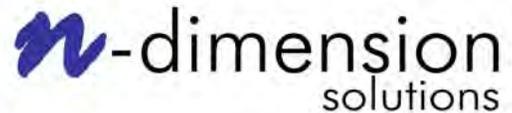




**Process Control Systems
Industry Conference**

Secure Access Control for Control System Operations

Andrew Wright, CTO
andrew.wright@n-dimension.com



... Access Control ...

- ◆ **Authentication**

- who you are

- ◆ **Authorization**

- what you may do

AAA

- ◆ **Audit**

- what did you do

... for Control System Operations

- ◆ **for control system cyber assets**

- servers, HMIs, operator stations, engineering stations, RTUs, IEDs, PLCs, historians, etc.

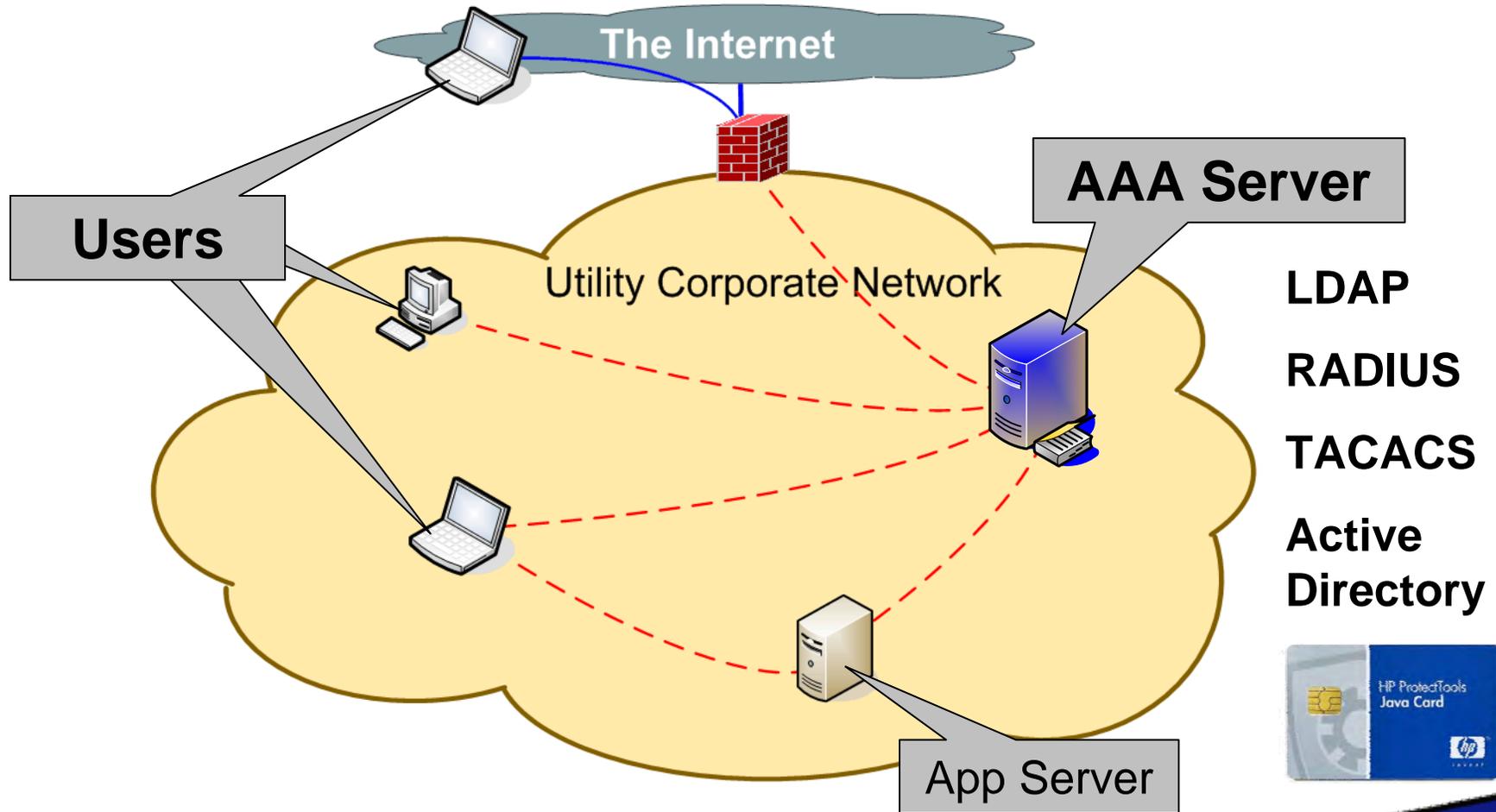
- ◆ **particularly with remote field equipment**

- eg. SCADA

Secure ...

