Document name	**Guideline for WECC Operations Network Node: Responsibilities and Procedures**
Category	( ) Regional Reliability Standard ( ) Regional Criteria ( ) Policy (X) Guideline ( ) Report or other ( ) Charter
Document date	December 3, 2012
Adopted/approved by	WECC Operating Committee
Date adopted/approved	02/08/2013
Custodian (entity responsible for maintenance and upkeep)	Data Exchange Work Group
Stored/filed	Physical location: Web URL:
Previous name/number	(if any)
Status	( ) in effect ( ) usable, minor formatting/editing required ( ) modification needed ( ) superseded by _____ ( ) other _____ ( ) obsolete/archived

Guideline for WECC Operations Network Node Responsibilities and Procedures

Prepared By

WECC Data Exchange Work Group

Version 1

December 3, 2012

Table of Contents

Purpose

The purpose of this document is to provide clear and consistent expectations to all users on the WECC Operations Network (WON).

Background

The WON was established to facilitate the exchange of operational data between Reliability Coordinators (RC), Transmission Operators (TOP), Balancing Authorities (BA), and other member utilities to facilitate exchanging power system reliability data. This network is a collection of connected entities that communicate over the WON to exchange power system-related data. This data includes analog values (e.g., bus voltages, line flows, generator outputs) and status information (e.g., circuit breaker statuses, switch statuses).

Access to the WON is granted only to members of WECC that have a reliability responsibility to the WECC interconnected electrical system that requires access to currently-approved, real-time power system data. Others may be granted a special exemption to these criteria at the discretion of the WECC Data Exchange Work Group (DEWG).

Security Responsibilities

All locations operating a WON connection shall employ all applicable standards and due diligence to protect the WON telecommunications infrastructure from unauthorized use or access. This includes the use of all applicable NERC Standards, other applicable standards, and industry-accepted practices.

All connected entities agree to comply with NERC CIP cyber security standards or, at a minimum, the WON Security Policy. The WON Security Policy may be referenced at the CIIMS document library at http://www.wecc.biz/committees/StandingCommittees/OC/CIIMS/Shared%20Documents/Forms/AllItems.aspx.

Data Handling

Data Source Considerations

The WECC RC requires all data as requested in the RC Data Request to be sent directly to the RC ICCP servers. That data is then relayed to a real-time database that is managed by the WECC RC (known as the Extra-high Voltage (EHV) Data Pool) and made available to any signatory of the WECC Universal Data Sharing Agreement (UDSA) on a request basis. Requests for all of the data the RC receives will require a project to build out additional servers and bandwidth as needed with the requestor responsible for all additional costs. Details regarding the current capacity of the EHV Data Pool and expenses related to build-out can be obtained by contacting the WECC RC.

Although it may be possible to use the EHV Data Pool as a "one stop shop" for data, WON users are encouraged to get data directly from the source where peer-to-peer connections exist. Although redundancy is in place to mitigate the risk of an unplanned outage, loss of the EHV Data Pool could result in a widespread loss of data for entities with a heavy reliance on this data source.

Data Requests

Data that is covered by the WECC UDSA can be shared by all signatories of that agreement, either peer-to-peer or through the EHV Data Pool. Requests to receive data through the EHV Data Pool should follow the procedures developed by the WECC RC. The documented procedures are available from the WECC RC.

Requests to receive data directly from another company should follow the procedures identified by the source company.

Timeliness of responses to requests for data set updates are often driven by a company's update cycle and therefore cannot be mandated. It is recommended that all requests for data be implemented within 10 business days.

Data Access Restrictions

Data that is covered by the WECC UDSA will be shared without restriction by all signatories of that agreement. This data shall be kept secret and protected from public or other unpermitted disclosure.

All data providers must ensure that they have no technical, resource, and/or license limitations that constrain data exchange to the WECC RC. The WECC RC, providing

data through the EHV Data Pool, must ensure it has no such limitations that constrain data exchange with all WON users.

Data Naming Conventions

The ICCP Object IDs for all data exchanged via the WON will adhere to the following naming convention:

- Each Object ID will begin with the unique four-character identifier, commonly referred to as the Utility Identifier. This unique prefix ensures globally-unique IDs for all data exchanged via the WON.

- The entire ID may not exceed 32 characters, containing capital letters (A-Z), numbers (0-9), underscores ('_'), or dollar signs ('$'). Other characters are not allowed due to Manufacturing Message Specification (MMS) restrictions.

The following data conventions also apply:

- Individual data points representing analog or status values should be defined with Virtual Manufacturing Device (VMD) scope.

- Analog values (MW, MV, KV, Hz, etc.) should be defined as RealQ (32-bit floating point with quality).

- Analog values that change frequently (MW, MV, KV, Hz) should be separated from infrequently changing values (schedule, Limits). Frequently changing values should be requested periodically; infrequently changing values should be requested by exception.

- Status values (breakers, switches,, etc.) should be defined as StateQ (status with quality).

- Status points should be placed in a separate dataset from analogs and requested by exception.

