Greetings to you all. Very happy to connect with you all again. I attended a very exciting and interactive Strategic Leadership Meet (SLM) at Charlotte, NC in May 2019 and we all had a very productive session. Our Vice President of Industries & Sciences, Graham Nasby shared some details in Page 2. ISA has released Strategic Framework in June 2019 which gives clarity of direction to move forward. Governance & Membership Team is working on a new platform “ISA Connect” and is expected to be rolled out by early 2020. This will be a game changer in networking among ISA members and professionals.

With clarity in strategic growth plan for ISA and very interactive “ISA Connect” platform, ISA members can expect exciting networking engagement and professional interaction adding more value to your membership in future. As Building Automation Professionals, we will have to collectively play an active role in creating a better world through automation in Building Technologies.

I invite the recipients of this newsletter to help us to bring all the professionals engaged in Building Automation Systems under BASDIV, ISA umbrella and strengthen our professional networking. We require more volunteers in various leadership roles to support in our journey. I request all those willing to be part of this journey to email with your details and domain you want to contribute.

The focus of the Building Automation Systems Division (BASDIV) of ISA is:
1. To bring together the professionals connected with BAS Technologies like the technologists, service providers, manufacturers, system integrators, building architects and building developers etc.
2. To share the knowledge in this complex and multidisciplinary domain and maximize utilization of this technology for improved energy management, occupants’ comfort & safety.
3. To create a greater number of certified system designers, engineers and technicians with the required skill set to handle successfully the BAS Projects all over the world.

If you are connected with Building Automation Systems in any capacity as practicing engineers, end users, solution providers, students interested in BAS, Architects, Builders etc.

Join ISA and BASDIV for professional networking
https://www.isa.org;
https://www.isa.org/basdiv

For queries email to: rathan@rsbizconsultant.com
In May 2019, senior leaders from all of the various committees within the International Society of Automation (ISA) gathered in Charlotte, North Carolina, USA to talk about the future strategic direction of the society. Lead by ISA's 2019 society president Paul Gruhn and the Executive Board, the ISA is in the midst of a significant realignment as it looks at how to better serve the needs of industry and its members. The Strategic Leadership Meeting, on May 17-20 last month was major part of this process.

Building on an initiative that began early 2018, the board has been hard at work with various working groups to identify an updated vision, mission and set of values for ISA.

In May 2018, the society’s new vision of “Create a Better World through Automation” was announced, which was then soon followed up by an updated mission statement of “Advance technical competence by connecting the automation community to achieve operational excellence”. Rather than just focusing on technologies and applications, as had often been done in the past, the board felt it was important to emphasize automation’s role in achieving operational excellence. The board also recognized the importance of developing automation professionals, at all points during their careers, in order to ensure we are making the best use of our human capital when it comes to building excellence in operations.

Most recently, the board has led several workshops at both 2018 Annual Leadership Conference and 2019 Strategic Leadership Meeting. The result of these workshops has been the development of a new ISA Strategic Framework, which was released in June 2019.

This new strategic framework for ISA, along with its objectives, will be now be used to frame the upcoming work by the board and senior ISA leadership about how to move forward in terms of targeted goals, tactics and programs.

Technical divisions, such as the Building Automation Systems Division, have an important role to play as ISA develops its newest strategies to engage and support the industries that we as Automation Professionals are involved with on a daily basis.

I invite you to follow the blogs on www.isa.org, to learn more about ISA’s work and efforts towards its new strategic vision.

Graham Nasby, P. Eng., PMP, CAP
ISA Vice-President of Industries and Sciences

ISA News:

ISA is excited to be launching a new member benefit in the coming year, ISA Connect.

This online discussion community, exclusively for members, will be your go-to source to engage in technical conversations and share best practices.

ISA Connect will provide members the ability to:

- Network and communicate with members around the world.
- Post, subscribe to, and follow technical discussions.
- Share and access resources in the technical library.
- Discover opportunities to get involved in ISA.

We are excited to offer new ways for members to cultivate professional relationships, engage in technical dialogue and develop the ISA community.

