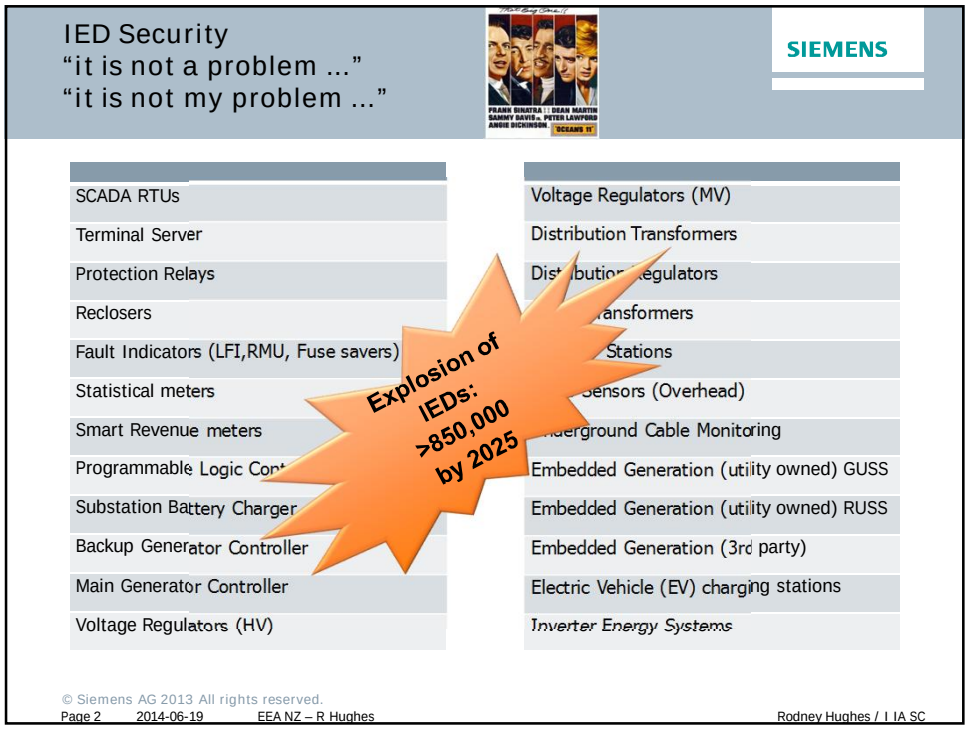

SIEMENS
Requirements and Experience of Practical Secure Access Control and Management of Intelligent Systems
Rodney Hughes* Siemens Australia (Ruggedcom) rodney.hughes@siemens.com
Randy Carson Siemens Canada (Ruggedcom) randy.carson@siemens.com
Restricted © Siemens AG 2013 All rights reserved.
siemens.com/answers


IED Security
"it is not a problem ..."
"it is not my problem ..."
SIEMENS
SCADA RTUs
Terminal Server
Protection Relays
Reclosers
Fault Indicators (LFI,RMU, Fuse savers)
Statistical meters
Smart Revenue meters
Programmable Logic Cont
Substation Battery Charger
Backup Generator Controller
Main Generator Controller
Voltage Regulators (HV)
Voltage Regulators (MV)
Distribution Transformers
Dist bution egulators
ansformers
Stations
ensors (Overhead)
derground Cable Monitoring
Embedded Generation (utility owned) GUSS
Embedded Generation (utility owned) RUSS
Embedded Generation (3rd party)
Electric Vehicle (EV) charging stations
Inverter Energy Systems
Explosion of IEDs: >850,000 by 2025
© Siemens AG 2013 All rights reserved.
Page 2 2014-06-19 EEA NZ – R Hughes
Rodney Hughes / I IA SC

SIEMENS

Not just power industry – any IED environment

- Utilities:
  power, water, gas,
  telecommunications;
- Transport control systems:
  road, rail, airport;
- Mining and/or industrial plant;
- Building/site management systems

- Smart Grid deployment
- Communicating sensors & controllers
- Cloud computing approaches
- Remote access to devices
- Smart phone access
- Wireless technology
- The “internet of things”

SIEMENS

Access for who? For what?

