NIST Special Publication 1500-203

Framework for Cyber-Physical Systems: Volume 3, Timing Annex

Version 1.0

Cyber-Physical Systems Public Working Group
Smart Grid and Cyber-Physical Systems Program Office
Engineering Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-203

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 1500-203

Framework for Cyber-Physical Systems: Volume 3, Timing Annex

Version 1.0

Cyber-Physical Systems Public Working Group
Smart Grid and Cyber-Physical Systems Program Office
Engineering Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-203

September 2017

U.S. Department of Commerce
Wilbur L. Ross Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

National Institute of Standards and Technology (NIST) Special Publication 1500-203

84 pages (September 2017)

NIST Special Publication series 1500 is intended to capture external perspectives related to NIST standards, measurement, and testing-related efforts. These external perspectives can come from industry, academia, government, and others. These reports are intended to document external perspectives and do not represent official NIST positions.

This document has been prepared by the Cyber-Physical Systems Public Working Group (CPS PWG), an open public forum established by the National Institute of Standards and Technology (NIST) to support stakeholder discussions and development of a framework for cyber-physical systems. This document is a freely available contribution of the CPS PWG and is published in the public domain.

National Institute of Standards and Technology Special Publication 1500-203
Natl. Inst. Stand. Technol. Spec. Publ. 1500-203, 84 pages (September 2017)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-203

Revision Tracking

Version	Date	Editor	Changes
1.0	20170914	David Wollman	First Release Version

Table of Contents

Table of Figures

Table of Tables

Acknowledgement

The National Institute of Standards and Technology (NIST) and the Cyber-Physical Systems Public Working Group (CPS PWG) would like to acknowledge the valuable leadership of the following individuals who helped guide the participants through the framework activity:

NIST Leadership:

Edward Griffor, David Wollman, Christopher Greer

Reference Architecture:

Industry Co-chairs:	Stephen Mellor, Shi-Wan Lin
Academic Co-chair:	Janos Sztipanovits
NIST Co-chair:	Abdella Battou

Security:

Industry Co-chairs:	Claire Vishik, Larry John
Academic Co-chair:	Bill Sanders
NIST Co-chairs:	Victoria Pillitteri, Stephen Quinn

Use Cases:

Industry Co-chair:	Stephen Mellor
Academic Co-chair:	John Baras
NIST Co-chair:	Eric Simmon

Data Interoperability:

Industry Co-chairs:	Peggy Irelan, Eve Schooler
Academic Co-chair:	Larry Lannom
NIST Co-chair:	Martin Burns

Timing:

Industry Co-chair:	Sundeep Chandhoke
Academic Co-chair:	Hugh Melvin
NIST Co-chair:	Marc Weiss

Additionally, NIST and the CPS PWG would like to express appreciation to all the participants from industry, government and academia that, through their generous donation of their intellect, experience and precious time, made this effort a success.

Executive Summary

The applications and benefits of *cyber-physical systems (CPS)* will be revolutionary and pervasive – this is evident today in emerging smart cars, intelligent buildings, robots, unmanned vehicles, and medical devices. Realizing the future promise of CPS will require interoperability between elements and systems, supported by new reference architectures and common definitions and lexicons. Addressing this challenge requires broad collaboration to develop consensus around key concepts and build a shared understanding of the underlying technologies. To this end, the National Institute of Standards and Technology (NIST) has established the CPS Public Working Group (CPS PWG), which is open to all, to foster and capture inputs from those involved in CPS, both nationally and globally.

The Public Working Group as initially organized comprised 5 subgroups: Vocabulary and Reference Architecture, Cybersecurity and Privacy, Data Interoperability, Timing, and Use Cases. The report of the Vocabulary and Reference Architecture subgroup, informed by the work of the other subgroups, is presented in an accompanying volume: *Framework for Cyber-Physical Systems, Volume 1: Overview*, NIST Special Publication 1500-201. The reports of the latter four of the subgroups are presented in an accompanying volume: *Framework for Cyber-Physical Systems, Volume 2, Working Group Reports*, NIST Special Publication 1500-202.

In Volume 2, the report of the Timing subgroup provides an overview of the Timing Aspect, presents the current status of, and needs for, time awareness in system elements of a CPS, discusses timing and latency in CPS, and describes special security issues that arise with respect to timing. This document, *Framework for Cyber-Physical Systems, Volume 3, Timing Annex*, NIST Special Publication 1500-203, presents additional content on timing in cyber-physical systems, to supplement information provided in Volume 2.

1 Introduction

This section provides an introduction for the document. It comprises the following:

- Section 1.1 provides a brief overview of cyber-physical systems.
- Section 1.2 describes the purpose and scope of the document.
- Section 1.3 explains the organization of the rest of the document.
- Section 1.4 provides an introduction to timing.

1.1 Overview

The applications and benefits of *Cyber-physical systems (CPS)* will be revolutionary and pervasive – this is evident today in emerging smart cars, intelligent buildings, robots, unmanned vehicles, and medical devices. Realizing the future promise of CPS will require interoperability between elements and systems, supported by new reference architectures and common definitions and lexicons. Addressing this challenge requires broad collaboration to develop consensus around key concepts and build a shared understanding of the underlying technologies. To this end, NIST has established the CPS Public Working Group (CPS PWG), which is open to all, to foster and capture inputs from those involved in CPS, both nationally and globally.

1.2 Purpose and Scope

The Public Working Group as initially organized comprised 5 subgroups: Vocabulary and Reference Architecture, Cybersecurity and Privacy, Data Interoperability, Timing, and Use Cases. The report of the Vocabulary and Reference Architecture subgroup, informed by the work of the other subgroups, is presented in an accompanying volume: *Framework for Cyber-Physical Systems, Volume 1: Overview*, NIST Special Publication 1500-201. The reports of the latter four of the subgroups are presented in an accompanying volume: *Framework for Cyber-Physical Systems, Volume 2, Working Group Reports*, NIST Special Publication 1500-202.

Volume 2 includes the report of Subgroup 4, Timing and Synchronization. This subgroup evaluated timing and synchronization needs of cyber-physical systems, including large-scale, distributed systems, and the subgroup included an existing organization, Time Aware Applications, Computers and Communications Systems (TAACCS), also led by NIST. The report of the Timing subgroup in Volume 2 provides an overview of the Timing Aspect, presents the current status of, and needs for, time awareness in system elements of a CPS, discusses timing and latency in CPS, and describes special security issues that arise with respect to timing.

This document, *Framework for Cyber-Physical Systems, Volume 3, Timing Annex*, NIST Special Publication 1500-203, presents additional information concerning timing in cyber-physical systems, to supplement content provided in Volume 2.

1.3 Organization of This Document

Beyond the introduction to timing in this section, this Framework document is organized as follows:

- Section 2: Managing Timing and Latency,
- Section 3: Timing Security and Resilience,
- Section 4: Timing Requirements (Use Cases), and
- Appendix A: References.

1.4 Introduction to Timing

This section provides an overview of selected timing concepts, definitions [1] and equations.

1.4.1 Timing signals

Every network element has a clock subsystem (often just called the “clock”), typically containing an oscillator that is used, with other phase-locked loops (PLLs) if necessary, to generate the various frequency signals (clock waveforms) used to clock the circuits in that system. The behavior of the network elements in terms of timing is that of this “master” clock subsystem since all other clock waveforms are derived from it. The most elementary of clock subsystems are based on free-running oscillators. More robust clock subsystems accept an external reference or derive a synchronization reference from a time signal interface. This reference is used to discipline the local clock and thus, to a large extent, the timing characteristics take on the attributes of this reference.

The Form of a Clock Waveform

The form of a clock waveform, especially pertaining to digital systems, is quite well known. In digital systems, clock signals are distributed to the various digital logic circuits and it is commonplace to visualize circuit state changes occurring at transitions of these clock signals. Figure 1 depicts a typical digital clock waveform, representative of a clock signal in a digital system. Whereas the physical (electrical) signal will have such attributes as rise-time, fall-time, overshoot, undershoot, and other such entities that make the actual (physical) signal different from the waveform depicted, the key attribute from a timing and synchronization perspective is the time instant representative of circuit action. Without loss of generality, one considers the rising edge of the waveform, as indicated in Fig. 1, as the time instant of interest. Such a waveform represents the essential physical attribute of a timing signal, namely the concept of an event in time (and space) representing an instant to which a time value is associated.

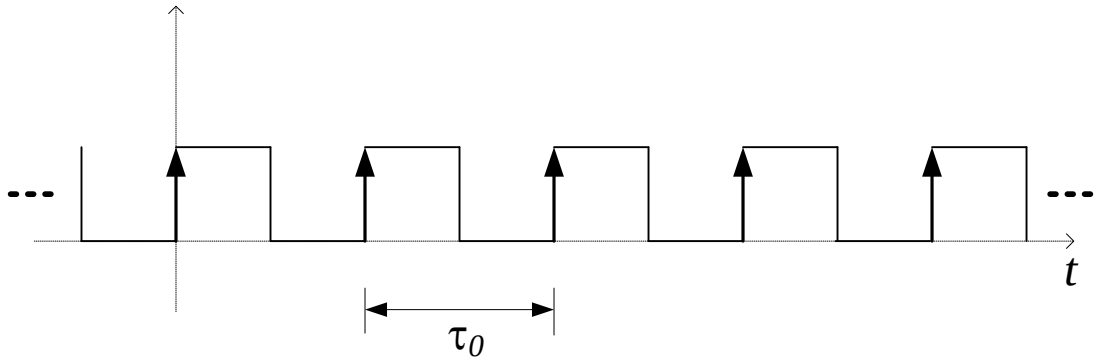


FIGURE 1. A GENERIC CLOCK WAVEFORM

An ideal clock waveform will be periodic. That is, the time separation between successive salient features (such as the rising edges of the waveform as chosen here) will be constant. In Fig. 1, the rising edges are separated by the time interval τ_0 (the units are usually seconds or some fraction, such as milliseconds, thereof); τ_0 is also the period of the ideal waveform. Implicit in this (periodic) mathematical model is that the waveform exists for all time, from $t = -\infty$ to $t = +\infty$. The frequency of the clock waveform is representative of the rate at which the salient features occur. In particular, for an ideal clock waveform the frequency, f_0 (sometimes referred to as the fundamental frequency when Fourier Series tools are employed), is given by Eq. (1)

$$f_0 = 1/\tau_0 \tag{1}$$

with units of hertz (Hz) for frequency and units of seconds for time.

The term frequency is used here to indicate the *rate* at which significant events occur. In the context of periodic signals, frequency is the reciprocal of the period and thus will have units such as Hz or kHz, etc. At other times the term "frequency" is used to indicate an offset, or error, rather than an absolute value, and the term can be taken as shorthand for "fractional frequency offset," as discussed later. Thus, when the frequency of a signal is expressed as 0 ppm (0 parts-per-million) then the rate of the signal is exactly equal to what is expected or desired. For example, if an oscillator has a "label frequency" of 1 kHz and its actual output signal is measured as 1.001 kHz, the frequency error is 1 Hz; expressed in fractional frequency units this corresponds to 10^{-3} or 10^3 ppm. It is then not uncommon to refer to the "frequency" of the signal as 10^3 ppm. There are some advantages in using the concept of fractional frequency rather than absolute rate. For example, if the oscillator output was multiplied up or divided down, the absolute rate and absolute frequency error would change accordingly but the fractional frequency error would remain 10^3 ppm.

The prototypical periodic waveform is the sinusoid. In fact, all periodic waveforms can be expressed as a linear combination of sinusoids (Fourier Series). Sinusoids have useful mathematical properties, including a compact mathematical form and consequently it is not uncommon to view a clock signal (even a "square wave" as in Fig. 1) as a sinusoid for purposes of analysis and for deriving certain results, because the key items of interest in a clock waveform pertain more to the zero-crossings, or other time instants of interest, rather than the specific wave-shape.

Consider the signal *w(t)* given by Eq. (2)

$$w(t) = A\cos(\Phi(t)) \tag{2}$$

where *A* is the amplitude of *w(t)* and $\Phi(t)$ is the "total phase function" (usually in units of radians). If *w(t)* is a simple (single) sinusoidal signal, then the phase function takes a particular form, namely that of Eq. (3)

$$\Phi(t) = \omega_0 t + \phi = (2\pi f_0)t + \phi \tag{3}$$

where ω_0 is the "angular frequency" expressed in radians per second and ϕ is the "initial phase" (a constant, often considered to be 0) in radians. This initial phase is dependent on the choice of mathematical time origin. The angular frequency can be related to a rate, expressed in units such as Hertz (Hz), f_0, via the factor of 2π. For a pure sine-wave ("single frequency"), the phase function is a linear function of *t* as expressed in Eq. (3). Since the cosine (and sine) functions have a period of 2π, *w(t)* will be periodic if $\Phi(t)$ is a linear function of *t* and the period will be τ_0 where τ_0 and f_0 are reciprocally related as in Eq. (1).

For a sinusoidal signal of the form given in Eq. (2), the "instantaneous frequency" (in units such as Hz or mHz or MHz, etc.), $\Psi(t)$, is defined as the derivative of the phase function

$$\Psi(t) = \frac{1}{2\pi} \cdot \frac{\partial}{\partial t}\left(\Phi(t)\right) \tag{4}$$

appropriately scaled (the factor of 2π addresses the conversion between rad/s and Hz).

Clearly, if $\Phi(t)$ is a linear function of *t* as in Eq. (3), then the instantaneous frequency is a constant (time-invariant) and equal to f_0. If $\Phi(t)$ is *approximately* a linear function of *t*, then one can obtain Eq. (5)

$$\Phi(t) = \alpha_0 + \omega_0 t + \phi(t) \tag{5}$$

where the first term, α_0, is a constant to establish the phase value at the chosen time origin. The term $\phi(t)$ then represents the deviation from pure sinusoidal behavior and has numerous connotations. In one sense, it represents *phase modulation*; in another sense, it represents *phase noise*; in yet another sense it represents *clock noise*. All these views are correct but are applied in different scenarios.

The instantaneous frequency can be written in Eq. (6) as

$$\Psi(t) = \frac{1}{2\pi} \cdot \frac{\partial}{\partial t}\left(\Phi(t)\right) = f_0 + \frac{1}{2\pi} \cdot \frac{\partial \phi(t)}{\partial t} = f_0 \cdot \left(1 + \frac{1}{2\pi f_0} \cdot \frac{\partial \phi(t)}{\partial t}\right) \quad . \tag{6}$$

The deviation from pure sinusoidal behavior, quantified by the term $\phi(t)$, introduces an instantaneous frequency offset (possibly time varying), say δf. From Eq. (6), one obtains Eq. (7)

$$\delta f = \frac{1}{2\pi} \cdot \frac{\partial \phi(t)}{\partial t} \quad \text{(units of Hz or mHz or MHz, etc.).} \tag{7}$$

The fractional frequency offset (from nominal), Δf, is defined in Eq. (8) as

$$\Delta f = \frac{\delta f}{f_0} = \frac{1}{2\pi f_0} \cdot \frac{\partial \phi(t)}{\partial t} \quad . \tag{8}$$

Fractional frequency offset is a dimensionless entity and is usually expressed in terms such as parts per million (ppm) or as a fraction such as 10^{-9}. Note that 10^{-9} is equivalent to 1 part per billion (ppb) and the fraction 10^{-6} is equivalent to 1 ppm. For example, 3×10^{-6} is 3 ppm.

Time Error (TE) and Time Interval Error (TIE)

For a practical clock waveform, the time separation between rising edges may not be constant across the whole waveform (i.e. over time). That is, practical clock waveforms are almost periodic or quasi-periodic. The time separation will be nominally T_0 with some deviation superimposed. These deviations constitute clock noise and, to a large extent, the analysis of clocks refers to the analysis of this clock noise or deviations from ideal behavior. Clearly, the frequency, as defined by Eq. (1) is appropriate for an ideal periodic waveform. For quasi-periodic signals, no one value of frequency can be provided since there is a time variance implicit in the statement that the time interval between rising edges is not a constant. Consequently, one introduces the concept of instantaneous frequency, and instantaneous frequency deviation (or instantaneous frequency offset), to quantify the time varying nature of "rate." When it is clear from the context of usage, the "instantaneous" qualifier is often dropped.

Considering that it is the time instants of a salient feature (such as a rising edge) that are the subject of interest, it is mathematically convenient to consider the ideal clock waveform as a train of pulses, each "pulse" representing one time period with the start of the pulse corresponding to the salient feature such as the rising edge or zero-crossing of the timing waveform. For a practical clock waveform, the rising edges of the practical clock waveform "almost" line up with the ideal waveform. Denoting by $p(t)$ the shape of an isolated pulse of the clock waveform, one can write Eq. (9) as

$$w(t) = \sum_{n=-\infty}^{n=+\infty} p(t - T_n) \tag{9}$$

where the salient feature, such as the rising edge, of the n^{th} clock pulse occurs at T_n. For the clock waveform shown in Fig. 1, $p(t)$ is a rectangular pulse of duration determined by the duty-cycle of the waveform. Note that this model permits the rising edges, or salient events, to be non-uniformly spaced in time. For periodic signals, the (ideal) spacing is uniform and the relevant time instant T_n is nominally an integer multiple of the period. The time error (TE) or (phase error) of the practical (quasi-periodic) clock waveform is defined by the sequence $\{x(n)\}$ as

$$x(n) = T_n - n\tau_0 \ . \tag{10}$$

That is, the time error is the deviation, in time units, of the rising edge of the practical clock (i.e., T_n) relative to the ideal clock (i.e., $n \cdot \tau_0$). The term "time error" is synonymous and interchangeable with the term "phase error;" the nomenclature "time error" is used here because the units are time units. In practical situations, one does not have an ideal clock as reference. Rather, one has two clock signals, and one is trying to analyze the behavior of one clock with respect to the other based on measurement data, whereby the time interval between corresponding rising edges is estimated using suitable test equipment. In this case, it is common to consider the "better" clock as "ideal."

The TE sequence, $\{x(n)\}$, is therefore a discrete-time signal (sequence) with underlying sampling interval τ_0 corresponding to a sampling frequency f_0. In many analyses associated with clocks and timing and metrology, the TE signal, $x(t)$, is introduced. The signal $x(t)$ represents the continuous-time (analog) signal corresponding to the discrete-time signal, $\{x(n)\}$. Provided all Fourier frequencies of interest are less than $0.5 \cdot f_0$, the two representations are theoretically the same.

One can define a time interval error sequence that is different from, though still related to, our definition of TE sequence/signal. In particular the time interval error sequence $\xi(i;n)$ is based on the time error $\{x(n)\}$ as in Eq. (10) and is defined by:

$$\xi(i;n) = x(i+n) - x(i) \quad . \tag{11}$$

The rationale for the definition in Eq. (11) is the following: If one is using the clock under study to measure the duration of an event that is nominally of duration $n \cdot \tau_0$ and starting at, nominally, $i \cdot \tau_0$, then $\xi(i;n)$ can be viewed as the observed measurement error.

It is common practice to disregard the initial phase term in the time error sequence. Particularly when the analysis relates to the frequency of the clock, as opposed to absolute time-of-day, the initial phase is not important. That is, one arbitrarily assumes that at the time origin ($n = 0$) the time error is zero. That is, $x(0) = 0$. With this in mind, the relationship between time error and time interval error can be established in Eq. (12) as:

$$x(n) = \xi(0;n) \quad . \tag{12}$$

Because of the close relationship between the two entities, it is not uncommon to use the terminology time interval error, or TIE, for the time error sequence as well. It will be clear from the context which entity is being referred to.

From a notational viewpoint, a discrete-time signal is denoted by $\{x(n)\}$ or $\{x_n\}$, implying that the time index is depicted directly in parentheses to provide the message that the independent variable is time. The use of subscripts is also common. Generally, the choice of notation is based on convenience.