Karen Modrow
Membership and Community Manager
ISA, NC, USA
ISA Strategic Framework

`Guides us down a path
Creates continuity and sustainability
Sets priorities and allocates resources
Is compelling`

VISION ➤ Aspirational statement of how the organization will impact the future
Create a better world through automation

MISSION ➤ Reason we exist, who we serve and how we serve them better than anyone else
Advance technical competence by connecting the automation community to achieve operational excellence

VALUES ➤ Guiding principles for the leadership and staff
Excellence, Integrity, Diversity and Inclusion, Collaboration and Professionalism

OBJECTIVES ➤ Major accomplishments for our core programs set by the Executive Board for the 3-year horizon

- **Industry Reach & Awareness**—Establish and advance ISA’s relevance and credibility as the home of automation by anticipating industry needs, collaborating with stakeholders, and developing and delivering pertinent technical content.
- **Membership Development & Engagement**—Enhance member value and expand engagement opportunities to nurture and grow a more diverse and global community to advance the automation profession.
- **Technical Education & Certification**—Become the recognized leader in automation and control education, providing training, certifications, and publications to prepare the workforce to address technology changes and industry challenges in the most flexible and relevant ways.
- **Leadership & Business Skill Development**—Create opportunities for members to improve critical leadership skills, to build a network of industry professionals, and to develop the next generation of automation professionals.

GOALS ➤ Specific, measurable, attainable, relevant, and timely milestones aimed at advancing the objectives

TACTICS ➤ Methods and plans that include assignments, accountability, and deadlines

KPIs ➤ Quantifiable key performance indicators
What is Cybersecurity

Cyber security refers to a set of techniques used to protect the integrity of networks & the protection of internet-connected systems, including hardware, software and data from attack, damage or unauthorized access.

Why Cybersecurity Is Required

The core functionality of cybersecurity involves protecting information and systems from major cyberthreats like Cyberterrorism, it is the disruptive use of information technology by terrorist groups. Cyberwarfare involves nation-states using information technology to penetrate another nation’s networks to cause damage or disruption. Cyberespionage is the practice of using information technology to obtain secret information without permission from its owners or holders.

Elements of cybersecurity

Ensuring cybersecurity requires the coordination of efforts throughout an information system, which includes: Application security, Information security, Network security, Disaster recovery/business continuity planning, Operational security, End-user education. One of the most problematic elements of cybersecurity is the constantly evolving nature of security risks. The traditional approach has been to focus resources on crucial system components and protect against the biggest known threats, which meant leaving components undefended and not protecting systems against less dangerous risks.

Types of cybersecurity threats

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. However, it’s necessary in order to protect information and other assets from cyberthreats, which take many forms. Ransomware is a type of malware that involves an attacker locking the victim’s computer system files. Malware is any file or program used to harm a computer user, such as worms, computer viruses. Social engineering is an attack that relies on human interaction to trick users into breaking security procedures. Phishing is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources.

What cybersecurity can prevent

The use of cybersecurity can help prevent cyberattacks, data breaches and identity theft and can aid in risk management. When an organization has a strong sense of network security and an effective incident response plan, it is better able to prevent and mitigate these attacks. For example, end user protection defends information and guards against loss or theft while also scanning computers for malicious code.

How to Maintain Effective Cybersecurity

Historically, organizations and governments have taken a reactive, “point product” approach to combating cyberthreats, cobbling together individual security technologies – one on top of another – to protect their networks and the valuable data within them. Not only is this method expensive and complex, but news of devastating cyber breaches continues to dominate headlines, rendering this method ineffective. Instead, organizations can consider a natively integrated, automated Next-Generation Security Platform that is specifically designed to provide consistent, prevention-based protection – on the endpoint, in the data center, on the network, in public and private clouds, and across SaaS environments. By focusing on prevention, organizations can prevent cyberthreats from impacting the network in the first place and reduce overall cybersecurity risk to a manageable degree.

To deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach. The National Institute of Standards and Technology (NIST), recently issued updated guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments. The voluntary cybersecurity framework, developed for use in the banking, communications, defense and energy industries; can be adopted by all sectors, including federal and state governments.
Cyber security in building automation systems

No system in the world is completely cybersecure, but there are best practices that can make your building network safer.

Three key principles to secure building networks

When securing the building network, there are three key principles to keep in mind: isolation, observability and controllability.

