SCADA Protocols

by Jakub Aniol and Azeem Mohammed

Introduction

SCADA is an acronym for Supervisory Control and Data Acquisition. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, power utilities and many others. These systems incorporate the transfer of data between a SCADA central host computer and a number of Remote Terminal Units (RTUs). A La Marche battery charger would be considered RTU.

SCADA protocols are the languages used by machines to communicate. La Marche offers a variety of protocols that are commonly used, such as: DNP 3, Modbus, IEC 61850 and SNMP.

Table of Contents

DNP 3.0

One of the communication protocols that La Marche offers is DNP 3 (Option code **21P**). This option may be equipped on A12B, TPSD and A75D/A75DE battery chargers. It may be connected via RS232, RS485 or an Ethernet port. If a customer desires to connect the equipment through fiber optic cable, a converter box may be purchased from La Marche.

In a DNP 3, data is organized into data types. Each data type is an **object group**, including:

- Binary inputs (single-bit read-only values)
  Example: AC or Breaker Tripped Alarm Indicator (FAILURE = 1)
  If a binary value is 0; this means AC is present
  If a binary value is 1; this means AC is not present or Breaker has tripped.
- Binary outputs (single-bit values whose status may be read, or may be pulsed or latched directly SBO type operations)
  Example: Float/Equalize Mode Indicator (FLOAT = 0, EQUALIZE = 1)
  If a binary value is 0; this means the battery charger is running in the float mode
  If a binary value is 1; this means the battery charger is running in the equalize mode.
- Analog inputs (multiple-bit read-only values)
  Example: Software version, Version of software on 225C card

Under this analog input, the SCADA central host computer will read software version installed in the battery charger. This cannot be changed by the user.

- Analog outputs (multiple-bit values whose status may be read, or that may be controlled directly or through SBO type operations)
  Example: Equalize Timer Mode (0, 1, 2, 3, 4)
  Under this analog output the SCADA central host computer will read what Equalize Timer Mode is currently set to. This can be changed by the user.

The tables below identify all the data points provided by the implementation.

Binary Input Points
Static (Steady-State) Object Number: **1**
Static Variation reported when variation 0 requested: **1 (Binary Input 2 without status)**

Point Index	Name/Description
0	AC or Breaker Tripped Alarm Indicator (FAILURE=1)
1	Low Voltage 1 Alarm Indicator (FAILURE=1)
2	High Voltage Alarm Indicator (FAILURE=1)
3	High Voltage Shutdown Alarm Indicator (FAILURE=1)
4	Low Current Alarm Indicator (FAILURE=1)
5	Ground Detection Enabled (ENABLED=1)
6	Positive Ground Alarm Indicator (FAILURE=1). *Point will always read 0 when Ground Detection Enabled (Binary Input Point 5) is 0.*
7	Negative Ground Alarm Indicator (FAILURE=1). *Point will always read 0 when Ground Detection Enabled (Binary Input Point 5) is 0.*
8	Summary Alarm Indicator (FAILURE=1)
9	Low Voltage 2 Alarm Indicator (FAILURE=1)
10	Overload Current Alarm Indicator (FAILURE=1)
11	Charger Failure Alarm Status (FAILURE=1)
12	Float/EQ Mode Indicator (FLOAT=0, EQUALIZE=1)

Binary Output Status Points
Object Number: **10**
Default Variation reported when variation 0 requested: **2 (Binary Output Status)**
Control Relay Output Blocks
Object Number: **12**

Point Index	Name/Description
0	Float/Equalize Mode Indicator (FLOAT=0, EQUALIZE=1)

Analog Inputs
Static (Steady-State) Object Number: **30**
Static Variation reported when variation 0 requested: **4 (16-Bit Analog Input w/o Flag)**

Point Index	Description, Units	Scale Factor
0	Board Number. Will read 225 for 225C card.	None
1	Software Version, Version of software on 225C card.	None
2	Voltage, Volts	0.1
3	Current, Amps	0.1
4	Equalize Cycle Time Hours Remaining, Hours, Minutes *Note: The last two digits are the minutes.*	None
5	Auto Equalize Timer, Days	None
6	Auto Equalize Timer, Hours, Minutes *Note: The last two digits are the minutes.*	None
7	Low DC Current Alarm Low Limit, Amps. Setting the Low DC Current Alarm below this will result in disabling the Low DC Current Alarm Status Indicator.	0.1
8	Temperature Probe Reading, Degrees C *Note: Reading will always read 0 when charging system is not equipped with a 340S card. A shorted probe will give a reading of –273 and an open probe will give a reading of+273*	None

Analog Outputs
Static (Steady-State) Object Number: **40**
Static Variation reported when variation 0 requested: **2 (16-Bit Analog Output Status)**

