DRAFT Timing Framework for Cyber-Physical Systems

Technical Annex
Release 0.8

September 2015

Cyber Physical Systems Public Working Group

Contents

1. Appendices to Timing Framework Elements

1.1. Appendix to Introduction to timing

1.1.1. Timing Signals

Every network element has a clock subsystem (often just called the "clock"), typically containing an oscillator that is used, with other PLLs if necessary, to generate the various frequency signals (clock waveforms) used to clock the circuits in that system. The behavior of the network element 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 traffic 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 1.1-1 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, we consider the rising edge of the waveform, as indicated in Figure 1.1-1, 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.

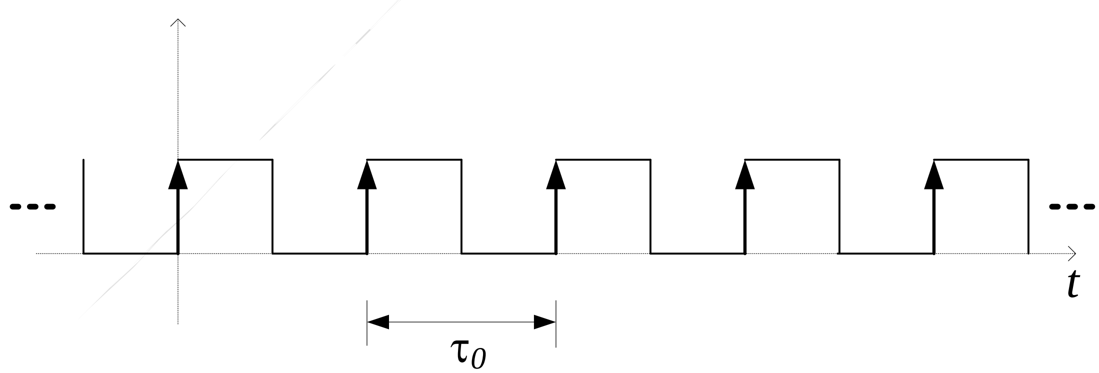


Figure 1.1-1: A generic clock waveform

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 Figure 1.1-1, 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 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:

$$\boldsymbol{f_0 = 1/\tau_0} \quad \text{(Units: Hz for frequency and seconds for time)}$$

Equation 1.1-1

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 0ppm (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 10^3ppm. It is then not uncommon to refer to the “frequency” of the signal as 10^3ppm. 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 10^3ppm.

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 nice mathematical properties, including a compact mathematical form and consequently it is not uncommon to view a clock signal (even a “square wave” as in Figure 1.1-1) 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

$$w(t) = A\cos(\Phi(t))$$

Equation 1.1-2

where A is the amplitude of $x(t)$ 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

$$\Phi(t) = \omega_0 t + \phi = (2\pi f_0)t + \phi$$

Equation 1.1-3

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 Equation 1.1-3. 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 Equation 1.1-1.

For a sinusoidal signal of the form given in Equation 1.1-2, the "instantaneous frequency" (in units such as Hz or mHz or MHz, etc.), $\Psi(t)$, is defined as the derivative of the phase function, appropriately scaled (the factor of 2π addresses the conversion between rad/s and Hz):

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

Equation 1.1-4

Clearly, if $\Phi(t)$ is a linear function of t as in Equation 1.1-3, then the instantaneous frequency is a constant (not time-varying) and equal to f_0. If $\Phi(t)$ is *approximately* a linear function of t, then we can write

$$\Phi(t) = \alpha_0 + \omega_0 t + \phi(t)$$

Equation 1.1-5

In Equation 1.1-5, 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 as

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

Equation 1.1-6

The deviation from pure sinusoidal behavior, quantified by the term $\phi(t)$, introduces an instantaneous frequency offset (possibly time varying), say δf. From Equation 1.1-6, we see that

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

Equation 1.1-7

The fractional frequency offset (from nominal), Δf, is defined as

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

Equation 1.1-8

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, $3\text{x}10^{-6}$ 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 Equation 1.1-1 is appropriate for a truly periodic waveform. For quasi-periodic signals, no one value of frequency can be provided since there is a time-varying nature implicit in the statement that the time interval between rising edges is not a constant. Consequently we introduce 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, we can write

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

Equation 1.1-9

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 Figure 1.1-1, $p(t)$ 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 $\{x(n)\}$ defined by

$$x(n) = T_n - n\tau_0 \, .$$

Equation 1.1-10

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 we do not have an ideal clock as reference. Rather, we have two clock signals and we are trying to analyze the behavior of one 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 that all Fourier frequencies of interest are less than $0.5 \cdot f_0$, the two representations are theoretically the same.

We 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 Equation 1.1-10 and is defined by:

$$\xi(i;n) = x(i+n) - x(i)$$

Equation 1.1-11

The rationale for the definition in Equation 1.1-11 is the following. If we are 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, we arbitrarily assume 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 as:

$$x(n) = \xi(0;n)$$

Equation 1.1-12

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 Sampling Theorem (Nyquist) we know 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 Figure 1.1-2, below.

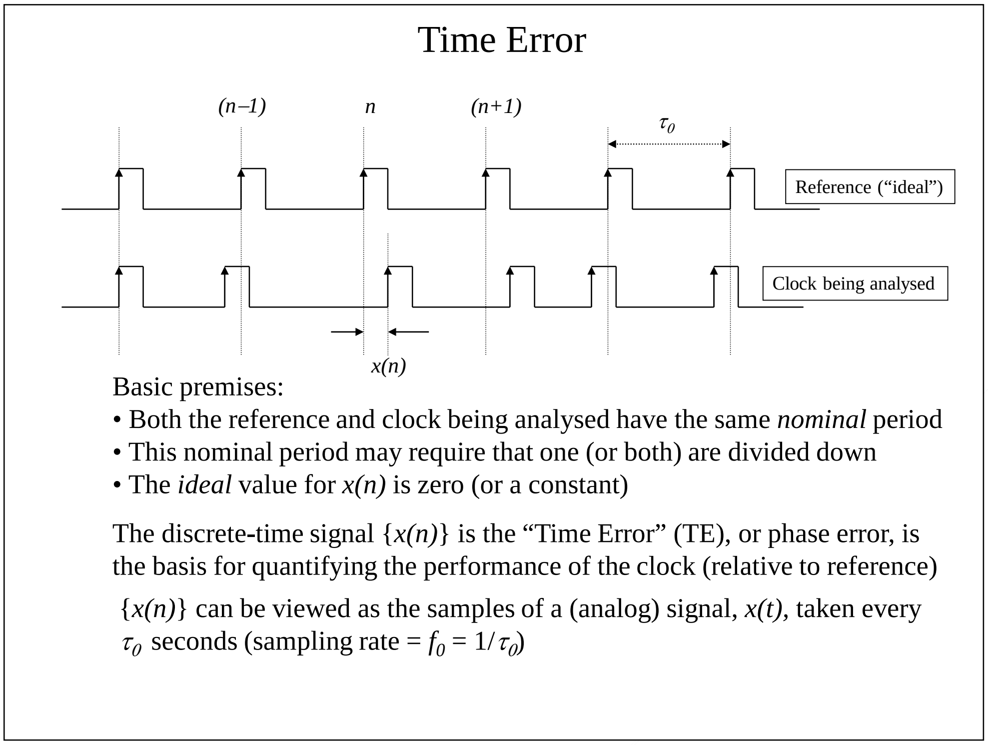


Figure 1.1-2: Concept of *Time Error*

The accuracy and stability of the network element time-base is degraded by a number of factors. This is especially noticeable 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. Clock performance determines slip performance. Better clocks mean 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.

1.1.2. 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 because that it is common in oscillators, particularly Rubidium frequency standards and Quartz crystals, for the frequency to vary linearly with time, at least approximately. All other deviations are modeled as a random component, lumped together as $\varepsilon(t)$. That is, the model can be expressed in terms of a time error (or phase error) signal, $x(t)$, as:

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

Equation 1.1-13

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 as:

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

Equation 1.1-14

In Equation 1.1-14 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 is possible to postulate components with spectra that roll-off at higher (negative) powers of f.

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 Equation 1.1-13. 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 time-master and time-slave of a two-way time transfer system, as discussed in section 1.1.5, has an unknown component of asymmetry, then the endpoints are unable to accurately establish the constant time error resulting from this asymmetry.

1.1.3. 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, we 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 UTC or 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 Earth 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 [2.5.1.2]. The following table identifies some of the time-scales in use and the choice of time origin (epoch).

Table 1.1-1: 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 = 35s*	Yes	Discontinuous
UT-1	Jan. 1, 1958	Earth's rotation	No	Astronomical
GPS	Jan. 6, 1980	TAI – GPS = 19s	No	Continuous
LORAN-C	Jan. 1, 1958	UTC + 23s	No	Discontinuous
Local	Jan. 1, 1972	TAI – UTC = 35s*	Yes	Discontinuous; based on time-zone offset
PTP	Jan. 1, 1970	TAI – PTP = 10s	No	Continuous
NTP	Jan. 1, 1970	UTC	Yes	Discontinuous

*: As of June 30, 2012.

The clock error model of Equation 1.1-13 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 that:

- Since a clock is a frequency device, the best clocks will exhibits 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.

1.1.4. 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 Equation 1.1-13, 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 (Equation 1.1-13), the term x_0 can be viewed as the constant time error. As recommended in ITU-T Rec. G.8260, 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 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:

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 following ITU-T Rec. G.823 Appendix II 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. 1.13). A frequency error sequence can be constructed in the following manner.

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

Equation 1.1-15

In Equation 1.1-15 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 τ (= $n \cdot \tau_0$). The 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 $\upsilon(i;n)$ given by

$$\upsilon(i;n) = y((i+n),n) - y(i;n)$$

Equation 1.1-16

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 $\tau = n \bullet \tau 0$ taken over adjacent, contiguous, periods of time. The time error value $x(i+n)$ is common to the two measurements. Equation 1.1-16 can be rewritten as

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

Equation 1.1-17

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:

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

Equation 1.1-18

The leading (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 as:

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

Equation 1.1-19

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 TVAR, related to MVAR as:

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

Equation 1.1-20

The factor of 3 in the expression is a scaling factor for normalization.

