NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Security Guideline for the Electricity Sector:

Time Stamping of Operational Data Logs

Preamble:

It is in the public interest for NERC to develop guidelines that are useful for improving the reliability of the Bulk Power System (BPS)[1]. Guidelines provide suggested guidance on a particular topic for use by BPS users, owners, and operators according to each entity's facts and circumstances and do not provide binding norms, establish mandatory reliability standards, or create parameters by which compliance to standards is monitored or enforced.

Purpose:

The purpose of this Guideline is to describe minimum recommendations for maintaining accurate time stamp indications for logged events on the bulk power system.

Applicability:

This Guideline is focused on all computer or microprocessor-based operational devices used to monitor, control, or analyze the bulk power system where accurate timing is required by the application. These applications include, but are not limited to, Power Plant Automation Systems, Substation Automation Systems, Programmable Logic Controllers (PLC), Intelligent Electronic Devices (IED), sequence of event recorders, digital fault recorders, intelligent protective relay devices, Energy Management Systems (EMS), Supervisory Control and Data Acquisition (SCADA) Systems, Plant Control Systems, routers, firewalls, Intrusion Detection Systems (IDS), remote access systems, physical security access control systems, telephone and voice recording systems, video surveillance systems, and log collection and analysis systems.

This Guideline does not specify where time stamping recorders or telemetry equipment should be placed within the bulk power system. Rather, this Guideline recommends the characteristics of the time stamps that are created by equipment that is selected and installed for other operational requirements.

[1] Note: For purposes of this document, the terms "Bulk Power System" and "Bulk Electric System" are considered to be identical. FERC, in Order 693, paragraph 75, states that for an initial period it will rely on the NERC definition of BES.

Version 0.995
Effective Date: TBD

Approved by:
Critical Infrastructure Protection Committee

This Guideline is not intended to require equipment upgrades to existing implementations. Rather, this Guideline is intended to assist in the configuration of time synchronization features on equipment that either already exists or is in the planning stages for upgrades and deployments.

This Guideline describes recommended minimum configurations that may be used unless a specific application requires greater accuracy or resolution. Where more stringent requirements may exist (e.g., in other company specific requirements, regional or NERC requirements such as the PRC-018-1 Disturbance Monitoring Equipment Installation and Data Reporting Standard) they take precedence over the precision as specified in this Guideline.

Background:

Proper time synchronization across Interconnections is a very important function for many reasons. As demands on the grid change, and the need for sophisticated information infrastructure increases, it will become more important than ever to ensure that events are accurately recorded and time-stamped consistently.

The distributed nature of the North American power grid makes time synchronization between each interdependent system a challenging task. The most effective means of maintaining consistent time stamping is for each entity to synchronize all equipment with an internal clock to a recognized reference point. The reference point should be a government certified and supplied source. The US Global Positioning System (GPS) service is widely recognized as a reliable and economical source for time synchronization and is available on the majority of the earth’s surface. Other appropriate sources are the WWV and WWVB radio time services provided by the US National Institute of Standards and Technology (NIST) or the CHU radio time service operated by the National Research Council of Canada.

Definitions:

Accuracy: The difference between the actual value of a measurement and the indicated value of the measurement. (IEEE definition from IEEE Std C37.1™-2007)
Accurate: Free from error; conforming exactly to a standard.

ACTS: **NIST Automated Computer Time Service**: A service provided by NIST for users who need to synchronize computer clocks to the correct time. When a computer connects to ACTS by analog telephone, it receives an ASCII (American Standard Code for Information Interchange) time code. The information in the time code is then used to set the computer's clock.

Atomic Time: a highly accurate time scale, currently based on the vibration of an “undisturbed” cesium atom, which is measured independently of the motion of the Earth.

CHU: Radio time service operated and maintained by the National Research Council of Canada at Barrhaven, Ontario (Canada) Radio 3330, 14670 and 7850 kHz.

Clock: The internal hardware and software that maintains time of day in a computer or intelligent microprocessor device. It is also known as a “real-time clock.”

Coordinated Time Synchronization Source: A hardware component or other device, generally local to control center, plant, or substation, that maintains an accurate time; traceable to a coordinated international standard time, and provides a time signal that can be used to synchronize the remaining devices at that location.

