Diagnosing PLC communications issues in Adroit

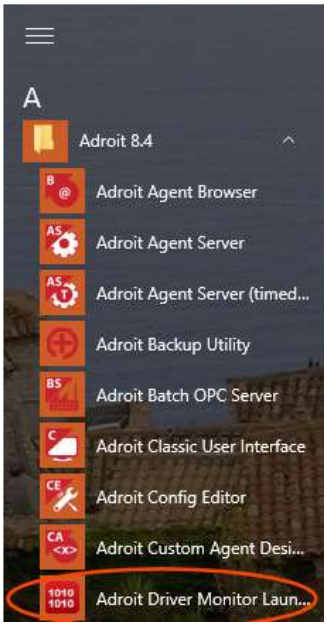
When SCADA-PLC communications are flaky it can be very difficult to figure out exactly what's going on without having access to the right kind of tools. Thankfully, Adroit Smart SCADA includes two very powerful utilities that address this:

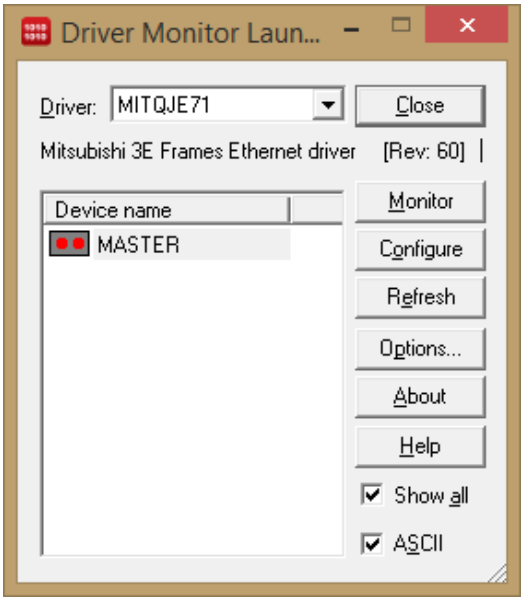
Driver Monitor	All Adroit PLC drivers include an in-built driver monitor allowing you to display and log timestamped SCADA-PLC communications exchanges that enables diagnosis of communications *reliability* issues
Scanning Monitor	The PLC scanning sub-system in Adroit includes a monitoring utility that enables diagnosis of communications *performance* issues

With in-built tools of this quality and usefulness, solution builders are well able to diagnose and correct potentially difficult communications issues.

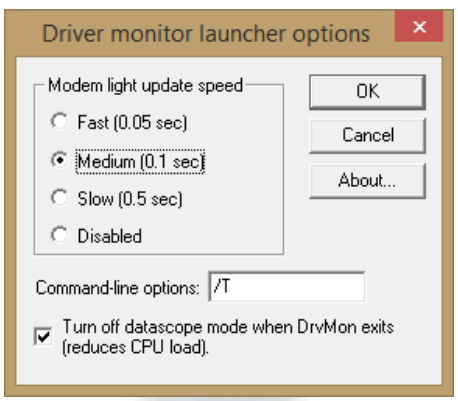
Driver Monitor

The screenshot on the left, below, is part of the Windows 10 start screen, showing items from the Adroit program group. Highlighted at the bottom is an icon to run the *Adroit Driver Monitor Launcher,* which when clicked will cause the driver monitor launcher to run as shown in the right hand side screenshot



