EAGLE Networking

White Paper

CENTRA LINE by Honeywell

TABLE OF CONTENTS

SCOPE

This document examines aspects of networking and network security Aspects relating to the EAGLE controller. It also contains a Network Integration Checklist.

It is intended to assist Honeywell Sales and Technical personnel in project coordination with the customer's IT department and operational staff.

RELATED DOCUMENTS

The related documentation can be accessed on the Honeywell docuserver via following link:

CentraLine EAGLE Technical Literature

Table 1. Related literature on Honeywell docuserver

Form No.	Title
EN2Z-0995GE51	EAGLE M-Bus and Modbus Whitelist
EN0Z-0978GE51	EAGLE PICS
EN0Z-0970GE51	EAGLE Product Data
MU1Z-0970GE51	EAGLE Mounting Instructions
EN1Z-0970GE51	EAGLE Installation and Commissioning Instructions
EN2Z-0971GE51	EAGLE Web Onboard HMI User Guide
EN2Z-0970GE51	EAGLE Web Interface User Guide
EN2Z-0937GE51	CARE User Guide
EN2B-0184GE51	Control Icons User Guide

Table 2. Additional related literature

Title
EBI_R310_Network_and_Security_Planning_Guide
EBI and/or SymmetrE BACnet PICS
Honeywell BACnet Architecture Best Practices

NETWORK SECURITY

Honeywell hereby expressly states that the EAGLE controller is not inherently protected against cyber attacks from the Internet and that it is therefore intended solely for use in private, protected networks.

Unprotected Internet connections can expose the EAGLE controller to cyber attacks from third parties who can then damage it and connected facility components or cause them to malfunction, or who can misuse it for illegal purposes for which the operator may then be held liable.

When directly connected to the Internet, the EAGLE controller automatically becomes a potential target for cyber attacks. Corresponding protective measures are therefore essential if safe and reliable operation is to be ensured.

If it is not necessary for the EAGLE controller to be accessible from the Internet, it should be operated in a closed network or be isolated from the Internet via appropriate IP port settings.

If it is necessary for the EAGLE controller to be accessible from the Internet (e.g., in order to allow for web-browser operation or perform remote maintenance), the use of a coded VPN connection is indispensable. Suitable VPN routers are available from numerous third-party manufacturers in a wide variety of designs, for operation at 230 V or 24 V.

Operating System

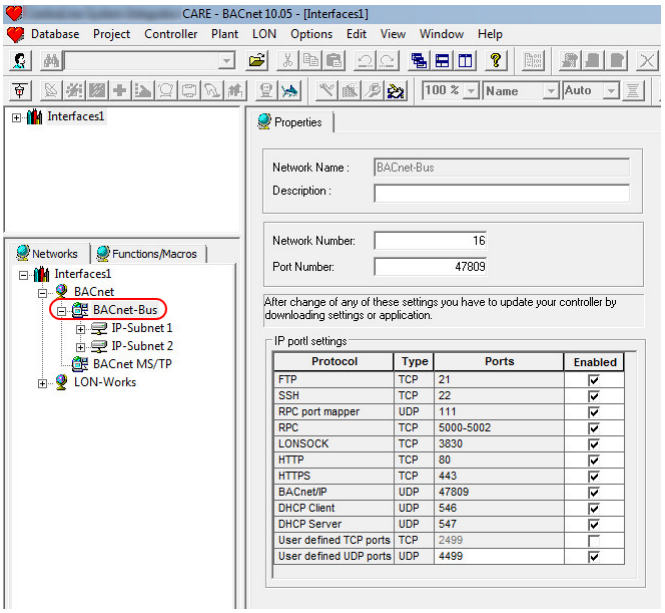
Until firmware 3.04.05, the EAGLE controller uses the Linux kernel version 2.6.33. Version 4.00.00 and higher has an upgraded kernel to 3.12.53.

Security Patches

Security patches are part of the firmware and can be loaded via the function “firmware download” of the CARE software.

IP Port settings

With the CARE tool (since version 10.04) it is possible to switch off not required ports or to enable additional ports.



The port for SMTP will be automatically added to the IP Port configuration.

Web Server

Until firmware 3.04.00 the Apache web-server is used.

Beginning with firmware 3.04.01 the Lighttpd web-server is used.