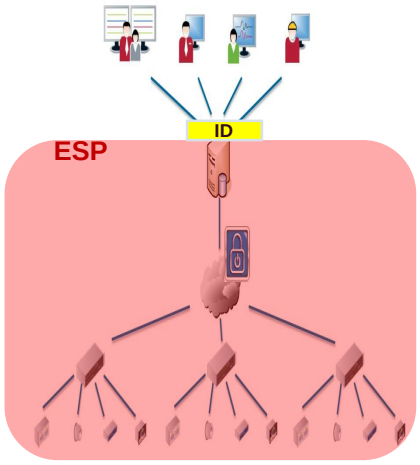
- Engineering personnel
- Commissioning personnel
- Maintenance personnel
- Vendor support personnel

- Geographical region
- Site specific
- Device Specific
- Command Specific
- Role Specific View – Edit

What is Secure Role Based Remote Access? (ESKOM @ Distributech Africa, March 2014)

SIEMENS

- WHAT IT IS:
- Role based user-2-device secure remote "engineering" access
- User connect seamlessly to remote IED
- No User connecting to IED network - Hides network info
- Manages connections and vendor applications
- Aligns to ID in NERC-CIP and aids in CIP compliance
- Systems are device and communications agnostic for remote engineering
- WHAT IT ISNT:
- Conventional RAS >>> user-2-network
- Firewall >>> network-2-network restrictions

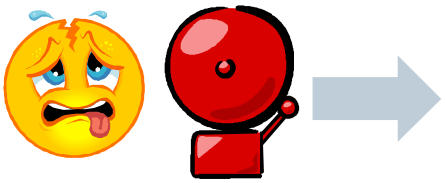


CIGRÉ Electra Magazine: December 2006

SIEMENS

7 Conclusions and Future Developments

The level of security of the older and most current SCADA systems is not enough for the present cyber situation. To make things worse the new IEC-61850 standard has no provisions for security yet. Because of its open network type communication, it also opens the system for cyber attacks. This new communication standard is really dangerous if used in a network with a poor security design. Because the protocol does no longer compartment the communication, it may loose control over the whole grid. All older communication standards do not address security as well.



- TB 419 Treatment of Information Security for Electric Power Utilities (EPUs)
- TB427 The Impact of Implementing Cyber Security Requirements using IEC 61850
- WGB5-D2 46

NERC CIP -003-3 R5
Identify Individuals who can **authorise** access

SIEMENS

R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

NERC CIP -003-3 R6
Changes to IED Firmware version
Changes to IED Configuration version and setting

SIEMENS

R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

NERC CIP 004-3a R4
Know who has access to what
Revoke <24 hours if dismissed
Revoke <7 days if access no longer required

SIEMENS

R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

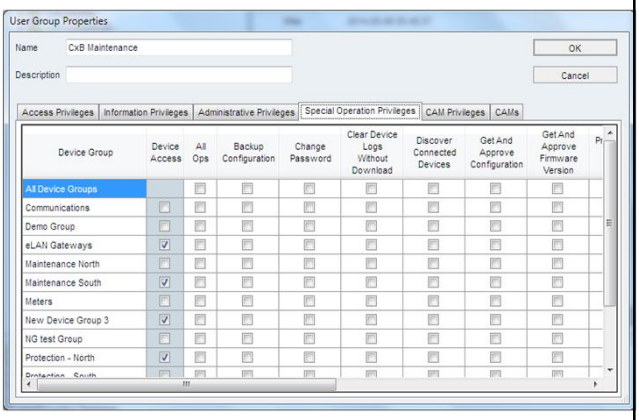
R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

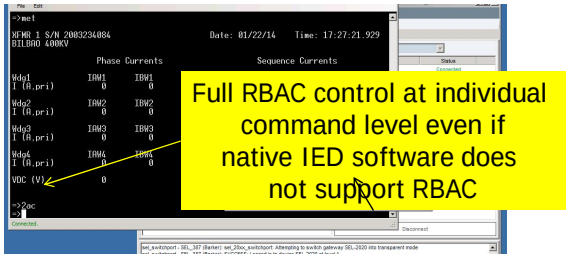
Who needs access?

