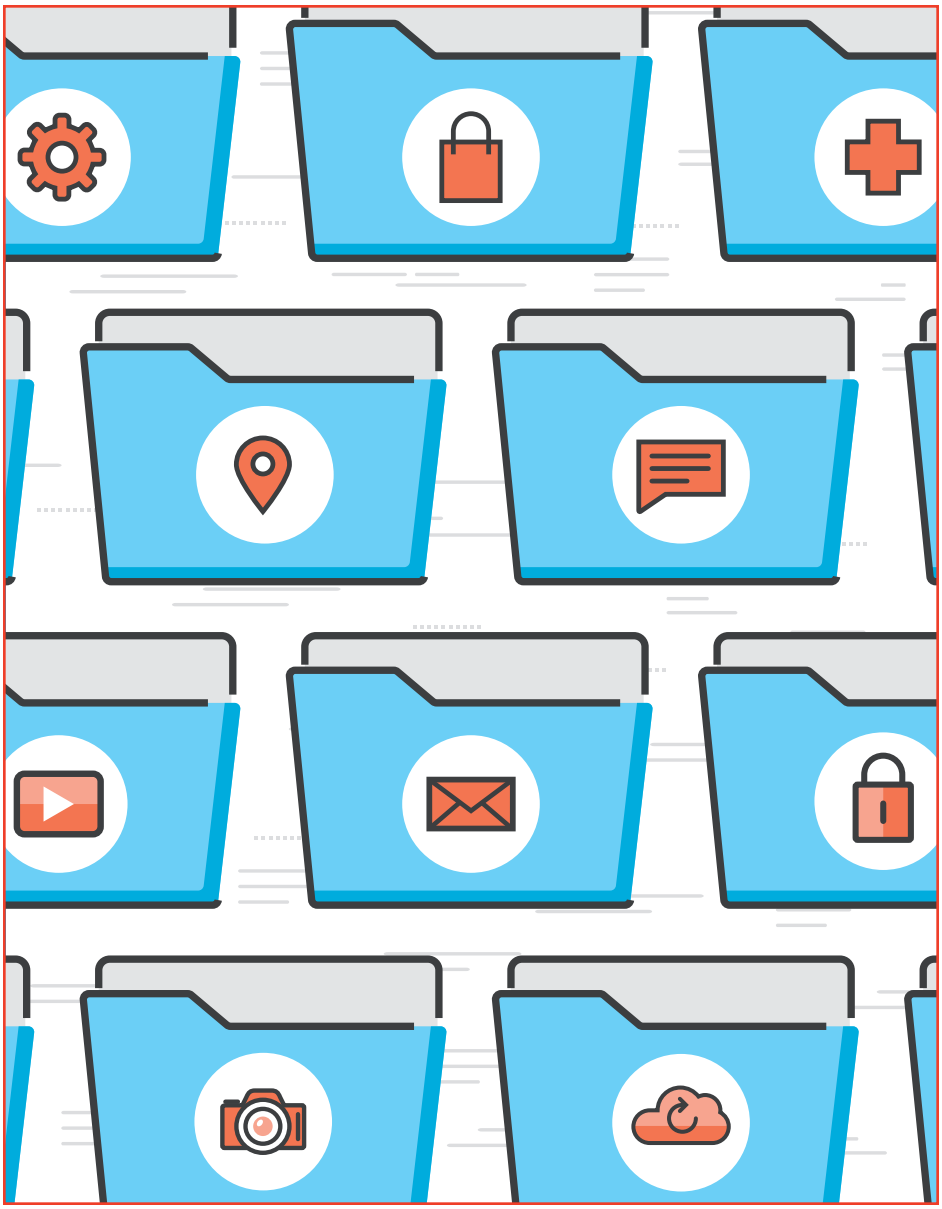
Spring 2017 Volume 14, Number 1

iHOMES and BUILDINGS

THE MAGAZINE OF THE CONTINENTAL AUTOMATED BUILDINGS ASSOCIATION



Organizing an Internet of Things

How to challenge gender norms in the facilities services industry

Go Green...Save Money?