EAGLE uses the **web server** to provide a user interface based on HTML web pages. The controller does support secure SSL (Secure Socket Layer) connections (https://…).

There are two options to stop the server:

1.) the web server can be blocked for network access with the IP port settings. This can be done via the CARE tool. In this case, the web interface will still be accessible from the USB port.

2.) For extremely sensitive environments (e.g., military installations, pharmaceutical plants) the web server can

be stopped. This can be configured with the CARE tool in the controller properties.

The number of concurrent Internet Browsers accessing the EAGLE has no hard limit, but is dependent upon the load on the CPU created by BACnet communication and application cycle times. Additional Browser login trials will be disabled as soon as the CPU would otherwise overrun its performance criteria for BACnet communication and Application handling. In this case, a message will be displayed on the browser which will ask the user to try to login at a later point in time.

Ports Required

This section defines those ports which are required to be opened within a software or hardware firewall in order to enable functionality of programming and/or operating and/or debugging EAGLE controllers in a network, or from outside the network.

Secure Internet Browser Access – Port 443 (firmware 3.04.01 and newer)

Beginning with firmware 3.04.01 EAGLE can be operated via secure web-browsing (SSL) with Internet Browsers. This requires 443 to be opened in the network. If port 80 is open as well, then the browser will forwarded a http URL to https. (Port 80 is not really necessary if the user directly enters a https-URL).

Port 443 cannot be changed via the CARE tool, but can be changed using a config file on the controller. This also requires updating the configuration of the controller port settings in CARE.

Browser Access also allows for downloading trend data in "csv" format from EAGLE to the Client PC/Laptop.

The SVGA web-pages of EAGLE are compatible with the following web-browsers:

IOS:

● Safari

Android:

● Chrome

● Safari

● Firefox

PC

● Internet Explorer: Tested versions 9.0.x and 11.0

● Firefox: Tested versions 15.0.x and 29.0

● Google Chrome: Tested versions 35.019 and 36.0.1985.125

The Internet Browser must support the following requirements:

- HTML 4.01 supported
- CSS-1 supported
- JavaScript 1.3 supported
- DOM Level 1 supported
- Frames supported
- Full Screen supported

The QVGA web-pages are not working with https.

Internet Browser Access – Port 80

SECURITY NOTE:

Http was the only way to access web pages with controller firmware 3.03 and older, but starting from firmware 3.04.01, port 443 should be opened.

Since firmware 3.04.01 the port 80 is used by default to forward the browser to the https port.

If the port 443 is closed the browser can access the webpages with the port 80.

In this case the port can be changed in the controller using a config file on the controller; this also requires updating the configuration of the controller firewall.

EAGLE can be operated with Internet Browsers. This will require port 80 to be opened in the network.

Browser Access also allows for downloading trend data in "csv" format from EAGLE to the Client PC/Laptop.

The SVGA web-pages of EAGLE are compatible with the following web-browsers:

IOS:

● Safari

Android:

● Chrome

● Safari

● Firefox

PC

• Internet Explorer: Tested versions 9.0.x and 11.0

• Firefox: Tested versions 37.02

• Google Chrome: Tested versions 41.0.2272.118

The Internet Browser must support the following requirements:

- HTML 4.01 supported
- CSS-1 supported
- JavaScript 1.3 supported
- DOM Level 1 supported
- Frames supported
- Full Screen supported

The QVGA are disabled by default, but can be enabled if a XI882a is used.

QVGA web operation has been optimized for Internet Explorer for WIN CE 5.0

FTP Access – Port 21

SECURITY NOTE:

FTP had been necessary for controller firmware 3.02.00 and older, but CARE does not use it anymore because it is unsecure.

SSH Access – Port 22

NOTE: This port cannot be changed.

EAGLE supports secure shell connections, beginning with firmware 3.03.00. This allows secure console or FTP connection (SFTP, this is not to be confused with FTPS, which works totally differently) for firmware download, application download and troubleshooting via file upload.

With firmware 3.04.04 or newer, the access with SFTP is restricted (secure file access mode). Via Ethernet the standard file system is not accessible anymore.

