eyePower Limited
John de Mierre House, 20 Bridge Road,
Haywards Heath, RH16 1UA, UK

Summary of eyePower Firmware Versions

Version 1.0

Date 10th June 2024

This is an overview of differences in eyePower PDU firmware between versions 1, 2 and 3.

eyePower has three microcontrollers, each with its own firmware. On the main circuit board, the relay controller manages power relays and the 1-Wire environmental sensors if connected. Also on the main board, the display controller manages the display and calculates voltage, current and power data. A separate network interface board has the third controller to provide SNMP, serve web pages and act as an Ethernet bridge to the main circuit board. All communicate internally.

Versions 1, 2, 3 firmware are not compatible with each other and should never be mixed between the different controllers, other than during bootload to update a unit. Within a major version 1-3, there are sometimes updates to only one controller which means not all firmware has the same minor version. This is managed by the use of a Windows bootloading utility that includes all three firmware files in the latest compatible build.

Version 1

The first eyePower units in 2013 shipped with version 1. Relay control was designated to a separate controller for maximum reliability. Much of the relay code, including the programming language for relay sequences, existed in products before eyePower and is well proven.

Version 1 Ethernet served the innovative web page with voltage/current graph, but the Ethernet controller did not store any status data from the relay/display controllers. It was effectively a serial data bridge between Ethernet traffic and the other two controllers. TCP control was included, so internal communication alternated between web updates and TCP control if pending.

Firmware updates were provided over time, usually to meet customer requests, but the most significant update was requested at the same time as version 2 development was ongoing. This is termed “latch on, lock off”. Each outlet can be defined as latch or lock, and be different depending on which supply A/B of a changeover unit is selected.

“Latch on” does not force an outlet to be on, so power on sequences are still possible. However, latch on will keep an outlet powered once it has been turned on. This prevents accidental turn off for equipment that is used 24/7 once power is established. The option to set “latch on” for only one supply of a changeover makes it possible to turn off the load once switched to a backup supply with limited capacity.

“Lock off” keeps an outlet off, which seems of limited use but was introduced to meet a specific user need where a UPS was not sized to maintain all the PDU load when running on battery. The original firmware already allowed change over and change back to trigger macro routines to shed and restore load. “Lock off” is different because the “off” outlets are pre-defined and are actioned at the same time as the changeover relay operates. This is so fast, the backup supply does not see the load which is rapidly dumped using the lock off definition.

Version 2

This version was a major project initially for one customer to provide SNMP data, not control, and allow a maximum of four units connected to one Ethernet feed. This uses one master PDU, with slave PDUs connected using RS422. More than three slaves would be possible with RS422, but eyePower provides a lot of status data which would have an unacceptably slow refresh rate with more units.

While version 1 Ethernet was a data bridge to the main board, version 2 Ethernet constantly polls four PDUs maximum to maintain a mirror of status data. SNMP polling reports this mirror data held by the Ethernet controller, without having to communicate with the main board. Similarly, the web page status and graph uses the mirror data.

Security of TCP control messages was a requirement. This sends control messages in the clear as no bad actor can benefit from seeing the control messages. However, they are authenticated with a 128 bit Message Authentication Code using a pre-shared key and unique message counter. The MAC algorithm is Chaskey, which has since been standardised in ISO/IEC 29192-6. The ISO standard uses 12 rounds, eyePower uses 16 rounds known as Chaskey-LTS (Long Term Strategy).

At the request of the customer, the web page displayed status, but all web control functionality was removed from the web page and the microcontroller itself.

Version 1 always assumed changeover unit supply B was the backup and would switch back to supply A when restored. Version 2 allowed changeover units to have A, B or no preference as the default supply. It also allowed for a forced changeover via the front panel, so PDUs could be changed over during quiet times ahead of maintenance work on a mains supply.

Changeover between asynchronous supplies was optionally allowed, made possible by opening inlet relays to prevent arcing across the changeover contacts.

Version 3

This version combines the two previous versions. Hence four units maximum, with status data mirrored in the Ethernet controller to provide SNMP polling and a better web page update. Changeover default supply can be A, B or no preference. Latch on, lock off from version 1 is included.

Version 3 reintroduces web page control of outlets that was removed in version 2. A small number of version 1 users had been offered password protection of the web page, but this was basic code and the Ethernet message between web page and PDU was not secure. Version 3 offers secure web control.

This web security does not use https, which we have studied in detail over the years. Updates would be required several times a year, to correct flaws in underlying third-party security code or https itself. Once flaws are documented, https is undermined. Maintaining https code and updating units is an impossible task over the 10-20 year unit life. Standard web security is not fit for this purpose.

Using http, the eyePower web page is loaded. Only at this point, a Man-In-The-Middle attack is possible if web code can be injected during page load. Simply watching the network traffic is not a valid attack. However, if you have MITM attackers injecting code on your network, you likely have bigger problems. Once the web page is loaded, best practice is followed and passwords do not leave the browser. The Chaskey algorithm, optionally used for TCP control, is used to authenticate web control messages with a token unique both to that unit and in time. Monitoring the web control messages is not an attack vector.

The web browser offers three levels of access – view, control and admin – each level of which can be password protected if required or disabled. Even if no password is required, an empty password is still encoded so the latest eyePower Windows configuration software must be used to set or clear passwords once the firmware is updated to version 3.

The front panel OLED now offers details about GPI status, internal voltage rails and optionally IP and MAC address.

Complex code for the changeover relay has been changed to isolate the unused supply during changeover, and until the changeover output is seen to track the selected supply.

Frequent updates of the Ethernet status mirror increased the serial rate from 9600 to 115200 bits per second in versions 2 and 3. This is internally, and on the rear RS422 connector. Updates now require a proper USB/RS422 adapter for Windows, whereas the slower version 1 data rate was reliable with an RS232 adapter.