GPS: **Global Positioning System**: U.S.-owned utility that provides users with positioning, navigation, and timing services.. [2]

IDS: **Intrusion Detection System**: a computer device used in both physical and cyber security that detects and reports on unauthorized access attempts to a physical space (physical IDS), or a computer system or network (cyber IDS).

IRIG: **Inter Range Instrumentation Group**: A Department of Defense organization which developed a specification for transmission of time synchronization over wide areas. IRIG-B is one of several IRIG formats.

Leap Second: A second that is added to or subtracted from Atomic Time to produce Coordinated Universal Time (UTC) to make it agree with astronomical time to within 0.9 second. Astronomical time is based on the rate of rotation of the earth. Since atomic clocks are more stable than the rate at which the earth rotates, leap seconds are occasionally needed to keep the two time scales in agreement.

NTP: **Network Time Protocol**: A protocol used to synchronize computer clocks via a network connection. See IETF (Internet Engineering Task Force) RFC (Request for Comment) 1305.

Precision: The closeness of agreement of the results of repeated measurements carried out over a short period of time and under the same conditions. (IEEE Definition from IEEE Std 270™-2006)

PTP: **Precision Timing Protocol**: (**IEEE Std 1588**™): A protocol designed to increase timing accuracy over traditional Ethernet based protocols. PTP is formalized by IEEE Std 1588™-2008 “Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.”

Resolution: The smallest increment of time to which the measurement can be distinguished.

SNTP: **Simple Network Time Protocol**: A protocol used to accurately synchronize computer clocks via a network connection. SNTP can be used when the ultimate performance of the full NTP implementation is not needed or justified. See IETF RFC 4430.

Telemetry Skew: a term used to describe the observable fact whereby communication delays or scan rates cause the receipt of information to not occur strictly in “real time”. Also know as “clock skew” in the design of synchronous electronic circuits.

[2] Additional detail on the GPS may be found at http://www.gps.gov/systems/gps/index.html,

Time Client: A computer-based end-device which depends on a time server to provide a source for time. Time clients are generally application devices requiring accurate time for their application, but rely on a Time Server to provide that accurate time. Example time clients include: EMS, SCADA systems, IEDs, synchrophasors, Intrusion Detection Systems, firewalls, authentication servers, routers, and video recording systems.

Time Server: A computer-based source of accurate time. Time Servers will typically access GPS, WWV, WWVB, or CHU time signals, and produce a locally distributable time signal (such as IRIG-B, NTP, SNTP, or PTP) for use by the local Time Clients.

UTC: **Coordinated Universal Time**[3]: Sometimes called Greenwich Mean Time, UTC nominally reflects the mean solar time along the Earth's prime meridian.

WWV: Radio time service operated and maintained by the US National Institute of Standards and Technology (NIST) at Ft. Collins, Colorado (US) Radio 2.5, 5, 10, 15, 20 MHz.

WWVB: Radio time service operated and maintained by the US National Institute of Standards and Technology (NIST) at Ft. Collins, Colorado (US) Radio 60 kHz.

Glossary of Terms Used in Reliability Standards:

Please refer to the NERC *Glossary of Terms Used in Reliability Standards* for the formal definition of the following terms:

Interconnection
SCADA

Guideline Statement:

All specific geographic sites containing applicable devices should include a coordinated time synchronization source. This coordinated source should have a demonstrated availability appropriate to the application. Clocks on all applicable devices within the geographic sites should be synchronized with this source in a manner appropriate to the application.

[3] According to the NIST web site (http://tf.nist.gov/general/misc.htm), "In 1970 the Coordinated Universal Time system was devised by an international advisory group of technical experts within the International Telecommunication Union (ITU). The ITU felt it was best to designate a single abbreviation for use in all languages in order to minimize confusion. Since unanimous agreement could not be achieved on using either the English word order, CUT, or the French word order, TUC, the acronym UTC was chosen as a compromise."

Guideline Detail:

1.1. All specific geographic sites containing applicable devices (e.g., control center, power plant, substation) should include a coordinated time synchronization source. This coordinated service should have a demonstrated availability appropriate to the application.

1.2. The coordinated time synchronization source should be directly traceable to the international time standard maintained in the United States by the US Naval Observatory on behalf of the US Government, or the equivalent Canadian or Mexican government entity, and should have an accuracy of ±1 ms. Common government time services providing such a time signal include GPS, WWV, WWVB, and CHU.

