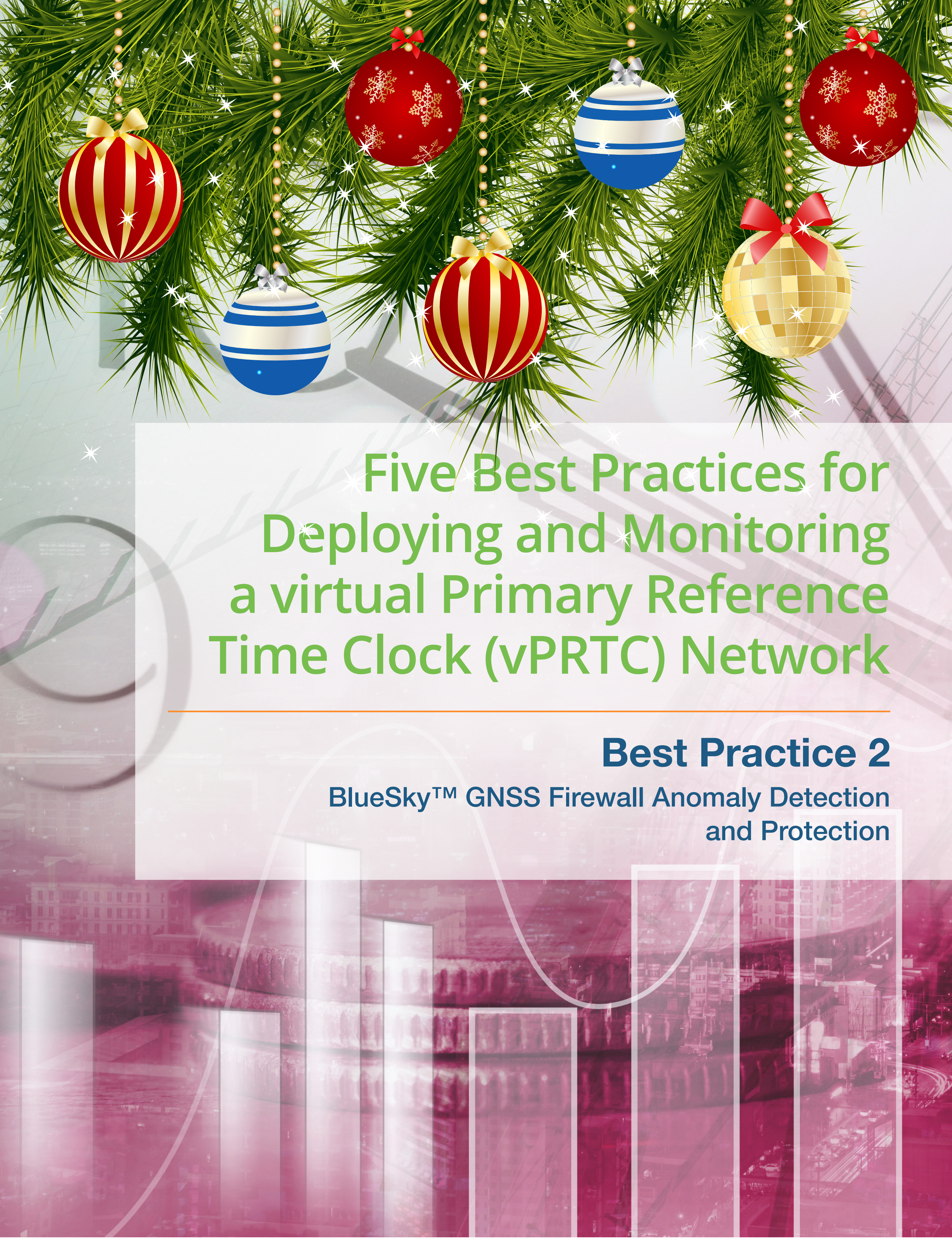


Five Best Practices for Deploying and Monitoring a virtual Primary Reference Time Clock (vPRTC) Network

