Our Ref. 200921SS

REF: E+PLC Range 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 E+PLC Range?

- **Update to CODESYS V3.5.15**

Both the E+PLC runtime executables (present on the devices) and CODESYS tools (installed on the PC) will be updated, to include a number of new and updated security features.

Of these, several will impact existing applications, and their potential should also be considered for new applications:

- File path locations have been updated, with systems flies now separated and hidden from users
- Runtime communication is now encrypted by default
- CODESYS Security Manager, which introduces certificates
- CODESYS Device User Management, which enforces an administrator password to be added upon first startup
- Web Visu enhancements to include HTTPS. Default configuration is with HTTP blocked, but this is configurable in the firewall settings

- **New E+PLC**

From September 2020, all units shipped will come with CODESYS V3.5.15. Units will not be able to be connected for configuration and download until a default administrator password has been set.

The CODESYS V3.5.15 Integrated Development Environment (IDE) is used to set the administrator password, and the prompt to do this will appear as part of the setup procedure.

- **Upgrading an Existing E+PLC Application**

Support documentation has been produced to provide a guide to upgrading to the latest version. The documents can be accessed from the following location, which is the 'E+PLC Customer Share' Box folders:

Eurotherm Ltd
Faraday Close, Durrington,
Worthing, BN13 3PL United Kingdom
Tel. +44 (0)1903 268500
Fax. +44 (0)8451 309936

eurotherm.co.uk

Reg. Office
Stafford Park 5
Telford
Shropshire TF3 3BL United Kingdom
Reg. In England No. 853008

schneider-electric.com

https://schneider-electric.box.com/s/egsqu6kypcepulje4c2c

Within the above folder is a subfolder entitled '**PC Software Tools'**, within which you will find a further subfolder containing '**E+PLC IDE (CODESYS)'**. Within this subfolder you will find:

- An .ISO disc image and an .EXE file, both of which contain the current software
- An Application Note for upgrading the firmware to the latest version
- An Application Note for upgrading applications to the latest version

The firmware must be requested from the support team; instructions to do this are covered in the documentation listed above. When upgrading firmware, the previously established upgrade process still applies, but it will not be possible to download to the new device until an administrator password has been set.

Note: Once a unit has been upgraded to CODESYS V3.5.15, it is not possible to downgrade.

Note: On an E+PLC400, it is not possible to reuse an older (a pre V3.5.15) SD card in a new product without completing the upgrade process (as outlined above).

- **Configuring E+PLC using CODESYS**

Configuration of the E+PLC requires the use of the CODESYS IDE. To use the IDE, the connection to the E+PLC needs to be authorized by entering the administrator username and password, to be able to then manage the application (file listing, file copy, download, start, stop etc.).

Each time the E+PLC is to be configured from within the CODESYS IDE, the password will need to be entered. The CODESYS IDE will then maintain the Authorized state until it is closed.

- **E+PLC Runtime Communication**

For CODESYS inter-PLC comms using network variables, no specific authorization or passwords are required.

- **Lost Password**

There are no service/recovery level passwords and there is no means to discover a lost administrator password. There is a device reset mechanism which would remove all application content from the E+PLC and allow the process of restarting the initial setup procedure.

- **Manual Update of CodeMeter**

Installation of CodeMeter. Due to a detected potential cybersecurity concern, users must update the third-party CodeMeter tool after installation of the CODESYS IDE. Go to https://www.wibu.com/support/user/user-software.html and install the latest patch.

- **Port configuration for Enhanced Cybersecurity Protection**

CODESYS products support a routing protocol for the communication between clients and the CODESYS Control runtime system. In order to minimize the risk of denial-of-service attacks, it is recommended that, at the end of system engineering, the configured Gateway Ethernet TCP Interface (typically 11740-11743), UDP ports 1740-1743 and Gateway Driver TCP port 1217 be blocked (as part of the device firewall configuration). Please note that this will restrict access from the CODESYS IDE, so for further access, these ports would have to be unblocked.

How can I get Technical Support?

For Technical Support or advice, please visit https://www.eurotherm.com/en/support/ where details can be found of the support options available in your region.

Eurotherm Ltd
Faraday Close, Durrington,
Worthing, BN13 3PL United Kingdom
Tel. +44 (0)1903 268500
Fax. +44 (0)8451 309936

eurotherm.co.uk

Reg. Office
Stafford Park 5
Telford
Shropshire TF3 3BL United Kingdom
Reg. In England No. 853008

schneider-electric.com

HA033523U008