Five Best Practices for Deploying and Monitoring a virtual Primary Reference Time Clock (vPRTC) Network

Introduction

The virtual Primary Reference Time Clock (vPRTC) is a highly secure and resilient network-based timing architecture that has been developed to meet the expanding needs of modern critical infrastructures including 5G, transportation, data centers, and power utilities.

The resilient architecture alleviates dependency on satellite-based timing sources such as Global Navigation Satellite Systems (GNSS) by placing autonomous time scale grade atomic clocks in enhanced Primary Reference Time Clock (ePRTC) area timing-hub sites at the core of a fiber-based terrestrial timing distribution network. Secure core-timing sites and fiber distribution are 100% in control of the network operator, and immune to potential jamming or spoofing cyber-attacks on satellite-based timing solutions.

Figure 1. Virtual Primary Reference Time Clock Architecture Providing Resilient Timing for Critical Infrastructure Operators

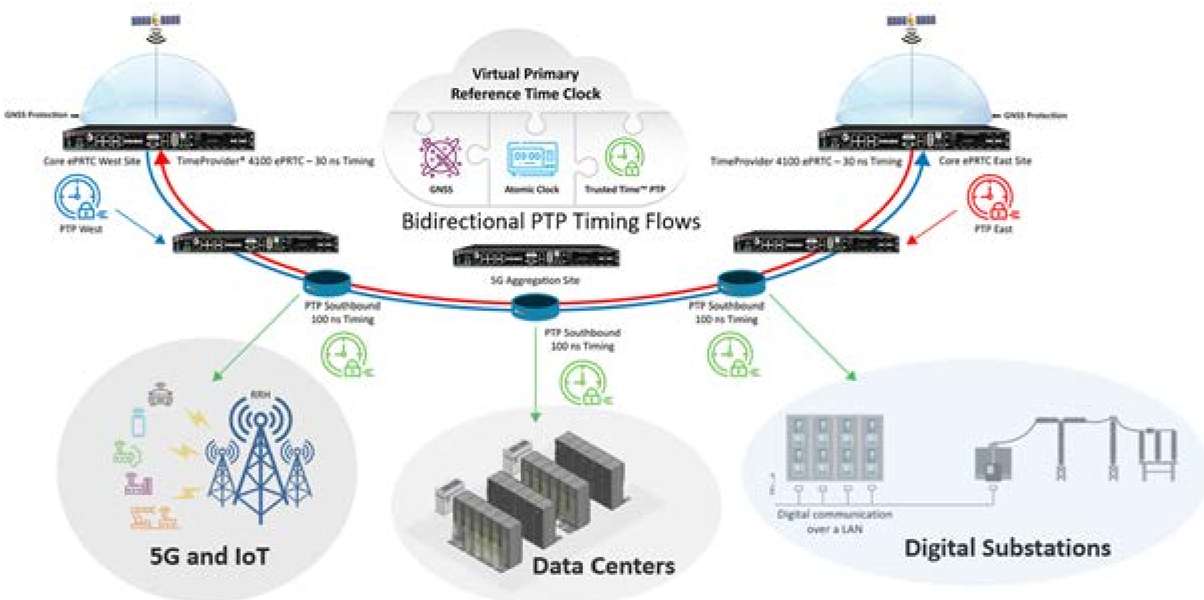


Figure 1 shows how each PTP site works together to provide downstream critical timing. This paper presents five key best-practices derived from millions of cumulative hours of operation of the vPRTC timing architecture across multiple industries. Table 1-1 summarizes best practices for vPRTC architecture.

© 2023 Microchip Technology Inc. and its subsidiaries

Table of Contents

© 2023 Microchip Technology Inc. and its subsidiaries

1. vPRTC Deployment and Monitoring Best Practices

Table 1-1. Summary of vPRTC Best Practices

Best Practice	Summary
1. Establish core ePRTC timing-hub sites	The vPRTC system allows chains of up to 15 hops where each hop can be about 150 km each, which allows for over 2000 km distance between ePRTC sites. The larger the distance between the ePRTC sites, the less chance of jamming and spoofing events affecting them both at the same time.
2. Deploy BlueSky™ GNSS Firewall at ePRTC sites	Install a BlueSky™ GNSS Firewall for anomaly detection and protection. With a small number of sites using GNSS for a very large network, the addition of GNSS firewalls at these sites provides protection to the entire network.
3. Design the vPRTC network for redundancy	Design the vPRTC network so that each TimeProvider® 4100 High Performance Boundary Clock receives 2 high accuracy Universal Coordinate Time (UTC) traceable timing feeds.
4. Optimize path selection between vPRTC nodes	Use the best and appropriate fiber path between the vPRTC nodes to ensure redundant delivery of timing from east and west directions as well as protected southbound PTP distribution to all end-application timing nodes.
5. Monitor vPRTC service assurance	Assure end-to-end vPRTC service with TimePictra® management to verify the integrity of the timing accuracy at each vPRTC node.