1.2.1. Applications such as the logging of human actions (e.g., logging manual entry of values) which utilize time stamping only accurate to approximately ±10 ms may use the NIST Automated Computer Time Service (ACTS).

1.3. All applicable devices co-located at a specific geographic site should maintain communication to either a local coordinated time synchronization source, or a remote coordinated time synchronization source as defined in Guideline detail 1.2.

1.4. Time Zones

1.4.1. All applicable devices should internally store time using the UTC time zone or another time zone which is clearly identified and convertible to UTC.

1.4.2. Operational events that are logged to hard copy or screens, or events that are presented to operators may be displayed using the local or other relevant time zone, and may be represented to any resolution needed to properly operate the system, so long as the internal time stamps are maintained with the specified time zone and resolution as defined in preceding Guideline details

1.4.3. All operational events should be communicated and stored with time stamps. The time stamps should use the UTC time zone or another time zone which is clearly identified and convertible to UTC. If multiple time stamps are available for a given event, application requirements should determine which time stamp (or time stamps) should be stored for the event.

1.5. Utilities should use the most accurate protocols to implement time stamping capabilities suitable for the application. Specific standards exist for different classes of application and should be referenced. Some examples include NERC Reliability Standard PRC-018-1 or IEEE C37.118. (See the reference section of the Guideline for additional information on these references.)

1.6. The objective is for all applicable devices in an Interconnection to have an internal time that does not deviate from a time reference within the same Interconnection by more than ±128 ms. The rationale for this is to keep the maximum deviation between an in-specification slow clock and an in-specification fast clock to less than approximately one quarter second (±256 ms).

1.6.1. In situations where the end time 'clients' are unable to contact a time source, an accuracy within ± 256 ms should be maintained for up to 4 hours or until contact with the time source is restored.

1.6.2. Testing should be performed to ensure that these recommendations can be met.

1.7. Timestamp accuracy and resolution should be appropriate for the application. Some applications may need to support an accuracy and/or resolution of better than 0.1 ms. Sources of time uncertainty should be known and recorded.

1.7.1. When replaced, clock accuracy and resolution should be analyzed to ensure that the accuracy or resolution required by the application is achieved. Due to evolving application requirements, it may be necessary for replacement devices to have greater accuracy or resolution than the devices they replace.

Additional Considerations:

The distribution of time synchronization to applicable devices can be achieved in several ways; the most common distribution methods being IRIG-B (Inter Range Instrumentation Group – Format B) signaling across coaxial cables and the use of the Network Time Protocol (NTP) over Ethernet networks. Both NTP and SNTP (Simple Network Time Protocol) implement the same network protocols; however, the algorithms implemented for the client and server software are less sophisticated for SNTP, and have additional supported configuration limitations. (Refer to the RFC 1305 and RFC 1430 documentation for additional information. RFC documentation links are included in the Related Documents and Links section of this Guideline.)

Effective and accurate event logging is crucial to a reconstructed timeline following a disturbance event. Lack of a coordinated accurate time stamp for recorded events makes any reconstruction of a timeline difficult and time consuming, if not impossible. In addition, the lack of coordinated time stamping of events may cause the recorded event data to be suspect when it is used to reconstruct a timeline of events among systems of different management or administrative domains.

Of specific interest when collecting, storing and analyzing time stamp information is the concept of telemetry skew. Telemetry skew happens when communication delays or scan rates cause the receipt of information to not occur strictly in "real time". For example, in a system where the time stamp is not propagated, when a breaker in a substation opens, internal logging functions in the breaker controller or other monitoring equipment in the substation should capture the time associated with the operation. At some point later, perhaps several hundred milliseconds, the RTU (Remote Terminal Unit) may detect the breaker operation, and capture the time. Later, the SCADA central server will poll the RTU, and detect that the status point associated with the breaker has changed, and store an updated point value in the database, optionally with a time stamp. Then, the SCADA alarm subsystem will generate an uncommanded operation alarm, with an alarm time associated, and present it to the SCADA system operator. Even later, the breaker status may be communicated to other control centers, and upon receipt of the status point, the updated value will be stored, time stamped, and perhaps alarmed at the other control centers.