The Time Error Signal

The time error sequence $\{x(n)\}$, can be viewed as a discrete-time signal corresponding to samples of an analog signal, $x(t)$, taken at the sampling rate f_0. This is the concept of the time error (analog) signal. Both $x(t)$ and $\{x(n)\}$ contain the same information. Having two viewpoints is solely a matter of convenience. Having both analog and discrete-time versions permits us to use a wide variety of analytical and mathematical tools. From the Nyquist Theorem, it is known that if the underlying analog signal, $x(t)$, is band-limited to frequencies below $(1/2)f_0$, then there is a one-to-one correspondence between the analog signal, $x(t)$, and the discrete-time signal, $\{x(n)\}$. Likewise, there is a one-to-one correspondence between the discrete-time signal $\{x(n)\}$ and the band-limited version of its analog counter-part.

It is known from experience that the time error signal generally occupies a small fraction of the overall bandwidth and its spectral support is typically limited to a small fraction of the sampling frequency, f_0. That is, it is generally a safe assumption that the highest (Fourier) frequency component of the time error signal is a small fraction (much less than ½) of the fundamental frequency f_0. In such situations, it is quite appropriate to under-sample the time error sequence. Thus, whereas each rising edge of the clock waveform occurs nominally at a (sampling) frequency f_0, the time error sequence can be maintained at a much lower sampling

rate. Very often the measurement is done at a reasonably high rate and the discrete-time signal low-pass filtered and then under-sampled.

The primary ideas underlying the time error are summarized in Fig. 2, below.

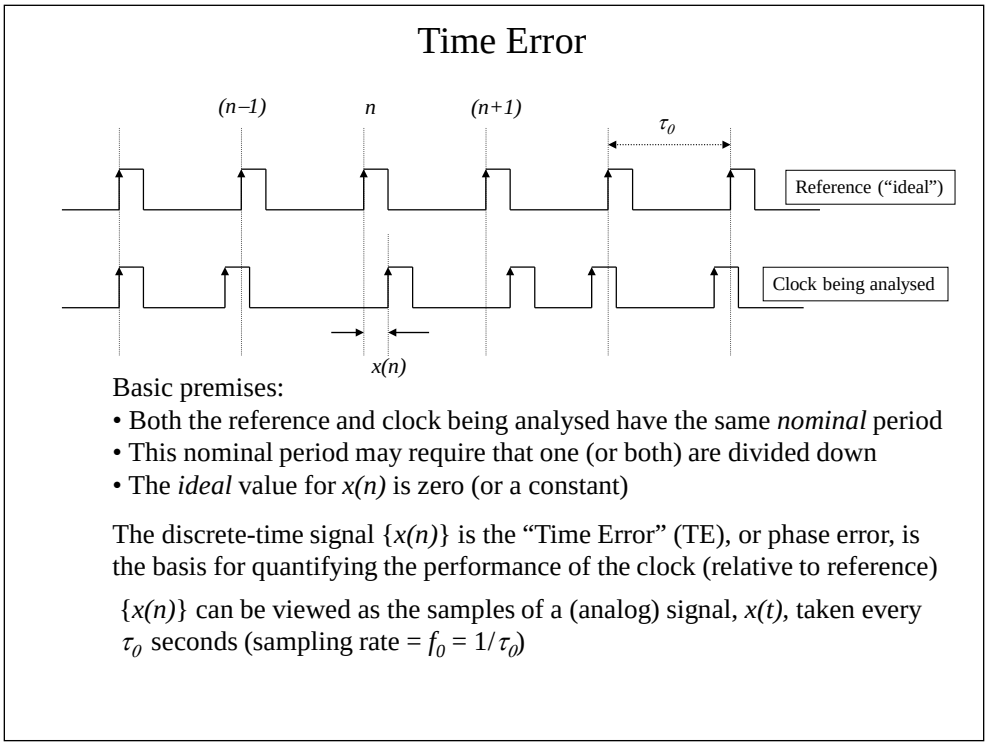


FIGURE 2. CONCEPT OF *TIME ERROR*

The accuracy and stability of the network element time-base is degraded by a number of factors. This is especially noticeable in a data network when the reference is derived from a traffic interface, from a signal that is transported from one point to another. The factors range from local temperature effects to accumulated jitter and wander in the transmission medium. The aim of network synchronization is to ensure that all the oscillators in a network are operating at the same rate or frequency. Because the clocks in a data network control the rate of bit transmission, data must be buffered to allow small differences in clock rates. Data arriving at a faster rate than a given clock eventually fill a buffer and can cause data to be dropped. This is called a data slip. Clock performance in a data network determines data slip performance. Better clocks or clock synchronization means fewer slips.

In order to take the mystery out of synchronization, it is important to understand some fundamentals regarding frequency and phase. Below is a short description of the most important parameters relating to the quality of clocks and network synchronization.

1.4.2 The Underlying Clock Error Model

The underlying model used in analyzing clocks and oscillators is discussed first. When two clock waveforms are compared, it is common to choose the time origin to coincide with the rising edge of the "ideal" clock. The rising edge of the clock being analyzed may not coincide with the ideal clock at the time origin. This is a deterministic time offset (often referred to as a phase offset) and is a constant that can be accounted for in a straightforward manner. Two other deterministic entities are included in the clock model. There could be an initial (at time $t = 0$) frequency offset, y_0, and the practical clock may also have a linear frequency drift, D. This drift term D is included because it is common in oscillators, particularly Rubidium frequency standards and quartz crystals, for the frequency to vary linearly with time, at least approximately. Generally, all other deviations are modeled as a random component, lumped together as $\varepsilon(t)$. There can be other deterministic terms, but the terms x_0, y_0 and D encompass the deterministic terms in a wide range of timing systems. That is, the model can be expressed in Eq. (13) in terms of a time error (or phase error) signal, $x(t)$, as

$$x(t) = x_0 + y_0 \cdot t + \tfrac{D}{2} \cdot t^2 + \varepsilon(t) \quad . \tag{13}$$

In practice, the "random" component is commonly modeled in terms of five noise types. These noise types are defined by their spectral behavior. "White" implies a flat spectrum; "flicker" implies a spectrum that falls off as f^{-1}; "random-walk" implies a spectrum that falls off as f^{-2}. Further subdivisions can be devised by considering processes in terms of "phase" and "frequency". Since frequency can be modeled as the first time-derivative of phase, and differentiation viewed in the power spectral domain corresponds to an f^2 factor, a spectrum (of phase) that falls off as f^{-2} can be viewed as a "flat" (or "white") spectrum for a frequency signal. The power spectrum, $E(f)$, of $\varepsilon(t)$, can be modeled in Eq. (14) as:

$$\begin{aligned} E(f) &= A_0 \cdot f^{0} + A_1 \cdot f^{-1} + A_2 \cdot f^{-2} + A_3 \cdot f^{-3} + A_4 \cdot f^{-4} \\ &= E_0(f) + E_1(f) + E_2(f) + E_3(f) + E_4(f) \end{aligned} \tag{14}$$

In Eq. (14) the component represented by E_0 has a flat spectrum and is considered "white phase noise;" the component E_1 is "phase flicker noise;" E_2 is "random-walk phase" or, equivalently, "white frequency noise;" E_3 is "frequency flicker noise;" and E_4 is "random-walk frequency." In practice, all these components are present to some degree but tend to dominate in different Fourier frequency ranges, if at all. At higher Fourier frequencies, the dominant component is usually white phase noise. As the Fourier frequency is lowered, the others tend to be (more) significant, proceeding from phase flicker noise to white frequency noise, to frequency flicker noise, to random-walk frequency. Clearly it is possible to postulate components with spectra that roll-off at higher (negative) powers of f. As for the deterministic terms of our model, these five encompass the stochastic noise of a wide range of systems.

There have been studies of other noise types with non-integer power laws. Yet these five power laws provide a complete picture in most cases.

The clock error model is related to the concepts of predictability and uncertainty. The two components of uncertainty are the deterministic and random contributions indicated in Eq. (13). In the absence of random error contributions, the future time error can be predicted if the current state and deterministic error components are known. However, the deterministic components are never known perfectly, hence there is a deterministic component of uncertainty. For example, when the communication path between the $clock_{master}$ and the $clock_{slave}$ of a two-way time transfer system, as discussed in section 1.4.5, has an unknown component of asymmetry, then the endpoints are unable to accurately establish the constant time error resulting from this asymmetry.

1.4.3 Extensions to Time (Time of Day)

Associated with each significant event, such as the rising edge of the waveform, there could be a label that represents "time." It should be emphasized that "time" is an artificial construct. One can consider a clock as a device that produces pulses with a desired periodicity and then associate a counter that counts these pulses and refer to the counter value as a "wall-clock" or "time-clock." The counter then represents the interval of time, as determined by the clock, elapsed relative to a chosen time origin. By suitable use of PLLs one can change the rate of the sampling clock without changing its inherent accuracy and thereby establish the count increment to any level of granularity desired. That is, one can count the number of seconds (milliseconds / microseconds / etc.) from the origin and thereby express "time" in suitable units such as seconds and minutes and hours and days and so on. Note that "time" implies a choice of time origin where "time = zero."

The concept of a "second" is defined in the International System of Units (Système International d'unités, SI) developed and maintained by the International Bureau of Weights and Measures (Bureau International des Poids et Mesures, BIPM), in terms of energy levels of Cesium atoms. Thus, a clock is accurate (in frequency) to the extent its rate agrees with the definition of the second. The clock is accurate as a wall-clock if it is traceable to Coordinated Universal Time (UTC) or International Atomic Time (TAI). TAI is the time-scale called International Atomic Time (Temps Atomique International), which is generated by the BIPM with the rate that best realizes the SI second, and the time origin determined by the transition to atomic time from astronomical time in 1958. UTC is considered "discontinuous" due to leap second adjustments. These are inserted into UTC to keep it within 0.9 seconds of UT1, the time scale linked with the astronomical time. Note that any real-time UTC or TAI signal is only a prediction of the exact value, since UTC and TAI are post-processed time scales [2]. The following table identifies some of the time-scales in use and the choice of time origin (epoch).

Table 1: Various Time-scales in Use

Time-scale	Epoch	Relationship	Leap Seconds	Comments
TAI	Jan. 1, 1958	Based on SI second	No	Continuous
UTC	Jan. 1, 1972	TAI – UTC = 37 s*	Yes	Discontinuous
UT1	Jan. 1, 1958	Earth's rotation	No	Astronomical
GPS	Jan. 6, 1980	TAI – GPS = 19 s	No	Continuous
LORAN-C	Jan. 1, 1958	UTC + 27 s	No	Discontinuous
Local	Jan. 1, 1972	TAI – UTC = 37 s*	Yes	Discontinuous; based on time-zone offset
PTP	Jan. 1, 1970	TAI – PTP = 10 s	No	Continuous
NTP	Jan. 1, 1900	UTC	Yes	Discontinuous

*As of December 31, 2016.

The clock error model of Eq. (13) is still appropriate. Furthermore, when comparing two different continuous time-scales, the difference in time origin can be absorbed into the constant term x_0.

It is worth noting:

- Since a clock is a frequency device, the best clocks will exhibit only white noise in frequency and hence a random walk in phase. Even the best clocks will walk off relative to each other unboundedly in time.
- Since the time standard is artificial, time must be transferred from the relevant time standard.
- There is often confusion with the human experience of time vs. metrological time.
- Standard "time" is a signal, that identifies an instant, plus data that provides the (time) label pertinent to that instant.
- Often what is needed is synchronization among locations, not UTC per se, though that is often the most efficient way to achieve synchronization.

1.4.4 Definitions and Metrics

The concept of metrics, in the context of clocks, relates to quantitative assessments of the clock error. Specifically, with respect to the clock model of Eq. (3), metrics refer to estimates of the "strength" of the different components of the clock error model. In most cases, it is not possible to completely separate the different components, and so the validity of estimates of one component can be affected by the presence of another.

Calculation of the metrics, or estimates of the strength of the different components is done on a time error sequence. This sequence is obtained from measurement and thus is always of limited duration, say N samples. The underlying sampling interval associated with the measurement is usually denoted by τ_0. This sequence can also be viewed as the samples of the time error signal, $x(t)$, taken at a sampling rate of $f_0 = 1/\tau_0$.

Constant Time Error

The concept of constant time error is similar to the "dc" component of error or "pedestal". In terms of the clock error model, Eq. (13), the term x_0 can be viewed as the constant time error. As recommended in ITU-T Rec. G.8260 [3], an estimate for the constant time error is obtained by taking the average of the time error sequence. In the presence of a frequency offset (non-zero y_0) or frequency drift (non-zero D) such an average is not meaningful. Assuming the random component is white-noise phase modulation (PM), the estimate is improved by increasing the interval over which the average is computed. If the noise is not white PM then averaging may or may not be effective and in the case of significant random-walk PM (or higher-order noise processes) increasing the averaging interval could be counter-productive. The following is extracted from ITU-T Rec. G.8260 [3]:

> *Constant time error estimate*: Given a time error sequence $\{x(n); n = 0,1,\ldots,(N-1)\}$, an estimate of the constant time error is the average of the first M samples of the time error sequence. M is obtained from the observation interval providing the least value for TDEV as computed for the given time error sequence. If a frequency offset is present, then a linear regression method in accordance with Appendix II of [ITU-T Rec. G.823] can be applied.

Frequency offset

The concept of "frequency offset" is essentially the rate of change of time error. It is nominally equal to the term y_0 in the clock error model, Eq. (13). A frequency error sequence can be constructed in the following manner, in Eq. (15):

$$y(i;n) = \frac{x(i+n)-x(i)}{n\cdot\tau_0} \quad . \tag{15}$$

In Eq. (15), the frequency estimate is established over a time interval of $\tau = n\cdot\tau_0$ and pegged to the i^{th} sample of the time error sequence. The constant time error component, x_0, is removed by the differencing operation.

The average value of $\{y(i;n)\}$ taken over the data is an estimate of y_0. In the absence of any higher order terms in the clock error model ($D \equiv 0$ and $\varepsilon(t) \equiv 0$) the average value will indeed

be equal to y_0 and somewhat independent of $\tau (= n \cdot \tau_0)$. The (frequency) stability of the clock is a quantitative measure of the variability of this frequency estimate.

AVAR, MVAR, TVAR (ADEV, MDEV, TDEV)

Two common measures for the stability of the frequency are the Allan Variance (AVAR) and the Modified Allan Variance (MVAR). The basis for the metrics commonly used for stability is the observation that if the clock is stable, the quantity $\upsilon(i;n)$ is given in Eq. (16)

$$\upsilon(i;n) = y((i+n),n) - y(i;n) \tag{16}$$

and will be small, ideally zero. It is clear that $\upsilon(i;n)$ is the difference between two measurements of the time interval error for an observation interval $\tau = n \cdot \tau_0$ taken over adjacent, contiguous, periods of time. The time error value $x(i+n)$ is common to the two measurements. Then, Eq. (16) can be rewritten in Eq. (17) as

$$\upsilon(i;n) = \frac{x(i+2n) - 2 \cdot x(i+n) + x(i)}{n \cdot \tau_0} \quad . \tag{17}$$

Stability metrics are essentially measures of the variance (or standard deviation) of this quantity. A smaller value indicates greater stability. The Allan Variance (AVAR) is an estimate of the mean-squared value of $\{\upsilon(i;n);\ i = 0,1,2,\ldots,(N-1-2n)\}$ and can be evaluated by the expression in Eq. (18)

$$\sigma_y^2(\tau)\Big|_{\tau=n\tau_0} = \frac{1}{2} \cdot \left(\frac{1}{\tau^2}\right) \cdot \left(\frac{1}{N-2n-1}\right) \cdot \left(\sum_{i=0}^{N-2n-1} \left(x(i+2n) - 2x(i+n) + x(i)\right)^2\right) \tag{18}$$

for which the leading factor of (1/2) in the expression is a scaling factor for normalization.

The Modified Allan Variance (MVAR) is computed by first taking an n-point average of $\{\upsilon(i;n)\}$ prior to computing the mean-squared value. The expression for evaluating MVAR can be written in Eq. (19) as

$$\mathrm{mod}.\sigma_y^2(\tau) = \frac{1}{2} \cdot \left(\frac{1}{\tau^2}\right) \cdot \left(\frac{1}{N-3n+1}\right) \cdot \sum_{j=0}^{N-3n} \left(\frac{1}{n} \cdot \sum_{i=j}^{n+j-1} \left(x(i+2n) - 2x(i+n) + x(i)\right)\right)^2 \quad . \tag{19}$$

The metrics AVAR and MVAR, viewed as functions of the observation interval τ, can provide guidance as to the dominant noise process.

An alternative view of MVAR, which is dimensionless, is a metric with time units called the Time Variance, TVAR, related to MVAR in Eq. (20) as

$$(TVAR): \sigma_x^2(\tau) = \frac{\tau^2}{3} \cdot \left(\mathrm{mod}.\sigma_y^2(\tau)\right) \tag{20}$$

where the factor of (1/3) is a scaling factor for normalization.

It is common practice to use the root mean square, "rms," viewpoint of strength rather than power, or, equivalently, standard deviation rather than variance. Associated with AVAR, MVAR, and TVAR are corresponding "deviations" ADEV, MDEV, and TDEV, which are simply the square root of AVAR, MVAR, and TVAR, respectively.

It has been found that the instability of most frequency sources can be modeled by a combination of power-law noises having a spectral density of their fractional frequency fluctuations of the form $S_x(f) \propto f^{\beta}$, where f is the Fourier or sideband frequency in hertz, and β is the power law exponent, as in Table 2 below. The fractional frequency offset power spectrum, $S_y(f)$, is closely related to the time error power spectrum, $S_x(f)$, and also follows a power-law model, $S_y(f) \propto f^{\alpha}$. Generally speaking, $\alpha = \beta + 2$. The τ-domain (τ is the observation interval) variances also follow a power law of the form $\sigma_x^2(\tau) \propto \tau^{\upsilon}$ and $\sigma_y^2(\tau) \propto \tau^{\mu}$ [4]. The τ-domain variances can be recognized as TVAR and MVAR (corresponding to standard deviations TDEV and MDEV).

Table 2: Power Law Spectra for Different Noise Types

	$S_x(f) \propto f^{\beta}$	$S_y(f) \propto f^{\alpha}$	$\sigma_x^2(\tau) \propto \tau^{\upsilon}$	$\sigma_y^2(\tau) \propto \tau^{\mu}$
Noise Type	β	α	υ	μ
White PM (WhPM)	0	+2	–1	–2
Flicker PM (FlPM)	-1	+1	0	–2
White FM (WhFM)	-2	0	+1	–1
Flicker FM (FhFM)	–3	–1	+2	0
Random Walk FM (RWFM)	–4	–2	+3	+1
Flicker Walk FM (FWFM)	–5	–3	+4	+2
Random Run FM (RRFM)	–6	–4	+5	+3

PM stands for phase modulation and FM stands for frequency modulation. Note that in other published material the spectrum analysis is often performed on $Sy(f)$, the power spectrum of

$\{y(n\tau_0)\}$, the fractional frequency offset but the relationship between the two is straightforward. The last two categories, namely Flicker Walk FM and Random Run FM are special cases and included here for completeness. Also note that the Allan Variance does not distinguish between WhPM and FlPM whereas this distinction can be made via MVAR (or TVAR).

MTIE

The acronym MTIE stands for "**m**aximum **t**ime **i**nterval **e**rror" and is represented as a function of the observation interval, τ. The implication of MTIE(τ) is the maximum phase (in time units) offset between the clock being analyzed and the reference clock (which is considered "ideal") over ***any*** interval of duration τ. Equivalently, it represents the maximum peak-to-peak time deviation over ***any*** interval of duration τ. Sometimes, the term MRTIE, for "**m**aximum **r**elative **t**ime **i**nterval **e**rror" or *relative*-MTIE, is used when comparing two clocks, usually when neither can be considered "ideal." In simplistic terms, MTIE is a measure of the difference in the number of rising edges of the two clocks in an interval of duration τ. This measure is provided in units of time. That is, MTIE is expressed in seconds (or subdivisions such as nanoseconds or microseconds). A precise definition of MTIE is provided in Eq. (21), below.

$$MTIE(\tau = n \cdot \tau_0) = \max_{i=0}^{N-n} \left\{ \max_{k=i}^{k=i+n-1} \left(x(k)\right) - \min_{k=i}^{k=i+n-1} \left(x(k)\right) \right\} \tag{21}$$

It can be easily seen that the inner parentheses in Eq. (21) represents the peak-to-peak phase deviation over an interval of $\tau = n \cdot \tau_0$ starting with time index i. Note from the definition of time interval error, that the peak-to-peak phase deviation within an interval, A, is the largest time interval error that can be observed for all sub-intervals that are contained within A. The MTIE value is just the maximum of this peak-to-peak deviation over the entire data set, essentially considering all possible intervals of duration $\tau = n \cdot \tau_0$.

