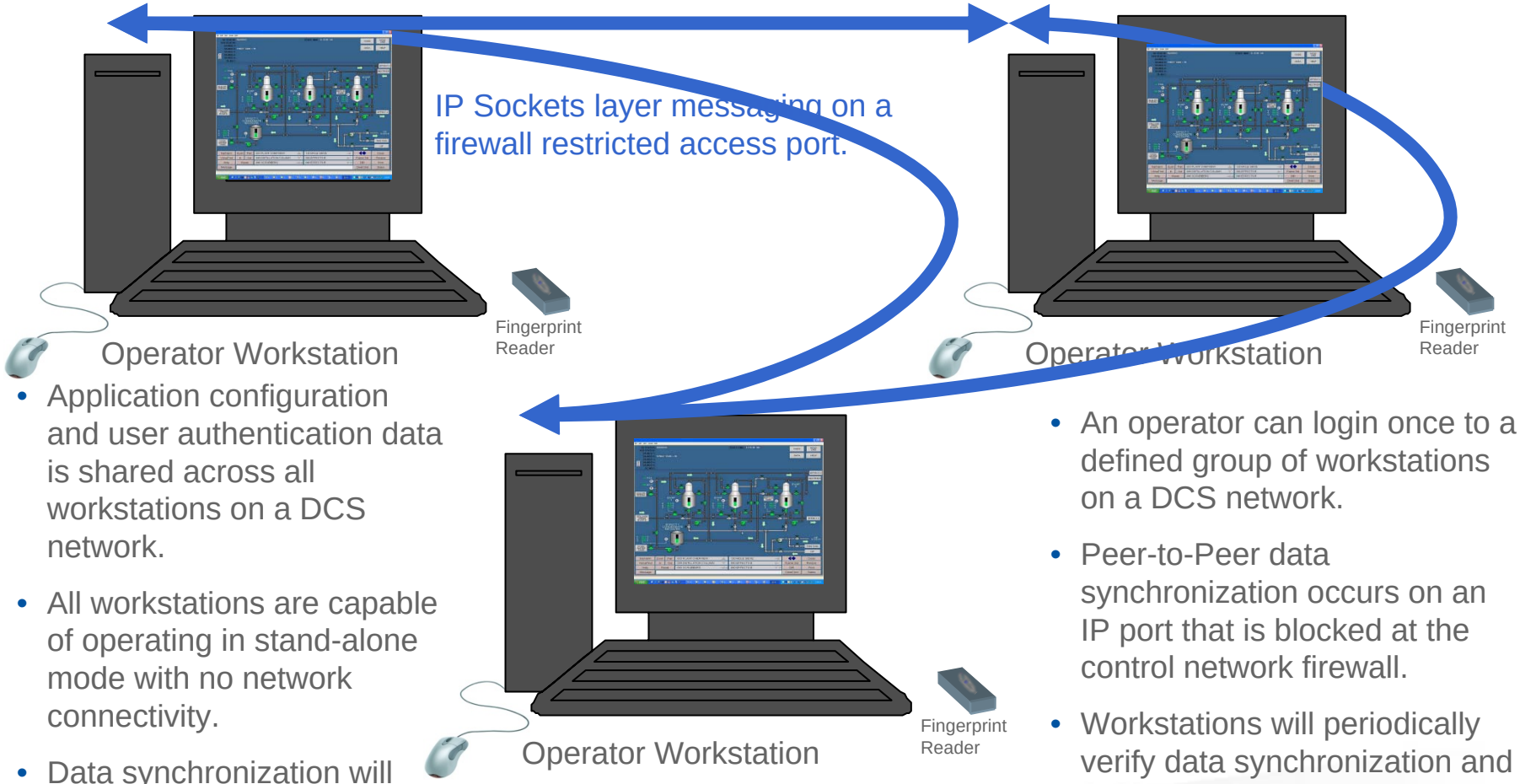
- User must authenticate by UserID and password immediately before registering fingerprint images.
- Fingerprints are stored by simply touching a finger on the reader.
- Users should store multiple fingerprint images (at least 4) to insure reliable recognition. Up to 10 images can be stored for each user. Different fingers can be used for each image.

Authentication

- Fingerprint recognition is equivalent to entering UserID and Password for gaining system access.
- Recognition and logon will normally take less than 1 second.

EASTMAN

Peer-to-Peer Synchronization Architecture



- Application configuration and user authentication data is shared across all workstations on a DCS network.
- All workstations are capable of operating in stand-alone mode with no network connectivity.
- Data synchronization will normally occur within a few seconds of any change.

- An operator can login once to a defined group of workstations on a DCS network.
- Peer-to-Peer data synchronization occurs on an IP port that is blocked at the control network firewall.
- Workstations will periodically verify data synchronization and "catch-up" any machines that have been offline.

EASTMAN

Costs

- One Time Software Purchases
  - Fingerprint Recognition SDK < $5000
  - Virtual Serial Port SDK < $500
- Per Operator Workstation
  - Fingerprint Reader < $40
  - USB Extension Cable (if needed) < $10

Project Status

- Piloted in manufacturing areas:
  - Tested on Novatech D/3, Emerson Ovation, DeltaV, and Honeywell TPS, Experion
  - Testing in all areas of Kingsport, TN Site
- Fully Operational in the Corporate Network Control Center
  - Used by technicians in the control center
  - Systems monitor I/T computers and networks
- Deployed 2H2007 to Manufacturing Control Rooms

Enhancements

- Network fault tolerance
- GATEway Service for non-trusted domains or workgroups
- GATE Usage Reports and Analyzer (automated)
- Automatic software updates (no reboot!)
- Future
  - Vista support
  - 2 factor authentication

Where Do We Go From Here

- Operator Authentication is Here to Stay
- Simply Using Windows Authentication is NOT Adequate for Control Systems
- Engage Vendors to Integrate Solutions into the Standard Product

Questions?

Contact Information:
Mark Heard
mheard@eastman.com
423-229-3516