BACnet Communication –Port 47808 (default)

In order to allow for communication with other EAGLE controllers (peer to peer) or 3rd party BACnet controllers (peer to peer) or with BACnet Clients (so-called "front-ends" like EBI, SymmetrE, or 3rd party), port 47808 (BAC0) must be opened.
Alternatively, the Honeywell CARE tool can be used to change the BACnet port to any port if required. It is, however, highly recommended to use the standard port 47808.
Some sites use "cross port" communication with different ports. This is not recommended.

Email Alarming / TLS – Port 587

The Honeywell CARE tool allows changing the TLS port to any port if required.

Sending emails is outbound traffic initiated by the EAGLE. TLS (Transport Layer Security) = Port 587 is the supported transmission and encryption security.
Due to cyber security vulnerabilities SSL 3.0 has started to become unsupported by some Email providers and hence is no more supported by EAGLE.

RPC Communication – Port 111, 5000, 5001, 5002

Starting with CARE 10.06.02, these ports are not required anymore and blocked by default in the IP port table.

LON Sock – Port 3830

NOTE: This port cannot be changed.

If you wish it to be possible to access EAGLE using the Honeywell CARE engineering tool, port 3830 must be opened.

NOTE: The CARE connection will make use of port 3830. This is proprietary communication in order to commission the device. This means that if CARE engineering is to be allowed from outside the network, network access has to be given accordingly.

BACnet Communication Settings

Please also refer to the EAGLE Communication Interfaces document for BACnet communication best practices and tuning.

If EAGLE controllers are to communicate with devices in other IP subnets, then the default gateway address must be set correctly. This is done using the Honeywell CARE engineering tool.

General

To start with, APDU (Application Program Data Unit) settings should be left as set by default in the Honeywell CARE engineering tool. Change these settings only if required and only after consulting the person responsible for the BACnet system integration.
If some EAGLE controllers of one CARE project are located on BACnet IP and some are located on BACnet MS/TP networks, then Max APDU Length should be set to 480 (CARE will automatically set Max APDU Length).

- Max APDU Length
- Max Segments accepted
- APDU Timeout

BACnet MS/TP

EAGLE needs the definition of the correct baud rate on a BACnet MS/TP net. If you don’t know the number of Max masters, leave it at the default of 127. The setting of Max Info Frames depends on the amount of messages which is sent by the device or through a router device.
It is recommended that a router be given the MAC address of "zero" and a higher number of Max Info Frames than other devices on BACnet MS/TP.

- Baud rate
- Max Masters
- Max Info Frames
- Window Size (is fixed to 16)

BACnet Routers

BACnet Routers may connect different BACnet Networks with different media. When, for example, devices in a BACnet MS/TP network communicate with EAGLE controllers on a BACnet IP network, then there may be restrictions to the APDU length. In this case, some Messages may not work.
It is recommended that Max APDU Length be set to the smallest APDU length in the network.
Refer also to section "Network Integration Checklist" for details.
BACnet Network numbers must be unique on the whole BACnet internetwork.

BACnet /IP Communication - NAT Routers

BACnet cannot be used over NAT routers.
The main workaround here is to use VPN; refer to “Honeywell BACnet Architecture Best Practices” for details on this solution.
Another workaround is to have a BBMD in the BACnet network, which is reachable over the internet. A remote

workstation can register itself as a foreign device with this BBMD.

Broadcasts

In a BACnet System, the below listed broadcasts are mandatory in order to allow BACnet Clients and Servers to identify each other.
Typically, these broadcasts are created upon start-up of a BACnet device or whenever the BACnet MAC address or the route to a device is unknown.

- "Who-Is" and "I-am" (used for identification of BACnet devices on the network)
- "Who-Is-Router-To-Network" and "I-Am-Router-To-Network" (used to identify BACnet routers on the network)

With EAGLE, "I-Am" messages in response to "Who-Is" messages are not broadcasted. They are sent as unicast messages to the device which issued the "Who-Is" request. This avoids sending the message into all BACnet networks and thus reduces network load in systems with many BACnet networks.
In addition, the EAGLE controller will create the following broadcasts as proprietary BACnet telegrams:

- User Synchronization, created upon change, deletion or addition of users. This will synchronize the user administration for browser access in all EAGLE controllers in the same (CARE) project on the network.
- BACnet Calendar Synchronization, created upon change, deletion, or addition of BACnet calendars. This will synchronize all BACnet calendars in all EAGLE controllers in the same (CARE) project on the network.
- Number of active Alarms in a controller.