1.1 Best Practice 1: Setting Up Your Resilient ePRTC Area Timing Hub Sites

The ePRTC performs two vital functions for any critical infrastructure network, the first being to provide a UTC reference of under 30 nanoseconds (ns) to the network with a stable frequency of 5.7 e-14, and the second being to offer a valid holdover source when GNSS is lost. When planning a network, 30 ns should be used for the error budget calculations; however, the actual performance of the TimeProvider® 4100 ePRTC units is much better, which allows the network a larger margin of error when deployed.

One bonus of the vPRTC timing network is the minimal number of sites that require GNSS. A typical network may only have three to five GNSS sites in total. The antenna installation has the biggest influence on the ePRTC accuracy and stability. The ePRTC can only be accurate to UTC when the antenna cable delay is known. Antenna cable delay varies depending on its material and construction. A typical delay for a cable is 3.9 ns per meter. When the ePRTC is trying to provide an accuracy of under 30 ns, a few meters can contribute error in the cable length and can destroy the hard-won accuracy.

When establishing your ePRTC sites, it's important to remember that there must be a minimum of two sites for network redundancy and protection. The ePRTC locations not only provide the accurate time for the entire networks, they also provide the backup in the event of GNSS jamming, spoofing, or failure. Table 1-2 is an ePRTC components list with descriptions on how to implement best practices.

Table 1-2. ePRTC Component List

ePRTC Components	Description
Calibrated GNSS Antenna Installation	It is vital to ensure that the GNSS antenna is accurately compensated for propagation delay through the cable length with elements such as lightning arresters, amplifiers, or splitters. Consult the TimeProvider® 4100 System User Guide for detailed instructions.
BlueSky™ GNSS Firewall	Recommended option for ePRTC installation to provide GNSS spoofing and jamming detection.
TimeProvider® 4100 PTP Grandmaster Server	When equipped with dual cesium clocks, there are two advantages. First, to protect the output performance of the ePRTC system. Second, dual cesium clocks further increase the performance and holdover ability of the ePRTC.
5071B Cesium Frequency Standard	Provides frequency and stability reference. It's best to have two cesium clocks at each ePRTC site, that way there is a backup to the critical infrastructure that's being established.
TimePictra® Software	Can view synchronization performance with end-to-end network visibility encompassing ePRTC systems at area timing hub locations and sub-tending aggregation and edge nodes.

© 2023 Microchip Technology Inc. and its subsidiaries

With the importance of the ePRTC sites, installing the antenna properly requires careful planning, and any errors can cause the ePRTC to be inaccurate. The antenna location itself must be selected based solely on the ability to reliably receive the GNSS signal. It must be placed so that it has a clear view of as much sky as possible. Any obstructions such as antennas, large metal objects, or buildings limit the performance of the GNSS signal. This strict requirement for a GNSS antenna for any timing location means that it is very expensive, sometimes very difficult to use GNSS for time in an urban environment and further shows one of the huge benefits to bringing time to the city from a distant ePRTC area timing hub site.

When the ePRTC is first installed, it will provide a UTC reference, accurate to 30 ns or better within the first 48 hours. As the ePRTC characterizes the cesium frequency standard, the holdover performance will improve over time up to a maximum of 40 days.

