

This document gives a brief overview of the requirements for time accuracy and traceability to MiFID II, examines time errors that influence business clock performance, and three key test methods to ensure the network system meets MiFID II standards. There is also a complementary document CX7002 PTP: Synchronizing Networks and Demonstrating MiFID II Time Compliance.

# Verifying the accuracy of business clocks in a trading venue

## Testing to MiFID II



## Timing accuracy and MiFID II

In their “A complete guide to time stamping regulations in financial sector”, the UK National Physics Laboratory state:

*“Accurate and traceable time is vital for today’s financial markets. In a world of high-frequency trading where fortunes can be made or markets crashed in a fraction of a second, absolutely accurate time stamping is essential to determine exactly who made what trade, and precisely when”*

The EU and European Securities and Markets Authority (ESMA) also recognize the importance of accurate time stamping and, in January 2018, published MiFID II. The purpose was to make European financial markets more transparent and to strengthen investor protection. This document cited the requirement for synchronization of business clocks; details of this are outlined in the Technical Standard RTS 25. In this document it states in article 4 that:

*“Operators of trading venues and their members or participants shall establish a system of traceability to UTC. They shall be able to demonstrate traceability to UTC by documenting the system design, functioning and specifications. They shall be able to identify the exact point at which a timestamp is applied and demonstrate that the point within the system where the timestamp is applied remains consistent. Reviews of the compliance with this Regulation of the traceability system shall be conducted at least once a year.”*

Elaborating on the need for accurate time when reporting on trades, the ESMA make it clear that timing sources within and between trading venues must have both accuracy (a maximum divergence from reference time) and a commonality to the reference time to ensure that authorities can establish the timeline of reportable events correctly. The levels of accuracy and maximum divergence from Coordinated Universal Time (UTC) specified for business clocks are dependent on the gateway-to-gateway latency of trading systems (in the case of operators of trading venues) or the types of trading activities (in the case of members/participants). The resultant requirements are illustrated below.

Gateway-to-gateway latency time of the trading system	Maximum divergence from UTC	Granularity of the timestamp
> 1 ms	1 ms	1 ms or better
≤ 1 ms	100 μs	1 μs or better

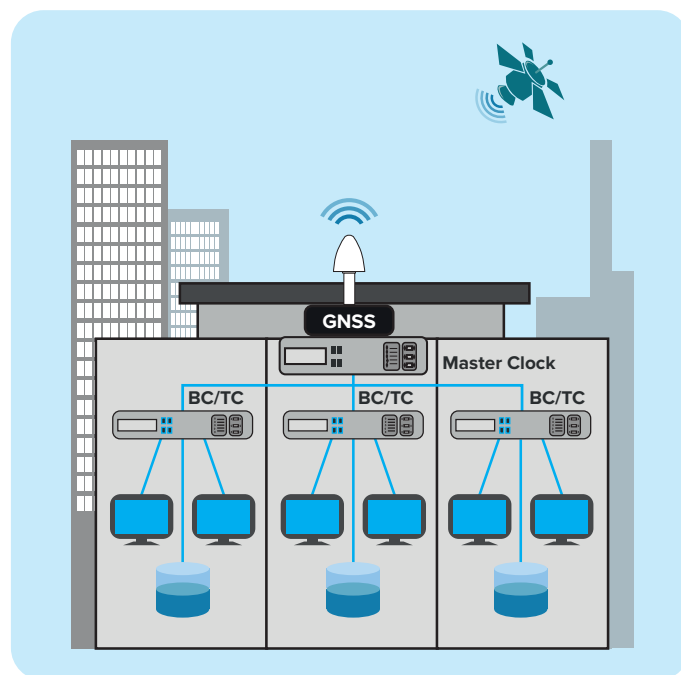
Two important aspects trading venues should address when building compliance and traceability into their networks are:

1. Proper network design
2. Verification through testing

### Network design

In some networks, such as mobile phone systems, accurate timing is required to prevent interference and system failure. This has its advantages because timing inaccuracy will make itself known through performance degradation and ultimately failures in the network. In trading venues, accurate timing is the requirement of the application rather than to assure operation. This has the disadvantage that timing inaccuracies and non-compliance to MiFID II can go unnoticed and will not cause the network at a trading venue to fail. Poor timing accuracy could go unnoticed for an extended period of time. This puts additional pressures on the operator to design a robust system and to have processes in place to test and verify compliance.