Each of these reported times will be different due to scanning rates, communication delays, and system processor loads and message queue lengths. It is conceivable that the total time deviation resulting from a telemetry sequence may exceed a minute. Of prime importance to the analysis of an event is the initial time stamp, which should be preserved for later analysis. Other time stamps may be used to determine when the succeeding systems identified that the point value was changed, but they will not be of primary use in developing an accurate electric system sequence of event timeline.

Electric utilities have relied on time stamping of critical events for many years. Initially, time stamping solutions were very expensive primarily due to the cost of establishing a timing signal at the site with the required accuracy. Now, with the GPS in place, the cost has been mitigated considerably by deriving actual time (traceable to a government standard) with an accuracy measured in microseconds from GPS signals. The IRIG B modulated signal produced by the time code receiver can be distributed to the equipment requiring the time signal by using coaxial cable or fiber optics. Most if not all equipment that would actually time stamp data or events (e.g. protective relays, sequence of events recorders, SCADA, RTUs, etc.) are equipped to accept the modulated IRIG B signal. Alternately, newer time code receivers producing IRIG B unmodulated signals have become more widely accepted as new products require higher time accuracy. Unmodulated signal accuracy on average can reach the level of ±100 nanoseconds while a modulated signal can reach an accuracy of ±50-100 microseconds at best. For applications requiring ultimate accuracy, the use of direct coaxial connections and termination at either the source or the load of the line is recommended. While both modulated and unmodulated IRIG B signals can be distributed using coaxial cable, unmodulated signals require shorter cable lengths to maintain higher accuracy. NTP/SNTP output is required for all network connected devices such as routers, firewalls, servers, IDS, etc.

When utilities implement time stamping, they should consider the capabilities of the time stamping functions and protocols, depending on the application.

Time Stamping Functionality – Standard Protocols & Formats

Some time stamping formats have been standardized, and others are in the process of development and standardization. Relevant formats are included in standards such as the IEEE Synchrophasor standard (C37.118) and the IEC-61850 (International Electrotechnical Commission) Utility Automation standard, and in documents such as IEEE draft standard PC37.239 Common Format for Event Data Exchange (COMFEDE) that utilizes the format described in C37.118 for its time stamp. Also referenced are IEC-60870 and DNP3 (Distributed Network Protocol Version 3) used for SCADA telemetry, and ISO-8601 (International Organization for Standardization) for the presentation of timestamps.

Within IEC-61850, the time stamp formats are defined in IEC-61850-7-2, clause 5.5.3.7, and in IEC-61850-8-1, clause 8.1.3.6. Note that IEC-61850 defines both a time stamp format (for data objects) and a separate entry time format (for event log entries and similar purposes). The Specific Communications Service Mapping in IEC-61850-8-1 defines different formats for time stamp and entry time. The Specific Communications Service Mapping in IEC-61850-9-2 references the timestamp and entry time definitions in IEC-61850-8-1. IEC-61850 time referenced to UTC based on seconds and fractions of seconds since 01/01/1970 (similar to DNP3). The resolution of IEC-61850 timestamps is to 1 part in 2^{24} of a second (binary fraction of a second) or about 60 ns. The IEC-61850 timestamps also indicate if they include leap seconds or not.

Within IEC-60870, time is defined in clause 6.8 of IEC-60870-5-4 and is used in IEC-60870-5-101, IEC-60870-5-102, IEC-60870-5-103 and IEC-60870-5-104. There are two absolute time formats, one of which is legacy and now rarely used, and a relative time format used for defining intervals. The IEC 60870 time stamps are "recommended" to be UTC time, but they also allow for the use of local time and the representation of "summer time" (i.e., Daylight Savings Time[4]) with a flag that indicates the time reported is "summer time". The resolution of IEC-60870 for both clocks and time tags is one millisecond.

DNP3 specifies time in "DNP3 Specification Volume 6: DNP3 Data Object Library." There are two DNP time formats, one absolute and one expressed as relative to an absolute time. The DNP3 time is defined as clock-face time in UTC, represented as a count of milliseconds since 00:00:00.000 01-Jan-1970, using the assumption of every second having 1000 milliseconds, every minute 60 seconds, every hour 60 minutes and every day 24 hours. This specifically means that it does not allow time stamping WITHIN the occasional leap second that is "added in" to keep the clock face and solar system in step. When that happens the minute has 61 seconds, but DNP3 calculates times as 60 seconds per minute every time. The resolution DNP3 for both clocks and time tags is one millisecond.

