

OPEN VS. CLOSED

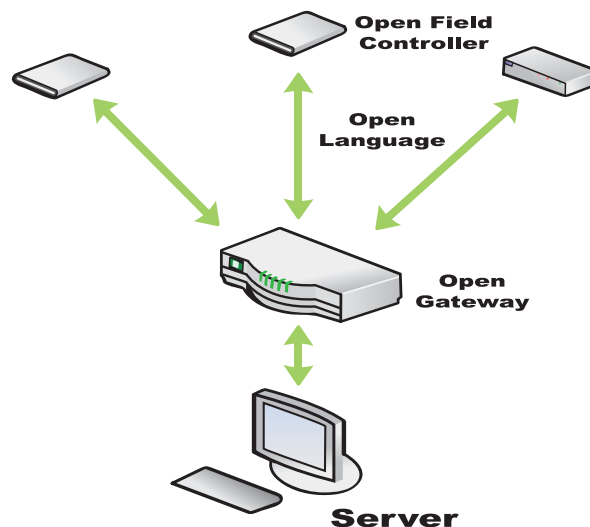
In the 21st century we now have the ability to look at B.M.S/E.M.S controls as technology centric versus the old school of thought, which was a company or product centric model. Technology and protocols exist today that enables intelligent machines to communicate without exception, regardless of the manufacturer.

Any component of a system, be it hardware, software or programming should be able to be replaced/executed seamlessly with any open protocol brand without loss of functionality. These 100% open protocol systems can be supplied by multiple vendors without your company being held hostage by any one supplier, thereby avoiding single source vendor lock-in

Competitive pricing and proper service rather than obligation should be the rule as to why to choose one company versus another. Here are some facts to help lower the costs of building, renovating and operating your facilities and how best to take advantage of this new opportunity.

100% Open Protocol

Ability to remove, change or replace any part of the system with any other brand. Not one "hook" to keep you locked in to the system provider's hardware and/or software.

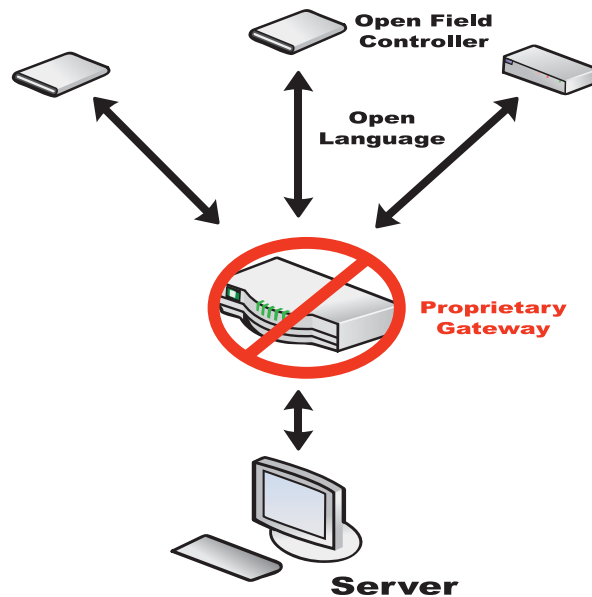


Closed/Proprietary Systems

To proprietary manufacturers, open protocol simply means you can share information between closed or proprietary subsystems. These so called “open protocol manufacturers”, use this terminology as a means of convenience, leaving the unsuspecting or unknowing client believing their systems are 100% open. This approach is not open and can lead to the inclusion of proprietary gateways, end devices and/or a complete system lock down.