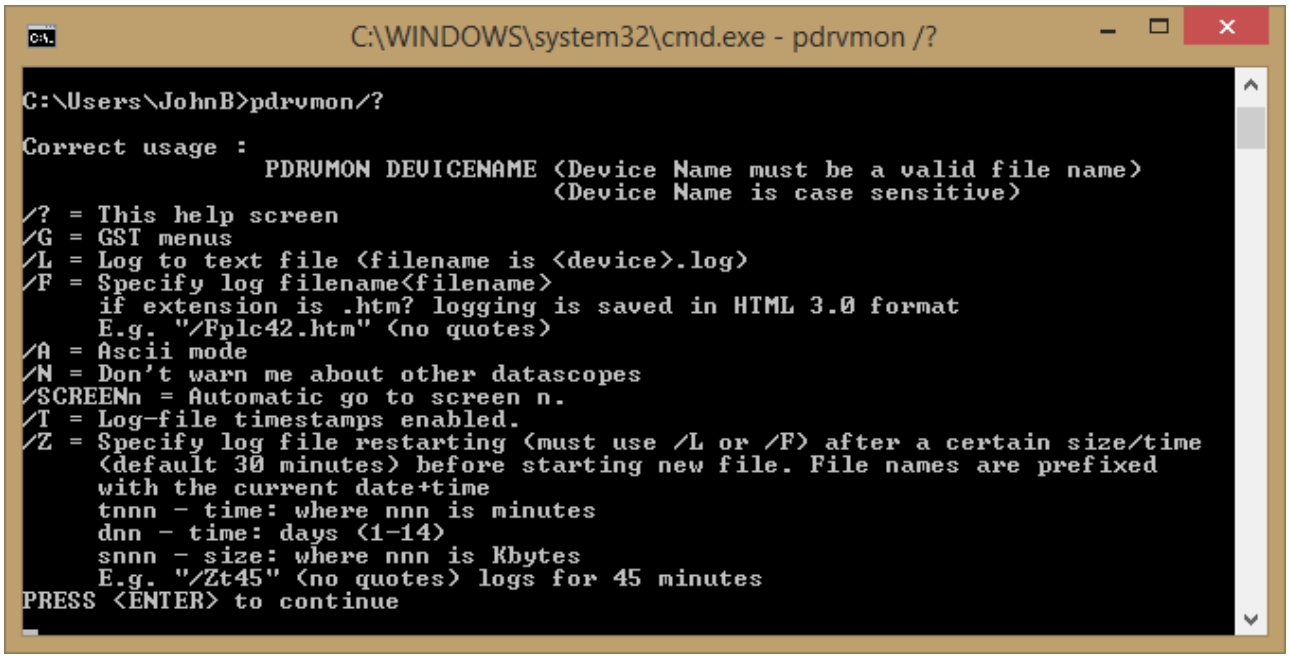


Clicking the options button displays the Options dialog which, amongst other things, allows you to specify command line options such as the '/T' shown which will cause timestamps to be displayed and logged along with the SCADA-PLC communications transactions.

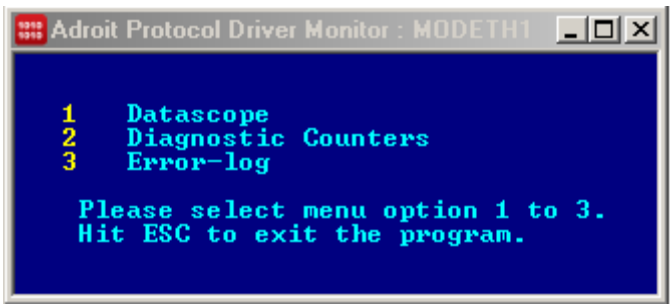


ADROIT TECHNOLOGIES
Tel: +44 1270 627 072
Adroit Technologies Ltd
PO Box 19 Nantwich
Cheshire England CW5 6FF
www.adroit-europe.com

It is also possible to launch the driver monitor directly from a command-line or desktop short-cut. The screenshot below shows this with the full set of available options