ISO Standard 8601 defines the international standard for the presentation of time. It describes how time is to be presented to a human, and includes provision for sub-second decimal presentation (e.g., to a tenth, hundredth, thousandth of a second).

[4] The term "summer time" is commonly used in Europe, Asia and Africa; "Daylight Savings Time" is used in the US. ISO standards use the more general term, rather than the US country specific term.

Leap Seconds

Based on lunar observations and with the advent of highly accurate atomic clocks astronomers and physicists[5] noticed that the atomic clocks did not exactly correlate with the observed time based on the position of the Earth relative to the Sun. Atomic clocks allow the keeping of very accurate time, however, this highly accurate time becomes out-of-step with the observed time in the natural world.

To make adjustments in the atomic time clock to agree with the observed world, a particular minute would adjust to contain either 61 or 59 seconds instead of the conventional 60 seconds. The particular minute, therefore, either has a positive or a negative leap second. Since UTC time correlates to the observed world, leap seconds are added to or subtracted from atomic time to produce UTC.
The first leap second was added on June 30, 1972. Since then (through the end of 2008), they have occurred at an average rate of less than one per year. Although it is possible to have a negative leap second (a second removed from UTC), so far, all leap seconds have been positive (an extra second has been added to UTC). Based on what we know about the earth's rotation, it seems unlikely that we will ever have a negative leap second.

By international agreement, UTC is maintained within 9/10 of a second of "solar" time. Thus, the introduction of leap seconds will permit a good clock to keep approximate step with Earth's rotation relative to the sun. Since the rotation of the earth is not uniform we cannot exactly predict when leap seconds will be added or deleted. When a leap second is necessary, an announcement is made at least several months in advance, and all leap seconds so far have been implemented on either June 30th or December 31st.

[5] As early as 1675, the first Astronomer Royal of England, John Flamstead, proposed that the earth's rotation rate might change from season to season. In 1695, British astronomer Edmond Halley noticed that the Moon was not where it was predicted to be in the night sky. Either the Moon's orbital calculations were wrong, or the Earth's rotation was slowing. After re-calculating the Moon's position, no calculation error was found; therefore, the Earth's rotation rate was slowing. In the beginning of the 20th century, American Astronomer Simon Newcomb concluded that observations of the Moon had been either ahead of or behind its predicted position.

With the development of atomic clicks in the 1950s, it became possible to more carefully study the changes in the Earth's rotation rate. It was observed during this study that the average day was about 16 ms longer than it was 1000 years before; the positions of the north and south poles "wander" from year to year producing a discrepancy as large as 30 ms per year; and seasonal variations based on warning of the Northern and Southern hemispheres (which contain different rations of land and water) amount to a few ms per year.

By 1967, the development of atomic clocks allowed physicists to determine the length of a second to a few billionths of a second, independent of the rotation of the Earth. This development lead to the creation of the Atomic Time scale and the Leap Second. Combining the highly accurate atomic time with inclusion of occasional leap seconds creates UTC time, which is highly accurate, but correlates with the observed world.

Additional information is available in the NIST Monograph *From Sundials to Atomic Clocks: Understanding Time and Frequency*. See the Related Documents and Links section for reference.

For example, a leap second was added on July 1, 1997. UTC was retarded by 1.0s (i.e., a second was added to UTC) so that the sequence of dates of the UTC markers was:

1997 June 30 23h 59m 59s
1997 June 30 23h 59m 60s
1997 July 01 0h 0m 0s

It should be noted that the advantage gained by using UTC (i.e., correlation to the observed world) must be balanced against the fact that simply subtracting the date of one event from date of another event does not provide the time difference between the two events. Any leap seconds that were added or subtracted between the two events must be taken into account when determining the time difference.

Global Positioning System (GPS) time is the atomic time scale implemented by the atomic clocks in the GPS ground control stations and the GPS satellites themselves. GPS time was set to zero at 0h 6-Jan-1980 and does not include leap seconds. The GPS protocol includes a correction which can be applied to the GPS time to produce UTC time. This correction is automatically transmitted by the GPS satellites once every 12½ minutes. Most GPS Time Servers apply this correction factor and provide a source of UTC time to their time clients.