- ◆ **against outsiders**
- ◆ **against outsiders who were recently insiders**
- ◆ against insiders (partly via deterrence)
- ◆ against attacks from compromised field sites

Secure Access Control in Enterprise Networks



LDAP

- ◆ **Lightweight Directory Access Protocol**
- ◆ **LDAP directory server is a database storing:**
 - username, person name, address, phone#, photo, etc.
 - authentication information, eg. password hash
- ◆ **LDAP client authenticates by “binding” to server**
 - communication can be (should be) within SSL
- ◆ **LDAP directory servers can be replicated**
 - single master allows updates only on one master
 - multi-master allows updates on any master



So What's the Problem for Control Systems?

- ◆ **No user authentication in many IEDs, RTUs, PLCs**
 - Device password shared amongst all users
 - Same password reused across multiple devices
 - Passwords seldom changed
- ◆ **No authentication protocols in many IEDs, RTUs, PLCs**
 - no support for LDAP, AD, RADIUS
- ◆ **Poor authentication protocols in control applications**
 - Passwords sent over wire in the clear
 - Incorrectly designed or implemented cryptographic protocols
 - eg. vulnerable to Man-In-The-Middle attacks
 - Little use of multi-factor authentication

More Problems

◆ Poor authorization

- Default passwords
- Network admission is usually all-or-nothing

◆ Poor auditing

- Limited logging mechanisms
- Irregular collection of logs
- Stranded logs

◆ Little use of encrypted communications

- Engineering access can be snooped or usurped
- (even if channel is strongly authenticated)

Yet More Problems

◆ No central management

- Hard to ensure uniform access control over entire infrastructure
- Hard to update access control in a timely fashion
 - change passwords, add or remove user, change authorization
- Hard to gather and review audit logs

