orolia

☑ Checklist

MIFID II Clock Sync Requirements

5 MIFID II Requirements for Clock Sync

1 Sync clocks to UTC using a traceable source like GPS

2 Prove the accuracy of clock offset

3 Ensure max clock drift doesn’t exceed 100 microsecond / 1 millisecond

4 Provide timestamps with a granularity of 1 microsecond / 1 millisecond

5 Be able to demonstrate where the timestamp is applied and that it remains consistent

MIFID II Readiness: Sync or Swim

MIFID II RTS 25 compliance is already in effect. Five requirements. Seems simple enough, right?

Not so fast … there are a few more details to consider. To help with those details, use this handy checklist to make sure that you’re aware of the key considerations, your timing chain is ready and you’re able to comply.

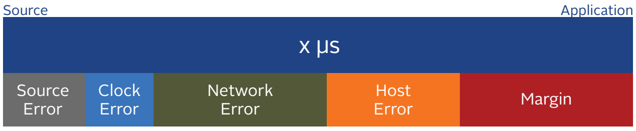
Timing Budget

Let’s quickly identify all the primary devices or components within the timing chain and how they relate to your timing budget.

Your timing budget is essentially the accuracy threshold you’re trying to stay beneath. It could be

100 microseconds or 1 millisecond, depending on how you’re categorized under the regulations.

The goal is to make sure the error or latency introduced by all these components add up to a number less than your target total time budget, with that delta being the “margin.”



Source error Where you are getting your time from (GPS, service provider, etc.) and the known error (usually below 10ns for GPS for example)

Clock error The error added when you consume the time source (from 25ns for GPS up to 1µs for a PTP Source)

Network error Asymmetry in the network, Packet Delay Variation (PDV), latency through switches, etc.

Host error Inaccuracy due to the consumption of time by the host’s timing client host, due to OS’s own inaccuracy, SW timestamping mechanism

Margin Everything else

Architecture

☐ 1. Is your architecture capable of meeting the regulations?

☐ 2. Is your time source traceable to UTC or GPS? If you aren't getting time directly from one of those sources, can you get the UTC or GPS offset details from your time source provider? This information is crucial to provide full traceability to UTC and comply with the regulations.

☐ 3. Is your timing network architecture clearly documented? Including function of relevant elements and associated specs?

☐ 4. Have you determined your time budget allowance for each of the components in the timing chain? If you have not, it would be helpful to determine the amount of offset each of those components adds to your overall offset. Knowing this will be important to understand where your inefficiencies are and where there is opportunity to improve performance.

☐ 5. Are you able to identify the exact point in your system where the timestamp is being applied? Can you demonstrate that this point remains consistent?

☐ 6. Do you have a mechanism in place to review all this on an annual basis to ensure ongoing compliance?

☐ 7. If you use GPS/GNSS, the ESMA states that you must mitigate risks associated with those signals (atmospheric interference, intentional jamming, spoofing, etc.). Do you have a solution to address issues like spoofing / jamming detection software or anti-jam antennas?

Testing

☐ 1. Have you tested your design in a lab environment to establish a performance baseline?

☐ 2. Have you tested all deployments to ensure your results are similar to what you achieved in the lab?

☐ 3. Do you have the proper mechanisms in place to document and retest if changes are made to any element in the timing chain?

☐ 4. Is your testing proportionate? Put another way, are you testing in a way that is more granular than what you are trying to measure?

□ 5. How does your timing implementation perform when:

- □ Competing for priority when there is heavy network traffic?
- □ Stability is an issue? Is the offset relatively deterministic and unchanging from day to day?
- □ Your primary reference is lost?
- □ You're the victim of a jamming or spoofing attack?

□ 6. How long are you able to remain in compliance while in holdover (when there is a loss of the reference and you're running solely off the internal oscillator of your time source)? Is that long enough to troubleshoot, identify and resolve most common issues?

Reporting

□ 1. Are you collecting the necessary details to link the timestamps on reportable events to the reference so you can see where the time it is being derived from?

□ 2. Do your reports provide the full offset value between UTC or GPS and your timestamps being applied to reportable events?

□ 3. Do you have a method to make sure report data is not lost (i.e., stored in redundancy or offline)? Regulations require you to keep data for five years.

Monitoring/Alerting

□ 1. Are you actively monitoring your timing network? What specifically are you monitoring?

We recommend monitoring:

- □ GPS/GNSS signal strength and integrity
- □ Clock health and status
- □ Timing network link health and status
- □ Accuracy of each timing element in the network

□ 2. Is your alerting propagating correctly to the system monitoring level?

□ 3. Do you know what to do if an alert is generated?

Training

□ 1. Do you have a documentation checklist/tracker be able to demonstrate traceability to UTC by documenting the system design, functioning and specifications RTS 25 Article 4?

□ 2. Can you demonstrate reviewing and checking whether the document is up to date and maintained periodically?

□ 3. Are all staff aware of and familiar with the limitations of the underlying technology? Do they understand the circumstances when the underlying technology might be unreliable?

- □ For GPS or other GNSS references, users should be aware of the relevant risks associated with solar flares, interference, jamming or multipath reflections, and making sure the receiver is correctly locked to the signal. There should be training to provide the appropriate steps to ensure that these risks are minimized.
- □ Do you have a separate general awareness document covering these considerations?
- □ Regulations require that operational staff be trained to understand divergence logs, generate reports, and recognize and monitor drift. Is this training in place?
- □ Do you have a diagnostic health check type document, including some scenario-based workflow orientated sanity checks, to mitigate against unnecessary incident management? The regulations mention this as a best practice.

□ 4. Can you demonstrate to the regulator that your staff has sufficient skills to demonstrate "proportionality" in monitoring to ensure that the monitoring provides useful alerts, not too many false positives, and ample time to react?

□ 5. Is your staff able to use the appropriate divergence values to monitor alert thresholds to ensure that any failures are reported as quickly as possible? And, can they flag warning and escalations no later than the time when the system becomes noncompliant?

Security/Maintenance

□ 1. Do you have a documented procedure to roll out security updates and version releases to your production network?

□ 2. What checks are implemented before rolling out recommended bug fixes and updates?

Whew ... sounds like a lot, doesn't it? It may seem overwhelming at first, but with some thought and planning achieving compliance with the RTS 25 requirements under MiFID II doesn't have to be difficult. If you are having trouble ensuring your networks are ready, contact Orolia today for expert guidence.

Need a hand? Spectracom, an Orolia brand, can help.
Contact us today for the right timing solutions.

Orolia USA Inc.
1565 Jefferson Road
Suite 460
Rochester, NY 14623
Phone: +1.585.321.5800

Spectracom SAS
Parc Technopolis, Bât. Gamma
3 Avenue du Canada
91974 Les Ulis, Cedex, France
Phone: +33 (0)1.64.53.39.80

Orolia Global Service AB Beijing Representative Office
Room 1509, KUNXUN PLAZA,
No.9 Zhi Chun Road,
Haidian District, Beijing 100191, China
Phone: 0086 10 8231 9601