Overview

The BECSys EZConnect system is a simple and secure method for providing connectivity to BECSys controllers. EZConnect eliminates the need for IT departments to make special router/firewall allowances for access to the water chemistry controller from outside the network, such as port forwarding and VPNs. EZConnect incorporates a peer-reviewed, multi-layered security approach; the EZConnect system offers significant security advantages over web-based interfaces, which are fundamentally more vulnerable to malicious attacks since an interface to the system is readily available to anyone with a web browser.

EZMail transmits email and text message alarm notifications through the secure EZConnect channel. This eliminates the need for users/IT to configure the controller with SMTP settings, and increases the reliability of email alarm notification delivery.

IT professionals will appreciate that the EZConnect security infrastructure has been vetted within the IEEE Internet-of-Things technical community. EZConnect is described in the paper entitled "Layered Security and Ease of Installation for Devices on the Internet of Things," which was peer-reviewed and published in *Proceedings of IEEE 1st International Conference on the Internet-of-Things Design and Implementation*, and presented at the *IEEE 1st International Workshop on Interoperability, Integration and Interconnection of Internet of Things (I4T)*, Berlin, Germany in April 2016.

Requirements

Network Requirements

- DHCP or static IP address for each controller, with DNS info
- Internet access allowing the following outbound ports to **ezconnect.becsys.com** as necessary
  - **Port 4001** for BECSys7, BECSys5, BECSysBW controllers
  - **Port 4005** for BECSysRCM (BECSys3, BECSys2 controllers)
  - **Port 4004** for PC's running BECSys for Windows
  - **Port 4003** for mobile devices running BECSys *Now!* mobile App

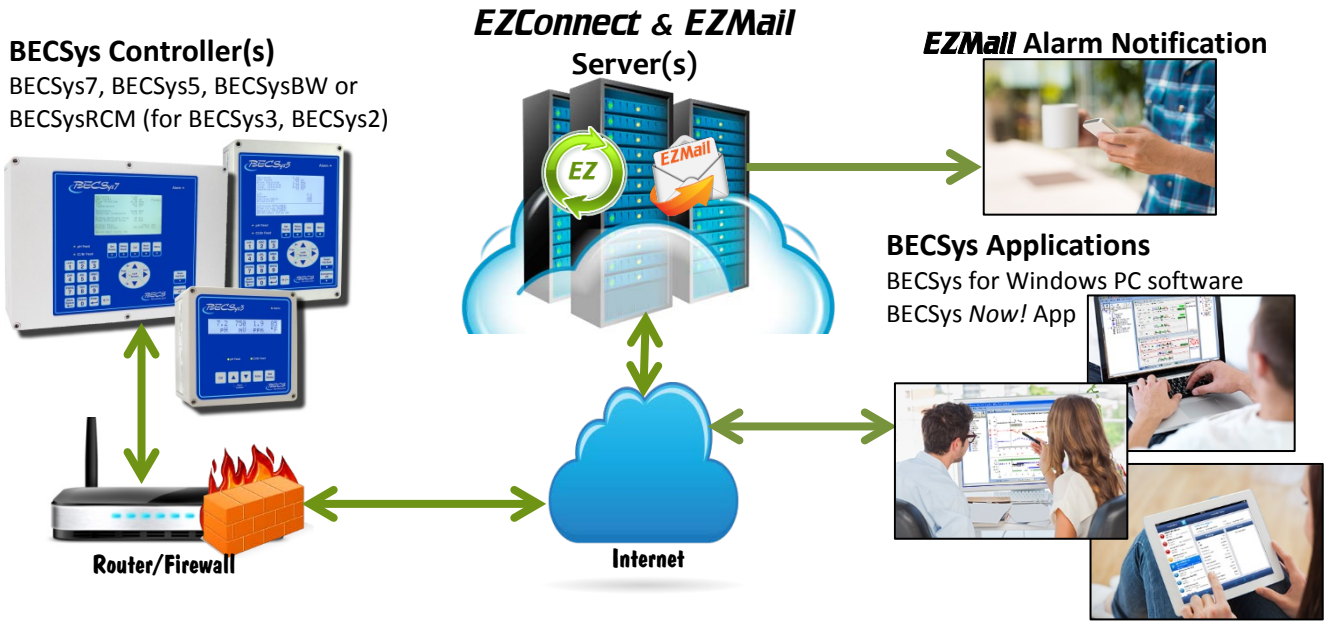
Controller & Application Requirements

- BECSys7, BECSys5, BECSysBW
  - v2.00 or higher firmware and
  - BECSys Gbit Ethernet
- BECSysRCM (for BECSys3 and BECSys2 controllers)
  - v1.50 or higher firmware
- BECSys for Windows
  - v1.55 or higher
- BECSys *Now!* Mobile App
  - v3.0 or higher

