Originalbetriebsanleitung © 2021 Elster GmbH · Edition 10.21

03251611

krom//schroder

Ⓓ GB → www.docuthek.com

Sicherheitshandbuch BCU 46x, BCU 480

Inhaltsverzeichnis

Sicherheit

Lesen und aufbewahren

Diese Anleitung vor Montage und Betrieb sorgfältig durchlesen. Nach der Montage die Anleitung an den Betreiber weitergeben. Dieses Gerät muss nach den geltenden Vorschriften und Normen installiert und in Betrieb genommen werden. Diese Anleitung finden Sie auch unter www.docuthek.com.

Zeichenerklärung

•, **1**, **2**, **3**... = Arbeitsschritt
▷ = Hinweis

Haftung

Für Schäden aufgrund Nichtbeachtung der Anleitung und nicht bestimmungsgemäßer Verwendung übernehmen wir keine Haftung.

Sicherheitshinweise

Sicherheitsrelevante Informationen sind in der Anleitung wie folgt gekennzeichnet:

⚠ GEFAHR

Weist auf lebensgefährliche Situationen hin.

⚠ WARNUNG

Weist auf mögliche Lebens- oder Verletzungsgefahr hin.

! VORSICHT

Weist auf mögliche Sachschäden hin.

Alle Arbeiten dürfen nur von einer qualifizierten Gas-Fachkraft ausgeführt werden. Elektroarbeiten nur von einer qualifizierten Elektro-Fachkraft.

Umbau, Ersatzteile

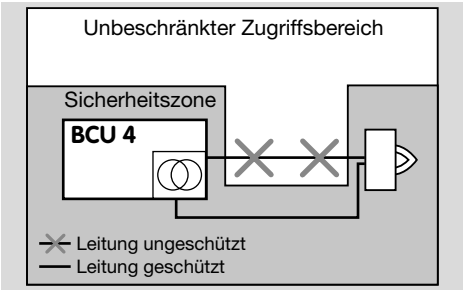
Jegliche technische Veränderung ist untersagt. Nur Original-Ersatzteile verwenden.

Einleitung

Die Brennersteuerungen BCU 460, 465 und 480 dienen zur Steuerung, Zündung und Überwachung von Gasbrennern im intermittierenden Betrieb oder Dauerbetrieb. Sie ersetzen den Schaltschrank vor Ort. Optional mit Luft- und Gasströmungsüberwachung. Über das austauschbare Leistungsmodul LM 400 werden die Ausgänge, z. B. Stellantrieb und Ventile, zur Steuerung der Brenner geschaltet. Auf der integrierten Parameter-Chip-Card sind alle für den Betrieb notwendigen Parameter gespeichert.
Das Busmodul BCM 400 dient als Kommunikationsschnittstelle für die Brennersteuerungen BCU 4xx zum Anschluss an eine Feldbusanschaltung. Durch die Vernetzung über Feldbus können BCU 4xx von einem Automatisierungssystem (z. B. SPS) gesteuert und überwacht werden.
Dieses Sicherheitshandbuch enthält Hinweise zur sicheren Einbindung der BCU in ein Controller-Netzwerk.

Physikalischer Geräteschutz

Die BCU 4 Serie ist durch verschiedene Sicherheitsmerkmale (z. B. Passwörter auf unterschiedlichen Ebenen) vor einem unbefugten Zugriff von außen geschützt.
Wählen Sie für die Montage der Brennersteuerung immer einen Standort in einer Sicherheitszone mit (beschränktem) Zugriff nur für befugte Personen.
Wir empfehlen dringend, die gesamte Verdrahtung vor äußerem Zugriff zu schützen.



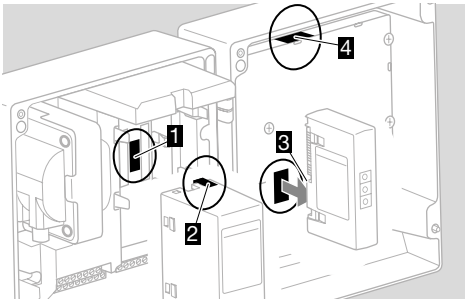
Geschützte und ungeschützte Verdrahtung

⚠ WARNUNG

Ungeschützte (Steuer-)Leitungen, alle extern angeschlossenen Bedienmodule und Zubehörteile vor Zugriff durch unbefugte Personen schützen, um die Geräte vor Manipulation zu schützen, was zu gefährlichem Verhalten führen kann.

Parameter-Chip-Card (PCC)
Die Konfiguration der BCU ist auf einer Parameter-Chip-Card gespeichert. Da die Parameter-Chip-Card eine vollständige Sicherung der Gerätekonfiguration einschließlich Schlüssel für die SafetyLink-Kommunikation enthält, ist es wichtig, die Parameter-Chip-Card an einem sicheren Ort aufzubewahren und vor Zugriff durch unbefugte Personen zu schützen, auch nach Außerbetriebnahme der BCU. Bei Außerbetriebnahme der gesamten Anlage ist darauf zu achten, dass die PCC technisch zerstört wird.