A greatly simplified view of a network from the standpoint of timing is shown below. The network must have an accurate source of UTC traceable time and a way to distribute this through the network.



UTC is identified as the reference time for MiFID II compliance. There are publicly available time servers available over the internet, however, it is generally accepted that these are not reliable or accurate enough to comply with MiFID II.

The most common method to receive UTC into a network is through GNSS (Global navigation satellite systems). This may be one of many systems including GPS, Galileo, BeiDou, GLONASS and others. GNSS is commonly used for time synchronization in communications networks around the globe. Time derived from GNSS is recognized as traceable to UTC with the use of leap seconds to compensate for the slowing of the earth’s rotation. The ESMA has stated in a guideline that:

*“The use of the time source of the U.S. Global Positioning System (GPS) or any other global navigation satellite system such as the Russian GLONASS or European Galileo satellite system when it becomes operational is also acceptable to record reportable events.”*

GNSS is very useful but is not fail proof and can be jammed or spoofed. As it cannot be considered 100% reliable, it is not uncommon, therefore, for data centres to also use atomic clocks. These will be disciplined to GNSS and, in the event of loss of the GNSS, maintain accurate time in holdover until GNSS service is restored.

To implement GNSS, an antenna with line of sight to the sky is connected to the GNSS receiver by an RF cable. The timing information from the GNSS receiver is then fed out into the network by the PRTC/GM (Primary Reference Time Clock/ Grandmaster) which communicates the time into the network. The cable from the GNSS receiver to the antenna can often be quite long. The, roughly, 5 ns per metre delay the RF cable and the group delay of the antenna can lead to significant timing error. However, this will be a constant error and can be compensated for by properly configuring the GM.

## Time distribution

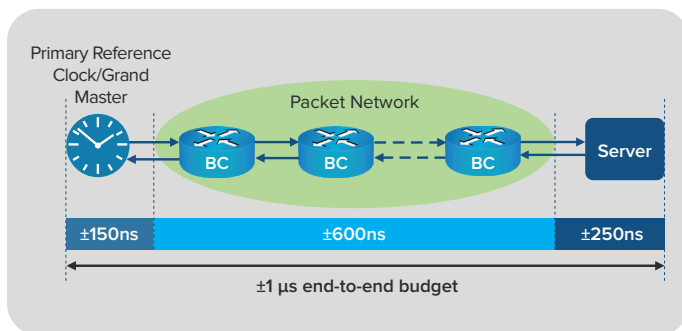
Modern packet-based networks have well established protocols for maintaining timing. The timing is transferred through the nodes of the network which, in the case of full timing support, act as boundary clocks (BC) or transparent clocks (TC). The server recovers the timing information to provide accurate time stamping.

BCs calibrate themselves by recovering and regenerating the Precision Timing Protocol (PTP) timing from the previous clock in the chain, thereby minimizing the Packet Delay Variation (PDV) accumulation at the edge of the network. If TCs are used, the delay through the TC is written into a correction field within the packet. The end clock then has a record of the delay for each TC on the path.

Network Timing Protocol (NTP) is widely used in computer networks, however, it is only accurate, in practice, to within a few milliseconds. The Chrony implementation of NTP improves this to a couple hundred microseconds, and with hardware stamping this can be improved to around 100  $\mu$ s. While Chrony with hardware time stamping may achieve 100  $\mu$ s, it would not be acceptable to allocate the entire network error budget to the timing distribution. The obvious choice is to implement PTP that can achieve accuracies several orders of magnitude better than the 100  $\mu$ s requirement of MiFID II.

## Error budget

Even a well-designed network with a stable time reference and PTP time distribution will experience time synchronization errors and a robust design should include allocation of an error budget to these various error sources.



## Common sources of error

**GNSS** – Ionospheric delays, RF noise and positional error in the satellites leads to tens of nanoseconds of error.

**Holdover** – Should the GNSS system go down, a backup system will be called upon. This is often a local highly stable atomic clock. When these clocks are not disciplined to a reference such as GNSS, they are said to be in holdover. Atomic clocks will drift slightly while in holdover. A well designed network will allow for periods of holdover in their error budget.

**Asymmetry in the network** – Protocols like PTP assume that the communication time in the forward and return directions is the same when the master clock is communicating with the subordinate clock. This symmetry is never perfect and can be affected by differing fibre lengths on the two paths or in differing queuing times in the two directions because of traffic conditions.