It is common practice to use the "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 I 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 $\sigma_y^2(\tau) \propto \tau^{\mu}$ [2.5.1.3]. The τ-domain variances can be recognized as TVAR and MVAR (corresponding to standard deviations TDEV and MDEV).

Table 1.1-2: 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 Equation 1.1-21, below.

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

Equation 1.1-21

It can be easily seen that the inner parentheses 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, albeit not as intuitive as Equation 1.1-21, is

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

Equation 1.1-22

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.

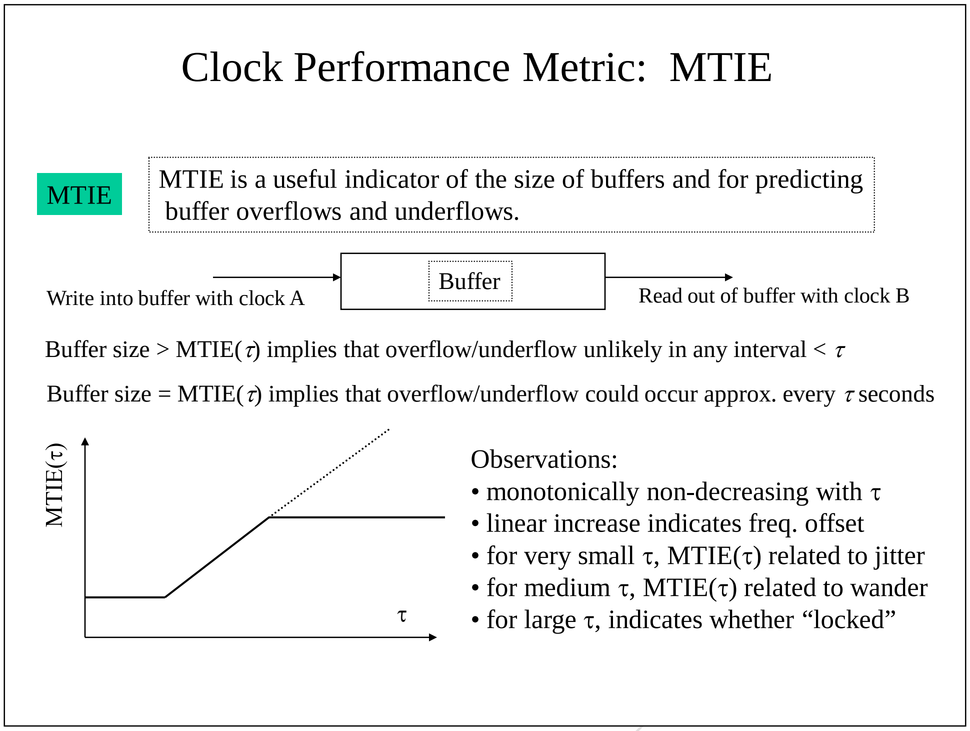


Figure 1.1-3: Underlying premise of MTIE

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.

1.1.5. Packet-based and Two-Way Time Transfer

Consider the situation where 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 Figure 1.1-4. The particular protocol (such as NTP or PTP) employed determines the method whereby the measurements ("time stamps") are communicated between the two entities.

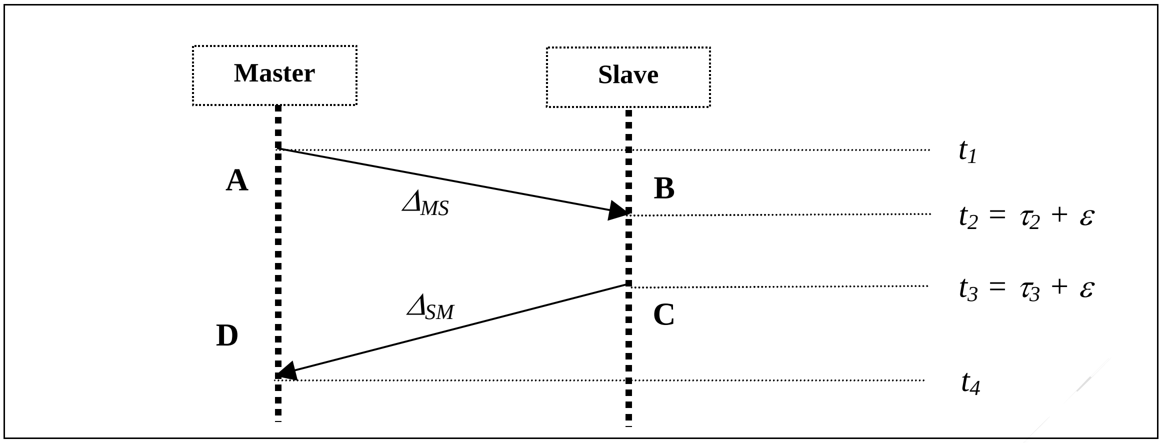


Figure 1.1-4 Time-stamps in packet exchange between Master and Slave

Referring to Figure 1.1-4, the sequence of events and important items of information associated with an exchange of packets between Master and Slave are:

- Event A: Packet is transmitted by Master and time-of-departure 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, $(t_1, \tau_2, \tau_3, t_4)$. 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 between the Master and Slave and vice versa, the following equations can be established:

$$\begin{aligned} t_4 &= \tau_3 + \varepsilon + \Delta_{SM} \quad \text{(from an S-to-M packet)} \\ t_1 &= \tau_2 + \varepsilon - \Delta_{MS} \quad \text{(from a M-to-S packet)} \end{aligned}$$

Equation 1.1-23

There are just two equations involving three unknowns. However, if we assume delay reciprocity (i.e., equal delay in the two directions) then

$$\varepsilon = \left(\frac{1}{2}\right)\left(t_4 - \tau_3 - \tau_2 + t_1\right)$$

$$\Delta_{MS} = \Delta_{SM} = \left(\frac{1}{2}\right)\left(t_4 - \tau_3 + \tau_2 - t_1\right)$$

Equation 1.1-24

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

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

Equation 1.1-25

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.

1.2. Appendix to Time and Latency

1.2.1. Standards making networks Time-Aware

1. IEEE 1588: Providing a layered architecture for time propagation which allows clock synchronization across heterogeneous networks (including wireless). 1588 specifies the media independent options and the mapping to media dependent options which are specified in network-specific standards.
2. IEEE 802.1AS: Specifying an Ethernet specific profile for 1588 that provides guarantees on synchronization accuracy.
3. IEEE 802.1Q: Providing 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 CPSs. 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-end latency.
4. IEEE 802.1CB: Providing seamless redundancy options to increase reliability of data-transfer in Ethernet networks.
5. IEEE 802.11v-2011: Specifying timing measurement capability for Wi-Fi networks and a mapping function to 1588.
6. IEEE 802.11ak: Specifying bridges 802.11 networks which will enable time-sensitive stream support over Wi-Fi networks (using time-based synchronization) in the future.
7. IEEE 802.3bf: Ethernet support for IEEE 802.1AS time synchronization protocol.
8. ITU-T Rec. G.8261 (also Y.1361) [2.5.5.2], Timing and synchronization aspects in packet networks.
9. ITU-T Rec. G.8262 [2.5.5.2], Timing characteristics of Synchronous Ethernet Equipment slave clock (EEC).
10. ITU-T Rec. G.8265 (also Y.1365) [2.5.5.2], Architecture and requirements for packet-based frequency delivery.
11. ITU-T Rec. G.8275 (also Y.1369) [2.5.5.2], Architecture and requirements for packet-based time and phase delivery.

Additionally there are consortiums created around these standards like WFA and AVnu which are helping test implementation and interoperability. Recently a new working group has been formed in Internet Engineering Task Force (IETF) called Deterministic Networking to bring time and time-sensitive data transfer into wide area networks (WANs).

1.2.2. Schedule Generation and Distribution

Performance Metrics

The CNM or the centralized network controller has to gather performance metrics and calculate topology of CPS nodes in a CPS domain in order to create a schedule.

The performance metrics are:

1. Bridge Delays
2. Propagation Delays

3. Forwarding/transmission delays

IEEE 1588 uses peer-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 looking into implementing/referencing these (via the IEEE 802.1Qbv specification).

One way 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 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.
4. 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

Figure 1.2-1 below describes a possible schedule distribution flow in a CPS. The Centralized Network Manager computes the topology for the CPS domain using the mechanism mentioned earlier. The CNM 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.

