Mitigating GPS Vulnerabilities, Enhancing GPS Security, and Implementing Alternative Timing Solutions.

Rob Jodrie Syncworks

September 18th 9:00-10:00 AM

Utilities Technology Council™

REGION 5 MEETING
SEPTEMBER 16 - 18, 2024
Minneapolis, MN

Discussion Points

- The reliable operation of our Nation's critical infrastructure is heavily dependent on GPS.
  - Industries including finance, communication, power utilities, and transportation, to mention a few.
- Because GPS is so widely deployed, local or global GPS outages of an extended duration could have significant economic impact on our Nation.
- GPS satellites orbit the earth at an altitude of over 12,000 miles. By the time the signal arrives at the antenna mounted on the roofs of our buildings, it is very low power and very easy to jam.
- The result is a service that represents a single point of failure to our timing networks.
- Fortunately, we can increase both the resiliency and security of our timing networks due to GPS outages and impairments.
- This presentation will provide a synchronization overview and delve into some of the options available to address these concerns.
- Solutions such as GPS firewalls, creating area timing hubs, and deploying GPS backup using packet timing will all be discussed.

Terminology and Specifications

- **Primary Reference Time Clock**
  - PRTC performance within 100 ns of UTC when connected to GPS
  - Switch to holdover Rubidium Oscillator with GPS LOS
- **Enhanced Primary Reference Time Clock**
  - ePRTC performance within 30 ns of UTC when connected to GPS
  - Performance within 100ns for 40-days with GPS LOS
    - G.811.1 Cesium Clock input to Time Server
- **Virtual Primary Reference Time Clock**
  - Performance within 100 ns of UTC without GPS connectivity
  - Optical ENET or DWDM Transport
  - PTP from ePRTC nodes provide Synchronization
- **Enhanced Primary Reference Clock Microchip TC-4500 Cesium**
  - The long-term accuracy of the ePRC should be maintained at 1 part in 10 to 12th
  - Recommendation ITU-T G.811.1
  - Frequency ONLY

Addressing GNSS Vulnerabilities for Critical Infrastructures

- Local-area GNSS Outages
  - Affecting single locations
    - Time Servers with Rubidium oscillators can hold time within 200 ns for 1-day.
  - Today's GNSS timing receivers offer some protection from jamming/spoofing
    - Multi-constellation (example: GPS, BeiDou, Galileo, and GLONASS)
    - Multi-band reception (L1, L2, and L5 RF signals)
    - Firewalls
- Wide-area GNSS Outages
  - Affecting multiple locations simultaneously
  - This is the more critical/concerning scenario
    - Wide-area outages in GNSS-denied environments for an extended period requires more resilient, robust solutions.

Alternative Timing Solutions for GNSS Backup

- Low Earth Orbit (LEO) Satellites
  - GPS alternative or backup
  - Indoor reception
  - Subscription based service
  - Currently available (accuracy close to GPS timing services)
- eLoran (enhanced Long-Range Navigation)
  - GPS alternative or backup
  - Indoor reception
  - Land based RF transmitters
  - Subscription based service
  - Availability TBD (accuracy close to GPS timing services)

Solutions to GNSS/GPS Denied Environments

- The best way to address GNSS/GPS vulnerabilities is to simply reduce the number of deployed GNSS/GPS timing receivers.
- One way to accomplish this is by using network-based Precision Time Protocol packet timing services.
- In the core of the network, a centralized PTP source clock can be created consisting of at least one GPS timing receiver configured as an Enhanced Primary Reference Clock (ePRTC) and a minimum of one cesium atomic clock.

enhanced Primary Reference Time Clocks (ePRTC)

- ePRTC Node (enhanced Primary Reference Time Clock)
  - Autonomous Time Scale
    - Calibrated via GPS and accuracy maintained with Cesium backup
    - Ability to hold Time within 100ns of UTC for 40-days during GPS outage
    - “Terrestrial” components are TP-4100 or TP-4500, Cesium, Fiber Transport Network
  - Within 30 ns of UTC under normal operating conditions
    - Class A Primary Reference Time Clock within 100 ns UTC
    - Improved Time Error Budget for systems/services

enhanced Primary Reference Time Clocks (ePRTC)

- **ePRTC Algorithms**
  - Learns offset between reference (typically GPS) and cesium atomic clock
  - Once offset is established uses Cesium as the system clock
  - Makes corrections to system outputs based on offset corrections
  - Updates correction data periodically if reference is available
    - Not enhanced holdover operation
  - If reference is lost continues to make corrections based on the ePRTC learning algorithms
    - Enhanced holdover operation

