MEBS6005 Building Automation Systems

http://ibse.hk/MEBS6005/

Communication Protocols

通訊協議

Ir Dr. Sam C. M. Hui

Department of Mechanical Engineering

The University of Hong Kong

E-mail: cmhui@hku.hk

Nov 2023

Contents

- Basic concepts
- Connectivity
- BACnet
- LonWorks
- KNX

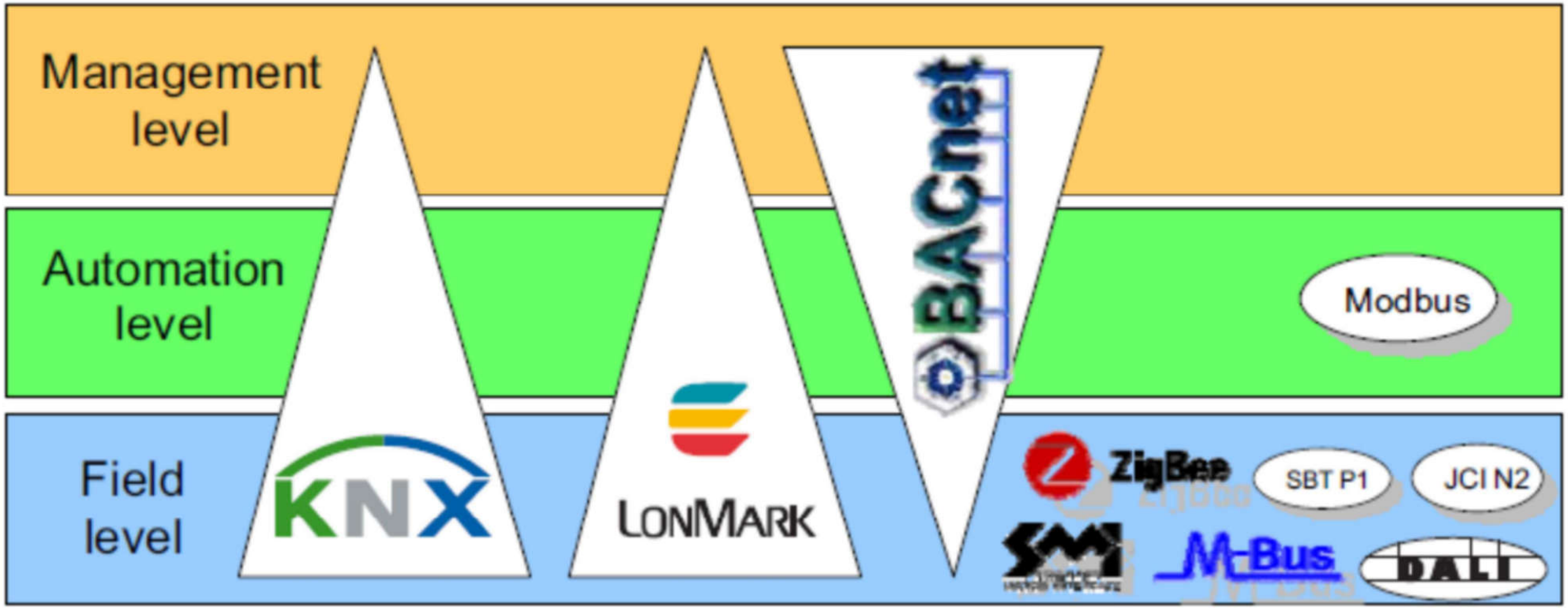
Basic concepts

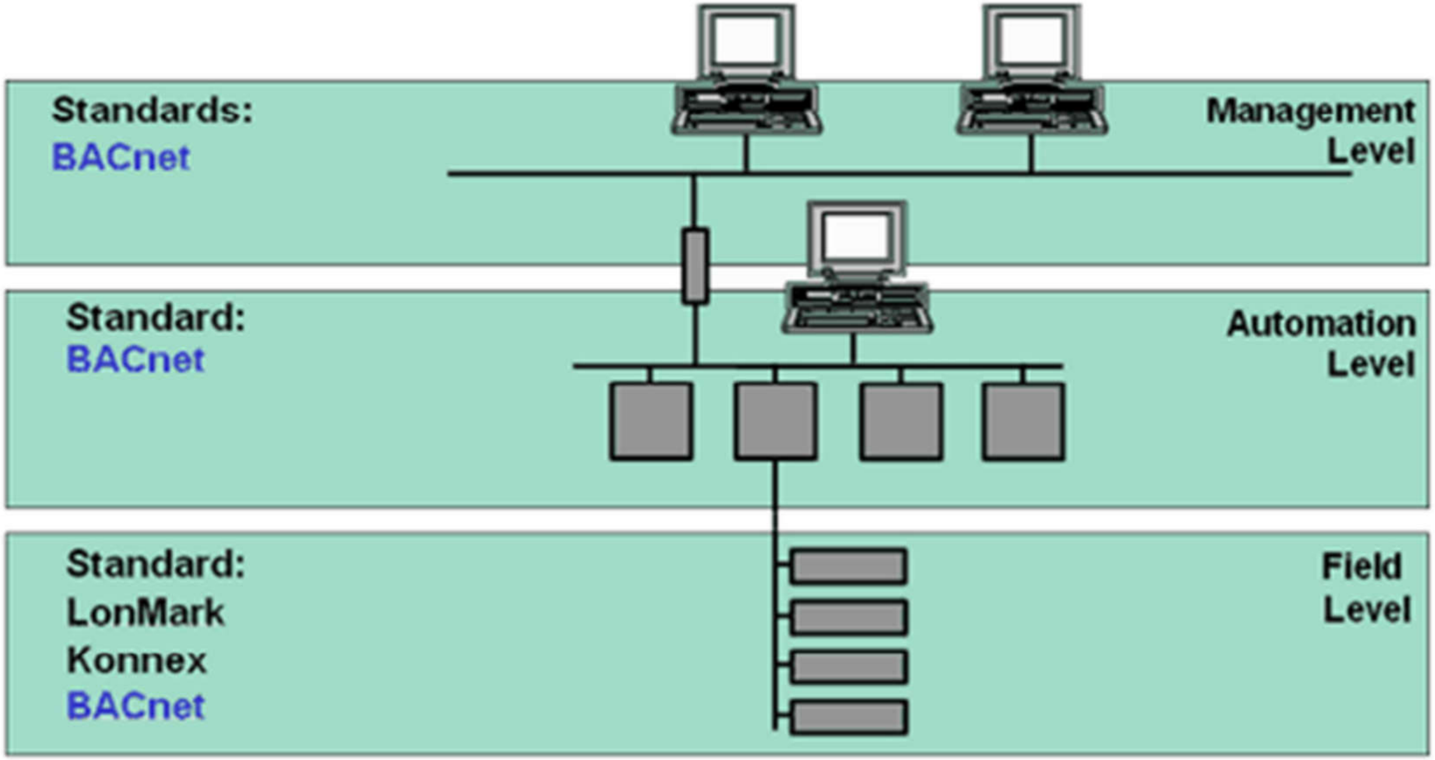
- A “protocol” is a formal agreement (e.g. Kyoto Protocol & Montreal Protocol)
- A Communications Protocol is an agreement on how to exchange of information between intelligent devices such as PCs or controllers
- The OSI 7-layer model is commonly used to identify the structure of the agreement
  - P.S.: The OSI Model is not a protocol; compliance with it does not imply connectivity

Basic concepts

- Data communication protocols
  - Sets of hardware & software rules, apply to:
    - Electrical signalling
    - Addressing
    - Network access (master/slave, peer-to-peer)
    - Error checking & flow control
    - Message sequencing
    - Segmentation & checkpointing
    - Presentation format (compression, encryption)
    - Message format

Communication protocols for building automation system (BAS)

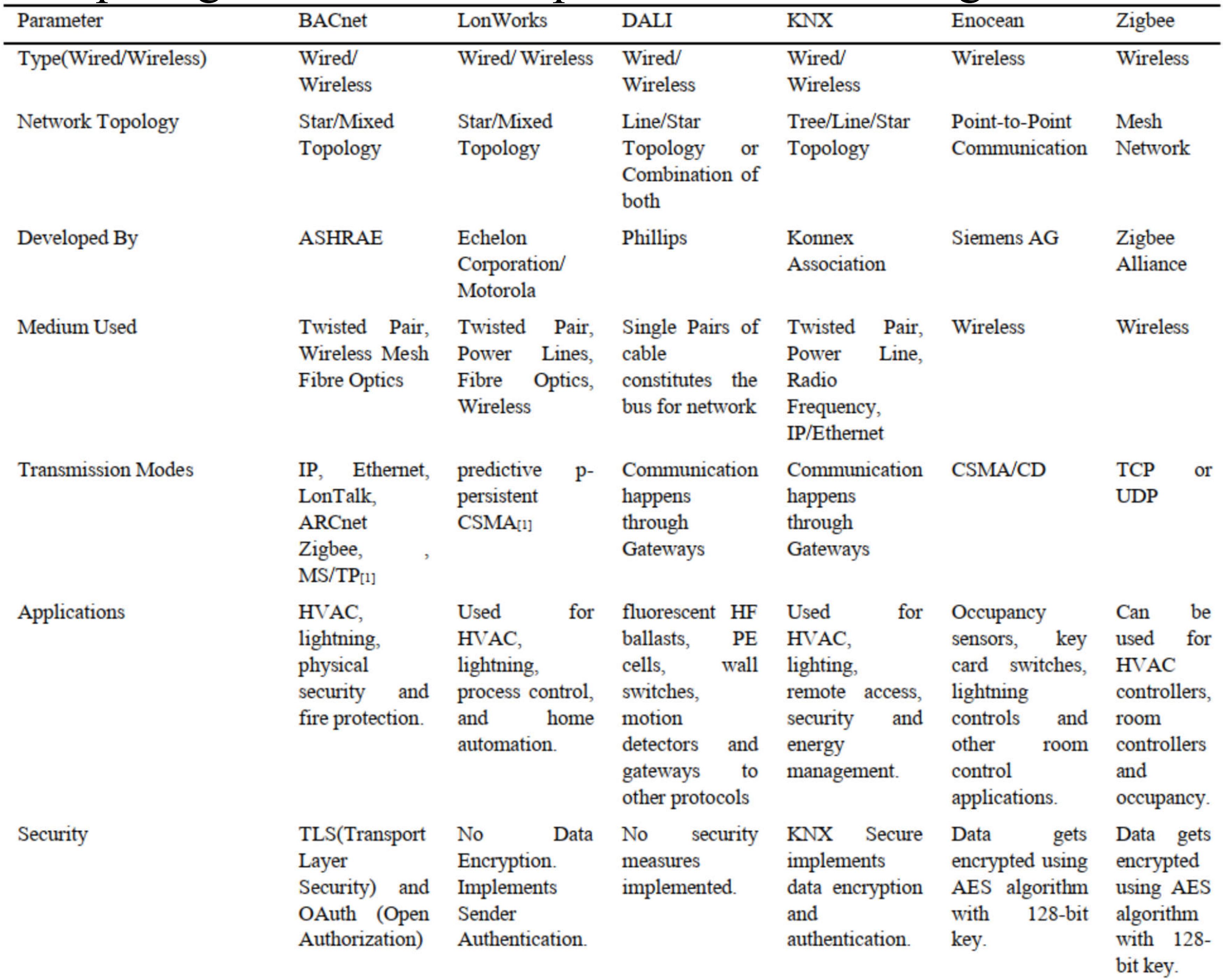




Basic concepts

- Examples of BAS communication protocols:
  - BACnet (building automation & control network)
  - LonWorks (local operating network)
  - KNX (Konnex)
  - DALI (digital addressable lighting interface)
    - For lighting controls
  - EnOcean (for wireless communication)
  - Zigbee (a wireless standard for home & building automation, based on an IEEE 802.15.4 standard)