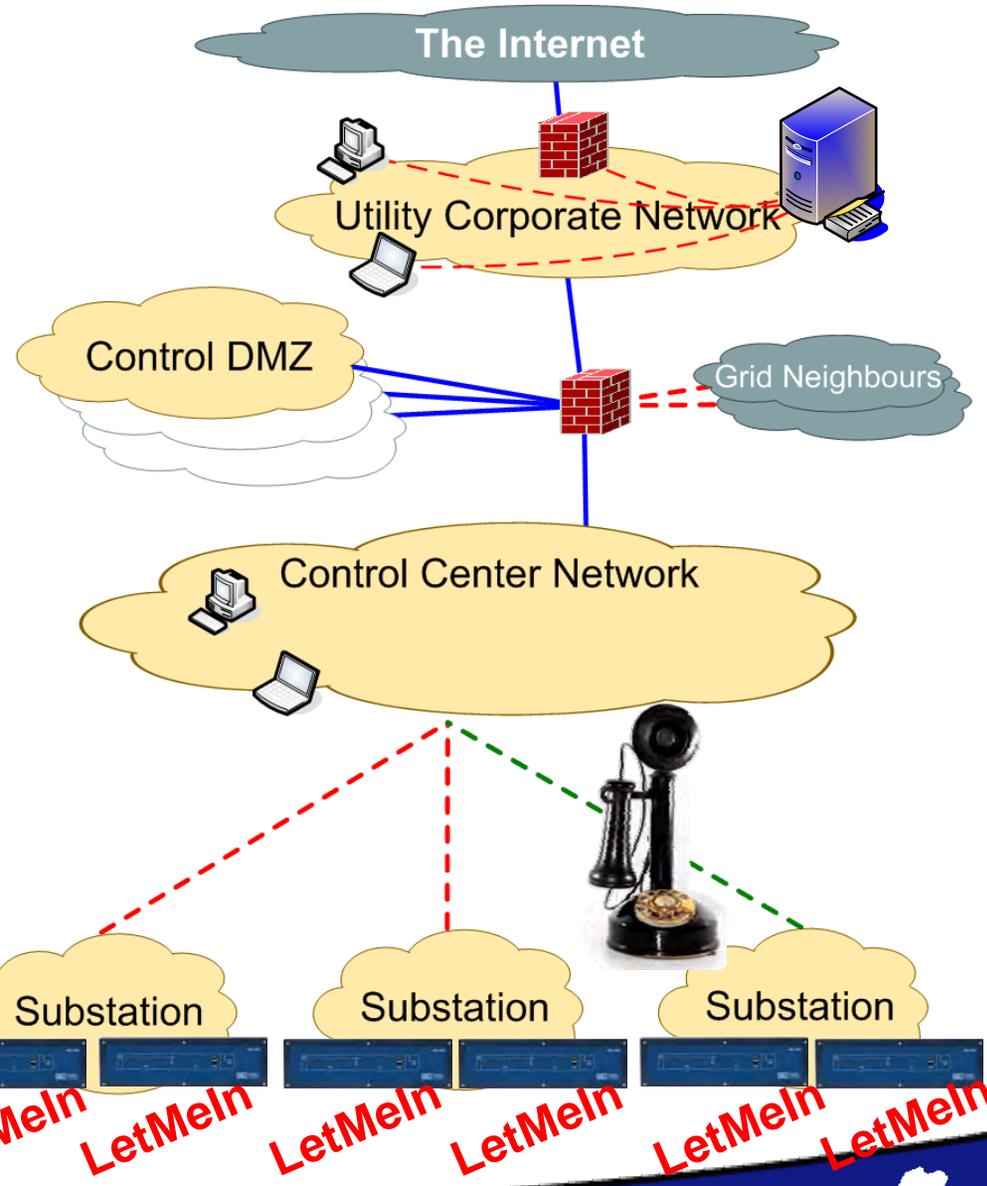
◆ Low bandwidth from field sites

- AD synchronization is infeasible over 1200 baud dialup

◆ Communications interruptions

- Loss of SCADA may be reason remote access is required

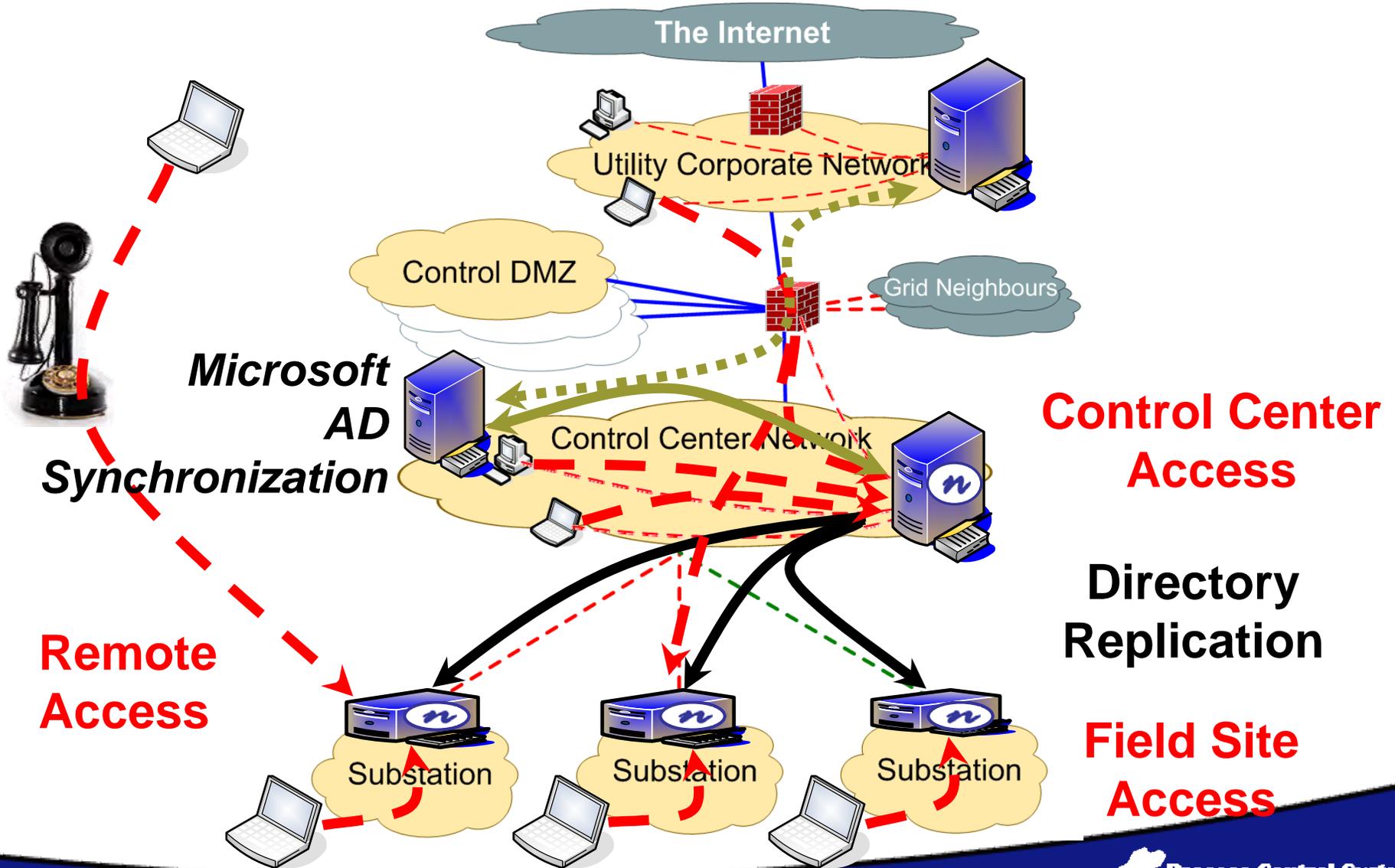