Point Index	Description, Units, Valid Settings/Range	Scale Factor
0	Equalize Timer Mode (0,1 2,3,4)	None
1	Equalize Timer Setting (0 to 144)	None
2	Low Voltage 1 Alarm Threshold, Volts (0 to 2000)	0.1
3	High Voltage Alarm Threshold, Volts (0 to 2000)	0.1
4	High Voltage Shutdown Alarm Threshold, Volts (0 to 2000)	0.1
5	Low DC Current Alarm Threshold, Amps (0 to 60000)	0.1
6	Low Voltage 2 Alarm Threshold, Volts (0 to 2000)	0.1
7	Overload Alarm Current, Amps (0 to 60000)	0.1

Modbus

Another communication protocol that is offered by La Marche is Modbus. (Option code **21Q**) There are three different Modbus protocols: Modbus ASCII, Modbus RTU and Modbus TCP/IP. Option 21Q may be equipped on A12B, TPSD and A75D/A75DE battery chargers. Modbus ASCII and Modbus RTU may be connected via Ethernet port, RS232 or RS485. Modbus TCP/IP may be connected only through an Ethernet port. If a customer desires to connect the equipment through fiber optic cable, a converter box may be purchased from La Marche.

The Modbus standard includes a number of function codes giving the master of the network the ability to gather or place values/parameters in every slave connected to the network:

- Read Coils
  Example: Float/Equalize Mode Indicator (FLOAT = 0, EQUALIZE = 1)
  If a binary value is 0; this means the battery charger is running in the float mode
  If a binary value is 1; this means the battery charger is running in the equalize mode.
- Read Discrete Inputs
  Example: Low Voltage Alarm Indicator (FAILURE = 1)
  If a binary value is 0; this means the output voltage is above the low voltage threshold and no alarm is present
  If a binary value is 1; this means the output voltage is below the low voltage threshold and the alarm is present.
- Read Input Registers
  Example: Voltage, Volts
  Under this input register the SCADA central host computer will read the output voltage that is coming out of the battery charger.
- Read Holding Registers
  Example: Low Voltage Alarm Threshold, Volts (0 to 2000)
  Under this holding register the SCADA central host computer will read what the Low Voltage Alarm threshold is currently set to. This can be changed by the user.

Supported Modbus Function Codes:
01 – Read Coil Status (0X)
02 – Read Discrete Input Registers (1X)
03 – Read Holding Registers (4X)
04 – Read Input Registers (3X)
05 – Write Single Coil
06 – Write Single Register

Coils	
Address	**Name/Description**
00000	Float/Equalize Mode Indicator (FLOAT=0, EQUALIZE=1)

Discrete Inputs	
Address	**Name/Description**
10000	AC or Breaker Tripped Alarm Indicator (FAILURE=1)
10001	Low Voltage 1 Alarm Indicator (FAILURE=1)
10002	High Voltage Alarm Indicator (FAILURE=1)
10003	High Voltage Shutdown Alarm Indicator (FAILURE=1)
10004	Low Current Alarm Indicator (FAILURE=1)
10005	Ground Detection Enabled (ENABLED=1)
10006	Positive Ground Alarm Indicator (FAILURE=1). *Point will always read 0 when Ground Detection Enabled (Discrete Input Point 5) is 0.*
10007	Negative Ground Alarm Indicator (FAILURE=1). *Point will always read 0 when Ground Detection Enabled (Discrete Input Point 5) is 0.*
10008	Summary Alarm Indicator (FAILURE=1)
10009	Low Voltage 2 Alarm Indicator (FAILURE=1)
10010	Overload Current Alarm Indicator (FAILURE=1)
10011	Charger Failure Alarm Indicator (FAILURE=1)

Holding Registers		
Address	**Description, Units**	**Scale Factor**
40000	Heartbeat *This register increases once per second and may be used to determine if communications are still occurring.*	None
40001	Board Number. Will read 225 for 225C card.	None
40002	Software Version, Version of software on 225C card.	None
40003	Voltage, Volts	0.1
40004	Current, Amps	0.1
40005	Equalize Cycle Time Hours Remaining, Hours, Minutes *Note: The last two digits are the minutes.*	None
40006	Auto Equalize Timer, Days	None
40007	Auto Equalize Timer, Hours, Minutes *Note: The last two digits are the minutes.*	None
40008	Low DC Current Alarm Low Limit, Amps. Setting the Low DC Current Alarm below this will result in disabling the Low DC Current Alarm Status Indicator.	0.1
40009	Temperature Probe Reading, Degrees C *Note: Reading will always read 0 when charging system is not equipped with a 340S card. A shorted probe will give a reading of –273 and an open probe will give a reading of+273*	None

