

Moving towards interoperability in building services control

This module examines the common protocols that are allowing building automation and control systems to converge

By integrating all levels of building services into building automation and control systems, widespread 'smart buildings' and 'smart cities' edge a little closer to reality. When system components such as water heaters – which have previously been marooned in their lonely control environments – are fully connected using the mature, open and interoperable systems, the possibilities go beyond simply meeting regulatory requirements, and towards the nirvana of 'smart energy grids'.

This CPD will consider examples of the common protocols that are allowing building automation and control systems (BACS) to converge, so enabling the means by which the information that drives 'smart cities' may be collected and communicated. The core tasks involved in providing successfully interoperable BACS have long been established¹ as:

Data exchange – What data is required, and how fast and often it is needed; the requirement for control and optimisation of data; and what needs to be displayed and adjusted.

Alarms and events – From where alarms emanate; where events are logged and displayed; what indication is used, and how they are acknowledged; the information required from the alarm; and how it may be modified.

Schedules – For HVAC equipment that runs on schedule, how those schedules are read and modified.

Trends – The origin of the trend data; how it is transmitted and stored; how it will be processed and displayed (and where); and how the trend parameters may be modified.

Network management – The network diagnostic and maintenance functions that are required, and where they exist. Increasingly, the data access and security functions are a significant element of network management functions.

When assessing the suitability of a BACS, the list of core tasks makes a useful reference point. Although there is not always a clear breakpoint in the BACS hierarchy, there are three commonly applied terms that describe the influence of a particular protocol (see Figure 1):



CIBSE CPD Module 68

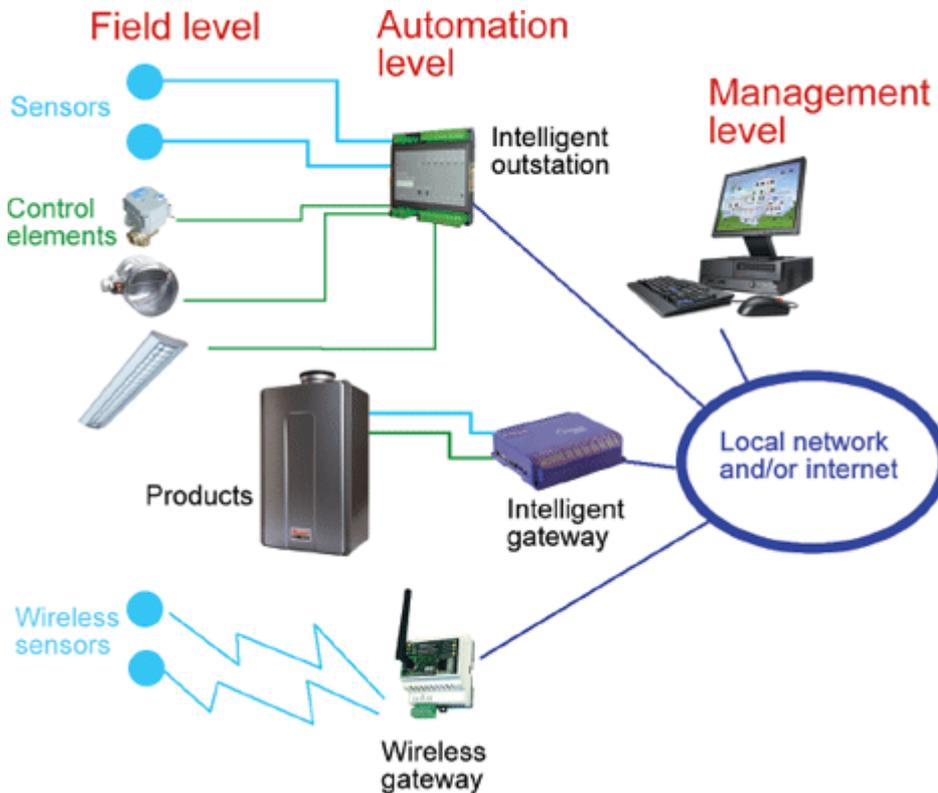


Figure 1: Levels of building control

Field level – Consisting of sensors and actuators. This is where the data is collected, and the final control takes place. Data typically passes in small packets, at frequent intervals.

Automation level – For room control and primary system control. Larger data transfers, aggregating the field level control and inputs with the control strategies, with cycle times of milliseconds/seconds.

Management level – For overall operation, monitoring and evaluation. This is the level where changes are made that may affect a whole system or automation sub-system. This may be undertaken locally to the system or, for example, through an internet connection. This requires a high data-exchange rate, as it potentially deals with data from the whole system.



Rinnai

sales@rinnaiuk.com | 01928 531870

CIBSE CPD Module 68

For the various components in a building to communicate, there needs to be a language – or protocol – that allows components to share information in an effective and efficient way, both at, and between, each of the operating levels. The standards that often determine this in building automation and control are BACnet and LonWorks. These exist alongside others more associated with the automation and field levels – such as Modbus and KNX, and more niche protocols such as DALI (digital addressable lighting interface). Each of the standards has its own strengths, weaknesses and protagonists. However, there is an increasing opportunity for coexistence of these systems, with the converters – ‘gateways’ and ‘bridges’ – becoming more widespread as the cost of microprocessor technology falls. (This software interoperability should not be confused with day-to-day operation and maintenance at the physical field level, where there will still be challenges in component interoperability.)