SCADA Access Control Challenges



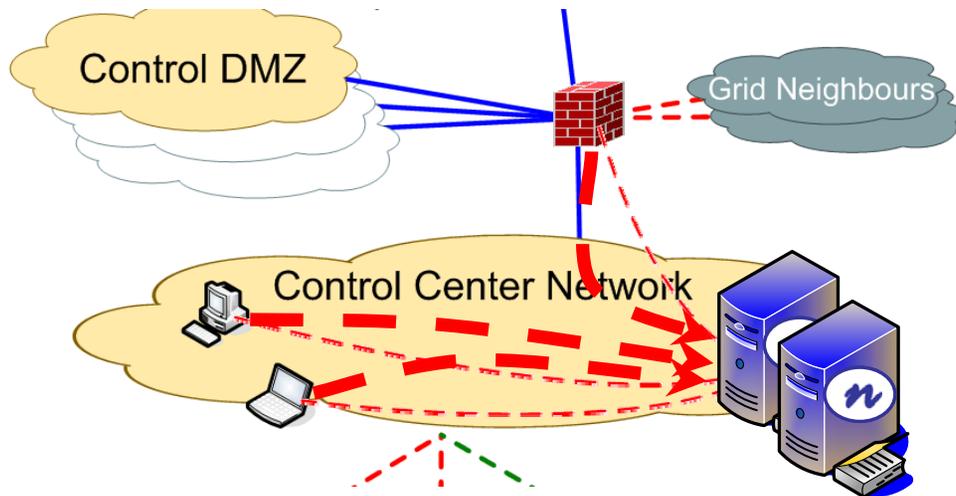
Secure Access Control

- ◆ based on LDAP and client VPN
- ◆ provides uniform, centrally managed AAA
- ◆ with similar functionality to enterprise AAA
- ◆ but avoiding all the problems