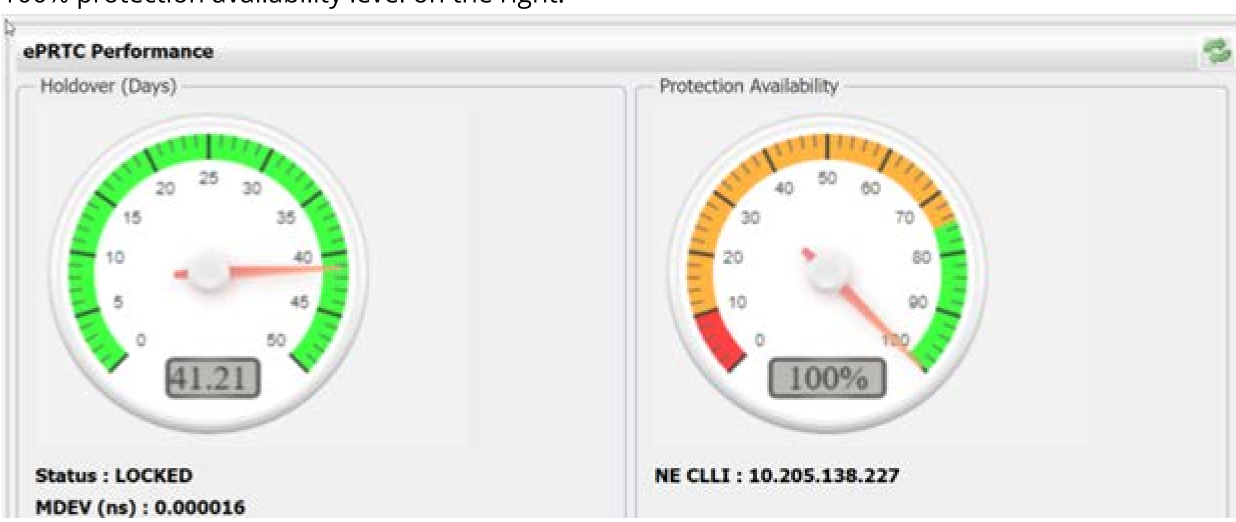
Monitoring your ePRTC locations with the TimePictra® Synchronization Management System is vital to have a high level of confidence in your network, to know the event of a sustained GNSS outage, and that the network will continue to operate.

The ePRTC system includes sophisticated artificial intelligence algorithms to predict the level of performance based on measured stability and stabilization time. Figure 1-1 shows the holdover in days and protection availability monitoring graphs. The holdover meter provides a view of the number of days that the ePRTC system can maintain 100 ns traceability to UTC if the GNSS signal is lost. The protection availability meter shows that the system is fully stabilized and able to meet the ePRTC specification for holdover. The ePRTC standard specifies that the system must be able to hold 100 ns for 14 days after the required stabilization period. The system will provide 14 days of holdover after 14 days of stabilization and will maintain 100 ns holdover for 40 days after a 40-day stabilization period.

GNSS outages tend to be quite short, but at times they can last for several days. The protection availability gauge shows the percentage of holdover availability which is vital to know exactly how severely some GNSS outages have affected the network reserve. Figure 1-1 shows ePRTC holdover performance monitoring from the TimePictra Synchronization Management.

Figure 1-1. ePRTC Holdover Performance Monitoring from the TimePictra Synchronization Management System

The system is ready for 4.21 days of holdover protection to ±100 ns drift from UTC on the left, and 100% protection availability level on the right.



1.2 Best Practice 2: BlueSky™ GNSS Firewall Anomaly Detection and Protection

The ePRTC site uses clocks that are calibrated with UTC traceable timing and GNSS as the timing reference. However, these clocks run autonomously from the calibrated cesium frequency standard. Threats in the form of GNSS spoofing or jamming attacks are continuously monitored using

© 2023 Microchip Technology Inc. and its subsidiaries

advanced firewall technologies to assure only valid signals from the sky are passed to the central clock. The central clocking system employs industry proven cesium atomic frequency standards to establish 30 ns guaranteed accuracy traceable to UTC. If GNSS is detected to be not valid, the vPRTC source maintains 100 ns traceability to UTC for a minimum of 14 days. There are two options for how to deploy the BlueSky™ GNSS Firewall for GNSS anomaly detection and protection.

Option 1: Deploy the BlueSky™ GNSS Firewall in-line between the antenna and the TimeProvider® 4100 system.