**Packet delay variation (PDV)** – Packets will always be delayed by some amount in the nodes of the network. The delay will be impacted by traffic density which is variable. When these packets carry timing information, the resulting PDV will lead to timing inaccuracies.

## Importance of error budget

A properly developed error budget can not only provide evidence that the network is well designed and will operate within the maximum divergence requirements specified in MiFID II, it can also save money.

For example, by not over specifying network components, the most cost-effective or commonly available appliances can be selected to ensure efficient network architectures are implemented. This goes hand-in-hand with the idea that items in the error budget should not be under specified. If an item in the network is given too loose an error budget for what is commonly achievable, then error budget is wasted, and it may be necessary to use more expensive components elsewhere in the network.

Therefore, if PTP is implemented, it is reasonable and prudent to require that it synchronizes the network to within around  $\pm 1 \mu$ s. This would allow the remaining error budget to be allocated to items such as holdover or to uncertainties in the timestamping process in the application.

## Verification

Article 4 of RTS 25 could be interpreted to say that the responsibility of the trading venue operator is limited to the proper design of a network traceable to UTC and capable of maintaining performance within the granularity and traceability requirements. However, the published guidance goes on to make several additional statements:

*“Relevant and proportionate testing of the system should be required along with relevant and proportional monitoring thereof to ensure that the divergence from UTC remains within tolerance.”*

*“Competent authorities need to be able to reconstruct all events relating to an order throughout the lifetime of each order in an accurate time sequence. Competent authorities need to be able to reconstruct these events over multiple trading venues on a consolidated level to be able to conduct effective cross-venue monitoring on market abuse.”*

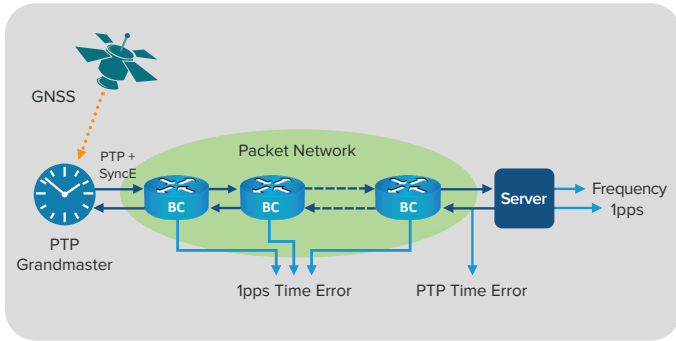
Different organizations have published varying views on how verification should be achieved. At the time of writing, there is no prescriptive standards giving exactly how performance is to be measured. In fact, the standard only specifies the divergence and granularity. Guidance is not given in terms of the period over which tests are to be made, the loading on the network, acceptable dynamic variation or other details. In reaction to this ambiguity, organizations that consult on MiFID II compliance audits are recommending sometimes conflicting verification criteria. Rather than getting into the specifics on the interpretation of the measurement results, based on the information that has been published, here are three common verification methodologies.

- Test the network periodically
- Monitor the performance continuously
- Test periodically while stressing the network

## Periodic testing

Perhaps the most obvious testing methodology is to perform timing accuracy tests during the annual audit. A suitable test instrument can be disciplined to GNSS and used to probe the network at various points. Measurements near the GM can verify that the network is being provided with accurate time. This will also verify that any changes in hardware such as changes to the antenna or antenna cable have been compensated for and are not adversely affecting timing. For example, if the length of the cable to the GNSS antenna has been changed, then measuring the accuracy of the delivered PTP to the network will verify if the settings have been adjusted properly in the GM to compensate for the cable change.

The test can be as simple or elaborate as the operator feels is necessary to verify performance. Measurements could be made at the GM and then at several points throughout the network. Alternatively, a few tests could be made at the network edge based on the principle that, if the timing is good at the edge, everything back to the timing source is working correctly.



One of the uncertainties in these methodology is determining for how long to make a measurement at any given point in the network. Longer measurements are more likely to catch occurrences of non-compliance. Ideally, an instrument used to make this measurement, would be able to measure multiple signals over an extended period, storing the results for later thorough analysis.

In addition, because the network timing accuracy is often affected by the activity on the network, the measurement period should be long enough to capture periods of high and low network activity.