Secure Access Control

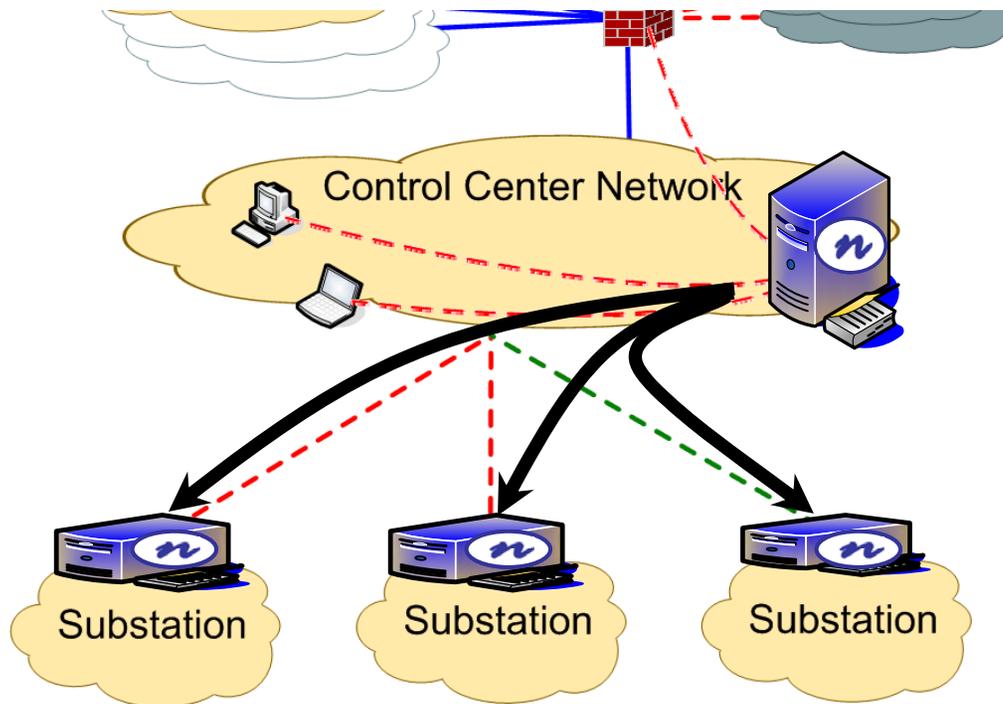


Control Center Access



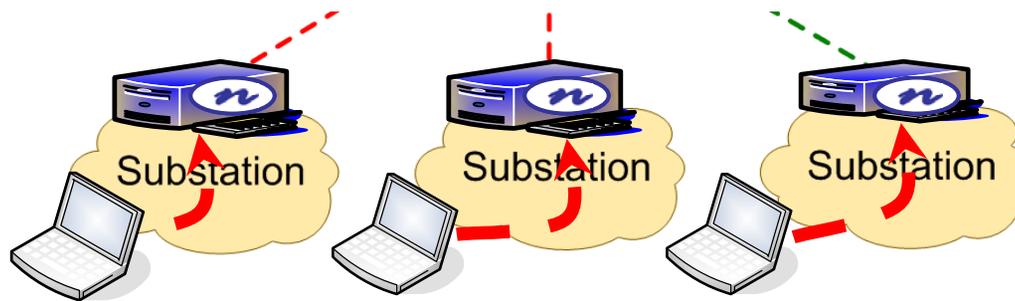
- ◆ **standard LDAP over SSL**
 - clients can be Unix, Linux, Cisco, n-Dimension, control system apps, etc.
- ◆ **high availability**
 - replicated LDAP server
 - with multi-master sync