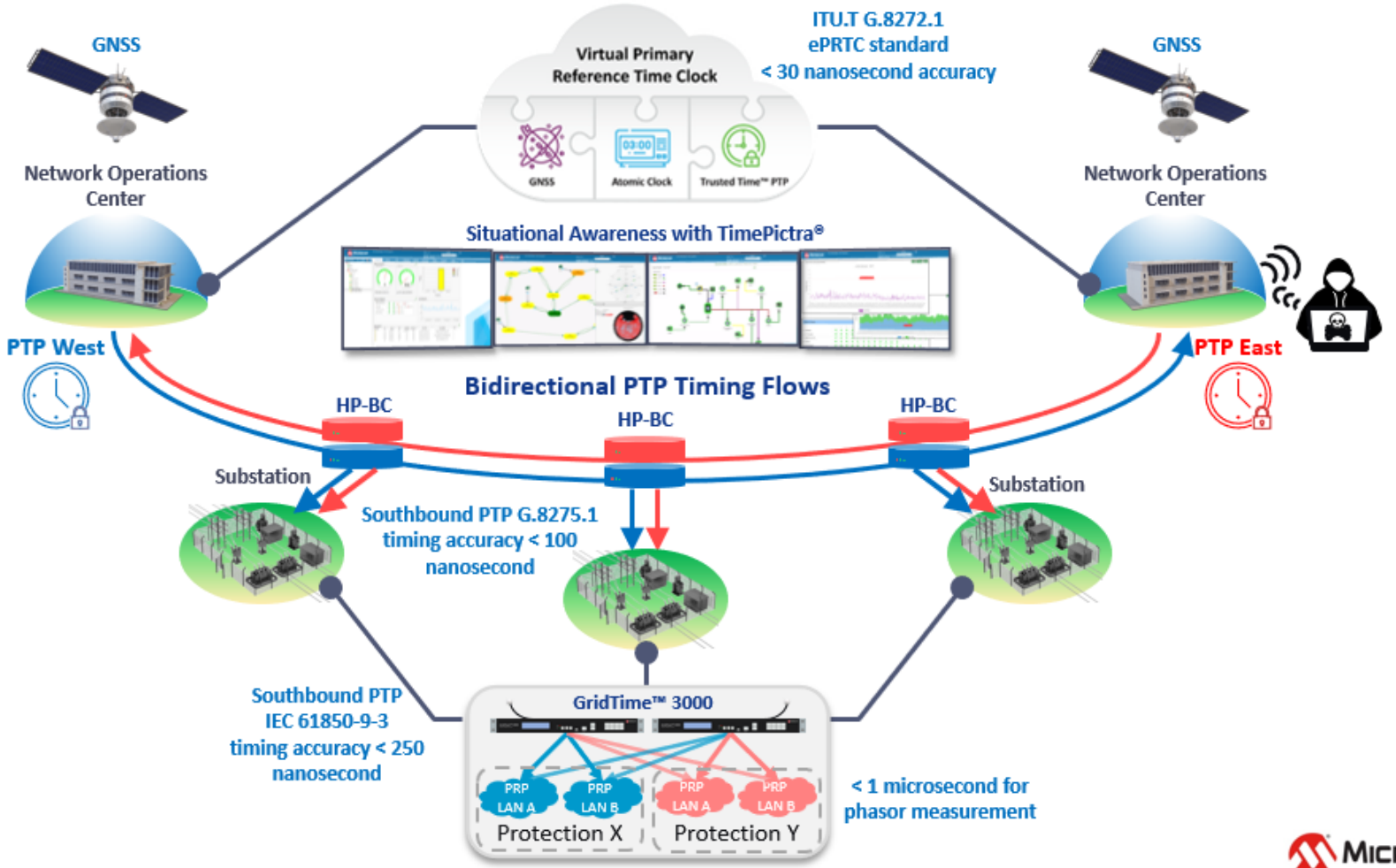
Benefits of ePRTC and vPRTC (GPS Vulnerability and Holdover)

- Executive Order 13905
  - Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services
    - GPS Vulnerability

- ePRTC Node (enhanced Primary Reference Time Clock)
  - Autonomous Time Scale
    - Calibrated via GPS and accuracy maintained with Cesium backup
    - Ability to hold Time within 100ns of UTC for 40-days during GPS outage
    - “Terrestrial” components are TP-4100 or TP-4500, Cesium, Fiber Transport Network
  - Within 30 ns of UTC under normal operating conditions
    - Standard Primary Reference Time Clock within 100 ns UTC
    - Improved Time Error Budget for systems/services.