An alternate formulation, although not as intuitive as Eq. (21), is Eq. (22)

$$MTIE(\tau = n \cdot \tau_0) = \max_{i=0}^{N-n-1} \left\{ \max_{k=1}^{k=n} \left[\left| x(i+k) - x(i) \right| \right] \right\} \quad . \tag{22}$$

One source of error in digital transmission is additive noise, whereby the additive noise causes the receiver to misinterpret the received (noisy) waveform as a "1" when the actual transmitted information was a "0", and vice versa. Significant attention is paid to the signal-to-noise ratio provided by a transmission link, and methods to mitigate bit-errors such as error correcting codes may be employed to improve the effective signal-to-noise ratio to acceptable levels. A second source of error, much less benign than a bit-error, is the result of inadequate

synchronization. In every digital network element, the received bit-stream is buffered, the write-to-buffer operation controlled by the receive clock and the read-from-buffer operation controlled by the internal clock of the network element. If these two clocks are not identical, then there is the distinct possibility of observing buffer overflow (write frequency high) or underflow (read frequency high). Buffer overflow/underflow involves the loss/repetition of a block of data of length corresponding to the buffer size. The deleterious impact of buffer overflow/underflow is significantly more malignant than an occasional bit error. Fortunately, proper attention to synchronization, in particular between the read and write clocks, can mitigate this problem or, at least, reduce the impact to permissible levels.

The MTIE metric is especially useful in dealing with buffer size problems. In particular, if it is known that the least interval of time allowed between buffer overflow/underflow events is τ, then MTIE(τ) identifies the buffer size (in time units) required to achieve this specification. Conversely, if the buffer size is established (from other considerations) as B (time units), then the clocking must be engineered to ensure that MTIE(τ) < B. A summary of the key underlying premise of MTIE is provided in Fig. 3, below.

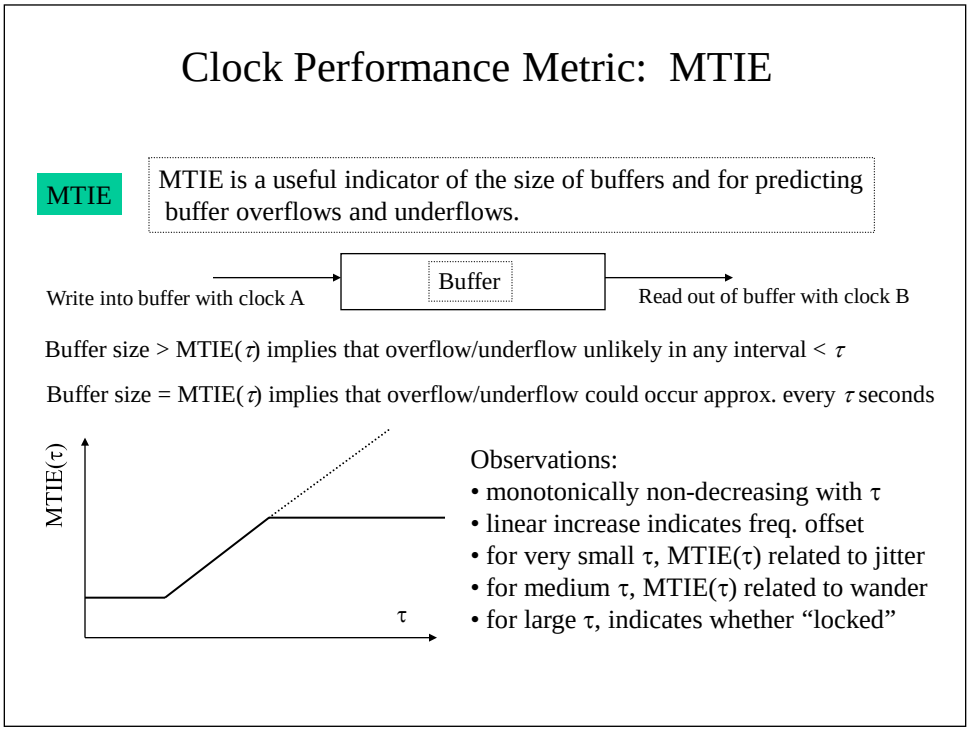


FIGURE 3. UNDERLYING PREMISE OF MTIE

As will be seen from the definition, MTIE(τ) is necessarily a monotonically non-decreasing function of τ. It is, conventionally, shown as a graph plotted on a log-log scale and therefore if

the two clocks have identically equal (long-term) frequencies, the MTIE curve will be a horizontal line. Any frequency offset between the two clocks appears as a linear slope.

1.4.5 Packet-based and Two-Way Time Transfer

Consider the situation in which a Slave clock (*aka* client) derives its timing from a source (*aka* Master or server). Packet exchanges between Master and Slave provide measurements of the transit delay between the two. This is explained with respect to Fig. 4. The particular protocol (such as Network Time Protocol, NTP, or Precision Time Protocol, PTP) employed determines the method whereby the measurements ("time stamps") are communicated between the two entities.

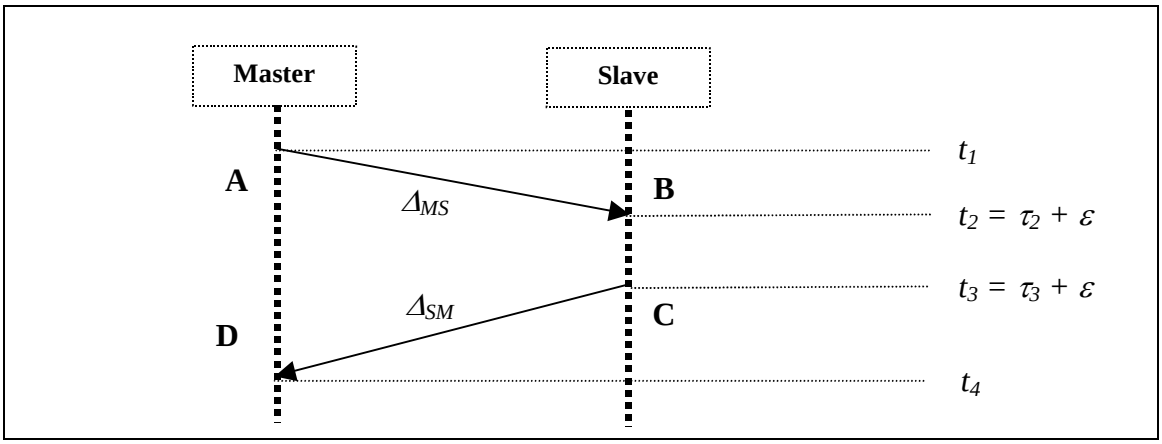


FIGURE 4. TIME-STAMPS IN PACKET EXCHANGE BETWEEN MASTER AND SLAVE

Referring to Fig. 4, the sequence of events and important items of information associated with an exchange of packets between Master and Slave are listed below.

- Event A: Packet is transmitted by Master and time-of-departure according to Master is t_1.
- Event B: Packet arrives at Slave that measures the time-of-arrival as τ_2; assuming that the slave time error is ε, the actual time-of-arrival is $t_2 = \tau_2 + \varepsilon$.
- Event C: Packet is transmitted by Slave that notes the time-of-departure is τ_3; assuming that the slave time error is ε, the actual time-of-departure is $t_3 = \tau_3 + \varepsilon$.
- Event D: Packet arrives at Master that measures time-of-arrival as t_4.

Such a two-way exchange of packets can provide information suitable for allowing the slave to align in time with the master (assuming that both sides have knowledge of the time stamps). If the exchange of information is only one-way, from Master to Slave, the Slave can still align its clock (frequency) with the Master (*syntonization*).

There are four measured values that can be communicated between the Master and Slave, namely, (t_1, τ_2, τ_3, t_4). Note that such a two-way exchange involves one packet (message) in each direction; they do not necessarily have to be consecutive, as long as the time-stamp information is communicated appropriately. In some instances, the rate at which packets are transmitted in the two directions can be different. Denoting by Δ_{MS} and Δ_{SM} the transit delays from the Master to the Slave (MS) and from the Slave to the Master (SM), respectively, the following equations can be established in Eq. (23)

$$\begin{aligned} t_4 &= \tau_3 + \varepsilon + \Delta_{SM}\ (from\ a\ Slave\ to\ Master\ packet) \\ t_1 &= \tau_2 + \varepsilon - \Delta_{MS}\ (from\ a\ Master\ to\ Slave\ packet)\ . \end{aligned} \tag{23}$$

There are just two equations involving three unknowns. However, if one assumes delay reciprocity (i.e., equal delay in the two directions) then Eq. (24) is obtained.

$$\begin{aligned} \varepsilon &= \left(\frac{1}{2}\right)\left(t_4 - \tau_3 - \tau_2 + t_1\right) \\ \Delta_{MS} &= \Delta_{SM} = \left(\frac{1}{2}\right)\left(t_4 - \tau_3 + \tau_2 - t_1\right) \end{aligned} \tag{24}$$

Error in (the estimate of) the local time-clock, ε, can be attributed to the following causes.

1. The transit delay in the two directions is not equal. The difference directly affects the time-clock estimate. Though if this asymmetry is known, it can be accounted for. The error, $\Delta\varepsilon$, is given by Eq. (25)

$$\Delta\varepsilon = \left(\frac{1}{2}\right)\left(\Delta_{MS} - \Delta_{SM}\right)\ . \tag{25}$$

2. The measured quantities, namely (t_1, τ_2, τ_3, t_4), may not be measured precisely. That is, whereas t_1 is the actual time-of-departure of the packet from the Master, the value used in the calculation may be an estimated time-of-departure. Likewise, τ_2 is meant to be the actual time-of-arrival; the value used may be an estimate. For such time values to be precise, they must be obtained by means that are at the physical layer and thus the time-of-departure (time-of-arrival) is not compromised by any (variable) delay attributable to such entities as the operating system and interrupt handling. It is

assumed that the measurement entity has available a clock such that the time-stamp value has sufficient resolution.

3. The transit delays Δ_{MS} and Δ_{SM} are not fixed and change from packet to packet because of the packet delay variation (PDV) in the network. Note that while the time-stamp uncertainty can appear to be a component of the PDV, it is a "controllable" component, and the error introduced mitigated or minimized by suitable implementation designs and algorithms.
4. The update rate affects the quality of synchronization. In particular, assuming that the packet delay variation has a flat spectrum (white noise), time-synchronization accuracy improves as the square-root of the update rate. Conversely if the update rate is low, noise mitigation techniques involving packet selection such as averaging and minimum picking are less effective.
5. The stability of the local clock in the Slave does impact the time error. In particular, the derivation of time offset, ε, given above assumes that the local clock is (extremely) stable over the observation interval during which the four representative time stamps are obtained.

There are numerous variations and enhancements of the basic principle described above. The two-way scheme described above is used for time alignment purposes. If the requirement for alignment is primarily frequency, then one-way methods can be used. Frequency alignment requires that the transfer delay be constant.

2 Managing Time and Latency

This section presents information relevant to managing time and latency in cyber-physical systems. Selected articles and references are provided in Refs. [5–21].

2.1 Standards Making Networks Time-Aware

Several standards (or standards suites) are identified below as relevant to making networks time-aware:

1. IEEE 1588 [9]: Provides a layered architecture for time propagation which allows clock synchronization across heterogeneous networks (including wireless). IEEE 1588 specifies the media independent options and the mapping to media dependent options which are specified in network-specific standards.
2. IEEE 802.1AS [22]: Specifies an Ethernet specific profile for IEEE 1588 that provides guarantees on synchronization accuracy. IEEE 802.3bf (2011) provided an accurate

indication of the transmission and reception initiation times of certain packets as required to support IEEE 802.1AS (Note however that IEEE 802.3bf has now been superseded).

3. IEEE 802.1Q [23]: Provides time-sensitive data transfer mechanisms which enable convergence of time-sensitive and best-effort data on the same Ethernet network without compromising bounded latency guarantees of time-sensitive streams. This includes time-aware scheduling features in hardware which enable lowest latency options that are important for control applications in CPS. The time-aware scheduling features include time-aware gates per port that can be scheduled for a flow, or time-based shapers that can guarantee end-to-end latency.
4. IEEE 802.1CB [24]: Provides seamless redundancy options to increase reliability of data-transfer in Ethernet networks.
5. IEEE 802.11-2016 [25]: 802.11 is a set of IEEE standards that govern wireless networking transmission methods. IEEE 802.11v-2011 specifies timing measurement capability for Wi-Fi networks and a mapping function to IEEE 1588. IEEE 802.11ak specifies bridges 802.11 networks which will enable time-sensitive stream support over Wi-Fi networks (using time-based synchronization) in the future.
6. ITU-T Rec. G.8261 (also Y.1361) [26], Timing and synchronization aspects in packet networks.
7. ITU-T Rec. G.8262 [26], Timing characteristics of Synchronous Ethernet Equipment slave clock (EEC).
8. ITU-T Rec. G.8265 (also Y.1365) [26], Architecture and requirements for packet-based frequency delivery.
9. ITU-T Rec. G.8275 (also Y.1369) [26], Architecture and requirements for packet-based time and phase delivery.

Additionally, there are consortia created around these standards like the Wi-Fi Alliance (WFA) and Avnu Alliance which are helping test implementation and interoperability. A working group has been formed in the Internet Engineering Task Force (IETF) called Deterministic Networking [27] to bring time and time-sensitive data transfer into wide area networks (WANs).

2.2 Schedule Generation and Distribution

Performance Metrics

The Centralized Network Manager (CNM) or the Centralized Network Controller gathers performance metrics and calculates the topology of CPS nodes in a CPS domain in order to create a schedule.

The performance metrics are bridge delays, propagation delays, and forwarding/transmission delays. IEEE 1588 uses peer-to-peer delay which can be exposed to the CNM or the centralized network controller via a management interface. The bridge delays for a specific stream based on size and routing model (store and forward or cut-through) can also be exposed in the same way. IEEE 802.1Q is considering implementing/referencing these capabilities (via the IEEE 802.1Qbv specification).

One method to measure latency could be as follows:

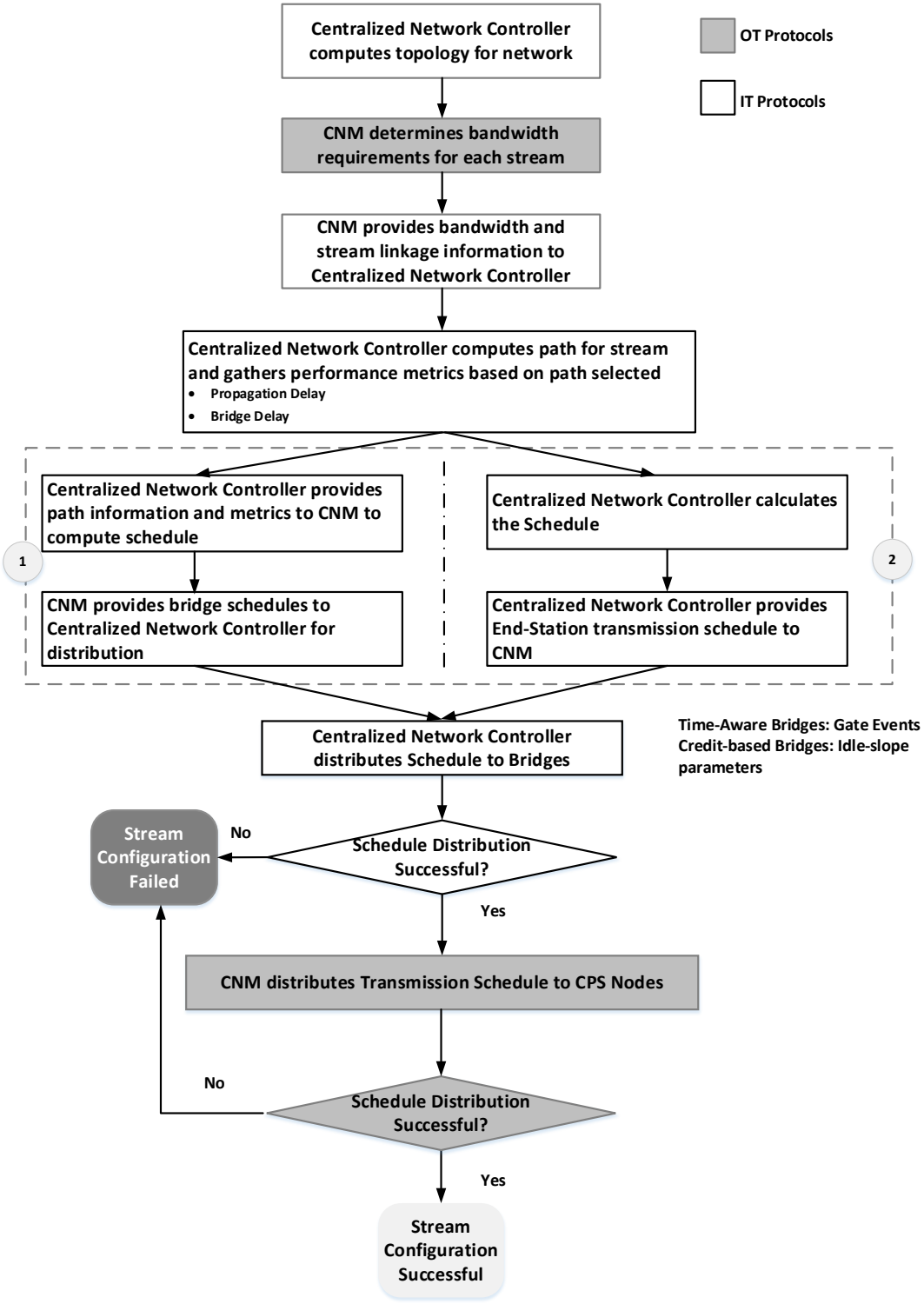
1. The CPS Manager brings all the CPS nodes to a steady-state. In this state, all devices are ready to exchange time-sensitive data and their clocks are synchronized.
2. The CPS Manager instructs transmitting nodes to send a test stream to the receiving nodes.
3. The transmitting node time-stamps the packet that it sends. Each bridge time-stamps the packet at its ingress and egress ports. The receiving node time-stamps the packet at its ingress port.

These time-stamps are sent to the CPS Manager and or the Centralized Network Controller which can then calculate the latency through each bridge and between the links.

Possible Schedule Distribution Flow

In Fig. 5 [28], a possible schedule distribution flow in a CPS is described. The Centralized Network Manager computes the topology for the CPS domain and determines the bandwidth requirements for each time-sensitive stream based on application requirements. The bandwidth can be specified by the period and the size of the frame. Optionally the application can also specify a range <min, max> for the offset from start of a period. This information is provided to the Centralized Network Controller. The Centralized Network Controller computes the path for the streams and gathers performance metrics for the stream (latency through the path and through the bridges). This information is then used to compute the schedule for the transmission time of each time-sensitive stream and the bridge shaper/gate events to ensure that each time-sensitive stream has guaranteed latency through each bridge. Additionally, queues in bridges are reserved for each stream to guarantee bandwidth for zero congestion loss.

The schedule generation may be implemented in the CNM or the Centralized Network Controller. Once the schedule is generated, it is distributed to the bridges by the Centralized Network Controller and to the CPS nodes (end-stations) by the CNM.



