Our Ref. 060620IR

REF: T2750 PAC Programmable Automation Controller enhanced for Cybersecurity Robustness

Dear Customer,

Cybersecurity is no longer a secondary requirement in the industrial control's world. Eurotherm considers cybersecurity to be as important as safety or high availability.

Industrial Control Systems (ICS) based on computer technology and industrial-grade networks have been in use for decades. Earlier control system architectures were developed with proprietary technology and were isolated from the outside world, thus making attacks more difficult. In many cases, physical perimeter security was deemed adequate and cybersecurity was not a primary concern.

Today, many control systems use open or standardized technologies such as Ethernet TCP/IP to reduce costs and improve performance. Many systems also employ direct communications between control and business systems to improve operational efficiency and manage production assets more cost effectively. This technical evolution exposes control systems to vulnerabilities previously thought to affect only office and business computers. Control systems are now vulnerable to cyberattacks from both inside and outside of the industrial control system network.

Consequently, many industrial control users are embarking on cybersecurity initiatives. Meanwhile, governments around the world are under pressure to address the ever increasing cybersecurity threat and there is an increasing demand for governments to introduce regulation.

For further information about cybersecurity, please refer to HA032968 – Cybersecurity Good Practices Guide.

What's new in the T2750 PAC?

- New Instruments

  From July 2020, all units shipped will come with version V6/0 firmware. Units will power up with normal control and configuration functions inhibited until an Instrument Password has been set. The Instrument Password is saved at the unit and this password need only be set once.

  Eurotherm Network Explorer supplied with Eurotherm PAC Software 9.5 is used to set the Instrument Password. It is recommended the Ethernet connection to set the password is made through a dedicated point to point connection.

- Upgrading an Existing Instrument

  When upgrading firmware, any application files (Databases, Sequences etc.) will be retained, but the application will not run until an Instrument Password has been set as for a new instrument.

  Duplex (Redundant) controllers can be upgraded whilst retaining control of the plant as for earlier versions. It is necessary to upgrade both primary and secondary controllers to the new firmware version. First upgrade the secondary controller and set an Instrument Password, synchronize, change over, then update the old primary (now secondary). Note: password is copied during synchronization.

- Duplex (Redundant) Controllers

  During synchronization of a redundant controller, the Instrument Password is copied from the Primary to the Secondary controller and the secondary controller stores that password such that it is now the permanent password of that unit.

- Configuring Instruments

  Configuration of the instrument requires the use of computer-based tools (e.g. LINtools). To use the tools, the computer connection to the instrument needs to be 'Authorized' by entering the Instrument Password at the tools to manage the application (file listing, file copy, download, start, stop etc.).

  Each time the instrument is to be configured at the computer, the password will need to be entered. Continued user activity at the tools will maintain the Authorized state which will otherwise timeout if not explicitly Unauthorized.

- ELIN Runtime Communication

  ELIN Communication with other instruments (e.g. T2750), including legacy instruments via LIN bridges (e.g. T103), no matter what software versions are in use, requires no specific authorization and no passwords are required.

  Communication with computer runtime servers needs to be whitelisted as part of the instrument configuration. Each individual computer needs to be listed in the Instrument Options to specify the level of access: Data (cached blocks), File Transfer or Both.   Whitelisted file transfers can be limited to those needed for runtime operation (e.g. setpoint programs). The whitelisting covers runtime data & file access, but not configuration access which always requires authorization.

- Lost Instrument Password

  There are no backdoor passwords and there is no means to discover a lost Instrument Password. With direct physical access to the instrument, it is possible to follow a procedure to reset the Instrument Password to the as shipped undefined state; the instrument will then behave as a new instrument and a password will need to be set before the instrument can be used.

- Legacy Operation Mode

  Users who order spares for a legacy system can enable a legacy operation mode in T2750 V6/0 for use until the system is updated to make use of the cybersecurity robustness enhancements. A new instrument will still require a password to be set once before the legacy mode is enabled, thereafter the instrument will operate as for legacy versions i.e. no authentication required to use tools and no whitelisting required for computer runtime servers. Owing to the reduced security offered by this mode, it is not the preferred mode of operation, consider disabling legacy mode as soon as practical.

Eurotherm PAC Software
Eurotherm PAC Software 9.5 has been released to provide all tools and documentation to support the new features of T2750 Version 6/0.

How can I get technical support?
For Technical Support or advice, either by telephone or email, please contact your local Eurotherm Helpdesk