Driver Monitor Modes of Operation

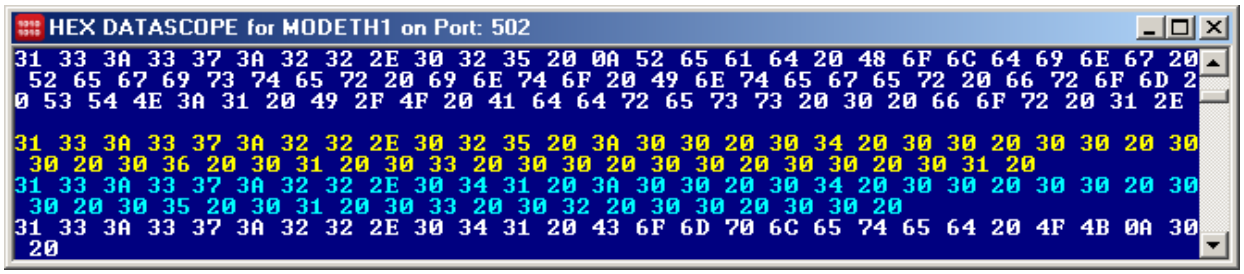


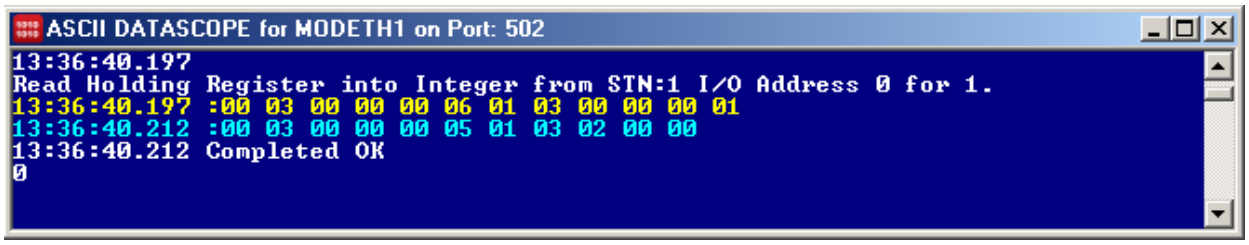
Selecting a device, and clicking the Monitor button in the driver monitor launcher, or running the driver monitor directly runs the driver monitor, which operates in one of three modes:

- ASCII or Hex *Datascope*, which displays, and optionally logs ('L' command-line option) data passing between SCADA and PLC for the particular driver instance selected
- *Diagnostic Counters* which displays a list of performance counters applicable to the particular PLC driver instance selected
- *Error-log* which displays a PLC-specific filtered view of any errors going out the the Windows event log

Datascope Mode (1)

The datascope can show either Hex or ASCII data. You can click ‘A’ while monitoring communications to toggle between Hex and ASCII mode.





The screenshots above show the same SCADA-PLC transactions, firstly in Hex mode, and secondly in ASCII mode. Instead of just logging raw transactions, some newer drivers paraphrase what’s going on in descriptive text, but usually the raw ASCII or Hex transactions are fairly easy to follow, in conjunction with the specific driver document which describes the various protocol transactions pretty rigorously.

The yellow messages are SCADA to PLC transmissions, and the cyan messages are PLC to SCADA transmissions. White text is paraphrased infomational content. Error situations are usually highlighted in red text.

You can click ‘L’ while monitoring communications to toggle between logging and not logging to text file. A file called *Device*.TXT, “MODETH1.TXT” in the above example, is saved into the Adroit installation folder (usually C:\Program Files (x86)\Adroit Technologies\Adroit).

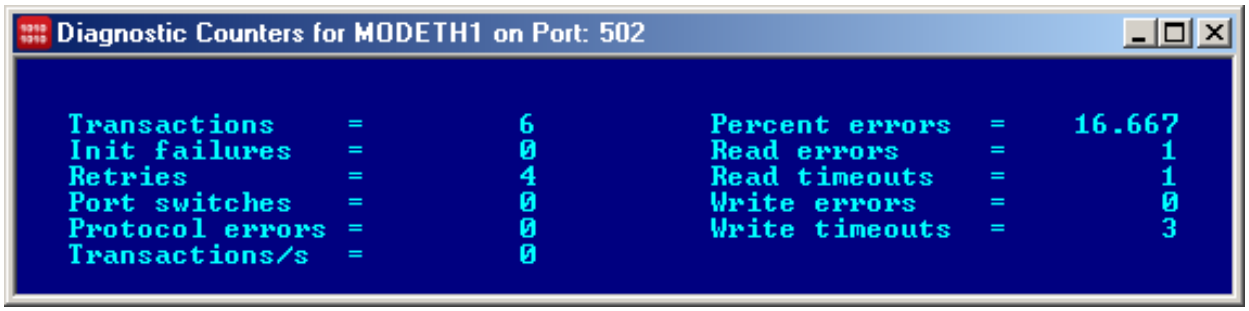
Clicking ‘H’ toggles logging to an HTML file which preserves colour information.

At any stage you can hit ‘Space-Bar’ to toggle between paused and un-paused mode. Transactions that happen while the display is paused continue to be logged, and in fact are subsequently displayed as soon as the display is un-paused.