Total Cost of Ownership: The Key Metric for Multi-DRM Strategy

EnOcean and the Internet of Things

Printable and Flexible Electronics Enabled Intelligent Buildings

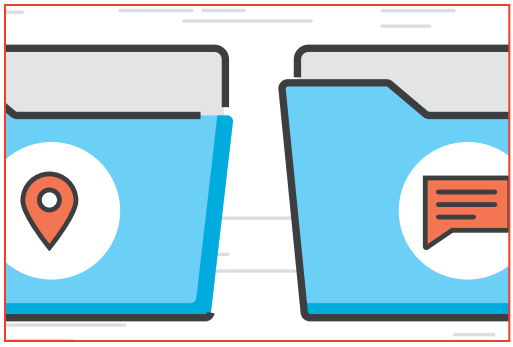
CABA™ Connect to what's next™

www.caba.org/ihomesandbuildings

iHOMES and BUILDINGS

THE MAGAZINE OF THE CONTINENTAL AUTOMATED BUILDINGS ASSOCIATION

Spring 2017, Volume 14, Number 1



Contents

Features

Columns

Departments

Ken Wacks' Perspectives

Organizing an Internet of Things

by Ken Wacks

In the spring 2016 issue of *iHomes and Buildings*, I explained that the "Internet of Things" (IoT) describes machine-to-machine communications among devices. In home and building systems these devices are typically sensors, actuators, controllers, and user interfaces.

The method by which IoT devices communicate was the subject of my fall 2016 article. If every device were assigned an Internet address, it would be possible for any Internet device to communicate with any other Internet device to send data, query status, or exercise remote control. I cautioned that if the cybersecurity and privacy issues discussed in the article were ignored, there would be the potential for unintended consequences where IoT descends into chaos.

Home and building systems have generally been organized around applications (lighting, entertainment, comfort, safety, etc.) with a controller to manage the devices, user inputs, and remote access. It is possible to deliver new services facilitated by IoT while maintaining the benefits of application control. We need to blend lessons learned from decades of deploying home and building systems with the potential benefits of IoT.

Bus communications

The art and science of communications evolved from remote signaling. A waving of a torch on a distant hill might have meant that a stranger was approaching. A lookout in a turret would be scanning for signals from multiple locations. Centuries later this person was replaced by a central processor handling multiple inputs and outputs.

When each input and output device has a unique connection to the processor, the identity of each remote device is unambiguous. The introduction of a shared bus required that each device be assigned an address so the processor could track the source and destination of signals.

Telephone systems during the second half of the 20th century were designed to share a common communications channel. Data from multiple sources were assigned to sequential time slots on a single long-distance line in a scheme called *time division multiplexing (TDM)*.

The Internet extended TDM with the transport of fixed-length data packets on a shared communications channel. Like physical mail each packet includes a source and destination address in order to deliver the packet to the intended destination. In this scheme each computer or device using the Internet is assigned a unique address.

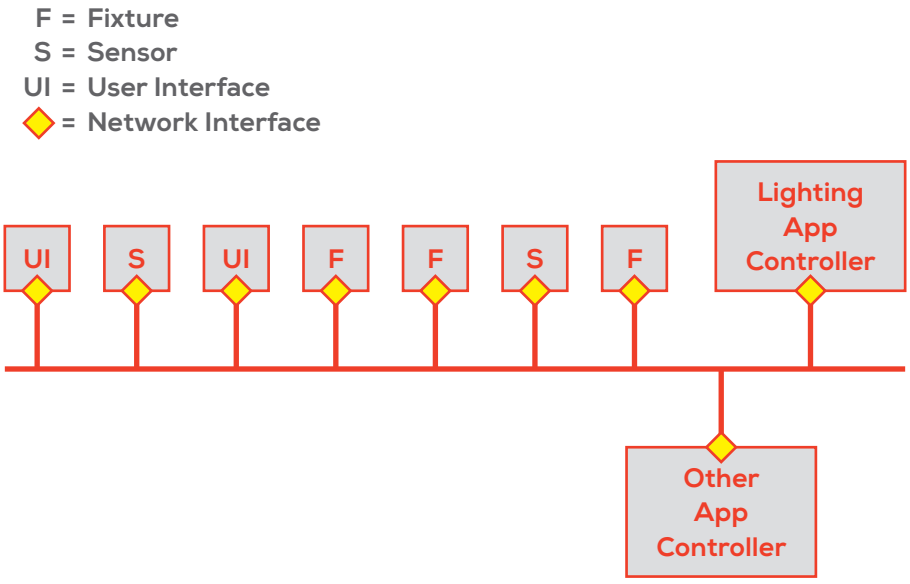
This method of sharing a communications channel was adopted for local area networks (LANs), as illustrated in the physical model of Figure 1 for a lighting control system. Even though the lighting components share a common bus, they are managed by a lighting application ("app") controller, as shown in the logical model of Figure 2. The shared medium in a LAN is called a *bus*, where messages to connected devices contain device addresses. There are many choices in LAN protocols for home and building automation networks using wired and wireless media.