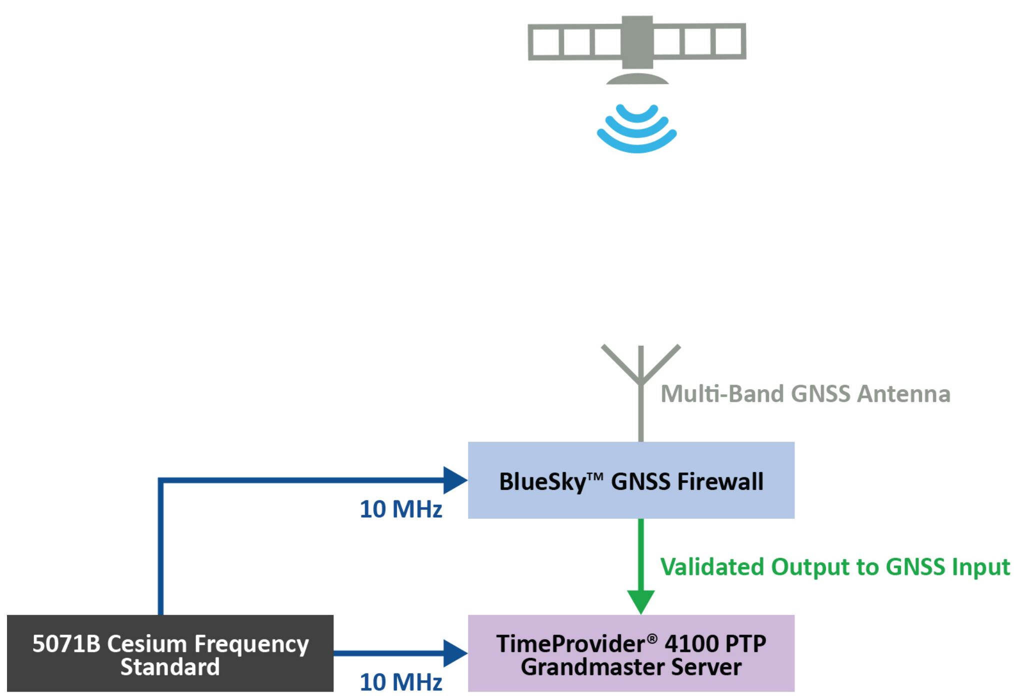
1. Connect the GNSS antenna to the BlueSky GNSS Firewall.
2. Connect the validated output from the BlueSky GNSS Firewall to the GNSS input on the TimeProvider 4100 ePRTC system.
3. Configure anomaly detection thresholds on the BlueSky GNSS Firewall.
4. If anomalies are detected and thresholds are exceeded, the firewall will generate alarms, and disable the validated output so that the ePRTC system will immediately enter holdover protection.

Option 2: Deploy the BlueSky™ *GNSS Firewall as a separate monitoring system.*

1. Connect the BlueSky GNSS Firewall to a separate GNSS antenna or to a splitter on the main antenna line.
2. Configure anomaly detection thresholds on the BlueSky GNSS Firewall.
3. If anomalies are detected and thresholds are exceeded, the firewall will generate alarms to notify the system operations center to analyze and to take appropriate actions.

Figure 1-2 shows the deployment case where the BlueSky GNSS Firewall is installed in-line between the GNSS antenna and the TimeProvider 4100 ePRTC GNSS input. The validated output of the BlueSky GNSS firewall can be configured to cut off the GNSS output to the ePRTC system if GNSS anomaly thresholds are exceeded isolating the ePRTC system from potential GNSS spoofing threats.

Figure 1-2. ePRTC Site Set Up with BlueSky GNSS Firewall Protection



© 2023 Microchip Technology Inc. and its subsidiaries

1.3 Best Practice 3: Configuring the TimeProvider® 4100 High Performance Boundary Clocks (HPBC) at Each vPRTC Node

The TimeProvider® 4100 system is a sophisticated network clocking element with the ability to transfer timing with extraordinary levels of precision and can be configured in different operational modes: ePRTC, PRTC-A, PRTC-B, Gateway Clock, and as a HPBC designed for the optical layer. In HPBC mode, it can meet or exceed ITU-T G.8273.2 Class D specifications with a typical error budget of 2 ns per HPBC hop.

When making a comparison between traditional boundary clocks and the vPRTC HPBCs, traditional boundary clocks are unidirectional, have a single clock domain, and a very basic de-jitter function. They are designed to have a single input and no ability to make measurements between multiple references. Whereas the HPBC clocking element has multiple PTP input clients and dual clock domains per port. With full bi-directional functionality, the system accepts PTP input from different directions (“East Site” and “West Site”) simultaneously. HPBCs monitor the incoming clocks and can select the most stable highest quality input. HPBCs also run a global Best Master Clock Algorithm (BMCA) function that enables fast switchover between PTP inputs as necessary. Figure 1-3 shows the West Site, East Site, and HPBC Hop configuration. Table 1-3 explains factors that contribute to configuring the TimeProvider 4100 HPBC at each vPRTC node.