Best Practice 2

BlueSky™ GNSS Firewall Anomaly Detection and Protection

www.microchip.com

MICROCHIP

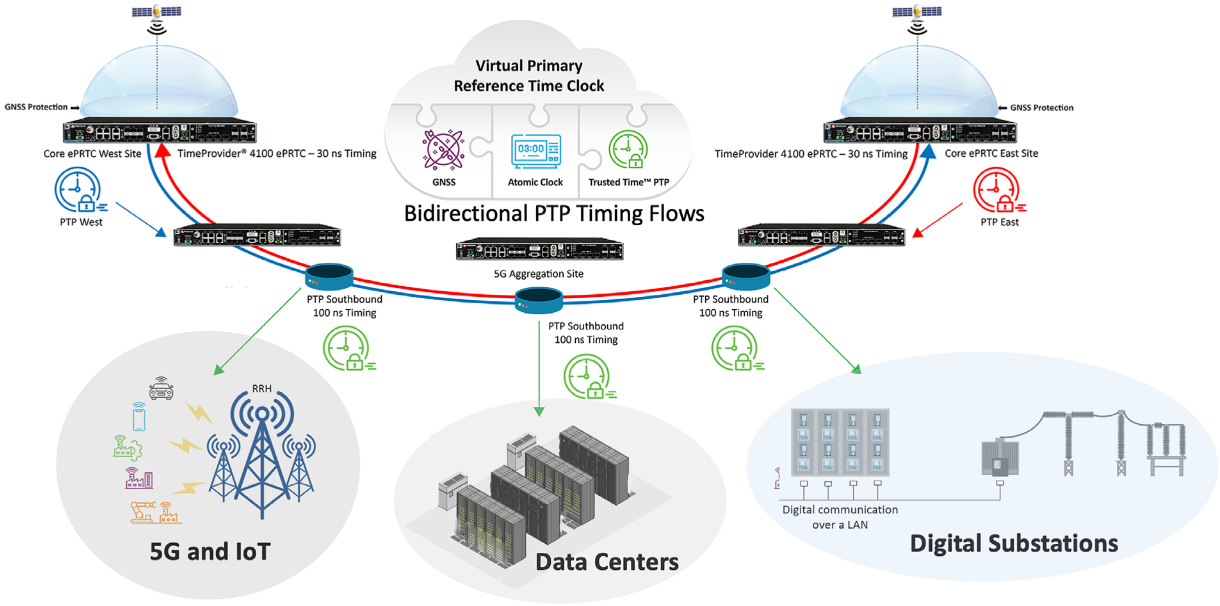
Five Best Practices for Deploying and Monitoring a virtual Primary Reference Time Clock (vPRTC) Network

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



This paper presents the second, out of five, key best-practices derived from millions of cumulative hours of operation of the vPRTC timing architecture accross multiple industries.

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 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.

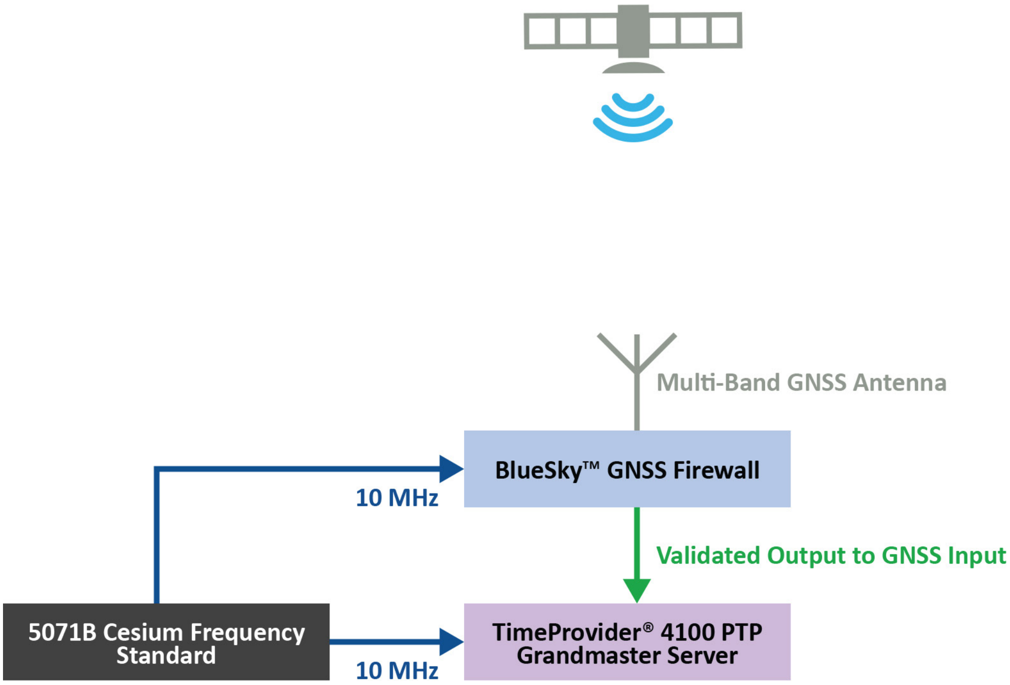

Multi-Band GNSS Antenna
BlueSky™ GNSS Firewall
10 MHz
Validated Output to GNSS Input
5071B Cesium Frequency Standard
10 MHz
TimeProvider® 4100 PTP Grandmaster Server

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

Summary

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.