LAN buses connect to the Internet via a *gateway* or a router. A gateway is an interface between networks running different protocols; a *router* adapts the same messaging protocol to a different network.

Logical home and building systems

A shared medium enables communications between any attached devices. However, home and building control systems have developed and are marketed as application-centric. This fundamental concept evolved from commerce among specialists. Just as we learned from the nursery rhyme about the butcher, the baker, and the candlestick-maker, so economics favors commerce among specialists. This can be expressed in a home automaton network as the logical interaction among applications shown in the logical models of Figure 2 and 3. The Home

Figure 1 – Shared Bus in a Local Area Network



Systems Coordinator in Figure 3 might be a user interface console, a smart phone, or a voice control device.

Each application controller is programmed with algorithms tailored to lighting, energy management, safety, etc. A promise of automation is interoperability and coordinated actions among applications. For example, if a safety system detects a fire in one part of a home or building, the following actions might be initiated, possibly with the assistance of a Home Systems Coordinator:

- Alert the residents with a siren.
- Flash the lights to illuminate a safe exit.
- Summon the fire department.
- Turn off any air-conditioning or heater fans.
- Turn off heating appliances.
- Mute any entertainment devices.
- Raise any automated shades.
- Flash lights visible from the street.

With every device interconnected via IoT, it is physically possible for the sensor that detects the fire to send messages to all the devices that perform the functions listed above. However, this would eliminate the additional functions provided by a safety controller, such as validating the sensor signal to eliminate false alarms and prioritizing the sequence of actions to focus first on life safety, then to summon help and protect property.

Benefits of IoT Coordination

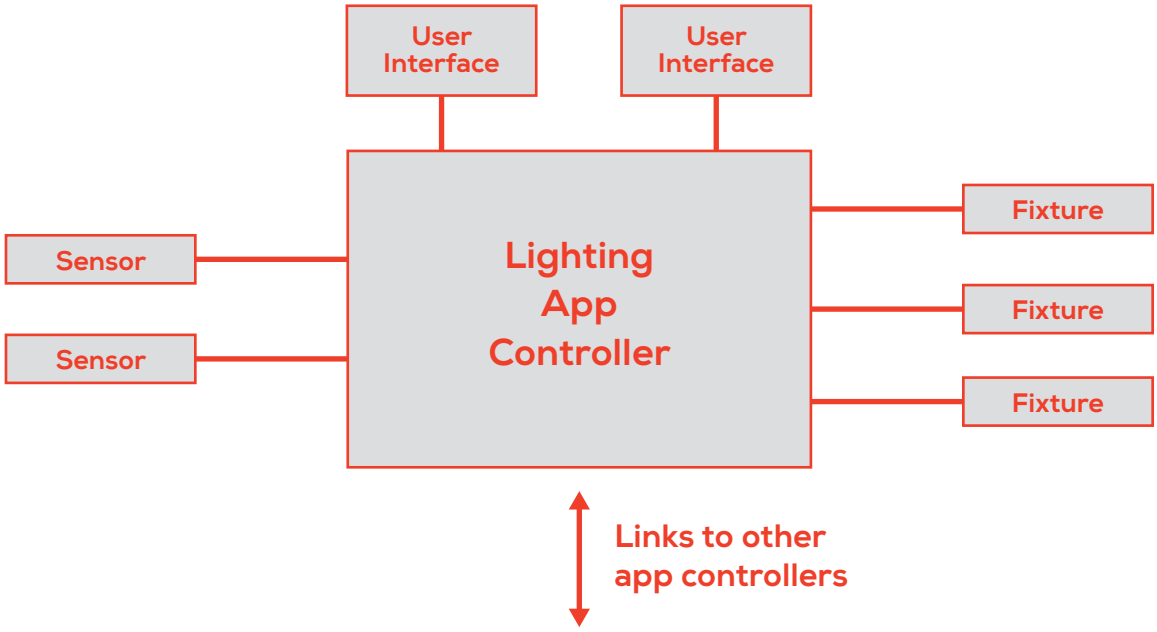
Coordinated action in a crisis is critically important. A fire safety controller might:

- Confirm the location of a fire based on inputs from all available smoke and heat detectors.
- Issue an alert to all other controllers about the fire and location.
- The other application controllers could be preprogrammed for specific reactions to a fire notice, which may depend on the location of the fire.

In an IoT environment every device could communicate with and possibly control every other device. However, there are benefits to depending on controllers specialized for each application rather than allowing a free-for-all:

- Each controller serves an application domain consisting of sensors and actuators.
- These controllers might set operating parameters for connected sensors, such sensitivity and thresholds for issuing notifications.
- Each controller processes user inputs from an associated user interface, which may be

Figure 2 – Logical Model of a Lighting Application



shared among applications via the Home Systems Coordinator in Figure 3.
- Each controller is programmed to manage which parameters are controllable and observable from other application controllers.
- Updates for one application do not jeopardize the integrity of the entire network.
- Each controller is responsible for network management as devices associated with an application are added, removed, provisioned, and configured.

Security and privacy domains

Achieving data security in a shared-medium network is challenging. Every device on the network bus can see the data for all connected devices. There are well-established techniques for data security that depend on a set of rules, protocols, and secrets known only to the sender and recipients of messages intended to be protected.

The key elements of data security are:

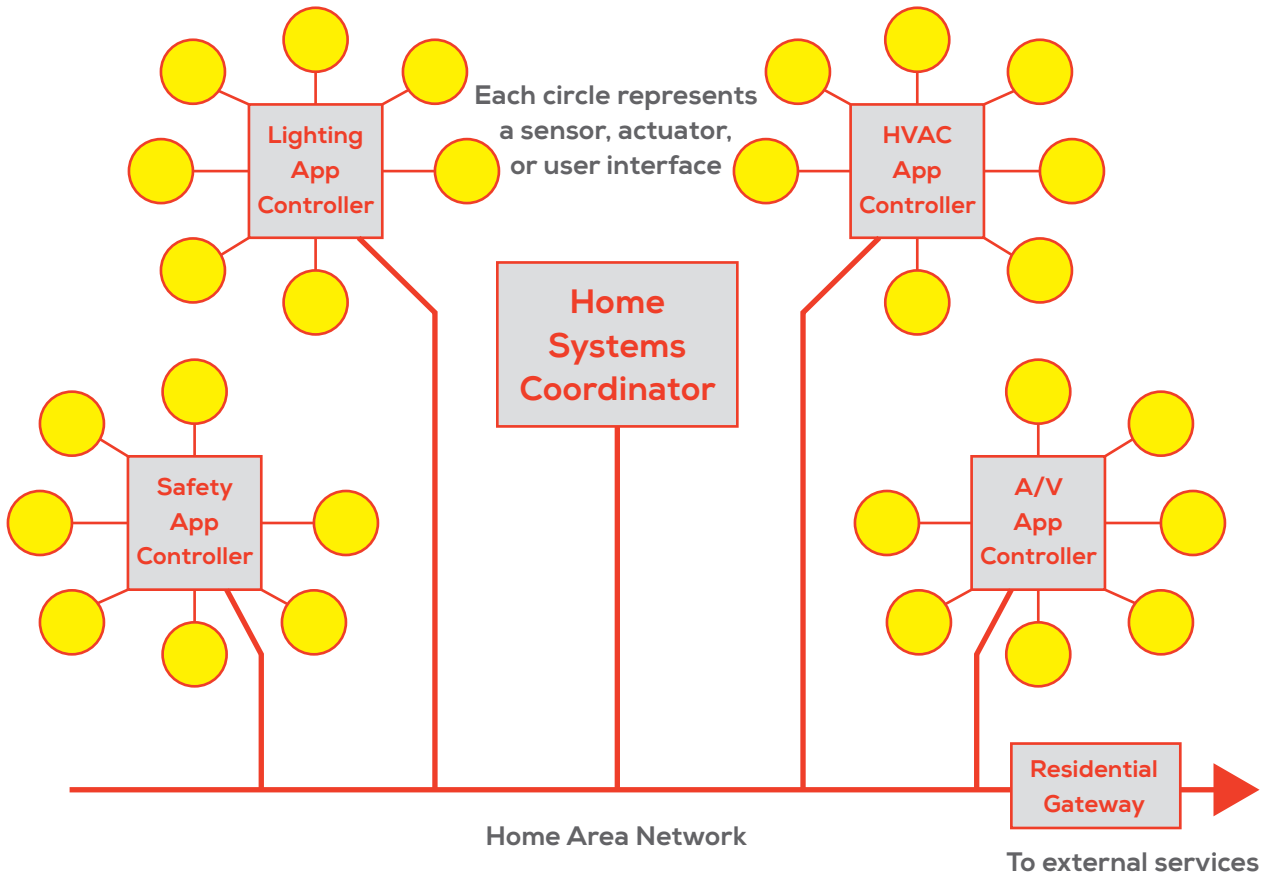
- **Authentication**: which devices and users are allowed onto the network.
- **Authorization**: what each device or user is allowed to do, such as requesting information or exerting control.
- **Encryption**: making the data or command understandable and verifiable only by the intended recipients to prevent message interception or insertion.