- vPRTC Node (virtual Primary Reference Time Clock)
  - Redundant Timing from East – West ePRTC Nodes
  - PTP Southbound 100 ns UTC
  - Does NOT require local GPS to meet PRTC 100 ns performance.
  - Local GPS *may* be deployed as backup to PTP

vPRTC for Resilient Synchrophasor Timing



MICROCHIP

Microchip TimeProvider 4500 & TimeProvider 4100

TimeProvider 4100 Server With 10 GbE Module Physical Outline

Microchip TimeProvider 4500 & TimeProvider 4100 Key Features

- ePRTC holdover enhancements (40/40)
  - Learning period of 40 Days holds within 100 ns for 40 days.
- Better than Class D BC standard
  - Decrease in accumulated Time Error in chain of High-Performance BC.
- PTP Unicast Capacity 2000 Clients

  Release 2.4
- 1PPS and NTP as a Time Reference
  - Supports a combination of 1 PPS signal and NTP as a time reference.
  - Compatible with Gateway Clock mode and ePRTC operation mode.

Securing GNSS with Microchip BlueSky Firewall

- Microchip BlueSky Firewall
  - Detect GPS/GNSS anomalies.
    - Jamming and Spoofing.
  - Synthesizer Simulates GPS Signal to Southbound Units.
    - Autonomous Timescale.
      - GPS Calibrates
      - Cesium Maintains Accuracy
    - Hardened GPS Output vs. Validated Output
  - RF Power Monitoring of L1, L2, and L5 Bands