Input Registers		
Address	**Description, Units, Valid Settings/Range**	**Scale Factor**
30000	Equalize Timer Mode (0,1 2,3,4)	None
30001	Equalize Timer Setting (0 to 144)	None
30002	Low Voltage Alarm Threshold, Volts (0 to 2000)	0.1
30003	High Voltage Alarm Threshold, Volts (0 to 2000)	0.1
30004	High Voltage Shutdown Alarm Threshold, Volts (0 to 2000)	0.1
30005	Low DC Current Alarm Threshold, Amps (0 to 60000)	0.1
30006	Low Voltage 2 Alarm Threshold, Volts (0 to 2000)	0.1
30007	Overload Alarm Current, Amps (0 to 60000)	0.1

IEC 61850

IEC 61850 is the new emerging standard that is now being offered by La Marche. IEC 61850 has a proven track record of deliverable benefits to both small and large utilities. Networking equipment costs money to install, configure and maintain. But the savings that IEC 61850 delivers in the cost of substation design, installation, commissioning, and operation combined with the ability to implement new capabilities that are not practical or cost effective using legacy approaches makes those networking costs a worthwhile investment for the future. The benefits of IEC 61850 include:

- Self-describing devices enable access to device configuration over the network dramatically reducing setup time and cost.
- Standardized device-object models provide a higher level of interoperability that reduces variances between different types and vendors of devices lowering startup cost.
- Standardized data naming conventions use power system context to avoid arcane number oriented point tags and eliminates manual I/O to power function mapping simplifying setup and improving understandability.
- Use of shared station level networking for data access, supervisory control, and process functions minimizes point to point wiring and dramatically reduces cost for incremental improvement of existing systems over time.

SNMP

Simple Network Management Protocol (SNMP) is a network protocol designed to manage devices over an IP network. It was defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices. It is a part of Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.

Explanation
SNMP consists of four major components

1. SNMP Manager
2. An Agent
3. Managed Devices
4. Management Information Databases

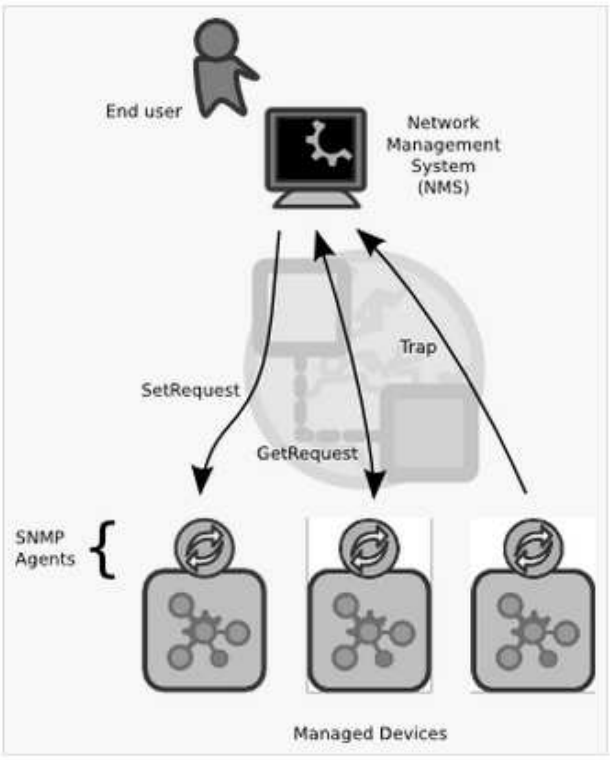
SNMP manager is installed on a computer that already has management software. This management console simply monitors, responds and manages to any query that is being sent from the agent. It will decide whether it needs to send email notifications or ignore them. This is a computer that is used to run one or more network management systems.

An agent is a piece of software installed on the devices that are connected to the management console. It reads any information on the device, and sends it back to management console.

The commonly shared database between the Agent and the Manager is called Management Information Base (MIB). In short, MIB files are the set of questions that the SNMP Manager can ask the Agent. The Agent collects these data locally and stores it, as defined in the MIB.

SNMP is a component of larger software package. To install SNMP, it requires major software such as LAN view, Spice works, etc.

Below is a simple block diagram of SNMP:



Application:

SNMP is a very powerful tool that can be used to proactively monitor devices over the network.

La Marche LTP model uses SNMP protocol to get information in real-time. It can display device logs on LAN or WAN.

References

http://www.manageengine.com/network-monitoring/what-is-snmp.html

http://www.trianglemicroworks.com/documents/DNP3_Overview.pdf

http://www.rtaautomation.com/modbustcp/

http://www.sisconet.com/downloads/mktlit_61850_overview.pdf