Figure 1-3. vPRTC with West Site, East Site, and HPBC Hop Configuration

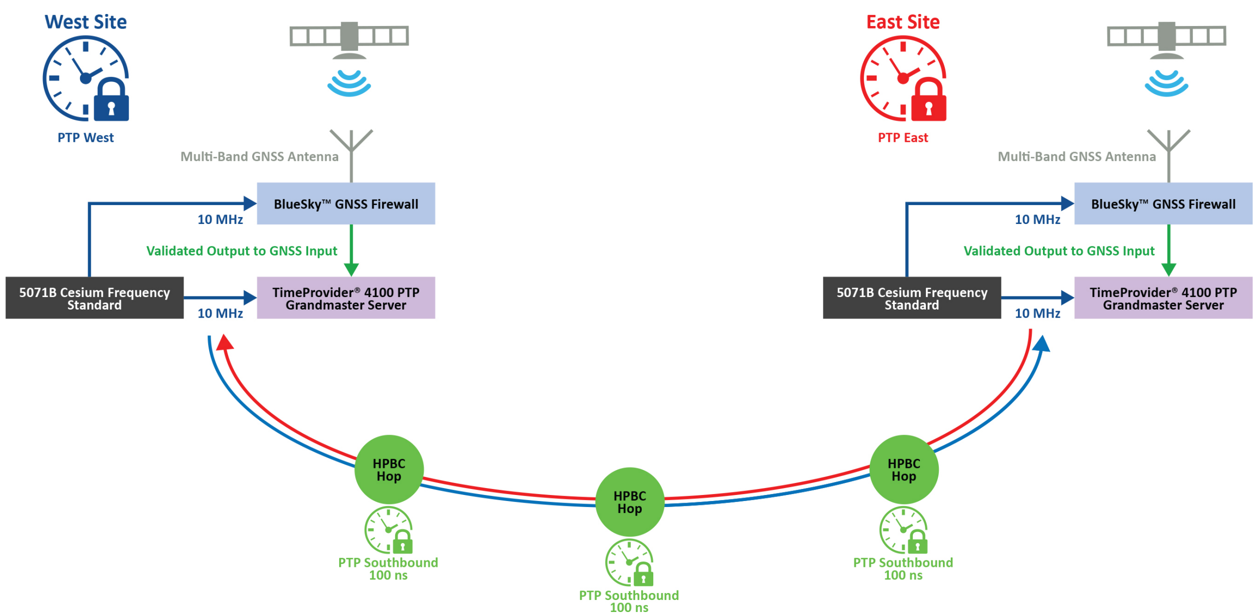


Table 1-3. Best Practices for Configuring the TimeProvider® 4100 HPBC at Each vPRTC Node

Factor	Recommended Best Practice
Hop count	Up to 15 HPBC hops. Max error contribution for planning (15 hops x 2 ns per hop = ±30 ns) max.
PTP Profile	G-8275.1 Full on path support.
Primary ePRTC Site Protection	Designate one ePRTC site to be the “primary” and the other to be the “secondary” site. • All HPBC clocks follow the same ePRTC site as “primary”. • If the “primary” ePRTC signals an issue, all HPBC clocks in the chain will automatically switch to the “secondary” ePRTC site. • If there is a fiber cut along the chain, all HPBC clocks east of the cut will lock to the east ePRTC site and similar for the west side of the cut.
Continuous monitoring	The HPBC continuously measures and compares the offset from both the east and west ePRTC sites to assure PRTC stability of the entire chain, and to enable easy diagnostics of any timing issues along the chain in either direction.

© 2023 Microchip Technology Inc. and its subsidiaries

...........continued	
Factor	**Recommended Best Practice**
TimePictra® Synchronization Management	It is recommended to monitor and manage all TimeProvider® 4100 HPBC clocks in the chain using the TimePictra® management system.

The TimePictra® synchronization management system provides concise monitoring screens to instantly detect and alert the operator to any alarm conditions. Customizable monitoring dashboard screens provide alarm status and a visual mapping of the HPBC chain with all links east and west showing lock and performance status conditions.

1.4 Best Practice 4: Redundant Fiber Interconnect Network Considerations

The optical transmission network for the vPRTC architecture is broken into two sections.

1. The core fiber interconnect for the connection between the ePRTC area timing hub sites and the east to west chain of TimeProvider 4100 HPBC clocks.
2. The southbound PTP distribution network from the individual TimeProvider HPBC clocks down to the end PTP client clocks in the operator's network.