Leap seconds can be problematic for the electric industry disturbance event correlation and sequence of events processing since, in theory, the leap second could be either negative or positive, causing the UTC timestamp of two events to not correctly indicate the order of the events, or the time difference between two events.

NIST ACTS

The ACTS dial-up time service provided by NIST only works with analog modems that use ordinary telephone lines. Digital modems, such as Digital Subscriber Line (DSL), cable and wireless modems cannot synchronize using ACTS. When a client computer connects to ACTS by analog telephone, it receives an ASCII time code. The information in the time code is then used to set the computer’s clock. The ASCII time code contains an on-time marker (OTM) code. Since the OTM is delayed as it travels from NIST to the client computer, ACTS sends it out 45 milliseconds early. This always removes some of the delay. Better results are possible if the user’s software returns the OTM to ACTS after it is received. Each time the OTM is returned, ACTS measures the amount of time it took for the OTM to go from ACTS to the user and back to ACTS. This quantity (the round-trip path delay) is divided by 2 to get the one-way path delay. ACTS then advances the OTM by the one-way path delay and the OTM changes from an asterisk to a pound sign (#). When the # sign appears, the time code is synchronized within a few milliseconds of UTC at NIST.

Reporting of Time Quality and Time Error

Within time stamp formats there are issues of how to report time quality. Factors include whether the clock itself is working, whether the device is synchronized to the clock, an indication of the time accuracy, and treatment of leap seconds. Examples of time accuracy reporting include providing an estimate of the error and providing an estimate of the time at which the device was last synchronized to the clock. For example, in the IEEE Synchrophasor standard, the time of last synchronization is used, with a range of up to about 10 seconds.

PTP – IEEE Std 1588™

Precision Time Protocol is a time-transfer protocol defined in the IEEE Std 1588™ standard. It has been developed to improve precision over current Ethernet protocols. Where the pervasive NTP can synchronize to within tens of milliseconds PTP has the ability to synchronize within tens of microseconds offering a significant increase in precision. The protocol functions autonomously discovering other PTP devices automatically thus maintaining synchronization even in a dynamic environment.

Although the protocol adds significant advantages, there are several factors that prevent wide adoption of PTP over NTP in Ethernet networks. The Precision Timing protocol also has limitations over Wide Area Networks (WAN's) and does not currently support encapsulation or authentication as is available with the Network Time Protocol. It is important to note that future versions of NTP could theoretically use the same hardware stamping techniques utilized in PTP to increase timing resolution but would have the same requirement for supporting hardware.

PTP is designed for *precision*, not necessarily *accuracy*. This distinction is one of the factors referenced above for adoption of PTP over wide-area links. A highly deterministic link may provide for precision, but not for accuracy; a non-deterministic link doesn't provide for either precision or accuracy.

The structure of PTP requires that for its use in any specific application, such as electric power, a companion standard called a "profile" must be developed. As of the writing of this Guideline, work on such a "profile" (IEEE Draft Standard PC37.238) for application of PTP to electric power is nearing completion within IEEE. Benefits and limitations of PTP for use in substations will depend on the issues identified and addressed in developing that standard. In addition, it is clear that new hardware would be required for supporting PTP, because most existing hardware does not contain that capability.

Possible Issues for GPS Based Time Reference Sources

It should be noted that almost all GPS based time reference sources operate on the Standard Positioning Service encoded signal that is available to the general public. There are two known issues:

a) A possibility exists that this signal may become purposely disabled under certain circumstances (see document reference "White House wants plans for GPS shutdown").
b) A possibility exists that this signal may be maliciously "spoofed"

Certain GPS time reference sources are able to receive the Precise Positioning Service encoded signal (see document reference “USNO NAVSTAR Global Positioning System”) with a Selective Availability/Anti-Spoofing Module (SAASM). The SAASM ensures that received GPS signal is genuine. This service is only available to select users.

While there is a possibility that a GPS satellite signal may be maliciously “spoofed”, some GPS based time reference receivers will perform “sanity” checking and will reject a signal that falls outside certain parameters.