Anti-Manipulations-Siegel
Die Gerätebauteile (1 Gehäuseoberteil, 2 Leistungsmodul, 3 Busmodul und 4 HMI-Bedienmodul) sind mit manipulationssicheren Siegeln geschützt. Ein Gerät mit beschädigten Siegeln niemals verwenden. Es könnte beschädigt sein und stellt eine unvorhersehbare Gefahr für die Anlage dar.



Lokale Kommunikationsschnittstelle
Die Konfiguration der BCU erfolgt über den optischen Adapter PCO 200. Stellen Sie sicher, dass die Verkabelung des optischen Adapters von der BCU entfernt wird, wenn er nicht verwendet wird.

Feldbusanschaltung
Feldbusanschaltung und Kommunikationsnetz müssen gegen unbefugten Zugriff geschützt sein, sonst besteht ein erhebliches Risiko für den Missbrauch und die Änderung sicherheitskritischer Daten.

Geräteentsorgung
Die BCU und auch die Parameter-Chip-Card enthalten sensible Daten (z. B. K"-SafetyLink-Schlüssel). Wenn die BCU nicht mehr verwendet wird und das K"-SafetyLink-Netzwerk noch besteht, bewahren Sie die Parameter-Chip-Card und/oder die BCU an einem sicheren, unzugänglichen Ort auf, wenn noch senisble Daten auf ihnen gespeichert sind. Wenn eine Kommunikation mit dem Gerät möglich ist, empfehlen wir, die K"-SafetyLink-Passphrase zu ändern. Defekte Geräte sind irreversibel zu entsorgen, einschließlich Elektronikplatinen.

Netzwerkkonfiguration

Für einen sicheren Betrieb müssen bei der Installation und allen späteren Änderungen oder Erweiterungen nachfolgende Punkte beachtet werden. Es muss ausgeschlossen werden, dass äußere Störungen die Leistung auf unvorhersehbare Weise beeinträchtigen können.

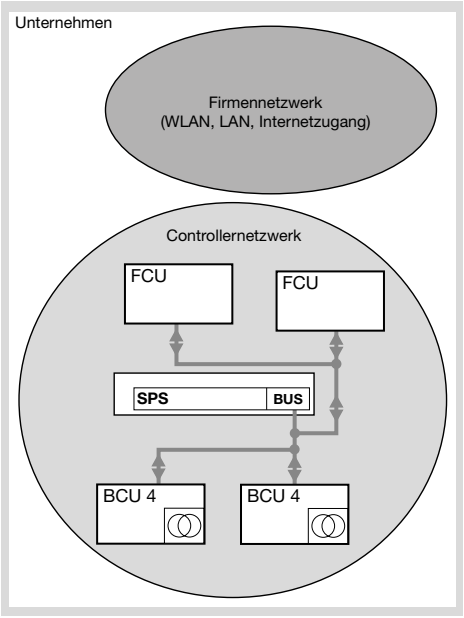
Isolierung Controller-Netzwerk

Die BCU sollte innerhalb eines isolierten Controller-Netzwerks installiert und angeschlossen werden. Folgende Methoden können angewendet werden:

1. Physische Trennung Controller- und Firmennetzwerk
2. Isolation durch Firewall
3. Netzwerk-Adressübersetzung (NAT)

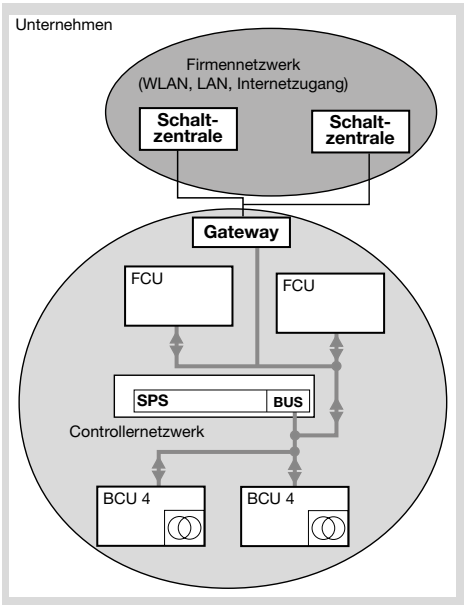
Physische Trennung

Diese Methode sorgt für höchste Sicherheit, da es keine physikalische Verbindung zwischen dem Controller-Netzwerk und dem Firmennetzwerk/Internet. Die Verwendung von drahtlosen Geräten zur Steuerung des Controller-Netzwerks kann die Sicherheit des Netzwerks gefährden.