For proper network security, every participating device must be programmed with the correct security algorithm. Security depends on trusted entities responsible for authenticating devices and users (with *passwords* and *tokens*), authorizing actions (with *certificates*), and maintaining the secret codes (with *keys*) for encryption. Effective security requires agreements not only on the algorithms, but also on the interactions among the devices and the trusted entities. A regime for validating security programs and for vetting trusting entities is essential.

Security can be inadvertently compromised by a weak link – perhaps a device that is miscoded or a trusted entity with a database that was not properly updated. Data security could be threatened deliberately for malevolent purposes. Adding layers of security can enhance protection against these threats.

Multiple layers of security are required to achieve "Defense in Depth," as illustrated in Figure 4. First, each

Figure 3 – Logical Organization of an Integrated Home System



component in the external network is protected. Then, the entire external network is protected. For example, a service provider must ensure that customer databases are secure from thieves. Most customers are concerned about loss of data on the Internet. In fact, encrypted Internet messages are more secure than some service provider computers. Credit card data have been stolen from service provider computers.

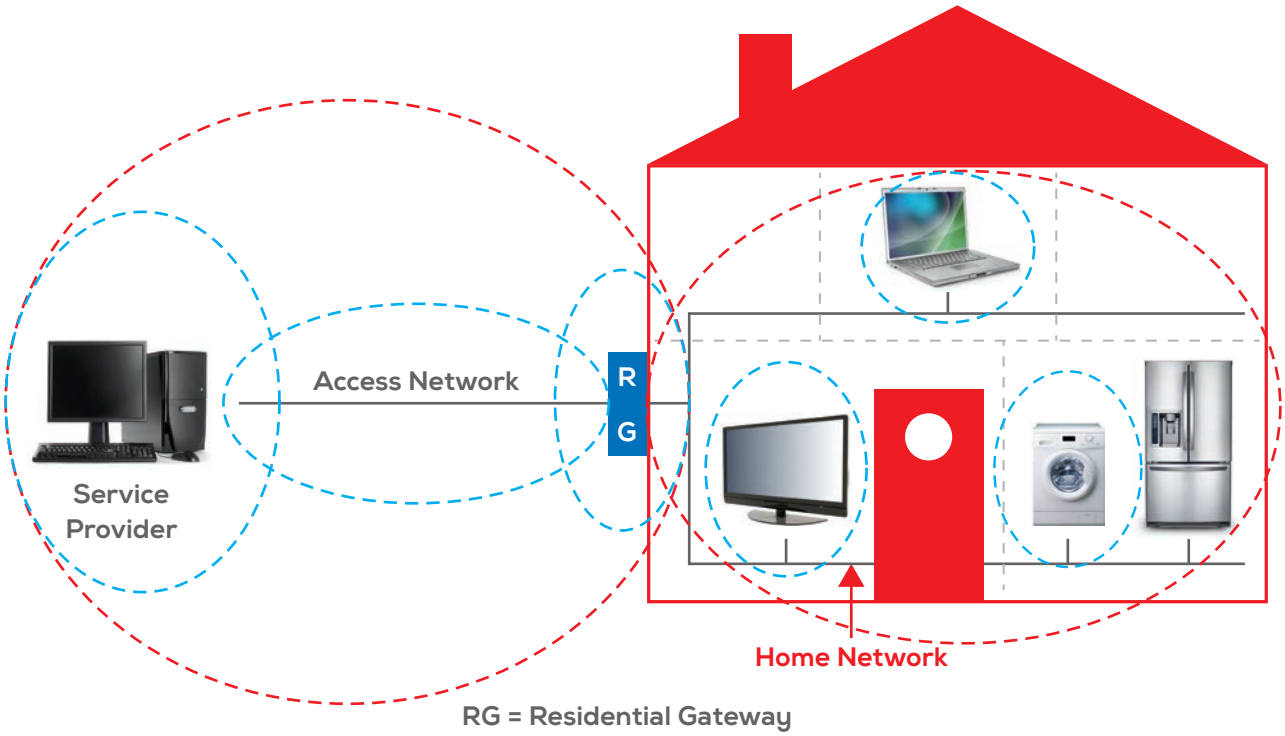
Appliances and devices in the house need individual security protection, especially the residential gateway through which the Internet is accessed. As I explained in my Autumn 2016 *iHomes and Buildings* article on IoT, a standard for the gateway is under development to incorporate security features, rather than burdening each IoT device in the home or building. As with the external network, the entire home network needs to be protected with an additional layer of security.

Privacy uses the tools of security, but is primarily a set of rules and prohibitions. For example, some devices might contain personal user data such as income and tax data. Such demographic data could enable a merchant to target a marketing campaign to specific users. Even with a properly functioning security system, these data could be sent securely from a home device to the merchant's computer. However, a privacy feature might allow the user the option to prohibit such transmissions. The home device or a gateway would be programmed to block these transmissions.

