WHAT EXACTLY IS "NETWORK INTEGRATION"?

Jim Sinopoli, PE, RCCD, LEED AP BD+C
Managing Principal
Smart Buildings LLC

Integrated building systems can truly save capital and operating building costs and have taken on a prominent role in green buildings. At some level, we all talk about "integrated and open systems", at times though we seem to be talking pass each other. When we talk about integration, especially the details of system installation, are we all taking about the same thing?

There are different ways to "integrate" building systems, different concepts of what integration is and some misperceptions to address. It would seem that if we had a common framework for what integrated building systems means that the industry would have an easier time of explaining the approach and its value proposition to building owners, developers and architects. A framework would move the discussion from what at times seems theoretical, futuristic and confused, to a common understanding of the core of what the industry is now all about. Clients could be better informed, designers and contractors may better understand what each is asking of the other and it could solidify the basis of what would be required for the certification of designers and contractors. What follows is a look at how systems can be integrated and a common framework for referencing the integration of systems that the industry is moving towards.

Methods of Integration

Hard-Wire

The most basic and oldest form of system "integration" is "hard-wired integration". A typical example is two stand alone building systems physically connected via an electrical "dry contact", RS-232 or RS-422 connection. An example may be a fire alarm system connected to the HVAC control system or an access control system for secondary alarm annunciation and monitoring. These systems do not share any data, but are simply connected to signal "off" and "on" conditions. This is your father's integration.

Proprietary/Bundled/Packaged Integration

This sounds like an oxymoron but a proprietary integration means you use systems from one manufacturer that have been designed to work with each other. The downside to this approach are significant and several fold: the client is locked in to one manufacturer for a complete system lifecycle, there's no or little competition in procuring additional equipment and services, the client could be missing out on advances by other manufacturers, and there's not one manufacturer having the full suite of building technology systems. Some of the best examples of these "packaged" systems are in the residential marketplace, the "home automation" package for condominiums, apartments and homes.

"Dating" Integration

This involves two manufacturers of different building systems, or possibly facilities or business systems, agreeing to open their products to each other. The companies may have developed Application Programming Interfaces (APIs) so their systems can communicate. This may work if we're dealing with two systems; however managing all the APIs to get multiple proprietary building systems to talk to each other can be difficult.

Open Standards Integration

Certainly using an industry standard protocol for the network layer of the building systems is a required component in true integration. There are a couple of caveats to using open protocols however. One is that the number of protocols used to integrate the building technology systems needs to be minimized in order to maximize integration and provide an efficient operation environment. One approach is to select major protocols for implementation (i.e. IP, DALI, BACnet/IP, Lonworks, etc.) which in many cases will cover almost all of the needs of the building systems.

The other, and maybe the more important caveat, is that the use of open protocols does not necessarily guarantee "openness", interoperability" or "integration". Without certified or laboratory tested products, protocols such as BACnet and Lonworks can be implemented in a way that may only be supportable by the original installer. It's the same situation with the IP protocol. IP can carry proprietary data. IP by itself doesn't guaranteed integration.

Front-End Workstations

Another method, primarily used for BAS and security systems, is to have all of the systems networked to one workstation. This was the approach taken by major BAS manufacturers starting 10-15 years ago. This approach essentially provides a facility manager with one standardized interface to manage and configure stand-alone systems. Each system may operate as a stand-alone system but the workstation provides a "unifying" tool and database for the systems. This is a somewhat proprietary integration, dependent on the manufacturer's application openness, and typically will address only a portion of the systems in a building.

