TECH BRIEF

The Global Leader in Resilient **PNT**

Network Port Isolation for Secure Networks

Network Master Clocks and Time Servers

What is Network Isolation?
Network isolation eliminates data exposure across network segments for management and security.

How Orolia Supports Network Isolation

- Orolia offers isolation via software for its multi-port time server module via rules-based routing
- Hardware isolation is available in 3 configurations

When leveraging a single master clock / time server across several network segments there are various approaches to port isolation.

Software Isolation

SecureSync® and NetClock® 9483 network appliances can be configured with four network ports. These ports share a common processor and network stack. The network traffic served by these ports is isolated by software. A detailed description of the rules-based routing for this configuration is found in the Tech Note: Routing of Data with Multiple Networks.

Hardware Isolation by Multiple Processors

The modularity of Orolia devices allow for configurations that physically separate processors and network stacks. Currently, this is how precision time protocol (PTP, IEEE-1588) is implemented in SecureSync and NetClock 9483. A dedicated processor manages all PTP messages from a single isolated port and also supports a high degree of reliability and precision. While there are no network messages passed between processors, bidirectional communication exists for timing and other configuration data.

Hardware Isolation by Unidirectional Communication of Timing Data

The next higher degree of isolation is through physical separation between the entire hardware associated to the port. What makes this different than completely redundant systems is the ability for a master to share precision timing via an unidirectional data stream to one or more slave units each with its own network traffic processing unit. In this configuration, slave units can achieve stratum-1 NTP server performance without network/processor connection to the master. This can support different levels of protected networks (unclassified, classified, or different levels of classification). While this approach isolates the data communications path, an electrical connection still exists.

Hardware Isolation with Electrical Isolation

This approach is the same as the previous case with the addition of breaking the electrical path by optics. This is achievable by external opto-couplers or integrated fiber-optic modules. Tech Brief: Time Synchronization for Secure Networks using Fiber, provides additional details.

www.orolia.com
sales@orolia.com

29 April, 2020. Network Port Isolation for Secure Networks