The datascope displays protocol transactions taking place between the Adroit PLC driver instance and the PLC device itself. As mentioned earlier, for newer drivers there is often information additional to the raw data transmission. For example if the above ASCII datascope display, the ‘0’ and the last line after ‘…Completed OK’ is the value of the 16-bit holding register 400001 – quite a useful piece of information

Diagnostic Counters Mode (2)

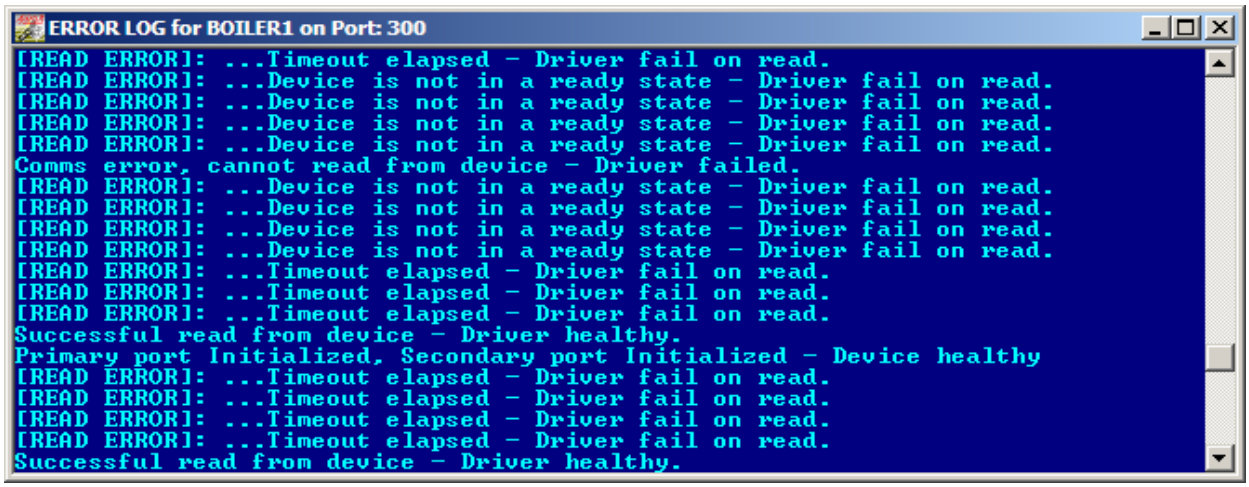
Diagnostic counters provide a quick overview of the most important counters available…



Transactions	Increments every time a SCADA-PLC communications transaction succeeds
Retries	Increments every time a failed transaction is retried
Errors	Increments when a transactions fails completely after the configured number of retries have been exhausted
Timeouts	Increments every time too few data bytes have been transferred in the time allotted for a transaction

Error Log Mode (3)

The error log display is a PLC device specific view of errors sent to the Windows event log, and can contain valuable information about the cause and potential resolution of problems…



Making sense of the Datascope display

With reference to the ASCII datascope display above, namely…

Read Holding Register into Integer from STN:1 I/O Address 0 for 1

…the relevant extract from the Adroit Modbus Ethernet driver document is:

Holding Registers 400001 – 465535

Read multiple holding registers function 03

Request from SCADA:

Transaction Hi ref	Transaction Lo ref	Protocol Id	Protocol Id	Hi Len	Lo Len	Slave/Unit Id
00	03	00	00	00	06	01

Function	Start Addr Hi	Start Addr Lo	Word count Hi	Word count Lo
03	00	00	00	01

Response from PLC:

Transaction Hi ref	Transaction Lo ref	Protocol Id	Protocol Id	Hi Len	Lo Len	Slave/Unit Id
00	03	00	00	00	05	01

