Development of a wireless distributed control system.

By AL Walker, President, Walker Technologies Corp

Article published in Automated Buildings Aug 2013


Walker Technologies has been in the HVAC control systems business since 1985 and has systems installed worldwide. Over the last 5 years, Walker Technologies has developed a viable wireless BMCS (Building Management and Control System) that is being used successfully in several applications. These include both stand alone fully wireless systems and as part of new or existing installed “wired” BMCS. However, because it is wireless, we have learned that a new set of rules must be used in order that these systems work as reliably as a conventional wired system.

ADVANTAGES OF WIRELESS BMCS

If a reliable wireless communication strategy is implemented in a BMCS, then there are huge advantages for both retrofit and new building construction. The major advantage of wireless systems is substantially reduced costs for installation, servicing and future expansion. Applied to multi unit facilities such as Malls and MDU’s, wireless gives owners a cost effective route to gaining the advantages of a BMCS to monitor and reduce energy use.

1. No cost for installing and commissioning of network LAN components. No issues with ground loop on communication network. No requirement for shielded cable.

2. Installed system is infinitely expandable. – Just add more wireless controllers and they will join in.

3. All BMCS control panels are located in a single central location. A wireless mesh network links to all other controllers. This central control panel allows simple servicing and expansion and removes the need for EMCS network communications cabling.

4. No engineering drawings or as-built drawings are needed when servicing or supporting the system at a later date. No lost or unrecorded control panels.

5. The structure of a wireless based control system results in less need for programming within the main control panels. This also reduces initial installation cost as well the cost of ongoing support. In many cases, a diligent owner can support the system in house by simple replacement of controllers.

THINGS THAT ARE DIFFERENT IN A WIRELESS BMCS

As with a comparison to wired versus wireless telephone connections, wireless links in a communicating BMCS system will always be less reliable than a direct wired link. This difference must be taken into consideration at the outset when developing and deploying such a system, but, as we have with cell phones, we can adapt to the difference.
THINGS THAT ARE DIFFERENT IN A WIRELESS BMCS (continued)

1. WIRELESS EXPERTISE
   Installation, management and support of an installed wireless control system requires a new set of skills, not those normally held by HVAC technicians. These skills are currently the domain of IT personnel. Having an IT expert manage the wireless components of the installation makes sense.

2. WIRELESS SIGNAL DROPOUT
   A new paradigm for wireless strategy is required. It is not possible to close a control loop across a wireless network. With our wired I/O BUS or SmartLAN, our contractors normally could close control loops over these communication links because throughput was determined. -- as long as the real time response of the control loop could handle it. Just as your cell phone can drop out annoyingly, you can expect wireless links within a controls system to be intermittent or to fail periodically as well. This drop out must be considered as part of the strategy for system communications.

3. AUTONOMOUS CONTROLLERS
   Within a wireless network, each wireless control device must be autonomous. It must perform all its control functions internally with its own wired I/O. This could be in concert with a regular stream of wireless command data such as setpoint, and other tuning parameters, however it must also have a fall back strategy for periods when it detects a loss of wireless command data. The best application of wireless is for systems of supervised unitary controllers. The practise of wiring several control loops into a single main controller does not work well with wireless. However, by moving the control programs from software in the main panels to the unitary controller a simpler, more serviceable control system is created. This gives huge advantages for the end user on the long term. More complex control strategies can still be implemented successfully by having control presets in the devices that are commanded by the supervisory control system. Presets and setpoint commands need to be saved in EPROM (?) memory in the wireless controller so that operation after a power failure is assured.

4. POWER FAILURE RECOVERY
   Considerable thought must be put into defining operation of control devices after a power failure. Although a ZIGBEE network will usually reboot and re establish communication paths fairly quickly, it could take several minutes before devices start receiving valid commands. This mandates that a clear power fail recovery strategy needs to be in place.
   -Occupied or setback state?
     If a device recovers in its unoccupied state and the area is really occupied then the tenant will not be happy. So a wireless controller must wake up as occupied and using the setpoint knob as the device setpoint. This is also the case if the setpoint knob is changed by the occupant at any time. Reversion to non-occupied state can occur after a valid supervisory command is received and also after a time period which, depending on system conditions, may be up to 12 hours. This is further impacted by fact that the head end may need data from controllers to “calculate” the occupied state.
   -Other tuning parameters and supervised variables.
   Hopefully this information has been saved in non volatile memory and verified by the head end prior to the power outage so “last values” will automatically be used until new ones are received.
RESULTS OF THE DEVELOPMENT PROCESS.

