PTP TRANSLATOR
QUICK START GUIDE

QUICK SETUP
1. Install the PTP Translator in the desired location
2. Connect the PTP Translator to the network switch
3. Connect to power, ensuring correct voltage is used
4. The top panel of the PTP Translator includes the following ports:
   - 1 x RJ45 Ethernet input (ADMIN/ETH) or
   - 1 x ST Fiber Connector output (P1)
5. When running the PTP Translator for the first time, the Time Output, Network, and Security settings can be configured by running the Configuration Tool software on any PC on the same network as the PTP Translator. See Configuration Tool Tips and Networking Tips for more help
6. Once the PTP Translator is fully setup, connect the clock outputs to your device/s

NETWORKING TIPS
- If the PTP Translator does not appear when you press Discover in the Configuration Tool, connect the PTP Translator directly using an Ethernet cable
- If using DHCP: before powering up ensure the PTP Translator is connected to the network
- Ensure your firewall(s) has UDP exceptions for the configuration program and for ports 9992, 9997 & 9999
- Ensure you have administrative rights on your PC

DEVICE CONNECTION TIPS
- Where connecting external devices to the TTL outputs, twisted pair cable is recommended
- A termination resistor of 120 Ω can be added to the end of a TTL run to achieve good impedance match.

CONFIGURATION TOOL TIPS
- The Configuration Tool software is available from www.tekron.com
- To connect to your PTP Translator, press the Discover button, then select the PTP Translator from the list, then press the Configure button
- Default login is – User Name: admin, Password: Password*
- Upon first connection you will be prompted to change the default password.
- In most applications, the TTL output should be configured to IRIG-B, with “Extensions” set to C37.118 (previously IEEE 1344, see right)
- Set this by going to the I/O tab, then for each port:
  1) Select the port
  2) Set the output type to IRIG-B
  3) Change the extensions to C37.118

*Warning: Please ensure that you record your password and store it in a secure manner. In accordance with Cyber Security “best practice”, if the administrative passwords are lost, the device must be sent back to the manufacture to recover the password.

www.tekron.com / Dec 2014