

CYLON BEMS NETWORKING

This document describes networking within the Cylon Building Environment Management System (BEMS), in order to identify Security considerations and aid troubleshooting for Ethernet Networking on Cylon systems.

CYBERSECURITY DISCLAIMER:

This product is designed to be connected to and to communicate information and data via a network interface. It is your sole responsibility to provide and continuously ensure a secure connection between the product and your network or any other network (as the case may be). You shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, secure VPNs, application of authentication measures, encryption of data, installation of anti-virus programs, etc.) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB Ltd and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

Overview

Architecture -----	2
UnitronUC32 technology	2
Cylon BACnet technology	2

Networking

Summary -----	3
IP Network Interface -----	3
Connection	3
Communications Controllers	3
IP Traffic -----	4
UNET protocol	4
HTTP protocol	4
FTP protocol	4
Email protocol	4
Unitron protocol	5
BACnet/IP protocol	5
Platform -----	5
Platform Upgrade	5
Remote Access -----	5
Modem	5
IP	5
Other Devices -----	6
SiteGuide	6
Gateways	6



OVERVIEW

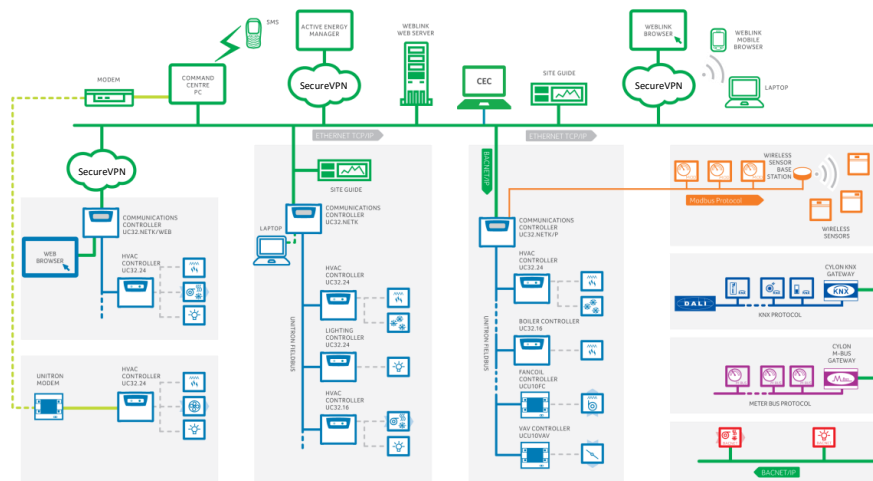
The **Cylon** BEMS uses standard IT interfaces/protocols in the same way as general IT networks (LAN etc.). The same type of general network integrity, reliability and security steps should be taken for the BEMS network as for an IT network.

However the BEMS networks tend to be isolated, use standard protocols with proprietary pay loads (less well-known, and so less prone to attack) and generally have less exposure/limited consequences if there is some kind of “breakdown”.

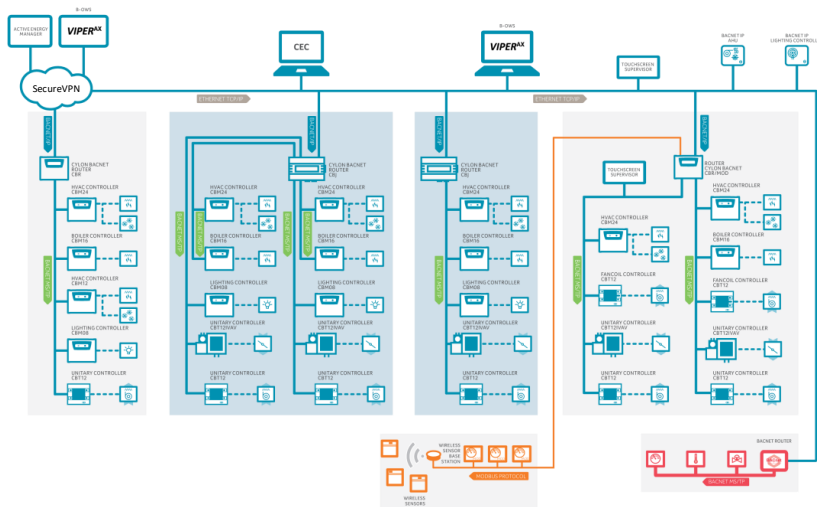
Architecture

The **Cylon** BEMS can be represented as follows:

UnitronUC32 technology



Cylon BACnet technology



Note: This document deals primarily with Unitron networking. Detailed information about BACnet networking can be obtained from <http://www.bacnet.org/>

NETWORKING

The communication between the Field Controllers is via priority protocols over serial RS485 links, and in general is not connected to other devices in a building (i.e. an isolated network).

The Communications Controllers communicate and allow access via an Ethernet based LAN. This typically is not isolated and can be connected to other devices on the “IT LAN”.

