NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE. OF THE AMERICAS, NEW YORK, NY 10018 (212) 840-1070 FAX (212) 302-2782

May 26th, 2015

Subject: Open Process Posting of NPCC Directory#4 *System Protection Criteria*

Attached for your review and comment is a draft of NPCC Directory#4 *System Protection Criteria* which has been posted to the NPCC Open Process for a second 45 day comment period with additional revisions redlined to the first posting of the document.

During 2014 the NPCC Task Force on System Protection (TFSP) conducted a comprehensive review of Directory#4 and posted the document to the NPCC Open Process for an initial comment period which concluded on February 2nd, 2015.

The TFSP has considered Member comments received during the first posting and has made further changes to the document.

Specific changes included in the current draft as a result of comments received include:

- The addition of criterion 1.6.2.2.1 for facilities lacking two batteries or elements lacking two independent sets of protective relays.
- Additional clarity surrounding breaker failure criteria (5.2.3)
- Additional guidance regarding the use of capacitive voltage transformers.(Appendix A—Section 2.7.3)

The NPCC Open Process may be accessed through the following link:

https://www.npcc.org/Standards/SitePages/NonStandardsList.aspx

Comments on NPCC Directory#4 *System Protection Criteria* will be received for forty five days through July 10th, 2015and all comments will be addressed by the TFSP.

Please contact me with any questions regarding the NPCC Open Process review or the content of this document.

Thank you.

Gerry Dunbar
Northeast Power Coordinating Council, Inc.
212.840.1070 (p)
212.302.2782 (f)
gdunbar@npcc.org

NPCC, Inc.

NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

NPCC
Regional Reliability Reference Directory # 4
Bulk Power System Protection Criteria

Task Force on System Protection Revision Review Record:
Draft December 16, 2014
Draft May 13, 2015

2nd Open Process Posting
Redlined to 1st Open Process Posting (12/19/14 to 2/2/2015)

Adopted by the Members of the Northeast Power Coordinating Council, Inc. December 01, 2009 based on recommendation by the Reliability Coordinating Committee, in accordance with Section VIII of the NPCC Amended and Restated Bylaws dated July 24, 2007 as amended to date.

Revision History

Version	Date	Action	Change Tracking (New, Errata or Revisions)

Table of Content

References

1.0 Introduction

1.1 Title Bulk Power System Protection Criteria

1.2 Directory Number 4

1.3 Objective

The purpose of this Directory is to provide the **protection** criteria for **protection** of the **Bulk Power System** in NPCC Inc. member **Areas**. It is not a design specification.

1.4 Effective Date **Immediately upon Approval by the NPCC Full Members**

Compliance Guidance Statement- **Protection system** designs submitted to the TFSP prior to the date of this revision are not subject to the submittal requirements described in Section 6, Compliance Requirements R1, R2, and R3.

1.5 Background

This directory establishes the basic **protection system** design criteria and review process for **protection systems** for the **Bulk Power System**.

Guidance for consideration in the implementation of these criteria is provided in Appendix A, and the procedure for reviewing new and ~~revised~~modified **protection system**s is provided in Appendix B.

1.6 Applicability

The requirements of an NPCC Directory apply only to those facilities defined as NPCC **bulk power system elements** as identified through the performance based methodology of NPCC Document A-10, "*Classification of Bulk Power System Elements*," the list of which is maintained by the NPCC Task Force on System Studies and approved by the NPCC Reliability Coordinating Committee.

Requirements to abide by an NPCC Directory may also reside in external tariff requirements, bilateral contracts and other agreements between facility owners and/or operators and their assigned Reliability Coordinator, Planning Coordinator, Transmission Operator, Balancing Authority and/or Transmission Owner as applicable and may be enforceable through those external tariff requirements, bilateral contracts and other agreements. NPCC

will not enforce compliance to the NPCC Directory requirements in this document on any entity that is not an NPCC Full Member.