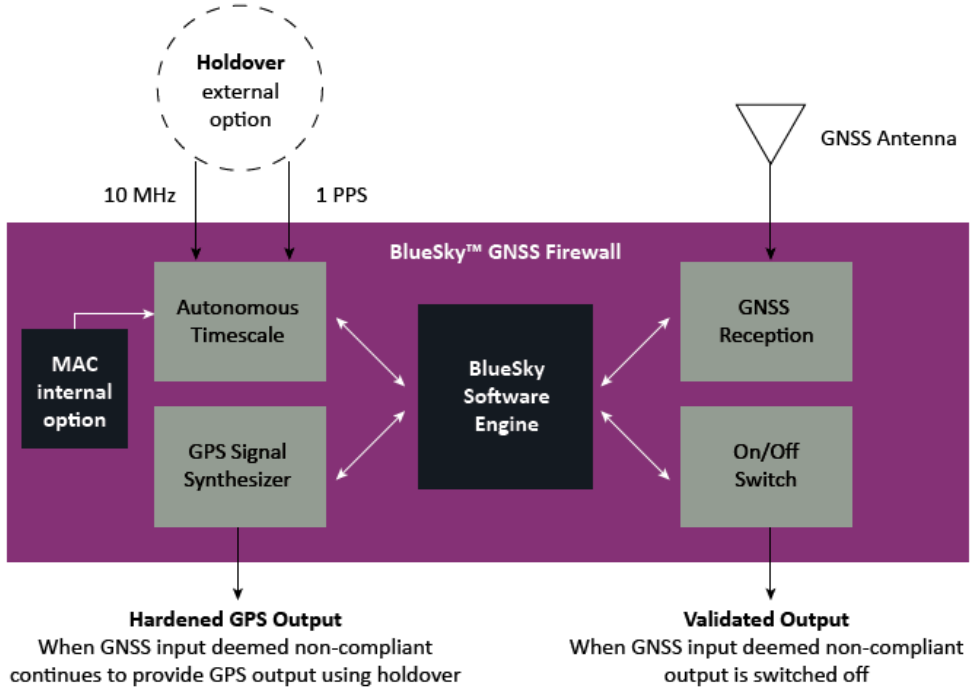
Microchip BlueSky Firewall

BlueSky GNSS Firewall 2200

DC

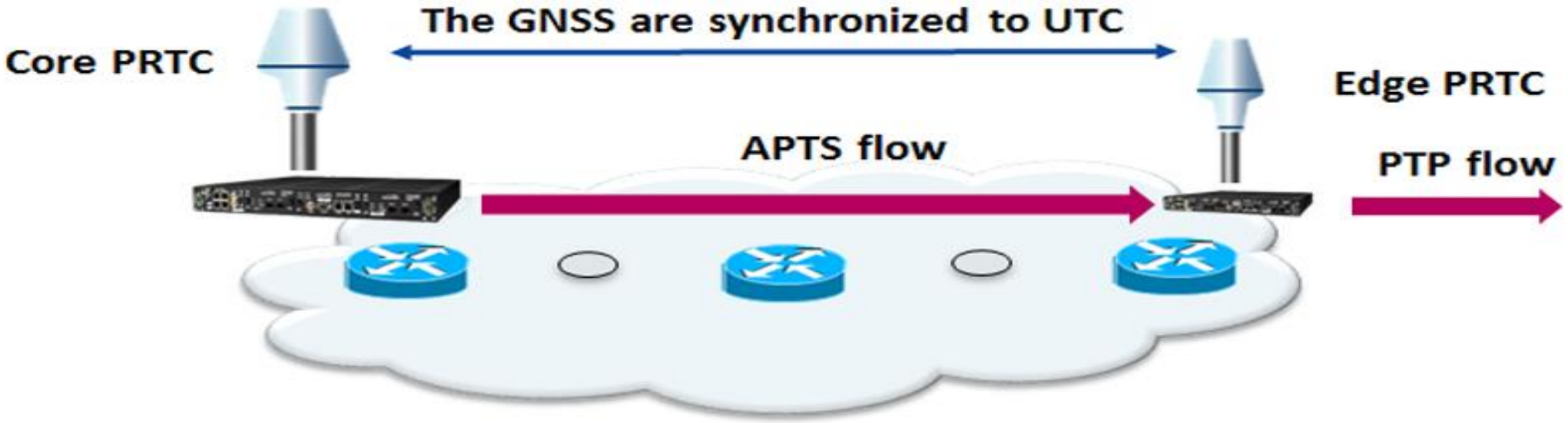
AC

Securing GNSS with Microchip BlueSky Firewall



- Hardened Output
  - If GNSS input is deemed non-compliant, the firewall continues to provide synthesized GPS output.
- Validated Output
  - If GNSS input is deemed non-compliant, the output is squelched.

Assisted Partial Timing Support (APTS) with Automatic Asymmetry Compensation (AAC)



APTS synchronizes the core PRTC with the edge PRTC using PTP.

The PTP flow into the edge PRTC is calibrated using the local GNSS, which is the same time reference (UTC) as the core GNSS.

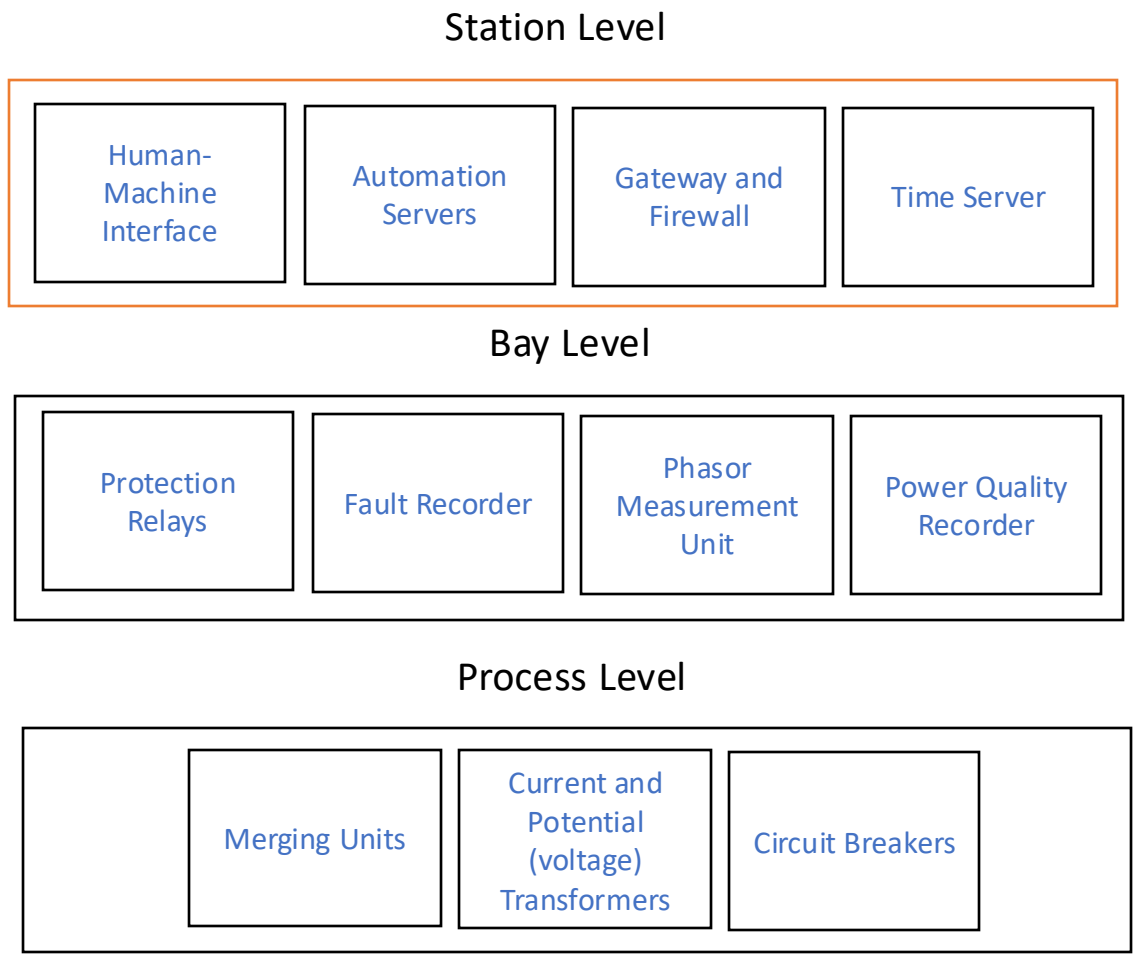
AAC enables the PTP input path to change and remain calibrated for time error—up to 32 different paths can be sustained.