Summary

- Ethernet level: 100BASE-T
- Cable: Screened or Unscreened CAT5e
- Ports used:
 - 47808 (BACnet)
 - 4950 (**Cylon Engineering Center** connects to the controllers on this port – can be changed)
 - 80 (**eWeb** and **sWeb** supervisors)
 - 25 (**eWeb** email)
- Controllers must use fixed IP addresses
- Controller IP addresses must all be in the same subnet
- Controllers must be on an isolated network or VLAN, which has only BEMS devices connected to it.

IP Network Interface

Connection

- Ethernet level: 100BASE-T
- Cable: Screened or Unscreened CAT5e

Communications Controllers

- Use fixed/static IP address
- IP addresses must all be in the same IP Subnet

Recommendation

Communications Controllers must be on an isolated network or VLAN, which has only BEMS devices/traffic connected to it.

IP Traffic

The amount of “IP traffic” depends on the site setup – the number of Communications Controllers, Field Controllers, the Strategy operation, the number of Alarms, the number of wide global points, connected Cylon software, supervisors, Gateways etc. Both TCP/IP and UDP/IP based protocols are used.

UNET protocol

The **UNET** is the main communication link between the Communications Controllers (**UC32.netK** devices) on a site. This uses a standard UDP/IP socket connection between devices. Both broadcasts and peer to peer links are used on ports 64200, 64202 and 64204. In general **UNET** packets are “small” (compared to “normal” IT traffic).

■ Traffic:

- Heartbeat every 30s (UDP broadcast)
- Each wide out global point is serviced every 50ms (approx.) (UDP broadcast)
- Any new alarms are broadcast
- When connected to one **UC32.netK** and requesting data from another trunk then there will be UDP peer to peer traffic

HTTP protocol

The Communications Controllers (**UC32.netK**) have an embedded HTTP server. This uses port 80. Standard basic access authentication is used to control access to the web server.

■ Example usage:

- User/installer browses the built in status/configuration web pages on the Communications Controller (typically done at installation time)
- End user browses the **eWeb** (site supervisor functions) web pages on the Communications Controller (typically done by end users/supervisor on a site)

FTP protocol

The Communications Controllers (**UC32.netK**) have an embedded FTP server. This uses port 21. FTP login utilises a normal username and password scheme for granting access.

■ Example usage:

- Downloading **eWeb** HTML pages from the **Cylon Engineering Center** to a Communications Controller.

Email protocol

The Communications Controller s (**UC32.netKs**) have an embedded email client. This uses port 25.

■ Example usage:

- An Alarm event on a Field Controller can be configured to generate and send an email via the Communications Controller

Unitron protocol

The default **Unitron** communication port used on the Communications Controller s (**UC32.netKs**) is 4950. Third-party devices/**Cylon** software can make TCP/IP requests to the Communications Controller via this port.

■ Example usage:

- Downloading of strategy to a Field Controller from the **Cylon Engineering Center** (at installation time)
- Viewing of **eWeb** web pages from browser on PC (request from browser to Communications Controller)
- **sWeb** makes Unitron requests (in background) from PC to Communications Controller
- **UCC** Supervisor running get point values

BACnet/IP protocol

The Communications Controller (**UC32.netK/P**) can act as a Unitron to BACnet/IP gateway. The default BACnet port used is 47808, BACnet communication is over UDP/IP.

Platform

The Communications Controller is an Embedded System which runs on an ARM based microprocessor with 16 Mb DRAM, and 16 Mb Flash memory. There is also storage in battery-backed SRAM and a Real-Time Clock. The operating system used is **ThreadX** (designed for embedded systems). You cannot download and run executables.

Platform Upgrade

The application running on the Communications Controller can be updated using dedicated application running on a **Windows** PC. The application is supplied by **Cylon** and communicates via HTTP and FTP (username/password required).

Remote Access

For connection to the site from outside the building, Modem and IP connection are supported.

Modem

A PSTN/GSM modem can be used. This gives is a serial connection to the Communications Controller (or Field Controller). Only **Unitron** communication is used via this method.

IP

The "local IT" infrastructure can be setup to give access to the local LAN from the internet (NAT/VLAN)

Note: Appropriate security measures, such as VPN and Firewall are required when connecting a site to the Internet

Other Devices

SiteGuide

The **SiteGuide** is a touch screen “human machine interface” to the Unitron BEMS. It connects over the LAN (IP network) and communicates with the Communications Controller.

■ SiteGuideV1

The original **SiteGuide** uses **Unitron** requests to the Communications Controller. It uses an embedded **Linux** platform, with a 7” touch screen.

■ SiteGuideV2

The updated **SiteGuide** uses HTTP request to the Communications Controller. The platform is an embedded **Android** device with a 10” touch screen.

Gateways

These devices connect over the LAN (IP network) and communicate with the Communications Controller. They act as gateway devices between the Unitron system and other systems found in buildings (e.g. Managing lighting or interfacing with meters).

■ KNX Gateway

Uses **Unitron** requests to the Communications Controller, on a low-end embedded-system platform.

■ M-BUS Gateway

Uses **Unitron** requests to the Communications Controller, on a low-end embedded-system platform.