Comparing communication protocols for building automation



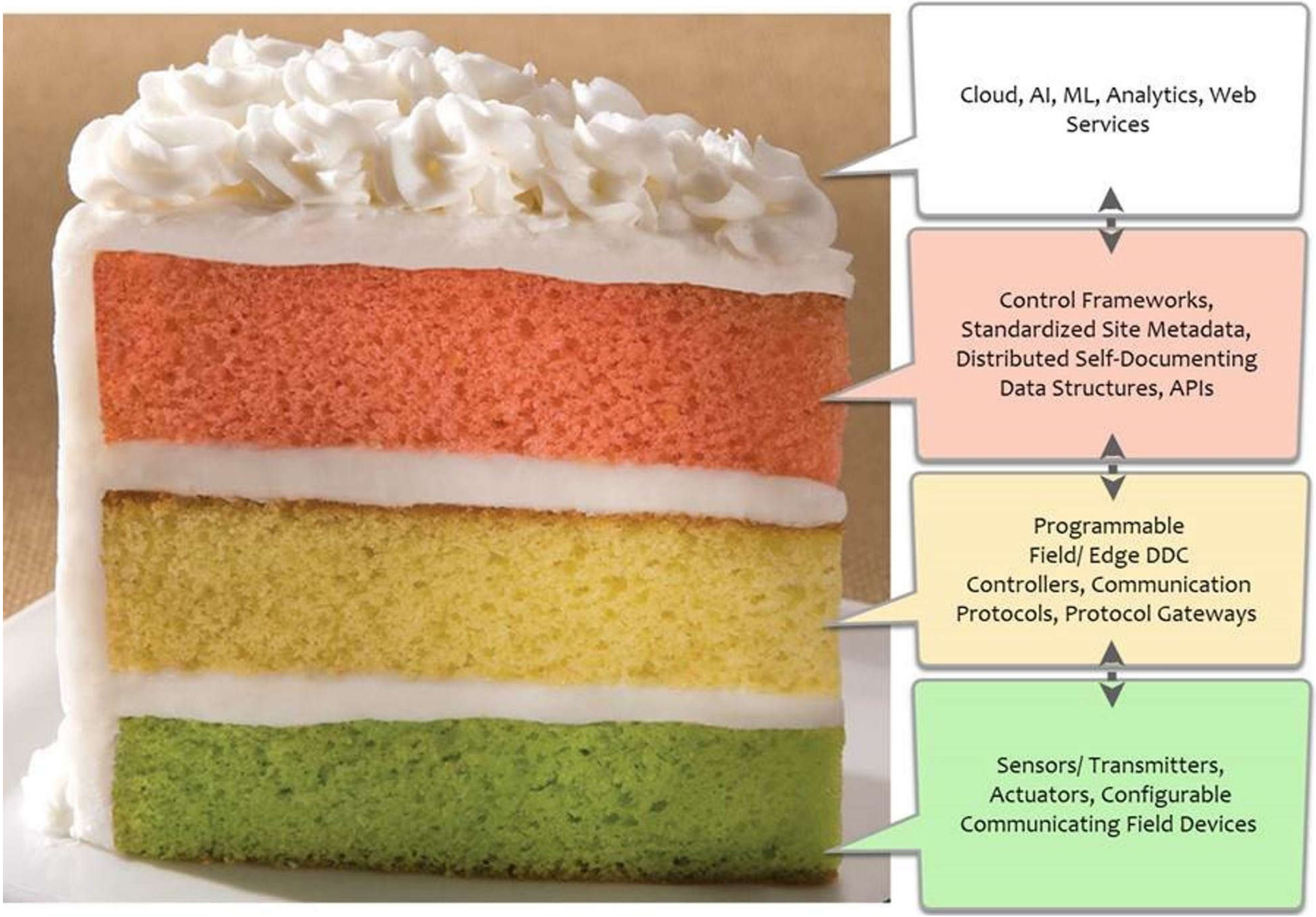
Parameter	BACnet	LonWorks	DALI	KNX	Enocean	Zigbee
Type(Wired/Wireless)	Wired/ Wireless	Wired/ Wireless	Wired/ Wireless	Wired/ Wireless	Wireless	Wireless
Network Topology	Star/Mixed Topology	Star/Mixed Topology	Line/Star Topology or Combination of both	Tree/Line/Star Topology	Point-to-Point Communication	Mesh Network
Developed By	ASHRAE	Echelon Corporation/ Motorola	Phillips	Konnex Association	Siemens AG	Zigbee Alliance
Medium Used	Twisted Pair, Wireless Mesh Fibre Optics	Twisted Pair, Power Lines, Fibre Optics, Wireless	Single Pairs of cable constitutes the bus for network	Twisted Pair, Power Line, Radio Frequency, IP/Ethernet	Wireless	Wireless
Transmission Modes	IP, Ethernet, LonTalk, ARCnet Zigbee, , MS/TP[1]	predictive p-persistent CSMA[1]	Communication happens through Gateways	Communication happens through Gateways	CSMA/CD	TCP or UDP
Applications	HVAC, lightning, physical security and fire protection.	Used for HVAC, lightning, process control, and home automation.	fluorescent HF ballasts, PE cells, wall switches, motion detectors and gateways to other protocols	Used for HVAC, lighting, remote access, security and energy management.	Occupancy sensors, key card switches, lightning controls and other room control applications.	Can be used for HVAC controllers, room controllers and occupancy.
Security	TLS(Transport Layer Security) and OAuth (Open Authorization)	No Data Encryption. Implements Sender Authentication.	No security measures implemented.	KNX Secure implements data encryption and authentication.	Data gets encrypted using AES algorithm with 128-bit key.	Data gets encrypted using AES algorithm with 128-bit key.

(Source: Lohia K., Jain Y., Patel C. & Doshi N., 2019. Open communication protocols for building automation systems, *Procedia Computer Science*, 160: 723-727. https://doi.org/10.1016/j.procs.2019.11.020)

Basic concepts

- The OSI 7-Layer model is ok for communications engineers, but a simpler, 3-layer model can be used to discuss BAS connectivity:
  - Physical : what media is used to connect the devices (i.e. twisted shielded pair, CAT-5 UTP structured cabling, coaxial cable, fiber optic cable)
  - Delivery : what standard is used to ensure messages are passed between devices (Ethernet, EIA232, EIA485, etc.)
  - Information : how is information represented (start/stop command, point value, etc.)

BAS-OSI (Open Systems Interconnection) cake



Cloud, AI, ML, Analytics, Web Services

Control Frameworks, Standardized Site Metadata, Distributed Self-Documenting Data Structures, APIs

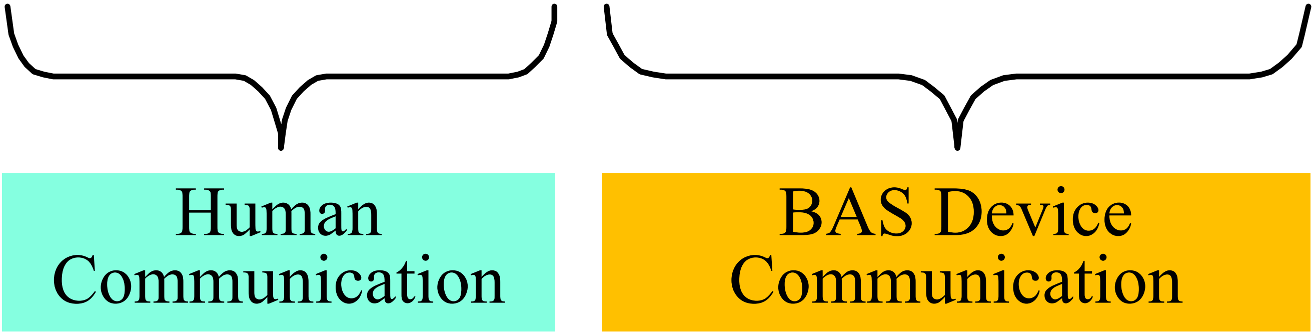
Programmable Field/ Edge DDC Controllers, Communication Protocols, Protocol Gateways

Sensors/ Transmitters, Actuators, Configurable Communicating Field Devices

(Source: https://www.automatedbuildings.com/news/mar20/reviews/200211114801open.html)

Examples of 3-layer model & an analogy to human communication

Physical	Paper	Paper	Coax	CAT-5 UTP
Delivery	Postal	Courier	Ethernet	LonTalk
Information	English	Chinese	BACnet	LonMark



Human Communication

BAS Device Communication

For two devices to exchange information, they must both use the same physical, delivery & information layer.

Basic concepts

- It may not be necessary to insist that devices agree on all three layers. For example:
  - For devices to use a common structured cabling system, they need only agree on the physical layer; this will allow common patch panels, common connectors & a common wiring management system to be used for all devices
  - For devices to “piggyback” onto an office automation (OA) LAN using Ethernet TCP/IP, they need only agree on the physical & delivery layers; the routers & bridges of the OA LAN need not understand the info contained in the messages to get the messages from one location to another

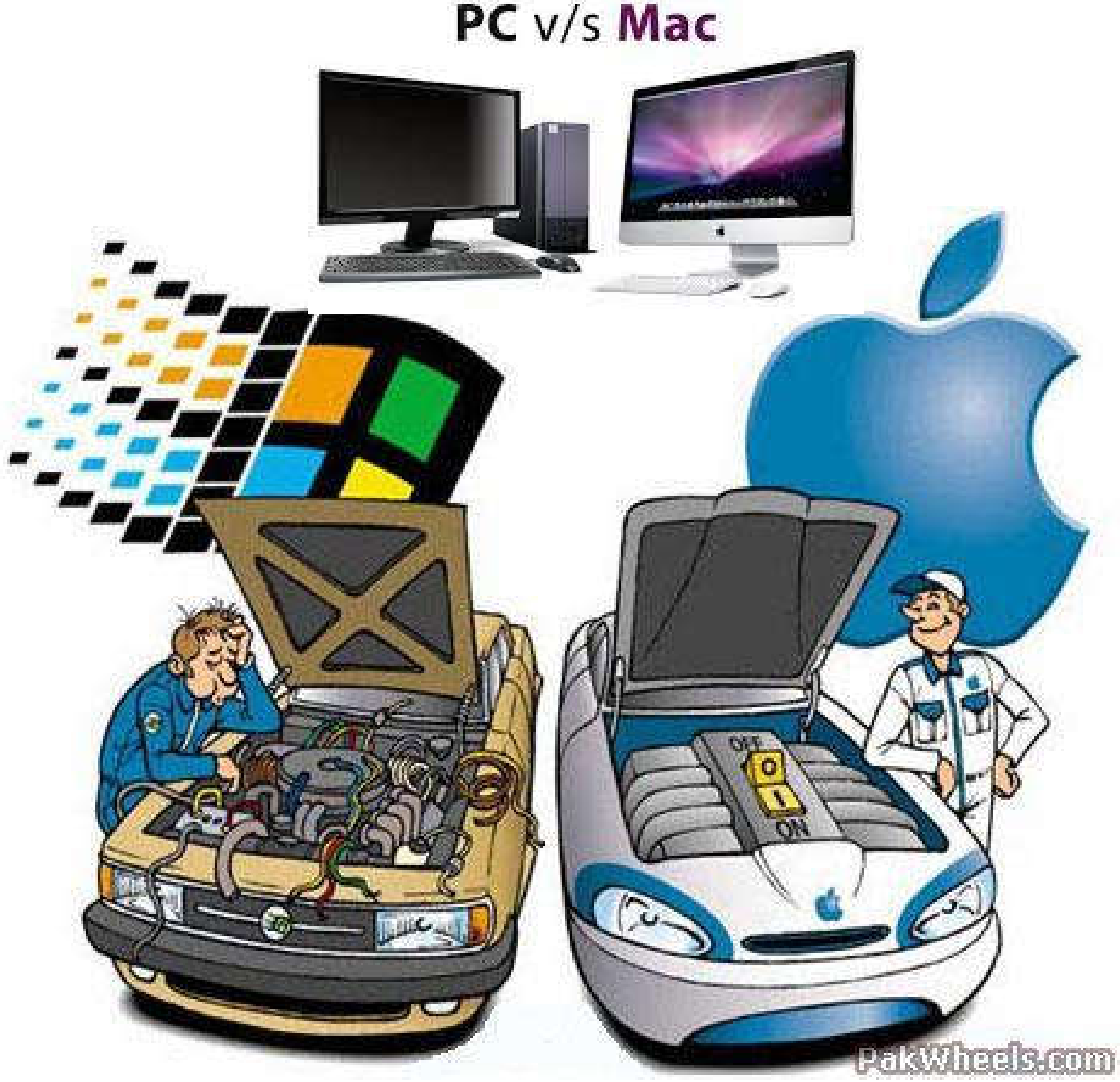
Basic concepts

- An “Open Protocol” is available to anybody, including competitors (only a few BAS vendors have such)
- A “Restricted Protocol” has the circulation controlled by a vendor (most BAS vendors have this)
- A “Standard Protocol” must first be an “Open Protocol” and, in addition, it must be used by a number of vendors (there are many competing “Standard Protocols” used in the BAS industry)

Basic concepts

- Types of systems
  - Open systems
    - No secrecy; codes and configurations are disclosed
  - Closed systems
    - Protected by secrecy; are patented or copyrighted
  - Proprietary systems
    - Developed by a proprietor (holds legal right & exclusive title); the system may be open or closed
  - Non-proprietary systems
    - Do not have a proprietor; often developed by non-profit organisation & are open

Example of a struggle between proprietary & open technology: IBM PC compatible vs Apple Mac



(Image sources: https://news.softpedia.com/news/mac-vs-pc-windows-desktops-up-to-535-more-expensive-than-macs-ibm-says-509518.shtml, https://www.pakwheels.com/forums/t/mac-vs-ibm-compatible/88146)

Basic concepts

- Prior to 1995 the building automation industry was dominated by proprietary systems
- Starting around 1995, two standards did gain acceptance & began to dominate the building automation industry: BACnet & LonWorks
    - Since that time, most of the major players in the industry have aligned themselves with one of these two standards; the two protocols have undertaken a battle to gain the upper hand in the industry