Microchip TimeProvider 4500 & TimeProvider 4100 PTP Output Power Profiles

- IEEE C37.238-2017
  - Power system protection, control, automation, and data communication applications utilizing an Ethernet communications architecture
- IEEE C37.238-2011
  - Superseded by C37.238-2017
- Utility Profile IEC/IEEE 61850-9-3:2016
  - Sync for Intelligent Electronic Devices that control and protect the equipment of the substation and HMI Systems
- Gateway function between communication network and substation clock.
  - PTP translation from telecom profile to power profile.

Transmission Substation

- Most transmission substations are made up of three different levels
  - Station
  - Bay
  - Process
- Station level and functions related to the overall facility and the provision of the communication interface to the grid control center
- Bay level and functions related to a specific part of the facility, i.e., the busbar, a transformer, an incoming bay, an outgoing feeder, etc.
- Process level as the primary equipment including the transformer, instrument transformers/sensors, switchgear, reactive plant, etc.



Synchronization Requirements for Power Utilities

- PMU (Phasor Measurement Units)
  - Synchrophasor Technology
    - High speed measurements of Phase Angle/Voltage/Current
    - 30-60 measurements per second
- Timely Fault Detection
  - Accurate Fault Location via Traveling Wave
- Automatic Protection Switching
- Accurate Timestamp for Event Correlation
  - Data collection without timestamps not useful
  - Determine RCA
- Falling Conductor Protection
  - De-energize powerlines prior to them hitting the ground
    - Personal Safety
    - Fire Prevention

Tekron Classic Product Range

TTM 01-G

A reliable & accurate GNSS clock with sub-microsecond timing that is used to synchronize Intelligent Electronic Devices in the power industry & other industries where precise & reliable timing is required.

PTP Translator

An electronically isolated & compact DIN rail mountable translator that bridges the connection between PTP networks and devices requiring legacy time codes such as IRIG-B

TCG 01-G

The TCG 01-G is a rack-mounted GNSS clock designed for use in substations. The TCG 01-G is remote configurable & outputs all the major time codes, including IRIG-B, NTP, IEEE 1588 v2 (PTP) & supports IEC 61850.

NTS 03-G+

The NTS 03-G+ is a secure, accurate and reliable 3, 4 or 6-port NTP Time Server for synchronizing control and SCADA networks. In addition to electrical isolation and robustness, new features such as remote configuration, enhanced security, support for Ethernet networking, optional PTP and PRP & IEC 61850 support, make the NTS 03-G+ ideal for use in power plants and substation environments.

ITR Isolated Timing Repeater

An electronically isolated & compact DIN rail mountable signal repeater that protects IEDs from signal surges, boosts signal strengths & converts one type of time sync signal to another.

TCG 02-G

The TCG 02-G is a full-rack GNSS Grand Master clock, available as a base unit or with three expansion module options. The TCG 02-G is remote configurable & outputs all the major time codes, including IRIG-B, NTP, IEEE 1588 v2 (PTP).

IRIG-B Analyser

Decode and validate your IRIG-B timing signals with Tekron's IRIG-B Analyzer. With multilevel signal support, the IRIG-B Analyzer enables accurate on-site fault diagnosis through a hand-held, rugged, portable and battery operated form factor.