Manufactured products for building services are often developed to incorporate control input/output through a particular protocol or set of protocols. This will often mean that the manufacturer may have its own embedded controls within the core of the equipment, and then a bespoke integrated gateway to allow the interoperable network to access certain parameters. So, for example, the water heater in Figure 2 provides BACnet and Modbus access to 45 parameters, such as temperature setpoints, measured temperatures, water flow rates, fault diagnosis, and operating status. The gateway will convert those readings as defined by the specifically chosen protocol so that they can be accessed across the building automation and control system.



Figure 2: Increasingly, formerly stand-alone systems – such as this water heater – are employing bespoke integrated gateways to provide connectivity and interoperability with standard network protocols



Rinnai

sales@rinnaiuk.com | 01928 531870

An overview of selected protocols used in building control systems

There are many protocols in use, and a proper explanation for each one could fill a textbook. The following is an overview of those that are seemingly most widely used (see suggested reading at the end of this article for more detail).

Since much of the work of building monitoring and control is converging with the business and enterprise networks, these control protocols will typically include – or have thirdparty additions for – internet services that allow the sharing of information, and interaction, with local and global networks. Any BACS that has a route to the internet must have robust and well-maintained network security.

Modbus was developed by Modicon (now Schneider Electric) and released in 1979. The standard was initially aimed at programmable logic controllers, and its biggest sector remains the industrial controller market. In 2004, it was transferred as an open standard to the Modbus Organisation, and is now freely available. The implementation of Modbus is relatively simple, requiring little ‘specialist’ network technology – it is a standard that many of the automation early users grew up with, and continues to maintain a large user base. Although not particularly aimed at building automation and control, the simple common messaging structure has attracted widespread adoption, using customised software interfaces. Modbus is able to work over ethernet media and the internet (as Modbus TCP/IP), but its fundamental design is such that, in the master/ slave relationship, only the master can initiate a communication – the slave (for example, a temperature sensor or speed controller) would need to wait to be polled for its output. So, at the automation and field levels, it continues to be widely used. It is available in the control offerings of many different vendors to support automation and field-level connectivity.

KNX – which, in 1999, succeeded European Installation Bus, European Home System and BatiBUS – grew out of standards that aimed to allow home and office control systems to communicate readily through a dedicated network separated from power systems. Because of robust assurance procedures, KNX-certified products made by different manufacturers can be confidently combined, and this has made the application of this protocol particularly strong at field and automation levels. The provision, by KNX, of accessible manufacturer-independent design, configuration and operation software tools has helped to grow the protocol’s popularity. At a local level, it often uses a simple twisted-pair cable for transmission. However, it can be used equally well over a wider range of media, including those in IP networks.



CIBSE CPD Module 68

LonWorks uses the LonTalk communications protocol that is held in the memory of the processor chip of every LonWorks-compatible device. LonWorks is a proprietary protocol developed by the Echelon Corporation, in conjunction with Motorola, in the early 1990s. Initially, this required a dedicated proprietary 'Neuron' chip – which also provided local control – but, since 1999, this is no longer a requirement, and other microprocessors with appropriate programming may be used.

The local operating network (Lon) collects together intelligent, independent products (nodes, such as boilers, valves or sensors), potentially employing a wide range of communications media that are then used to provide feedback and control. It can also be used over the internet. Processing capabilities and input/output in each node can undertake control action using input data and actuators, while also interacting with any other devices on the network using LonTalk.

LonTalk is a protocol that is optimised to transfer – reliably and swiftly – the short packets of information that are required in control and feedback applications. All devices on a LonWorks network must be 'bound' to each other – that is, set up to be known to each other – and, similarly, any gateway device that moves information between networks and protocols will only receive data from those devices it is bound to. All LonMark-marked products must have been verified to conform to the LonWorks protocol, and are offered by many manufacturers.

LonWorks has more than 210 data types – known as standard network variable types (SNVTs, pronounced 'sniv-its') – that define whether the data represent variables such as temperature, pressure, humidity, or counters to measure such things as on/off cycles, and in what format it will be offered across the network. These standardised variables have helped in maintaining and developing the success of LonWorks.

LonWorks spans all levels of control hierarchy, and is seen as being particularly strong at field and automation level.

BACnet was originally developed in 1987 through ASHRAE and has been an ISO standard since 2003. It enables interoperability between different building systems and devices – not providing the control logic, but supplying the means for communication and data handling. It is written specifically to allow interoperability between all HVAC devices, as well as with other building systems and devices, such as lighting, security systems, vertical transportation, and access control.



Rinnai

sales@rinnaiuk.com | 01928 531870

CIBSE CPD Module 68

Typically, each device – known as a BACnet object – is formed of a micro-based controller with specific software that links to the component (such as a water heater). Within that device there are standardised definitions, including a device number (unique within its local network) and a collection of information about the device, and any input and output points that it monitors and controls.