Directory Replication to Field Sites



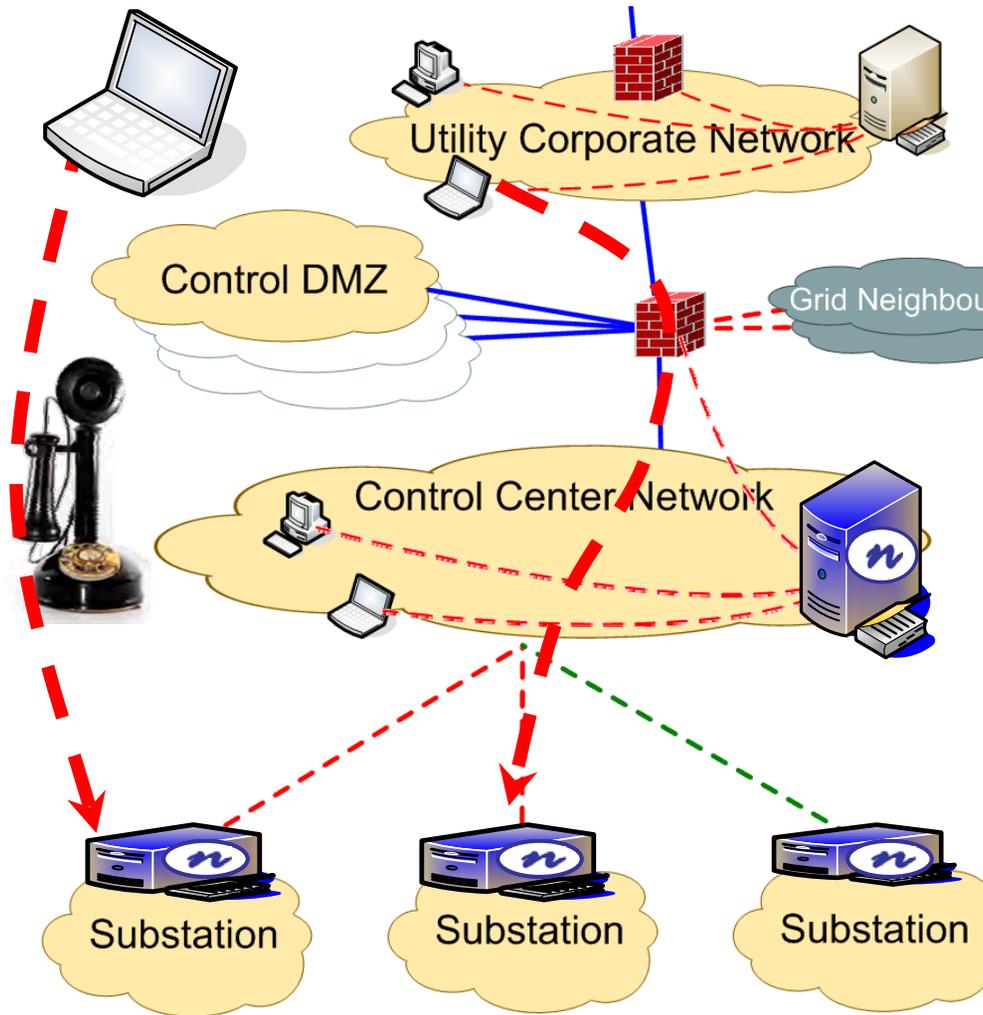
- ◆ **replication must be one way**
 - actions in substation cannot affect master directory
 - substation directory read only
- ◆ **push relevant data only**
 - only authentication info
 - only authorized users
 - only changes
- ◆ **over IP or dialup using SSL**
 - can use engineering access connection