Benefits

- ✓ Highly secure; peer-reviewed, multi-layered security approach
  - No need to publish or distribute controller IP address
- ✓ Hassle-free setup and operation
  - IT does not need to establish VPN or forward ports on router
  - IT does not need to configure SMTP settings on controller for alarm notifications
- ✓ User needs only the controller ID Number and an Authentication Code
  - Authentication Codes are 8 characters randomly generated by controller
- ✓ Manager has full control over remote access, e.g. s/he can…
  - provide and revoke remote access for a particular user without affecting other users' access
  - provide and revoke temporary access, for diagnostic or service analysis
- ✓ Can operate concurrently with BMS interface
  - BMS interface via MODBUS TCP/IP, BACnet, Metasys N2 or LonWorks protocol

System Description



EZConnect Operation

When EZConnect is enabled on a BECSys controller, that controller automatically contacts the secure BECSys EZConnect Server and registers its presence using the controller ID Number (for BECSys7, BECSys5 and BECSysBW the ID Number is the controller Serial Number; for BECSys RCM the ID Number is the Ethernet MAC Address). Manager-generated Authentication Codes are uploaded, which must be matched by every attempt to access the BECSys controller through the EZConnect system.

When a connection to the BECSys controller is attempted through BECSys for Windows PC software or the BECSys *Now!* mobile App, the secure BECSys EZConnect Server will verify that the requested controller is registered and authenticate the user by assuring the provided Authentication Code matches one from the customer-generated Authenticate Codes uploaded to the EZConnect Server for that controller. Only after passing these security checks will view-only access be granted to the controller; in order to make changes to the controller, the user must additionally possess and enter one of the Access Codes separately defined in the controller.

EZConnect can be disabled by the owner of the controller, in which case remote connectivity can still be provided to the BECSys controller using the traditional approach described in the Ethernet Application Note.

All information is transferred with encryption. Since the customer manages the Authentication Codes that provide access through the EZConnect system, s/he can withdraw or change an Authentication Code at any time, which will consequently terminate accessibility for anyone with that Authentication Code without affecting access for those using one of the other Authentication Codes.

Note that the controller IP address is not disclosed to those being granted access to the controller; this is an important benefit of the EZConnect security strategy.

EZMail Operation

When EZConnect is enabled, the operator also has the option to enable EZMail to send out email and text message alarm notifications. When EZMail is enabled the controller simply transfers alarm notifications to the EZConnect server via the existing secure EZConnect connection. The EZConnect server then passes the notifications to a dedicated email server maintained by BECS Technology exclusively for the purpose of transmitting alarm notification messages.

When EZMail is disabled, the controller can still send email notifications. However, valid SMTP settings will need to be configured and maintained in the BECSys controller as described in the Operator's Manual and the Alarm Notification Application Note. Note that if the email server information changes, it is the responsibility of the owner/operator to update the SMTP settings in the controller in order to continue to receive alarm notification emails/texts. Note also that email services (such as Gmail and Yahoo) may change their policies without notice, blocking alarm notification emails from BECSys controllers.

Security Layers

Message Encryption

All messages between the BECSys controllers, BECSys EZConnect Server, and the BECSys for Windows PC software and BECSys *Now!* App are encrypted with the industry standard TLS (Transport Layer Security) v1.2 cryptographic protocol, with all previous TLS versions (1.1, 1.0) and all SSL versions disabled. The only exception is the BECSysRCM, which uses AES-128 encryption. In addition to encrypting all data sent across the Internet, TLS also ensures that the EZConnect server contacted by the BECSys controller and the BECSys Application (BECSys for Windows software or BECSys *Now!* App) is the legitimate server operated by BECS Technology and not an imposter with potentially malicious intent.

