

Security Guidelines for the Electricity Sector: Securing Remote Access to Electronic Control and Protection Systems

NERC	Guideline
Guideline Title: Securing Remote Access to Electronic Control and Protection Systems	Version: 1.0
Revision Date:	Effective Date: June 10, 2003

Purpose:

The purpose of this guideline is to describe recommendations for securing Remote Access associated with maintenance of Electronic Control and Protection Systems (ECPS) applicable to critical facilities. This guideline identifies some of the key elements associated with managing remote access to ECPS to help ensure reliability of the Electricity Infrastructure. For purposes of this guideline, maintenance includes fault data extraction, configuration, and diagnostics.

Applicability:

This guideline is focused on ECPS remote access other than that provided for by the primary exchange of real-time data and control signals.

This guideline is applicable to anyone who owns, manages, or maintains ECPS and/or services that support the Critical Electric Infrastructure.

A computer system environment is as critical as its most critical component and as vulnerable as its most vulnerable component.

Background:

ECPS control the systems that generate, transmit, and distribute electricity. For business reasons, it is necessary to provide a means for users to remotely access ECPS. Remote Access to these systems may require special considerations for security. Unauthorized Remote Access to an ECPS may result in interruption of electric service, damage to the elements of the electric grid, or a danger to life and property. ECPS vendors and other support personnel increasingly use Remote Access tools such as pcAnywhereTM, telnet, and FTP for support purposes directly over the Internet to the internal controls networks.

As a result, it is critical to preserve the security of the Remote Access to the ECPS. Authentication of the user is a critical element of the security policy.

Version Number: 1.0
June 10, 2003

Security Guideline:
Securing Remote Access to Electronic Control
and Protection Systems

Page 1 of 5

Security Guidelines for the Electricity Sector: Securing Remote Access to Electronic Control and Protection Systems

Definitions:

Electronic Control and Protection Systems:

Those systems used to regulate physical processes, including but not limited to: electronic protective relays, substation automation and control systems, power plant control systems, energy management systems (EMS), supervisory control and data acquisition (SCADA), programmable logic controllers (PLC). ECPS attributes include a Time Critical nature and automated response.

Remote Access:

Access to an ECPS by anything other than a directly connected operations system.

Includes, for example, the functions of administration, diagnostics, configuration, non-operator observation, and non-routine or infrequent control.

Includes, for example, applications such as telnet, SSH, and remote desktop software such as pcAnywhere™, Dameware™, VNC™. Currently available operating systems may natively include this type of functionality.

Includes all private and public telecommunications links, for example, dial-up modem, frame relay, ISDN, public switched telephone network, leased line, microwave, fiber optic, Internet, wireless.

Time Critical:

Involves a specific bounded time window within which one or more specified actions must be completed with some defined level of certainty.

Guideline Statement:

Effective and secure Remote Access controls are critical to protecting ECPS. Anyone who owns, maintains, or manages ECPS should have documented policies and procedures in place to manage authorization, authentication, and monitoring of remote access to such systems and devices. Such documentation should clearly define roles, responsibilities, and procedures for establishing authorization, and the methods selected for electronic access, authentication, and monitoring.

Version Number: 1.0
June 10, 2003

Security Guideline:
Securing Remote Access to Electronic Control
and Protection Systems

Page 2 of 5

Security Guidelines for the Electricity Sector: Securing Remote Access to Electronic Control and Protection Systems

The details included in this security guideline can generally be implemented with currently available technology.

Guideline Detail:

1. Policies and procedures governing use and installation of Remote Access for ECPS, including identifying responsible parties, should be established. These should be reviewed periodically and updated as required.
2. Remote Access should only be enabled when required, approved, and authenticated.
3. Multi-factor (two or more) authentication should be used. Factors include something “you know” (for example: passwords, destination IP address and/or telephone number), something “you have” (for example: token, digital certificate), something “you are” (for example: biometrics). Other factors may include: source IP address and/or telephone number, GPS location. These will make access more difficult for unauthorized users and will help to ensure identity of authorized Remote Access users.
4. Automatically lock accounts or access paths after a preset number of consecutive invalid password attempts. Consider automatically unlocking the account or access path after a pre-determined period of time or by other methods to ensure safe and reliable system operations.
5. Encryption should be used when traversing unsecured networks to gain Remote Access. This will help ensure confidentiality and integrity of any information transfer.
6. Approved Remote Access authorization lists should be established. These lists should be reviewed periodically and updated as required.
7. Change or delete any default passwords or User IDs. Consider using meaningful but non-descriptive IDs.
8. All Remote Access enabling hardware and software should be approved and installed in accordance with Policy. The location and specification of Remote Access enabling hardware and software should be documented and maintained in a controlled manner. Periodic audits should be conducted to ensure compliance.

Version Number: 1.0
June 10, 2003

Security Guideline:
Securing Remote Access to Electronic Control
and Protection Systems

Page 3 of 5

Security Guidelines for the Electricity Sector: Securing Remote Access to Electronic Control and Protection Systems

9. Remote Access connections should be logged. Logs should be periodically reviewed.
10. Consider risk to the process when allowing Remote Access and specifying hardware and software.
11. Policy considerations for Remote Access modems:
 - A. Change default settings as appropriate:
 - a. Set dial-out modems to not auto answer.
 - b. Increase ring count before answer.
 - c. Utilize inactivity timeout if available.
 - B. Change passwords periodically.
 - C. Use callback whenever possible.
 - D. Require authentication before connection.
 - E. Make maximum use of available security features.

Exceptions:

This security guideline does not pertain to real time transfer of data and control commands.

This security guideline does not address the integrity or confidentiality of the data on the device or of communications to the device.

This security guideline does not address measures to preserve the availability of the device (i.e., measures to protect against denial of service attacks).

There may be some legacy ECPS for which it is technically or economically infeasible to apply all of the specifics contained in this security guideline.

Related Documents:

Internet sites:

Electricity Sector Information Sharing and Analysis Center
(<http://www.esisac.com>)

The SANS (System Administration, Networking, and Security) Institute
(<http://www.sans.org>)

The Open Web Application Security Project (OWASP)
(<http://www.owasp.org>)

Version Number: 1.0
June 10, 2003

Security Guideline:
Securing Remote Access to Electronic Control
and Protection Systems

Page 4 of 5

Security Guidelines for the Electricity Sector: Securing Remote Access to Electronic Control and Protection Systems

The National Security Agency
(<http://www.nsa.gov/snac/index.html>)

The Center for Internet Security (CIS)
(<http://www.cisecurity.org>)

The National Infrastructure Protection Center
(<http://www.nipic.gov/publications/publications.htm>)

National Institute of Standards and Technology
(<http://csrc.nist.gov/publications/nistpubs/index.html>)

U.S. government's CIO Council
(<http://bsp.cio.gov/>)

The Cyber Emergency Response Team
(<http://www.cert.org/>)

Revision History:

Date	Version Number	Reason/Comments

Version Number: 1.0
June 10, 2003

Security Guideline:
Securing Remote Access to Electronic Control
and Protection Systems

Page 5 of 5