1.6.1 Functional Entities

Transmission Owners
Generator Owners
Distribution Providers

1.6.2 Facilities

1.6.2.1 New Facilities

These criteria shall apply to all new **Bulk Power System** (BPS) facilities.

1.6.2.2 Existing Facilities

It is the responsibility of individual companies to assess the **protection systems** at existing facilities and to make modifications which are required to meet the intent of these criteria as follows.

1.6.2.2.1 Facilities found lacking two batteries or **elements** lacking two independent sets of **protective relays**

If an entity becomes aware of an existing facility that lacks an independent battery for each **protection group,** or an **element** that lacks two independent sets of **protective relays**, a mitigation plan to meet the requirements of this Directory must be submitted to TFSP within six months. The mitigation plan shall correct these deficiencies within three years. Justification for a longer timeframe must be approved by TFSP.[1]

[1] A BPS Risk Mitigation Plan was put in place in 2010 based on a recommendation by the Task Force on System Protection following an extensive survey by NPCC member entities of their BPS protection system conformance to Directory No. 4 (Criteria A5 at the time). The purpose of this plan was to provide direction to separately mitigate the two attributes identified by TFSP as the highest risk to reliability namely the lack of two independent sets of protective relays or two batteries. At the time, members who owned protection systems that were subject to these high risk items were directed to provide a schedule to mitigate the identified deficiencies based on their original survey which occurred in 2009.

~~1.6.2.2.1~~1.6.2.2.2 Planned Renewal or Upgrade to Existing BPS Facilities

It is recognized that there may be portions of the **bulk power system,** which existed prior to each member's adoption of the *Bulk Power System Protection Criteria* (Directory 4 and its predecessor Document A-5) that do not meet these criteria. If **protection systems** or sub-systems of these facilities are replaced as part of a planned renewal or upgrade to the facility and do not meet all of these criteria, then an assessment shall be conducted for those criteria that are not met. The result of this assessment shall be reported to TFSP. It is recommended this reporting be in accordance with the procedure stipulated in Appendix B of this Directory and using the appropriate portion of the "**Protection System** Review forms", for review and disposition by the TFSP, or in a form consistent with the intent of the procedure.

~~1.6.2.2.2~~1.6.2.2.3 Facility Classification Upgraded to **Bulk Power System**.

These criteria apply to all existing facilities which become classified as **bulk power system**. A mitigation plan shall be submitted to TFSP for review to bring such a facility into compliance with these criteria.

Where the owner of the **protection system** has determined that the cost and risks involved to implement physical separation, as per Section 5.12, cannot be justified, the reason for this determination and an assessment shall be reported to the TFSP. It is recommended this reporting be in accordance with the procedure stipulated in Appendix B of this Directory and using the appropriate portion of the "**Protection System** Review forms", for review and disposition by the TFSP, or in a form consistent with the intent of the procedure.

2.23.3 **Load** responsive **protection relays** applied to transmission autotransformers should allow all possible loadability, consistent with equipment **protection** requirements.

2.24 Capacitor Banks

2.24.1 Each **protection system** should be designed to minimize the effects to the **bulk power system** of **faults** and **disturbances**, while itself experiencing a single failure.

2.24.2 Capacitor bank **protection** should be applied with due consideration for capacitor bank transients, **power** system voltage unbalance, and system **harmonics**.

2.24.3 **Protection** may be provided to minimize the impact of failures of individual capacitor units on the remaining capacitor units, however, these types of **protections** do not need to be duplicated:

a. Overvoltage **Protection**
b. Individual fuses for each capacitor unit
c. Overvoltage **Protection** for each capacitor units

2.25 Static Var Compensation (SVC) **Protection**

2.25.1 The low voltage branch circuits contain the reactive controlling equipment, filters, etc. These may include all or some of the following:

a. Thyristor Controlled Reactors (TCR)
b. Thyristor Switched Capacitors (TSC)
c. Switched or Fixed Capacitors
d. **Harmonic** Filters

2.25.2 **Protection** for the branch circuits that are not part of the **bulk power system** need not be duplicated. **Protection** for these branch circuits should be applied with due consideration for capacitor bank transients, power system voltage unbalance, and system **harmonics**.