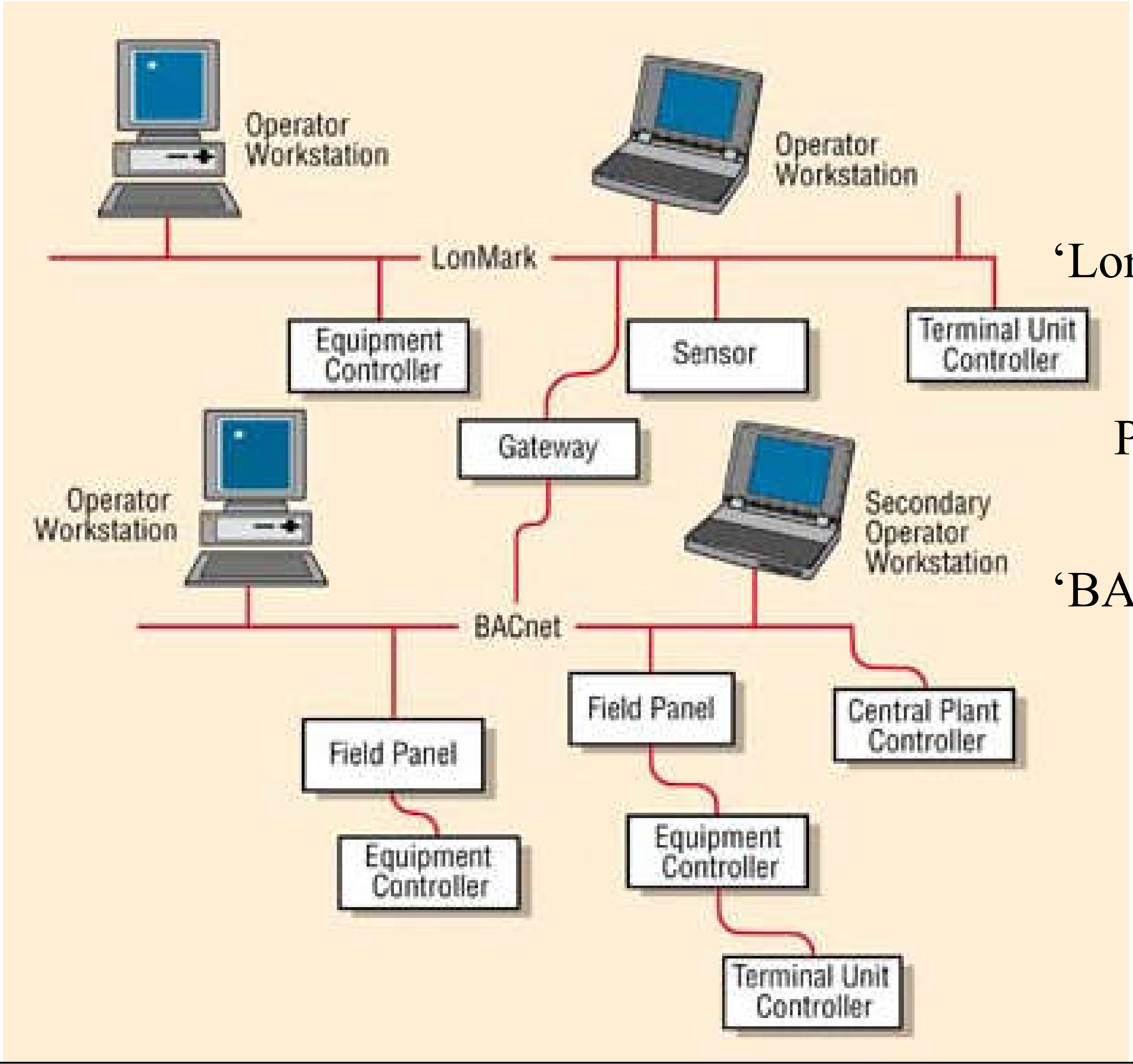
Example of various types of HVAC DDC systems

Type	**Open**	**Closed**
Proprietary	LonWorks	Various DDC manufacturers
Non-proprietary	BACnet	None known

ASHRAE BACnet™

LonWorks®

Modern building automation systems

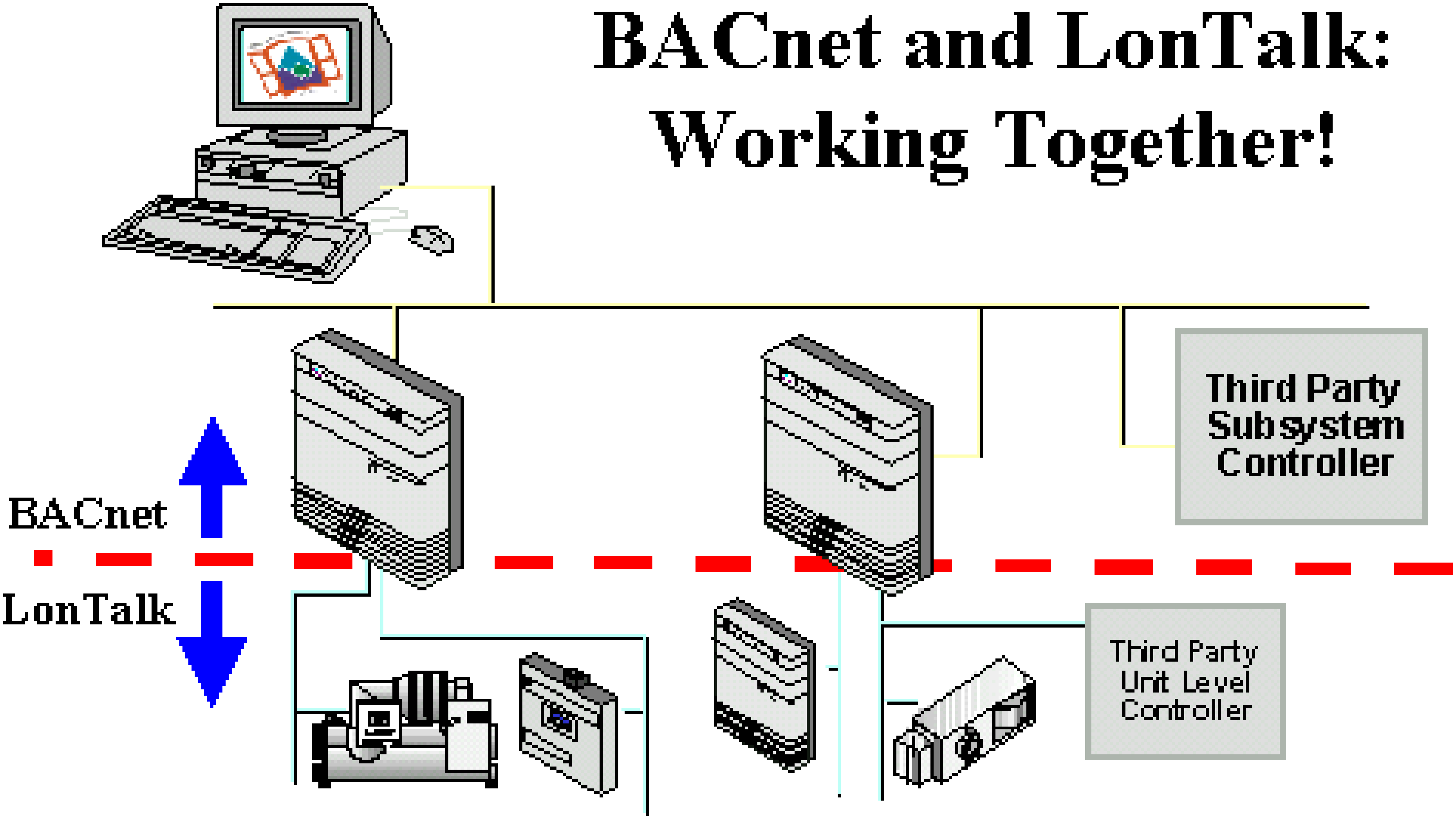


‘LonMark’

Protocols

‘BACnet’

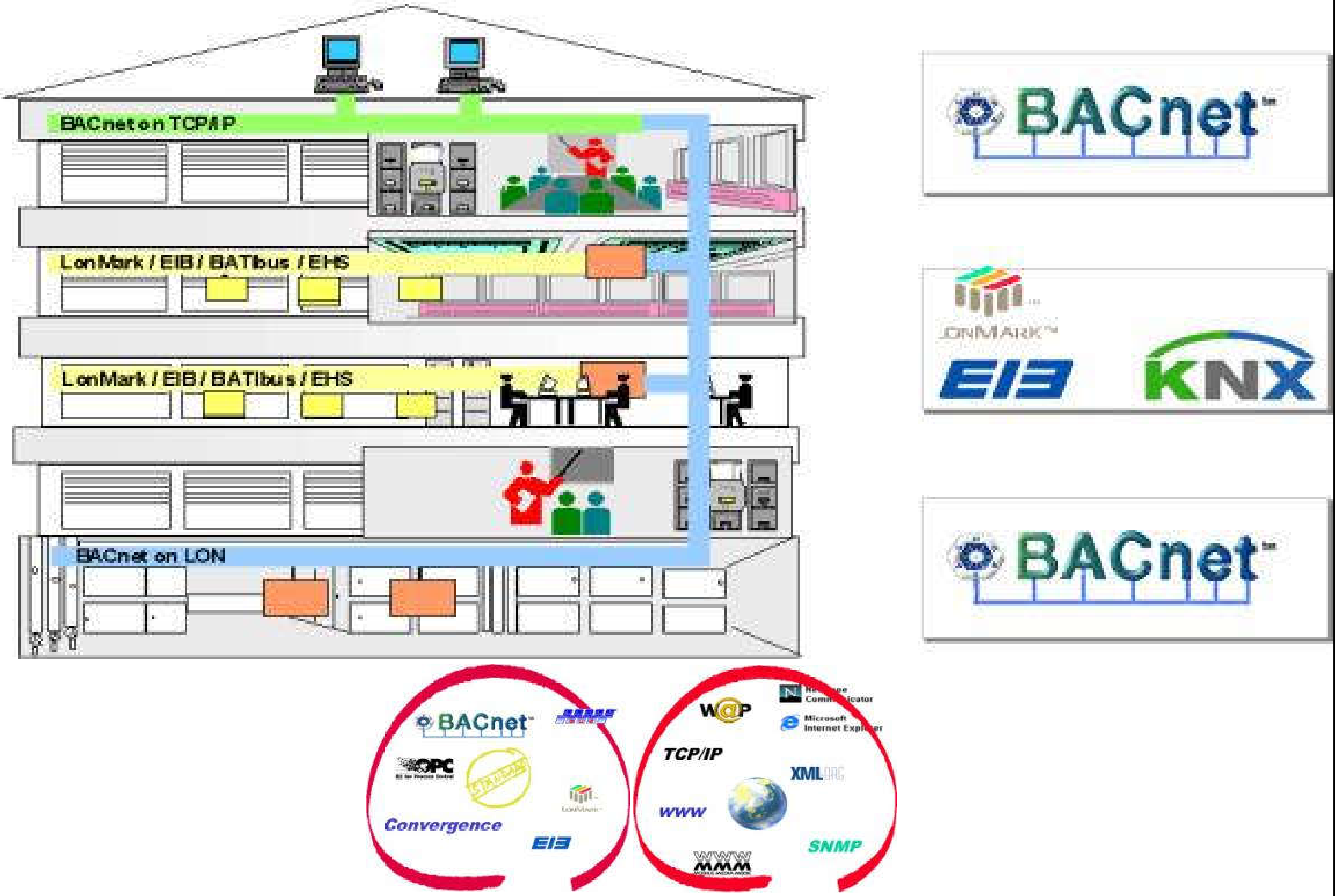
BACnet and LonTalk working together



BACnet and LonTalk:
Working Together!
BACnet
LonTalk
Third Party Subsystem Controller
Third Party Unit Level Controller

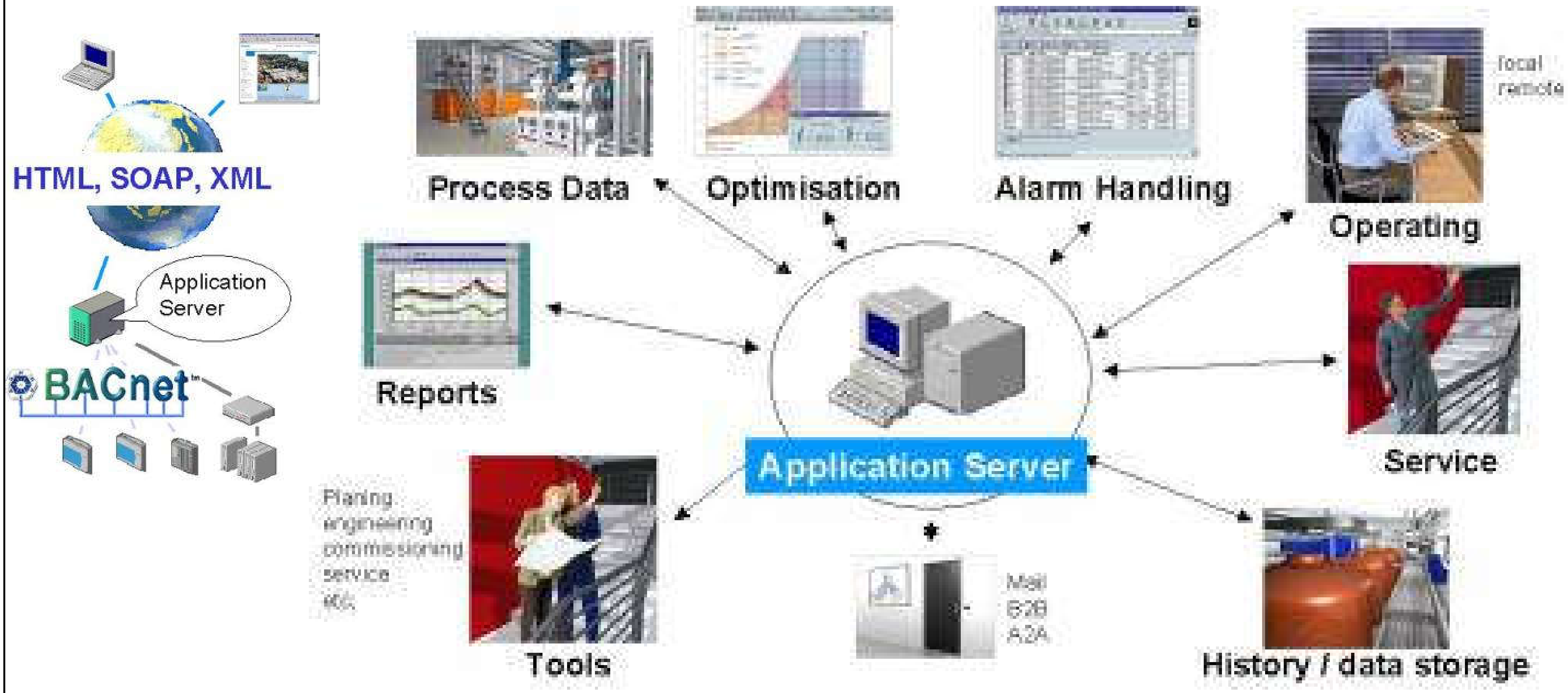
(Source: https://www.automatedbuildings.com/news/jan00/articles/trane/trane.htm)