Quality codes

Quality of data is reflected in the quality codes transferred with the power system data and displayed to the end user. There are several issues related to the preservation of quality from the source EMS to the end user.

- Quality codes must be assigned in the source EMS. If a stand-alone ICCP node is being used, the EMS-assigned quality shall be implemented and transferred to the

ICCP node. The mapping of vendor-specific EMS quality codes to the ICCP quality codes is the responsibility of the source EMS.

- The receiving ICCP node is responsible for a similar mapping of the ICCP-defined quality codes into the target EMS vendor-specific quality codes.

- The receiving ICCP node is responsible for detecting the late arrival or the non-arrival of a dataset and is required to set the non-update flag in the quality codes of the associated power system data points.

- If a utility requires the additional security of being able to detect when data is arriving, but is not changing (and quality remains good), there are three recommended ways to accomplish this:

  1. A constantly changing analog or status point can be embedded into the dataset and checked at the target EMS. This requires the source EMS to create such constantly-changing points.

  2. The target EMS can develop the ability to scan incoming datasets and detect the fact that no point has changed in a given period of time.

  3. The change of value (COV) counter transmitted in the extended quality codes of specific points can be checked by the target EMS.

Change Management and Coordination

It is recommended that entities have formal agreements with data-sharing partners to specify how changes are to be communicated and coordinated. In the absence of formal agreements between companies, data owners should communicate changes prior to their implementation.

Testing and data checkout

It is the responsibility of the data recipient to coordinate testing. Testing and data checkout should be performed following the addition of new data or changes to existing data that affect state estimator solutions or real-time decision making. For data that is exchanged through the EHV Data Pool, data checkout should be conducted directly between the source company and recipient. The WECC RC should be called to validate EHV Data Pool data only when the data checkout is unsuccessful.

Node Outages

For planned momentary outages due to a failover or restart, the WECC RC must be notified via phone prior to the outage. Furthermore, it is recommended that WON users communicate planned outages to other data-sharing partners.

For planned outages of longer duration, the same notification recommendations apply. However, for longer outages, the notification should be sent at least 24 hours in advance.

For unplanned outages, the WECC RC must be notified via phone call as soon as possible. To ensure that system operators/dispatchers are immediately aware of this unplanned loss of ICCP data, a message should be sent via the WECCNet Messaging System.

Performance Requirements

WON users shall provide sufficient hardware, software, telecommunications, and other resources necessary to ensure reliable, accurate, and timely data exchange as required by the NERC Reliability Standards.

Redundancy Recommendations

It is recommended that all WON users provide redundant systems and connections to the WON. All system upgrades, expansions, and replacements should include the elimination of single points of failure.

Documentation Recommendations

It is recommended that each WON user have documented procedures for the support activities necessary to ensure reliable data exchange. At a minimum the following procedures and activities should be documented:

- Data maintenance and updates
- Testing
- System availability monitoring and measurement
- Troubleshooting

- EMS (real-time network applications) data-mapping standards

- Data-naming conventions

- Fault management (maintenance and display of error statistics)

- Alarm response

Trouble Response

Following the loss of a data link or other problems that result in the loss or degradation of data exchange between control centers, all efforts should be made to restore data exchange within one hour.

Dispute Resolution

Disputes arising over issues addressed in this document (e.g., data requests, trouble response times, outage notification) may be referred to the WECC Data Exchange Work Group (DEWG).

Glossary

WON Computer/Device – Any devices connected via TCP/IP networking to the WECC Operations Network

EHV Data Pool – A data repository of generation, flow, voltage, and frequency information on the whole Western Interconnected System provided for and by member companies via the ICCP data exchange protocol.

DEWG – The Data Exchange Work Group (DEWG) is responsible for supporting the data needs of the WECC Reliability Coordinator function and other entities identified by the WECC OC and for developing and overseeing methodologies to facilitate the exchange of real-time, modeling, and other operational data to help ensure reliable electric power system operations. The Data Exchange Work Group is a member group established by the Operating Committee (OC) and the critical Infrastructure and Information Management Subcommittee (CIIMS).

WECCNet Messaging System – A data messaging system used by WECC participating entities (e.g. Utilities, Reliability Coordinator), dispatchers and network administrators. The system is used to convey information related to WECC electrical system elements including, but not limited to; informational notices, outages, and emergency and abnormal conditions, as well as restorations.

Whitelisting – Application whitelisting is a methodology used to prevent unauthorized programs from running. The purpose is to protect systems from harmful applications. The whitelist is a simple list of applications that have been granted permission to run. When an application tries to run, it is checked against the list and, if found, allowed to run. Blacklisting, the opposite approach to whitelisting, is the method used by most antivirus programs.

WECC RC – WECC operates two Reliability Coordination Offices (RCO) that provide situational awareness and real-time supervision of the entire Western Interconnection.

UDSA – WECC's Universal Data Sharing Agreement (UDSA) was developed as part of the Western Interconnection Synchrophasor Program (WISP) in 2012 to provide a common data-sharing agreement for all WECC members.