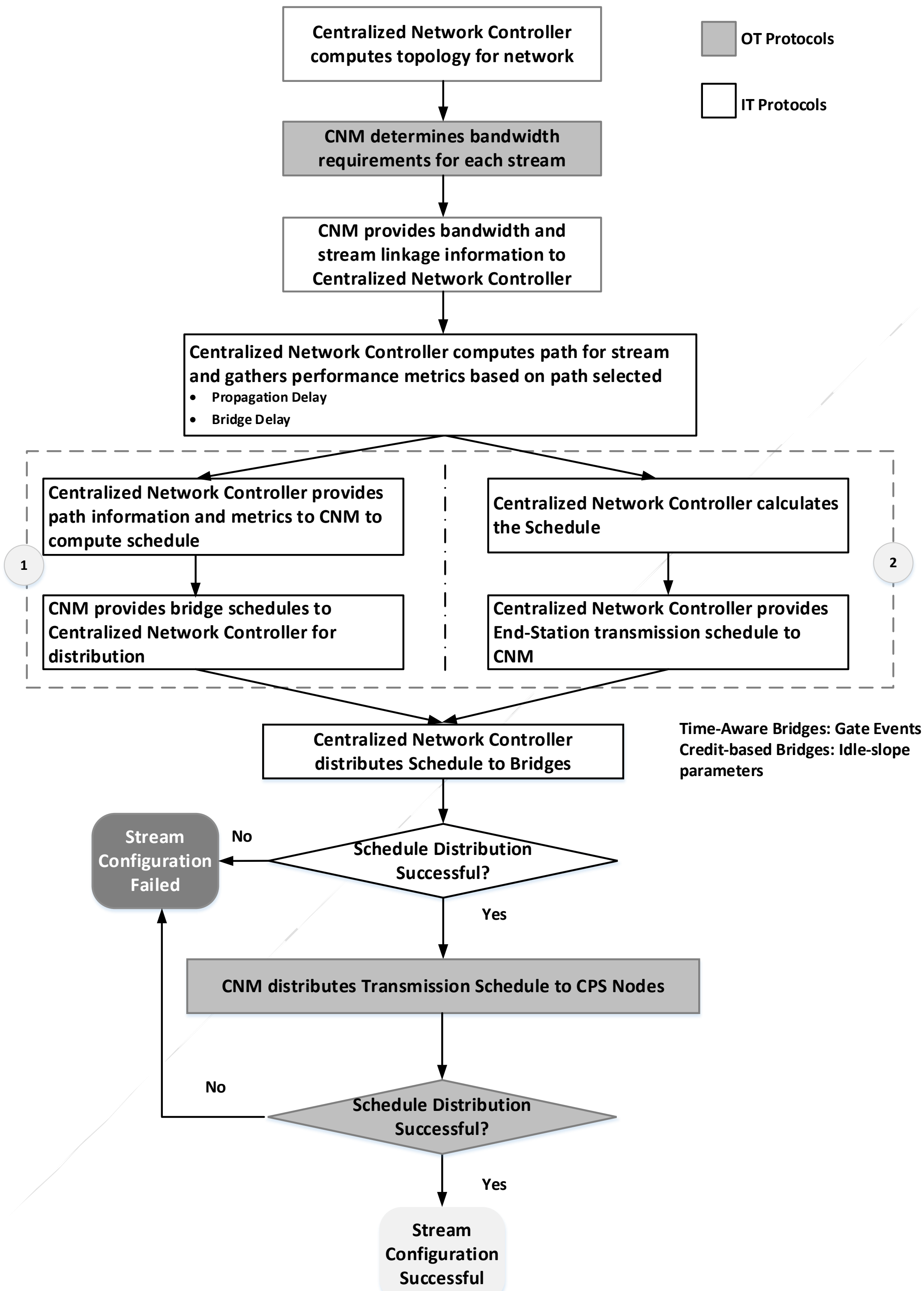


Figure 1.2-1: CPS Schedule Generation and Distribution

(Source: Sundeep Chandhoke, National Instruments)

1.2.3. Use of time in Operating systems

CPS can employ operating systems with a wide range of complexities, from a simple application-level infinite loop (e.g. the Arduino platform) to a virtual machine 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 Figure 1.2-2.

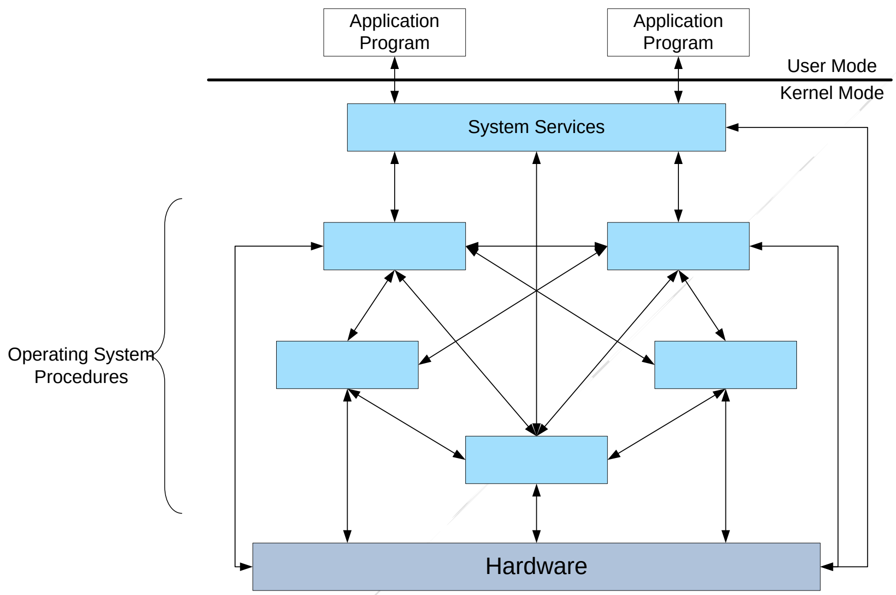


Figure 1.2-2: Monolithic Operating System

(Source: A. Frank - P. Weisberg, Operating Systems – Structure of Operating Systems)

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. The layered model is shown below in Figure 1.2-3.

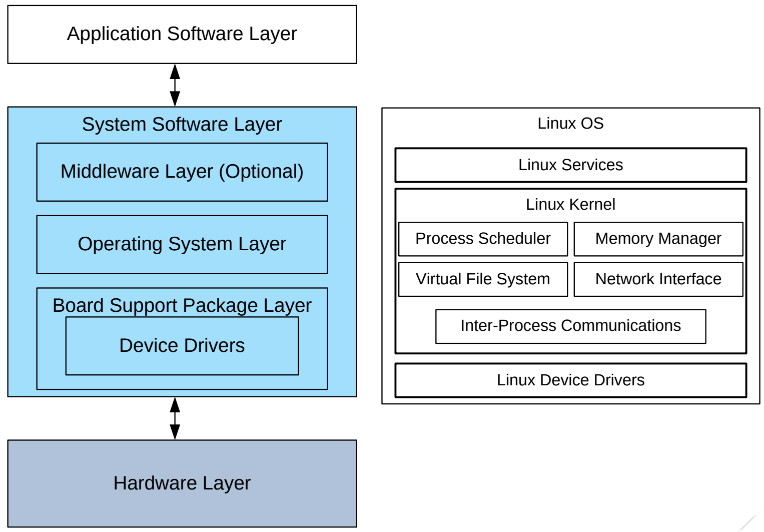


Figure 1.2-3: Figure A3.3: Layered Multithreaded OS (Linux Shown as an example)

(Source: A. Frank - P. Weisberg, Operating Systems – Structure of Operating Systems)

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 Figure 1.2-4, as a request for accurate time is shown traversing through the layers.

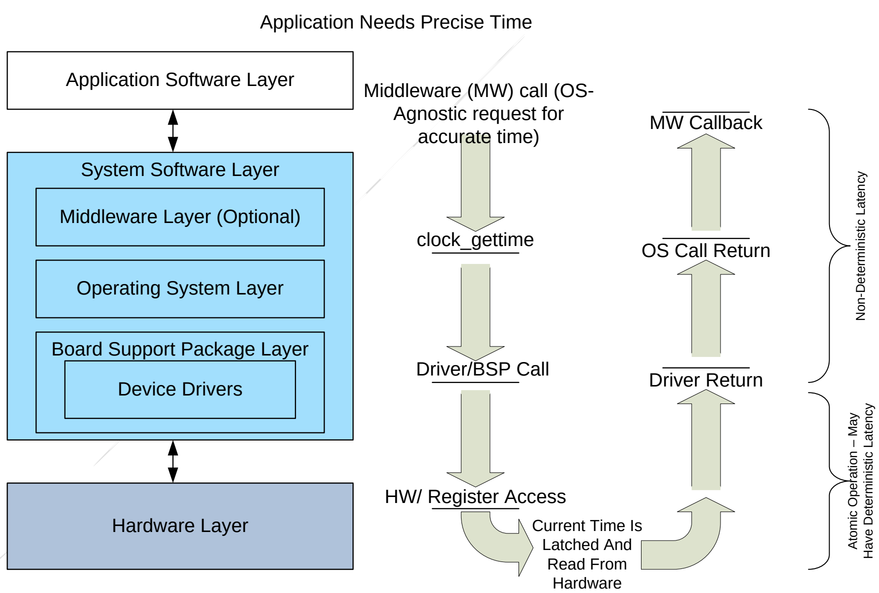


Figure 1.2-4: Application Request for Time

(Source: A. Frank - P. Weisberg, Operating Systems – Structure of Operating Systems)

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, 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.

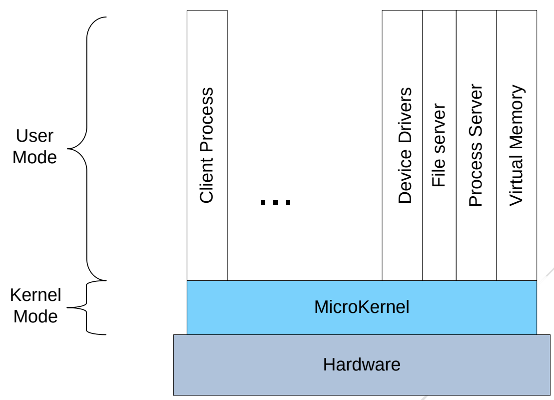


Figure 1.2-5: Microkernel OS

(Source: A. Frank - P. Weisberg, Operating Systems – Structure of Operating Systems)

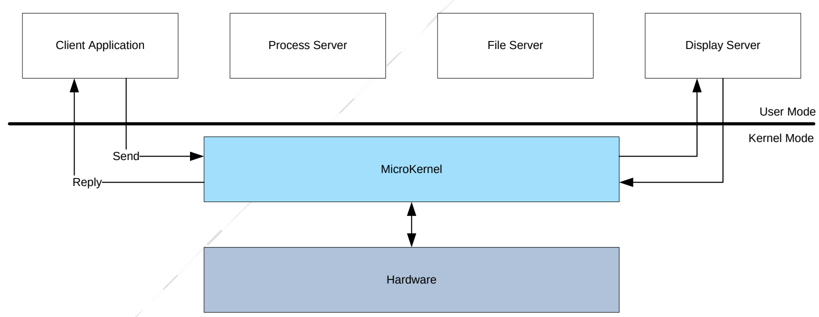


Figure 1.2-6: Microkernel message passing model

(Source: A. Frank - P. Weisberg, Operating Systems – Structure of Operating Systems)

In the microkernel case, the time and latency determinism is driven by the message passing process.

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, where 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.