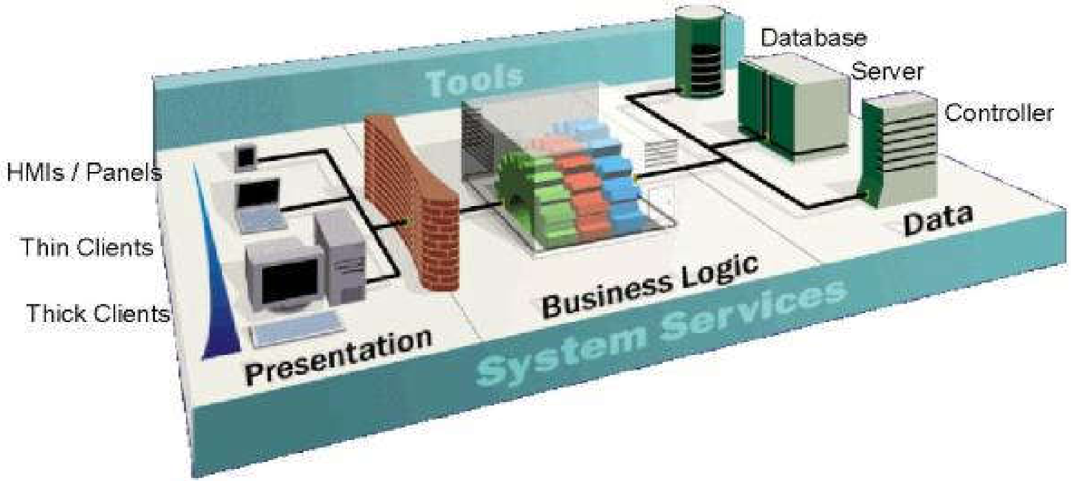
Different protocols & communication standards working together



(Source: http://www.automatedbuildings.com/news/jan02/art/hk/hk.htm)

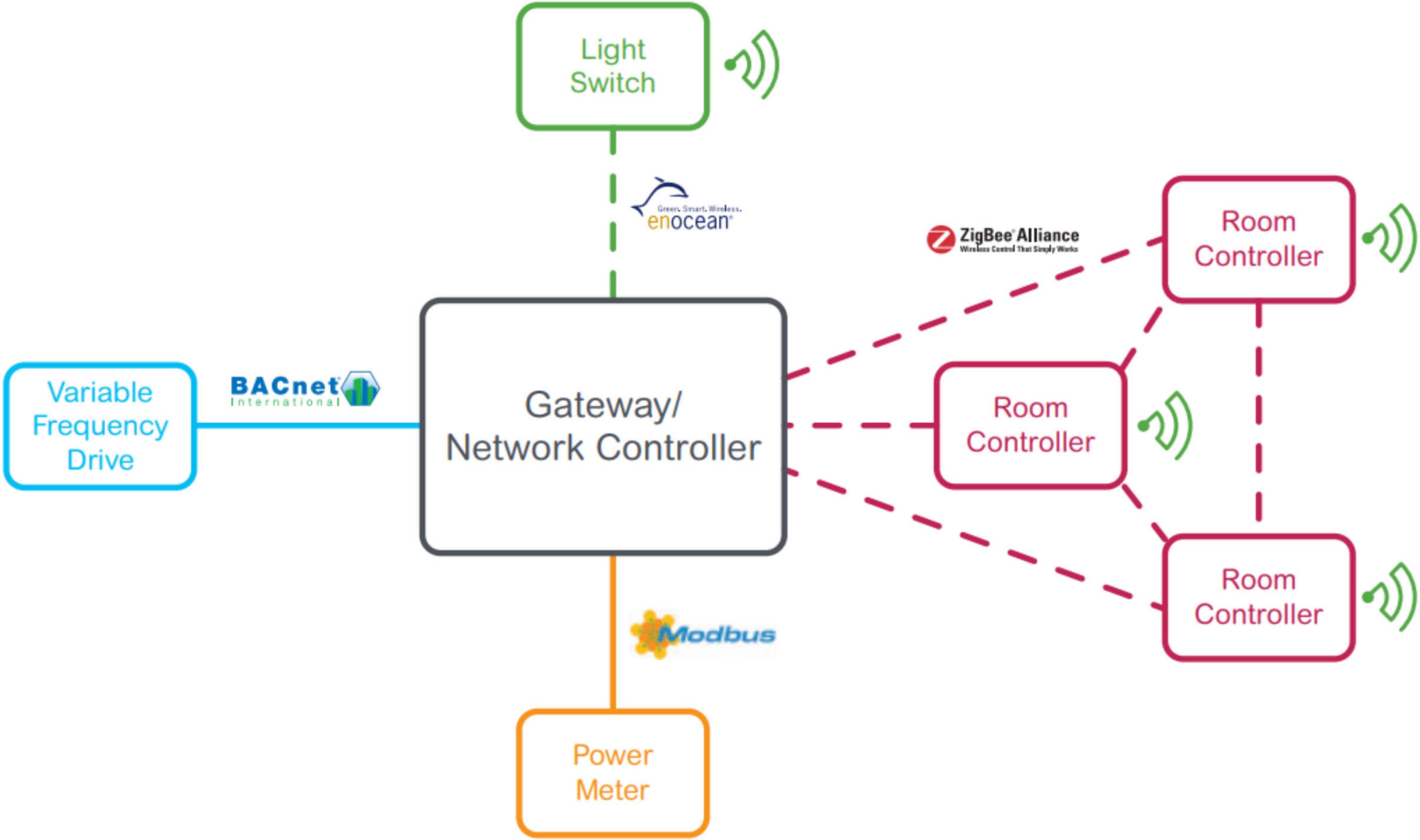
Use of application server to support the BAS technical solutions





(Source: http://www.automatedbuildings.com/news/jan02/art/hk/hk.htm)

Example of various connected devices via multiple protocols

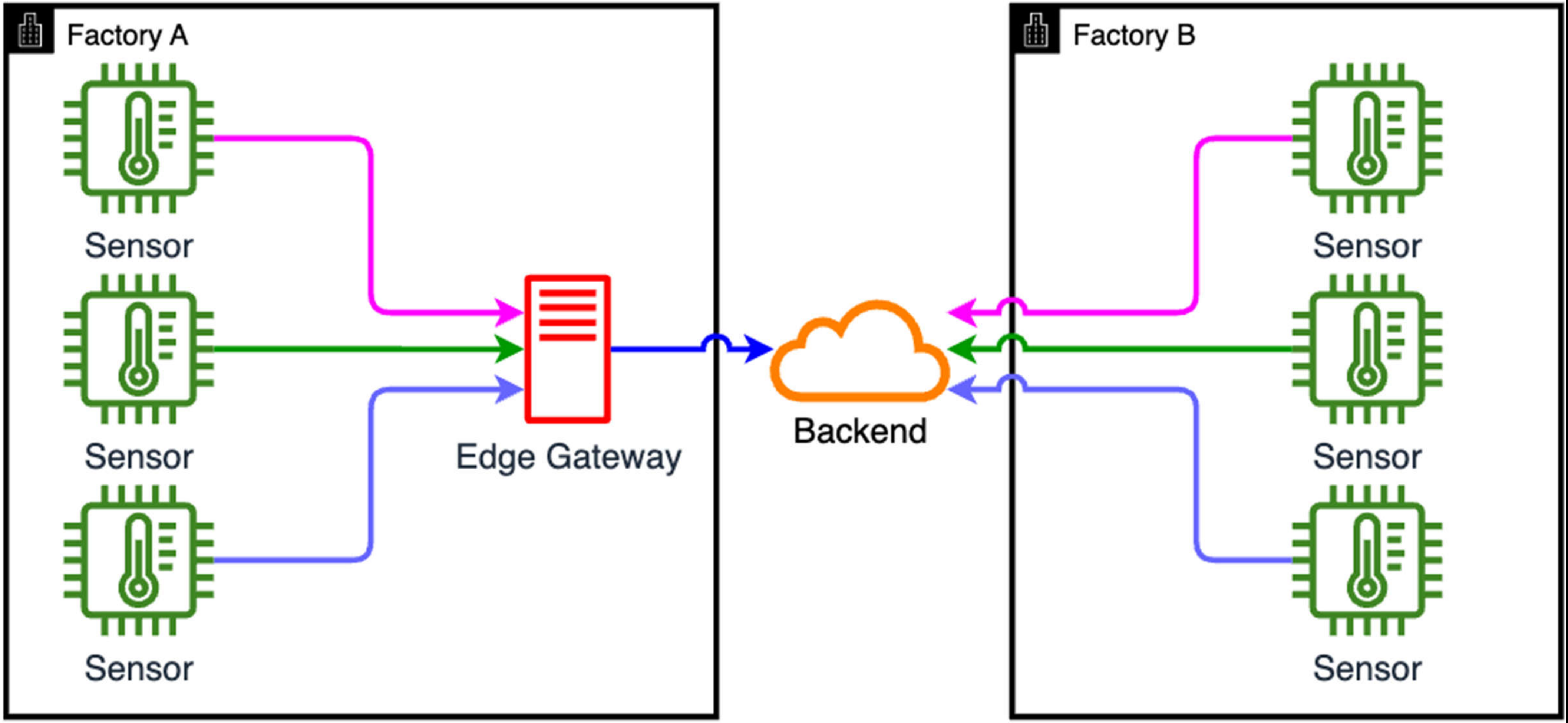


(Source: https://blog.se.com/wp-content/uploads/2015/11/SE-Protocols-Guide_A4_v21.pdf)

Basic concepts

- A BAS device can support only one protocol
- A BAS system can support a specific protocol in one of two ways:
  - Native : All devices in the system use this protocol. The protocol is used for all functions: (i.e. read, write, download, upload)
  - Gateway : Devices in the system do not use this protocol but a “protocol translator” is available. In this case, the specific protocol is typically only used for read & write but not upload or download

Gateway vs. Gateway-less device considerations



(Source: https://www.linkedin.com/pulse/gateway-vs-gateway-less-industrial-iot-considerations-malinowski)

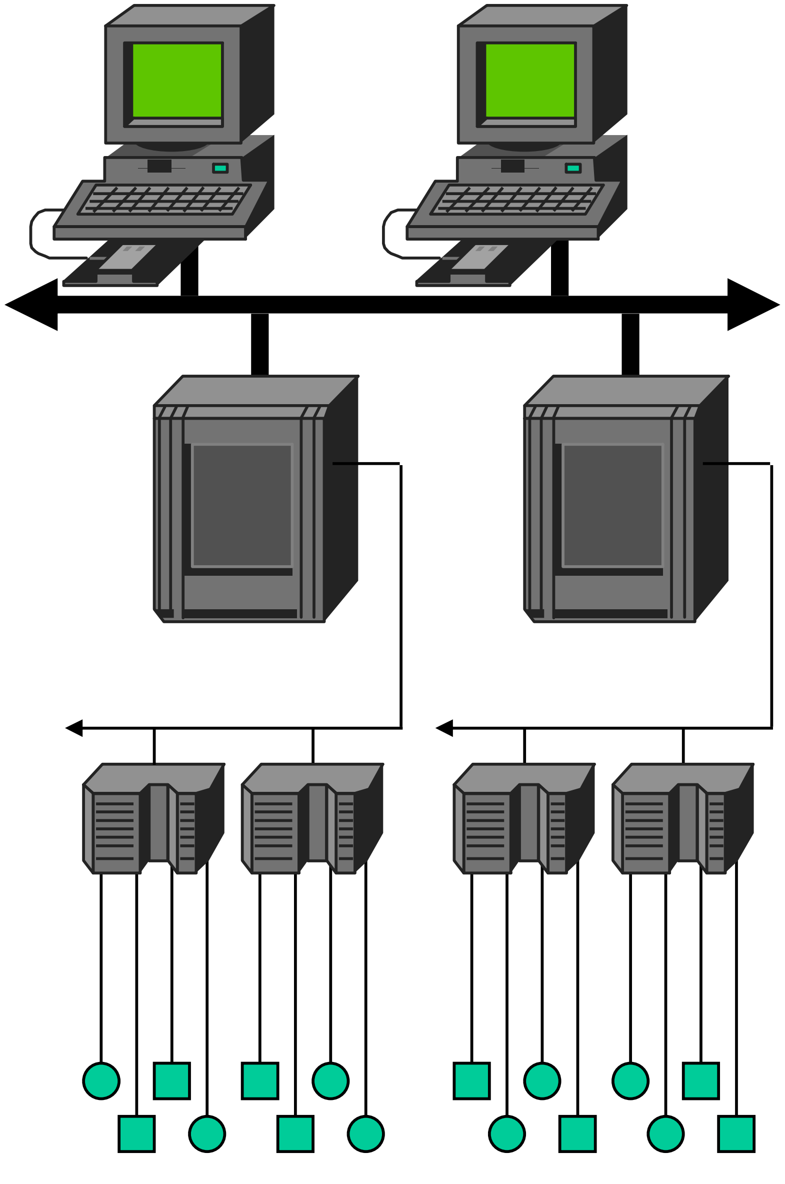
Connectivity

- BAS is a tool to assist in the management of the building (In today’s environment, this means providing connectivity to a number of protocols)
  - 1. Existing vendor-specific protocols
  - 2. Competing “Standard” protocols
  - 3. Protocols from other industries
  - 4. Protocols from other BAS
- Which protocol is “native” to the BAS devices is irrelevant - what is important is the list of protocols to which the BAS system can connect
  - Being locked into any one protocol is not a good idea