The above synchronization messages are issued cyclically and whenever a change occurs. The cycle time of these messages can be configured in the CARE engineering tool. The synchronization of BACnet Calendars and Users can be switched off completely. This is recommended if there is only one EAGLE controller in a CARE project and it is not planned to add another controller. (Synchronization messages are not needed)
Alarm synchronization is used between all Excel Web controllers on the BACnet internetwork.
BACnet, Networks, Private Transfer Settings, Object synchronization max send time is the repeat time in minutes.
BACnet, Networks, Private Transfer Settings, Alarm synchronization max send time is the repeat time in minutes.

BACnet Broadcast Management Device (BBMD)

If a BACnet/IP Network spreads over different IP Subnets, then the use of BBMDs is required. Refer to section "Network Integration Checklist" for details.

Terminal Access

For troubleshooting, EAGLE allows terminal access on a dedicated serial port (serial port no. 1). Depending on the application, this serial port may be used to connect an M-Bus to the controller. The console output is then redirected to the SSH terminal.

Modem Access

EAGLE does not support modems.

Network Access via USB

The USB interface on the EAGLE allows establishing network connections with client PCs/Laptops for the following functionality and purpose:

- Access via Internet Browser
- Access via Honeywell CARE engineering tool

When connecting your PC to the USB port on top of the EAGLE controller for the first time, your PC will detect a USB network card and tries to install a driver for it. In the Honeywell CARE tool installation folder, there is a "Drivers" subfolder where you can find two *.inf files (one for 32-Bit and one for 64-bit Windows), which will direct the Windows driver to install to the correct drivers. Alternatively, you will need to have access to the Microsoft update server via the internet to be successful. The IP address of the EAGLE controller on the USB port is fixed to 192.168.255.241.
This IP address can be changed with a config file.

Wireless LAN

When installed in networks supporting wireless LAN, EAGLE can be operated via Wireless LAN.
Depending on the mobile unit, EAGLE can be operated via Internet Browser and/or engineered using the Honeywell CARE engineering tool.

Encryption

BACnet

BACnet communication is not yet encrypted. The current BACnet drivers do not yet support encryption.
The password for ReinitializeDevice or backup and restore is "<UserName>:<Password>". This string is openly transmitted via BACnet. The allowed users can be configured in the CARE application. All users with the access level "Building engineer" or higher can execute this function.
BACnet/IP can be used with VPNs.

Web Server

EAGLE supports encrypted communication (HTTPS) which is recommended for cyber security reasons. See also chapter "Certificate handling".

Internet Browser Login

Internet Browser login uses an authentication mechanism based on Session IDs and MD5 encryption. Neither User Name nor Password is openly transmitted over the network. Beginning with firmware 3-02-02, the MD5 encryption is using "salt", and the mechanism of creating the MD5 hash string for the password is improved significantly.
Browser login retry limit:
60 sec wait time after five wrong inputs.
If an input (correct or false) is done during the 60 sec wait time, 60 sec wait-time starts again.
There is an adjustable browser log-off timeout, which can be set in the Internet browser operation for EAGLE.

SFTP login

FTP login retry limit = 300 sec wait time after five wrong inputs.

SSH Login (firmware 3.03.00 and newer)

SSH login uses encryption for user name and password and for the transmitted data.
SSH login retry limit:
300 sec wait time after five wrong inputs.

Password Handling

Internet Browser Login

For the login with Internet Browsers, every user needs a user name and password.
The highest user level (SystemAdmin) needs a password which must consist of 5 characters minimum, which is defined in the Honeywell CARE engineering tool (CARE project login password).
When operating the EAGLE via Internet, it is highly recommended to use a "safe" password. By default, the CARE engineering tool will propose a "safe" password upon creation of an EAGLE project in CARE.

Certificate Handling (firmware 3.04.01 and newer)

For the https communication the two types of certificates are possible:

1.) Certificates issued by a trusted CA

SECURITY NOTICE!

Certificates issued by a trusted Certification Authority (CA) are mandatory for any controller that is facing the Internet.

2.) Self-signed end-entity Certificates

SECURITY NOTICE!

Self-signed certificates must not be used for internet-facing controllers, because they are not secure. Users may consider using self-signed certificates in secured networks, like VPN or closed networks, based on their own security assessment.

