SEL Application Note AN2023-01

Using Communication Reports to Troubleshoot Operational Technology (OT) Protocols in Substations

Eduardo S. Palma

INTRODUCTION

Communications protocols for applications in OT environments have several characteristics, such as:

- Fixed number of devices (IEDs, merging units, bay controllers, clocks, and Ethernet switches).
- Fixed number of communications ports of all the devices in the network.
- Fixed number of Ethernet or serial protocols used or enabled by design.
- Fixed path of traffic for messages or direction of flow from originator device to destination device.
- Fixed redundancy requirements for protection and communications applications.
- Fixed time requirements for availability for critical traffic, with the goal of a seamless failover.

Designing the fixed or stable behavior of OT communications networks is a task that involves best practices, cooperation, and testing. With continuous monitoring, this behavior can be validated, and when an anomaly happens, troubleshooting can help us find the root cause.

From protective relays, we can collect COMTRADE or Compressed Event (.cev) files to analyze a power system disturbance after it has been recorded. The file contains analog values and digital statuses that are sampled at high speed. Most IEDs provide software that is used to collect and analyze these files, such as SEL-5601-2 SYNCHROWAVE® Event Software. This software graphically aids protection and power system engineers to understand expected and unexpected power system behaviors.

SEL protective relays do not automatically record a communications troubleshooting report of a communications-related issue; instead, communications statistics and real-time data can be automatically polled through an SEL Flex parsing protocol or manually queried through a Terminal Access window. Flex parsing is supported by the SEL Real-Time Automation Controller (RTAC) to send and parse ASCII messages in poll-and-response style. All SEL relays respond to ASCII commands, and the data are presented in plaintext format. These are some of the communications-related ASCII commands: PING, MAC, ETH, COM 87L, COM SV, COM PRP, TIME Q, COM PTP, GOOSE or GOO S, COM RTC, COM A, COM B, MET PM, and LOOP. Please review the instruction manual of your SEL relay to locate the description and verify which of these ASCII commands are supported.

For SCADA protocols such as DNP3, Modbus, IEC 61850 MMS, Ethernet/IP Address, SEL, and IEC 60870-5-101/103/104, there are no standardized reports for troubleshooting unexpected

behaviors between clients and servers in Ethernet networks or between primary and secondary in serially connected networks. This Application Note highlights tools used for capturing and storing the messages of SCADA communications protocols during unexpected behavior in a report file that can be used for troubleshooting OT protocols in substations.

COMMUNICATION MONITORING AND REPORTING TOOLS

The Communication Monitor (Comm Monitor) is a tool inside the ACSELERATOR RTAC® SEL-5033 Software used to capture and manually save reports in packet capture (.pcap) report file so that these reports can be analyzed by engineers familiar with OT protocols to troubleshoot any unexpected or undesired behavior.

While in online mode, the ACSELERATOR RTAC offers communications captures of:

1. EIA-232 or EIA-485 serial traffic saved by the Comm Monitor for these protocols: CP2179, DNP3, IEC 60870-5-101, IEC 60870-5-103, IEEE C37.118 Synchrophasors, L&G 8979, Modbus remote terminal unit, and SEL Protocol.
2. Ethernet TCP/IP traffic saved by the Comm Monitor for these protocols: DNP3, Modbus TCP, IEC 61850 MMS*, IEC 60870-5-104, IEEE C37.118 Synchrophasors, SNMP, OPC UA*, and SEL Protocol.

*if licensed or applicable to the SEL RTAC model

Just like the ACSELERATOR RTAC, the RTAC web interface can capture multiple connections of network or serial device traffic into a .pcap file.

Wireshark software is a free and open-source software that runs on Microsoft Windows OS or Mac OS. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

The RTAC web interface, ACSELERATOR RTAC Comm Monitor, and Wireshark software are online traffic sniffers. The RTAC, or computer port, must be enabled and connected to the networked devices for the manual capture to begin and then manually stopped to be saved into a .pcap file. To capture Ethernet traffic with managed Ethernet switches, enable the port-mirroring feature to passively listen and capture Ethernet traffic.