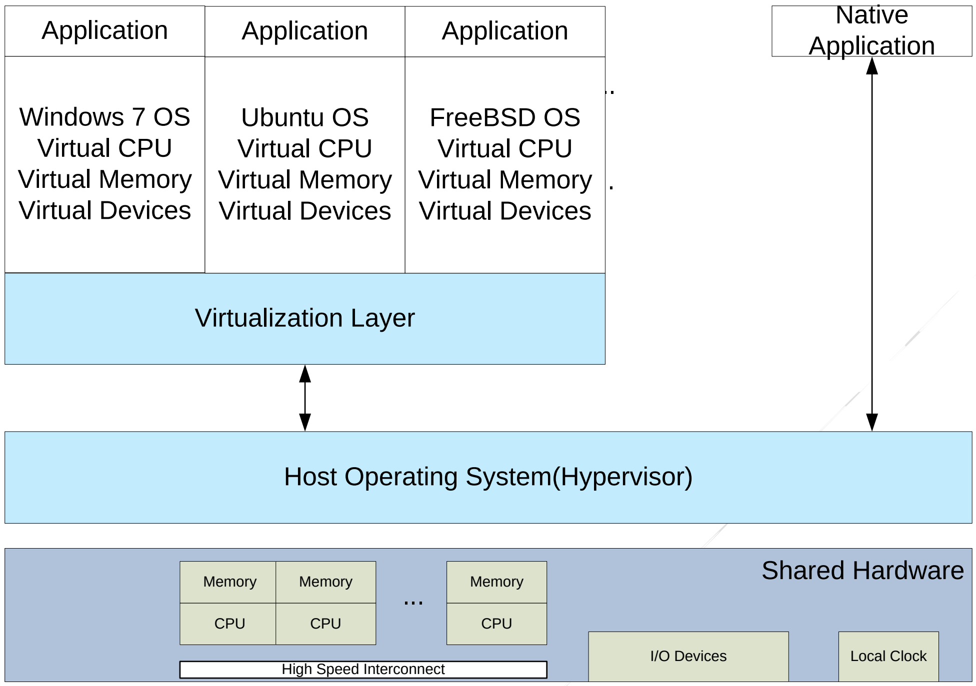


Figure 1.2-7: Virtual Machine Architecture

(Source: A. Frank - P. Weisberg, Operating Systems – Structure of Operating Systems)

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 to 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.

1.3. Appendix to Security and Resilience

1.3.1. 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. GPS time is in fact not adequate and is combined within a crystal oscillator for a more stable time. Timing inadequacies may cause synchronization failures for 4G LTE. The accuracy of time will be a pacing item for 5 and 6G service.

1.3.2. Compromising and Securing Time

Compromising GPS and other wireless frequencies

A. Jamming and Spoofing

Given the vital dependency of timing on 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 20,000 km. The relatively weak 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 [2.5.4.13][2.5.4.14]. Other forms of wireless communications such as 4G LTE, WiFi, and 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 [2.5.4.15]. However, researchers have also shown that anti-spoofing algorithms can detect attacks by observing GPS receiver characteristics [2.5.4.17]. 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 [2.5.4.18].

To meet the elements of secure time, detection and location of jammers and spoofers via research and technology advancements such as GPS Jammer Detection and Location (JLOC) using ad-hoc networks such as vehicles [2.5.4.16] and mobile phones, can enable the CPS to predictably failover to other time sources 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 1.3-1 Impact of GPS Anomalies by CIKR Sector describes the minimum acceptable oscillator, holdover time and impact of GPS anomalies on each of the 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.

CPS relying on GPS time can also establish elements for integrity monitoring of the time reference source [2.5.4.19]. Integrity is a measure of the trust placed in the correctness of the information with respect to GPS time [2.5.4.20]. 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
- *alarm limit*: the timing accuracy exceeds a tolerance level required by the system's most stringent application

Table 1.3-1 Impact of GPS Anomalies by CIKR Sector [2.5.4.21]

GPS Timing Essential CIKR Sector	Least Robust Oscillator	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)
Communications Sector	OCXO High-Stability (HS)	24 *	N	Y	N
Emergency Services Sector	OCXO (HS)	24 *	N	Y	N
Information Technology Sector	OCXO Medium Stability (MS)	1 #	Y	Y	Y
Banking and Finance Sector	TCXO	< .24 -1.7 #	Y	Y	Y
Energy/Electric Power Subsector	OCXO (MS)	1 #	Y	Y	Y
Energy/Oil and Natural Gas Sector Subsector	OCXO (MS)	1 #	Y	Y	Y
Nuclear Sector	OCXO (MS)	1 #	Y	Y	Y
Dams Sector	OCXO (MS)	1 #	Y	Y	Y
Chemical Sector	OCXO (MS)	1 #	Y	Y	Y
Critical Manufacturing Sector	TCXO	1.7 #	Y	Y	Y
Defense Industrial Base Sector	TCXO	1.7 #	Y	Y	Y
Transportation Sector	OCXO (HS)	24 *	N	Y	N

B. 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 2.4-2 describes the effect of solar storms on GPS time.

A geomagnetic storm induces ground currents and Earth surface potentials Geomagnetically Induced Currents (GIC) at substations (damages equipment) and on power lines causes faults and trips [2.5.4.22]. Loss of GPS timing synchronization of data for 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 HF blackouts, satellite communications losses and 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 in providing high-confidence forecasts of ionospheric and other space weather characteristics [2.5.4.22] would improve the systems' ability to achieve predictable failure to alternative timing sources.

Table 2.4-2 Space/Weather Impact on GPS [2.5.4.21]

Solar Storm Effect	Single Frequency GPS Timing Error (Range)	Single Frequency GPS Position Error (Range)	Time of Day	Duration of Event
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)

1.3.3. 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 time 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 Glonass and EU Galileo Programs).

In the following sections, we cover some domestic alternatives across a variety of broadcast architectures including dedicated wide area networks, WWVB, and eLORAN.

Communications Sector Timing Distribution [2.5.4.24]

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 timing for about 1.1 days. 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 Gigabit Ethernet 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 SONET/SDH or Gigabit Ethernet, which is then multiplexed into the network. In experimental tests, time transfer accuracy of a few nanoseconds over commercial asynchronous fiber optical network is achievable between two sites over 500 kilometers apart [2.5.4.25].

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.

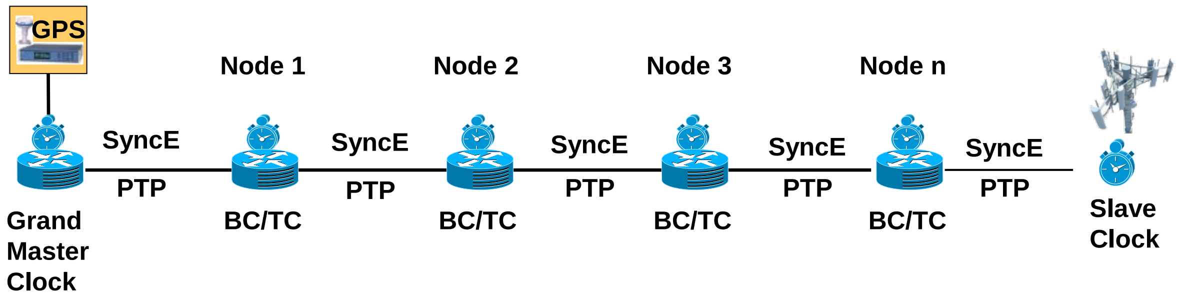


Figure 1.3-1 SyncE with PTP

As shown in

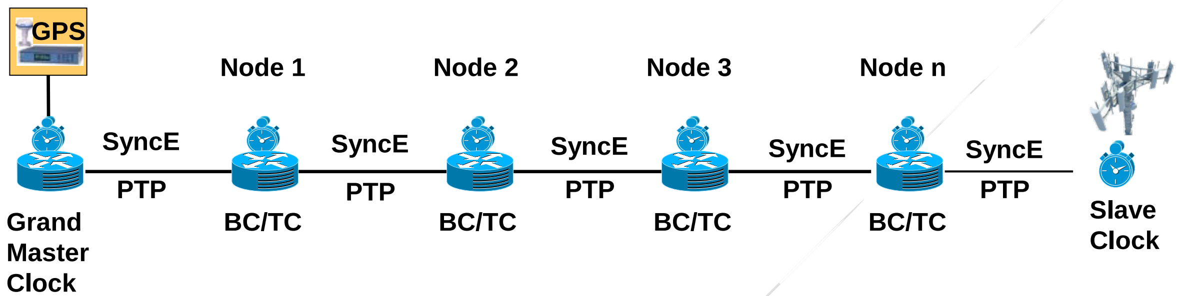


Figure 1.3-1, the Grand Master (GM) clock connects directly to GPS or if GPS is not available another timing reference source, which provides the primary reference clock for entire chain. Multiple timing chains could be supported from a single GM. Boundary Clocks (BC) and Transparent Clocks (TC) are chosen and placed depending on the particulars of the network topology. All network equipment in the timing chain must support both SyncE and PTP.

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 µs timing accuracy have not yet been determined nor validated.

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/ WWVH Timing Radio Broadcasts [2.5.4.4]

Regarding methods of GPS backup for time and frequency synchronization, this section presents the status 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 periods up to about 24 hours. The use of High Frequency (HF) signals from WWV for timing is also mentioned.

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

WWVB has been shown to be capable of providing frequency accuracies of about 1 part in 1011 over days. Most of the studies of the use of this signal are from the 1960's and 70's. Achieving 10^{-11} accuracy required careful selection of tracking times and a very stable reference. A typical data set taken in Maryland of the WWVB signal transmitted from Colorado is shown in Figure 1.3-2. The vertical range of the plot is 50 microseconds, hence the scale of each line is 5 microseconds. One can see a diurnal variation of about 20 microseconds. In addition, using older technology, there were occasional cycle slips.