Product Application Matrix

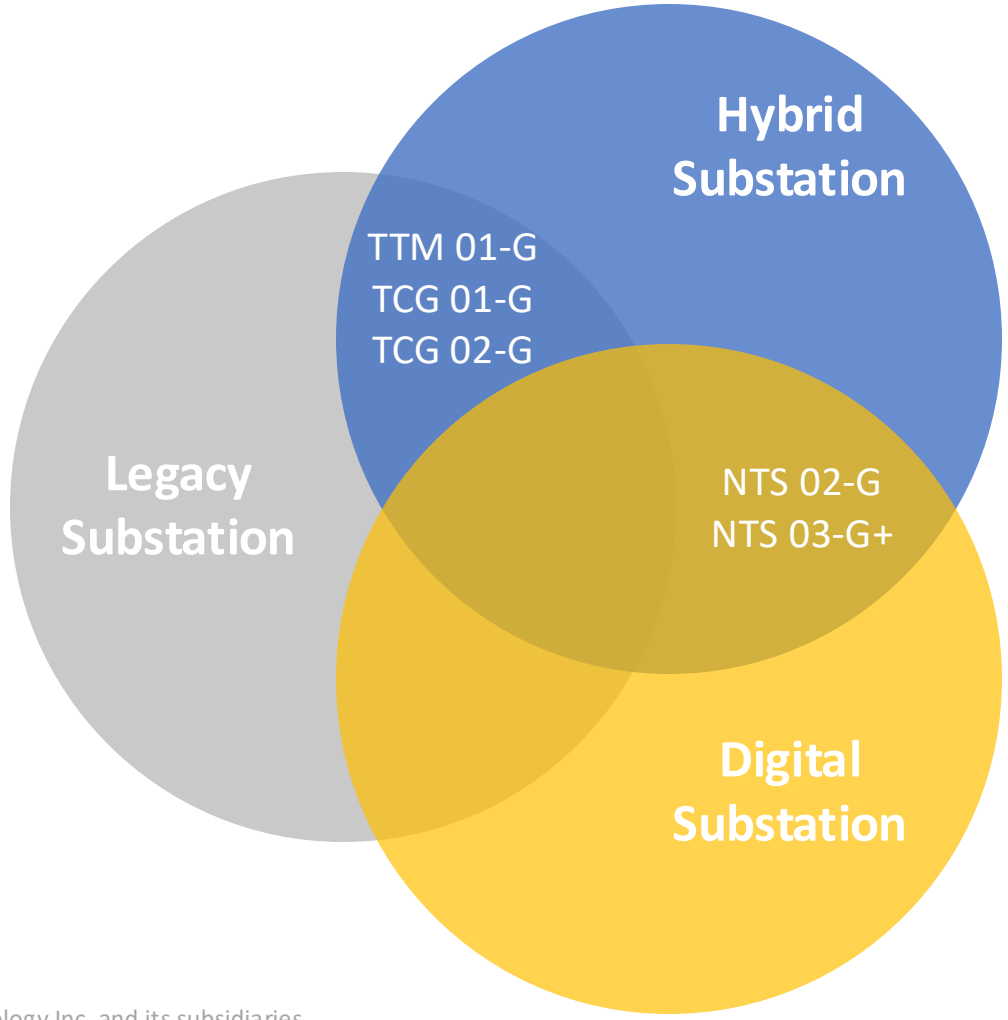
TTM 01-G

TCG 01-G

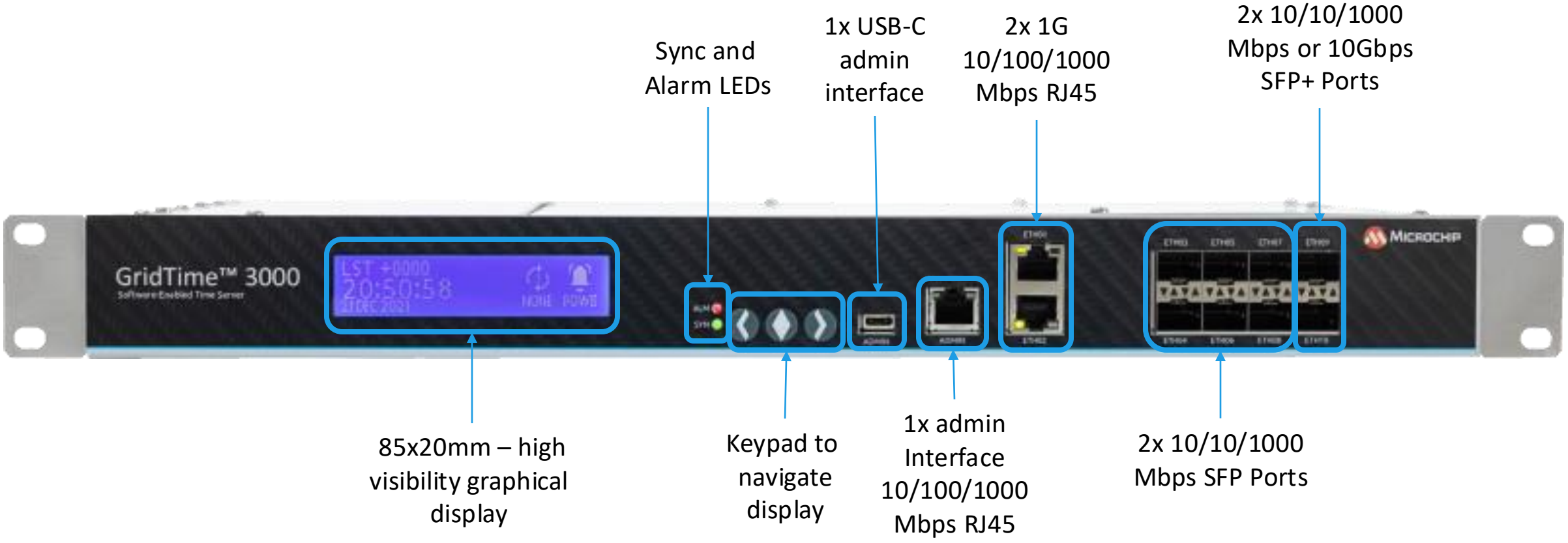
TCG 02-G

NTS 02-G

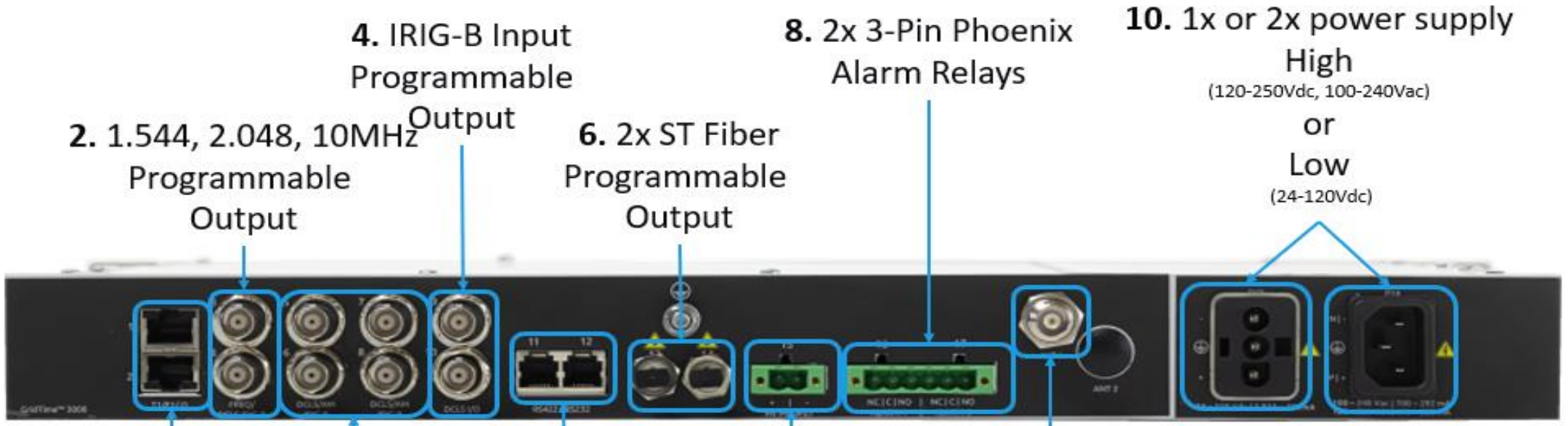
NTS 03-G+



GridTime 3000 GNSS Time Server Front Panel



GridTime 3000 GNSS Time Server Back Panel



Standards Compliance

Power Industry Standards

- **IEC 61850-3:2015**
- IEEE 1613:2009
- **IEC 61000-6-5:2015**
- IEC 62439-3:2016 PRP
- C37.238-2011 Power Profile
- C37.238-2017 Power Profile
- IEC/IEEE 61850-9-3:2016 Power Utility Profile
- NERC CIP

Generic standards

- CE, **UL,** FCC, CSA, RCM
- EN: 55032:2015
- IEC 62368-1-2014
- SNMP v1, v2c, v3
- IEEE 802.1Q – VLAN filtering and tagging
- IEEE 802.3
- IEEE 1588 v2
- ITU-T G.8265.1 Telecom Profile
- ITU-T G.8275.1 Telecom Profile
- NTPv1, v2, v3, v4
- RFC 2030 SNTP