Field Site Access



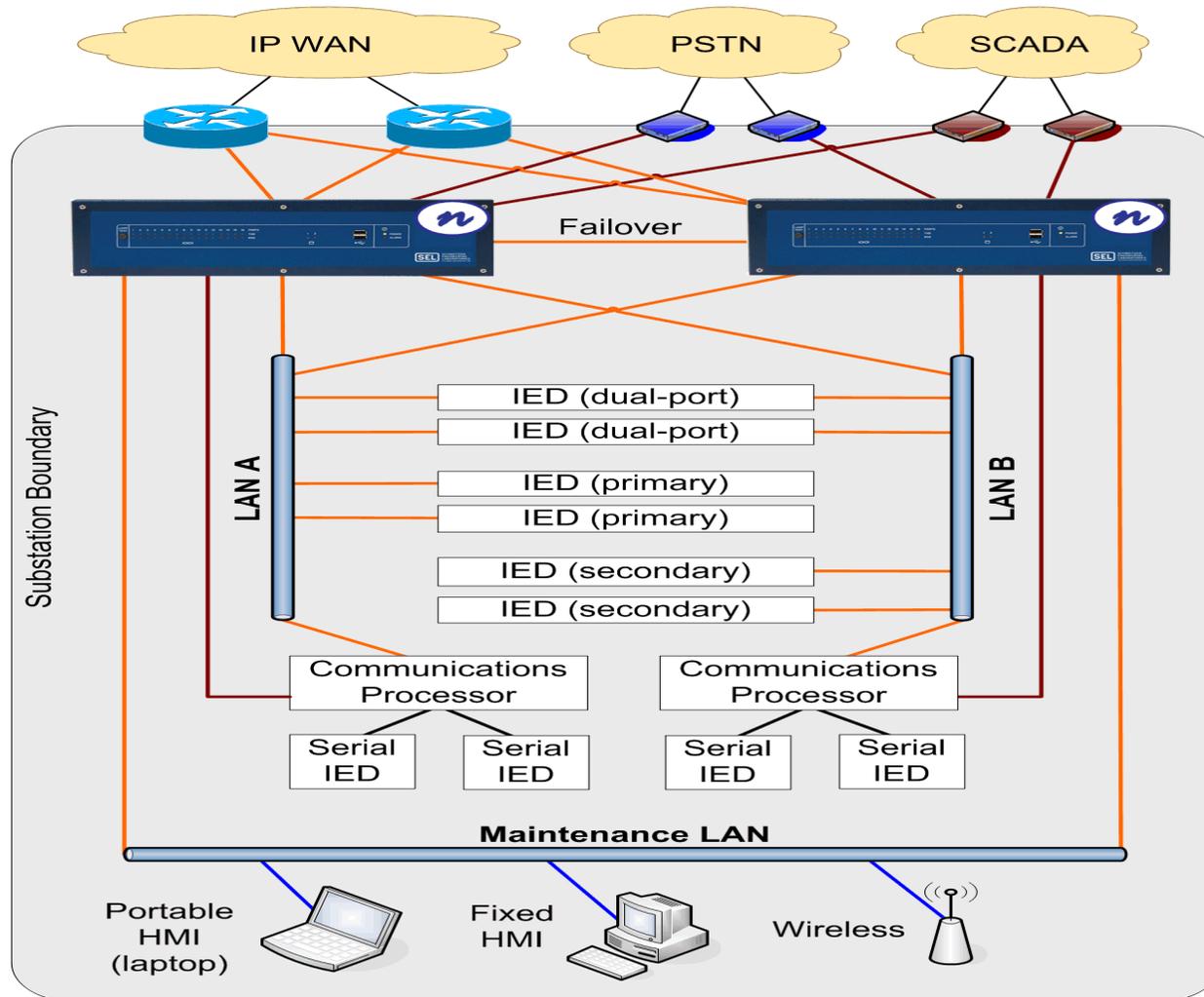
- ◆ **users first establish PPTP VPN to access gateway**
 - user is authenticated
- ◆ **all access to field devices is thru gateway**
- ◆ **gateway can enforce authorization by IP address**
 - vendor can be confined to appropriate systems
- ◆ **gateway logs accesses to field devices**