Firewall-Isolation

Wenn es notwendig ist, eine Verbindung zwischen dem Controller-Netzwerk und einem anderen Firmennetzwerk bereitzustellen, empfehlen wir eine ordnungsgemäß konfigurierte Firewall (gesichertes Gateway) zu verwenden. Die Rolle der Firewall besteht darin, den Datenverkehr aus unbekannten Quellen herauszufiltern und gleichzeitig nur Anfragen von zuverlässig identifizierten Clients einzugeben.

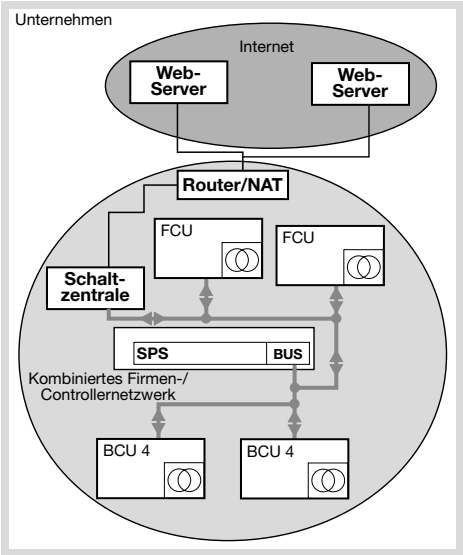


Ein mögliches Beispiel für ein solches sicheres Gateway wäre ein VPN-Setup mit festgelegten autorisierten Benutzern.

Für einen sicheren Aufbau eines Controller-Netzwerks ist Folgendes zu beachten:

1. Wenn der Firewall-Port geöffnet ist oder die Funktion aktiviert ist, sollte dies immer mit dem vollen Verständnis des jeweiligen Dienstes erfolgen.
2. Eine Standardkonfiguration ist keine sichere Lösung.
3. Die gesamte Kommunikation zum Netzwerk sollte deaktiviert werden, außer für explizit erforderliche Datenflüsse.

Network Address Translation (NAT)
Network Address Translation (NAT) ermöglicht eine teilweise Isolierung des externen Netzwerks vom Leitsystem-Netzwerk. Wenn NAT richtig konfiguriert ist, sollte es keine Verbindung von einem externen System zum Steuerungssystem zulassen. Da es auf dem Markt verschiedene Lösungen gibt, um Netzwerke auf diese Weise zu konfigurieren, ist es nicht möglich, die richtige Konfiguration jedes einzelnen von ihnen hier zu erklären. In einem solchen Szenario wird dringend empfohlen, die Bedienungsanleitung für alle Systemteile zu lesen und die Empfehlungen der einzelnen Hersteller zu befolgen.



Konfiguration von SPS und Schaltzentrale
Für die Peripheriegeräte empfehlen wir folgende Schritte vor der Verbindung mit einer Brennersteuerung:

1 Das Betriebssystem und die jeweilige Software nach den Empfehlungen des Herstellers konfigurieren und auf dem neuesten Stand halten. Nur die vom Hersteller unterstützte Betriebssystemversion verwenden.
2 Den Viren- und Runtime-Schutz installieren und aktivieren.
3 Die Firewall installieren und aktivieren.
4 Die Whitelist aktivieren, damit nur erlaubte Anwendungen ausgeführt werden können.
5 Nur vertrauenswürdige Software verwenden. Keine illegal erworbene Software verwenden.

Kommunikationsprotokolle

Die im Gerät unterstützten The PROFIBUS, PROFINET, Modbus, EtherNet/IP-Protokolle unterstützen keine Sicherheitsfunktionen. Wir empfehlen, die in den Kapiteln auf Seite 2 (Physikalischer Geräteschutz) und Seite 3 (Netzwerkkonfiguration) beschriebenen Hinweise zu befolgen.
Zur Datenüberwachung wird in der BCU das Chipcom/UDP-Protokoll unterstützt. Dieses Protokoll enthält keine Sicherheitsmerkmale. Um die Kommunikationssicherheit zu gewährleisten, sollten die Empfehlungen aus dem Kapitel auf Seite 3 (Netzwerkkonfiguration) befolgt werden, da die Isolierung des Netzwerks der einzige Weg ist, um die Datensicherheit zu gewährleisten.

SafetyLink-Protokoll
Für den Austausch sicherheitskritischer Daten zwischen BCU und FCU-Geräten ist eine proprietäre Erweiterung des SafetyLink-Protokolls erhältlich. Die Erweiterung ermöglicht eine Sicherung der Datenintegrität, wenn Folgendes beachtet wird:

1. Das Installationspasswort wird sicher aufbewahrt und nicht zwischen isolierten Installationen ausgetauscht.
2. Alle Einheiten, die das Passwort „kennen“, erhalten physikalischen Geräteschutz, so dass das Passwort nicht aus diesen extrahiert werden kann. Dazu gehört auch die Sicherheit der Parameter-Chip-Card. Jedes Gerät ohne physikalischen Geräteschutz stellt die Netzwerksicherheit in Frage.
3. Den Netzwerkschlüssel niemals an Unbefugte weitergeben.