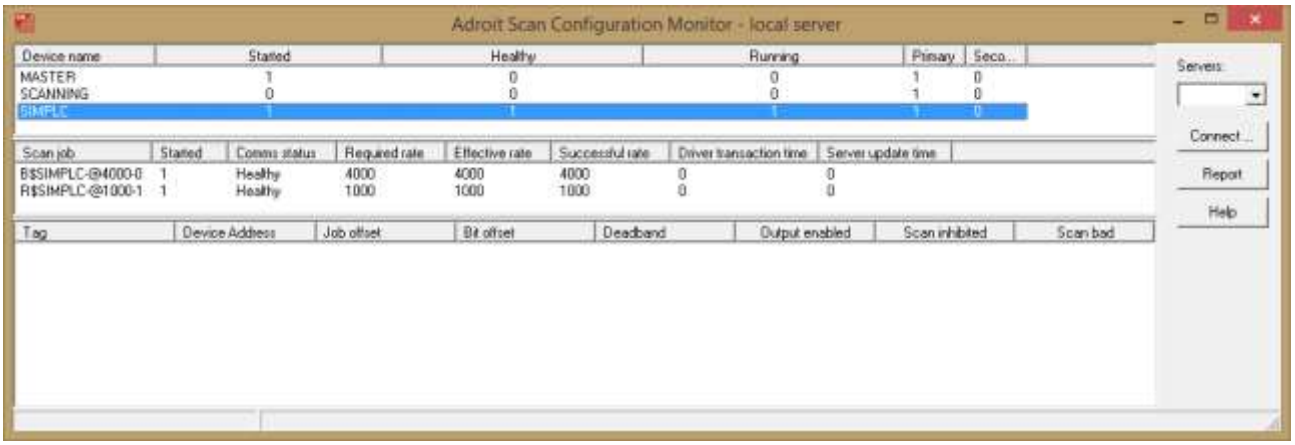
Function	Byte Count	Data Hi	Data Lo
03	02	00	00

i.e. the data value read back from the PLC is 0000 (Hex) or simply 0 as the ASCII datascope tells us

Scanning Monitor

Even when SCADA-PLC communications are robust and reliable, it is possible that you may not be achieving the required throughput. For example, a scan task or job – a *Scan Agent* in Adroit – that is built for, say, 1-second scanning is only managing to poll the PLC every 3 seconds. This could be due to simply too many items being scanned from the PLC, or more likely, it will be due to badly configured scanning leading to too many small, fragmented scan jobs instead of fewer larger scan jobs. To diagnose this kind of thing, another tool – the Adroit Scanning Monitor exists.

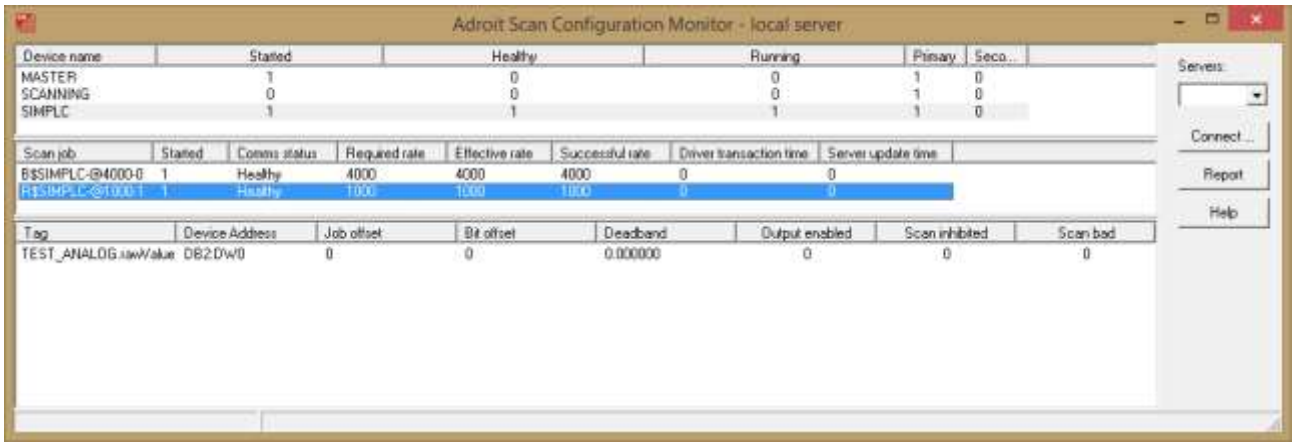
The scanning monitor has three different panes, as seen in the screenshot below which shows a simple scanning configuration with only two tags – a Digital and an Analog being scanned using the in-built simulated PLC driver instance, SIMPLC



The top pane lists the PLC *Device Agents* or driver instances that exist in the loaded Adroit SCADA server configuration. Other columns in this pane show whether the device is started, whether it is healthy, running, and whether it is operating on its primary or secondary channel.