2.25.3 **Protection** against abnormal non-**fault** conditions within the SVC via control of the TSC and TCR valves should be designed so as to not interfere with the proper operation of the SVC.

2.26 Logic System

2.26.1 The design should recognize the effects of contact races, spurious

operation due to battery grounds, dc transients, radio frequency interference or other such influences.

2.26.2 It is recognized that timing is often critical in logic schemes. Operating times of different devices vary. Known timing differences should be accounted for in the overall design.

2.27 Microprocessor-Based Equipment and Software

A **protection system** may incorporate microprocessor-based equipment. Information from this equipment may support other functions such as **power** system operations. In such cases, the software and the interface should be designed so as to not degrade the **protection system** functions.

2.28 Control Cable, Wiring and Ancillary Control Devices

Control cables and wiring and ancillary control devices should be highly dependable and secure. Due consideration should be given to published codes and standards, fire hazards, current-carrying capacity, voltage drop, insulation level, mechanical strength, routing, shielding, grounding and environment.

3.0 Guideline for Application of Remote Access to **Protection System**

The following guideline is established for the application of remote access to **protection system** Intelligent Electronic Devices (IEDs), such as relays, programmable logic controllers (PLC), and **teleprotection** equipment that have remote access capabilities, and are designed and configured for remote access applications.

This guideline assumes that appropriate physical measures are in place, and that they meet all applicable standards.

3.1 Definitions for Use in this Guideline Only

The flowing defined terms are used for illustration of the guideline presented in this Section only. These terms are not defined in Appendix A of this Directory, or any other NPCC documents.

PLC - Programmable Logic Controller, used to create and implement logical actions and automation.

Remote Access - accessing a device from a remote geographical area via a communications link; once accessed, provides similar local device functionality, at a distance.

Authenticate - to prove to be genuine or is an approved user.

Intrusion - An unauthorized electronic entry into an IED. Access normally provides user access to the functionality of the device.

Cryptography – is the study and application of codes and ciphers. Codes or encryption is used to transform data into a form that is not directly usable. Decryption transforms encrypted data using a decryption key back into the original useful form.

VPN – Virtual Private Network. It uses encryption to provide a private channel between private networks using a public network as its carrier i.e., two users using the Internet to provide confidentiality, integrity, and authentication.

3.2 Governing Principles

The industry has become more reliant on computer technology for power **system protection**, control, communications, and automation of its **power** system. Electromechanical and solid-state technologies are being replaced with microprocessor devices, offering, among other functions, local and remote communications access. **Protection system** IEDs are employed to protect, and or operate **bulk power system elements**. Unauthorized access to an IED could result in interruption of electric service, damage to the **power** system equipment, major **disturbances**, or a danger to life and property. **Protection system** IEDs also contain a large amount of information that utility personnel have come to rely on, including telemetry, power system **disturbance** analysis, **fault** location, preventive maintenance information, as well as asset condition and optimization data. However, this technology has also created vulnerabilities that are similar to those seen in traditional computer networks. Therefore, the following should be the governing principles of any cyber security program:

- Prevent penetration from cyber attacks.
- Prevent local and remote access to critical cyber assets by non-authorized personnel.
- Monitor cyber assets to detect unauthorized access or attempts to access.
- Limit exposure.