"IT" indicates Information Technology, and
"OT" indicates Operational Technology

FIGURE 5. CPS SCHEDULE GENERATION AND DISTRIBUTION

(Courtesy: Sundeep Chandhoke, National Instruments [28])

2.3 Use of Time in Operating Systems

CPS can employ operating systems (OS) with a wide range of complexities, from a simple application-level infinite loop to a virtual machine (VM) hypervisor running several instances of virtualized systems on a multi-blade, multi-core hardware platform. The issues that arise throughout these systems with respect to time-awareness are how to get time to the application with a bounded latency and accuracy, and how to schedule tasks with a bounded time latency and accuracy.

The operating system models typically employed in CPS are illustrated below in Fig. 6 [29].

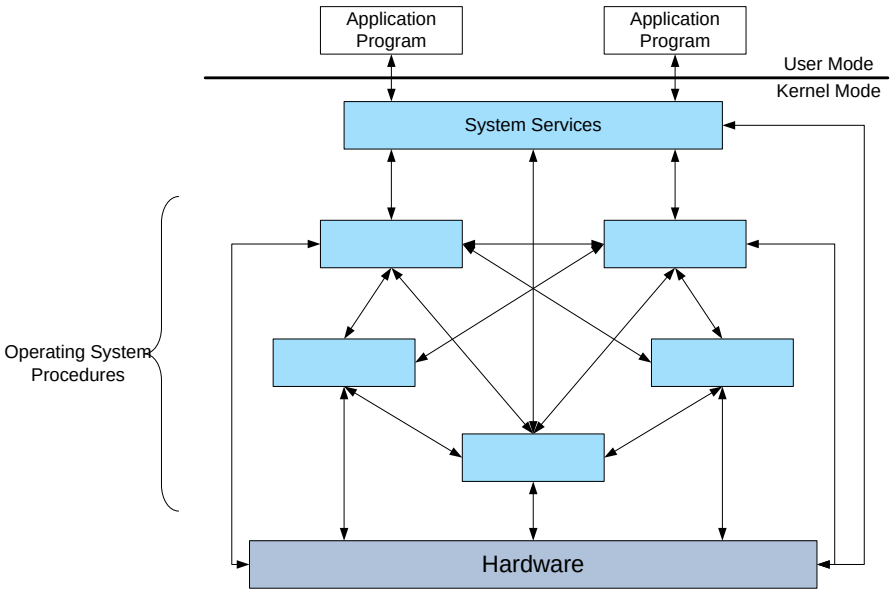


FIGURE 6. MONOLITHIC OPERATING SYSTEM

(Courtesy: Rajkumar Buyya, The Design of PARAS Microkernel, Centre for Development of Advanced Computing (C-DAC), Bangalore, India, 1998 [29])

A monolithic operating system is single threaded, and is often referred to as a 'main loop' or 'infinite loop' system. It contains basic system services, typically just function calls to access libraries, common processes, and the platform hardware. Access to time services is not a challenge, however the operating system complexity is low, and often unsuitable for many applications. Without context switching from one task to another, lower priority tasks can pre-empt higher priority tasks, since operations will be performed uninterrupted until they complete.

For multi-threaded operating systems, tasks can be divided by priority, and isolated from each other. The system complexity increases to maintain this isolation, both to allow the independent operation of tasks and to assure that access to common resources such as memory and I/O are coordinated. Multi-threaded systems can utilize a layered model, or can be message-based.

With greater flexibility and capability comes greater complexity, and a greater challenge to incorporate the control of determinism from layer to layer. This is illustrated below in Fig. 7 with a request for accurate time shown traversing through different layers.

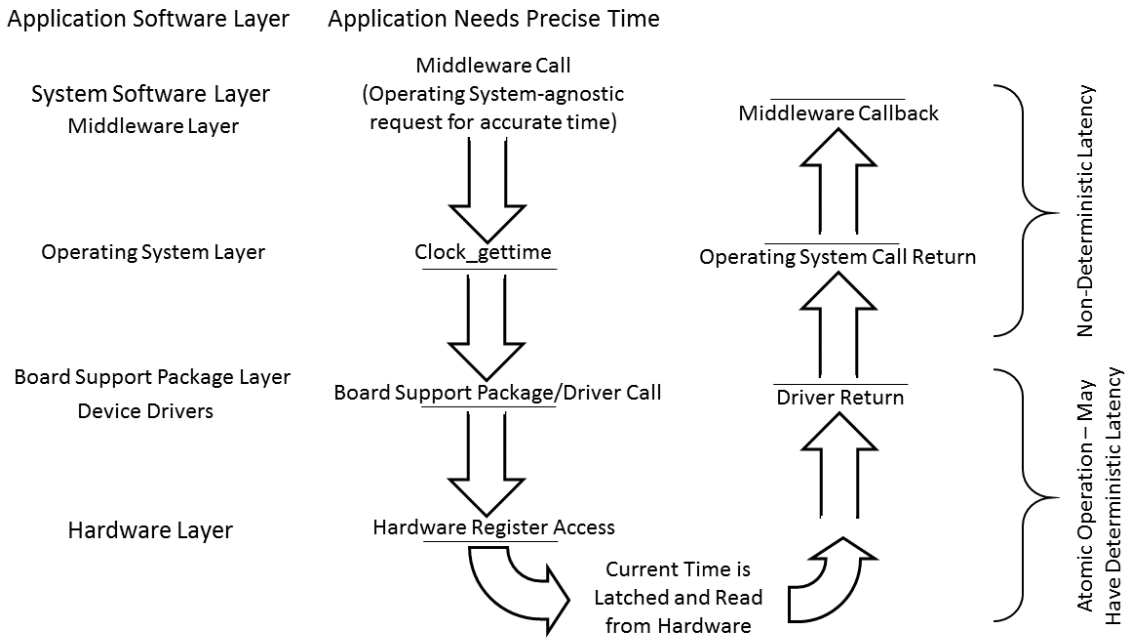


FIGURE 7. APPLICATION REQUEST FOR TIME

To account for the non-determinism contained in the traversal of the OS layers, a timestamp model could be employed which accurately captures the exit and entry of the processor in each layer. The residence time can then be accumulated and added to the timestamp value captured in hardware. This approach would require very low latency hardware support in the processor which is not present in the systems currently employed.

In a microkernel-based multi-threaded system, as shown in Fig. 8 [30], the layers are minimized, and communication takes place between user modules using message passing. This can have more flexibility, extensibility, portability and reliability than a layered architecture. Replacing service calls with message exchanges between processes adds overhead that can affect performance, and can add to latency and non-determinism. The microkernel is a good choice for an operating system that needs to be ported to multiple platforms. The changes needed to port the system are within the microkernel, not the other services. In general, there is also less code running in the operating system as the services are outside it. The kernel therefore can be tested and validated independently and more rigorously.

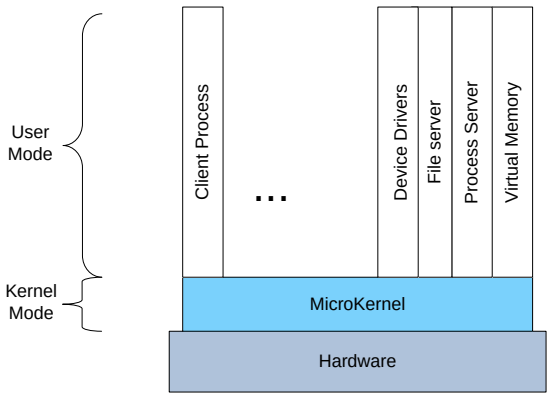


FIGURE 8. MICROKERNEL OS

(Courtesy: William Stallings, Operating Systems: Internals and Design Principles (6th Edition), 2008, Pearson International Edition [30])

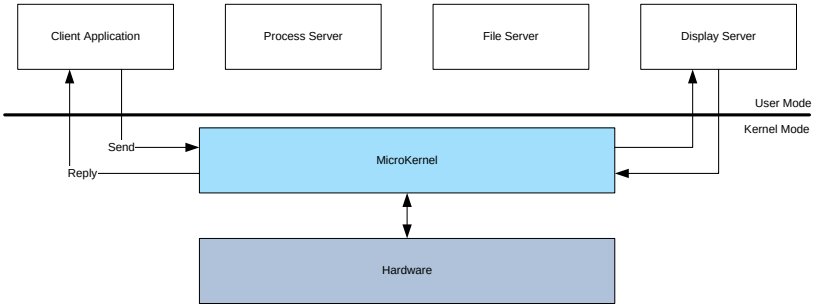


FIGURE 9. MICROKERNEL MESSAGE PASSING MODEL

(Courtesy: Rajkumar Buyya, The Design of PARAS Microkernel, Centre for Development of Advanced Computing (C-DAC), Bangalore, India, 1998 [29])

In the microkernel case, the time and latency determinism is driven by the message passing process, shown in Fig. 9 [29].

Many applications are less concerned about the uncertainty in the traversal of the operating system and more about bounding the latency and total execution time of tasks. The process scheduler in the multithreaded OS determines the time allocated to tasks as well as the frequency these tasks are processed. Establishing determinism in the task scheduler will be key to providing the tools needed to bound the latency and completion time of critical tasks.

The logical extension of the microkernel is the virtual machine (VM) architecture, shown in Fig. 10 (adapted from Ref. [31]), in which several microkernels or layered operating systems are run together on a single hardware platform. This platform can either be a single CPU that task-switches between systems, or multiple CPUs that share the virtual machine operational load. The VM treats hardware and the operating system kernel as though they were all hardware. It provides an interface identical to the underlying bare hardware. The operating system host creates the illusion that a process has its own processor and (virtual) memory. Each guest provided with a (virtual) copy of underlying computer.

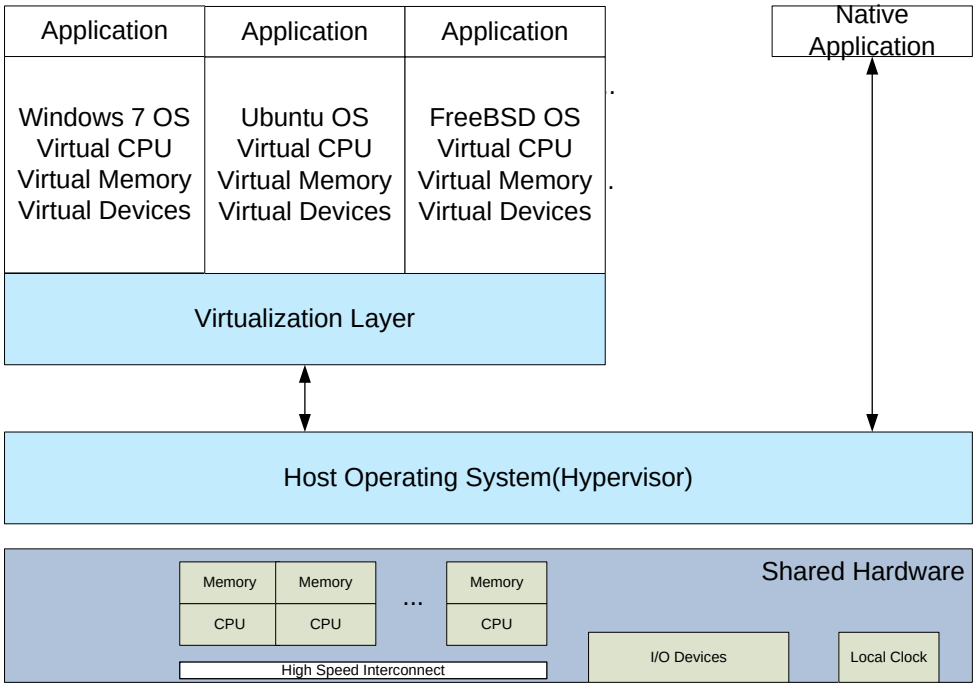


FIGURE 10. VIRTUAL MACHINE ARCHITECTURE

(Courtesy: modified figure from Silberschatz, Galvin, and Gagne, Operating System Concepts, 8th Edition, 2009, John Wiley and Sons, Inc. [31])

VM-based systems not only need to be able to propagate time and deterministic behavior from real hardware to VMs, they also need well defined VM execution times to allow for VM scheduling within single CPU timeline or across multiple CPUs.

The network between virtualized nodes is implemented in the Host Operating System (referred to as a Hypervisor). This virtualized network also would have the timing protocol (e.g. PTP) built into it, in order to extend the physical network timing system to the virtualized processors. As implemented today, this is not included by default, and is separate and different from the networking layer that comes with an operating system. The virtualized PTP protocol would essentially emulate a PTP aware switch that handles the network traffic between the virtualized computers.

3 Timing Security and Resilience

3.1 The Case for Secure Time

Everything done within the digital age relies upon a time source. For example, today's mobile networks have strict requirements for accurate frequency synchronization as well as phase and

time synchronization. Timing inadequacies may cause synchronization failures for 4G LTE. The accuracy of time will be a pacing item for 5G and 6G service.

3.2 Compromising and Securing Time

Compromising GPS and other wireless frequencies

Jamming and Spoofing

Given the vital dependency of timing on the Global Navigation Satellite System (GNSS), it is essential for CPS designers to be aware of the ease of disruption of GNSS as a timing source. GNSS signals are transmitted from an altitude of approximately 20,000 kilometers. The relatively weak radio frequency (RF) signals are the basis of the unintentional or intentional jamming risk. The effect is to corrupt the signal rendering the receiver to be incapable of decoding the data. The need for secure and resilient time has been highlighted by several incidents reported by the media where use of inexpensive commercial-off-the-shelf equipment led to significant disruptions [32–33]. Other forms of wireless communications such as 4G LTE, WiFi (wireless local area networking based on IEEE 802.11 standards), and Worldwide Interoperability for Microwave Access (WiMax) networks can also be easily disrupted.

GNSS signals are also susceptible to meaconing (an industry term coined from “mislead” and “beacon”) or spoofing. The goal of spoofing is generally malicious as the intention is to mislead by providing a counterfeit signal. Spoofing of radio signals existed in World War I. The threat of GNSS spoofing has also been demonstrated [34]. However, researchers have also shown that anti-spoofing algorithms can detect attacks by observing GPS receiver characteristics [35]. GPS encrypted signals prevent spoofing but are only available for US military and authenticated users. For civilian use, authenticating the signals can greatly increase the complexity of spoofing attacks. Navigation Message Authentication (NMA) is moving forward on GPS for the second frequency civilian code called L2C. NMA attaches a digital signature to the GPS navigation messages [36].

Ongoing research and technology advancements are needed to enable detection and location of jammers and spoofers. GPS Jammer Detection and Location (JLOC), using ad-hoc networks such as vehicles [37] and mobile phones, can enable the CPS to predictably failover to other time sources for validation and redundancy to ensure the integrity of the system time. Ensuring system resiliency by meeting minimum timing system specifications can also mitigate the effects of jamming and spoofing. Table 3 [38] describes the minimum acceptable oscillator, holdover time and impact of GPS anomalies on each of the Critical Infrastructure and Key Resources (CIKR) sectors. Having a combination of viable timing source alternatives also provides a layer of security and resiliency for meeting timing requirements in various CPS domains.

Table 3: Impact of GPS Anomalies by CIKR Sector

GPS Timing Essential Critical Infrastructure and Key Resources (CIKR) Sector	Least Robust Oscillator (Minimum Acceptable)	Holdover Time (hours)	Unintentional Interference Impact: 8 hours (Y or N)	Intentional Jamming Impact: Multiple Days (Y or N)	Space Weather Impact: 16 hours (Y or N)
Chemical Sector	OCXO (MS)	1	Y	Y	Y
Communications Sector	OCXO (HS)	24	N	Y	N
Critical Manufacturing Sector	TCXO	1.7	Y	Y	Y
Dams Sector	OCXO (MS)	1	Y	Y	Y
Defense Industrial Base Sector	TCXO	1.7	Y	Y	Y
Emergency Services Sector	OCXO (HS)	24	N	Y	N
Energy Sector	OCXO (MS)	1	Y	Y	Y
Financial Services Sector	TCXO	<.24 – 1.7	Y	Y	Y
Information Technology Sector	OCXO (MS)	1	Y	Y	Y
Nuclear Reactors, Materials, and Waste Sector	OCXO (MS)	1	Y	Y	Y
Transportation Systems Sector	OCXO (HS)	24	N	Y	N

TCXO: Temperature-Compensated Crystal Oscillator
OCXO: Oven-Controlled Crystal Oscillator
HS: High-Stability
MS: Medium-Stability

(Source: R.J. Caverly "GPS Critical Infrastructure: Usage/Loss/Impacts/Backups/Mitigation" [38])

CPS relying on GPS time can also establish elements for integrity monitoring of the time reference source [39]. Integrity is a measure of the trust placed in the correctness of the information with respect to GPS time [40]. The elements for integrity monitoring can include:

- *time-to-alarm*: an integrity breach must raise an alert within a specified period,
- *integrity risk*: an estimated probability that an integrity breach has occurred, and

- *alarm limit*: the timing accuracy exceeds a tolerance level required by the system's most stringent application.

Space Weather and Disaster Compromise

The ability to maintain continuity of time during geomagnetic storm activity, systems fluctuations and unreliable power grid performance has a major impact on time and cyber activities. The same architectures, tools and report structures used to support cyber events should and will be used to support natural disasters, catastrophic failures and measures to correct for unknown anomalies. Table 4 [38] below describes the effect of solar storms on GPS time.

Table 4: Space Weather Impact on GPS

Solar Storm Effect	Single Frequency GPS Timing Error (Range)	Single Frequency GPS Position Error (Range)	Time of Day	Duration of Event
Total electron content (TEC) increase in ionosphere	Less than 100 ns Typical 10-30 ns	Less than 100 m Typical 10-20 m	Day side of the earth	Hours to days
Scintillation	Less than 100 ns for individual satellites	Loss of precision due to loss or corruption of individual GPS satellites	Worse in early evening	Individual events minutes but can persist for hours to days (diurnal)
Solar radio bursts	Severe events can deny GPS reception	Severe events can deny GPS reception	Day side of the earth	Minutes to hours (duration of the solar burst)

(Source: R.J. Caverly "GPS Critical Infrastructure: Usage/Loss/Impacts/Backups/Mitigation" [38])

A geomagnetic storm induces ground currents, or Geomagnetically Induced Currents (GIC), which can damage equipment at power substations and cause faults and trips on power lines [41–42]. Loss of GPS timing synchronization of data for Supervisory Control and Data Acquisition (SCADA) systems and synchrophasors leads to corrupted grid state estimation and compromises the situational awareness and control capabilities of the power system. Furthermore, during the storm communications degradations include high frequency (HF) radio blackouts, satellite communications losses and Code Division Multiple Access (CDMA) Cellular and Land Mobile Radio Simulcast loss due to loss of GPS timing synchronization.

One means of mitigating space weather impacts is the development of space and ground-based capabilities to provide high-confidence forecasts of ionospheric and other space weather characteristics [41] which would improve the systems' ability to achieve predictable fail-over to alternative timing sources.

3.3 Some National Timing Backup Alternatives

Given the vulnerability of the GPS and other wireless infrastructure for acquiring reference time traceable to a national lab, alternative means can be used. There are many companies drafting and implementing position/navigation/timing /cyber solutions. Very few address the consequence of GPS time loss, spoofing, or cyber solutions that are not software based. The only true competition to pervasive time loss happens to be alternative GNSS constellations (e.g. Chinese Compass, Russian Global Navigation Satellite System (GLONASS) and the European Union's (EU's) Galileo Programs).

Some domestic alternatives across a variety of broadcast architectures, including dedicated wide area networks, WWVB, and eLORAN, are covered in the following sections.

Communications Sector Timing Distribution

One way to mitigate the impacts from vulnerable GPS timing receivers is to design and implement timing distribution architectures that do not use vulnerable receivers but use no, or very few, resilient and robust GPS/timing and frequency systems (TFS). In the case of using very few GPS receivers, if the TFS associated with the GPS receivers employ extended holdover oscillators, then when GPS is lost or disrupted through jamming, the overall GPS/TFS will continue to provide all the requisite timing information (e.g., frequency, time-of-day, and one pulse-per-second synchronization) for an extended holdover period. For example, a High Stability Rubidium will holdover one microsecond time accuracy for about a day. Although these oscillators are more expensive per unit, fewer of them would be needed in networks that have a method to distribute accurate timing without degrading it. Two such network architectures are being experimented with today: 1) dedicated networks using PTP over Optical Transport Network (OTN) and 2) SyncE with PTP.