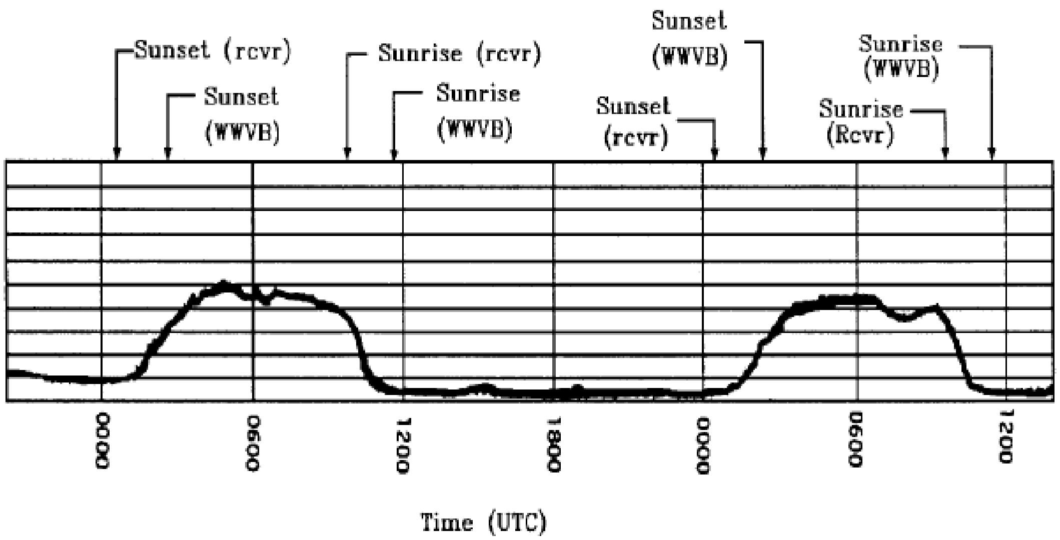


Figure 1.3-2 Phase of WWVB as received in the eastern United States (chart is 50 microseconds wide)

For use as a GPS backup in Assisted Partial Timing Support (APTS) there are several new conditions that offer opportunities. 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. There are current efforts to obtain data that could be used to show predictability of WWVB over 24 hours and longer, given a characterization. Note that WWVB is available everywhere in the continental US (CONUS) for time on wall clocks and wristwatches. Hence the signal strength is strong enough for availability across the CONUS.

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 VLF signals to obtain accuracies in the microsecond region. In addition, there are current plans to introduce phase modulation to the WWV signal, which would improve short term noise, and lower 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.

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
- 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 ~20 m, 2-dimensional root-mean-square (2D RMS) position, and ~100 ns time accuracy [2.5.4.6] 95% of the time. This is a 5-10 times improvement over the performance guaranteed by its predecessor LORAN-C [2.5.4.3].

Technical Description

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 ~ 3km) 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 are ducted 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 calculating the relative time of arrival 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,

- 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 skywaves and signal re-radiation off of large metal structures.

Deliberate Threats and Mitigations

The deliberate threats are jamming and spoofing. However:

- On-air Loran signal is nearly unjammable
- On-air Loran signal is easier but still difficult to spoof

A. Loran Signal Is Nearly Unjammable [2.5.4.24]

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.

B. Loran Signal Spoofing Is Easier But Still Difficult [2.5.4.24]

To spoof a Loran signal with a continuous wave (CW) tone would necessitate creating say 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 R&D on eLORAN could result in more cost-effective, certifiable, and secure eLoran anti-spoofing receiver designs (e.g., by adding authentication through digital signatures).

1.3.4. Network Time Compromise

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 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 eavesdrop 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 analysed.
  Message interception can be done by a MitM or injector.

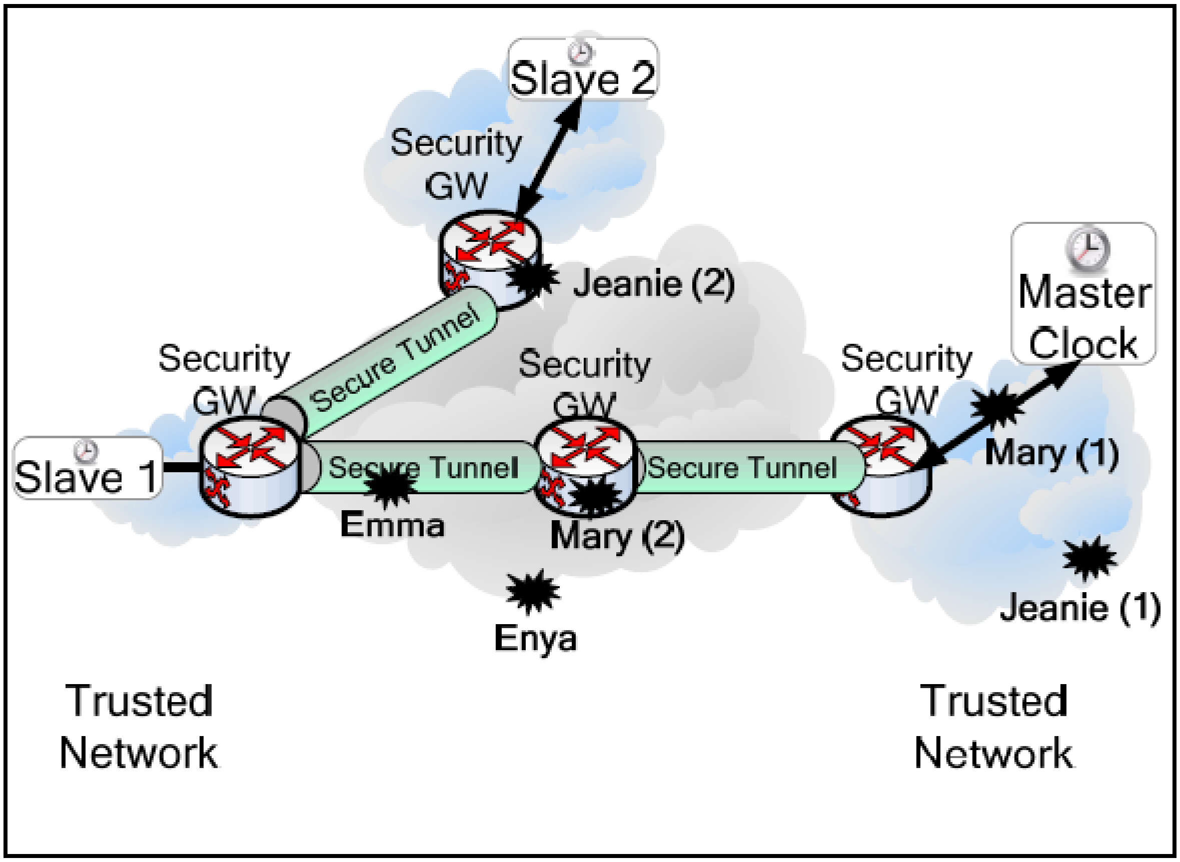
- Message Interruption (active attack)
  A MitM can selectively interrupt, e.g. intercept and remove, certain packets, or can bluntly block all communication in a network (segment).
  Basis for a Denial of Service (DoS) attack.

- Message Insertion (active attack)
  An injector or MitM injects newly crafted packets or previously recorded unicast or multicast packets into a network.
  Also 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.

1.3.5. Threat Analysis for SOTA Time Networks

Reference [2.5.4.9] conducted an in-depth analysis of SOTA secured PTP networks (based on IPsec, MACsec and Annex K). The analysis distinguishes between internal and external MitM and injector attackers that are located in a network as shown in Figure 1.3-3. The figure shows three trusted (secured) networks, which are interconnected via secure tunnels (e.g. secure point-to-point network connections) that bridge unsecured network spaces. These gaps are further described in Table 1.3-3 and Table 1.3-4. The Security Subcommittee of the IEEE 1588 Working Group is currently working to address the security gaps for PTP networks. The IETF NTP WG is also currently working on a replacement for AutoKey.



	Internal Attacker	**External Attacker**
Man-in-the-Middle (MitM)	Mary (1) and (2)	Emma
Injector	Jeanie (1)	Enya

Figure 1.3-3: Attacker Types and Attack Strategies (from [2.5.4.9])

Table 1.3-3: 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. NIDS)
Packet Delay Manipulation	Modification (in widest sense) (MitM)	Reduced accuracy	MITM relays packets with delay	• Distributed overlaid passive supervisory structures (i.e. NIDS) • Trusted platform attestation
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 802.15.4 network with packets • Rogue node overwhelms target with time protocol packets	• Distributed overlaid passive supervisory structures (i.e. NIDS) • Host IDS (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	• Rogue node jams network • Rogue node jams all	• Distributed overlaid passive supervisory structures (i.e. host IDS or NIDS)

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

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

		• Limited or no availability of target	time-related network packets[6]	• 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 a digital certificate)[3]	• Distributed overlaid passive supervisory structures (i.e. NIDS) • Host IDS (HIDS) that monitors level of activity • Trusted platform attestation
Master Time Source Attack	Interruption (MitM or injector)	Reduced accuracy	GPS jamming	• Overlaid passive supervisory structures (i.e. NIDS)

1105

1106 **Table 1.3-4: Internal attacks on a 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 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,	• Distributed overlaid passive supervisory

[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.

			potentially after adjustment of anti-replay measures (e.g. packet counter)	structures (i.e. NIDS) • Trusted platform attestation
Spoofing	Insertion (MitM or injector)	False time	Impersonation of legitimate master or clock	• Trusted platform attestation • Authentication & 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 & authorization of network peers
Interception and Removal	Interruption (MitM)	Reduced accuracy	Time control packets are identified /decoded and selectively omitted	• Distributed overlaid passive supervisory structures (i.e. NIDS) • Trusted platform attestation
Packet Delay Manipulation	Modification (in widest sense) (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	Insertion	• Impairment of entire	• Rogue node floods	• Distributed overlaid

Time Protocol DoS	(MitM or injector)	(low-bandwidth) network • Limited or no availability of target	802.15.4 network with packets • Rogue node overwhelms target with time protocol packets	passive supervisory structures (i.e. NIDS) • Host IDS (HIDS) that monitors level of activity • Trusted platform attestation • 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 IDS (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 computational expensive cryptographic algorithms (i.e. validation of digital certificate)	• Distributed overlaid passive supervisory structures (i.e. NIDS) • Host IDS (HIDS) that monitors level of activity • Trusted platform attestation
Master Time Source Attack	• Interruption (MitM or injector)	• Reduced accuracy • False time	• GPS jamming • GPS spoofing	• Distributed overlaid passive supervisory

	• Insertion (MitM or injector)			structures (i.e. NIDS) • Host-based IDS that monitors level of activity • Trusted platform attestation

1.3.6. Securing Time Networks

SOTA Security Extensions and Protocols

There are various approaches to protect communication in time networks:

1. NTP's Autokey extension protects against packet modification and replay attacks, while providing end point (e.g. server) authentication via digital certificates. The IETF NTP Working Group is currently developing a revised network time security protocol [2.5.4.10][2.5.4.11].