There are a number of services that may be included in the devices, which are grouped into: object access, alarm and event management; scheduling; trending; files; and device and network management. As well as the device number, a particular building automation device may include none – or many instances, of – these services. When used across IP networks, BACnet does not require the use of TCP, but utilises the faster UDP protocol.

As an open standard, BACnet may be employed by any manufacturer, and innovative evolution is encouraged. However, there is a standardised classification methodology that ensures the terms and format are understandable, so that devices may be specified in terms of their function. Optionally, devices may be tested as compliant with the BACnet standard, and awarded a BTL Mark.

BACnet provides services that transcend the management, automation and field levels, and is often used in combination with other automation and field-level networks because it has strong management and wide area networking capabilities. BACnet relies on third parties to develop administration and design tools – many vendors provide impressive software offerings with their BACnet-enabled products. The BACnet specification is under continuous development through ASHRAE SSPC 135, representing all industry sectors.

The interoperability of all these protocols is key for the proper operation of smart buildings. Practically – either through in-built processes or third-party devices – all these protocols may coexist (at some level) to form an integrated BACS.

However, effective BACS is no replacement for robust, well-designed and controlled end systems. Manufacturers need to develop products with appropriate internal control software/firmware so the BACS can communicate with the vital operational parameters. So, considering a continuous-flow direct water heater, the combustion process may be closely controlled to optimise operation, but unless that information can pass to the management level – for example, through appropriate ‘objects’ or ‘SNVTs’ – opportunities for ‘smart’ operation may be limited.



Rinnai

sales@rinnaiuk.com | 01928 531870

CIBSE CPD Module 68

As technologies – such as autonomous wireless sensing and product control interfaces – evolve, the BACS will have to be flexible and robust to maintain meaningful operation. Realistically, this might enable a water heater in the sports centre of tomorrow to aggregate feedback from internet-sourced weather forecasts, the number of customers on site, and the demand on local gas supplies – setting appropriate flow-water temperatures and combustion parameters to satisfy customers and make responsible use of resources.

Key terms that underpin IP-based control protocols, with simplified explanations

Ethernet. Ethernet is the most widely installed local area network(LAN) technology that provides the physical communication service. It reads and writes ‘frames’ of information through a medium (for example, twisted-pair cables or optic-fibre). The frame has a limited size, and includes the sending and receiving of MAC (ethernet medium access control) addresses (no two ethernet devices should ever have the same address). Ethernet supports all popular network protocols, and is principally used for IP.

Protocol. A special set of rules to allow communications between devices. These may be hardware rules (for example, the type of cable) or software rules (for example, the type of packet). Computers rely on protocols as humans do on language.

IP (internet protocol). This allows data sent from one computer to reach another across a network. Each device has at least one IP address that uniquely identifies it. IP ‘packets’ contain small amounts of information, and many packets are needed to send a complete message. For equipment to communicate on the internet, a second ‘transport layer’ protocol must also be used, such as TCP or UDP.

Packets (or ‘datagrams’). IP data is sent in little chunks of data called packets. (Packets are carried in frames.) Each of these packets contains both the sender’s and the receiver’s address, plus other information. Any packet is sent first to a ‘gateway’ computer – or ‘router’ – that can relay the packet to its correct destination. If it is outside the local network (on an intranet or the internet), it forwards the packet to an adjacent gateway that, in turn, reads the destination address and so forth, until one gateway recognises the packet as belonging to a device within its immediate neighbourhood or domain. Successive packets may take different routes, with different travel times, and some may not make it to the destination at all.



Rinnai

sales@rinnaiuk.com | 01928 531870

CIBSE CPD Module 68

TCP (transmission control protocol) is a protocol used with IP to send data in packets between devices. By first setting up a connection between the sender and receiver, it provides end-to-end reliability, sequencing (of packets arriving in a random order) and flow control. Whereas IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual packets of a message.

UDP (user datagram protocol) works with IP without first setting up a sender-to-receiver connection, and passes 'datagrams' –self-contained, independent entities of data, each with sufficient information to be routed from the source – to the destination. It readily performs the use of 'one to many' messages (unlike TCP). It is used by applications that require speed, and do not require the level of service of TCP (the applications do the control/checking themselves). It is particularly useful where short – and possibly independent – messages are being conveyed.

© Tim Dwyer, 2014.

Further reading

CIBSE Guide H Chapter 4 , 2009.

BRE IP 1/07 *Internet Protocol: an introductory guide* is a good introduction to IP and associated terminology.

There is an interesting overview of practical experiences of protocols at www.automatedbuildings.com/news/oct11/articles/andydavis/110925014909andydavis.html

A more formal comparison is at www2.ic.uff.br/iwssip2010/Proceedings/nav/papers/paper_49.pdf

References

1. Ehrlich, P. and Pittel, O., *Specifying interoperability*, ASHRAE Journal 41(4):25-29, 1999.



Rinnai

sales@rinnaiuk.com | 01928 531870