A high-level overview of these two experimental timing distribution architectures is provided below.

Dedicated Wide-Area Networks
Dedicated coaxial and optical networks can transport timing signals with minimal jitter. For example, the CPS can use packet based time distribution protocols such as PTP over Synchronous Optical Networking (SONET)/Synchronous Digital Hierarchy (SDH) or Optical Transport Network (OTN), which is then multiplexed into the network. In experimental tests, time transfer accuracy of a few nanoseconds over a commercial asynchronous fiber optical network is achievable between two sites over 500 kilometers apart [43]. Another experiment showed time transfer stability using PTP over OTN better than 50 nanoseconds over 200 kilometers [44].

Synchronous Ethernet (SyncE) with PTP
The second architecture that holds promise for distributing precise timing over long distances

to timing users is SyncE with PTP. SyncE distributes a traceable frequency reference at the physical layer to packet-based (Ethernet) nodes. The SyncE network's oscillators are therefore locked to the master's oscillator frequency. All oscillators on the network would have the same drift characteristics.

In SyncE with PTP, the Grand Master (GM) clock connects directly to GPS or, if GPS is not available, another timing reference source, which provides the primary reference clock for entire chain. Multiple timing chains could be supported from a single GM. Boundary Clocks (BC) and Transparent Clocks (TC) are chosen and placed depending on the particulars of the network topology. Full on-path support, where all network equipment in the timing chain must support both SyncE and PTP, is needed.

The main advantage of the SyncE with PTP architecture is that PTP and SyncE deployed together offer better timing performance than PTP alone. However, timing accuracy, distance limitations, number of chained BC/TC nodes, and network restrictions are still under research for deployment of SyncE, PTP, and BC/TC. Distance limitations and the specific network architecture to support the distribution of 1 microsecond timing accuracy continues to be an area of research. CERN, the European Organization for Nuclear Research, has implemented a version of SyncE and PTP called White Rabbit that combines with measured equipment delays and measured asymmetries to provide sub-nanosecond time transfer over the CERN system [45]. The IEEE 1588 standard is currently undergoing an update that includes a high-accuracy option, which incorporates some of the White Rabbit technology [9].

In conclusion, dedicated networks can provide precise timing synchronization between remote sites in any of the 16 CI Sectors with no, or a minimum, reliance on GPS timing receivers.

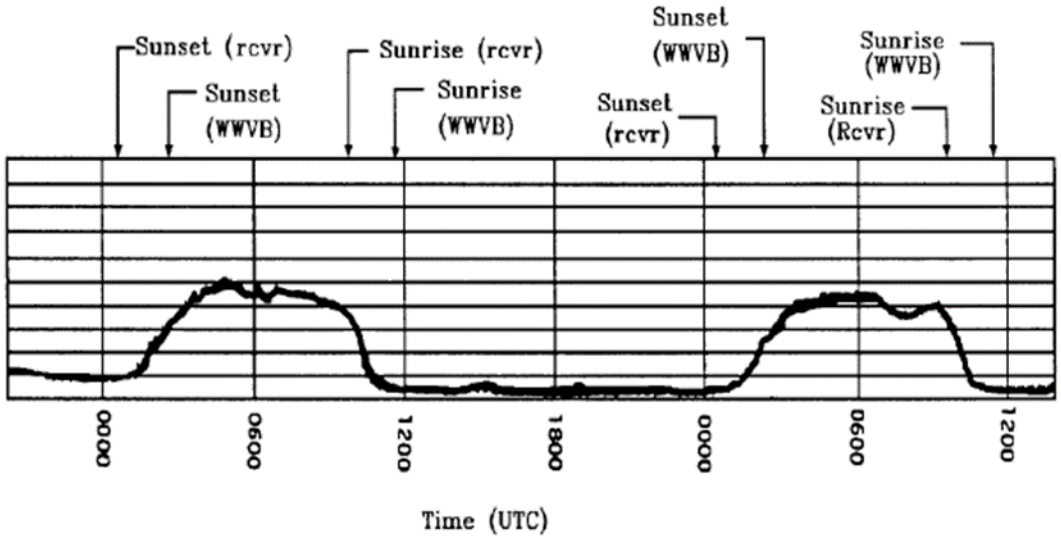
WWVB / WWV / WWVH Timing Radio Broadcasts

Regarding methods of GPS backup for time and frequency synchronization, this section presents the status [46-47] of the 60 kHz timing signal, WWVB, of NIST. In particular, this signal may be useful to assist in holding 1 microsecond in circumstances where GPS is generally available to calibrate it, but might be unavailable for short periods depending on the accuracy required, the distance to the transmitting station and the availability of nearby reference stations. The use of High Frequency (HF) signals from WWV for timing is also mentioned.

In considering alternative time signals to GPS, given that LORAN is not currently available in the U.S., it is useful to look at the existing timing signals that are still available. NIST still broadcasts these timing signals: LF signal WWVB on 60 kHz, and HF signals WWV and WWVH on 2.5, 5, 10, 15, and 20 MHz [47].

WWVB is capable of providing frequency accuracies of about 1 part in 10^{11} over days. Most of the studies of the use of this signal are from the 1960s and 1970s. Achieving 10^{-11} accuracy required careful selection of tracking times and a very stable reference; a data set taken in Maryland of the WWVB signal transmitted from Colorado is shown in Fig. 11 [47] below. The

vertical range of the plot is 50 microseconds, hence each line represents 5 microseconds. One can see a diurnal variation of about 20 microseconds. In addition, using older technology, there were occasional cycle slips.



(Chart is 50 microseconds wide)

FIGURE 11. PHASE OF WWVB AS RECEIVED IN THE EASTERN UNITED STATES

(Source: G. Kamas and M. Lombardi, NIST Special Publication 559 (Revised 1990) [47])

For use as a GPS backup in Assisted Partial Timing Support (APTS) there are several new conditions that offer opportunities [46]. In WWVB receivers, options include modern hardware to improve accuracy and stability of reception, and the use of GPS to characterize the WWVB signal, requiring only stability to hold precision time. In addition, recently, phase modulation has been introduced on the 60 kHz carrier for transmitting data. This has the potential to lower the short-term noise, and further reduce the possibility of a cycle slip. However, this is a new enough development that studies have not yet been done of the capability of these options.

WWVB cannot be received reliably over the U.S. East coast, especially in Florida. Over long baselines, the signal delay has diurnal and longer-period variations that cannot be modeled. These variations often have short-wavelength components. The transmission frequency of WWVB is about the same as the carrier frequency used by LORAN, and the comments of LORAN and eLORAN also apply to WWVB.

The HF signals of WWV and WWVH based on historic measurements have less interest for use by the Communications Sector and other precise timing sectors, since they historically showed a frequency accuracy of 10^{-7}. Nevertheless, there may be options for use in holdover at much

higher stabilities using modern hardware and combining multiple received signals. Work was done using such a technique in 1969 using differences of multiple Very Low Frequency (VLF) signals to obtain accuracies in the microsecond region. In addition, WWVB has been broadcasting with phase modulation, which improves short term noise, and lowers the chance of loss of cycle. Thus, with WWV signal improvements, modern receiver hardware, and the use of GPS to characterize signals when GPS is available, there may be sufficient options to consider use of these HF WWV and WWVH signals for Critical Infrastructure timing holdover [46].

eLORAN

One possible backup to GNSS that is currently under consideration for aviation, maritime, critical infrastructure and military use is enhanced Long Range Navigation system (eLORAN). eLORAN is a modernized version of the Long RAnge Navigation (LORAN) and LORAN-C navigation systems. The eLORAN system, although not yet fully defined, uses the following techniques to improve navigation and timing performance:

- receivers are provided with detailed, surveyed, propagation delay maps in areas where precise navigation and timing are required; and
- the system uses local monitoring stations to measure weather dependent propagation delays, and the weather dependent corrections are provided to receivers by an additional data channel.

During controlled proof-of-concept demonstrations, eLORAN has been demonstrated to provide approximately 20 meter, 2-dimensional root-mean-square (2D RMS) position, and approximately 100 nanosecond time accuracy 95% of the time [48], representing a 5 times to 10 times improvement over the performance of its predecessor LORAN-C. Time accuracy depends on the distance to the transmitter and the availability of reference stations to provide real-time estimates of the local path delay. These parameters are called “additional secondary factors” in the LORAN system.

LORAN and its variants are terrestrial radio frequency navigation systems that use at least three synchronized transmitters to provide 2D position and time to receivers. Post World War II (WW2), LORAN systems operate at the low frequency (LF) of 100 kHz (equivalent to a wavelength of 2997.9 m or approximately 3 km) where RF propagates as ground waves. Ground waves are RF signals that propagate along the surface of earth, which extends their transmitter’s range. However, since the ground waves propagate along the surface of earth, they cannot provide reliable altitude information. LORAN is a time-division-multiple-access (TDMA) system where the transmitters broadcast pulses within predetermined time slots. By measuring the differences of arrival times of the pulses, the receiver can calculate its position relative to the known tower positions. At least three synchronized towers are required to provide the user with 2D position and time.

The relative time of arrival measurement made by the receiver is dependent on the distance between the transmitting tower and the receiver, atmospheric and ionospheric conditions, the geographical terrain and terrain conditions along the signal's transmission path, the transmitter and receiver clocks, and RF interference sources, among other system considerations. Navigation and timing performance is dictated by the:

- system's ability to correct the atmospheric and terrain induced time of arrival dependencies,
- quantity and geographic diversity of towers, and
- tower synchronization and the RF interference environment.

Accidental RF interference may be caused by terrestrial weather in the form of lightning strikes, space weather in the form of solar radio bursts and geomagnetic storms, and system self-interference in the form of sky waves and signal re-radiation off of large metal structures.

The deliberate threats are jamming and spoofing. However, the on-air LORAN signal is nearly unjammable, and the on-air LORAN signal is also difficult to spoof [49].

Jamming: To compete with and overpower a typical 400 kW LORAN tower at 300 km, the jammer needs: ~40 W at 5 km; or, alternatively ~0.4 W at 0.5 km. While not a lot of power is required, it has to be radiated power. The LORAN signal wavelength (3 km) makes efficient radiated power transmission difficult, especially with an electrically short antenna using a small un-matching ground-screen (limiting factor is top-bottom voltage differential). The required monopole antenna for jamming is very large and difficult to set up. Both the set up and operation of an LORAN/eLORAN jammer would make detection and geolocation of the jammer's location relatively easy.

Spoofing: To spoof a Loran signal with a continuous wave (CW) tone would necessitate creating, for example, a 100 ns error at 5 km requiring ~160 mW, or creating a 500 ns error at 5 km requiring ~4 W power (radiated peak). Antennas for spoofing are smaller but still pose logistics and detectable set up problems.

The discussion above has quantified the inherent LORAN/eLORAN system advantages over GPS regarding near-unjammability and difficult spoofability. Further research and development on eLORAN could result in more cost-effective, certifiable, and secure eLORAN anti-spoofing receiver designs (e.g., by adding authentication through digital signatures).

3.4 Network Time Compromise

The working group discussed the following attacks and defenses in sections 3.4 through 3.6 for illustrative purposes; further analysis will continue to be necessary for comprehensive coverage of the evolving threats and mitigation strategies.

Terms and Definitions:

Network-related

Unsecured Network: An unsecured network has no means to protect, authenticate or encrypt data packets that are exchanged between its hosts. Basic access control might be provided (via host whitelisting or Media Access Control (MAC) address filtering), but can be easily bypassed by an attacker.

Secured Network: In a secured or trusted network all hosts share a set of security credentials that provide a combination of (a) host authentication / authorization, (b) message authentication and (c) message encryption. This can be complemented by physically protecting (e.g. isolating) the network.

Hybrid Network: A hybrid network consists of both unsecured and secured segments.

General Attack Concepts

Internal Attacker: An internal attacker belongs to or has access to (via a compromised host) a secured network, e.g. it has access to security credentials.

External Attacker: An external attacker does not have access to the credentials of a secured network, but can intercept (via eavesdropping) encrypted or authenticated network traffic. It can also (blindly) modify / generate and inject network messages. It is assumed that the underlying cryptographic credentials are strong enough to withstand a brute force attack by an external attacker (which, for example, is not provided in NTP's Autokey protocol), e.g. an external attacker is not able to become an internal attacker.

Man-in-the-Middle (MitM): MitM attackers are located in a position that allows interception and modification of in-flight protocol packets. This includes situations where the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled and manipulated by the attacker.

Denial of Service (DoS): DoS or Distributed DoS (DDoS) is an attempt to make a network or system resource unavailable for its intended purpose. The attack can be executed by flooding the network with extraneous packets or interrupting the packet stream.

Injector: A traffic injector cannot intercept legitimate packets, but can record them, replay old messages, and generate its own traffic.

Message Interception (passive attack): The attacker quietly eavesdrops on network communication. While non-damaging per se, it is part of the reconnaissance phase of an attack, during which networks are mapped or network traffic is analyzed. Message interception can be done by a MitM or injector.

Message Interruption (active attack): A MitM can selectively interrupt, e.g. intercept and remove, certain packets, or can bluntly block all communication in a network (segment). This is a basis for a Denial of Service (DoS) attack.

Message Insertion (active attack): An injector or MitM injects newly crafted packets or previously recorded unicast or multicast packets into a network. It also is a basis for a Denial of Service (DoS) attack, where a node (via packet flooding) either jams an entire network or selectively targets one node.

Message Modification (active attack): A MITM attacker intercepts and modifies in-flight protocol packets.

3.5 Threat Analysis for Time Networks

Mizrahi [50–51] conducted an in-depth analysis of state-of-the-art secured PTP networks (based on Internet Protocol Security (IPsec), IEEE MAC Security Standard (MACsec) and IEEE 1588 Annex K, described in more detail in the next section). The analysis distinguishes between internal and external MitM and injector attackers located in a network. Based on information in [50–51] and input by CPS PWG Timing subgroup members, Table 5 provide a listing of threat types, characteristics, impacts, examples and potential countermeasures, for external attacks on secured time network. Similarly, Table 6 provides this information for internal attacks on a secured time network.

Table 5: External Attacks on Secured Time Network

Threat Type (conducted by external attacker)	Threat Characteristic	Impact	Example	Potential Countermeasures
Interception and Removal	Interruption (MitM)	-Reduced accuracy	-Time control packets are selectively omitted[1]	-Distributed overlaid passive supervisory structures (i.e., network intrusion detection systems, NIDS)
Packet Delay Manipulation	Modification (in the widest sense) (MitM)	-Reduced accuracy	-MitM relays packets with delay	-Distributed overlaid passive supervisory structures (i.e. NIDS) -Trusted platform attestation

[1] An attacker can identify an authenticated / encrypted time protocol packet based on the length of the packet, e.g. source / destination address / port.

Threat Type (conducted by external attacker)	Threat Characteristic	Impact	Example	Potential Countermeasures
Flooding-based general Denial-of-Service (DoS) or Time Protocol DoS	Insertion (MitM or injector)	-Impairment of entire (low-bandwidth) network -Limited or no availability of target	-Rogue node floods IEEE 802.15.4 network with packets -Rogue node overwhelms target with time protocol packets	-Distributed overlaid passive supervisory structures (i.e. NIDS) -Host intrusion detection system (HIDS) that monitors level of activity -Trusted platform attestation -Clock drift correction
Interruption-based general DoS or Time Protocol DoS[2]	Interruption (MitM or potentially injector)	-Impairment of entire network communication -Limited or no availability of target	-Rogue node jams network -Rogue node jams all time-related network packets	-Distributed overlaid passive supervisory structures (i.e. HIDS or NIDS) -Trusted platform attestation -Clock drift correction
Cryptographic Performance Attack	Insertion (MitM or injector)	-Limited or no availability of target	-Rogue node submits packets to peer, that trigger execution of computationally expensive cryptographic algorithm (like the validation of digital certificate)[3]	-Distributed overlaid passive supervisory structures (i.e. HIDS or NIDS) -Trusted platform attestation
Master Time Source Attack	Interruption (MitM or injector)	-Reduced accuracy	-GPS jamming	-Distributed overlaid passive supervisory structures (i.e. NIDS)

[2] This attack is more blunt than the Interception and Removal attack above, as here all time-protocol-related packets are omitted.

[3] The exchange and validation of a certificate as part of the authentication and authorization of a node can be the building block of such an attack.

Table 6: Internal Attacks on Secured Time Network

Threat Type (conducted by internal attacker)	Threat Characteristic	Impact	Example	Potential Countermeasures
Packet Manipulation	Modification (MitM)	-False time	-In-flight manipulation of authenticated / encrypted time protocol packets	-Separate peer-to-peer (P2P) link keys per connection (to limit impact) -Trusted platform attestation
Replay Attack	Insertion / Modification (MitM or injector)	-False time	-Insertion of previously recorded time protocol packets, potentially after adjustment of anti-replay measures (e.g. packet counter)	-Distributed overlaid passive supervisory structures (i.e. NIDS) -Trusted platform attestation
Spoofing	Insertion (MitM or injector)	-False time	-Impersonation of legitimate master or clock	-Trusted platform attestation -Authentication and authorization of network peers
Rogue Master Attack	Insertion (MitM or injector)	-False time	-Rogue master manipulates the master election process using malicious control packets (i.e. manipulates the best master clock algorithm)	-Trusted platform attestation -Authentication and authorization of network peers
Interception and Removal	Interruption (MitM)	-Reduced accuracy	-MitM (i.e. transparent clock) relays packets with delay	-Distributed overlaid passive supervisory structures (i.e. NIDS) -Trusted platform attestation -Delay threshold
Flooding-based general DoS or Time Protocol DoS	Insertion (MitM or injector)	-Impairment of entire (low-bandwidth) network -Limited or no availability of target	-Rogue note floods 802.15.4 network with packets -Rogue node overwhelms target with time protocol packets	-Distributed overlaid passive supervisory structures (i.e. NIDS) -Host intrusion detection system (HIDS) that monitors level of activity -Trusted platform attestation

Threat Type (conducted by internal attacker)	Threat Characteristic	Impact	Example	Potential Countermeasures
				-Clock drift correction
Interruption-based general DoS or Time Protocol DoS	Interruption (MitM or potentially injector)	-Impairment of entire network communication -Limited or no availability of target	-Rogue node jams network -Rogue node jams selectively network packets	-Distributed overlaid passive supervisory structures (i.e. NIDS) -Host intrusion detection system (HIDS) that monitors level of activity -Trusted platform attestation -Clock drift correction
Cryptographic Performance Attack	Insertion (MitM or injector)	-Limited or no availability of target	-Rogue node submits packets to master that trigger execution of computationally expensive cryptographic algorithms (i.e. validation of digital certificate)	-Distributed overlaid passive supervisory structures (i.e. NIDS) -Host intrusion detection system (HIDS) that monitors level of activity -Trusted platform attestation
Master Time Source Attack	-Interruption (MitM or injector) -Insertion (MitM or injector)	-Reduced accuracy -False time	-GPS jamming -GPS spoofing	-Distributed overlaid passive supervisory structures (i.e. NIDS) -Host intrusion detection system (HIDS) that monitors level of activity -Trusted platform attestation

3.6 Securing Time Networks

State-of-the-Art Security Extension and Protocols

There are various approaches to protect communications in time networks, including:

1. Network Time Protocol's (NTP's) [52] Autokey extension [53] and symmetric-key authentication methods protect against packet modification and replay attacks, while providing endpoint (e.g. server) authentication via digital certificates. The IETF NTP Working Group is also developing a revised network time security protocol [54–55].
2. IEEE 1588 Annex K [9] provides group source authentication, message integrity, and replay protection (the latter via a replay counter that reliably identifies stale messages) [56]. A trust relation is established by a challenge-response three-way handshake

mechanism [56], which is based on a set of pre-shared keys [57]. The keys are shared by the whole domain or by subsets of the domain. Annex K is an experimental extension and various improvements have been suggested. These include an improved handshake and replay counter [58]. The IEEE 1588 Working Group Security Subcommittee is developing optional specifications for improving PTP security [9].