2. IEEE 1588 Annex K 1.5.4 provides group source authentication, message integrity, and replay protection (the latter via a replay counter that reliably identifies stale messages) [2.5.4.26]. A trust relation is established by a challenge-response three-way handshake mechanism [2.5.4.27], which is based on a set of pre- shared keys [2.5.4.28]. The keys are shared by the whole domain or by subsets of the domain 1.5.4. Annex K is an experimental extension and various improvements have been suggested. These include an improved handshake and replay counter [2.5.4.29]. The IEEE 1588 Working Group Security Subcommittee is currently developing optional specifications for improving PTP security [2.5.4.12].

3. IPsec is a suite of L3 security protocols for IP networks that, depending on the configuration, authenticates and / or encrypts IP packet payloads (and also authenticates non-modifiable sections of the IP header). IPsec supports a 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 extend 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.

Table 1.3-5 shows that MACsec as a L2 hop-by-hop protocol performs slightly better than the IPSec and 1588 Annex K, but still leaves significant gaps.

Table 1.3-5: Vulnerabilities of MACSec, IPSec, and Annex K [2.5.4.9]

Attack	*Attacker Type*											
	Internal MITM			*Internal Injector*			*External MITM*			*External Injector*		
	MACsec	*IPsec*	*1588 Annex K*	*MACsec*	*IPsec*	*1588 Annex K*	*MACsec*	*IPsec*	*1588 Annex K*	*MACsec*	*IPsec*	*1588 Annex K*
Interception and modification	•	•	•									
Spoofing	•	•	•		•							
Replay	•	•	•	•	•	•						
Rogue master	•	•	•	•	•	•						
Interception and removal	•	•	•				•	•	•			
Delay manipulation	•	•	•				•	•	•			
L2/L3 DoS	•	•	•	•	•	•		•	•		•	•
Cryptographic performance	•	•	•	•	•	•	•	•	•	•	•	•
Time source spoofing	•	•	•	•	•	•	•	•	•	•	•	•

Message Authentication via ICV

Encryption is in contrast to packet authentication (via an integration check value (ICV) based on symmetric message authentication code functions) generally seen as a minor requirement [2.5.4.9]. Best standard practices and recommendations in network security include:

- 128 – 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 [2.5.4.30].
- 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 2 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 [2.5.4.29].
- Key rotation and key freshness as well as perfect forward secrecy[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 [2.5.4.31].
- Message authentication / encryption requires deterministic latencies to avoid accuracy degradation [2.5.4.8][2.5.4.32].

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

PTP packets are subject to modification by transparent clocks (e.g. an update of the *correctionField*). This is supported as follow:

- 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 on the achievable accuracy.
- Annex K can provide – dependent on setup and key distribution - hop-by-hop or end-to-end integrity protection.

Reference [2.5.4.27] distinguishes between security-unaware, security-aware and security capable transparent clocks and outlines how the latter can be used in hybrid time networks.

1.3.7. Potential Countermeasures in Detail

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 [2.5.4.29] argue that key management as a whole needs to be addressed (in PTP).

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

Therefore the use of digital certificates and public key infrastructures (PKI) should be considered, which supports both peer authentication and authorization. Such a PKI 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 [2.5.4.30] 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 OCSP or certificate stapling (see RFC 6066 [2.5.4.33] 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 IKE or IKE2 (Internet Key Exchange) 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 TLS. TLS provides application-layer process-to-process authentication rather than device to-device-authentication.

Trusted Platform Attestation

SOTA 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 HW and SW 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. [2.5.4.34] suggest 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. describe in [2.5.4.34] a clock drift correction algorithm, which uses time series prediction to re-synchronize slaves during DoS attacks.

1.3.8. Secure Time Use Cases

GPS: Tripping generators off of the grid

Tripping generators off of the 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 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 of tripping generators when needed can lead to blackouts or significant power system damage.

<u>Impacts of Denial and Spoofing</u>

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

A. 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.

B. Impacts of Spoofing

[5] On the other hand PTP slave devices are aware of DoS attacks [2.6.4.18], so a NIDS does not add value other than logging and monitoring attacks.

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 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 [2.5.4.35] and [2.5.4.36].

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 [2.5.4.36].

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.

Prevention of Impacts by Adoption of Elements of Secure Timing

Three elements of secure timing would mitigate the impacts of GPS jamming and spoofing:

(1) Detection of jamming and spoofing by the potentially impacted end-use device/equipment
(2) Alarming the human operator associated with the device
(3) 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 R&D community **Error! Reference source not found.**[2.5.4.38][2.5.4.39]. 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. An electric substation is made of primary equipment (switchgears, breakers, transformers) and secondary equipment (sensors, merging units, intelligent electronic devices).

One pre-requisite to perform efficient protection functions is to have synchronized data provided by the various devices forming the secondary equipment. Depending on the considered function, the synchronization is either local (self-consistent), i.e. the devices of one substation have to be synchronized or global, i.e. the devices from two different substations have to be synchronized. From a synchronization performance point of view, different classes of synchronization are identified and range from 1 µs (class T5) to 1 ms (class T1) through 4, 25 and 100 µs.

An IEEE1588-based synchronization architecture consists of a GPS receiver per substation which distributes the time to the different devices (see Figure 1.3-4).

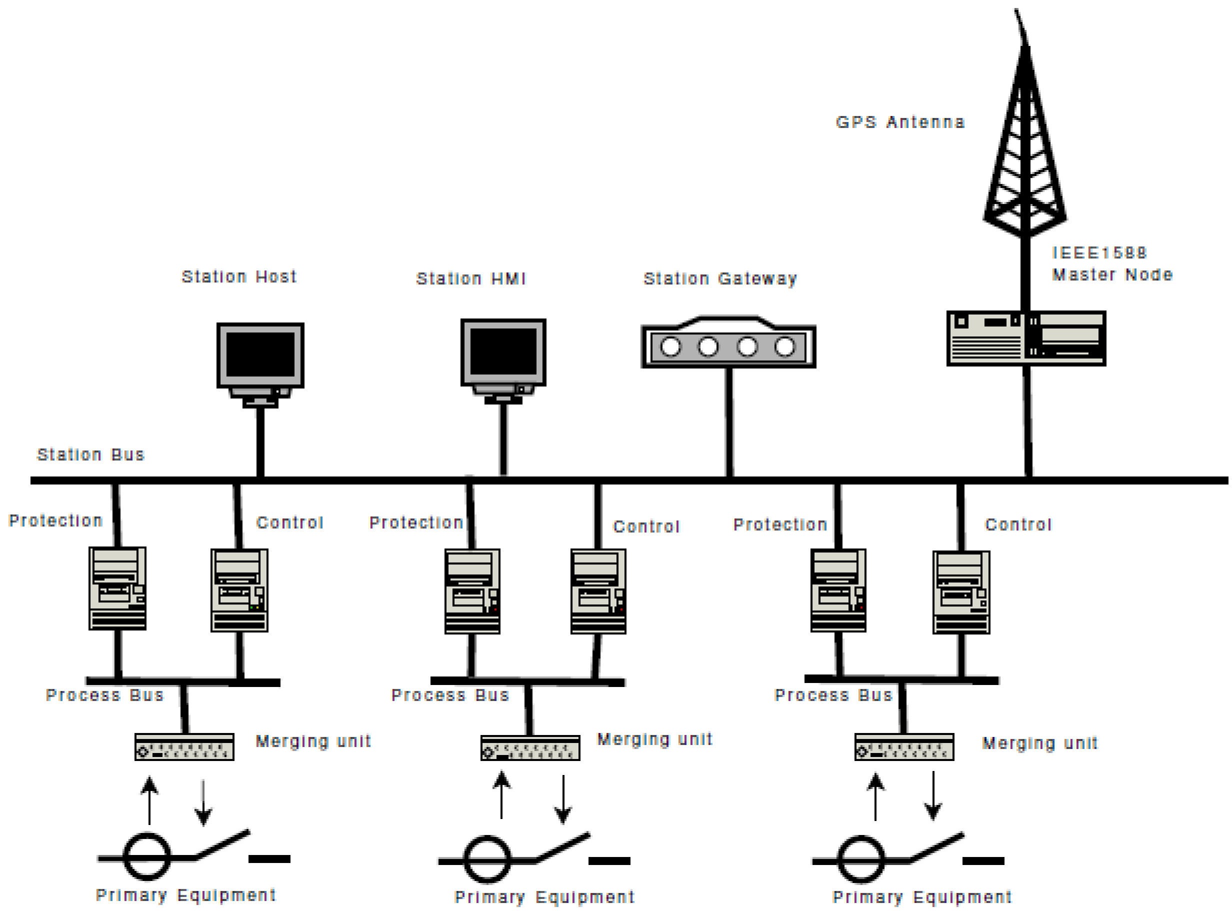


Figure 1.3-4 Synchronization architecture of electric substation [2.5.4.34]

<u>Impacts of Cyber Attacks</u>

The system in Figure 1.3-4 Synchronization architecture of electric substation [2.5.4.34]Figure 1.3-4 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.

Prevention of Impacts by Adoption of Elements of Secure Timing

Figure 3 shows the main components of a secure synchronization architecture:

- All PTP-enabled (internal) subsystems have a secure time protocol stack implementation (A). 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 GPS and PTP network 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 [2.5.4.40].
- Predictable failure can be achieved through the IDS which inspects Station Bus traffic for suspicious patterns (i.e. 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 (F) on the station gateway.

- The local station bus can be further physically protected (e.g. isolated) to prevent attacks from temporally attached external nodes (see Crain / Sistrunk DNP3 vulnerability [2.5.4.41]).
- PTP enabled subsystems can compensate DoS attacks via clock drift correction [2.5.4.34].

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 (for example a malware infection of the Station Host in Figure 1.3-5), the entire substation is again vulnerable to all attacks listed in Table 1.3-3.

