A Leading Provider of Smart, Connected and Secure Embedded Control Solutions
Time Security

● How do networks acquire time?
  ● GPS/GNSS
  ● NTP

● How to ensure secure or trusted time
  ● Prevent unauthorized access
  ● Validate the integrity

Required: Situational Awareness
Secure Firewall

- Protects against GNSS spoofing and jamming
- Simple connection between GNSS antenna and GPS system
- Optional internal MAC for holdover
- 1PPS and 10 MHz timing reference inputs for extended holdover (connection to external cesium reference)
- Redundant AC or DC power options
- “BlueSky Performance Monitoring” integrated within TimePictra management software suite
Green vs. Red is Not the Problem

Good  Uncertain  Bad
Visibility: The First Step

- Network Infrastructure providers need to recognize the threat
- Many read the news, but have not felt the pain
- Visibility is a smart first step towards proactively securing GNSS reception… rather than waiting for disaster to strike

- Ability to quickly recover from anomalous GNSS events is greatly aided by real-time diagnostics and reporting
- Most users don’t actively monitor the health of GNSS…the “set it and forget it” culture needs to be changed
- Knowing is half the battle: Situational awareness reduces time spent identifying and localizing the issue
Hardening: The Second Step

- CVE patches
- DoS protection
- Continuous rigorous testing by manufacturer
- Authorize and limit user access

Minimize Attack Vectors and Limit Exposure Surface
The SyncServer S600 & S650

Best in Class NTP Time Servers PTP Grandmasters

SyncServer S600

SyncServer S650

Optional Timing I/O Modules
Key SyncServer Attributes

- **Accuracy**
  - Nanosecond accurate time stamping

- **Security**
  - Hardened, multiport networking
  - Secure, hardware-based timestamping

- **Reliability**
  - High-availability time services operation
  - 34 Year MTBF

- **Easy-to-Use**

**Application Verticals**
- Banking/Finance
- Enterprise
- Gov/Mil/Aero
Thank you!