### Continuous monitoring

If it is assumed that the purpose of the verification methodology includes the ability to determine the network conditions retrospectively at the time of any reportable event, then it may be advantageous to continuously monitor the network timing accuracy.

### Related Products



#### Calnex Sentinel

Sentinel is a dedicated network synchronization test instrument able to make multiple simultaneous measurements, store the test results and generate detailed reports for audit purposes. Features include:

- PTP, NTP and SyncE in one portable box
- Built-in GPS receiver and Rubidium (Rb) clock
- Measure ALL parameters at the SAME time
- Test networks for Frequency and Phase
- Test networks with Boundary Clocks and Transparent Clocks

In this case, we would want a test instrument that could be configured to measure continuously. Through a remote interface, such as an API, results could be downloaded and archived for use at a later date making it possible to verify the status of the network timing at any time in the past. This methodology has the additional advantage that it will allow the operator to look at the performance of the timing during periods of extremely high traffic flow.

### Stress testing

In another article of MiFID II which is concerned with testing the algorithmic trading, the subject of stress testing is discussed:

*“As part of its annual self-assessment referred to in Article 9, an investment firm shall test that its algorithmic trading systems and the procedures and controls referred to in Articles 12 to 18 can withstand increased order flows or market stresses. The investment firm shall design such tests, having regard to the nature of its trading activity and its trading systems. The investment firm shall ensure that the tests are carried out in such a way that they do not affect the production environment. Those tests shall comprise:*

*(a) running high messaging volume tests using the highest number of messages received and sent by the investment firm during the previous six months, multiplied by two;*

*(b) running high trade volume tests, using the highest volume of trading reached by the investment firm during the previous six months, multiplied by two.”*

While this is not specifically directed at the clock accuracy, the principle still applies. Network timing accuracy is affected by the loading on the network and the queueing and asymmetry it can create. However, it is difficult to know ahead of time when these periods of increased flow will happen. Therefore, when periodic verification is done on the timing accuracy, it would be good practice to run these tests while emulating high traffic activity.

Direction	Packet #	Arrival Time	Message Type	Message ID	Source ID	Destination ID	Sequence	PTP Body Fields
0	0	0.00000000	SYNC	0x0	0x0	0x0	19826	-4
0	1	0.00031605	DEL-RESP	0x0	0x0	0x0	30231	127
0	2	0.00068189	DEL-RESP	0x0	0x0	0x0	30231	-4
0	3	0.00104773	SYNC	0x0	0x0	0x0	19827	-4
0	4	0.00141357	DEL-RESP	0x0	0x0	0x0	30232	127
0	5	0.00177941	DEL-RESP	0x0	0x0	0x0	30232	-4
0	6	0.00214525	SYNC	0x0	0x0	0x0	19828	-4
0	7	0.00251109	DEL-RESP	0x0	0x0	0x0	30233	127
0	8	0.00287693	DEL-RESP	0x0	0x0	0x0	30233	-4
0	9	0.00324277	SYNC	0x0	0x0	0x0	19829	-4
0	10	0.00360861	DEL-RESP	0x0	0x0	0x0	30234	127
0	11	0.00397445	DEL-RESP	0x0	0x0	0x0	30234	-4
0	12	0.00434029	SYNC	0x0	0x0	0x0	19830	-4
0	13	0.00470613	DEL-RESP	0x0	0x0	0x0	30235	127
0	14	0.00507197	DEL-RESP	0x0	0x0	0x0	30235	-4
0	15	0.00543781	SYNC	0x0	0x0	0x0	19831	-4
0	16	0.00580365	DEL-RESP	0x0	0x0	0x0	30236	127
0	17	0.00616949	DEL-RESP	0x0	0x0	0x0	30236	-4
0	18	0.00653533	SYNC	0x0	0x0	0x0	19832	-4
0	19	0.00690117	DEL-RESP	0x0	0x0	0x0	30237	127
0	20	0.00726701	DEL-RESP	0x0	0x0	0x0	30237	-4
0	21	0.00763285	SYNC	0x0	0x0	0x0	19833	-4

#### Calnex PFV

- PTP Field Verifier – decode and view multiple PTP fields in an easy-to-use table format
- Check transmitted PTP messages for compliance with IEEE, IEC, ITU-T and user-defined standards and rules



calnexsol.com