3.3 Guideline

3.3.1 Authentication

One of the foundations of the cyber security program is controlled, or secure, access. This dictates that some form of user authentication be used. Three common means of authenticating a user's identity are:

3.3.1.1 Something the user knows, such as passwords, or IP addresses.

3.3.1.2 Something the user has, such as a key, or cryptographic token.

3.3.1.3 Something the user is, such as fingerprints and voiceprints

At minimum, at least two factors of authentication should be used, e.g., passwords, and a destination – telephone number, or an IP address. The use of more factors such as encryption, etc. will result in providing more secure authentication. However, most present day and legacy **protection system** IEDs do not yet support this technology. Existing equipment often contains some level of security features. At a minimum, they usually provide multi-level passwords. These features should be activated as a first step in security implementation

3.3.2 Substation IED Access Point

A list of all substation IEDs that have remote electronic access configured should be compiled and maintained. This list should also include the access method(s) (e.g., dial-in, WAN, etc), the associated phone numbers and/or IP address, passwords, and other pertinent data.

3.3.3 Approved Remote Access Authorization List

A list of approved users, and the station IEDs they are authorized to access, should be established and maintained. It is vital that all such access information be classified as confidential, and managed as such.

3.3.4 Remote Access Configuration

Protection system IEDs should be configured to afford remote access only where needed and approved, and then, only when proper authentication is provided.

3.3.5 Password

Most **protection system** IEDs offer multiple access levels, each with separate passwords. Normally, a "view" only level is provided which allows a user to extract and or view information only. An alternate access level is provided to allow trained and authorized users to "make" settings and configuration changes, and initiate breaker operations. It is this level of access that is susceptible to an intrusion which could cause the most damage to the power system. Only limited users should have access to this level by considering the followings:

3.3.5.1 Establish multi-tiered passwords with different privileges for different classes of users.

3.3.5.2 Default passwords should be changed when remote access is configured.

3.3.5.3 Make sure that all IEDs have "strong" passwords, i.e., passwords that are not dictionary words, not easily guessable, not blank, or have no password at all. It is recommended that all passwords contain a combination of letters and numbers, and should be at least six characters long.

3.3.6 Logging/Alarming

When remote connections are used to access the relay beyond "view-only" mode, this should be alarmed and/or logged where possible.

3.3.7 Controlling Authority Approval

For both local and remote communications, excluding viewing, notification and approval of the Controlling Authority should be required to access in-service **protection system** IEDs. Only authorized users, as per Sections 3.3.3 and 3.3.5 above, should have remote access capabilities.

3.3.8 Disable User Function

Often, **protection system** IEDs are put into service with functions that are not used. These functions can create vulnerabilities, and therefore, should be disabled if possible.

3.4 Other Available Higher Level Authentication Factors and Some General Good Practices

As stated in Section 3.3.1, a minimum of two factors of authentication should be used. However, the use of more factors will result in providing more secure authentication. This Section is intended to provide additional factors and practices that could be implemented where warranted, and where the technology allows.

3.4.1 For WAN based access systems, implement Virtual Private Network (VPN) technology. VPN technology is also applicable when using ISDN, DSL, and cable.

3.4.2 Limit, as far as possible, dependence on the public telephone network for substation communications to IEDs. Instead, use secure communications facilities whenever possible.

3.4.3 Call back (where the IED device or modem hangs up on the original caller and calls back on a second line to a preconfigured phone number) may be utilized as a portion of an IED's security to prevent unauthorized access. This security measure added to other security measures will improve the IEDs security. Security can be further enhanced by using a different telephone line for the return call.

3.4.4 For dial-up modem access, use a hardware lock and key dongle on the analog phone line at each modem and the lock and key combination will act as a gatekeeper. When a call is initiated, the lock at the called modem will verify the existence of a valid key at the calling modem Time.

3.4.5 Isolation from the Business/Corporate Network

Isolation of the substation **protection system** IEDs from the Corporate Network should be provided where possible. Data can be transferred from the substation IEDs to a server connected to a Corporate Network via appropriate firewalls. This practice is warranted because most Corporate Networks are Internet connected and therefore are exposed to external users.