3. IPsec is a suite of Layer 3 (L3) security protocols for IP networks supporting either transport mode or tunnel mode that, depending on the configuration, authenticates and / or encrypts IP packet payloads. With Authentication Header (AH), IPsec authenticates non-modifiable sections of the IP header to provide authentication. With Encapsulating Security Payload (ESP) provides both authentication and encryption, In tunnel mode, where an entire IP packet is encapsulated and transmitted between two security gateways. It protects against packet modification, replay attacks and, when used in encrypted tunnel mode, to some extent against eavesdropping.
4. MACsec is a protocol for L2 link-level security based on IEEE 802.1AE (that specifies the encryption and authentication protocol) and IEEE 802.1X (that details session initiation and key management). The security architecture in MACsec follows a hop-by-hop encryption / authentication approach, where packets are decrypted / validated at each bridge in the network, and then encrypted / re-authenticated again before being relayed to its destination. Under the scenarios considered in Ref. [50], MACsec had some advantages relative to IPSec and 1588 Annex K, but still leaves significant gaps.

Message Integrity

Cryptographic functions such as hashing in contrast with packet authentication (via an integrity check value, ICV, based on symmetric message authentication code functions) provides integrity verification[50]. Standard practices and recommendations in network security include:

- 128-bit to 256-bit symmetric key length to avert brute-force attacks; in contrast Autokey has only an effective key length of 32-bit, which is exploited by the “cookie snatching” attack [59].
- AES, the de-facto standard for symmetric encryption, can also be used for message authentication, for example in CMAC (Cipher-based MAC). In contrast, IEEE 1588 Annex K currently supports two algorithms for message authentication:
    - HMAC-SHA1-96, which is outdated and not deemed to be safe anymore.
    - HMAC-SHA256-128, which is robust, but computationally expensive and therefore only suboptimal [58].

- Key rotation and key freshness as well as perfect forward secrecy (PFS)[4] must be provided.
- An authenticated code must not only cover the time protocol section of a network packet, but also the source / destination address in the respective (L2 / L3) packet header; IEEE 1588 Annex K for example omits this feature and is open to MitM-style attacks [60].
- Message authentication and other uses of cryptographic functions (e.g. hashing) requires deterministic latencies to avoid accuracy degradation [8, 61].

Hop-by-Hop versus End-to-End Integrity Protection

PTP packets are subject to modification by transparent clocks (e.g. an update of the correction field). This is supported as follows:

- MACsec provides hop-by-hop integrity protection so transparent clocks (TC) can modify packets in transit. The integrity of protocol packets is protected by induction on the path from the originator to the receiver.
- IPsec, in contrast, provides end-to-end (device or gateway) integrity protection. Here the integrity protection is maintained on the path from the originator of a protocol packet to the receiver. This allows the receiver to directly validate the protocol packet without the ability of intermediate TCs to manipulate / update the packet. While this is a more conservative and safer approach (as there is no potentially rogue intermediate node that can maliciously corrupt data packets), it impacts the achievable accuracy.
- Annex K can provide – dependent on setup and key distribution – hop-by-hop or end-to-end integrity protection.

Reference [56] distinguishes between security-unaware, security-aware and security-capable transparent clocks and outlines how the latter can be used in hybrid time networks.

3.7 Potential Countermeasures

Authentication and Authorization of Network Peers

Common practice to provide host authentication and message integrity in time networks is based on pre-shared master or link keys, potentially in combination with host whitelisting. However, in large scale and / or dynamic networks this approach is not feasible, as it lacks flexibility, scalability, and robustness, while authorization is only granted based on the knowledge of a security credential. Önal et al [58] argue that key management as a whole

[4] PFS means that the compromise of one key cannot lead to the compromise of others, e.g. new key material should not be calculated from old key material or distributed via encryption using old key material.

needs to be addressed (in PTP). NTP provides both symmetric and Autokey authentication approaches. However, given the vulnerabilities of Autokey, only symmetric-key authentication should be used.

The PTP Security Working Group is drafting informative guidance on key management schemes supported by the optional PTP Security Type-Length-Value (TLV) for both peer authentication and authorization. Such a key management scheme could have the following features:

- A tightly managed flat hierarchy of certificate authorities (CA), that in conjunction with registration authorities (RA) issue certificates for all hosts (e.g. master, slaves, (transparent) clocks, router, bridges, etc.) in a time network.
- CAs will issue combined X.509 identity and attribute certificates. The former will be used to authenticate hosts and to negotiate unicast (e.g. peer-to-peer) and multicast session keys, while the latter provides device authorization and other relevant attributes (for example clock parameters for the master clock election process). Note that the Trusted Certificate Scheme in NTP's Autokey extension is flawed [59] and cannot be used as a template.
- During the authentication / authorization process certificates from both endpoints will be mutually authenticated. Additional certificate validation can be provided via Online Certificate Status Protocol (OCSP) or certificate stapling (see RFC 6066 [62] for details). Common key negotiation algorithms (like Elliptic curve Diffie–Hellman) also provide perfect forward secrecy.
- Digital certificates are supported by all mentioned protocols. They can be used for hop-by-hop and end-to-end integrity protection:
    - In IPsec via the Internet Key Exchange (IKE) or IKE2 protocol.
    - In MACsec via IEEE 802.1X, as it encapsulates the Extensible Authentication Protocol (EAP) and, in particular, EAP-TLS.
    - Annex K can be complemented by IPsec, MACsec or alternatively by Transport Layer Security (TLS). TLS provides application-layer process-to-process authentication rather than device to-device-authentication.

Trusted Platform Attestation

State-of-the-art secured time networks are susceptible to a range of internal attacks conducted by legitimate devices, which cannot be deflected via peer authentication or authorization. Such devices act maliciously for a range of reasons including software bugs and malware infections.

A potential solution to this problem is the provision of validated hardware and software platforms, based on the work of the Trusted Computing Group. Potential features could include the Trusted Network Connect (an open architecture for network access control) and trusted software stacks.

Intrusion Detection Systems

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations. Network intrusion detection systems (NIDS) are placed at strategic points within a network to monitor traffic to and from all devices within the network. They perform an analysis of passing traffic to detect attacks. Host intrusion detection systems (HIDS) in contrast run on individual hosts or devices on the network and monitor the inbound and outbound packets from the device only.

Malicious activities are detected by different means including blacklisting / whitelisting, statistical analysis, deep packet inspection etc.

NIDS are a proven approach to detect (flooding-based) DoS attacks[5] and can potentially find Interception and Removal attacks, Interruption-based DoS attacks and Cryptographic Performance Attacks. They may be suitable to detect Packet Delay Manipulation attacks (as they require accurate time for this task) and Master Time Source attacks.

Delay Threshold

Tournier et al. [63] suggests detecting packet delay manipulations via a mechanism that sets a threshold for each delay based on the previous experiences.

Clock Drift Correction

Tournier et al. [63] describes a clock drift correction algorithm, which uses time series prediction to re-synchronize slaves during DoS attacks.

3.8 Secure Time Use Cases

GPS: Tripping generators off of the electric grid

Tripping generators off of the electric grid can be done for operational or malevolent purposes. Grid managers, in particular Balancing Authorities, will trip generators off of the grid when supply exceeds demand. Energy demand can change on a diurnal, hourly and even minute-by-minute basis. Automated protection schemes or grid operators may trip generators to maintain system stability, for example, when different generators run out of phase with each other

[5] On the other hand, PTP slave devices are aware of DoS attacks [56], so a NIDS does not add value other than logging and monitoring attacks.

and/or the grid. The risk of tripping generators as an attack is potentially more damaging as the intention is to thwart automated control systems or human operators to take actions based on false premises resulting in significant governor and voltage control issues. The action of unnecessarily tripping generators or inaction in tripping generators when needed can lead to blackouts or significant power system damage.

There is a dramatic difference between the impacts of GPS timing denial and spoofing within automated synchrophasor control schemes.

Impacts of Denial: GPS time denial from either a localized attack or from widespread disruption due to a severe geomagnetic storm will cause synchrophasors to cease to function. That alone will not generally have a direct impact on the grid unless it occurs in the middle of executing a control action, which is a low probability. When GPS is lost or denied due to intentional jamming, grid managers will resort to manual operations as they have done in the past. Grid managers will remain able to remotely dispatch or trip generators off line if grid stability conditions warrant it.

Impacts of Spoofing: The impacts of timing spoofing – almost always an intentional malicious act – can be much more severe than denial. Spoofing is potentially more damaging than jamming because it can cause automated control systems or human operators to take incorrect and potentially harmful actions in controlling grid systems.

An attack could begin with an attack on the GPS-timing supporting synchrophasors or phasor measurement units (PMUs). Without spoofing detection or mitigation in place the attack would be unimpeded and could persist for a long period of time. The PMU is incorporated in a control scheme that is designed to trip generators offline if their frequency or phase becomes significantly different from that of the power grid (in order to prevent damage to those generators). This attack is modeled after the scenarios in Refs. [64–65].

In accordance with that scenario, a threshold could be set in the PMU such that if the generator phase were 10 degrees or more out of phase with the phase of the grid the PMU would trip the generator offline. This timing walk-off of a GPS receiver within a PMU by 10 degrees has been demonstrated in a lab environment [65].

Several large generators (e.g., 1000 MW or greater) suddenly tripping offline would create an instantaneous supply-demand imbalance and grid instability in a local control area or region. The individual utility control centers and regional control center would attempt to take action to prevent a blackout.

Mitigation of Impacts by Adoption of Elements of Secure Timing:
Three elements of secure timing would mitigate the impacts of GPS jamming and spoofing:

- Detection of jamming and spoofing by the potentially impacted end-use device/equipment;

- Alarming the human operator associated with the device; and
- Enabling manual or automated switchover (failover) to an equally precise, trusted, backup timing source either internal or external to the device.

There are commercially available products on the market today that satisfy all three elements of secure timing with respect to jamming threats. For spoofing, there are no commercially available products available to civilian users.

Commercial phasor measurement units or synchrophasors, like other commercial GPS-based equipment, do not currently possess any of the three elements of secure timing. Therefore GPS-based synchrophasors, when used in automated control applications, put the grid at risk as illustrated above.

There are some methods to mitigate GNSS spoofing that have been developed by the research and development community [35, 66-67]. Driven by customer demand, commercial anti-spoofing products will become available for civilian users.

Network: Digital substation automation

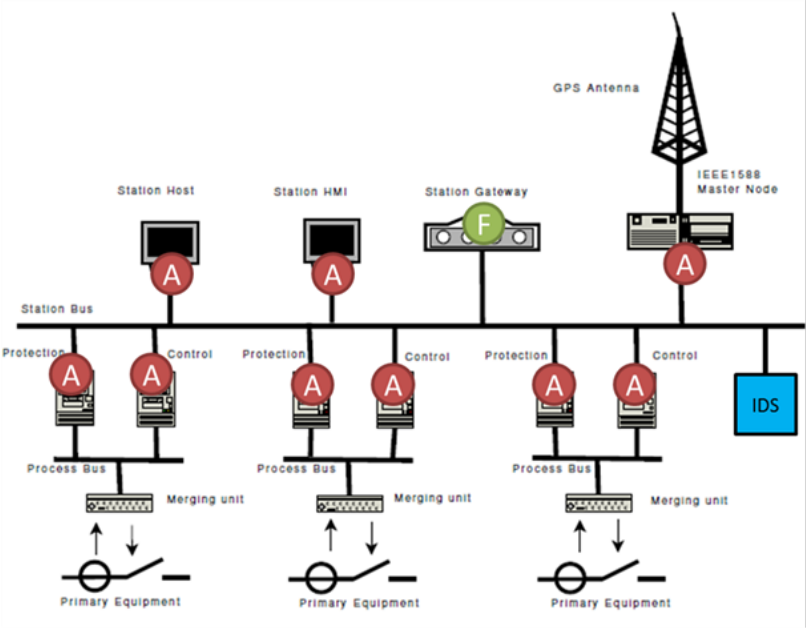
An electric substation is a node in the power grid network that transmits and distributes electric energy from power sources to consumers. Equipment used at an electric substation can be categorized as primary equipment (switchgears, breakers, transformers) and secondary equipment (sensors, merging units, intelligent electronic devices) [63].

To enable efficient protection functions, synchronized data provided by the various devices forming the secondary equipment is needed. This synchronization, depending on the desired function, is either local (self-consistent, in which the devices of one substation are synchronized) or global (devices from different substations are synchronized). Different classes of synchronization are identified, ranging from 1 microsecond (class T5) to 1 millisecond (class T1) [63].

Impacts of Cyber Attacks: An IEEE1588-based synchronization architecture, shown in Fig. 12 [63], consists of a GPS receiver per substation which distributes the time to the different devices. This system is vulnerable to the following attacks:

- A timing-denial attack could be conducted either via GPS denial or via (selective) interference with network / PTP traffic on the Station Bus. This attack would result in a loss of accurate time in one or more subsystems, resulting in an infringement of local or global synchronization.
- A spoofing-style attack could be initiated by any device (temporarily) connected to the station bus, or via an external device that reaches the substation via a poorly protected Station Gateway. This attack would provide individual or all subsystems with false time, therefore resulting in an infringement of local or global synchronization.

Spoofing-style attacks can eventually lead to the failure of the substation or the grid it is connected to by compromising the fidelity of the time. For example, undetected timing errors can cause the phasor measurement units to have erroneous values leading to false alarms with respect to grid instability. DoS style attacks over extended periods on the (autonomously operating) substation could potentially have a similar impact, if communication to the remote operator / SCADA system via the Station Gateway or other redundant backup communication channel is affected as well.



"A" indicates secure time protocol stack implementations,
"F" indicates firewall, and
"IDS" indicates Intrusion Detection System

FIGURE 12. SYNCHRONIZATION ARCHITECTURE OF AN ELECTRIC SUBSTATION

(Adapted from J. Tournier et al. "Strategies to Secure the IEEE 1588 Protocol in Digital Substation Automation" in *Fourth International Conference on Critical Infrastructures (CRIS)* 2009 [63], Fig.1 © 2009 IEEE, used with permission.)

Mitigation of Impacts by Adoption of Elements of Secure Timing: Fig. 12 shows the main components of a secure synchronization architecture:

- All PTP-enabled (internal) subsystems have a secure time protocol stack implementation (indicated by "A" in Fig. 12). They share a set of security credentials that – in combination with a security protocol like IPsec or MACsec - provide a combination of source channel assurance through host authentication / authorization, and source data assurance through message authentication and message encryption. Secure credentials can be based on pre-shared symmetric keys or digital certificates, with the latter being a more flexible approach that supports host authorization as well.
- Traceability to standard reference time via GPS is maintained assuming that the GPS and PTP networks are secure.

- A diversity of network paths, devices and grandmaster sources can also mitigate certain attacks. A redundant grandmaster with rubidium can provide holdover of UTC time to within a day and sometimes up to a week depending on how long the rubidium clock was disciplined by the GPS receiver. The CPS network topology using PTP can be architected to have multiple paths to reach the redundant grandmasters. Ring topologies include but are not limited to Rapid Spanning Tree Protocol (RSTP), Media Redundancy Protocol (MRP) and high-availability seamless redundancy (HSR). In experimental tests, MRP was shown to be able to maintain time synchronization within the hundreds of nanoseconds range whereas RSTP exceeded the microsecond tolerance threshold [68].
- Predictable failure can be achieved through the Intrusion Detection System (indicated by "IDS" in Fig. 12) which inspects Station Bus traffic for suspicious patterns (e.g. packet flooding / DoS, etc.). If a compromise of the source or path node is detected, the reference source or PTP paths can be redirected using diverse and redundant paths. If no redundant source and paths are available, the CPS must account for the loss of timing synchronization and operate under a timing fail-safe mode.
- Additional user provided assurance can be achieved by:
    - Isolating the Station Bus from the outside network via a firewall (indicated by "F" in Fig. 12) on the station gateway.
    - The local stations bus can be further physically protected (e.g. isolated) to prevent attacks from temporally attached external nodes (see Crain / Sistrunk Distributed Network Protocol (DNP3) vulnerability [69]).
    - PTP enabled subsystems can compensate DoS attacks via clock drift [63].

Properly implemented secure synchronization architecture will provide source channel assurance, source data assurance and traceability. However, if one of the secured internal subsystems is compromised (e.g., a malware infection of the Station Host in Fig. 12), the entire substation is again vulnerable to all attacks listed in Table 5.

4 Timing Requirements (Use Cases)

To illustrate the variety of timing requirements in CPS, examples are provided in the table below. The application areas chosen in the figure mostly lie within what are termed Critical Infrastructure & Key Resources (CIKR). In addition, some of the timing use cases listed include currently unsolved timing problems.

Table 7: Examples of Timing Requirements in CPS

CPS Application Areas	Example	Type of Timing UTC/Phase/Freq	Accuracy Requirements*
Communications Sector		Frequency	Better than 10^{-11} (SONET, SDH)
	Evolution of Mobile from 4G to 5G	Phase	< 1 μs
	Software-Defined Networking and Network Function Virtualization	UTC	< 100 ns
	Real-Time Communications Cross Layer Quality of Service Provisioning	UTC	1 ms
	Real-Time Media Synchronization	UTC	1μs
Emergency Services Sector	Phase for Positioning (CDMA E911, LMRs)		nss
Energy/Electric Power Subsector	Synchrophasors Fault Localization	UTC Frequency Phase	1 μs to 5 μs
Health Sector	Patient Care Devices signal correlation	Phase	ms
	Remote Surgery/Intervention	Bounded Latency Phase	< 150 ms (< 10 ms with haptic feedback)
Critical Manufacturing Sector			ms
	Robotics Real-Time Coordination	UTC Phase	1 μs
Defense Industrial Base Sector	Various	Various	ns to ms
Transportation Sector	Wireless Modal Communications		ns
	Unmanned Aerial Vehicles (UAV) Unmanned Ground Vehicles (UGV) Positioning and Navigation	UTC	ns
	Intra-Vehicle Synchronized Signaling	Phase	10 ms to 50 ms
	Vehicle-to-Vehicle and Vehicle-to-Road Synchronized Signaling	UTC Phase	10 ms to 50 ms
	Aircraft Diagnostics	UTC Phase	10 ms to 50 ms
	Aerospace Test Instrumentation and Telemetry	Phase	< 100 ns
	Bridge Structural Integrity Monitoring	Phase	< 100 ns

CPS Application Areas	Example	Type of Timing UTC/Phase/Freq	Accuracy Requirements*
	Traffic Control	Phase UTC	10 ms to 50 ms
Smart Buildings	HVAC Optimization Computational Fluid Dynamics Modelling	Phase	10 ms to 50 ms
	Energy Management System Fault Diagnosis	Phase UTC	1 ms
Environmental Monitoring	Pollution Monitoring/Alert System	Phase UTC	< 1 s
	Extreme Weather Mitigation	UTC	< 1 s
Smart Agriculture	Precision Nutrient Management Location	UTC	< 100 ns
Consumer Devices	Multimedia Synchronization	UTC	1μs
	Virtual Reality Psycho-acoustics	Phase	1 μs

* The accuracy requirements in this table reflect the input of CPS PWG Timing subgroup members based on a variety of sources (including [38] and private communications).

Appendix A. References

[1] ITU-R Recommendation TF.686-3 (12/2013) “Glossary and Definitions of Time and Frequency Terms,” TF Series Time signals and frequency standards emissions, available from http://www.itu.int/rec/R-REC-TF.686-3-201312-I/en Note: this document contains references to additional glossary and definition material published by NIST, BIPM, IEC and the ISO.

[2] The time scales UTC and TAI and the International System of Units, SI, are defined and maintained by the International Bureau of Weights and Measures (Bureau International des Poids et Mesures, BIPM). See http://www.bipm.org

[3] ITU-R G.8260 (08/2015) “Definitions and terminology for synchronization in packet networks” Series G: Transmission Systems and Media, Digital Systems and Networks, available from https://www.itu.int/rec/T-REC-G.8260/en

[4] D.B. Sullivan et al. (1999) “Characterization of Clocks and Oscillators,” NIST Tech. Note 1337, available from http://tf.boulder.nist.gov/general/pdf/868.pdf

[5] H. Kopetz and G. Bauer (2003) “The time-triggered architecture,” *Proceedings of the IEEE*, 91(1):112–126.