To isolate sensitive data and keep it secure, create trusted islands, whether physical or logical. Air gaps, where two networks are completely separated. Another approach is to create completely physically dedicated networks. There may be cost trade-offs to these security strategies, but isolating is one way to ensure a vulnerable network won’t open the door to sensitive assets.

Observability means knowing about anomalies on the network. Be aware of what is happening in the network, and when it has been compromised. There are many ways to get reports on link status and user logins in your building network. Put these systems in place to identify malicious activity on the network.

Controllability entails managing access to the network. Set proper passwords, refresh them, and use authentication. Be sure to renew or delete accounts, as necessary, so it is clear exactly who has access to network systems. No one should be able to get into the network without the manager’s knowledge.

Take Basic Action Today

Cybersecurity does not need to be overwhelming or difficult. For the most part, cybersecurity is about thinking logically and strategically. A few alterations can be made to the network immediately. Above all, implement policies and procedures that are based on the CIA Triad of confidentiality, availability and integrity. The Internet of Things (IoT) is very predictable and well-behaved, so use this to your advantage. Develop policies and procedures that will keep sensitive assets secure in the case of a cyberattack or threat. Look at realistic ways to isolate networks. Consider isolating building systems from IT, for example. Use a dedicated building network, with separate virtual local area network (VLAN) for each service provider and vendor. Isolation is a straightforward way to limit connections between vulnerable networks and confidential data. Observe what is happening on the networks. It is important to understand how the network normally behaves and to recognize anomalies. Ask for regular reports on the number of connected devices and number of disconnected ports, track of and manage who has access to your server.

Conclusion

Network hacking is a serious, growing threat that needs to be addressed by proper cybersecurity. Smart devices bring immense benefits to our daily lives, but we must understand how to properly secure them. No one wants to see their building in the news for some catastrophic hack and leak of information. Implementing some of these best practices is the first step in safeguarding against cyberattacks.

IEC 62443, formerly known as ISA 99, is the global standard for the security of Industrial Control System (ICS) networks and helps organizations to reduce both the risk of failure and exposure of ICS networks to cyber threats. This standard was produced by the International Society of Automation (ISA) and taken over by the International Electrotechnical Commission for further development. The framework of this standard guides operators of ICS networks through requirements, controls and best practices necessary for a secure industrial network.

See next schematic for Cyber Security Levels:

Sheshagiri Nayak

Country Liaison India, BASDIV, ISA
Asst. Vice President (Automation & Robotics)
Godrej & Boyce Mfg Co Ltd, Mumbai, India. Contact: seshu@gdrej.com

References:

- ISA /IEC62443 Guideline Cybersecurity
- ISO/IEC 27001 Information Security System
Buildings are becoming more and more advanced and the demands on building services are increasing. Building Automation is changing from local BMS to remote management of multiple buildings. The different control systems are becoming smarter for building predictive maintenance. Smart Sensors become the basic part of this change. The current analog sensors must change in view of huge cabling required to connect and as well for remote health monitoring. These smart sensors shall have networking feature with wired or wireless media. The internet of things is becoming very relevant for the new buildings for a common remote building management solution integrated with Information Technology. The IT/OT integration with AI and Analytics. The key areas for Building Management are all energy hungry and need to be managed very efficiently. For this we need to manage different types of sensors for the different applications.

The SMART Buildings, there is very essential to manage all areas with common system and as such need standard protocols for sensors and controller for integration.

The Sensor Data and data from associated controllers are very essential for analytics and artificial intelligence for cost effective solution and user convenience.

Smart buildings also need standard networking infrastructure with serial, Ethernet and wireless for handling automation. A smart building uses digital control systems to manage the comfort, operational and energy HVAC, Lighting, Safety and Security requirements.

Sensors form the basic unit of any such automated system

The commonly used protocols for inter communication are Modbus, BACnet, Bluetooth, KnX, Zigbee, Industrial Ethernet, HART, Proﬁbus.

The Physical media for Communication network is generally RS485 multi drop and Ethernet IP, Wi-Fi and as well in special cases power line Ethernet. Normally Ethernet adds cost and hence sensors are mostly on RS485.

For ease of installation for greenfield and as brown field systems wireless sensors are a big advantage. Wi-Fi, Bluetooth, ZigBee, Lora are being used for communication. Bluetooth is very low-cost network and is now being adopted multiple building automation solutions like Lighting control etc.