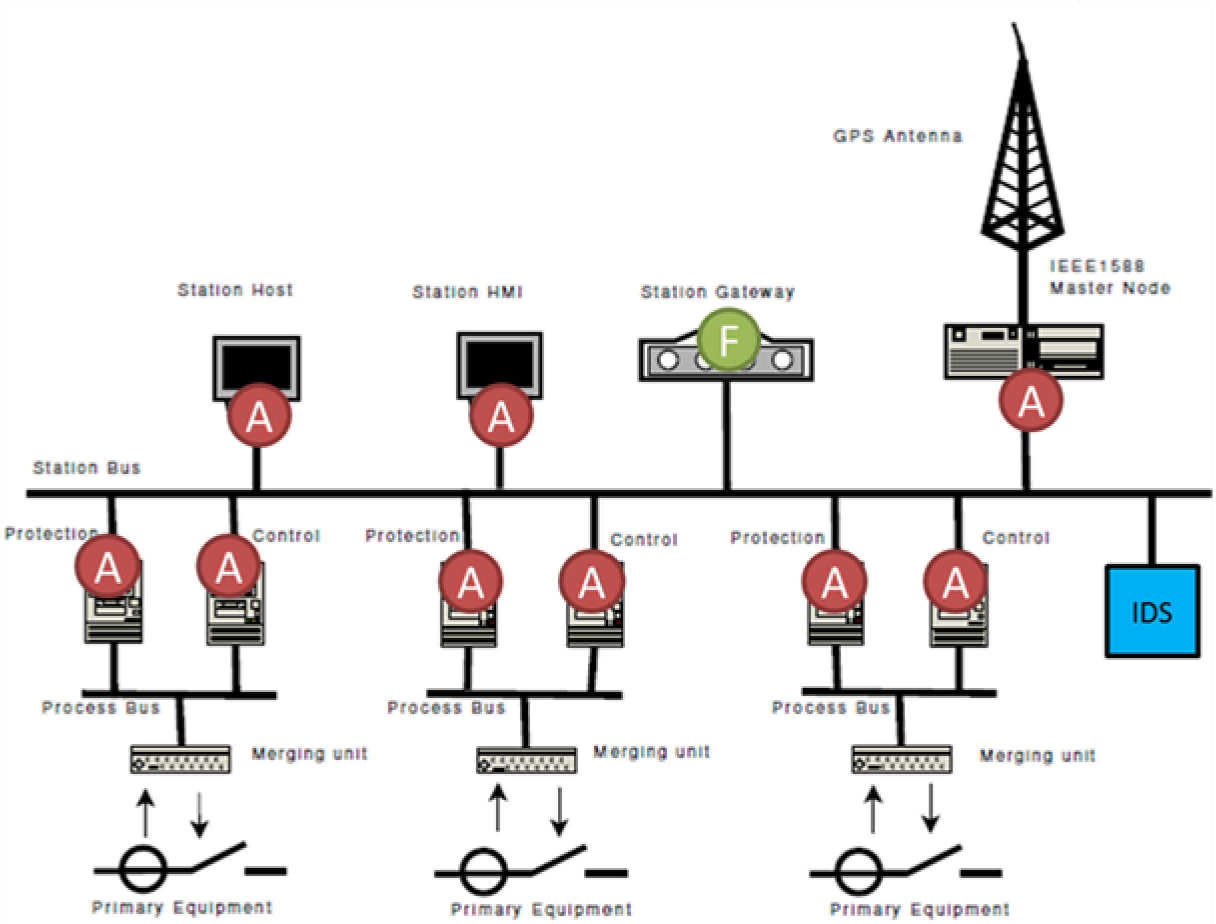


Figure 1.3-5 Secure synchronization architecture of electric substation

1.4. Timing Use Cases Appendix

To illustrate the variety of timing requirements in CPS, we give examples in the table below. The application domains 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 1.4-1 Examples of timing requirements in CPS

CPS Application Domain	Domain 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 Microsecond
	Software Defined Networking & Network Function Virtualization	UTC	<100 Nanosecond
	Real-Time Communications-Cross Layer Quality of Service (QoS) Provisioning	UTC	Millisecond
	Real-Time Media Synchronization	UTC	Microsecond
Emergency Services Sector	Phase for positioning		~ Nanoseconds (CDMA E911, LMRs)
Energy/Electric Power Subsector			1-4.6 Microsecond (Synchro-Phasors; Fault Loc.)
Health	Patient Care Devices (PCD) Signal correlation	Phase	Millisecond
	Remote Surgery/Intervention	Bounded Latency, Phase	
Critical Manufacturing Sector			Millisecond
	Robotics- realtime coordination	UTC, Phase	Microsecond
Defense Industrial Base Sector	various	various	Nanoseconds to Milliseconds
Transportation Sector			~ Nanoseconds (Wireless modal comms)
	UAV/UGV Unmanned Aerial/Gnd Vehicle Positioning &Nav	UTC	Nanoseconds (GNSS or alternative)
	Intra-vehicle Synchronized Signalling	Phase	10-50 Millisecond
	V2V /V2R Synchronized Signalling	UTC,Phase	10-50 Millisecond
	Aircraft Diagnostics	UTC,Phase	10-50 Nanosecond

	Aerospace Test Instrumentation & Telemetry	Phase	<100 Nanosecond
	Bridge Structural Integrity Monitoring	Phase	<100 Nanosecond
	Traffic Control	Phase, UTC	10-50 Milliseconds
SmartBuildings	HVAC Optimization	Phase	Computational Fluid Dynamics Modelling 10-50 Millisecond
	Energy Management System – Fault Diagnosis	Phase, UTC	1 Millisecond
Environmental Monitoring	Pollution Monitoring/Alert System	Phase, UTC	< 1 sec
	Extreme Weather Mitigation	UTC	< 1sec
Smart Agriculture	Precision Nutrient Management	UTC	Location <100 Nanoseconds
Consumer Devices	Multimedia Synchronization	UTC	1 Microsecond
	Virtual Reality Psychoacoustics	Phase	1 Microsecond

*The accuracy requirements in this table come from a variety of sources and private communications.

1.5.References Appendix

1.5.1. References from Introduction

[2.5.1.1] ITU-R Recommendation TF,686-3 (12/2013) Glossary and Definitions of Time and Frequency Terms 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.

[2.5.1.2] 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

[2.5.1.3] D.B. Sullivan, D.W. Allan, D.A. Howe, and F.L. Walls, "Characterization of Clocks and Oscillators," NIST Tech. Note 1337, June 1, 1999, available from: http://tf.boulder.nist.gov/general/pdf/868.pdf

1.5.2. References from Time Awareness

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

[2.5.2.2] Jasperneite, J.; Feld, J., "PROFINET: an integration platform for heterogeneous industrial communication systems," Emerging Technologies and Factory

Automation, 2005. ETFA 2005. 10th IEEE Conference on , vol.1, no., pp.8 pp.,822, 19-22 Sept. 2005

[2.5.2.3] Timing Committee Telecommunications and Timing Group- Range Commanders Council, “IRIG Serial time code formats,” September, 2004. [Online]. Available: http://www.irigb.com/pdf/wp-irig-200-04.pdf

[2.5.2.4] Kaplan, Elliott D., and Christopher J. Hegarty, eds. Understanding GPS: principles and applications. Artech house, 2005.

[2.5.2.5] IEEE Instrumentation and Measurement Society, “1588: IEEE standard for a precision clock synchronization protocol for networked measurement and control sytems” IEEE, Standar Specification, July 24, 2008

[2.5.2.6] K. Harris, “An application of IEEE 1588 to industrial automation,” in Precision Clock Synchronization for Measurement, Control and Communication, 2008, ISPCS. IEEE International Symposium on. IEEE, 2008, pp 71-76

[2.5.2.7] M. Shepard, D. Fowley, R. Jackson, and D. King, “Implementation of IEEE Std-1588 on a Networked I/O Node, “ in Proceedigns of the 2003 Workshop on IEEE-1588, NIST publication NISTIR 7070, Gaithersburg, MD, 2003.

[2.5.2.8] F. Steinhauser, C. Riesch, and M. Ridigier, “IEEE 1588 for time synchronization of devices in the electric power industry,” in Precision Clock Synchronization for Measurement, Control and Communication, 2010, ISPCS. IEEE International Symposium on. IEEE, 2010, pp 1-6

[2.5.2.9] Giorgio C. Buttazzo: Hard Real-Time Computing Systems: Predictable Scheduling Algorithms and Applications, Third Edition. Real-Time Systems Series 24, Springer 2011, ISBN 978-1-4614-0675-4, pp. 1-521

[2.5.2.10] R. Wilhelm, D. Grund: Computation takes time, but how much? Commun. ACM 57(2): 94-103 (2014)

[2.5.2.11] 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, W. Yi: Building timing predictable embedded systems. ACM Trans. Embedded Comput. Syst. 13(4): 82 (2014)

[2.5.2.12] 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, P. Stenström: The worst-case execution-time problem - overview of methods and survey of tools. ACM Trans. Embedded Comput. Syst. 7(3) (2008)

[2.5.2.13] J. Rushby and W. Steiner, “TTA and PALS: Formally verified design patterns for distributed cyber-physical systems,” in 30th IEEE/AIAA Digital Avionics Systems Conference (DASC), Seattle, WA, 2011.

[2.5.2.14] ARINC, “ARINC 653 family of standards,” November, 2010. [Online]. Available: https://www.arinc.com/cf/store/

[2.5.2.15] Edward A. Lee: Computing needs time. Commun. ACM 52(5): 70-79 (2009)

[2.5.2.16] PHYTER, DP83640 Precision. "IEEE 1588 precision time protocol transceiver." (2008).

[2.5.2.17] Corbett, James C., et al. "Spanner: Google’s globally distributed database."ACM Transactions on Computer Systems (TOCS) 31.3 (2013): 8.

[2.5.2.18] Y. Zhao, E.A. Lee, and J. Liu. A programming model for time-synchronized distributed real-time systems. In Real-Time and Embedded Technology and Applications Symposium (RTAS), Bellevue, WA, USA, April 3-6 2007. IEEE.

