Our Ref. 200417DM

REF: EPC2000 Programmable Controllers 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 EPC2000 Programmable Controllers?

- New Instruments

  From June 2020, all units shipped will come with revision V4.01 firmware. Units with either serial or Ethernet communications enabled, will power up with the communications in lockdown mode and will need the communications configuration password setting via iTools Engineering Studio (V9.83). Note: This action only needs to be performed the first time communications is enabled. Once set, the unit will operate as normal.

- Cloning

  After the clone file is restored, the communications configuration password will be restored only if the following is true:

  - The password is not the default of '1234567890' AND
  - The password is a minimum of 8 characters

  In the event the above criteria are not met, the account will be disabled until a new password is configured via iTools Engineer Studio (V9.83). All other HMI user account passcodes will be restored as normal.

- Upgrading an existing unit

  Due to changes in the database, the EPC2000 Programmable Controller will cold start automatically after the upgrade is complete. The user should clone the EPC2000 before the upgrade and restore the clone file after the upgrade is complete. The behavior of the unit is then as per 'Cloning' previously mentioned.

HA033523U006

- Cold starting

  When the EPC2000 Programmable Controller is cold started the unit will restart with the communications in lockdown mode and requires the communications configuration password be set via iTools Engineer Studio (V9.83).

- Default and Recovery Passwords

  In all instruments with V4.01 firmware or higher, the ability to log in to the EPC2000 Programmable Controller with a recovery password will be disabled. In the event of loss of password, please contact your local Eurotherm office.

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

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

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

eurotherm.co.uk   schneider-electric.com