

Keeping the Power Flowing During GNSS

It is essential to achieve accurate timekeeping and clock synchronization across equipment and systems for the reliable operation of modern power grids. Today, time signals from constellations of Global Navigation System Satellites (GNSSs) enable power distribution grids to operate safely and efficiently. GNSS time signals offer an extremely straightforward and easy-to-implement method of provisioning accurate time synchronization across all parts of a power grid. However, with its increasing popularity, the GNSS network is subject to jamming and spoofing attacks, as national states, unintentional disruptors and malicious actors seek to interrupt the satellites' time and positioning capabilities.



Loss of clock accuracy and precise time desynchronization across the power grid impacts phasor measurement, fault detection, protection coordination and billing errors.

Clock and Time Synchronization Key

Modern power distribution grids are undergoing significant transformation due to the integration of smart grid technologies, distributed energy resources and real-time data

Keeping the Power Flowing During GNSS

analytics. Central to the functionality of these systems is the need for precise and synchronized timing. Devices such as Phasor Measurement Units (PMUs), protection relays and smart meters rely on synchronized clocks to make coordinated, real-time decisions. Loss of clock accuracy and synchronization, whether from technical malfunction, GNSS signal degradation or cyber intrusion, poses a serious threat to the reliable and secure operation of the grid.

Impact of Loss of Clock Accuracy and Time Synchronization

Signals from GNSS constellations are extremely easy to interrupt. Over the past decade, there has been a significant rise in GNSS jamming and spoofing activity by malicious actors and rogue nation-states. Interruptions include taxi and delivery drivers using cheap GNSS jammers to deviate from a corporate, pre-planned route and government-led jamming that mitigates the risk of drone attacks during official visits.

Consequently, power grids are at risk of significant interruption due to the loss of reliable clock systems. The severity of disruption varies, but includes:

Inaccuracy of Phasor Management Unit (PMU) timestamps: PMUs rely on GNSS time signals to synchronize the measurement of voltage and current across the power distribution grid.

Determining accurate phase angle measurement is essential for real-time monitoring, with even a 1 μ s error resulting in a phase angle miscalculation of 0.022 degrees at 60 Hz.

Event and fault logging: Maintaining accurate time for the time-stamped logs across the network, from substations to control centers, is paramount to analyze root cause and event correlation during and after grid problems.

Coordination of protection relays: Loss of time synchronization can result in incorrect operation or failure to trip of protection relays, which compromises grid safety, causes equipment damage and impacts customer satisfaction.

Keeping the Power Flowing During GNSS

Demand response and load balancing: Unsynchronized clocks can result in a poor reaction to load oscillation artifacts, which can result in voltage fluctuations and, potentially, grid instability. This also introduces billing errors and other data integrity issues and undermines customer trust. Also, grid instability has long been associated as a major contributing factor behind cascading power grid failures.

Mitigating the Risks

With the increasing jamming and spoofing of GNSS signals, the chances of a power grid losing its critical time-synchronization capability multiply daily. The disruption of utility services and power grids is now a matter of national security, mandating access to a more reliable and robust time source than GNSS.

To mitigate the impacts of the loss of clock synchronization highlighted above, two viable technologies are available from Microchip that provide two time source technologies to reduce the loss of GNSS signals. Both comply with the internationally recognized Recommendation ITU-T G.8272.1, delivering a time accuracy of ± 30 nanoseconds. The enhanced Primary Reference Time Clock (ePRTC) comprises a highly accurate and reliable physical hardware clock, such as a cesium-based atomic clock with a GNSS receiver. The atomic clock provides a holdover trusted time source in case the satellite signal is lost. ePRTC is aimed at on-premise locations such as utility power grid substations.

An alternative to ePRTC is a virtual PRTC (vPRTC). This approach provides a virtual clock arrangement based on an ePRTC but is capable of being distributed across large networks and remote sites. Implementing an architecture of one or two ePRTCs and distributing synchronization via vPRTC offers a cost-effective and practical approach to synchronization.

However, with the recent rise in GNSS vulnerabilities, such as jamming and spoofing globally, Microchip recommends removing the risks associated with GNSS and implementing a robust and resilient time distribution network.

Keeping the Power Flowing During GNSS

A typical fiber-connected time network for power grids comprises an ePRTC and vPRTC arrangement, with the ePRTC located within a major urban distribution area communicating with vPRTC units in the administrative offices within individual substations. Accurate time signals from the vPRTC are then sent to the electrical switch gear via the highly accurate IEEE 1588 standard for Precision Time Protocol (PTP).