Connectivity

- Myths regarding Protocols:
  - Compliance with the OSI 7-layer model implies connectivity
  - Use of a standard LAN such as Ethernet TCP/IP implies connectivity
  - Having an “Open Protocol” implies connectivity (Question: how many vendor’s equipment can be connected using this “Open Protocol”; is it a “Standard Protocol”?)
  - Which protocol is native to the BAS device is important (Correction: what is important is the list of protocols to which the BAS can connect)

Layers of a BAS



Management Layer

Operator Workstation
Graphical User Interface
Data Archiving

Automation Layer

System Controller
Historical Data Collection
Supervisory Control
BAS Features

Field Layer

DDC Controller
Connect to Sensors / Actuators
Equipment Level Interlocks
Control Loops

Layers defined by European Standardization Committee

Connectivity

- Connectivity at each layer can be accomplished through one of two approaches:
  - “Native” standard
  - Gateway (i.e. translator)
- Each layer approaches connectivity differently because there are different objectives for connectivity at each layer & different technical/cost constraints at each layer
  - Wired & wireless connectivity; cost of ownership

Connectivity

- Field Layer
  - Includes DDC controllers & factory-mounted controllers
  - Responsible for connecting to sensors / actuators, equipment level interlocks & control loops
  - Very large quantity installed in a building, so “pennies count”; network cost must be low
  - Connectivity focus: integrating building equipment into BAS

Connectivity

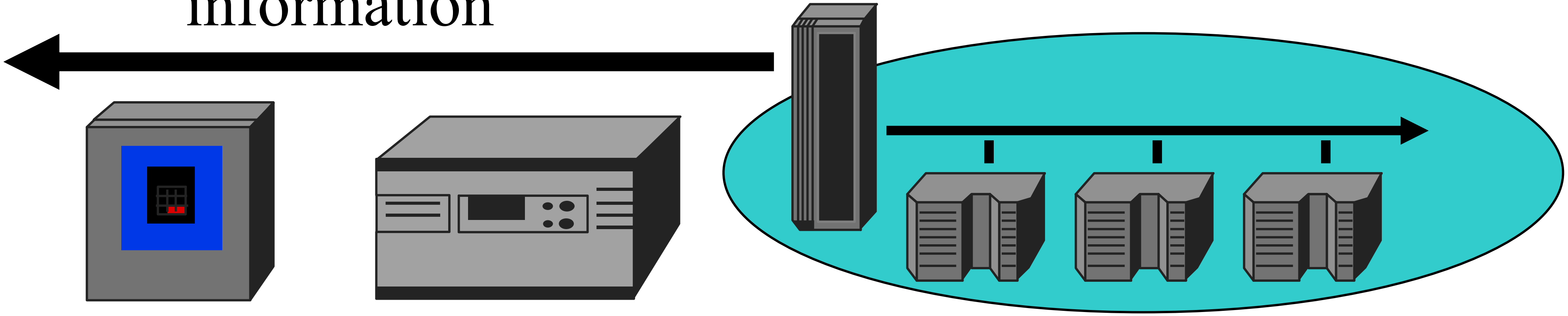
- Automation Layer
  - Includes BAS system controllers
  - Responsible for historical data collection, supervisory control & BAS features
  - Small quantity installed in a building, so network cost is not critical
  - Connectivity focus: integrating other building systems into BAS

Connectivity

- Management Layer
  - Includes PC based operator workstations
  - Responsible for graphical user interface (GUI) & data archiving
  - Small quantity installed in a building, so network cost is not critical
  - Connectivity focus: integrating other systems (i.e. office/factory automation) into BAS

BACnet

- BACnet = Data communication protocol for Building Automation and Control Networks system:
  - A standard protocol designed by consensus to allow devices from different vendors to exchange information



Vendor 1 Controller

Vendor 2 Controller

Vendor 3 Island of Automation with BACnet ™ Gateway

BACnet

- BACnet
  - Industry standard developed by ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers) since 1987
    - Became ASHRAE/ANSI Standard 135 in 1995
    - Adopted in USA, Europe and many countries as the reference standard for BAS (e.g. ISO 16484-5 in 2003)
  - BACnet applications: HVAC, fire, lighting, security, lifts, utility company interface
  - Use only layers 1, 2, 3 & 7 of the OSI model

BACnet infrastructure compared with the OSI model

OSI Layers		**BACnet Layers**					
7	Application	BACnet Application					
3	Network	BACnet Network					
2	Data link	Ethernet	ARCNET	MS/TP	Point-to-point	IP	LonTalk
1	Physical	Ethernet	ARCNET	EIA-485	EIA-232	Internet	LonTalk

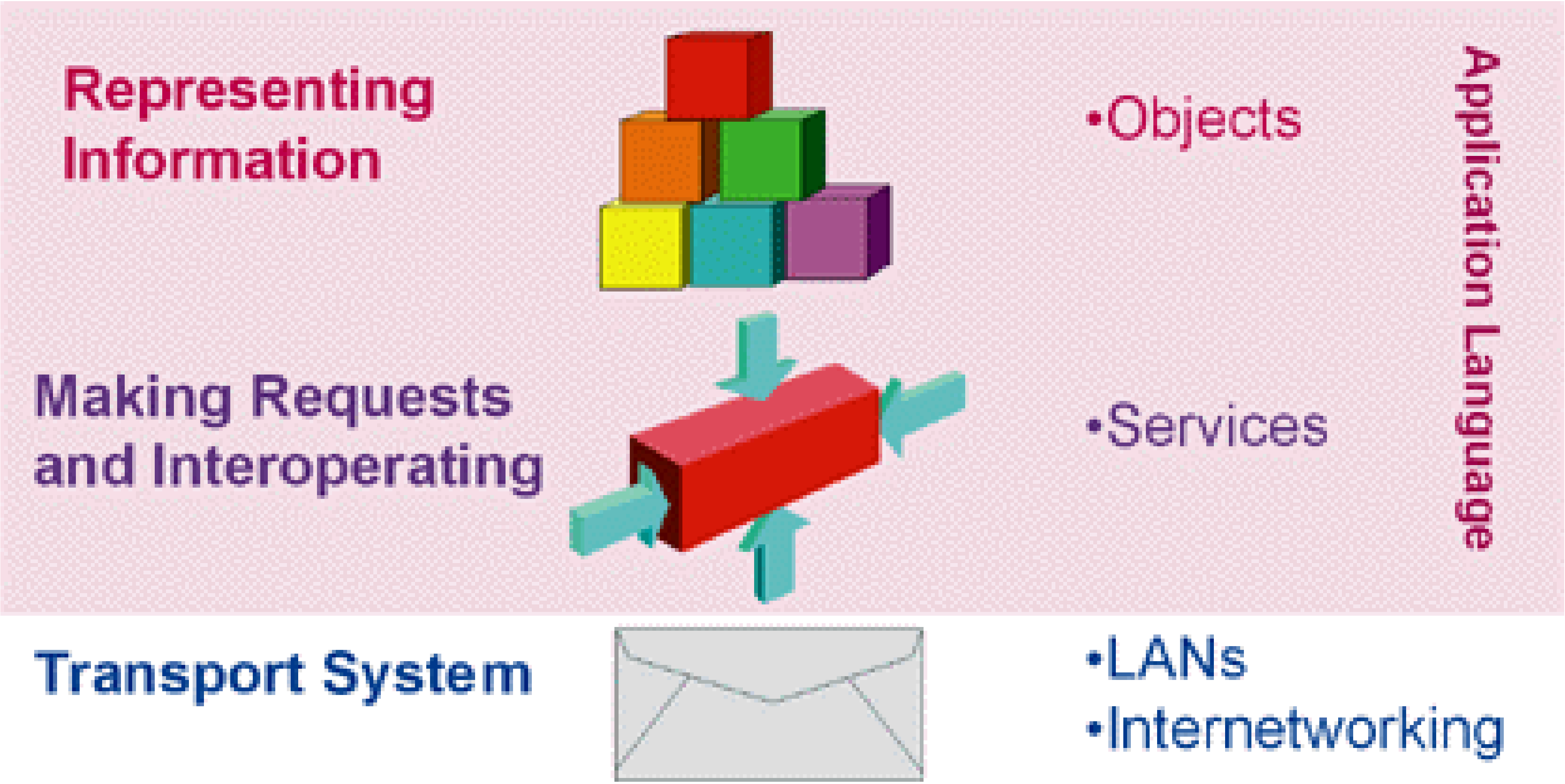
MS/TP = Master/Slave Token Passing; IP = Internet Protocol

* EIA-485 is most often used for application specific controllers (low cost)

* EIA-232 & point-to-point is typically used for dial-up access through a modem

LonTalk: commun. protocol for LonWorks network

How does BACnet work?



Representing Information

•Objects

Making Requests and Interoperating

•Services

Application Language

Transport System

•LANs
•Internetworking

BACnet

- BACnet Application Layer
  - Similar to OSI application layer
  - Consists of 18 standard types “objects”, 35 “services” & 6 events “algorithms”
    - BACnet Objects
      - Used to identify & access info from various devices
      - Abstract data structures that represent various aspects of the software, hardware, or an operation, e.g. an analogue input, analogue value, binary output, calendar & schedule
    - BACnet Services
      - Provide commands & additional services for objects

BACnet Standard Objects

Analog Input
Analog Output
Analog Value
Binary Input
Binary Output
Binary Value
Calendar
Command
Device
Event Enrollment
File
Group
Loop
Multistate Input
Multistate Output
Program
Recipient Table
Schedule

Plus vendor specific objects

Analog Input Properties

Object Identifier	Object Type	Present Value
Description	Device Type	Status Flags
State	Out of Service Flag	Update Interval
Units	Minimum Value	Maximum Value
Resolution	Vendor Specific Property #1	Vendor Specific Property #n

Each vendor is free to extend the standard set of properties with additional vendor specific properties

BACnet Standard Services

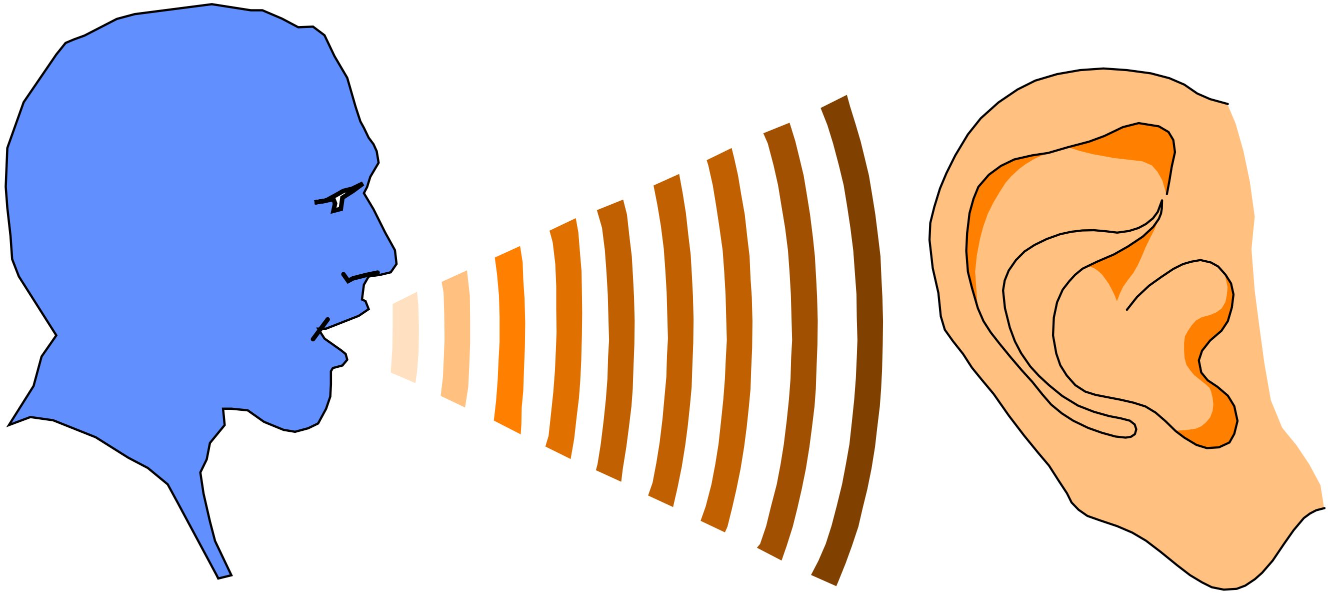
- Alarm & Event Services
- File Access Services
- Object Access Services
- Remote Device Management Services
- Virtual Terminal Services