As Walker Technologies developed our wireless system we used the ski chalets on MT Washington in Courtenay B.C. The mountain usually gets a large amount of snow (up to 500cm) over the winter so we expected large variations in wireless connectivity. We built the mesh network between 5 chalets using high powered radios to jump the distance between chalets. To determine occupancy we polled motion detectors on each baseboard thermostats—usually 4 to 10 in each chalet. We then automatically changed the chalet’s occupied state based on the number of zones that were occupied. This setup proved to be an extremely good mechanism to underline the differences between wireless and wired communications and helped us lay out the rules in the following:

1. **Wireless connections are not like wired connections.**
   
   While we know that if a wired connection fails there is a problem, usually mechanical, that can be fixed. When a wireless connection fails, it will likely fix itself, but unfortunately we can not be sure when that will happen.

2. **Wireless Full Duplex is a conflict of terms.**
   
   You can not expect a full duplex wireless connection to be full duplex. Wireless connections across a mesh network are one way. A full duplex connection in a mesh network consists of two single wireless connections, one from the source to the destination across the wireless network and a second one from the destination back to the source. It is more or less guaranteed that each signal path will be different; with different routing, different obstructions and different reflections between source and destination. It can not be assumed that both connections will be active at all times and this must be figured into the strategy.
   
   If we are using zone occupancy to determine occupied state of a group of zones, loss of feedback information may cause the head end system to make the wrong decision. In making control decisions a wireless head end must also consider the age of its data when making control decisions.

3. **Wireless connections are time sensitive.**
   
   We all know what it is like to use our cell phone while driving (hands free). Our conversation will always be impacted by time as we drive in and out of cell zones. This also impacts fixed wireless links. Wireless communications vary throughout the day and are affected by temperature, humidity, barometric pressure and humanity, not to mention the delivery truck that just parked out front. We never know when there will be an interruption of the wireless data stream between two points, so as a general strategy we need to continuously re-transmit information. The time delay for this retransmission depends on the requirements of the system, but getting data updates every few minutes is generally appropriate. This also gives us a critical piece of information that allows us to dynamically monitor the integrity of the wireless network and the specific data from individual controllers.

4. **The age of wireless data must be considered**
   
   One piece of information that is crucial when looking at any data received over the wireless network is the age of the data. This is important not only for inbound data from devices sending status information back to the head end, but also for devices receiving setpoint and scheduling information from the head end. At both ends, the devices need to be aware of transmission status and have a course of action to take when communication fails either momentarily or permanently.
The simplest way to monitor communication status is to keep track of the time since last transmission. In our systems this is know as the Last Transmission Time (LTT). We use minutes as the metric – one to two minutes is normal, several minutes is warning of some issue. An hour or so may indicate a problem and the individual zone should be checked.

At the head end, an alarm triggered by a high LTT from any device will give and automatic annunciation of communication issues. The same information reported in the feedback from devices gives continual assurance that these devices are receiving commands. In training the end user, it is straight forward to educate them on the importance of paying attention to LTT and what to do if this gets too high.

5. Point to point and global Commands both have their place.

We have found that within a ZIGBEE mesh network, point to point commands from devices back to the head end seem to work well, allowing report data to their assigned controller within a one minute time frame. Data is sent in small packets every 30 seconds from each controller. These packets are received randomly so some collisions will occur. This strategy is the best fit because we can not successfully create a timely master slave relationship using a mesh network.

For commands such as setpoint and schedule information sent out to individual controllers, we do have control of the command frequency so we use a token passed between head end controllers to ensure that outbound commands are sequenced over time. Each controller also sends data out with delays between packets. By including address information in the command packets these out going commands can be sent globally.

In a mesh network, global commands propagate to all controllers through the network and so, tend to “ring” in the wireless network for a short time. However global information gets through to the destination controller much more reliably and often when a controller has a high LTT for data coming back it is still receiving global command data that is sent out to all controllers.

CONCLUSION

If a new set of rules is followed for the structure and interconnection of devices used, a wireless BMCS can be successfully deployed. Because a wireless system is less expensive and generally less complex, the cost of ownership is lower. Wireless allows BMCS systems to be applied cost effectively in areas where use of these systems was previously too expensive.

awalker@walkersys.com