[2.5.2.19] Broman, David, Patricia Derler, and John Eidson. "Temporal issues in cyber-physical systems." Journal of the Indian Institute of Science 93.3 (2013): 389-402.

1.5.3. References from Timing and Latency

[2.5.3.1] Open Networking Foundation, “OpenFlow Switch Specification,” October 14, 2013. [Online]Available from: https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.4.0.pdf

[2.5.3.2] Paul Congdon, “Link Layer Discovery Protocol Overview (LLDP),” March 8, 2003. [Online] Available from: http://www.ieee802.org/1/files/public/docs2002/LLDP%20Overview.pdf

[2.5.3.3] PROFINET. [Online] presentation at: http://www.profibus.com/technology/profinet/

[2.5.3.4] IETF Network Working Group, “Simple Network Management Protocol (SNMP)”. [Online] available at: https://www.ietf.org/rfc/rfc1157.txt

[2.5.3.5] CANopen. [Online] available from: http://www.can-cia.org/index.php?id=canopen

[2.5.3.6] Center for Hybrid and Embedded Software (CHESS), UC Berkeley, “PTIDES”. [Online] see: http://chess.eecs.berkeley.edu/ptides/

[2.5.3.7] National Instruments, “LabVIEW System Design Software”. [Online] see: http://www.ni.com/labview/

1.5.4. References for Secure and Resilient Timing and Appendix to Security and Resilience

[2.5.4.1] IEEE Instrumentation and Measurement Society, IEEE 1588-2008 IEEE Standard for Precision Clock Synchronization Protocol for Measurement and Control Systems, 24 July 2008.

[2.5.4.2] NTP: The Network Time Protocol. [Online] http://www.ntp.org/

[2.5.4.3] (1994). SPECIFICATION OF THE TRANSMITTED LORAN-C SIGNAL. U.S Department of Transportation.

[2.5.4.4] ATIS COAST Standards Body, document SYNC-2014-00052R000 from NIST, “CONTRIBUTION TO STANDARDS PROJECT — COAST-SYNC: WWVB for Assisted Timing.” John Lowe; Marc Weiss. October 2013.

[2.5.4.5] A.J. Kerns, K.D. Wesson, and T.E. Humphreys, "A Blueprint for Civil GPS Navigation Message Authentication," IEEE/ION PLANS, Monterey, CA, May 2014. [Online] available from: http://radionavlab.ae.utexas.edu/images/stories/files/papers/nmaimpPLANS2014.pdf

[2.5.4.6] Johnson, G. S. (2007). An Evaluation of eLoran as a Backup to GPS. *Technologies for Homeland Security, 2007 IEEE Conference on* (pp. 95-100). Woburn, MA: IEEE.Satisfiability. (n.d.). Retrieved October, 2014, from http://en.wikipedia.org/wiki/Satisfiability

[2.5.4.7] A. Pearson and K. Shenoi. “A Case for Assisted Partial Timing Support Using Precision Timing Protocol Packet Synchronization for LTE-A,” *IEEE Communications Magazine*, August 2014, pp. 136-143.

[2.5.4.8] T. Mizrahi, RFC 7384: Security Requirements of Time Protocols in Packet-Switched Networks. https://www.rfc-editor.org/rfc/rfc7384.txt

[2.5.4.9] T. Mizrahi, Time synchronization security using IPsec and MACsec, International IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication (ISPCS), 2011

[2.5.4.10] *D. Sibold, S. Roettger, K. Teichel*, “Network Time Security”, October 2014. https://tools.ietf.org/html/draft-ietf-ntp-network-time-security-05

[2.5.4.11] *D. Sibold et al.*, “Protecting Network Time Security Messages with the Cryptographic Message Syntax (CMS)”, October 2014, https://tools.ietf.org/html/draft-ietf-ntp-cms-for-nts-message-00

[2.5.4.12] *IEEE 1588 Working Group Website.* https://ieee-sa.centraldesktop.com/1588public/ 20 Nov. 2013.

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

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

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

[2.5.4.16] Fontanella, D., Bauernfeind, R., and Eissfeller, B. "In-Car GNSS Jammer Localization Using Vehicular Ad-Hoc Networks." *Inside GNSS*. May/June 2013.

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

[2.5.4.18] Kerns, A.J., Wesson, K.D., Humphreys, T.E., "A blueprint for civil GPS navigation message authentication," Position, Location and Navigation Symposium - PLANS 2014, 2014 IEEE/ION , pp.262-269, 5-8 May 2014

[2.5.4.19] "The Global Differential GPS System: Integrity and Performance Monitoring." *NASA Jet Propulsion Laboratory*. http://www.gdgps.net/products/monitoring.html

[2.5.4.20] Hein, G., Kneissl, F., and Stober, C. "Combined Integrity of GPS and Galileo", Inside GNSS, January/February 2010. http://www.insidegnss.com/node/1827

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

[2.5.4.22] "Severe Space Weather Events – Understanding Societal and Economic Impacts: A Workshop Report." 2008, p.78. http://www.nap.edu/catalog/12507/severe-space-weather-events--understanding-societal-and-economic-impacts

[2.5.4.23] Kappenman, J. "Geomagnetic Storms and Their Impacts on the U.S. Power Grid." January 2010. http://web.ornl.gov/sci/ees/etsd/pes/pubs/ferc_Meta-R-319.pdf

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

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

[2.5.4.26] R. Cohen, PTP Security Tutorial, International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), 2007

[2.5.4.27] A. Treytl, G. Gaderer, B. Hirschler, Traps and pitfalls in secure clock synchronization, International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), 2007

[2.5.4.28] A. Treytl, B. Hirschler, Validation and Verification of IEEE 1588 Annex K, International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), 2011

[2.5.4.29] C. Önal and H. Kirrmann, Security improvements for IEEE 1588 Annex K, International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), 2012

[2.5.4.30] S. Röttger, Analysis of the NTP Autokey Extension (in German), University of Braunschweig and Physikalisch-Technische Bundesanstalt Braunschweig, 2011

[2.5.4.31] A. Treytl, B. Hirschler, Security Flaws and Workarounds for IEEE 1588 (Transparent) Clocks, International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), 2009

[2.5.4.32] A. Treytl, B. Hirschler, Practical Application of 1588 Security, International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), 2008

[2.5.4.33] RFC 6066. Lnternet Engineering Task Force (IETF) Transport Layer Security (TLS) Extensions: Extension Definitions. January 2011. https://tools.ietf.org/html/rfc6066

[2.5.4.34] J. Tournier, O. Goerlitz, Strategies to Secure the IEEE 1588 Protocol in Digital Substation Automation, Fourth International Conference on Critical Infrastructures (CRIS), 2009

[2.5.4.35] Daniel P. Shepard, D.P.; Humphreys, T.E., Fansler, A.A. "Going Up Against Time: The Power Grid's Vulnerability to GPS Spoofing Attacks." GPS World, August 2012.

[2.5.4.36] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks, slide no. 11, September 21, 2012.

[2.5.4.37] "Time Anomaly Detection Applique", 2013. http://www.mitre.org/research/technology-transfer/technology-licensing/time-anomaly-detection-appliqu%C3%A9-tada

[2.5.4.38] Langley, R.B. "Innovation: GNSS Spoofing Detection." GPS World. http://gpsworld.com/innovation-gnss-spoofing-detection-correlating-carrier-phase-with-rapid-antenna-motion/

[2.5.4.39] Pearson, T. and Shenoi, K. "A Case for Assisted Partial Timing Support Using Precision Timing Protocol Packet Synchronization for LTE-A." *IEEE Communications Magazine,* 52 (8), August 2014, pp. 135-143.

[2.5.4.40] Amelot, J., Li-Baboud, Y., Vasseur, C., Fletcher, J., Anand, D., and Moyne, J. "An IEEE 1588 Performance Testing Dashboard for Power Industry Requirements," *Proceedings of International IEEE Symposium on Precision Clock Synchronization for Measurement Control and Communication (ISPCS)*, pp. 132-137, 12-16 Sept. 2011.

[2.5.4.41] Crain, A. and Sistrunk, C. Advisory (ICSA-13-210-01). https://ics-cert.us-cert.gov/advisories/ICSA-13-219-01

[2.5.4.42] E. O. Schweitzer, E.O; Guzmán, A. "Real-Time Synchrophasor Applications for Wide-Area Protection, Control, and Monitoring." © 2009 by Schweitzer Engineering Laboratories, Inc.

[2.5.4.43] http://www.bpa.gov/news/newsroom/Pages/Synchrophasor-success-lands-B...

[2.5.4.44] Goldstein, A. Email to the CPS_Sync list dated 16 SEPT 2014.

[2.5.4.45] http://www.microsemi.com/products/timing-synchronization-systems/time-frequency-distribution/gps-instruments/xli-saasm ; also Symmetricom's GPS Disciplined Master Timing Reference (ATS 6501B). Warriner, J., private communication on 21 February 2014.

[2.5.4.46] *I. Fernández Hernández,* "Design Drivers, Solutions and Robustness Assessment of Navigation Message Authentication for the Galileo Open Service," ION GNSS+ 2014, Tampa, FL, September 2014.

[2.5.4.47] *J.T. Curran, M. Paonni, J. Bishop,* "Securing GNSS: An End-to-end Feasibility Analysis for the Galileo Open-service," ION GNSS+ 2014, Tampa, FL, September 2014.

[2.5.4.48] *Factsheet: National Risk Estimate: Risks to U.S. Critical Infrastructure from Global Position System Disruptions,* June 2013. http://www.gps.gov/news/2013/06/2013-06-NRE-fact-sheet.pdf

1.5.5. General Timing Definitions and Related Standards

[2.5.5.1] ITU-R Recommendation TF,686-3 (12/2013) Glossary and Definitions of Time and Frequency Terms 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.

[2.5.5.2] All ITU-T published recommendations can be downloaded from: http://www.itu.int/rec/T-REC-G/e

We list ITU-T Published Recommendations associated with timing in telecom networks.

1. 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)

2. 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
    - Recommendation ITU-T G.8261.1, Packet Delay Variation Network Limits applicable to Packet Based Methods (Frequency Synchronization).
    - Recommendation ITU-T 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
3. 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