RS485 Network:

RS-485 network allows devices (up to 256) to communicate at half-duplex on a single pair of wires, plus a ground wire. Both the length of the network and the number of nodes can easily be extended using a variety of repeater products on the market.

Network topology is probably the reason why RS485 is the favorite of the serial interfaces in data acquisition and control applications. RS485 is the only of the interfaces capable of internetworking multiple transmitters and receivers in the same network. Currently available high-resistance RS485 inputs allow this number to be expanded to 256. RS485 repeaters are also available which make it possible to increase the number of nodes to several thousands, spanning multiple kilometers. It is the reason why RS485 is so popular with computers, DDC, PLCs, micro controllers and intelligent sensors in scientific and technical applications. In the picture below, the general network topology of RS485 is shown.
N nodes are connected in a multipoint RS485 network. For higher speeds and longer lines, the termination resistances are necessary on both ends of the line to eliminate reflections. Use 100 Ω resistors on both ends. See Table 1.

<table>
<thead>
<tr>
<th>Characteristics of Serial Networks</th>
<th>RS232</th>
<th>RS422</th>
<th>RS485</th>
<th>USB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Differential</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>Max Drivers and Receivers</td>
<td>1</td>
<td>1</td>
<td>256</td>
<td>1</td>
</tr>
<tr>
<td>Network Topology</td>
<td>Point to Point</td>
<td>Multi Drop</td>
<td>Multi Drop</td>
<td>USB serial Network</td>
</tr>
<tr>
<td>Max Distance</td>
<td>15m</td>
<td>1200m</td>
<td>1200m</td>
<td>5m, extended with hubs</td>
</tr>
<tr>
<td>Max Speed at 12 m</td>
<td>20kbs</td>
<td>100kbs</td>
<td>10mbps</td>
<td>450 Mbs</td>
</tr>
</tbody>
</table>

**TABLE 1**

**Wireless Sensor Network**

Today, smart grid, smart homes, smart water networks, intelligent transportation, are infrastructure systems that connect our world more than we ever thought possible. The common vision of such systems is usually associated with one single concept, the internet of things (IoT), where through the use of sensors, the entire physical infrastructure is closely coupled with information and communication technologies; where intelligent monitoring and management can be achieved via the usage of networked embedded devices.

In such a sophisticated dynamic system, devices are interconnected to transmit useful measurement information and control instructions via distributed sensor network. With advent of IoT the Control and monitoring architecture for building is undergoing a big change. A typical architecture is shown in Picture 3.

A **wireless sensor network (WSN)** is a network formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc. WSNs are regarded as a revolutionary information gathering method to build the information and communication system which will greatly improve the reliability and efficiency of infrastructure systems. Compared with the wired solution, WSNs feature easier deployment and better flexibility of devices. With the rapid technological development of sensors, WSNs will become the key technology for IoT.

![Picture 3](image-url)
A **WSN** can generally be described as a network of nodes that cooperatively sense and control the environment, enabling interaction between persons or computers and the surrounding environment. WSNs nowadays usually include sensor nodes, actuator nodes, gateways and clients. A large number of sensor nodes deployed randomly inside of or near the monitoring area (sensor field), form networks through self-organization. Sensor nodes monitor the collected data to transmit along to other sensor nodes by hopping. During the process of transmission, monitored data may be handled by multiple nodes to get to gateway node after multi-hop routing and finally reach the management node through the internet.

![Diagram of WSN](image)

**Picture 4**

### Sensor nodes

**The sensor node** is one of the main parts of a WSN. The hardware of a sensor node generally includes four parts: the power and power management module, a sensor, a microcontroller, and a wireless transceiver, see Figure below. The power module offers the reliable power needed for the system. The sensor is the bond of a WSN node which can obtain the environmental and equipment status. A sensor is in charge of collecting and transforming the signals, such as light, vibration and chemical signals, into electrical signals and then transferring them to the microcontroller. The microcontroller receives the data from the sensor and processes the data accordingly. The Wireless Transceiver (RF module) then transfers the data, so that the physical realization of communication can be achieved.

It is important that the design of the all parts of a WSN node consider the WSN node features of tiny size and limited power.