Empfehlungen und bewährte Methoden

Das BCU/FCU-System ist so konzipiert, dass es bei ordnungsgemäßer Installation und Konfiguration eine angemessene Sicherheit bietet. Nachfolgende Hinweise dienen zur sicheren Installation, Konfiguration und Inbetriebnahme.

Konfiguration der SPS/Schaltzentrale

! VORSICHT

Sicherheitsprobleme durch Verwendung von Wechselmedien!
Niemals USB-Sticks, Disketten, CDs usw. verwenden, die von unbekannten Quellen stammen. Das Verwenden desselben USB-Sticks auf Heim-/Hobbycomputern und Produktionsrechnern erhöht die Gefahr, eine Schadsoftware auf einen Produktionsrechner zu laden.

Bevor die Brennersteuerung an ein Automatisierungssystem physikalisch angeschlossen wird, empfehlen wir Folgendes:

1. Betriebssysteme und Software auf aktuellen Stand bringen und nach den Empfehlungen des Herstellers konfigurieren. Unbedingt die vom Hersteller unterstützte Betriebssystemversion verwenden. Sonst besteht erhöhte Gefahr von Sicherheitslücken für das Systém.
2. Viren- und Laufzeitschutz installieren und aktivieren.
3. Firewall installieren und aktivieren.
4. Whitelist aktivieren, damit nur erlaubte Anwendungen ausgeführt werden können.
5. Nur vertrauenswürdige Software verwenden; Keine unbekannten (z.B. gecrackte) Anwendungen installieren.
6. Das werkseitige Standardpasswort sofort ändern. Für eine höhere Sicherheit empfehlen wir sichere Passphrasen zu verwenden.

Drahtlose Geräte

Das Verwenden von drahtlosen Geräten (z.B. WLAN-Routern oder Bluetooth-Adaptern) erweitert die Reichweite des Netzwerks. Die Sicherheit der physischen Isolierung ist bei drahtlosen Geräten nicht gewährleistet. Die Verbindung zwischen Netzwerk und drahtlosem Gerät sollte nicht dauerhaft bestehen. Sie sollte unterbrochen werden, sobald die notwendigen Daten ausgetauscht worden sind. Die drahtlose Schnittstelle sollte deaktiviert sein, wenn sie nicht benötigt wird.

Unbenutzte Datenleitungen

Verbindungen über unbenutzte Datenleitungen zu BCU/FCU-Geräten (z. B. Ethernet-, RS-485-Bus-Leitung oder Opto-Adapter) sollten deaktiviert werden.

BCSoft Dienstprogramm

Zur Konfiguration des BCU/FCU-Systems darf nur die Software BCSoft verwendet werden. Falls Drittanbieterwerkzeuge oder generischen Datenmonitore verwendet werden (müssen), ist sicherzustellen, dass sie mit dem System kompatibel sind und aus vertrauenswürdigen Quellen stammen. PC-Software und Anleitung BCSoft, siehe www.docuthek.com.

Melden einer Sicherheitslücke

Eine Sicherheitslücke ist definiert als ein Softwarefehler oder eine Schwachstelle, die ausgenutzt werden kann, um die Betriebsfähigkeit oder Sicherheitsfunktionen der Software zu reduzieren.
Honeywell untersucht alle Berichte über Sicherheitslücken, die Honeywell-Produkte und -Dienstleistungen betreffen. Einzelheiten zu den Sicherheitsrichtlinien von Honeywell finden Sie unter: https://www.honeywell.com/product-security.
Wenn Sie eine potenzielle Sicherheitslücke für ein Honeywell-Produkt melden möchten, befolgen Sie die Anweisungen unter: https://www.honeywell.com/product-security unter dem Abschnitt „Vulnerability Reporting“.
Informationen zu aktuellen Malware-Bedrohungen, die sich auf industrielle Steuerungstechnik auswirken, finden Sie unter: https://www.honeywellprocess.com/en-US/support/Pages/security-updates.aspx.

Kontakt

Bei technischen Fragen wenden Sie sich bitte an die für Sie zuständige Niederlassung/Vertretung. Die Adresse erfahren Sie im Internet oder bei der Elster GmbH.
Zentrale Service-Einsatz-Leitung weltweit:
Tel. +49 541 1214-365 oder -499
Fax +49 541 1214-547
Technische Änderungen, die dem Fortschritt dienen, vorbehalten.

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.de