3.) Depending on the web-browser and on the version of the web-browser, web-browsers will display security warnings and/or display insecure connections, despite the SSL encryption is working. This is due to the following reasons:

- Self-signed certificates do not have the standard security of CA-signed certificates, because the Honeywell controller is no Certification Authority.
- The web-browsers do not trust the self-signed certificate and show an insecure connection.
- The users have to accept insecure connections, if they want to connect to the controller.

The following self-signed certificates are possible:

a) Self-signed startup certificate
At first startup the controller issues a certificate with the local IP address in the Common Name.
Once the IP address changes, this start-up certificate must be replaced: Ideally by a CA-signed Certificate.

b) Self-signed certificate configured by the Honeywell CARE tool.
CARE allows having the domain owner´s information entered and downloaded to the controller, which then will create and sign the certificate.

c) Certificate created by an OpenSSL tool (e.g. XCA)
OpenSSL tools allow creating a Root Certificate plus a Derived Certificate.
The advantage of the Root Certificate is that once it has been loaded into the web-browser, the web-browser will accept the Derived Certificates (which must have been loaded into the controllers beforehand), and no web-browser warnings will be issued.

Content of self-signed certificates:

Self-signed certificates must contain the information of the network domain owner, because, because the owner of the network domain is requesting and owning the certificate. (He has paid for the certificate along with - or in addition to - the job contract or service contract. In this contect see below table for typical questions and answers:

	CA-signed Certificate (CA = Certification Authority)	**Controller self-signed certificate**	**Self signed Root Certificate and Derived Controller Certificate**
		Do not use in Internet-facing controllers	
Question	**Answer**	**Answer**	**Answer**
Who requests the Certificate	**The owner of the domain.** The owner sends a Certificate Signing Request (CSR) to a CA	**The owner of the domain.** The owner or operator of the domain requests a self-signed certificate from Honeywell (Excel Web II).	
Who signs the Certificate	**The CA**	**Honeywell** The Honeywell controller	**The owner of the domain**
Who owns the Certificate	**The owner of the domain** The owner has bought the certificate	**The owner of the domain** The owner has bought the certificate along with (or in addition to) the job contract or service contract	
Benefit	**Secure** **No effort for web-users**	**No effort for the owner of the domain**	**Little effort for web-users**
Disadvantage	**Cost of certificate**	**Browser warnings** **Insecure**	**Create/Download Certs**

FTP Login (firmware 3.02.00 and older)

For the FTP log-in, three password levels exist:

- FTP User – a limited user which can only access one single directory
- Administrator – the Administrator password can be changed in the CARE project.

SSH Login (firmware 3.03.00 and newer)

For the SSH log-in, two password levels exist:

- SSH User – a limited user which can only access one single directory
- Administrator – the Administrator password can be changed in the CARE project.

Forgotten Passwords

The passwords for the Administrator and the Root user can be changed in the Honeywell CARE project. If the project is lost and the passwords are forgotten, the only way to recover a controller is to reset it to factory defaults. This can be done using the Honeywell CARE engineering tool with the USB interface.

NOTE: A reset to factory defaults will erase all application and all network settings. Only the default IP address for network access via the USB-B port will remain.

SNMP

EAGLE does not support the Simple Network Management Protocol.

NETWORK INTEGRATION CHECKLIST

1) Involve Customer IT department right from the start of the project concept phase.

2) Agree on System Integrator responsibility.

- Amongst others, this responsibility includes the coordination of tasks listed under points 3) through 9) below.

3) Get contact details of one responsible person per BACnet vendor that will integrate into the network.

4) Agree on level of BACnet Integration with customer.

- Work bottom up! Start with defining the minimum functionality required by the customer. Once this is achieved, try to enhance the interoperability.

5) Check BACnet Interoperability of all BACnet devices that need to be integrated.