**With costs of microcontroller** and new sensors coming down, the building automation technology is changing; apart from building control and monitoring the control systems also being ministered and diagnosed for their health. This making the buildings management more predictable.
MODBUS

Modbus is an open protocol designed and developed by Modicon, acquired in 1979 by Schneider Electric. Initially it was designed for industrial application to share data within various equipment. In 2004 it become de facto standard, widely used in various industry which includes Building Automation System. The Modbus protocol adopts client/server model to manage communication between master and several slave devices. The master can be automation server/station and slave can be chiller, power meter and UPS.

OSI Model

![Modbus OSI Model](image1)

Application

The Modbus protocols is one of the robust protocols in the market and adapted in various application to share data such as power meters, chillers, variable speed drives (VSD) and UPS.

Highlights

- Modbus RTU
  - Network topology must me in daisy chain.
  - Twisted pair, shielded cable AWG 22. Suggested type Belden 3106A/3107A.
  - Cable length should not exceed 1000m.
  - Maximum number of slaves to master should not exceed 124.
  - Repeater must be added on every 31 slaves per communication port.

- Modbus TCP/IP
  - Network topology can be star, ring or mixed.
  - Unshielded-Twisted Cable (UTP) such as category 5, 5e, 6 with RJ45 connector.
  - Cable length should not exceed 1000m.
  - Maximum number of TCP/IP device must not exceed 100 per Automation server.
  - Maximum number of TCP/IP gateway must not exceed 10 per Automation server.

Standards

- International de facto standard.

Software License

- No fees.

BACnet

BACnet stands for Building Automation Control System Network, specifically designed for building services industry by American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). These services include control and monitoring of Heating, Ventilation, Air-Conditioning and Refrigeration (HVAC & R) equipment, Lighting control system, access control system, fire alarm system, lift system and electrical services.

The BACnet is an international standard adapted by 800 vendors around the world and maintained by ASHRAE standard project committee 135.

OSI Model

![BACnet OSI Model](image2)

Application

The BACnet protocols is exclusively developed/designed for Building automation/service industry. This protocols widely used in building services equipment such as chillers, variable air volume (VAV) system, variable speed drive (VSD) and smart room sensors.
### Highlights
- **BACnet MS/TP**
  - Network topology must be in daisy chain.
  - Twisted pair, shielded cable AWG 22 – 24 low capacitance Suggested type Belden 9841.
  - Cable length should not exceed 1,200m.
  - Maximum number of slaves to master should not exceed 64.
  - Repeater must be added when networks contains more than 64 controllers or cable length exceeds 1,200m.

- **BACnet TCP/IP**
  - Network topology can be star, ring or mixed.
  - Unshielded - Twisted Cable (UTP) such as category 5, 5e, 6 with RJ45 connector.
  - Cable length should not exceed 1000m.
  - Maximum number of TCP/IP device must not exceed 254 per Automation server.

### Standards

### Software License
- No fees.

### LonWorks

Local Operating Networks is abbreviated as Lonworks, one of the widely used communication protocols in the building automation industry. It was developed by Echelon in 1988 and recognized by ANSI in 1999. The protocols conform to the ISO/IEC 14908 worldwide. Lonworks is supported by Lonmark international and adapted by more than 400 companies worldwide.

### OSI Model

<table>
<thead>
<tr>
<th>OSI Model</th>
<th>Lonworks Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Neuron C Program</td>
</tr>
<tr>
<td>Presentation</td>
<td>Network Variable</td>
</tr>
<tr>
<td>Session</td>
<td>Network Management</td>
</tr>
<tr>
<td>Transport</td>
<td>Message Service</td>
</tr>
<tr>
<td>Network</td>
<td>Addressing &amp; Routing</td>
</tr>
<tr>
<td>Data Link</td>
<td>Media Access</td>
</tr>
<tr>
<td>Physical</td>
<td>Physical Connection</td>
</tr>
</tbody>
</table>

### Application

Lonworks is peer-to-peer protocol and can run on twisted pair, ethernet or powerline. The Lonworks protocols are very common in building services and adapted in various equipment's such as variable air volume (VAV) system, variable speed drive (VSD) and smart room sensors.

### Highlights
- **Lonworks TP/FT-10**
  - Network topology: Free topology. Daisy chain, star or mixed topology.
  - Twisted pair cable 2 Conductor 16AWG, Tinned Copper Suggested type Belden 85102.
  - Cable length should not exceed 500m node to node.
  - 64 devices can be connected to a segment of up to 2,700m long.