Private transfer services are available to provide vendor specific capabilities

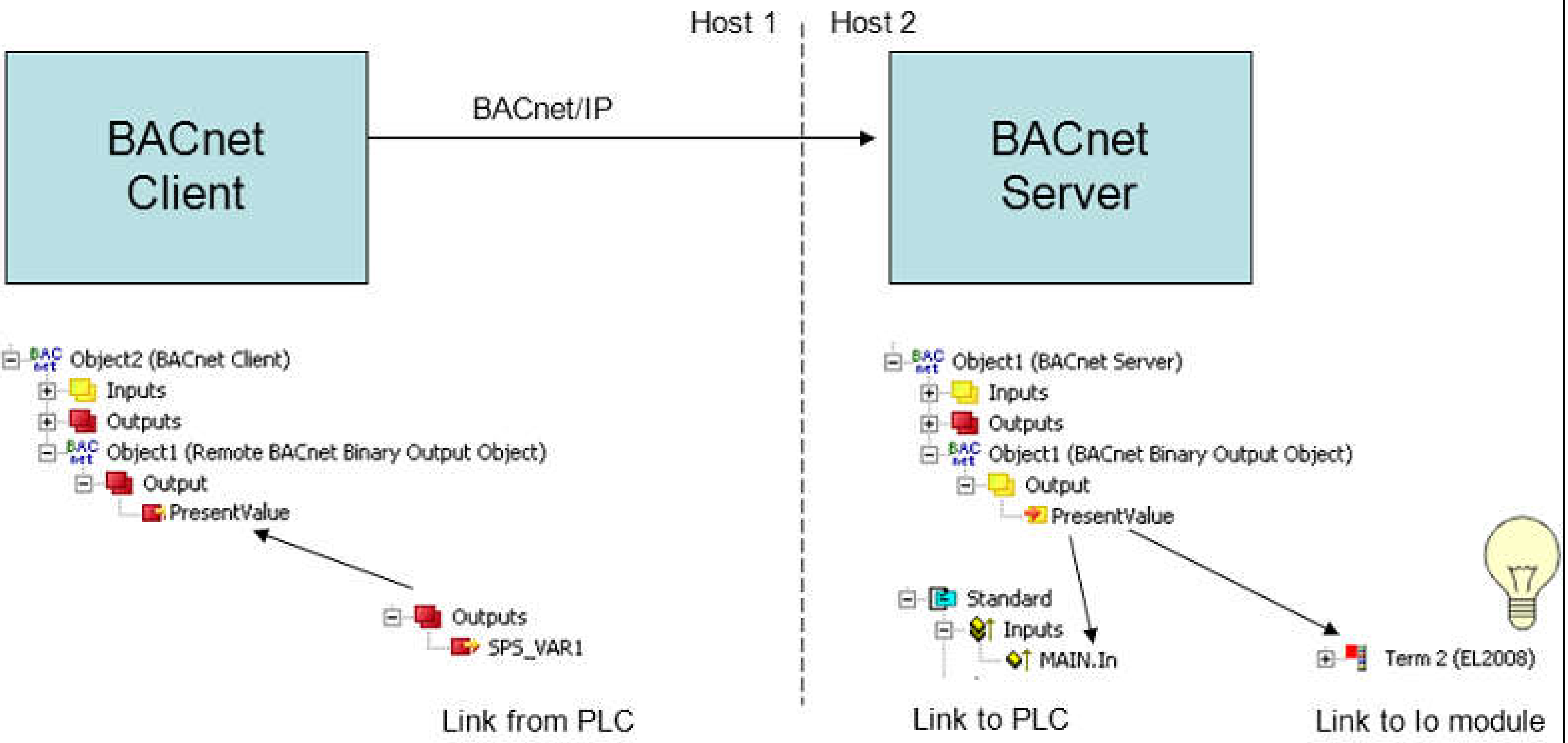
BACnet Protocol Data Units

- Confirmed Request
- Simple Acknowledge
- Segment Acknowledge
- Reject

- Unconfirmed Request
- Complex Acknowledge
- Error
- Abort



BACnet Client & BACnet Server linking process



PLC = Programmable Logic Controller

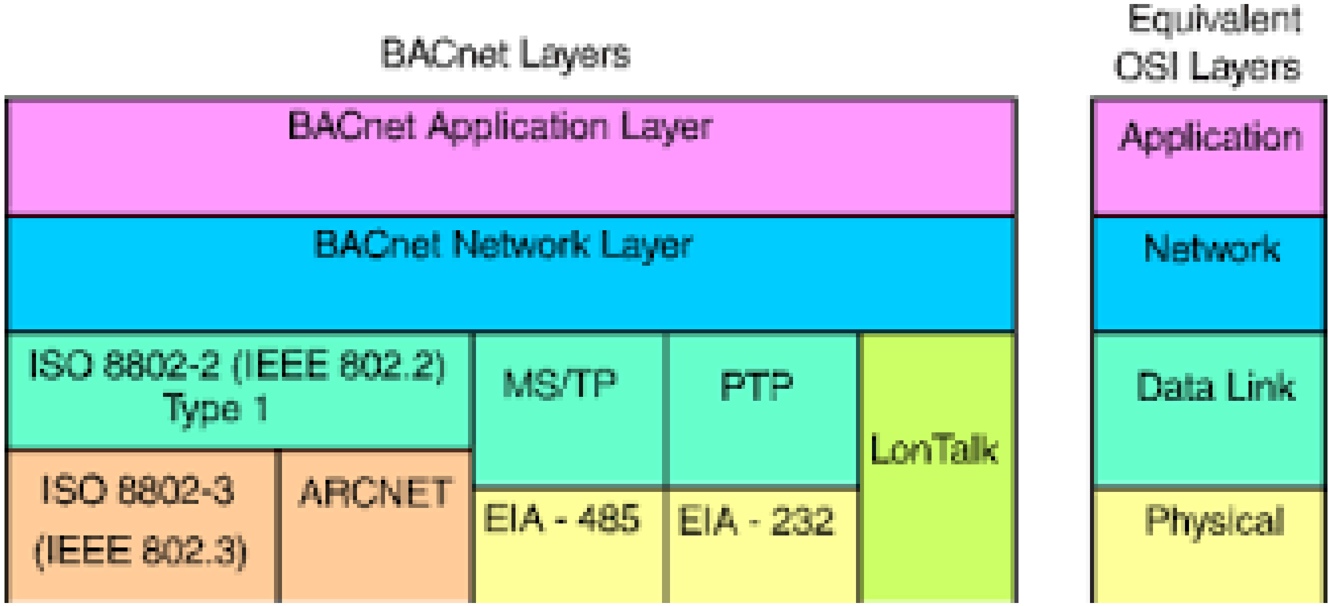
(Source: https://infosys.beckhoff.com/english.php?content=../content/1033/tcbacnet/12748435211.html&id=)

BACnet

- BACnet Network Layer
  - Similar to OSI network layer
  - Provide the means by which a message can be routed from one BAcnet network to another
- BACnet Data Link Layer
  - Similar to OSI local data link layer
  - Relates to the packaging & data transfer within one specific network
    - It allows 5 LAN technologies: Ethernet (ISO 8802-3), ARCNET (ANSI 878-1), master/slave token passing (ANSI/ASHRAE 135), point-to-point (ANSI/ASHRAE 135), LonTalk (Echelon)

BACnet

- BACnet Physical Layer
  - Similar to OSI physical layer
  - Refer to the physical media (wiring) in which data are transferred
  - Allows 6 LAN technologies:
    - Ethernet
    - ARCNET
    - EIA 485
    - EIA 232
    - Internet
    - LonTalk



BACnet Layers

Equivalent OSI Layers

BACnet Application Layer

Application

BACnet Network Layer

Network

ISO 8802-2 (IEEE 802.2) Type 1

MS/TP

PTP

LonTalk

Data Link

ISO 8802-3 (IEEE 802.3)

ARCNET

EIA - 485

EIA - 232

Physical

BACnet

- Advantages of using Internet for BACnet systems
  - Allows 2 or more remote networks to communicate simultaneously & operate together
  - More powerful & faster remote access
  - Real-time integral operation
  - User friendly (everyone is familiar with Internet browser)
- Caution with Internet: security issues & hackers!

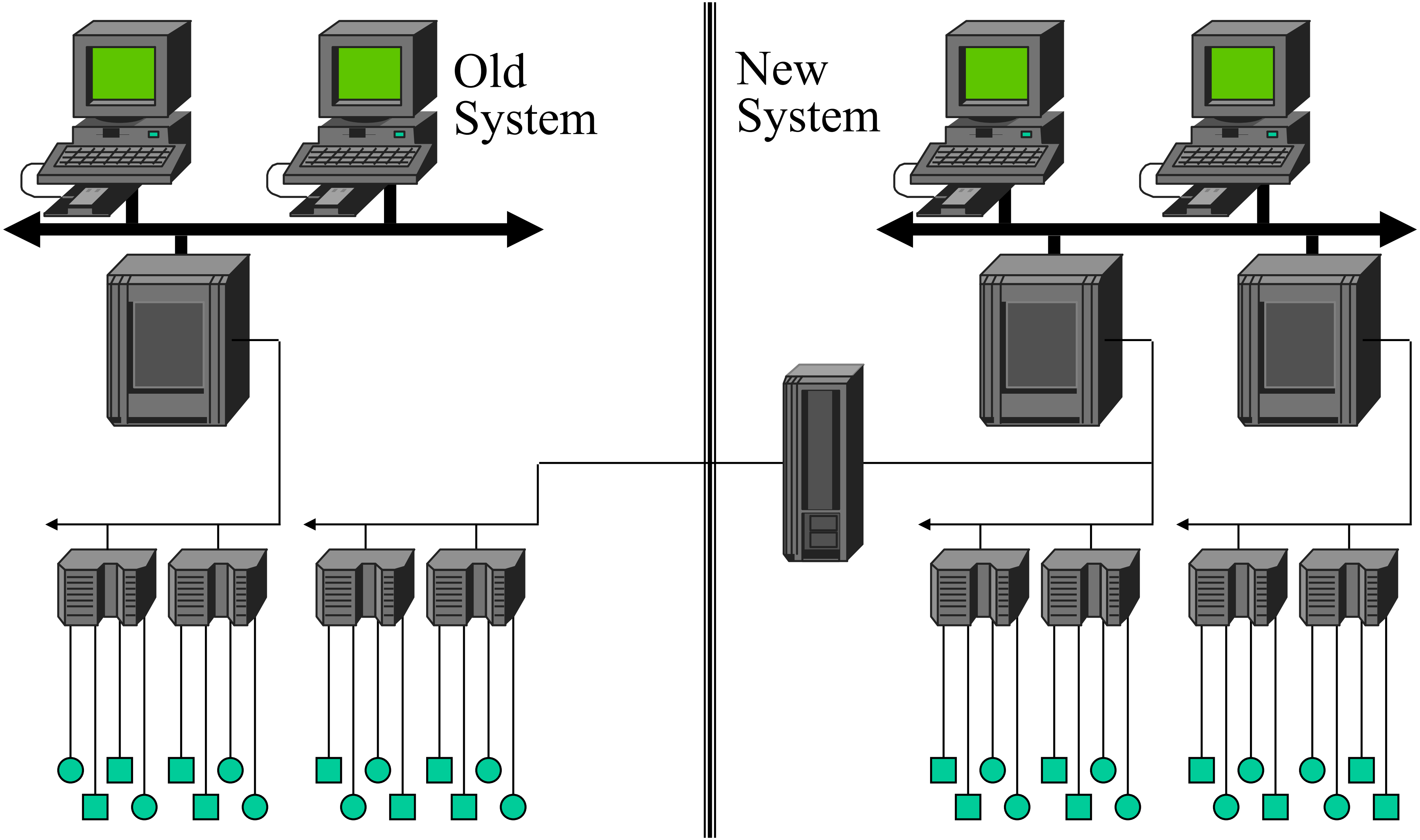
BACnet

- BACnet conformance classes
  - BACnet defines standard Protocol Implementation Conformance Statement (PICS) to allow proper conformance by various manufacturers
  - Has 6 levels of conformance
    - **Class 1** : Receive “read value” message
    - **Class 2** : Class 1 + receive “write value” message
    - **Class 3** : Class 2 + receive “read/write attribute” message
    - **Class 4** : Class 3 + send “read/write value” message + send “read/write attribute” message
    - **Class 5** : Class 4 + receive “create/delete object” message
    - **Class 6** : Class 5 + send “create/delete object” message

BACnet

- Native BACnet
  - A terminology adopted by BACnet manufacturers
  - Those DDC systems in which every component is BACnet compatible at the device level
  - 2 native BACnet devices can talk with minimal interface
- BACnet gateways
  - Gateways (= intelligent translator) as an interface between close proprietary systems & BACnet
  - Requires continuous maintenance; may create a bottleneck for info transfer