GPS users are advised to discuss the available options with their equipment manufacturer should operation under the above conditions be desired. GPS users are also advised to have a suitable procedure available to manually override the time being produced as required. In the event that the GPS signal is lost or if the time reference is manually overridden, the accuracy of the time reference should remain as specified in Section 1.6 of this Guideline.

Issues on securing time synchronization protocols

NTP and SNTP protocols are used to synchronize computer clocks. By default these protocols are not secured, and older versions of NTP (prior to version 4) have few security mechanisms built in to protect against common vulnerabilities such as buffer overflow and packet manipulation, or authentication designed to protect against replay attacks. Because it is designed for a meshed network topology, NTP that is improperly configured to rely on a single master time source lacks the built-in failover capability and is vulnerable to failure of that master. SNTP was specifically designed for use in hierarchical ("tree") network topologies where a single master time source is used. Both protocols should be implemented with some form of authentication (PKI, manual keys, or IPSec), configured to prevent replay attacks.

Additional information on securing time synchronization protocols may be found in the reference articles “NTP Security” and “Security aspects of time synchronization infrastructure”.   See the Related Documents and Links section for reference.

Discussion of the NTP Epoch in 2036

The NTP V3 protocol provides 64-bit timestamps which consists of two parts: a 32-bit “seconds” part and a 32-bit “fractional second” part, giving NTP a timescale of 2^{32} seconds or 136 years. Since NTP uses an epoch (start date) of January 1, 1900 there will be a rollover in 2036 (1900 + 136 years = 2036). There are two different options for preparing your systems for this event in the future.

The first option is to check the clock settings on the systems. Since NTP uses the difference between timestamps, and not their absolute values, the wraparound is invisible to the system as long as the timestamps are within 68 years of one another (i.e., ½ of 136 years). If the clock is set to no earlier than the system build date then the likelihood of the relative span between timestamps exceeding 136 is negligible.

The second option would be to adopt timestamping systems and solutions that make use of the pending NTP v4[6] standard which would use 128-bit timestamps. Currently the IETF has taken over development of the standard from the RFC community and has stated:

> *The goal of this working group is to document NTPv4 based on the extensive work of the NTP community and to advance the standardization status of NTP. It is an explicit goal of this effort to have NTPv4 interoperate with the deployed base avoiding any backwards-incompatible changes.*

The use of 128-bit timestamping would mean the timescale would expand to 2^{64} seconds, or close to 585 billion years.

Additional information may be found in the references article “The NTP Era and Era Numbering”. See the Related Documents and Links section for reference.

Related Documents and Links:

Note: Documents listed herein with hypertext links are publically available at the time of publication by following the indicated links. All other documents are available by requesting them from the respective organizations.

August 14, 2003 Blackout: NERC Actions to Prevent and Mitigate the Impacts of Future Cascading Blackouts, February 10, 2004 available at http://www.nerc.com/docs/docs/blackout/BOARD_APPROVED_BLACKOUT_RECOMMENDATIONS_021004.pdf

”Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations,” U.S.-Canada Power System Outage Task Force, April 5, 2004 available at http://www.nerc.com/filez/blackout.html

Distributed Network Protocol Version 3: DNP3 Technical Specification, Volume 6: DNP3 Data Object Library

IRIG standards are issued by the Inter Range Instrumentation Group of the Range Commanders Council under the authority of the US Department of Defense available at https://wsmrc2vger.wsmr.army.mil/rcc/manuals/200-04/TT-45.pdf

IEC-61850 time synch format:

- IEC-61850-7-2:2003, Communication networks and systems in substations – Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI)

[6] See http://www.ietf.org/dyn/wg/charter/ntp-charter.html

- IEC-61850-8-1:2004, Communication networks and systems in substations – Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3

- IEC-61850-9-2:2004, Communication networks and systems in substations – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3

IEC-60870:

- IEC 60870-5-4:1993, Telecontrol equipment and systems – Part 5: Transmission protocols – Section 4: Definition and coding of application information elements

- IEC-60870-5-101:2003, Telecontrol equipment and systems – Part 5-101: Transmission protocols – Companion standard for basic telecontrol tasks

- IEC-60870-5-102:1996, Telecontrol equipment and systems – Part 5: Transmission protocols – Section 102: Companion standard for the transmission of integrated totals in electric power systems