[6] J. Jasperneite and J. Feld (2005) "PROFINET: an integration platform for heterogeneous industrial communication systems," *2005 IEEE Conference on Emerging Technologies and Factory Automation*, https://doi.org/10.1109/ETFA.2005.1612610

[7] Timing Committee Telecommunications and Timing Group- Range Commanders Council (2004) “IRIG Serial Time Code Formats” available online at http://www.irigb.com/pdf/wp-irig-200-04.pdf

[8] E. Kaplan and C. Hegarty, eds. (2005) *Understanding GPS: principles and applications*. Artech House.

[9] IEEE 1588 Standard (IEEE 1588-2008), “1588: IEEE standard for a precision clock synchronization protocol for networked measurement and control systems” https://standards.ieee.org/findstds/standard/1588-2008.html Note: 1588 Working Group is described at https://ieee-sa.imeetcentral.com/1588public/

[10] K. Harris (2008) “An application of IEEE 1588 to industrial automation,” *2008 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, pp 71-76, https://doi.org/10.1109/ISPCS.2008.4659216

[11] M. Shepard, D. Fowley, R. Jackson, and D. King (2003) "Implementation of IEEE Std-1588 on a Networked I/O Node," *Proceedings of the 2003 Workshop on IEEE-1588*, NIST publication NISTIR 7070.

[12] F. Steinhauser, C. Riesch, and M. Rudigier (2010) "IEEE 1588 for time synchronization of devices in the electric power industry," in *2010 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, pp 1-6. https://doi.org/10.1109/ISPCS.2010.5609787

[13] G. Buttazzo (2011) *Hard Real-Time Computing Systems: Predictable Scheduling Algorithms and Applications, Third Edition*. Springer, pp 1-521. https://doi.org/10.1007/978-1-4614-0676-1

[14] R. Wilhelm and D. Grund (2014) "Computation takes time, but how much?" *Communications of the ACM* 57(2): 94-103 https://doi.org/10.1145/2500886

[15] P. Axer, R. Ernst, H. Falk, A. Girault, D. Grund, N. Guan, B. Jonsson, P. Marwedel, J. Reineke, C. Rochange, M. Sebastian, R. von Hanxleden, R. Wilhelm, and W. Yi (2014) "Building timing predictable embedded systems" *ACM Transactions on Embedded Computing Systems (TECS)* 13(4): 82 https://doi.org/10.1145/2560033

[16] R. Wilhelm, J. Engblom, A. Ermedahl, N. Holsti, S. Thesing, D.B. Whalley, G. Bernat, C. Ferdinand, R. Heckmann, T. Mitra, F. Mueller, I. Puaut, P. Puschner, J. Staschulat, and P. Stenström (2008) "The worst-case execution-time problem - overview of methods and survey of tools" *ACM Transactions on Embedded Computing Systems (TECS)* 7(3): 36 https://doi.org/10.1145/1347375.1347389

[17] J. Rushby and W. Steiner (2011) "TTA and PALS: Formally verified design patterns for distributed cyber-physical systems" *30th IEEE/AIAA Digital Avionics Systems Conference (DASC),* https://doi.org/10.1109/DASC.2011.6096120

[18] E. Lee (2009) "Computing needs time" *Communications of the ACM* 52(5): 70-79 https://doi.org/10.1145/1506409.1506426

[19] J. Corbett et al. (2013) "Spanner: Google's globally distributed database" *ACM Transactions on Computer Systems (TOCS) 31.3*, available at https://www.usenix.org/system/files/conference/osdi12/osdi12-final-16.pdf

[20] Y. Zhao, E. Lee, and J. Liu (2007) "A programming model for time-synchronized distributed real-time systems" *13th IEEE Real Time and Embedded Technology and Applications Symposium (RTAS 2007*), pp 259-268. https://doi.org/10.1109/RTAS.2007.5

[21] D. Broman, P. Derler, and J. Eidson (2013) "Temporal issues in cyber-physical systems" *Journal of the Indian Institute of Science* 93(3): 389-402

[22] IEEE 802.1AS-2011 Standard (2011) "2.1AS-2011 - IEEE Standard for Local and Metropolitan Area Networks - Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks" http://standards.ieee.org/findstds/standard/802.1AS-2011.html

[23] IEEE 802.1Q Standard (2014) "802.1Q-2014 - IEEE Standard for Local and metropolitan area networks--Bridges and Bridged Networks" https://standards.ieee.org/findstds/standard/802.1Q-2014.html Note: additional information on working group WG802.1 is at http://www.ieee802.org/1/

[24] IEEE 802.1CB "802.1CB - Frame Replication and Elimination for Reliability" draft standard (in preparation) http://standards.ieee.org/develop/project/802.1CB.html and http://www.ieee802.org/1/pages/802.1cb.html

[25] IEEE 801.11-2016 Standard (2016) "IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" http://standards.ieee.org/about/get/802/802.11.html

[26] ITU-T Recommendations. All ITU-T published recommendations can be downloaded from http://www.itu.int/rec/T-REC-G/e
ITU-T Published Recommendations associated with timing in telecom networks are listed below:

ITU-T Published Recommendations (PDH/SDH)
ITU-T Recommendation G.803, Architecture of transport networks based on the synchronous digital hierarchy (SDH)
ITU-T Recommendation G.810, Definitions and terminology for synchronization networks
ITU-T Recommendation G.811, Timing characteristics of primary reference clocks
ITU-T Recommendation G.812, Timing requirements of slave clocks suitable for use as node clocks in synchronization networks
ITU-T Recommendation G.813, Timing characteristics of SDH equipment slave clocks (SEC)
ITU-T Recommendation G.823, The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy
ITU-T Recommendation G.824, The control of jitter and wander within digital networks which are based on the 1544 kbit/s hierarchy
Recommendation ITU-T G.825, The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)

ITU-T Published Recommendations (Packet Sync - Frequency)
ITU-T Recommendation G.8261, Timing and synchronization aspects in packet networks
ITU-T Recommendation G.8262, Timing characteristics of Synchronous Ethernet Equipment slave clock (EEC)
ITU-T Recommendation G.8264, Distribution of timing through packet networks
ITU-T Recommendation G.8261.1, Packet Delay Variation Network Limits applicable to Packet Based Methods (Frequency Synchronization)
ITU-T Recommendation G.8263, Timing Characteristics of Packet based Equipment Clocks (PEC) and Packet based Service Clocks (PSC)
ITU-T Recommendation G.8265, Architecture and requirements for packet based frequency delivery
ITU-T Recommendation G.8265.1, Precision time protocol telecom profile for frequency sync
ITU-T Recommendation G.8260, Definitions and terminology for synchronization in packet networks

ITU-T Consented Recommendations (Packet Sync – Phase/Time)
ITU-T Recommendation G.8271, Time and phase synchronization aspects of packet networks
ITU-T Recommendation G.8272, Timing characteristics of Primary reference time clock
ITU-T Recommendation G.8271.1, Network limits
ITU-T Recommendation G.8272, Primary Reference Timing Clock (PRTC) specification
ITU-T Recommendation G.8273, Clock General Requirements
ITU-T Recommendation G.8273.2, Telecom Boundary Clock specification
ITU-T Recommendation G.8275, Architecture for time transport
ITU-T Recommendation G.8275.1, IEEE-1588 profile for time with full support from the network

[27] IETF Deterministic Networking (DetNet) Working Group, 2015, described at https://datatracker.ietf.org/wg/detnet/charter/

[28] S. Chandhoke, National Instruments, personal communication, 2014 (also see M. Weiss, “Time-Awareness in the Internet of Things” 2014, available online at https://www.nuigalway.ie/media/publicsub-sites/engineering/files/Time-AwarenessIoT.pdf)

[29] R. Buyya (1998) *The Design of PARAS Microkernel*, Centre for Development of Advanced Computing (C-DAC), Bangalore, India http://www.buyya.com/microkernel/

[30] W. Stallings (2008) *Operating Systems: Internals and Design Principles (6th Edition)*, Pearson International Edition

[31] Silberschatz, Galvin, and Gagne (2009) *Operating System Concepts, 8th Edition,* John Wiley and Sons, Inc.

[32] "GPS jamming: No jam tomorrow" *The Economist*, March 10, 2011, available at http://www.economist.com/node/18304246

[33] "GPS jamming: Out of Sight" *The Economist*, July 27, 2013, available at http://www.economist.com/news/international/21582288-satellite-positioning-data-are-vitalbut-signal-surprisingly-easy-disrupt-out

[34] D. Shepard, J.A. Bhatti, and T. Humphreys (2012) "Drone Hack: Spoofing Attack Demonstration on Civilian Unmanned Aerial Vehicle" *GPS World*, August 1, 2012, available at http://gpsworld.com/drone-hack/

[35] R. Langley (2012) "Innovation: GPS Spoofing Detection" *GPS World*, Jun 1, 2013, available at http://gpsworld.com/innovation-gnss-spoofing-detection-correlating-carrier-phase-with-rapid-antenna-motion/

[36] A.J. Kerns, K.D. Wesson, and T. Humphreys (2014) "A blueprint for civil GPS navigation message authentication," *Proceedings of IEEE/ION PLANS 2014*, Monterey, CA, May 2014, pp 262-269. https://doi.org/10.1109/PLANS.2014.6851385

[37] D. Fontanella, R. Bauernfeind, and B. Eissfeller (2013) "In-Car GNSS Jammer Localization Using Vehicular Ad-Hoc Networks" *Inside GNSS*, May/June 2013, available at http://www.insidegnss.com/auto/mayjune13-WP.pdf

[38] R.J. Caverly (2011) "GPS Critical Infrastructure: Usage/Loss Impacts/Backups/Mitigation" April 27, 2011, available at http://www.swpc.noaa.gov/sites/default/files/images/u33/GPS-PNTTimingStudy-SpaceWeather4-27.pdf

[39] "The Global Differential GPS System: Integrity and Performance Monitoring" NASA Jet Propulsion Laboratory, available at http://www.gdgps.net/products/monitoring.html (website accessed July 7, 2017).

[40] G. Hein, F. Kneissl, and C. Stober, (2010) "Combined Integrity of GPS and Galileo", *Inside GNSS*, January/February 2010, available at http://www.insidegnss.com/auto/IGM_wp-janfeb10.pdf

[41] National Research Council (2008) *Severe Space Weather Events: Understanding Societal and Economic Impacts: A Workshop Report*, The National Academies Press, p 78. https://doi.org/10.17226/12507

[42] J. Kappenman (2010) "Geomagnetic Storms and their Impacts on the U.S. Power Grid," Metatech Corporation, Meta-R-319, prepared for Oak Ridge National Laboratory for the

Federal Energy Regulatory Commission (FERC), the U.S. Department of Energy (DOE), and the U.S. Department of Homeland Security (DHS), January 2010, available at https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf

[43] K. Jaldehag, S. Ebenhag, P. Hedekvist, C. Rieck, and P. Lothberg (2009) "Time and Frequency Transfer Using Asynchronous Fiber Optical Networks: Progress Report" *Proceedings of 41st Annual Precise Time and Time Interval (PTTI) Meeting,* pp 383-396.

[44] M. Weiss et al. (2016) "Precision Time Transfer using IEEE 1588 over OTN through a Commercial Optical Telecommunications Network" *2016 International IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication (ISPCS)* 4-9 September 2016, pp 1-5. https://doi.org/10.1109/ISPCS.2016.7579503

[45] M. Lipinski et al. (2012) "Performance results of the first white rabbit installation for CNGS time transfer" *2012 International IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication (ISPCS)* 24-28 September 2012, pp 1-6. https://doi.org/10.1109/ISPCS.2012.6336610

[46] J. Lowe and M. Weiss (2013) "CONTRIBUTION TO STANDARDS PROJECT — COAST-SYNC: WWVB for Assisted Timing" ATIS COAST Standards Body, document SYNC-2014-00052R000 contributed by NIST.

[47] G. Kamas and M. Lombardi (1990) Time and Frequency Users Manual, NIST Special Publication 559 (Revised 1990), p 91, available at http://tf.boulder.nist.gov/general/pdf/461.pdf

[48] G.S. Johnson et al. (2007) "An Evaluation of eLoran as a Backup to GPS" *2007 IEEE Conference on Technologies for Homeland Security*, pp 95-100. https://doi.org/10.1109/THS.2007.370027

[49] The MITRE Corporation (2014) "Detection, Localization, and Mitigation Technologies for Global Positioning System (GPS) Jamming and Spoofing (Final)" Redacted for Public Release, February 2014.

[50] T. Mizrahi (2011) "Time synchronization security using IPsec and MACsec" *2011 International IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication (ISPCS)* 12-16 September 2011, pp 38-43. https://doi.org/10.1109/ISPCS.2011.6070153

[51] T. Mizrahi (2014) "Security Requirements of Time Protocols in Packet-Switched Networks" RFC 7384 Internet Engineering Task Force (IETF), available at https://www.rfc-editor.org/rfc/rfc7384.txt

[52] NTP: The Network Time Protocol, available at http://www.ntp.org/

[53] B. Haberman et al. (2010) "Network Time Protocol Version 4: Autokey Specification" RFC 5906 Internet Engineering Task Force (IETF), available at https://tools.ietf.org/html/rfc5906

[54] D. Sibold, S. Roettger, K. Teichel (2016) "Network Time Security" Internet Engineering Task Force (IETF), available at https://tools.ietf.org/html/draft-ietf-ntp-network-time-security-15

[55] D. Sibold et al. (2016) "Protecting Network Time Security Messages with the Cryptographic Message Syntax (CMS)" Internet Engineering Task Force (IETF), available at https://tools.ietf.org/html/draft-ietf-ntp-cms-for-nts-message-06

[56] A. Treytl, G. Gaderer, B. Hirschler, and R. Cohen (2007) "Traps and pitfalls in secure clock synchronization" *2007 International IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication (ISPCS)* 1-3 October 2007, pp 18-24. https://doi.org/10.1109/ISPCS.2007.4383768

[57] A. Treytl and B. Hirschler (2011) "Validation and Verification of IEEE 1588 Annex K" *2011 International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS)* 12-16 September 2011, pp 44-49. https://doi.org/10.1109/ISPCS.2011.6070156

[58] C. Önal and H. Kirrmann (2012) "Security improvements for IEEE 1588 Annex K: Implementation and comparison of authentication codes" *2012 International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS)* 24-28 September 2012, pp 1-6. https://doi.org/10.1109/ISPCS.2012.6336632

[59] S. Röttger (2011) "Analysis of the NTP Autokey Extension" (in German) University of Braunschweig and Physikalisch-Technische Bundesanstalt Braunschweig; see also presentation D. Sibold and S. Röttger (2012) "Analysis of NTP's Autokey Protocol" (in English) *IETF 83 Proceedings*, available at https://www.ietf.org/proceedings/83/slides/slides-83-tictoc-1.pdf

[60] A. Treytl and B. Hirschler (2009) "Security Flaws and Workarounds for IEEE 1588 (Transparent) Clocks" *2009 International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS)* 12-16 October 2009, pp 1-6. https://doi.org/10.1109/ISPCS.2009.5340204

[61] A. Treytl and B. Hirschler (2008) "Practical Application of 1588 Security" *2008 International IEEE Symposium on Precision Clock Synchronization for Measurement,*

Control and Communication (ISPCS) 22-26 September 2008, pp 37-43. https://doi.org/10.1109/ISPCS.2008.4659210

[62] D. Eastlake (2011) "Transport Layer Security (TLS) Extensions: Extension Definitions" RFC 6066 Internet Engineering Task Force (IETF), available at https://tools.ietf.org/html/rfc6066

[63] J. Tournier and O. Goerlitz (2009) "Strategies to Secure the IEEE 1588 Protocol in Digital Substation Automation" *Fourth International Conference on Critical Infrastructures (CRIS)* 27-30 April 2009, pp 1-8. https://doi.org/10.1109/CRIS.2009.5071498

[64] D. Shepard et al. (2012) "Going Up Against Time: The Power Grid's Vulnerability to GPS Spoofing Attacks" *GPS World*, August 2012, available at http://gpsworld.com/wirelessinfrastructuregoing-against-time-13278/

[65] D. Shepard et al. (2012) "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks" *Proceedings of the ION GNSS Meeting*, Nashville, TN, 2012, available at https://radionavlab.ae.utexas.edu/images/stories/files/papers/PMUAndUAVSpoofingION2012.pdf

[66] The MITRE Corporation (2014) "Time Anomaly Detection Appliqué (TADA)" available at http://www.mitre.org/research/technology-transfer/technology-licensing/time-anomaly-detection-appliqu%C3%A9-tada

[67] T. Pearson and K. Shenoi (2014) "A Case for Assisted Partial Timing Support Using Precision Timing Protocol Packet Synchronization for LTE-A" *IEEE Communications Magazine*, 52 (8) pp 135-143. https://doi.org/10.1109/MCOM.2014.6871681

[68] J. Amelot et al. (2011) "An IEEE 1588 Performance Testing Dashboard for Power Industry Requirements" *2011 Proceedings of International IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication (ISPCS)* 12-16 September 2011, pp 132-137. https://doi.org/10.1109/ISPCS.2011.6070157

[69] A. Crain and C. Sistrunk (2013) Advisory (ICSA-13-210-01), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), available at https://ics-cert.us-cert.gov/advisories/ICSA-13-219-01

Appendix B. Definitions and Acronyms

The following definitions and acronyms are presented as a ready reference to the intended meaning of their use in the text of this document. It is recognized that within various technical domains, many of these terms and acronyms have multiple meanings. The intent is to provide clarity for the interpretation of this framework and not to make a definitive statement about the "universal" definition of the terms and acronyms.

B.1 Definitions

Selected terms used in this document (or in NIST SP 1500-201 or NIST SP 1500-202) are defined below.