Remote Access

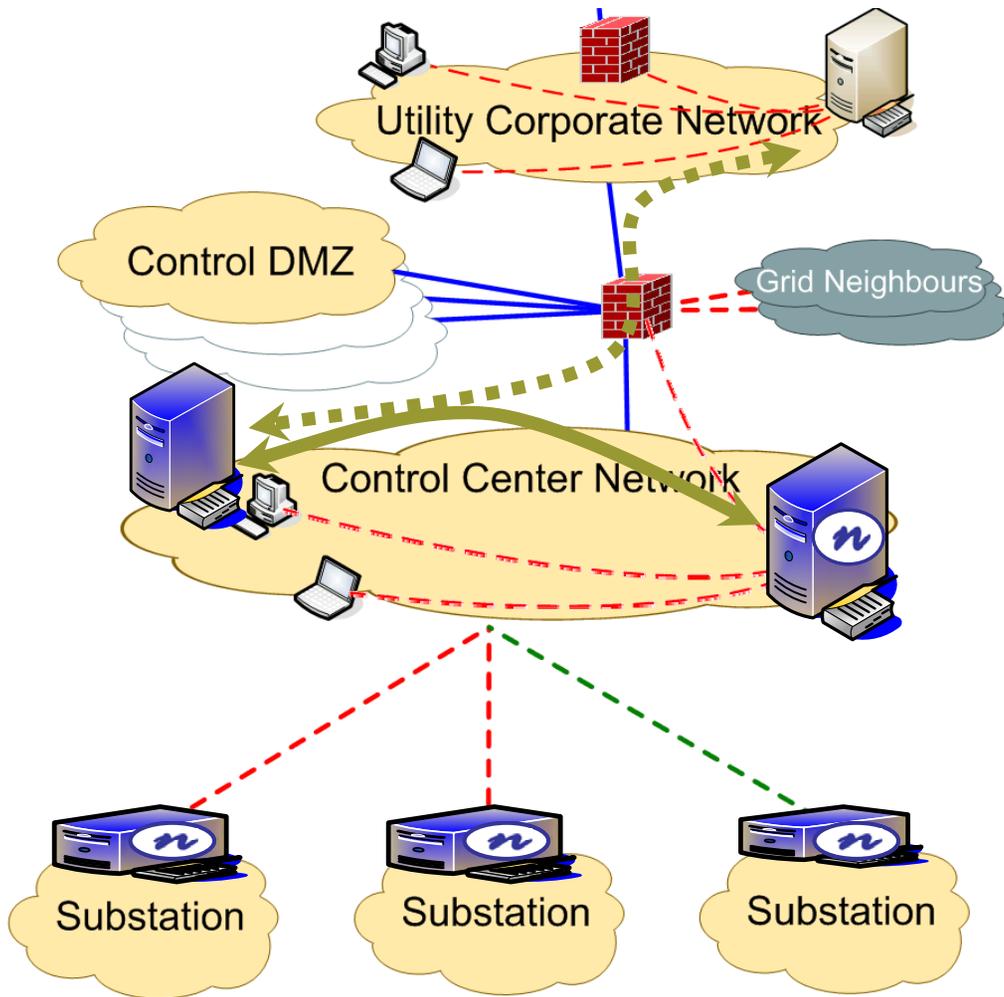


- IP to gateway uses VPN
- dialup uses VPN over PPP
- gateway can enforce authorization by IP address
- gateway logs accesses to field devices

Substation Detail

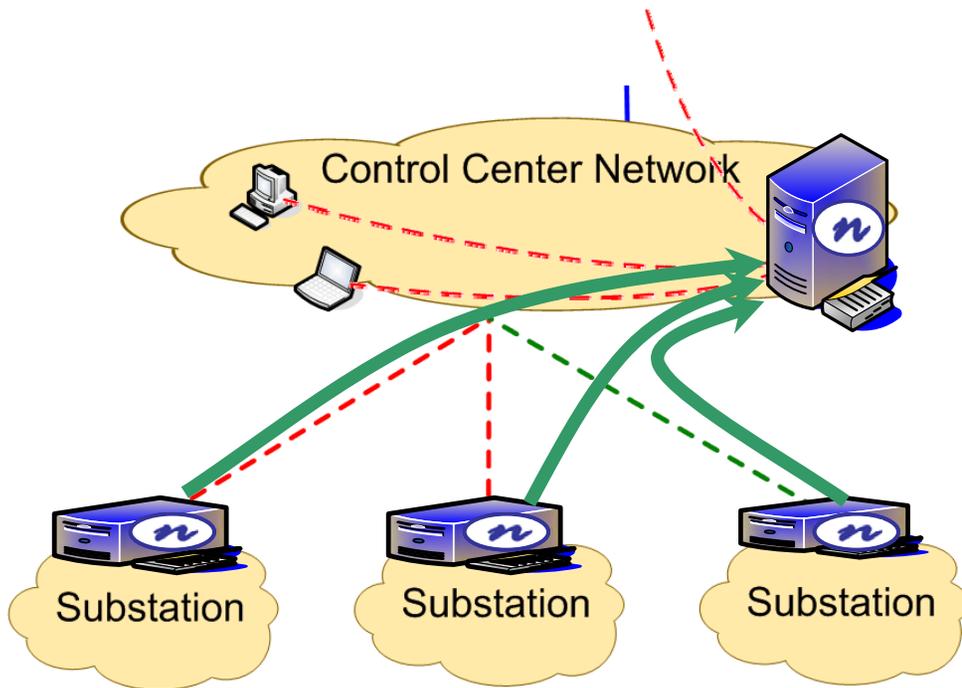


Microsoft AD Synchronization



- **User/group/password sync with Microsoft AD**
- **Only between master LDAP server and AD**
- **LDAP over SSL**

Audit



- ◆ **access logs collected periodically from substation gateways during replication**
 - over IP or dialup using SSL

Multi-Factor Authentication

- ◆ **much stronger than passwords alone**
- ◆ **prevents copying / selling credentials**
 - prevents certain insider attacks
- ◆ **must NOT depend on connection to central server**
- ◆ **smart cards are appropriate**

Physical Security

- ◆ **physical access to the substation could be managed by the same system**
- ◆ **smartcard reader and PIN pad at entry door**
- ◆ **cyber access not granted unless physical access was successful**

- ◆ **for the future ...**

Summary

- ◆ **strong, uniform, centrally managed**
- ◆ **using open protocols and proven technologies**
- ◆ **over IP or dialup communications**
- ◆ **operates without connectivity**
- ◆ **accommodates legacy control system devices**
- ◆ **no special client software**
- ◆ **minimal user burden**

Implementing Secure Access Control

- ◆ requires “only” LDAP, VPN, plus a little glue, plus substation-grade hardware
- ◆ many issues are surprisingly tricky
- ◆ don't try this at home ...

Available Soon from N-Dimension

on  substation hardware

Questions?