Scenario 1: Proprietary Gateway

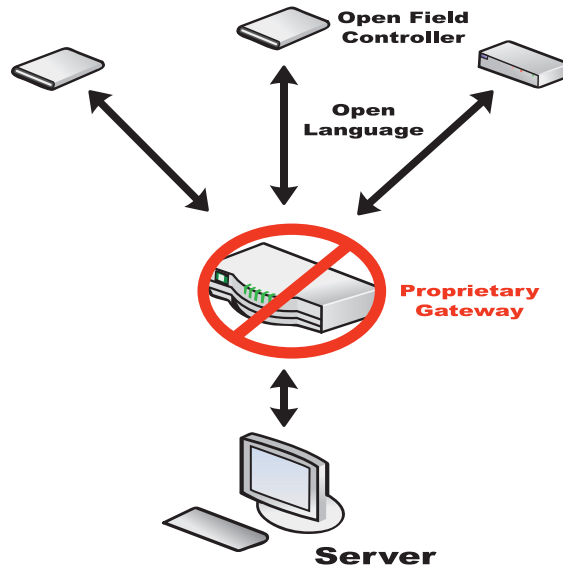
A gateway is a Hardware-Software device that bridges the BMS system to the Graphical User Interface. Some manufacturer’s gateways include a separate and propriety language causing information to be locked down and/or not available to the end user without buying tools from the manufacturer. Some manufacturers do not make these tools available.



Choice of contractor is also important. Why also the contractor? Because they are key to a successful installation and ongoing maintenance. If the contractor is limited in access to product, tools, training then they are limited in what can be installed and who can support and expand the system.

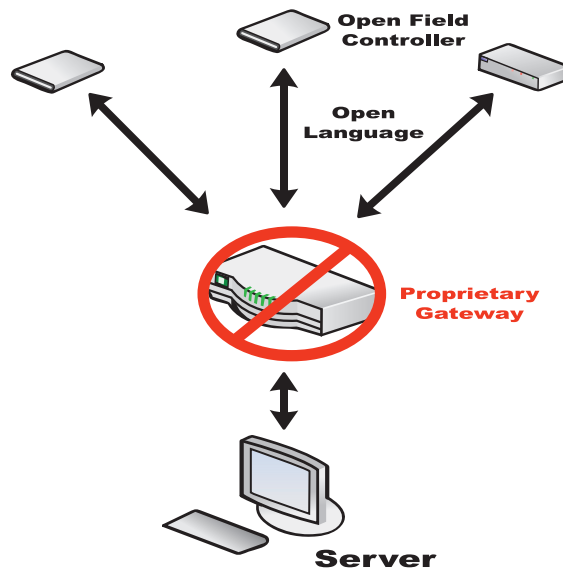
Scenario 2: Proprietary Field Controllers

Not all “open” field controllers are truly open. Companies have the ability to install their own “Hooks” or encrypted code in these devices. These “Hooks” cause the need for that user to purchase additional and costly programming tools to communicate or program these end devices.



Scenario 3: Complete Propriety Lock-in

All components are locked down by propriety software, hardware or manufacturer.



Benefits of an Open System

- Lower installation costs.
- Lower operational costs.
- Greater expandability.
- Easier to manage.
- Extremely flexible.
- Forward compatible with future building automation technologies

Building owners must be wary of vendor claims of having more than one system “talk” at a high level to another, which is simply another way for system vendors to maintain their lock on their components. This is neither open nor interoperable. It’s misleading and, in the long run, expensive.

There’s a growing need for information and training regarding the pitfalls and benefits in selecting a path. Building owners need to be sure they’re selecting the right long-term solution by asking the hard questions:

- Will my system be open to competitive bids after the initial installation?
- Can I install a system with multiple user interfaces from multiple suppliers?
- Is there built-in security at the low-level network-infrastructure level?
- Can I maintain my system by myself?
- Will I receive all the tools I need to fully maintain my system?
- Can I choose multiple bidders for my subsystems and have their products all integrate into one enterprise system?
- Is my system designed for only a small portion of my integration needs, or can it work with all of the components and facility types in my portfolio, cost effectively?
- Can I select products from multiple vendors and distributors and not be locked into a single vendor or source?
- Will all of the products that I select be guaranteed to work on the same network infrastructure?

A ‘No’ answer to any of these questions, is cause to be wary. An open system is not just an open protocol; it must take into account all the aspects of the system, from the lowest-level devices to the highest-level enterprise integration. **You should always have the freedom to choose who you work with now and in the future.**