GE
Measurement & Control

Bently Nevada* Asset Condition Monitoring

TDISecure* Communication Processor Cyber Security

fact sheet

Background

Cyber security is a critical concern for owners of Ethernet connected industrial instrumentation and controls systems (I&C). Critical national infrastructure, such as power generation, is subject to regulatory requirements on I&C systems. For example, the U.S. Federal Energy Regulatory Commission acting through the North American Electric Reliability Corporation has established Critical Infrastructure Protection standards for the U.S. power generation industry and the U.S. NRC has even stricter requirements for nuclear power generators.

Vibration Monitoring Systems (VMS), also referred to as Machinery Protection Systems, can be subject to cyber security risk evaluations and in many instances cyber hardening of some form is necessary. Hardening can be as simple as physical site security, configuration software controls and authentication, and virus protection. In extreme cases, arguments are made to eliminate Ethernet access to devices except from inside the security perimeter.

Effective plant asset management, particularly effective fleet management of machinery assets, often depends on remote access using condition monitoring software such as GE's System 1*. In most VMSs, there is a module in the vibration monitor rack that acquires waveform data from monitors in the rack and serves the data over the Ethernet to the condition monitoring software. In cases where cyber security is a significant concern, a direct Ethernet connection to the VMS may not be possible.

TDISecure

TDISecure ensures complete isolation of the VMS from remote access by enabling removal of the Ethernet remote access connection. TDISecure interfaces to the VMS by receiving the buffered analog sensor signals from the VMS. TDISecure digitizes

the analog signals, acquires measurements and waveforms, and supports remote access using its own Ethernet connection. No level of hacking or network attacks on TDISecure can touch the VMS.

The TDISecure is a communications interface device that:

- Is physically separate and independent from the machinery protection system;
- Provides analog communication exclusively between 3500 and TDISecure;
- Provides digital communication between TDISecure and GE's System 1* Optimization & Diagnostic Software;
- Can acquire dynamic vibration signals from non-Bently Nevada VMS and send to System 1.

Key Features

- Retains remote, real-time access for Rotating Equipment and Reliability Engineers
- 24 Dynamic analog signal inputs with parallel sampling and synchronization to a Keyphasor*
- Up to four Keyphasor inputs and ability to directly power four Keyphasor Proximitors or use buffered Keyphasor analog signals

- Achieves the required degree of cyber security by isolating the System 1 digital network from physical and logical connections to the machinery protection system
- Dynamic and transient data of similar quality to the internal communication processors from Bently Nevada* 3500 and 3500 ENCORE machine protection systems
- Data acquisition from non-Bently Nevada systems, including static, dynamic, and transient data
- 24 Direct process measurement analog signal inputs that can be configured as independent process inputs or can be associated to a dynamic input
- Ability to replicate protection system configuration for common channel types; replication ensures measurements and alarm levels are the same as those in the protection system
- Superior remote access performance, data quality, and cost compared to Data Diode solutions

Architecture for NRC/NERC Compliance with TDISecure

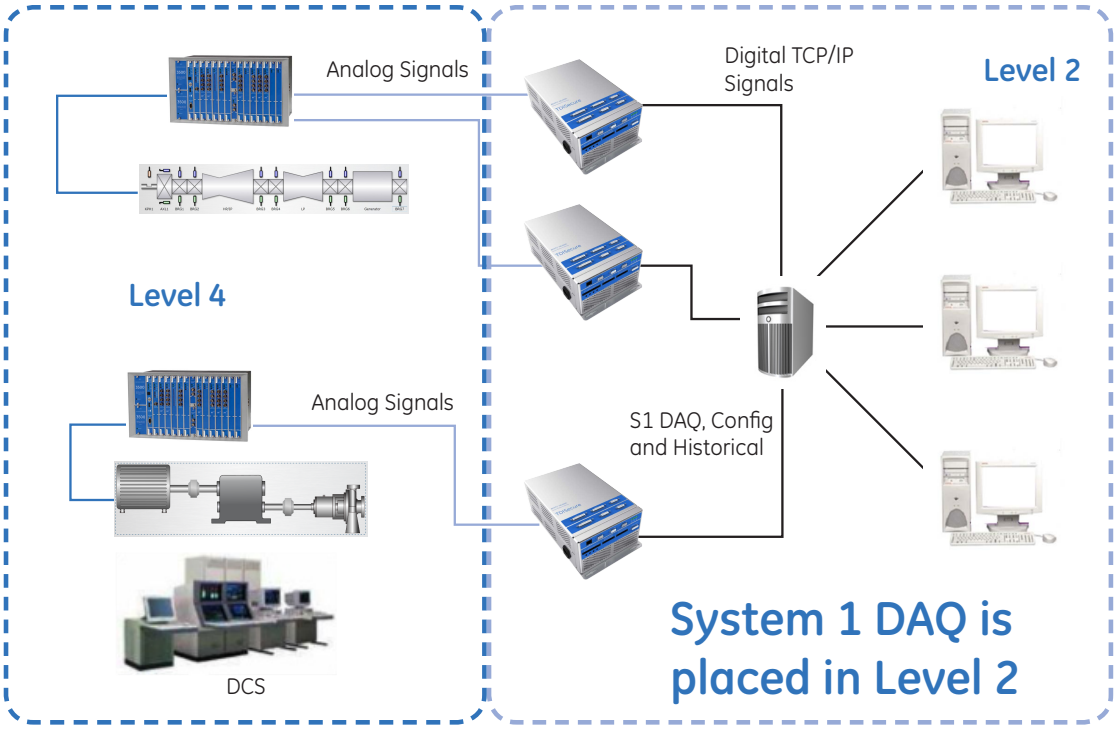

Figure 1 illustrates how TDISecure is deployed to meet the cyber security requirements in a U.S. Nuclear Regulatory Commission architecture. As described in NRC Regulatory Guide 5.71; devices in Level 4 (sometimes referred to as Zones) require the greatest security. Ethernet connections from a critical device in Level 4 must be unidirectional to a less secure level or not exist. TDISecure solves this problem because it is not a safety or protective system and can install in Level 2 and it's connections to the VMS in Level 4 is only using buffered analog signals. This architecture enables location of the System 1 Data Acquisition Computer in Level 2 where it can serve data to remote clients.

For additional information, please contact your local GE Representative, visit ***www.ge-mcs.com/bently***.

GEA30763 (07/2013)