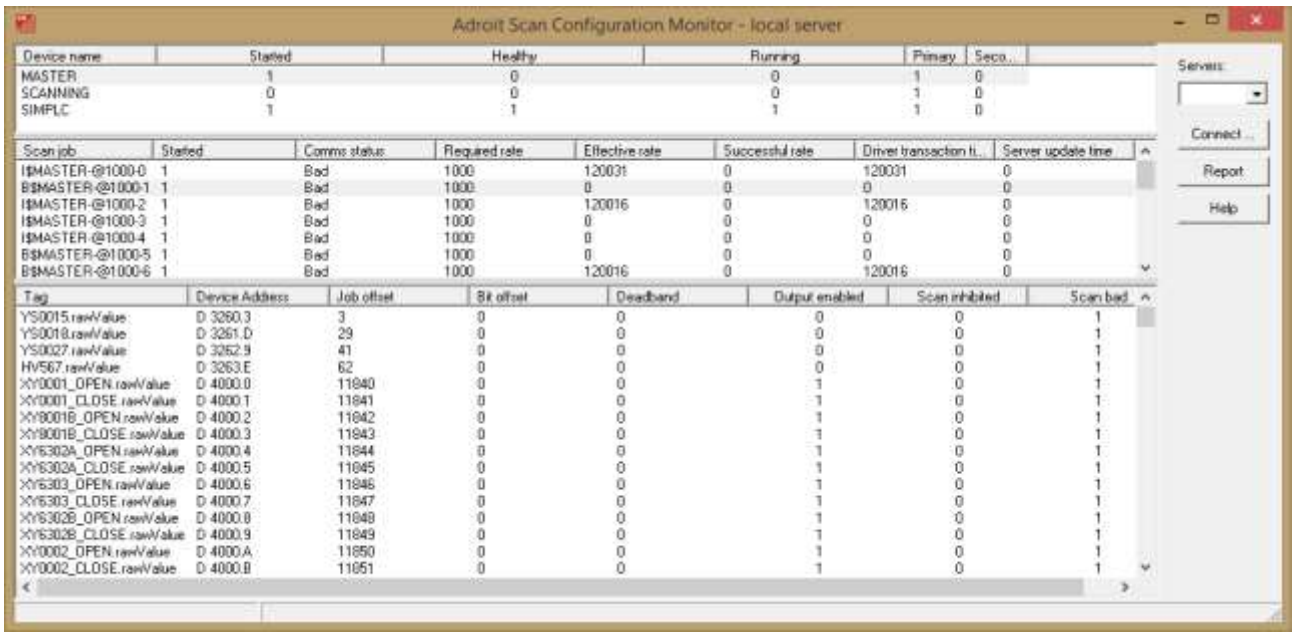
The second pane lists the scan jobs or *Scan Agents* that exist for the selected device, in this case the SIMPLC device. There are two scan jobs because the two tags being scanned are of different data types. The digital tag is of type Boolean, hence the scan agent name starts with B. The rest of the scan agent name reflects the device, SIMPLC, and the configured scan rate – 4 seconds for the digital. The analog tag is of type Real, hence the scan agent starts with R and its scan rate is 1 second. Other columns in this pane show whether each scan job is started, healthy, it's required, effective, and successful scan rates, as well as the time taken in the driver and the time taken to update the server. In this very simple scanning configuration, using only a couple of tags and a simulated driver, as you would expect, everything is running completely smoothly - scan times are fully achieved, etc.

The third pane is only meaningful if you select a scan job in the second pane, as below. The third pane then lists all tags and corresponding PLC addresses *associated* by the scan job. For example, we can see that tag TEST_ANALOG.rawValue is associated with PLC register DB2:DW0, meaning that PLC register DB2:DW0 will be polled at 1000 millisecond intervals and changes updated into tag TEST_ANALOG.rawValue. If the tag were *output-enabled* then changes to the tag value would immediately be sent out to the PLC. Other columns in this pane show more details about how each scan point is configured



As already mentioned, this is a very simple scanning configuration used to illustrate the scanning monitor.

A more realistic scanning configuration is shown below, with the device MASTER *Started* but not *Healthy* and *Running* because there is no PLC connected



By clicking the *Report* button on the scanning monitor, you can produce a CSV report loadable in MS Excel which summarizes the scanning configuration and provides a subjective score as to how optimal it is