BECSys Proprietary Communication Protocol and Applications

The protocol used by EZConnect and BECS' Applications has intentionally limited semantic capability, i.e. it only supports downloading logs and reading/writing parameters stored on the controller that deal with the controller's function as an aquatic controller. The protocol does not include any commands that can be used to interact with either the local network or the embedded operating system, and cannot be used to upload new software of any kind. Simply put, the communications through EZConnect cannot be used to give a malicious user access to the local network.

To manipulate the controller in controlling its body of water, a hacker would need to know this proprietary communication protocol, which is not published or shared, or reverse engineer it. Reverse engineering would be extremely difficult because communication is encrypted. Additionally the hacker would need to know the ID Number of the controller and possess a valid EZConnect Authentication Code to even gain access to a controller, since the IP address of the controller is not disclosed.

Only BECS-developed Applications are supported through the EZConnect system; there is no web-based interface to either the BECSys controller directly or the EZConnect Server. Web-based interfaces are easier for those with malicious intent to attack, since an interface to the system is readily available to anyone with a web browser. In contrast, the BECSys for Windows software and BECSys *Now!* App fundamentally limit the activities a user can perform.

Controller Access Codes

Every BECSys Controller has multiple levels of Access Code (Password) protection. When configured on the controller, any and all parameter changes can only be performed after the user has been granted one of these access levels. These Access Codes are enforced for both local (controller front-panel user interface) and remote changes, including remote access through the EZConnect system. This layer of security against unauthorized changes is completely controlled and managed by the owner/operator.

EZConnect Authentication Codes

The BECSys Controller maintains a list of EZConnect Authentication Codes, which identify users that have been authorized to access that controller remotely. Authentication Codes are 8-character alphanumeric values generated at random by the BECSys Controller. When the Manager wishes to grant someone external access, s/he provides that person with an Authentication Code that was generated by the BECSys controller. At any time in the future, that person's external access can be withdrawn by simply changing or deleting that Authentication Code. Manager and/or Rep Access Codes must be enabled (set) to view and/or modify the EZConnect Authentication codes in the BECSys7, BECSys5 and BECSysBW. On the BECSysRCM, Authentication Codes are only available through a USB connection or a local Ethernet connection.

Physical ROM Program Store

The processor core that performs the actual control functions in BECSys Controllers is a dedicated chip that reads its program only from a physical read-only memory (ROM). The only way to alter the code executed by this processor is to physically replace the program memory chip. This makes it extremely difficult, if not impossible, for those with malicious intent to subvert the fundamental control function by replacing the controller code (this is typically referred to as "hijacking").

BMS Support

Controllers with EZConnect can also concurrently interface with a Building Management System through an optional MODBUS TCP/IP protocol. BACnet, Metasys N2 and LonWorks protocols are supported via a protocol converter available from BECS. Security for any BMS connection is handled by the Building Management System. Connections to the controller via EZConnect maintain all security measures described above, even when a BMS interface is active.

Related Documents

Ethernet Application Note	.pdf	ENG-4604-DOC
Alarm Notification Application Note	.pdf	ENG-4588-DOC
R.D. Chamberlain, M. Chambers, D. Greenwalt, B. Steinbrueck, and T. Steinbrueck, "Layered Security and Ease of Installation for Devices on the Internet of Things," in *Proc. of IEEE Int'l Conf. on Internet-of-Things Design and Implementation*, 2016.	.pdf	Available upon request
BMS Application Note	.pdf	ENG-5508-DOC
BECSys for Windows Data Sheet	.pdf	ENG-4377-DOC
BECSys Gbit Ethernet Data Sheet	.pdf	ENG-6076-DOC
BECSys3 Water Chemistry Controller Data Sheet	.pdf	ENG-4261-DOC
BECSys5 Water Chemistry Controller Data Sheet	.pdf	ENG-4262-DOC
BECSysBW Automatic Filter Backwash Controller Data Sheet	.pdf	ENG-4264-DOC
BECSys7 Equipment Room Controller Data Sheet	.pdf	ENG-4263-DOC