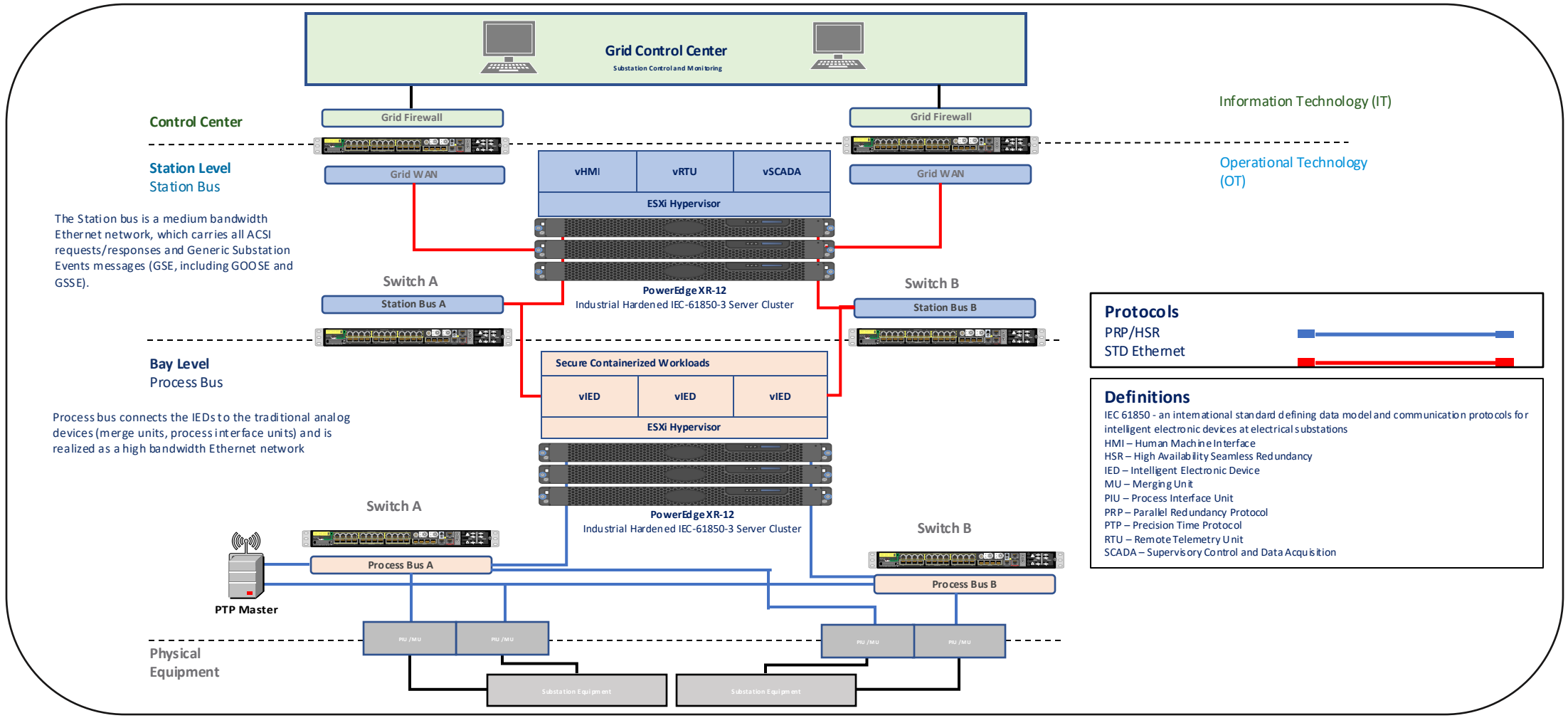
virtual Protection Automation & Control

These member companies have come together to form the vPAC Alliance and have started to fulfill its mission to develop a standards-based, open, interoperable, and secure architecture for substations.

vPAC alliance

ABB
adani Power
ADVANTECH
American Electric Power
arteche
Avangrid
Black & Veatch
CRYSTAL
DELL Technologies
doble
Edison
Endeavour Energy
GE Vernova
Grid to great
intel.
Kalkitech
MOXA
NovaTech Automation
OMICRON
Pacific Gas and Electric Company
PHOENIX CONTACT
POWERGRID
QUANTA TECHNOLOGY
Schneider Electric
Red Hat
SIEMENS energy
SKP
TESCO Automation
vmware by Broadcom
WELOTEC

vPAC Substation



Thank You

Rob Jodrie
rjodrie@syncworks.com

Joe Parrilli
joe.parrilli@microchip.com