Interfacing old & new systems



BACnet

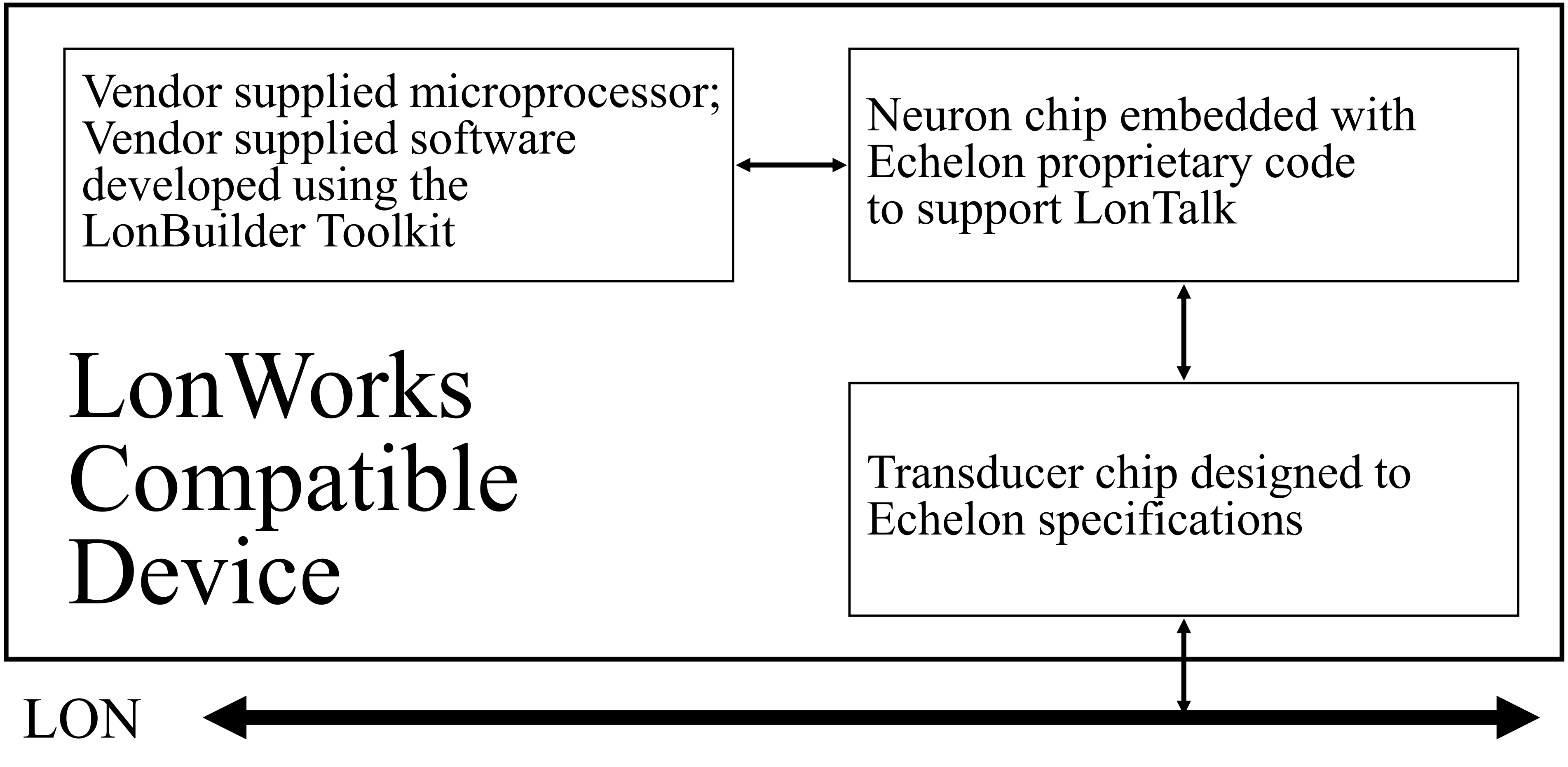
- Further info about BACnet:
  - ASHRAE's BACnet committee (SSPC 135) http://www.bacnet.org
    - BACnet Tutorial Overview
    - BACnet/IP
    - BACnet: Answers to Frequently Asked Questions
  - Bibliography
  - BACnet International (BI) (formerly, BACnet Manufacturers Association) http://www.bacnetassociation.org

LonWorks

- LonWorks is a family of hardware & software products developed by the Echelon Corporation (www.echelon.com)
  - LON = local operating network (designed to move short, event-driven, effective data)
  - LonTalk = open proprietary protocol for LonWorks; based on OSI 7-layer model
    - Provide the set of rules & methods for managing and exchanging messages between nodes & devices

LonWorks

LonWorks compatible devices must use transducer & Neuron chip from Echelon.



Vendor supplied microprocessor; Vendor supplied software developed using the LonBuilder Toolkit

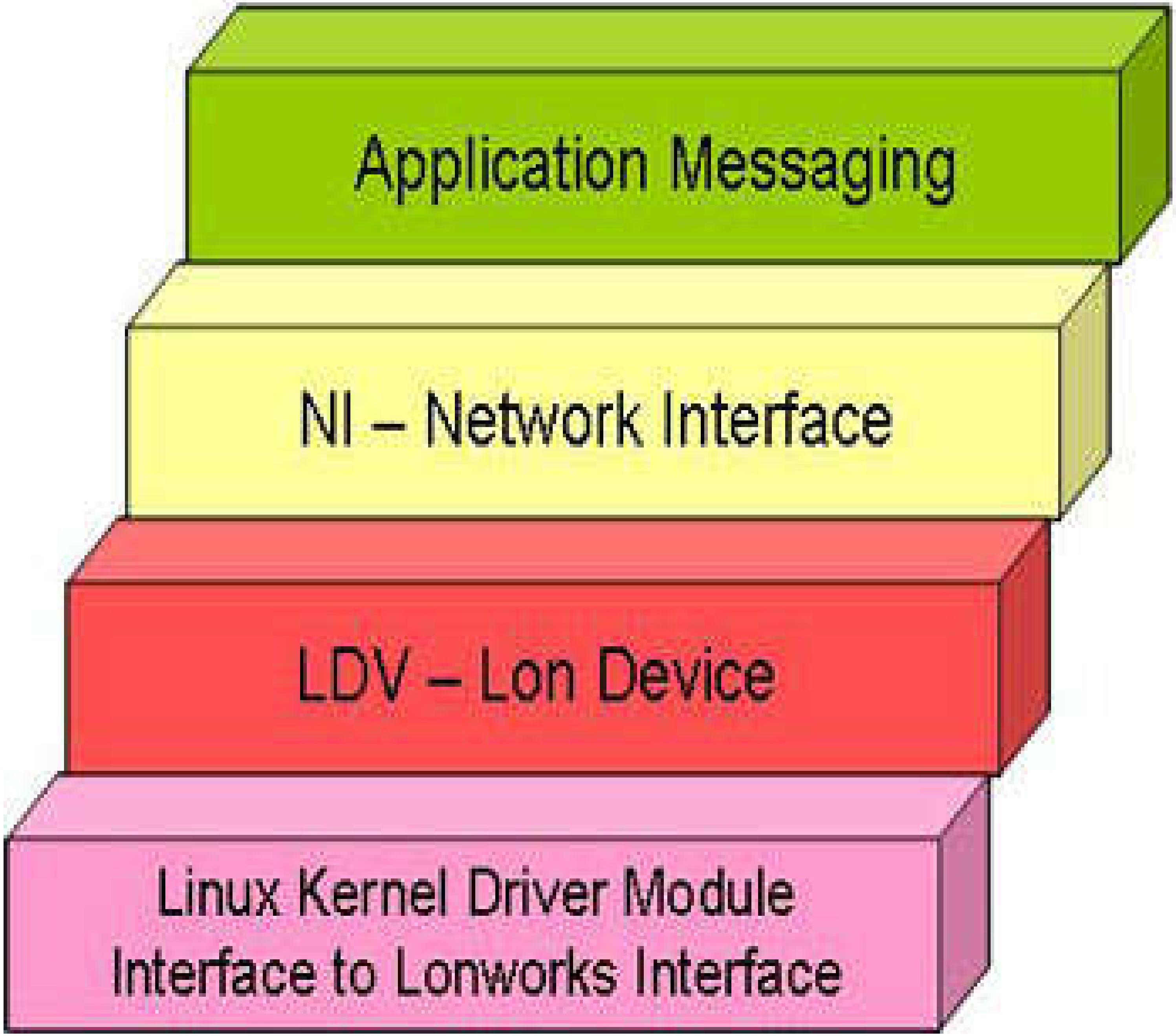
Neuron chip embedded with Echelon proprietary code to support LonTalk

Transducer chip designed to Echelon specifications

LonWorks Compatible Device

LON

Lonworks Software Stack



Application Messaging

NI – Network Interface

LDV – Lon Device

Linux Kernel Driver Module
Interface to Lonworks Interface

(Source: https://abtechteam.com/fieldbus_LonWorks.html)

LonWorks

- LonWorks: Physical Layer
  - The following options are supported:
    - Twisted pair
      - 1,250K baud (Transformer coupled Twisted Pair / Bus)
      - 78K baud (Twisted Pair/Free Topology)
      - Can supply up to 36.5 watts of DC power to devices
      - Supports bus / star / loop / combination topologies
      - 39K baud using standard EIA485 signaling
    - Power line carrier (10K, 5K or 2K baud)
    - Radio frequency (4.8K baud)

LonWorks

- LonTalk: Delivery Layer
  - Echelon proprietary; embedded in “Neuron” chip
    - Peer-to-Peer communications
  - Similar to Ethernet, except:
    - Lower cost implementation
    - Each device monitors network traffic level for advanced collision avoidance
    - Devices can be prioritized
    - Designed for real-time control networks rather than batch-oriented OA networks
    - Optimized for small messages (<66 bytes)

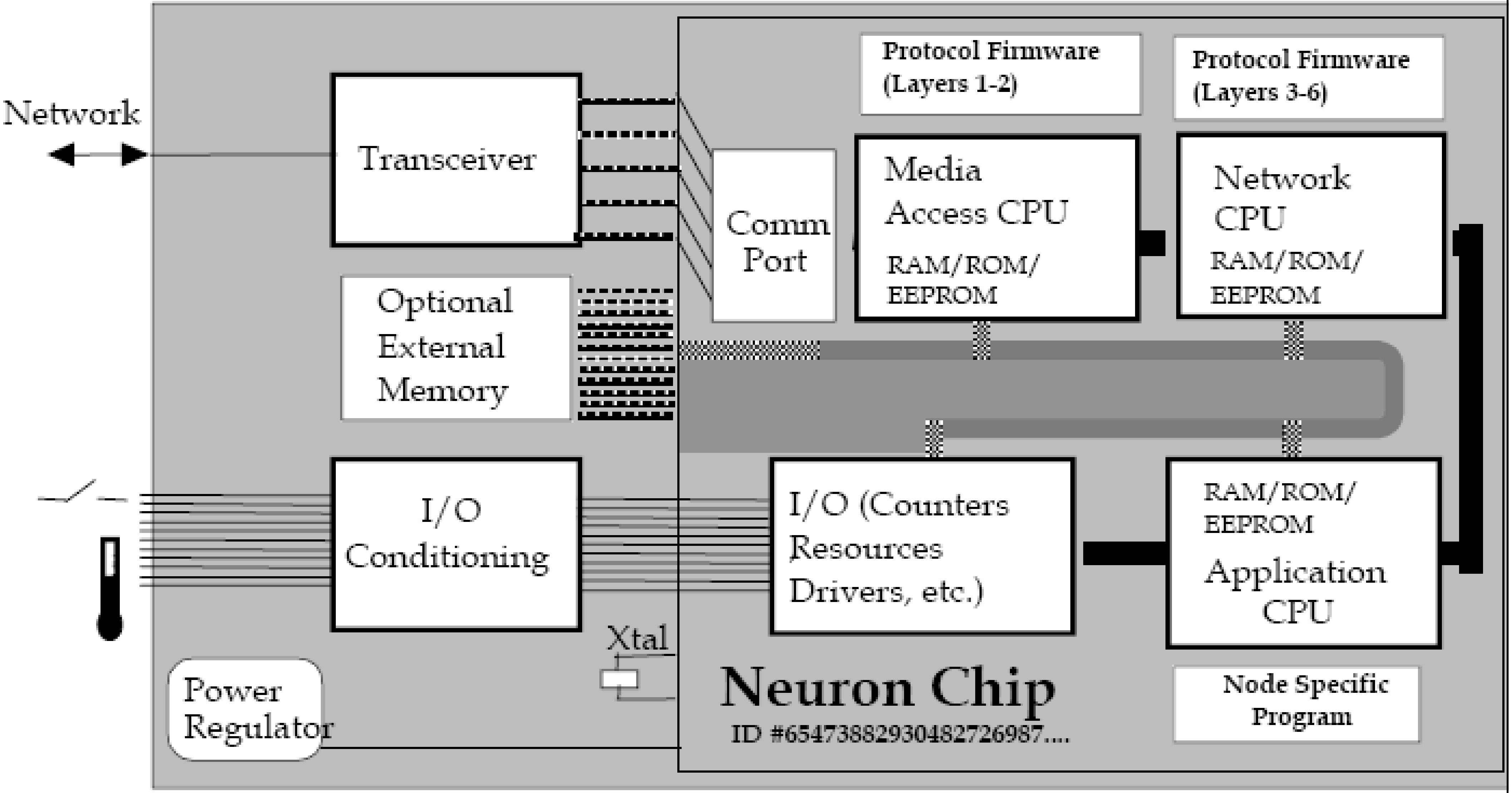
LonWorks

- LonTalk protocol
  - Designed specifically for control systems
    - Small packets (temp., pressure, status, etc, at about 12 bytes/packet) but can require hundreds or thousands of nodes & have the ability to send their packets within a very short time [c.f.: data networks – large data packets (kilobyte or megabyte packets) with a relatively small amount of simultaneous users]
  - Date types, profiles, etc. reviewed by the LonMark Interoperability Association (ensure they are interoperable)

LonWorks

- Neuron chip　神經元芯片
  - It is a microprocessor typically embedded in LonWorks products (to simplify the process for standardisation)
    - A complete system programmed on a chip; contains Read-Only Memory (ROM), Random Access Memory (RAM), and the input/output interface ports & communications protocol
    - "Neuron" = nerve cell body & all its process
  - Includes 3 microprocessors or CPU:
    - **CPU-1**: media access control (MAC) processor (layers 1 & 2 of OSI 7-layer model)
    - **CPU-2**: network processor (layers 3 to 6 of OSI 7-layer model)
    - **CPU-3**: application processor (run codes written by the user & manufacturer)