Using IoT wisely

Integrated home and building systems are assembled from carefully designed applications created by experts in each field. They are responsible for choosing the equipment optimized for executing the application. This equipment should conform to interoperability standards so messages can be exchanged with other controllers for coordinated actions where appropriate. IoT can facilitate this coordination, but is not a substitute for:

Figure 4 – Layers of Security



Application organization and optimization
Which control functions, sensors, actuators, and user interfaces are needed?

Application interactions
What parameters of an application are controllable and observable from which other applications?

Data security
Where is data security needed? What level of security is warranted based on the consequences of possible breaches? Which security algorithms are appropriate? Who are the trusted entities for administering security certificates?

Layers of control and security
Where are the logical domain boundaries between customers and service providers, between customers and associates (colleagues, family, etc.), between customers and the public, and between customers and the government?

Customer privacy
What customer data should and can be kept private? Whom might the customer allow to view and/change private data? How are privacy violations detected and remedied?

IoT technology can facilitate the interconnection of devices on a communications network. However, IoT does not replace an organized structured system design. For IoT to become a useful adjunct to homes and buildings, engineers should adhere to the basic principles of disciplined and organized system design. ●

Dr. Kenneth Wacks has been a pioneer in establishing the home systems industry. He advises manufacturers and utilities worldwide on business opportunities, network alternatives, and product development in home and building systems. The United States Department of Energy appointed him to the GridWise® Architecture Council to guide the electric industry toward smart grids. For further information, please contact Ken at 781.662.6211; kenn@alum.mit.edu; www.kenwacks.com.