Appendix B
Procedure for Reporting to TFSP New and Modified Protection Systems

1.0 Introduction

As stated in Section 6.0 of this Directory, **"**an entity, proposing to install a new **protection system** or a modification to an existing **protection system**, shall submit documentation to TFSP" in accordance with this Appendix. Presentation should be made to the TFSP early in the engineering design stage.

2.0 Additional Requirements for Presentation and Review

2.1 As stated in NPCC Document A-10, Classification of **Bulk Power System Elements**, Paragraph 4.1, "within three months of an **element** being added to the **Bulk Power System** List, a plan and schedule for achieving compliance shall be provided to TFSP for review and acceptance. TFSP may require modifications to the proposed plan and schedule."

2.2 A presentation will be made to the TFSP on new facilities or a modification to an existing facility when requested by either a member entity or the TFSP.

2.3 A presentation will be made to the TFSP when the design of the **protection** facility deviates from the criteria set forth in this Directory.

2.4 A presentation will be made to the TFSP when a member entity is in doubt as to whether a design meets the **protection** criteria set forth in this Directory.

2.5 For specific relay replacement programs that largely follow the same design, a presentation will be made to the TFSP for the initial installation in full as described in Section 4.2. For subsequent installations in the program, only a Protection System Review Form and a cover letter referencing the program and initial presentation will be required.

3.0 Data Required for Presentation and Review of Proposed Protection Facilities

3.1 The **protection system** owner will advise the TFSP of the basic design of the proposed system. The data will be supplied on the "Protection System Review Forms" (formerly C-22 forms) as listed below, accompanied by a geographical map, a one-line diagram of all affected areas, and the associated **protection** and control function diagrams as well as network architecture drawings if applicable. A physical layout of **protection** panels and batteries for the purpose of illustrating physical separation will also be included. Physical layout drawings of cabinets located in the

substation yard housing protection system IED components will also be included if applicable.

- Protection System Details
- Line Relaying (Phase)
- Line Relaying (Ground)
- Transformer/Reactor Relaying
- Generator Relaying
- Bus Relaying
- Shunt Capacitors and Filters Relaying
- HVdc Converter Relaying
- Special Protection Systems
- Communication links
- Equipment Details
- Current Transformers
- Voltage Transformers
- Station Battery
- Physical Separation
- Breakers
- Disturbance Monitoring Equipment
- ~~Transmission Relay Loadability~~
- Exception Request

The proposed **protection system** will be explained with due emphasis on any special conditions or design restrictions existing on the particular **power** system.

4.0 Procedure for Presentation

4.1 The **protection system** owner will arrange to have a technical presentation made to the TFSP

4.2 To facilitate scheduling, the chairman of the TFSP will be notified approximately four months prior to the desired date of presentation.

4.3 Copies of materials to be presented will be distributed to TFSP members 30 days prior to the date of the presentation.

5.0 TFSP Procedures

5.1 The TFSP will review the material presented and develop a position statement concerning the proposed **protection system**. This statement will indicate one of the following:

5.1.1 The need for additional information to enable the TFSP to reach a decision.

5.1.2 Acceptance of the member statement of conformance to the **Protection** Criteria.

5.1.3 Acceptance of the submitted proposal

5.1.4 Conditional acceptance of the submitted proposal*.

5.1.5 Rejection of the submitted proposal*.

* Position Statements 4.1.4 and 4.1.5 which will include an indication of areas of departure from the intent of the **protection** criteria and suggestions for modifications to bring the **protection system** into conformance with the NPCC criteria.

5.2 The results of the TFSP review will be documented in the following manner in a letter:

5.2.1 A position statement, which will also be included in the minutes of the meeting at which the proposed **protection system** was reviewed.

5.2.2 If necessary, a letter will outline areas of nonconformance with the **protection** criteria stipulated in this Directory and recommendations for correction will be submitted to the **protection system** owner. If necessary, the matter will be brought to the attention of the RCC.

The Task Force will maintain a record of all the reviews it has conducted.