- Compare BACnet “PICS” of all products to be integrated:
  - Do all devices use the same character set, e.g., ANSI X 3.4 or ISO Latin 1?
  - Limit interoperability requirements to those BIBBs that are mandatory for a BACnet Client and a BACnet Server to interoperate. Be aware that most job specifications define more BIBBs on Client/Server side that are necessary for interoperation, or for the needed functionality of the system. Remember that BIBB A on the Client-Side must equal BIBB-B on the Server side.
  - Agree on the notification class settings on the jobsite. For 3rd party integrations following settings and properties needs to be aligned in the system:
    - Does the BACnet client automatically subscribe to recipient-List, or does the client have to be manually added to the CARE project?
    - Instance number of the notification classes
    - Name of the notification classes
    - Priortities
    - Ack-Required
  - Check for the following fall-back mechanisms in the BACnet client devices. If these fall-back mechanisms exist, a BACnet client device will be able to interoperate with nearly any BACnet server device:
    - Does the BACnet client make use of polling with “ReadProperty” if the BACnet server does not support “COV”? Typically, BACnet MS/TP devices do not support COV reporting.
    - Does the BACnet client make use of “ReadProperty” if the BACnet server does not support “ReadPropertyMultiple”?
    - Does the BACnet client make use of “ReadProperty” with ArrayIndex if the BACnet server does not support “ReadProperty” of the complete Array (e.g., because of APDU size restrictions)?
  - Verify that the "CreateObject" is done in a way supported by the BACnet server device. Not all properties can be defined in CreateObject message.
  - Check if the BACnet client is able to read and write the schedules and calendars.
  - Check if the BACnet client is able to read the trend logs from the controller.
  - Verify how lists are written: Is "WriteProperty" used in order to write the complete list, or is "AddElement" used in order to write single entries in the list?
  - Verify how arrays are written: Is the array size set and are single elements written, or is the complete array written?
  - Verify the version of the BACnet standard that is supported: Typically, BACnet devices supporting the version 135-2001 are not compatible with BACnet devices supporting version 135-2004. In this regard, the most critical areas are schedules and trend, because here the 135-2004 version has defined many enhancements which are not compatible to the 135-2001 version.
- BTL-Listed products have been successfully testing for compliance with the BTL test plan. However, BTL-listed products will not guarantee interoperability in every detail, and BTL-listed products will not replace the detailed checks that are outlined in this document.

6) Inform yourself about the customer's network security concept.

- Are there any V-LAN‘s (Virtual LAN's) designed? Will you get a V-LAN only for BACnet?

7) Agree upon – or inform yourself about – network infrastructure.

- Network structure and media
- Per HVAC electrical panel a network switch (ideally panel-rail mounted) should be installed in order to allow parallel network access for EAGLE to the

BACnet network, for an Internet Browser (e.g., Touch-panel operator unit), and for a laptop (CARE start-up and downloads, debugging via FTP)

- Responsibility of network installation
- When you have V-LAN's keep in mind that, maybe, you must send information from one to the other V-LAN (for reference points).

8) Agree on BACnet networking issues.

- Are all BACnet devices talking BACnet IP or BACnet MS/TP?
- Who provides the necessary routers for BACnet routing in the network?
- Get IP addresses (or address range) from the Customers IT group and allocate IP addresses (or an address range) to every vendor.
- Define only one BBMD (BACnet Broadcast Management Device) per IP subnet.
- Define only one BACnet router between two BACnet networks (tree structure of networks. There is always only one path between two devices).
- BACnet network numbers must be unique in the whole BACnet internetwork.
- Agree on common network number for BACnet/IP.
- Define ranges for network numbers for remote busses (e.g. BACnet MS/TP) for each vendor.
- Agree on Time Master functionality (typically, this is one BACnet front-end) and the time synchronization method, i.e. Standard or UTC (UTC stands for Universal Time Code and includes time zone information).
- Make BACnet traffic estimation, based on number of points and refresh rate of these points on the BACnet front-end.
- Agree on a common BACnet/network diagnostic tool to be used by all vendors and be the customer. (Typically, this could be the Cimetrics "bas-o-matic" tool or "wireshark" (recommended). Check to determine which BACnet clients are used for checking and troubleshooting, e.g. Cimetrics "BACnet Explorer", Cimetrics "OPC Server")

9) Agree on addressing conventions for BACnet devices.

- A BACnet device is either a BACnet client (e.g., EBI, SymmetrE, or 3rd party front-end like Siemens Desigo), or a BACnet server like EAGLE or 3rd party like Siemens PXC controllers.
- Allocate unique device names.
- Allocate BACnet Device IDs to every vendor.
- In a BACnet network, the Device ID needs to be unique. These could be based, for instance, on the IP address range. For EAGLE, the Device ID equals the controller number and can be freely defined if the automatic CARE allocation mechanisms should not be used.