The .pcap files can be any length of time, from the time the capture is manually started until the capture is manually stopped. In the .pcap file, we save all the sniffed packets for that capture. If a specific unexpected behavior is going to be captured, the .pcap sniffing must be manually started before it occurs and then stopped so the file can record all the necessary data during that unexpected behavior.

In the latest firmware version update of R151, the SEL-3555, SEL-3350, and SEL-3560 RTACs have a tool called Packet Dissector. The web interface of these three models of the RTAC provides web-based online troubleshooting for serial or Ethernet communications to the following protocols: DNP3, Modbus, SEL, IEC 60870-5-101/104, IEC 61850 MMS, GOOSE, L&G 8979, CP2179, and IEEE C37.118 client and server devices.

The RTAC web-based Packet Dissector and Wireshark software facilitate the viewing and filtering of .pcap files. Filtering or hiding all the other packets that do not match a filter makes it easier to follow the behavior of a SCADA protocol chronologically. In Figure 1, the DNP3 (in lowercase letters) filter is applied in the RTAC web-based Packet Dissector to show only the DNP3 traffic.

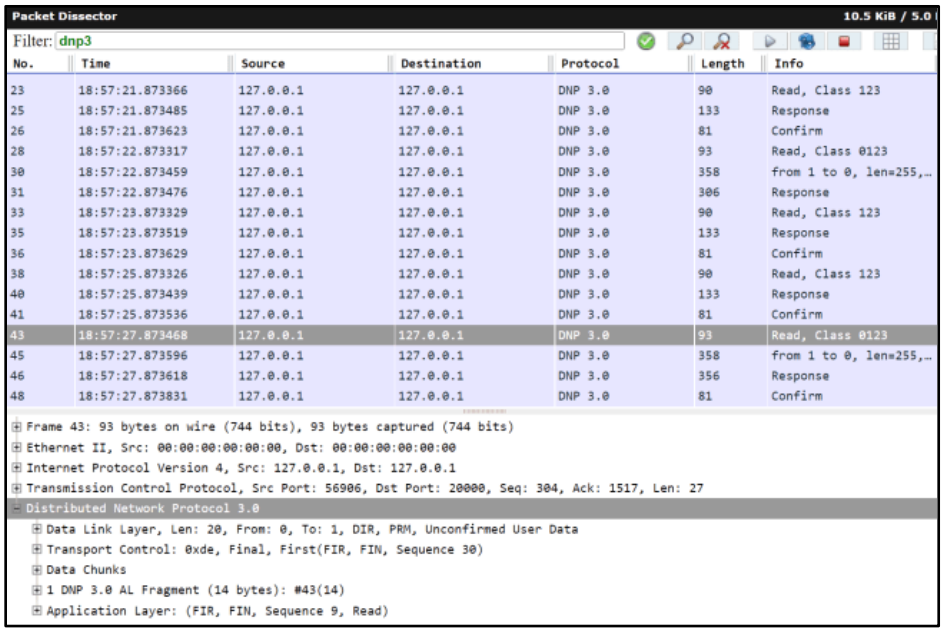

Figure 1 Packet Dissector capture of DNP3 traffic.

Another source of information for troubleshooting communications-related issues is the ACSELERATOR RTAC when it is in online mode. While the software is online with the RTAC, the visible program organization unit (POU) pins of each device communicating to the RTAC show troubleshooting statistics and online statuses. These POU pins are tags that can be mapped to be logged and time-stamped by the RTAC Tag Processor to alarm if there are changes in value or digital state. Logging these tags should be segregated under a logging category such as "communications troubleshooting," or something similar. Optionally, these tags can be sent by the RTAC to a Syslog server.

CONCLUSION

Troubleshooting communications-related issues can be accomplished with tools used for capturing, storing, and analyzing the messages of SCADA communications protocols during unexpected behaviors. The .pcap report files can be used for troubleshooting OT protocols. If applicable, it is recommended for the .pcap file and settings files of the SEL devices involved to be gathered and emailed to your SEL technical support team for troubleshooting and root cause analysis.

LAN2023-01

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com