LonWorks device components



LonWorks

- LonWorks SNVTs
  - SNVT = Standard Network Variable Type
  - LonWorks controllers uses it to define data objects
  - SNVT allows for implementation of multiple applications for multiple manufacturers, make it easier for interpretation
- LonWorks SCPTs
  - SCPT = Standard Configuration Parameter Type
    - Provide a standard for documenting network message formats
  - SCPTs are used to download configuration data e.g. set points, offsets, gains, etc. to the devices by the network management tools

LonWorks

- LonWorks Transceivers
  - Transceiver = transmitter + receiver
  - Means of communication between the LonWorks network & the Neuron Chip
  - To interoperate properly, products must have compatible transceivers, otherwise, a router will be required
- LonWorks Routers
  - Intelligent hardware that filter the passing of messages between two network segments
  - Used to extend the length of a network or the number of nodes, and/or to change the media type
  - Can be configured in 3 ways: 1) a learning router, 2) a configured router, 3) a repeater

LonWorks

- What is LonMark?
  - A brand name & an association (formed in 1994), to promote and support those manufacturers that produce “interoperable” LonWorks products
  - Provide device-level assurance of interoperability through certification (LonMark logo)
    - Not all LonWorks products are LonMark certified
    - Different levels of how LonTalk is implemented
  - LonMark = Information Layer

LonWorks

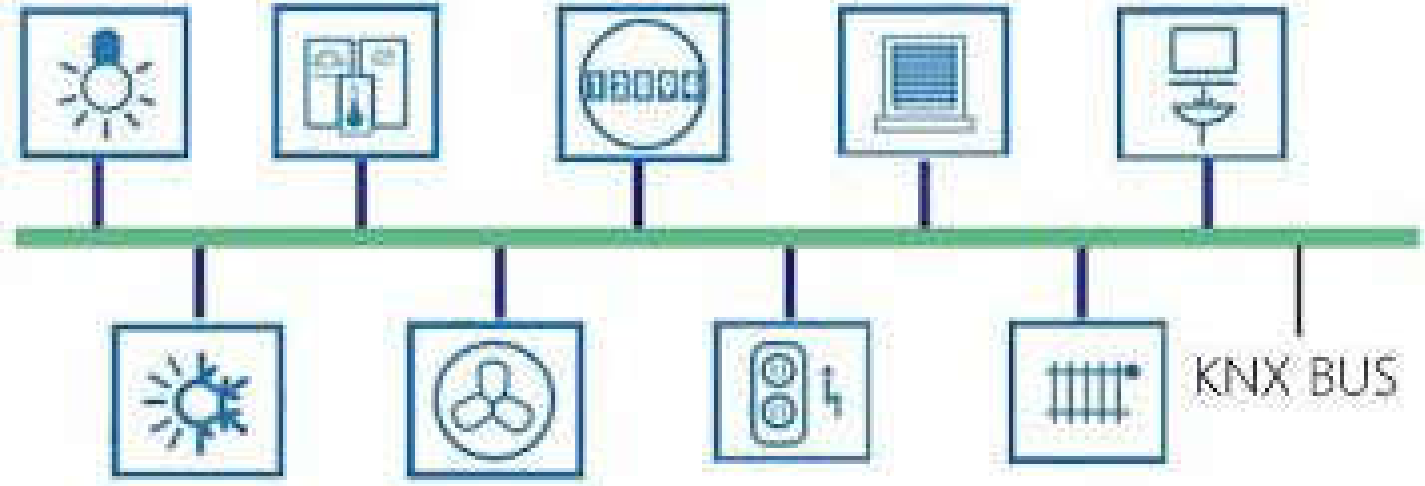
- Further info about LonWorks:
  - Echelon LonWorks system
    http://www.echelon.com
    - Online LonWorks Demonstrations
    - Introduction to the LonWorks System (PDF)
  - LonMark Interoperability Association
    http://www.lonmark.org
    - LonMark Design Guidelines
    - LonMark Technical Corner

KNX

- KNX (Konnex) communication protocol is an approved European (EN) & International (ISO) Standard (EN 50090, ISO/IEC 14543) which is widely found in BAS applications
  - KNX devices can manage lighting, blinds & shutters, HVAC, security systems, energy management, audio video, white goods, displays, remote control, etc.
  - KNX is based on three earlier standards: the European Home Systems Protocol (EHS), BatiBUS & the European Installation Bus (EIB or Instabus)

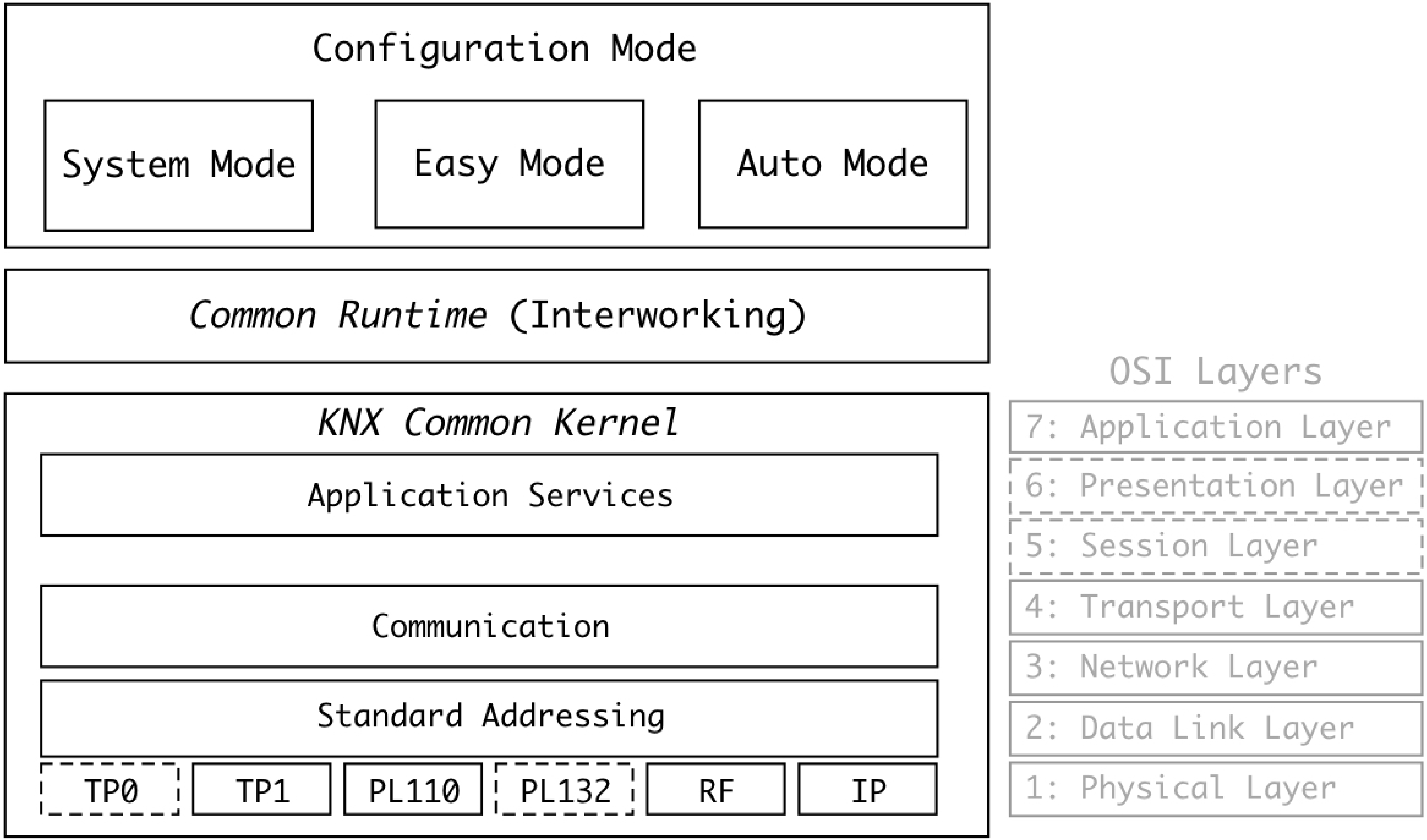
KNX

- KNX can use twisted pair (in a tree, line or star topology), powerline, radio frequency (RF), or Internet Protocol (IP) links
- KNX devices form distributed applications and tight interaction is possible



(Further info: KNX Basics https://www.knx.org/wAssets/docs/downloads/Marketing/Flyers/KNX-Basics/KNX-Basics_en.pdf)

The KNX Model system architecture

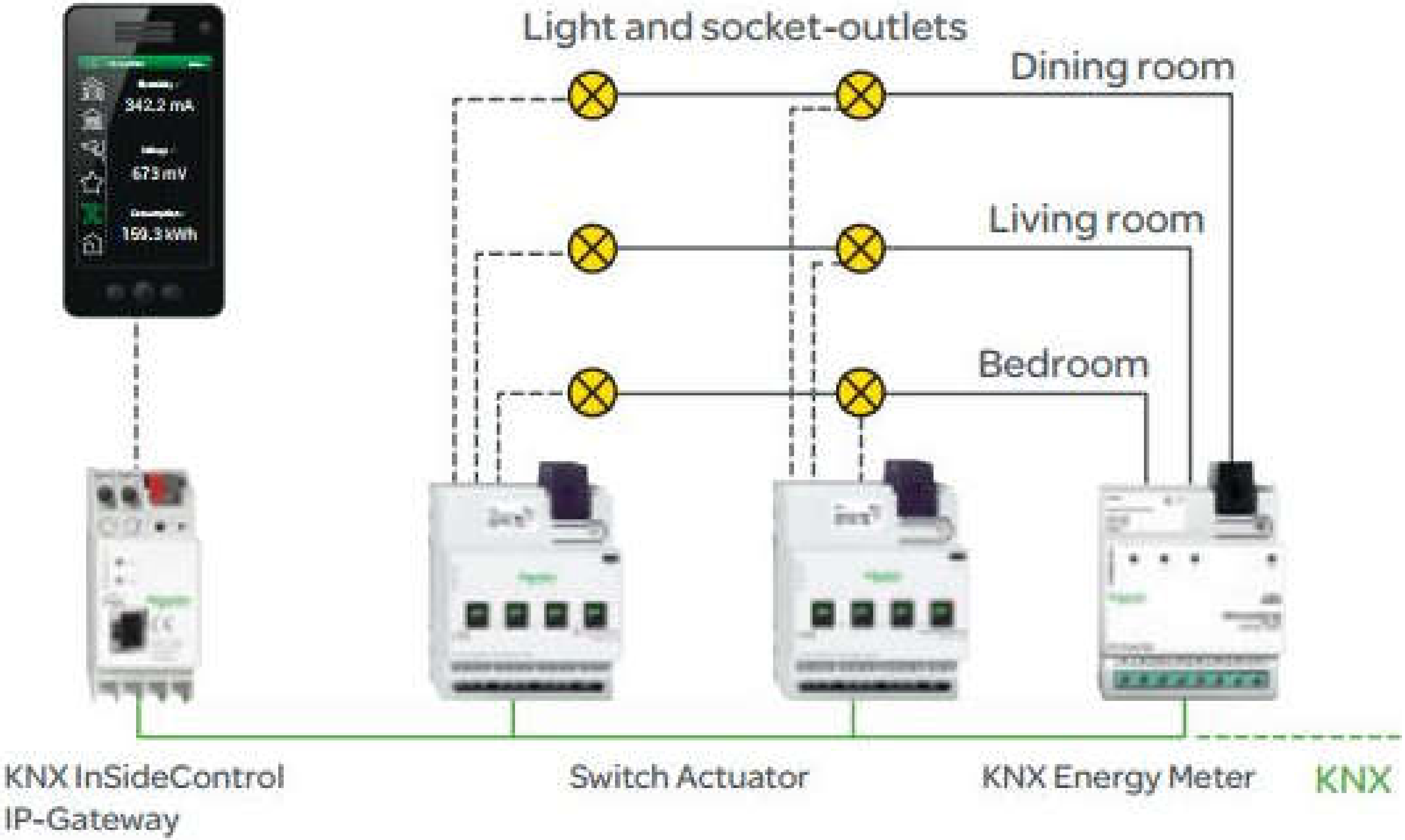


(Source: https://en.wikipedia.org/wiki/KNX)

KNX

- KNX system consist of:
  - A distributed bus system that allows devices to exchange information directly bus voltage: 24 VDC (+6/-4 V)
  - CSMA/CA protocol protects against data loss resulting from telegram collisions
  - Up to 12,000 bus nodes can be connected
  - Data transmission rate of 9.6 kBit/s, termination resistors not required
- Two types of devices: the sensor & the actuator
  - Together with controllers & other logic functions, system devices & components

KNX application example



(Source: https://store.chipkin.com/articles/knx-application-examples)

KNX

- Three configuration modes of KNX devices:
  - A-mode (Automatic mode): devices which can configure themselves & are able to be installed by the end user
  - E-mode (Easy Mode): used for simple systems & provides basic functionalities to the devices and can be programmed without any specialised knowledge & tools
  - S-mode (System Mode): used for complex installations requiring a high level of customisation & features
- Configuration may be achieved through local activity on the devices (e.g. pushing a button) or active network management communication over the bus

Further reading

- The Ultimate Guide to Building Automation Protocols https://guides.smartbuildingsacademy.com/the-ultimate-guide-to-building-automation-protocols
- Lohia K., Jain Y., Patel C. & Doshi N., 2019. Open communication protocols for building automation systems, *Procedia Computer Science*, 160: 723-727. https://doi.org/10.1016/j.procs.2019.11.020