### Standards
- ISO/IEC 14908 – Worldwide
- EN 14908 – Europe.
- ANSI/CEA-709/852 – USA.

### Software License
- Fees applicable – Paid by product manufacturer.

---

**Noorul Hassan.** PEM has over 18 year of diverse experience in HVAC, Electrical and Building Automation system. He involved in wide variety of energy management, system optimization and building automation projects. He previously served as electrical design engineer for SKM equipment, Building Automation System Design Engineer for Sauter Middle east. Currently he is working as Building Automation System Service Engineer for Schneider Electric Building Australia. He is a Certified Professional Energy Manager (PEM).

Contact: noorulhassanus@yahoo.com
What you need to know about BACnet in 6 Steps

By Orlando Pezantes
Automation Specialist

1. What is BACnet?
   BACnet is a Building Automation and Controls Network developed by ASHRAE and an ISO standard used in more than 30 countries. It is a data communication Protocol or set of communication rules that allow systems from different vendors to communicate between them and share information.

   Bacnet specification defines the aspects of BACnet protocol:
   a. **Objects**: logical representation used to represent:
      i. Physical device
      ii. Analog inputs (Temperature, flow, pressure, etc.)
      iii. Binary outputs (Relays, dampers, on/off a device)
   b. **Services**: are the information exchange between objects reads, writes. Object that provide the service is the server and the one request the service is the client. An object could have both functions depending of the system's needs.
   c. **Properties**: are information about an object. An object must have at least the next properties:
      i. Identifier
      ii. Name
      iii. Type

2. What is an Object in BACnet?
   An object may be a single point, a group of points or a device that perform a specific function and have all the information that any other device in the network need to work with it.

3. What is a BACnet property?
   Properties are a collection of characteristics that belong to an object and describe or modify their condition and actual status; like engineering Units, communication parameters or status, controller settings: setpoint, Proportional band, reset, derivative time, etc.

   **Object properties** are: name, type, actual value, unit, setpoint and limits between others. The properties have a name and its value. The next Table show some object properties:
<table>
<thead>
<tr>
<th>Name</th>
<th>Air Flow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Analog</td>
</tr>
<tr>
<td>Value</td>
<td>5.5</td>
</tr>
<tr>
<td>Unit</td>
<td>CFM</td>
</tr>
<tr>
<td>Setpoint</td>
<td>5.0</td>
</tr>
<tr>
<td>Upper Limit</td>
<td>7.0</td>
</tr>
<tr>
<td>Lower Limit</td>
<td>4.0</td>
</tr>
</tbody>
</table>

4. How does work a BACnet Router?

A BACnet router transmit the messages between BACnet networks, implement the BACnet network layer protocol and allow devices on disparate networks to communicate. It sends messages in both directions.

The transmission media could be wired or wireless.

5. What network use BACnet?

The main two networks used by BACnet are:

- **BACnet IP** that is an Ethernet based protocol
- **BACnet Master Slave Token Passing (MSTP)** that is a Serial Protocol.

BACnet MSTP uses RS485 (also known as EIA485) as its physical layer and is using more at field level (sensor, transmitters, controllers).

BACnet/IP uses UDP as its transport protocol. The default UDP port for BACnet traffic is 47808 (0xBAC0), this network is using in an upper level (between controllers, controllers/computers or to access internet).

BACnet controller have two addresses: MS/TP MAC address (set by a rotary switch) and the BACnet System address, this is called the device ID or Device Instance, and is generated automatically or manually by software.

Routers have an IP address and a MAC address.

The Complete address of any controller called its Device Instance or Device ID is a combination of the Router IP address, Router Mac Address and Controller Mac Address.

If the device is setting:

- a. Router BACnet/IP network: 1600
- b. Router Mac address is 01 (rotary switch).
- c. Router Network is 161
- d. One controller in that network has a MAC address of 03 (rotary switch).

The BACnet Device ID for this Controller would be: 1610103

References:

- Carrier: BACnet Basics Users Guide 2013
- Carrier: i-VU Open System IP & MS/TP Networks
- BACnet International Journal ISSN 2191-7825
- BACnet International Journal: Achieve BBMD Support with the BAS Router 02/11