There are many benefits to using dedicated timing paths with the vPRTC network. Not only do timing paths bring deterministic timing performance to the single-ns level, but also to the total separation of the traffic and the timing networks. This separation means any planned or unplanned updates or changes to the traffic network, such as firmware, line cards, or adding new equipment from existing or new vendor, cannot have any effect on the timing network.

The fiber interconnect for a resilient vPRTC east/west network using a single path design is made with one of the following three options:

1. DWDM using the Optical Timing Channel (OTC) or Optical Supervisory Channel (OSC)
   a. The OTCs often use SFPs at Fast Ethernet speed, which does allow for longer distances. It should be considered that Fast Ethernet timing channels prohibit the use of protocols like WhiteRabbit, which is why vPRTC is so widely deployed for timing over a wide area.
   b. OTCs will typically use an external filter, which means that the 2 lambdas used are very close to each other and in most cases reduce the static asymmetry to almost nothing.
2. Single fiber with bidirectional SFPs
   a. Commonly used for medium distances (approximately 100 km).
   b. Bidirectional SFPs have the advantage of using a single fiber, which saves money, but also means there are no problems with mismatched fiber pairs.
   c. The one drawback is to know the length of the fiber, so that the correct offset from the chromatic dispersion can be calculated.
3. Fiber pairs (least common)
   a. Using a pair of fibers can lead to issues; if the pair is not matched in length, any significant mismatch will create an offset.

The vPRTC timing architecture is very flexible and supports either the Optical Timing Channel (OTC) approach with a dedicated lambda, or the Optical Supervisory Channel (OSC) approach where timing is flowing with the management traffic. This flexibility allows the vPRTC architecture to operate with a wide range of optical vendor equipment and operator architectural timing transport preferences.

The southbound PTP timing distribution from the TimeProvider® 4100 HPBC sites is very flexible to suit the operator's end application PTP timing needs and transport options. The key benefit of the vPRTC architecture is that the TimeProvider® 4100 HPBC clock nodes all meet the PRTC-A 100 ns accuracy to UTC without depending on a local GNSS connection. The vPRTC is a much more resilient timing architecture with redundant paths back to operator-controlled area timing hub sites

© 2023 Microchip Technology Inc. and its subsidiaries

with cesium atomic frequency standard protected ePRTC systems. Table 1-4 shows best practices for southbound PTP distribution from the resilient TimeProvider® 4100 HPBC nodes.

Table 1-4. Best Practices for Southbound PTP Distribution from the Resilient TimeProvider® 4100 HPBC Nodes

Factor	Best Practice
PTP Profile	Configure the southbound PTP profile to support your end requirement needs (power, communications, and so on).
Redundancy	Assure that all PTP client clocks have access to a primary TimeProvider® 4100 Grandmaster as well as an alternate TimeProvider 4100 GrandMaster.
BMCA Switching	Configure PTP client devices to utilize the BMCA algorithm option for the PTP profile used to facilitate resilient switching if required.

1.5 Best Practice 5: End to End vPRTC Service Assurance and Monitoring with TimePictra®

The vPRTC architecture has several unique features that are mandatory to deliver deterministic and accurate timing within a network.

These features are:

- Use of PTP between nodes, so that any path can be used, at whatever speed is appropriate.
- Use of PTP between nodes, so that an East and West timing solution can be used on the same path, while maintaining the complete independence of these timing directions.
- Comparison measurement between the East and West timing directions at every node along the sync chain.
- The vPRTC network not only delivers precise time, but the vPRTC network is self-monitoring and self-diagnosing.

The combination of these features means that TimePictra® can monitor every timing chain in a customer's network and confirm that each HPBC is aligned with both ePRTC nodes.