- IEC-60870-5-103:1997, Telecontrol equipment and systems – Part 5-103: Transmission protocols – Companion standard for the informative interface of protection equipment

- IEC-60870-5-104:2006, Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles

IEEE Std 270™-2006 IEEE Standard Definitions for Selected Quantities, Units, and Related Terms, with Special Attention to the International System of Units (SI)

IEEE Std 1588™-2008: IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems

IEEE Std C37.1™-2007 IEEE Standard for SCADA and Automation Systems

IEEE Std C37.118™-2005, IEEE Standard for Synchrophasors for Power Systems

IEEE Draft Standard PC37.238: IEEE 1588 Draft Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications

IEEE PSRC Working Group report to the Relay Communications Subcommittee, Report on a Common Data Format for IED Event Data available at http://www.pes-psrc.org/h/H5-b_Report_IED_Sampled_Data_Draft4_1.pdf

Jespersen, James, Fitz-Randolph, Jane: From Sundials to Atomic Clocks: Understanding Time and Frequency, National Institute of Standards and Technology, Monograph 155, 1999 edition available at http://tf.nist.gov/timefreq/general/pdf/1796.pdf

NERC Glossary of Terms Used in Reliability Standards, April 2009, available at http://www.nerc.com/docs/standards/rs/Glossary_2009April20.pdf

NERC CIP Reliability Standards: http://www.nerc.com/page.php?cid=2|20. Refer to "Critical infrastructure Protection (CIP)" selection on page

NERC Reliability Standard PRC-018-1 Disturbance Monitoring Equipment Standard Installation and Data Reporting Standard available at http://www.nerc.com/files/PRC-018-1.pdf

"The NTP Era and Era Numbering" available at http://www.cis.udel.edu/~mills/y2k.html

"NTP Security" available at http://www.giac.org/certified_professionals/practicals/gsec/2115.php

RFC1305 and RFC4330 Network Time Protocol (NTP) and Simple Network Time Protocol (SNTP) http://www.ietf.org

"Security aspects of time synchronization infrastructure" available at http://securityvulns.com/advisories/timesync.asp

Standard ISO8601:2004 Data elements and interchange formats – Information interchange – Representation of dates and times

USNO NAVSTAR Global Positioning System available at http://tycho.usno.navy.mil/gpsinfo.html

"What time is it? The importance of time in networks" Cisco, October 2007 available at http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6602/prod_white_paper0900aecd806dab49.pdf

"White House wants plans for GPS shutdown" available at http://www.msnbc.msn.com/id/6720387/

Revision History:

Date	Version Number	Reason/Comments
Sept 2003	Version – 0.0.1	Initial draft.
	Version – 0.0.2	Updates.
	Version – 0.0.3	Added Telemetry skew comments
	Version – 0.0.4	Added non-proscriptive comments
Oct 2003	Version – 0.0.5	Shall to should; explain 150ms vs. 250ms time; add definition for forensic
Nov 2003	Version – 0.0.6	Added more non-proscriptive clarifying language

	Version – 0.0.7	PCSS TF Review
	Version – 0.0.8	Additional Review by PCSS TF
	Version – 0.9	Additional Review by PCSS TF, addition of IRIG
April, 2004	Version 1.0	Comments from CIPC, WECC, and DEWG
March, 2008	Version 1.01	Document Updated
June 1, 2008	Version 1.02	Document updated
July 8, 2008	Version 1.03	Additional Information added
July 28, 2008	Version 1.04	Additional information and clarification added
July 29, 2008	Version 1.05	Edits from Conference Call
August 4, 2008	Version 1.0.6	Post call edits – CSSWG Ballot version
August 13, 2008	Version 0.9	Final CSSWG Approved – sent to SGWG
November 7, 2008	Version 0.91	Updates based on CIP Review process
October, 2009	Version 0.990	Updates based on 9/29 conference call
October 7, 2009	Version 0.991	Updates based on 10/07 call
October 8, 2009	Version 0.992	Updates based on action items from 10/7 call
October 14, 2009	Version 0.993	Updates from WG via email
October 28, 2009	Version 0.994	Final updates from WG members
November 11, 2009	Version 0.995	Final cleanup for CIPC agenda package