SIEMENS

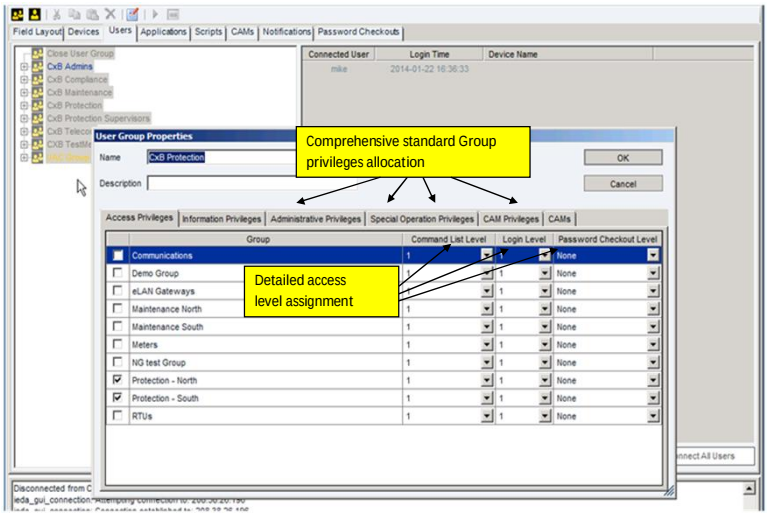
- engineering staff
- commissioning staff
- maintenance staff
- vendor support staff



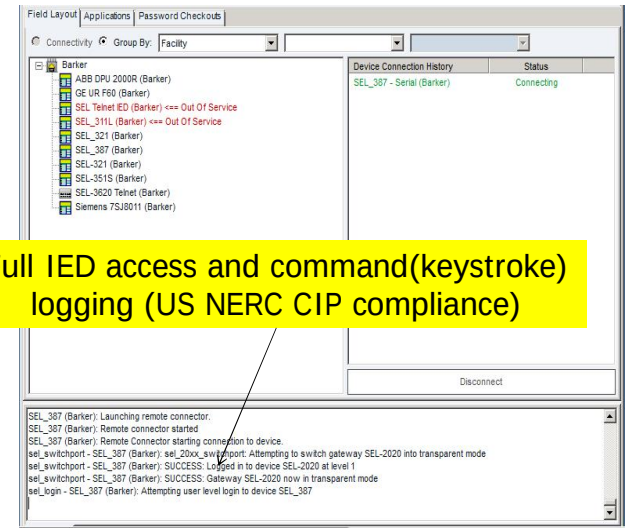
To do what by whatever means



To do what by whatever means

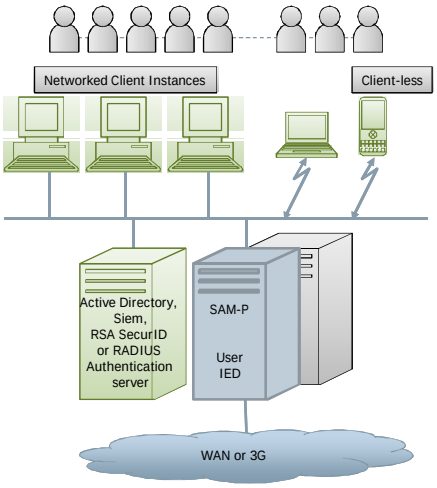


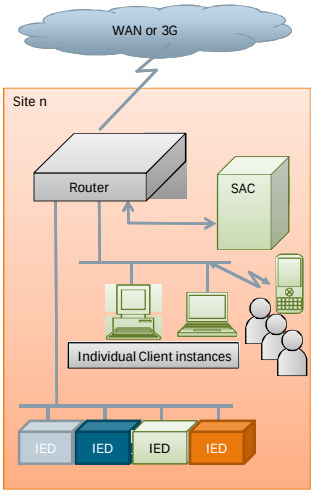
What have they done?



Full IED access and command(keystroke) logging (US NERC CIP compliance)

Architecture





Summary

- Resilient central and remote architecture
- Centrally managed Users
- Comprehensive user-specific RBAC mechanisms
- Centrally accessed with IED password obfuscation
- IED-type agnostic operation
- Enhanced management of ‘integrated’ IED

Further Information

Rodney Hughes
Business Development Manager
Industry / AU / IA SC

27 Greenhill Rd
Wayville
SA 5034
Australia

Mobile: +61 437 911 594

E-mail:
rodney.hughes@siemens.com

siemens.com/answers