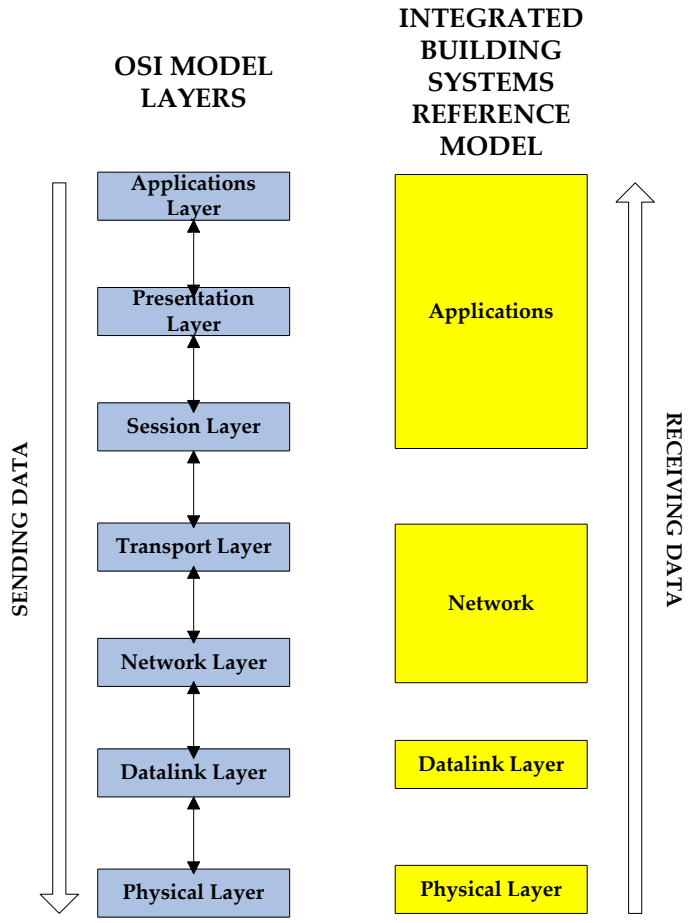
The Framework for Referencing Integration

What we are trying to do is maximize the integration of building system networks into one network with integration taking place at the physical, network and application levels. Integrated systems share resources. This sharing of resources underpins the financial metrics and improved functionality of integrated systems.

System integration means bringing the building systems together both physically and functionally. Physically obviously refers to the cabling, space, infrastructure support, etc. It also touches on common use of open protocols by the systems. Functionally, systems integration addresses the capability of multiple systems to interoperate and thus provide functionality that cannot be provided by any one system. This is the theory that the "Whole (integrated systems) is Greater in Functionality than the Sum of the Parts" (separate building technology systems).

There is a key differentiation between integrated and interfaced systems. Interfaced systems are essentially stand-alone systems that share data, but continue to function as stand-alone systems. Integrated systems strive for a single database, considerably reducing the cost and support for synchronizing separate databases.

At the forefront of the evolution to open network standards is the International Standards Organization's (ISO) development of the Open System Interconnection (OSI) model. The OSI model presents seven layers of network architecture, (the flow of information within an open communications network), with each layer defined for a different portion of the communications link across the network. It's withstood the test of time, and it's this framework and some of its derivatives that should serve as our reference point for integration.



The model is straight forward. A network device or administrator creates and initiates the transmission of data at the top layer (the application layer) which moves from the highest layer to the lowest layer, to communicate the data to another network device or user. At the receiving device the data travels from the lowest layer to the highest layer to complete the communications. When the data is initially sent, each layer takes the data of the preceding layers and adds its own information or header to the data. Basically, each layer puts its own "envelope" around the preceding "envelope." On the receiving side, each layer removes its information or "envelope" from the data packet.

What do these layers do?

Physical Layer
This layer guarantees that bits of data

transmitted by a device on the network are accurately received by another device on the network. It defines the mechanical and the electrical characteristics of the physical interface, including connectors, network interface cards, and voltage and transmission distances. An example would be RS-232 connections.

Data Link Layer
The data link layer takes the data bits and "frames," and creates packets of the data to guarantee reliable transmission. The data link layer adds source and destination addresses to the data stream as well as information to detect and control transmission errors. An example is Ethernet, which is defined by both the physical and data layer

Network Layer
The network layer routes data packets through the network. It deals with network addressing and determines the best path to send a packet from one network device to another. The Internet Protocol (IP) is the best example of a network layer implementation.

Transport Layer
The transport layer is responsible for reliable transport of the data. At times, it may break upper layer data packets into smaller packets and then sequence their transmission. The Transport Common Protocol (TCP), one of the major transport protocols, is typically used with the best known network layer protocol, IP, and is referred to as TCP/IP.

Session, Presentation and Application Layers
Many times these layers are considered as one layer. The session and presentation layers manage dialogue between end-user applications, and formats and deliver the data to the application layers.

Systems designers and contractors should frame the discussion of system integration using the ISO model and focus on the physical, data, network, and application layers. It could very well add some clarity and understanding to both industry and client discussions.

For more information about smart buildings, technology design or to schedule a Continuing Education program for your office write me at jsinopoli@smart-buildings.com .