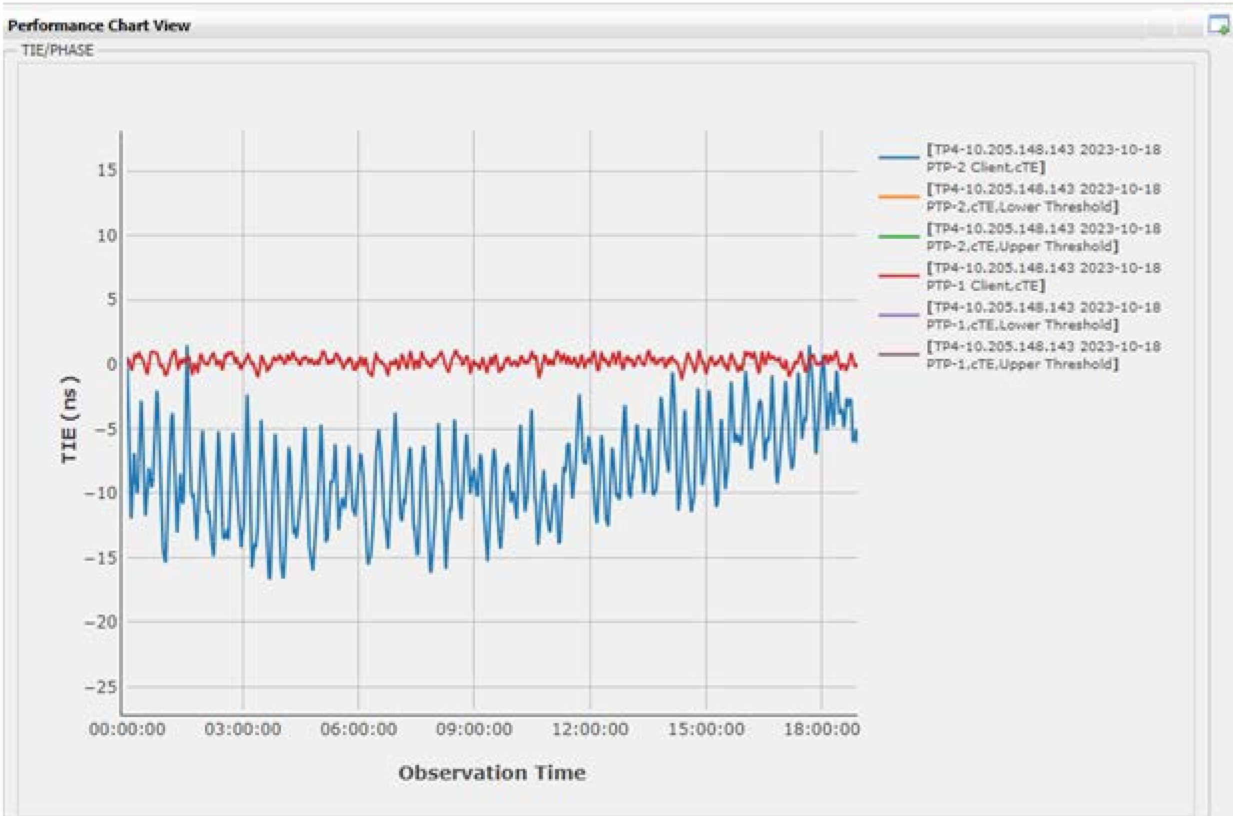
When a vPRTC chain is established, the measurements taken by TimePictra® will show 3 components:

- The difference between the UTC sources at each end of the vPRTC timing chain.
- Static asymmetries that exist along the vPRTC chain.
- Sudden changes in static asymmetries that show there has been a change in fiber or configuration.

In some networks, the customer may only use one ePRTC, choosing to use a standard PRTC-B for the other reference. Figure 1-4 shows East timing coming from the PRTC-B. The blue line shows the noise associated with GNSS over the 18 hours of the graph. The differences show that there is 5 ns difference between the East and West, which is within the limits required.