Term	Definition	Source
accuracy	Closeness of the agreement between the result of a measurement and the true value of the measurand.	ITU-R Rec. TF.686
ageing	The systematic change in frequency with time due to internal changes in the oscillator. NOTE 1 – It is the frequency change with time when factors external to the oscillator (environment, power supply, etc.) are kept constant.	ITU-R Rec. TF.686
aspect	Conceptually equivalent concerns, or major categories of concerns. Sometimes called "cross-cutting" concerns.	NIST SP 1500-201
assurance	The level of confidence that a CPS is free from vulnerabilities, either intentionally designed into it or accidentally inserted during its lifecycle, and that the CPS functions in the intended manner.	NIST SP 1500-201
assurance level	The Evaluation Assurance Level (EAL1 through EAL7) of an IT product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation, an international standard in effect since 1999. The increasing assurance levels reflect added assurance requirements that must be met to achieve Common Criteria certification. The intent of the higher levels is to provide higher confidence that the system's principal security features are reliably implemented. The EAL level does not measure the security of the system itself, it simply states at what level the system was tested.	NIST SP 1500-201
assured time	Time derived from a known good time reference in a secure manner.	NIST SP 1500-202

Term	Definition	Source
calibration	The process of identifying and measuring offsets between the indicated value and the value of a reference standard used as the test object to some determined level of uncertainty. NOTE 1 – In many cases, e.g., in a frequency generator, the calibration is related to the stability of the device and therefore its result is a function of time and of the measurement averaging time.	ITU-R Rec. TF.686
certificate	A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity. Additional information in the certificate could specify how the key is used and its cryptoperiod.	NIST SP 800-21
certificate revocation list (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority	NIST SP 800-63; FIPS 201
checksum	Value computed on data to detect error or manipulation	CNSSI-4009
clock	A device that generates periodic signals for synchronization. Note: Other definitions are provided in different references that are tailored to particular applications. Suitable references include ITU-T Rec. G.810, ITU-R Rec. TF.686 and IEEE Std. 1377-1997.	IEEE Std. 1377-1997
concern	Category of analysis by which a CPS can be considered	NIST SP 1500-201
CPS architecture	A concrete realization of a reference CPS architecture designed to satisfy use-case-specific constraints.	NIST SP 1500-201
CPS Framework	Abstract framework and analysis methodology for understanding and deriving application-domain-specific CPS architectures. Activities and outputs to support engineering of CPS.	NIST SP 1500-201
CPS network manager	A work-station or CPS node connected to a CPS domain that manages and monitors the state and configuration of all CPS nodes in one or more CPS domains.	NIST SP 1500-202
CPS time domain	A CPS time domain is a logical group of CPS nodes and bridges which form a network with their own timing master.	NIST SP 1500-202
credential (electronic)	Digital documents used in authentication that bind an identity or an attribute to a subscriber's token	CNSSI-4009

Term	Definition	Source
cross-cutting concern	See aspect	NIST SP 1500-201
cryptographic (encryption) certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes	NIST SP 800-32
cryptographic hash (function)	A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties: 1) (One-way) It is computationally infeasible to find any input which maps to any pre-specified output, and 2) (Collision resistant) It is computationally infeasible to find any two distinct inputs that map to the same output.	NIST SP 800-21
cryptographic key	A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification	NIST SP 800-63
cyber-physical device	A device that has an element of computation and interacts with the physical world through sensing and actuation.	NIST SP 1500-201
cyclical redundancy check (CRC)	A method to ensure data has not been altered after being sent through a communication channel	NIST SP 800-72
digital entity	An entity represented as, or converted to, a machine-independent data structure consisting of one or more elements in digital form that can be parsed by different information systems; and the essential fixed attribute of a digital entity is its associated unique persistent identifier, which can be resolved to current state information about the digital entity, including its location(s), access controls, and validation, by submitting a resolution request to the resolution system.	NIST SP 1500-202
digital signature	An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation	NIST SP 800-63
epoch	Epoch signifies the beginning of an era (or event) or the reference date of a system of measurements.	ITU-R Rec. TF.686
facet	Facets are perspectives on CPS that each express a distinct set of well-defined processes, methods and tools to support the CPS development process and for expressing the architecture of a system. The Framework	NIST SP 1500-201

Term	Definition	Source
	identified facets are conceptualization, realization and assurance.	
formal syntax	Specification of the valid sentences of a formal language using a formal grammar. NOTE 1 A formal language is computer-interpretable. NOTE 2 Formal grammars are usually Chomsky context-free grammars. NOTE 3 Variants of Backus-Naur Form (BNF) such as Augmented Backus-Naur Form (ABNF) and Wirth Syntax Notation (WSN) are often used to specify the syntax of computer programming languages and data languages. EXAMPLE 1 An XML document type definition (DTD) is a formal syntax. EXAMPLE 2 ISO 10303-21, contains a formal syntax in WSN for ISO 10303 physical files.	NIST SP 1500-202

Term	Definition	Source
fractional frequency deviation	The difference between the actual frequency of a signal and a specified nominal frequency, divided by the nominal frequency.	ITU-T Rec. G.810
frequency	If T is the period of a repetitive phenomenon, then the frequency f = 1/T. In SI units the period is expressed in seconds, and the frequency is expressed in hertz (Hz).	ITU-R Rec. TF.686
frequency drift	A systematic undesired change in frequency of an oscillator over time. Drift is due to ageing plus changes in the environment and other factors external to the oscillator. See “ageing”.	ITU-R Rec. TF.686
frequency instability	The spontaneous and/or environmentally caused frequency change of a signal within a given time interval. NOTE 1 – Generally, there is a distinction between systematic effects such as frequency drift and stochastic frequency fluctuations. Special variances have been developed for the characterization of these fluctuations. Systematic instabilities may be caused by radiation, pressure, temperature, and humidity. Random or stochastic instabilities are typically characterized in the time domain or frequency domain. They are typically dependent on the measurement system bandwidth or on the sample time or integration time. See Recommendation ITU-R TF.538.	ITU-R Rec. TF.686
frequency offset (see also fractional frequency deviation)	The frequency difference between the realized value and the reference frequency value. NOTE 1 – The reference frequency may or may not be the nominal frequency value.	ITU-R Rec. TF.686
frequency standard	An accurate stable oscillator generating a fundamental frequency used in calibration and/or reference applications. See Recommendation ITU-T G.810.	ITU-R Rec. TF.686
hash	Value computed on data to detect error or manipulation. See Checksum.	CNSSI-4009
jitter	The short-term phase variations of the significant instants of a timing signal from their ideal position in time (where short-term implies here that these variations are of frequency greater than or equal to 10 Hz). See also “wander”.	ITU-R Rec. TF.686
key data storage (key escrow)	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an	NIST SP 800-32

Term	Definition	Source
	employer, or other party, upon provisions set forth in the agreement.	
network synchronization	A generic concept that depicts the way of distributing a common time and/or frequency to all elements in a network.	ITU-T Rec. G.810
network time protocol (NTP)	The network time protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a terrestrial or satellite broadcast service or modem. NTP provides distributed time accuracies on the order of one millisecond on local area networks (LANs) and tens of milliseconds on wide area networks (WANs). NTP is widely used over the Internet to synchronize network devices to national time references. See www.ntp.org. See also IETF documents (e.g., RFC 5905).	ITU-R Rec. TF.686
non-functional requirement	Non-functional requirements specify criteria useful to evaluate the qualities, goals or operations of a system, rather than specific behaviors or functions of a system.	NIST SP 1500-201
oscillator	An electronic device producing a repetitive electronic signal, usually a sine wave or a square wave.	ITU-R Rec. TF.686
password	A secret that a Claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings	NIST SP 800-63

Term	Definition	Source
phase coherence	Phase coherence exists if two periodic signals of frequency M and N resume the same phase difference after M cycles of the first and N cycles of the second, where M/N is a rational number, obtained through multiplication and/or division from the same fundamental frequency.	ITU-R Rec. TF.686
phase synchronization	The term phase synchronization implies that all associated nodes have access to reference timing signals whose significant events occur at the same instant (within the relevant phase accuracy requirement). In other words, the term phase synchronization refers to the process of aligning clocks with respect to phase (phase alignment). NOTE 1 – Phase synchronization includes compensation for delay between the (common) source and the associated nodes. NOTE 2 – This term might also include the notion of frame timing (that is, the point in time when the timeslot of an outgoing frame is to be generated). NOTE 3 – The concept of phase synchronization (phase alignment) should not be confused with the concept of phase-locking where a fixed phase offset is allowed to be arbitrary and unknown. Phase alignment implies that this phase offset is nominally zero. Two signals which are phase-locked are implicitly frequency synchronized. Phase-alignment and phase-lock both imply that the time error between any pair of associated nodes is bounded	ITU-T Rec. G.8260
PID loops	Proportional, integrative, derivative loop used in automation.	NIST SP 800-82
precision time protocol (PTP)	A time protocol originally designed for use in instrument LANs now finding its way into WAN and packet based Ethernet network applications. PTP performance can exceed NTP by several orders of magnitude depending on the network environment. See IEEE 1588.	ITU-R Rec. TF.686
pre-shared key (symmetric key)	A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.	SP 800-63; CNSSI-4009

Term	Definition	Source
reference timing signal	A timing signal of specified performance that can be used as a timing source for a slave clock.	ITU-T Rec. G.810
repeatability	Closeness of agreement between the results of successive measurements of the same measurand carried out under the same conditions as follows: with respect to a single device when specified parameters are independently adjusted to a stated set of conditions of use, it is the standard deviation of the values produced by this device. It could also be termed "resettability"; with respect to a single device put into operation repeatedly without readjustment, it is the standard deviation of the values produced by this device; with respect to a set of independent devices of the same design, it is the standard deviation of the values produced by these devices used under the same conditions.	ITU-R Rec. TF.686
reproducibility	With respect to a set of independent devices of the same design, it is the ability of these devices to produce the same value. With respect to a single device, put into operation repeatedly, it is the ability to produce the same value without adjustments. NOTE 1 – The standard deviation of the values produced by the device(s) under test is the usual measure of reproducibility.	ITU-R Rec. TF.686
second	The SI unit of time, one of the seven SI base units. The second is equal to the duration of 9 192 631 770 periods of the radiation corresponding to the transition between the two hyperfine levels of the ground state of the cesium-133 atom. Note: The symbol for second, the SI unit of time, is s.	IEEE Std 270-2006 (Revision of IEEE Std 270-1966); IEEE Standard Definitions for Selected Quantities, Units, and Related ... |
signature	See digital signature	NIST SP 800-63

Term	Definition	Source
stability	Property of a measuring instrument or standard, whereby its metrological properties remain constant in time.	ITU-R Rec. TF.686
syntonization	The relative adjustment of two or more frequency sources with the purpose of cancelling their frequency differences but not necessarily their phase difference.	ITU-R Rec. TF.686
system	A system is a composite set of logical components that together satisfy a concrete set of Use Cases.	NIST SP 1500-201
AI : international atomic time	The timescale established and maintained by the BIPM on the basis of data from atomic clocks operating in a number of establishments around the world. Its epoch was set so that TAI was in approximate agreement with UT1 on 1 January 1958. The rate of TAI is explicitly related to the definition of the SI second as measured on the geoid. See “second”, “universal time”, “UT1” and SI Brochure.	ITU-R Rec. TF.686

Term	Definition	Source
temporal determinism	Property of a device or process whereby the latency introduced is known a priori.	NIST SP 1500-202
time interval	The duration between two instants read on the same timescale.	ITU-R Rec. TF.686
time scale (timescale; time-scale)	A system of unambiguous ordering of events. NOTE – This could be a succession of equal time intervals, with accurate references of the limits of these time intervals, which follow each other without any interruption since a well-defined origin. A time scale allows to date any event. For example, calendars are time scales. A frequency signal is not a time scale (every period is not marked and dated). For this reason "UTC frequency" must be used instead of "UTC".	ITU-T Rec. G.810
time stamp (timestamp; time-stamp)	An unambiguous time code value registered to a particular event using a specified clock.	ITU-R Rec. TF.686
time standard	A device used for the realization of the time unit. A continuously operating device used for the realization of a timescale in accordance with the definition of the second and with an appropriately chosen origin.	ITU-R Rec. TF.686
time synchronization:	Time synchronization is the distribution of a time reference to the real-time clocks of a telecommunication network. All the associated nodes have access to information about time (in other words, each period of the reference timing signal is marked and dated) and share a common timescale and related epoch (within the relevant time accuracy requirement. Examples of timescales are: UTC TAI UTC + offset (e.g., local time) GPS PTP local arbitrary time Note that distributing time synchronization is one way of achieving phase synchronization	ITU-T Rec. G.8260

Term	Definition	Source
timescales in synchronization	Two timescales are in synchronization when they, within the uncertainties inherent in each, assign the same date to an event and have the same timescale unit. NOTE 1 – If the timescales are produced in spatially separated locations, the propagation time of transmitted time signals and relativistic effects are to be taken into account.	ITU-R Rec. TF.686
timing signal	A nominally periodic signal, generated by a clock, used to control the timing of operations in digital equipment and networks. Due to unavoidable disturbances, such as oscillator phase fluctuations, actual timing signals are pseudo-periodic ones, i.e., time intervals between successive equal phase instants show slight variations.	ITU-T Rec. G.810
traceability	The property of a result of a measurement whereby it can be related to appropriate standards, generally international or national standards, through an unbroken chain of comparisons. (ISO/IEC 17025:2005). Ability to compare a calibration device to a standard of even higher accuracy. That standard is compared to another, until eventually a comparison is made to a national standards laboratory. This process is referred to as a chain of traceability.	found in IEEE Std 1159-1995; IEEE Recommended Practice for Monitoring Electric Power Quality; also ITU-R Rec. TF.686

Term	Definition	Source
universal time (UT)	Universal time is a measure of time that conforms, within a close approximation, to the mean diurnal motion of the sun as observed on the prime meridian. UT is formally defined by a mathematical formula as a function of Greenwich mean sidereal time. Thus UT is determined from observations of the diurnal motions of the stars. The timescale determined directly from such observations is designated UT0; it is slightly dependent on the place of observation See Recommendation ITU-R TF.460. UT0: UT0 is a direct measure of universal time as observed at a given point on the Earth's surface. In practice, the observer's meridian (position on Earth) varies slightly because of polar motion, and so observers at different locations will measure different values of UT0. Other forms of universal time, UT1 and UT2, apply corrections to UT0 in order to establish more uniform timescales. See "universal time", "UT1" and "UT2" and Recommendation ITU-R TF.460. UT1: UT1 is a form of universal time that accounts for polar motion and is proportional to the rotation of the Earth in space. See "universal time" and Recommendation ITU-R TF.460. UT2: UT2 is a form of universal time that accounts both for polar motion and is further corrected empirically for annual and semi-annual variations in the rotation rate of the Earth to provide a more uniform timescale. The seasonal variations are primarily caused by meteorological effects. See "universal time" and Recommendation ITU-R TF.460. NOTE 1 – The UT2 timescale is no longer determined in practice.	ITU-R Rec. TF.686

Term	Definition	Source
UTC : coordinated universal time	The time scale, maintained by the Bureau International des Poids et Mesures (BIPM) and the International Earth Rotation Service (IERS), which forms the basis of a coordinated dissemination of standard frequencies and time signals. See Recommendation ITU R TF.460. It corresponds exactly in rate with TAI, but differs from it by an integer number of seconds. The UTC scale is adjusted by the insertion or deletion of seconds (positive or negative leap seconds) to ensure approximate agreement with UT1. See “universal time” and Recommendation ITU R TF.460.	ITU-T Rec. G.810 and ITU-R Rec. TF.686
wander	The long-term phase variations of the significant instants of a timing signal from their ideal position in time (where long-term implies here that these variations are of frequency less than 10 Hz). See “jitter”. Note: there is work in ITU-T SG15/Q13 to address wander/jitter associated with time signals such as 1PPS where the 10Hz breakpoint is not meaningful.	ITU-R Rec. TF.686

B.2 Acronyms

Selected acronyms used in this document (or in NIST SP 1500-201 or NIST SP 1500-202) are defined below.

Acronym	Expansion
3D	Three dimensional
6LoWPAN	IPv6 over low-power personal area networks
ACM	Association for Computing Machinery
AES	Advanced Encryption Standard
AIAA	American Institute of Aeronautics and Astronautics
ANSI	American National Standards Institute
API	Application programming interface
APTS	Assisted Partial Timing Support
ARINC	Aeronautical Radio, Incorporated
ASIC	Application-specific integrated circuit
ATIS	Alliance for Telecommunications Industry Solutions
BIPM	Bureau International des Poids et Mesures
C-TPAT	Customs Trade Partnership Against Terrorism
CAD	Computer-aided design
CBP	Customs and Border Protection
CHESS	Center for Hybrid and Embedded Software
CMS	Cryptographic Message Syntax
CNM	CPS Network Manager
COAST	Copper/Optical Access, Synchronization, and Transport Committee
CPS PWG	Cyber-Physical Systems Public Working Group
CRC	Cyclic redundancy check
CRIS	Critical Infrastructures
CRL	Certificate Revocation List
CRM	Customer relationship management
CSI	Container Security Initiative
CSRA	Cybersecurity Research Alliance
DIS	Draft International Standard
DMV	Department of Motor Vehicles
DNS	Domain Name System
DO	Digital Object
DoS	Denial of service
EEC	Synchronous Ethernet equipment slave clock
EMI	Electromagnetic interference

Acronym	Expansion
EPRI	Electric Power Research Institute
ERM	Enterprise resource management
EU	European Union
FDIS	Final Draft International Standard
FIPP	Fair Information Practice Principles
FPGA	Field-programmable gate array
GNSS	Global navigation satellite system
GPS	Global positioning system
GRC	Governance, Risk, and Compliance
GUI	Graphical user interface
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
HSPD-12	Homeland Security Presidential Directive 12
HTTPS	Hypertext Transfer Protocol over TLS
HVAC	Heating, ventilating, and air conditioning
HW	Hardware
I/O	Input/output
ICNRG	Information Centric Networking
ICS	Industrial control systems
IdP	Identity provider
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IF-Map	Interface for Metadata Access Points
IFF	Identification Friend or Foe
IHMC	Florida Institute for Human and Machine Cognition
IIC	Industrial Internet Consortium
IIOT	Industrial Internet of Things
IJSWIS	International Journal on Semantic Web and Information Systems
IoT	Internet of Things
IoT ARM	Internet of Things Architectural Reference Model
IoT-A	Internet of Things – Architecture
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv6	Internet Protocol version 6
IRIG-B	Inter-Range Instrumentation Group timecode B
ISA	Instrumentation, Systems, and Automation Society

Acronym	Expansion
ISO	Independent Service Operator
ISO	International Organization for Standardization
ISPCS	International IEEE Symposium on Precision Clock Synchronization for Measurement, Control, and Communication
IT	Information technology
ITU	International Telecommunication Union
ITU-R	International Telecommuncation Union – Radiocommunication Sector
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
JDL	Joint Director of Laboratories
KPI	Key performance indicator
LLDP	Link Layer Discovery Protocol
LNCS	Lecture Notes in Computer Science
LSB	Least-significant-bit
LTE-A	Long Term Evolution Advanced
M2M	Machine-to-machine
MAC	Media Access Control
MACsec	Media Access Control Security
MD5	Message Digest
MDR	Metadata Registries
MitM	Man in the middle
MOM	Manufacturing operations management
MTBF	Mean time between failures
NFPA	National Fire Protection Association
NFV	Network Function Virtualization
NILM	Non-intrusive load monitoring
NIPP	National Infrastructure Protection Plan
NISO	National Information Standards Organization
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development
NMA	Navigation message authentication
NSTAC	National Security Telecommunications Advisory Committee
NTP	Network Time Protocol
NVOCC	Non-Vessel Operating Common Carrier
OED	Oxford English Dictionary
OEM	Original equipment manufacturer
OMG	Object Management Group
OPC UA	OPC Unified Architecture

Acronym	Expansion
OSE	Open System Environment
OT	Operational technology
OWL	Web Ontology Language
PALS	Physically-Asynchronous Logically-Synchronous
PDH	Plesiochronous digital hierarchy
PDV	Packet delay variation
PEC	Packet-based equipment clock
PID	Persistent identifier
PII	Personally identifiable information
PKI	Public key infrastructure
POSIX	Portable Operating System Interface
PPD	Presidential Policy Directive
PPM	Parts per million
PROFINET	Process Field Net
PRTC	Primary reference timing clock
PSC	Packet-based service clock
PTIDES	Programming Temporally Integrated Distributed Embedded Systems
PTP	Precise Time Protocol
QR	Quick Response
R&D	Research and development
RA	Reference architecture
RDA	Research Data Alliance
RDF	Resource Description Framework
REST	Representational State Transfer
RF	Radio frequency
RFC	Request for Comments
RFID	Radio-frequency identification
RP	Relying party
RTAS	Real-Time and Embedded Technology and Applications Symposium
SCADA	Supervisory Control and Data Acquisition
SDH	Synchronous digital hierarchy
SDN	Software Defined Networking
SEC	SDH equipment slave clock
SHA256	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SOA	Service-oriented architecture
SoS	System-of-systems

Acronym	Expansion
SPARQL	SPARQL Protocol and RDF Query Language
SW	Software
TAI	International Atomic Time (Temps Atomique International)
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TI	Time interval
TLS	Transport Layer Security
TNC	Trusted Network Communications
TOCS	Transactions on Computer Systems
TS	Technical Specification
TSC	Timestamp counter
TSU	Timestamp unit
TTA	Time-Triggered Architecture
UAV	Unmanned Aerial Vehicle
UMA	User Managed Access
UML	Unified Modeling Language
URL	Universal Resource Locator
US	United States
USB	Universal Serial Bus
UTC	Coordinated Universal Time
UUID	Universally Unique Identifier
VCSE	Virtual Control System Environment
W3C	World Wide Web Consortium
WCET	Worst-case execution time
WSS	Web Services Security
XEP	XMPP Extension Protocol
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol