03251611

krom//schroder

Ⓓ Ⓖⓑ → www.docuthek.com

Security manual BCU 46x, BCU 480

Contents

Safety

Please read and keep in a safe place

Please read through these instructions carefully before installing or operating. Following the installation, pass the instructions on to the operator. This unit must be installed and commissioned in accordance with the regulations and standards in force. These instructions can also be found at www.docuthek.com.

Explanation of symbols

•, **1**, **2**, **3**... = Action
▷ = Instruction

Liability

We will not be held liable for damage resulting from non-observance of the instructions and non-compliant use.

Safety instructions

Information that is relevant for safety is indicated in the instructions as follows:

⚠ DANGER
Indicates potentially fatal situations.

⚠ WARNING
Indicates possible danger to life and limb.

! CAUTION
Indicates possible material damage.

All interventions may only be carried out by qualified gas technicians. Electrical interventions may only be carried out by qualified electricians.

Conversion, spare parts

All technical changes are prohibited. Only use OEM spare parts.

Introduction

Burner control units BCU 460, 465 and 480 are designed to control, ignite and monitor gas burners in intermittent or continuous operation. They replace the local control cabinet. Air and gas flow monitoring as an option. The outputs for controlling the burners, e.g. for actuator and valves, are activated via the replaceable power module LM 400. All the parameters required for operation are saved on the integrated parameter chip card.

The bus module BCM 400 is used as a communication interface for burner control units BCU 4xx for connection to a fieldbus interface. Networking via the fieldbus enables BCU 4xx units to be controlled and monitored by an automation system (e.g. PLC).

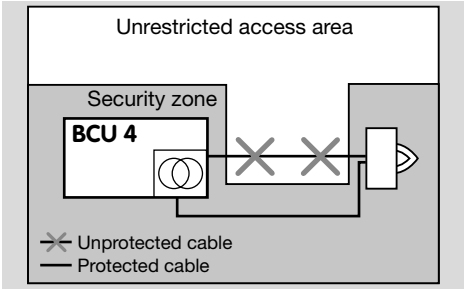
This security manual contains instructions for the safe integration of the BCU in a controller network.

Physical device protection

The BCU 4 series is protected from unauthorized external access by various security features (e.g. passwords at various levels).

Always select a location in a security zone with (restricted) access for authorized personnel only to install the burner control unit.

We highly recommend that all the wiring be protected from external access.



Protected and unprotected wiring

⚠ WARNING

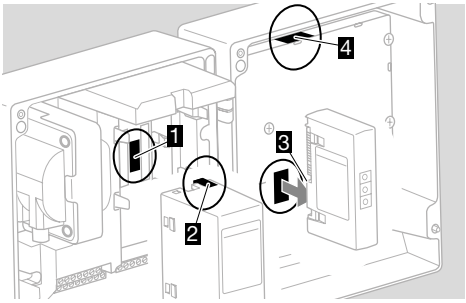
Unprotected (control) cables, all control modules and accessories connected externally must be protected from access by unauthorized personnel to protect the devices from tampering, which could result in hazardous situations.

Parameter chip card (PCC)

The configuration of the BCU is stored on a parameter chip card. Since the parameter chip card contains a complete backup of the device configuration, including the key for SafetyLink communication, it is important to keep the parameter chip card in a safe place and to protect it from being accessed by unauthorized personnel, even after the BCU has been decommissioned. If the entire system is decommissioned, it must be ensured that the PCC is technically destroyed.

Anti-tampering seals

The device components (1 upper housing section, 2 power module, 3 bus module and 4 HMI) are protected by anti-tampering seals. Never use a device if the seals have been damaged. The device could be damaged and represent an unforeseeable risk to the system.



Local communication interface

The BCU is configured using the optical adapter PCO 200. Ensure that the cabling for the optical adapter is removed from the BCU if it is not used.

Fieldbus interface

The fieldbus interface and communication network must be protected from unauthorized access. Otherwise, there is a significant risk of abuse and of safety-critical data being changed.

Device disposal

The BCU and the parameter chip card contain sensitive data (for example, the K-SafetyLink key). If the BCU is no longer in use and the K-SafetyLink network still exists, keep the parameter chip card and/or the BCU in a safe, inaccessible place if sensitive data is still stored on them. If communication with the device is possible, we recommend that you change the K-SafetyLink pass phrase. Defective devices must be irreversibly disposed of, including the electronic printed circuit boards.

Network configuration

The following points must be borne in mind during installation and all subsequent changes or expansions to ensure safe operation. The possibility must be ruled out that external faults can adversely affect performance in an unforeseeable way.

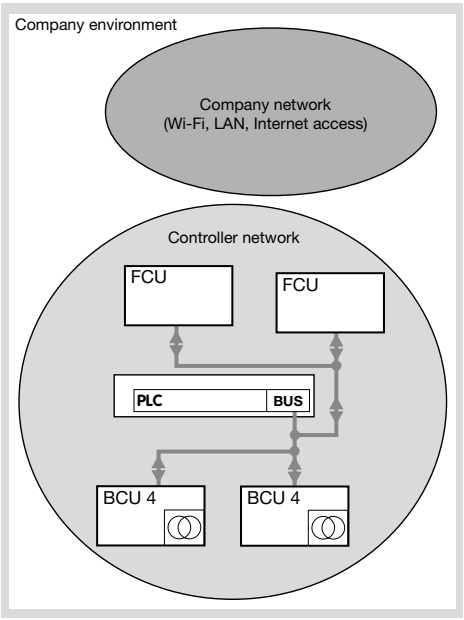
Controller network isolation

The BCU should be installed and connected inside an isolated controller network. The following methods may be used:

1. Physical separation between the controller and company network
2. Isolation using a firewall
3. Network address translation (NAT)

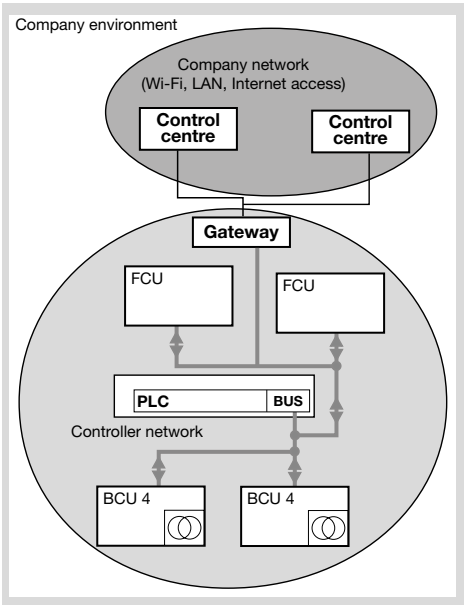
Physical separation

This method delivers maximum security as there is no physical connection between the controller network and the company network/Internet. The use of wireless devices to control the controller network may endanger the security of the network.



Firewall isolation

If there is a need to provide a connection between the controller network and another company network, we recommend that a correctly configured firewall (secured gateway) be used. The role of the firewall is to filter out data traffic from unknown sources and, at the same time, only to enter queries from reliably identified clients.



One possible example of a secure gateway would be a VPN set-up with defined authorized users.

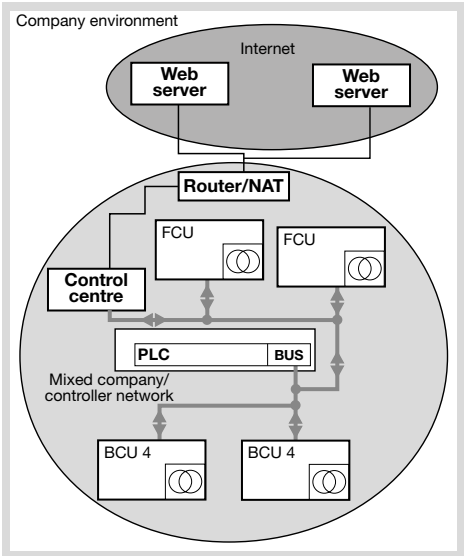
The following should be noted to ensure that a controller network has a secure configuration:

1. If the firewall port is open or the function is enabled, this should always be done with the full understanding of the relevant service.
2. A standard configuration is not a secure solution.
3. All communication to the network should be disabled apart from explicitly required data streams.

GB

Network address translation (NAT)

Network address translation (NAT) allows the partial isolation of the external network from the controller network. If NAT is correctly configured, it should not permit any connection from an external system to the controller. Since there are various solutions available on the market to configure networks in this way, it is not possible to explain the correct configuration of each of them in this document. In a scenario of this type, we highly recommend that you read the operating instructions for all the system parts and follow the recommendations of the various manufacturers.



Configuration of the PLC and control centre

We recommend that the following action be taken for peripherals before they are connected to a burner control unit:

1 Configure the operating system and the relevant software in accordance with the recommendations of the manufacturer and keep them up to date. Only use the operating system version supported by the manufacturer.

2 Install and enable virus and runtime protection systems.

3 Install and enable a firewall.

4 Enable a whitelist so that only authorized applications can be run.

5 Only use trustworthy software. Do not use any software which has been acquired illegally.

Communications protocols

The PROFIBUS, PROFINET, Modbus, EtherNet/IP protocols supported in the device do not support any security functions. We recommend that you follow the instructions described in the sections on page 2 (Physical device protection) and page 3 (Network configuration).

The Chipcom/UDP protocol is supported in the BCU for data monitoring. This protocol does not contain any security features. To ensure communications security, follow the recommendations from the section on page 3 (Network configuration) as the isolation of the network is the only way to guarantee data security.

SafetyLink protocol

A proprietary expansion of the SafetyLink protocol is available to exchange safety-critical data between BCU and FCU devices. This expansion ensures data integrity if the following precautions are taken:

1. The installation password is stored securely and not exchanged between isolated installations.
2. All the units which “know” the password are provided with physical device protection so that the password cannot be extracted from them. This also includes the security of the parameter chip card. Every device without physical device protection places the network security at risk.
3. Never disclose the network key to unauthorized persons.

Recommendations and time-tested methods

The BCU/FCU system is designed to ensure that it delivers reasonable security if it is installed and configured correctly. The following instructions cover the secure installation, configuration and commissioning procedures.

Configuration of the PLC/control centre

> **! CAUTION**
>
> Security problems caused by the use of interchangeable media.
> Never use USB sticks, CDs, etc. from unknown sources. Using the same USB sticks on home/hobby computers and production computers increases the risk of loading malware onto a production computer.

We recommend that the following action be taken before the burner control unit is physically connected to an automation system:

1. Update the operating systems and software and configure them as recommended by the manufacturer. It is essential that you use the operating system version supported by the manufacturer. Otherwise, there is a risk of vulnerabilities for the system.
2. Install and enable virus and runtime protection systems.
3. Install and enable a firewall.
4. Enable a whitelist so that only authorized applications can be run.
5. Only use trustworthy software. Do not install any unknown (e.g. cracked) applications.
6. Change the factory default password immediately. We recommend that secure pass phrases be used to ensure greater security.

Wireless devices

The use of wireless devices (e.g. Wi-Fi routers or Bluetooth adapters) extends the range of the network. Security from physical isolation cannot be guaranteed if wireless devices are used. The connection between the network and wireless device should not be permanent. It should be broken as soon as the required data has been exchanged. The wireless interface should be disabled when it is not required.

Unused data cables

Connections via unused data cables to BCU/FCU devices (e.g. Ethernet, RS485 bus cables or opto-adapters) should be disabled.

BCSoft utility software

Only the BCSoft software should be used to configure the BCU/FCU system. If third-party tools or generic data monitors are (must be) used, it must be ensured that they are compatible with the system and come from trustworthy sources. See www.docuthek.com for PC software and manual for BCSoft.

Reporting a vulnerability

A vulnerability is defined as a software error or a weakness which can be exploited to adversely affect or reduce the performance or security functions of the software.

Honeywell reviews all vulnerability reports relating to Honeywell products and services. Details of Honeywell's security policies are available at: https://www.honeywell.com/product-security.

If you would like to report a potential vulnerability for a Honeywell product, follow the instructions at: https://www.honeywell.com/product-security in the section entitled "Vulnerability Reporting".

Information about current malware threats which may affect industrial control equipment is available at: https://www.honeywellprocess.com/en-US/support/Pages/security-updates.aspx.

Contact

If you have any technical questions, please contact your local branch office/agent. The addresses are available on the Internet or from Elster GmbH.

We reserve the right to make technical modifications in the interests of progress.

Honeywell
kromschroder

Elster GmbH
Strotheweg 1, D-49504 Lotte (Büren)
Tel. +49 541 1214-0
Fax +49 541 1214-370
hts.lotte@honeywell.com, www.kromschroeder.com