F6880

Digital Network Analyzer

DETECT AND ADDRESS ISSUES IN IEC 61850 NETWORK TRAFFIC

The Doble F6880 Digital Network Analyzer (DNA) reveals details that are essential to helping protection engineers and relay test technicians quickly resolve issues in IEC 61850 network traffic.

This compact and lightweight instrument is paired with powerful software that analyzes Intelligent Electronic Device (IED) communications and provides diagnostic and analytical functionality in real time.

The DNA is a digital substation multimeter, capable of plotting sampled values (SV) and GOOSE messages via real-time oscillography, phasor, and tabular data views.

It is also a system event recorder, capturing events via customizable triggers and producing analysis reports that allow the user to evaluate network performance and power system anomalies, like voltage sag, harmonic distortion, and underfrequency.

The F6880 compares IEC 61850 SV and GOOSE information from configuration files (SCL and others) with the present network traffic to identify system misconfiguration issues such as missing, duplicated, or unknown messages.

The DNA can even be left connected in the substation for extended periods, offering remote access and control.

FEATURES AND BENEFITS

- Lightweight and compact for easy portability
- Multiple field and laboratory applications, in-person and remote use cases
- Software for detailed analysis of captured events and evaluation of network performance
- System event packet capture (PCAP) for analysis in a wide range of network analysis tools
- Numerous user-configurable views available for observing system status in real-time
- Fast setup and intuitive user experience

www.doble.com
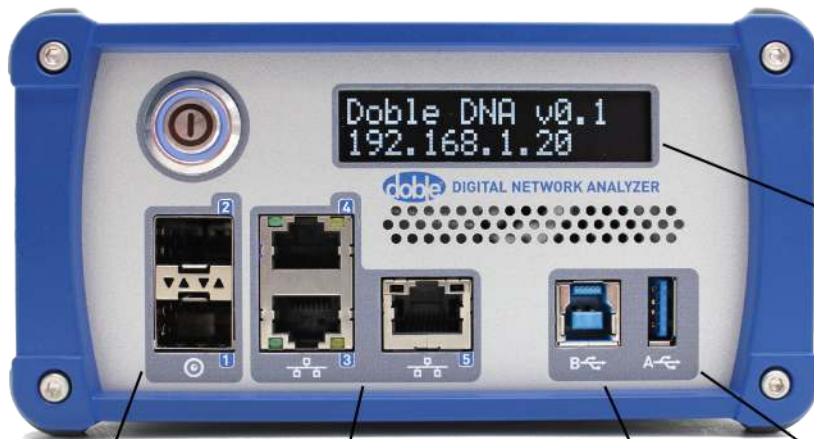
Display
Firmware Version
IP Address

2 x SFP Ports
Copper/Fiber
1 Gbps each

3 x RJ-45 Ports
10/100/1000 Mbps each

USB 3.0 Type B
Control

USB 3.0 Type A
Future Use

- 152 mm x 203 mm x 83 mm
  (6 in x 8 in x 3 1/4 in)
- 0.96 kg (2 lbs. 2 oz)
- Lightweight and easily
  portable

The F6880 compares IEC 61850 sampled values, GOOSE, and MMS from designed networks to packet structures on discovered networks to find anomalies that compromise system performance.