NOTE: CARE allows free allocation of Device IDs between 1 and 4194302 (4.194.302)

- Some customers have gotten the idea to define the Object ID (=instance) of a BACnet device. This is of no use for the system operator or for the IT department, but sometimes required by the customer for whatever reason. As per BACnet standard, the smallest Object ID (lowest number) for a BACnet device is 33554433. (The BAcnet formula is: Object ID = Device ID (=instance) + 33554432. You can create specific Object IDs for BACnet devices in CARE, by allocating specific Device IDs:

Example: Customer wants an Object ID of 3700000
You enter the following Device ID in CARE:
Device ID = Object ID - 33554432 = 37000000 - 33554432 = 3445568

NOTE: The highest possible Object ID that can be created in CARE is 37748734.

This will allow you to have (37748734-33554432) = 4 Million 194 Thousand and 302 Honeywell BACnet devices in one system, which will be sufficient for most installations.

10) Agree on naming conventions for BACnet data-points

- Agree on naming conventions for data-points names (key names), schedules, and calendars.

NOTE: Object IDs for data-points, schedules, calendars and trends cannot be freely allocated! Rather, this is done automatically by CARE in order to ensure that these Object IDs are unique on a (CARE) project wide basis! When using CreateObject service to create schedules, calendars and trends Object IDs can be freely defined.

- Agree on the use of a unique character set for the project (EAGLE can support UTF-8, ISO 8859-1, or ISO 10646 (UCS-2). If there are workstations which use ANSI X3.4, then select UTF-8 and avoid characters which are not defined in ANSI X3.4).

11) Verify application-specific BACnet issues

- Switching priorities for outputs and analogue value objects (Typically, priority "8" is used for manual operator overrides via BACnet front-ends or operator units, priority "1" is used for manual overrides at the input/output module)
- Agree on used notification classes, its settings (ack required, transition event priorities), and the mechanism how the recipients will be added.
- Agree on the alarm transition reporting (to off_normal, to_normal, to_fault) for every data-point.
- Agree on alarm priorities (priorities of the BACnet notification classes)
- Agree on the event types (event or alarm) for every data-point.

12) Verify Honeywell CARE engineering tool related application issues

- Check to which 3rd-party BACnet devices the EAGLE needs to write and from which it needs to read. Verify if all LonWorks parameters of XL10/12 devices that

the customer wants to change ONLINE are supported by EAGLE / CARE – see “nvs_supported.xls” spreadsheet on the GE51 docuserver.

13) Plan BACnet/MSTP networks

- Maximum number of devices per MS/TP segment Calculate the load or limit the number of devices per network segment to 32. Consider using repeaters or further MS/TP networks. Not all repeaters may be suitablefor BACnet.
- Group devices which need to communicate much data between each other on one MS/TP network.
- Cabling:
  - Twisted pair / with or without shield / with or without ground (one side ground connection only).
  - Use of isolated port or electrically coupled port.
  - Cable length.
- Baud rate: EAGLE controllers need the definition of the correct baud rate but they are able to communicate with other controllers which do support auto-bauding or auto-configuration.
- Topology.
  - No star topology; use a line.
  - Not too many bias resistors.
  - Bus termination at both ends of the line.
- Agree on MAC addresses on MS/TP networks.

USEFUL LINKS

Honeywell Technical Assistance Portal GE51

http://web.ge51.honeywell.de/tac/
(Includes links to Best Practices, FAQ, CE/UL Certifications, Software Download, Product Documents, E-Catalogue, etc.)

IP Port Numbers List

http://www.iana.org/assignments/port-numbers

BACnet International Association

http://www.bacnetinternational.org/

BACnet Interest Groups Worldwide

http://www.bacnet.org/Contact/Groups.htm

BACnet Interest Group Europe

http://www.big-eu.org

Manufactured for and on behalf of the Environmental and Energy Solutions Division of Honeywell Technologies Sàrl, Rolle, Z.A. La Pièce 16, Switzerland by its Authorized Representative:

CentraLine
Honeywell GmbH
Böblinger Strasse 17
71101 Schönaich, Germany
Phone +49 (0) 7031 637 845
Fax +49 (0) 7031 637 740
info@centraline.com
www.centraline.com

Subject to change without notice
EN2Z-0992GE51 R0117