© 2023 Microchip Technology Inc. and its subsidiaries

Figure 1-4. East West Between ePRTC and PRTC-B

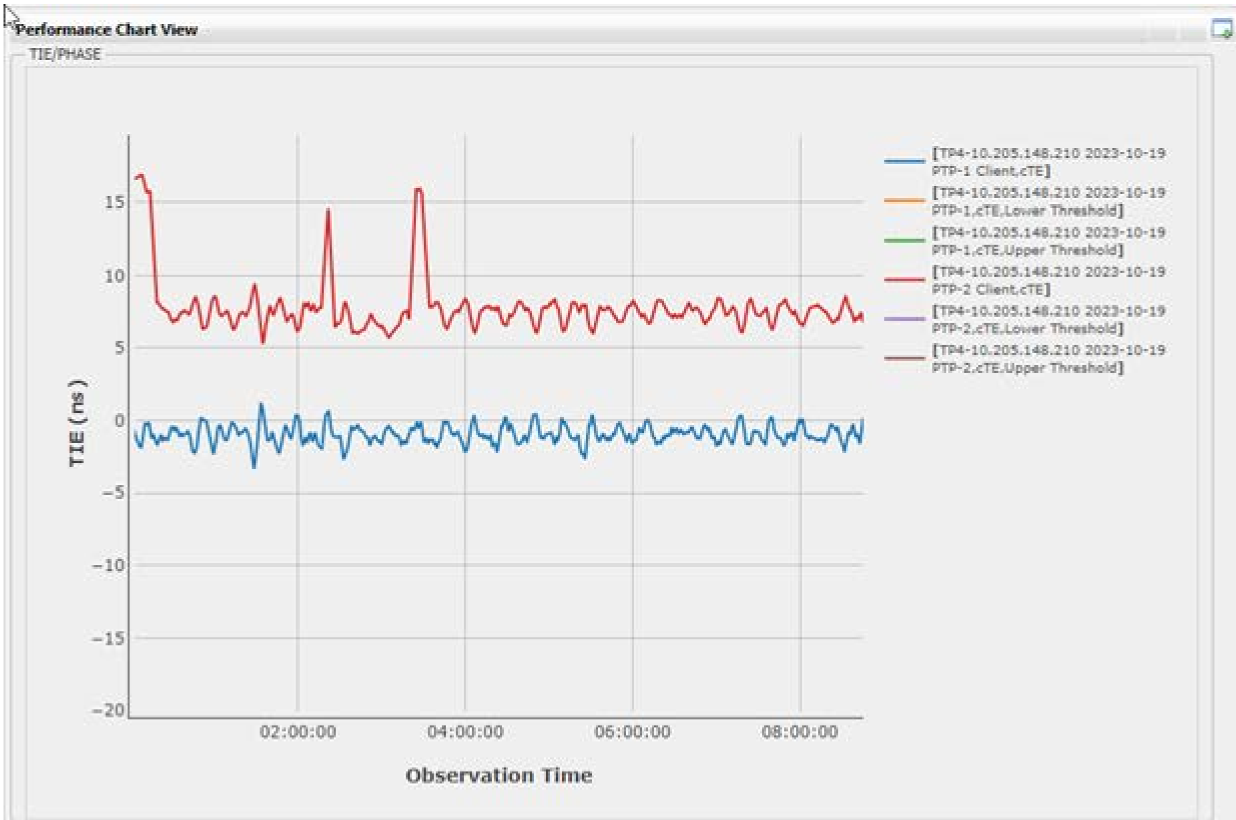


Now compare the graph shown in Figure 1-5, where both East and West come from ePRTC units. A similar offset is seen between East and West; however, there is a large reduction in the noise that comes from GNSS. TimePictra® will raise alarms if the East and the West diverge by any value from 1 ns to 5000 ns. If strict planning rules needed to be followed, the thresholds for the separation of East and West would be set to 60 ns (2×30 ns), however, a more realistic number would be to set the thresholds to ±20 ns.

The second important metrics to monitor with TimePictra® is the ePRTC availability and holdover available value as shown above in Figure 1-1. These two metrics give the network operations team even more confidence that not only is the network delivering the correct time, but in the event of an outage, the network will continue to run for at least 30 days.

© 2023 Microchip Technology Inc. and its subsidiaries

Figure 1-5. East Site and West Site Between Two Different ePRTC



© 2023 Microchip Technology Inc. and its subsidiaries

2. Conclusion

The virtual Primary Reference Timing Clock is a new concept for a highly secure and protected network-based timing architecture developed to meet the expanding needs of modern critical infrastructures. Please contact your Microchip representative to learn more about how our solutions enable operators to build a vPRTC network delivering ultra-high precision timing services with unmatched stability, security, and reliability.

For more information on vPRTC, see the Microchip web at Virtual Primary Reference Time Clock.

© 2023 Microchip Technology Inc. and its subsidiaries

3. Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the most current publication.

Revision	Date	Description
A	11/2023	Initial Revision

© 2023 Microchip Technology Inc. and its subsidiaries

Microchip Information

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable". Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure

© 2023 Microchip Technology Inc. and its subsidiaries

that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet-Wire, SmartFusion, SyncWorld, TimeCesium, TimeHub, TimePictra, TimeProvider, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, Clockstudio, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, EyeOpen, GridTime, IdealBridge, IGaT, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, IntelliMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, MarginLink, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, mSiC, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, Power MOS IV, Power MOS 7, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, Trusted Time, TSHARC, Turing, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, and Symmcom are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

© 2023 Microchip Technology Inc. and its subsidiaries

All other trademarks mentioned herein are property of their respective companies.

© 2023, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 978-1-6683-3409-6

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4485-5910 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-72400 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-72884388 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820

© 2023 Microchip Technology Inc. and its subsidiaries