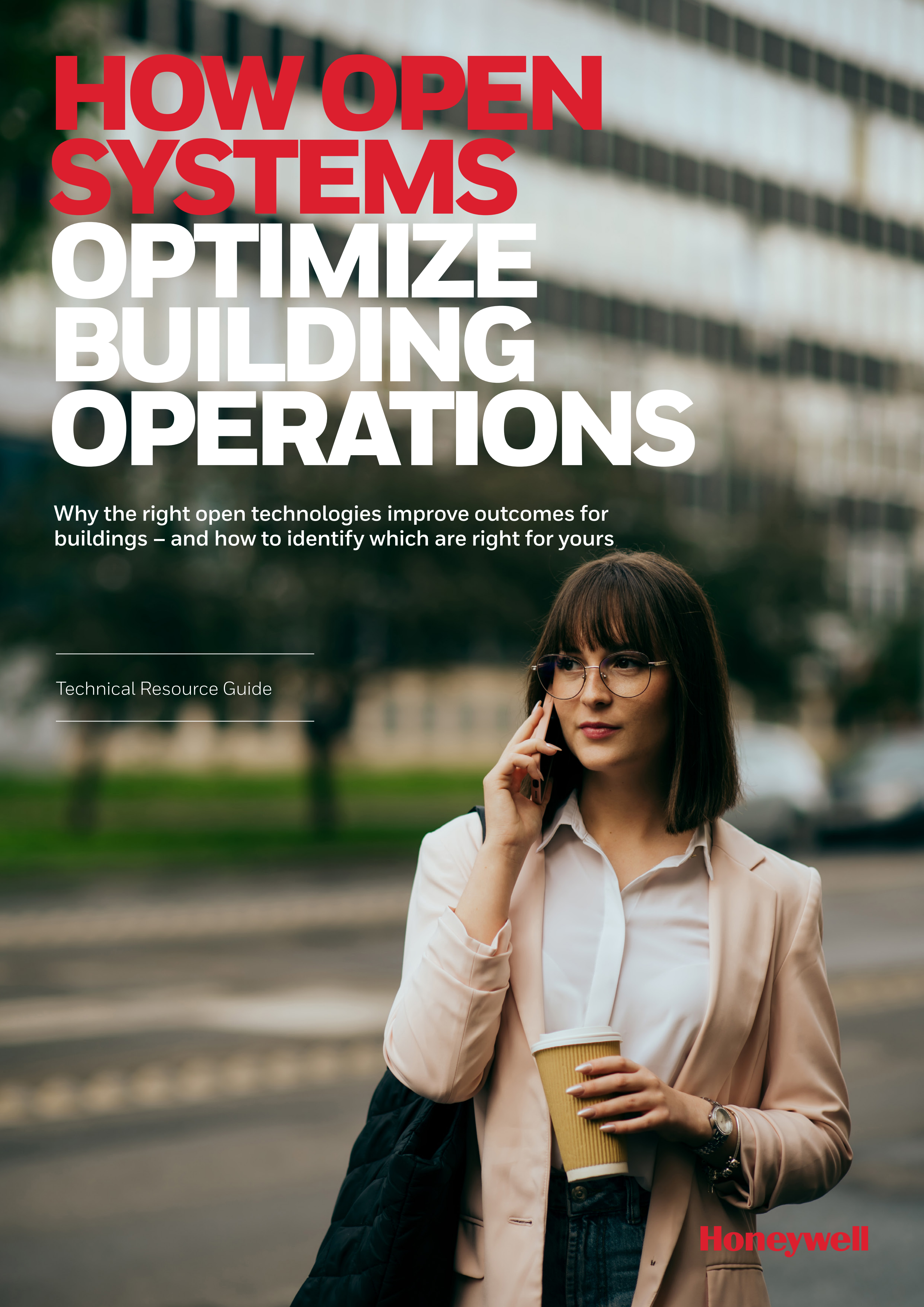
HOW OPEN SYSTEMS OPTIMIZE BUILDING OPERATIONS

Why the right open technologies improve outcomes for buildings – and how to identify which are right for yours

Technical Resource Guide



Honeywell

THE OPEN SYSTEMS PARADIGM

Unraveling the real advantages of open technologies

> This guide explores the many elements that make up an open system, clarifying the advantages and disadvantages of each.
>
> Our goal is to dispel the complexity of open systems, to advocate for truly open connectivity and extensibility, and to help you understand which factors will enable you to achieve optimal outcomes for you building.

Selecting an integrated Building Management System (iBMS) entails numerous technology and supplier decisions that will have a significant impact on your building operations – affecting not just the upfront purchase price, but also the system's lifecycle costs, its reliability and flexibility, and the risks or issues that may arise from this system.

In other words, making the wrong decisions can prove frustrating or costly in the long-term. Conversely, making sound technology decisions can help minimize risk, prolong future compatibility, and reduce your total cost of ownership over the lifespan of your building.

Open systems are a key step in the right direction: They provide numerous benefits that can help organizations obtain sophisticated yet cost-effective building management. However, many incorrect assumptions and false "open" criteria can introduce confusion, leading to poorer choices and adverse effects.

OPENNESS STARTS WITH TRANSPARENCY

Honeywell is committed to open technologies, open extensibility, open systems – and a market of choice that enables every organization to achieve the best capabilities for its buildings. Which is why we also believe in full transparency about what "open technologies" are and how best to use them.

This guide is designed to help you understand what "open" truly means in each of its uses, so you can use that knowledge to choose the right technologies for your building.

TABLE OF CONTENTS

WHAT "OPEN" MEANS

1

> The term "open" is increasingly being used by building owners, facility managers, procurement teams, and consulting engineers when specifying a new BMS or building technology.

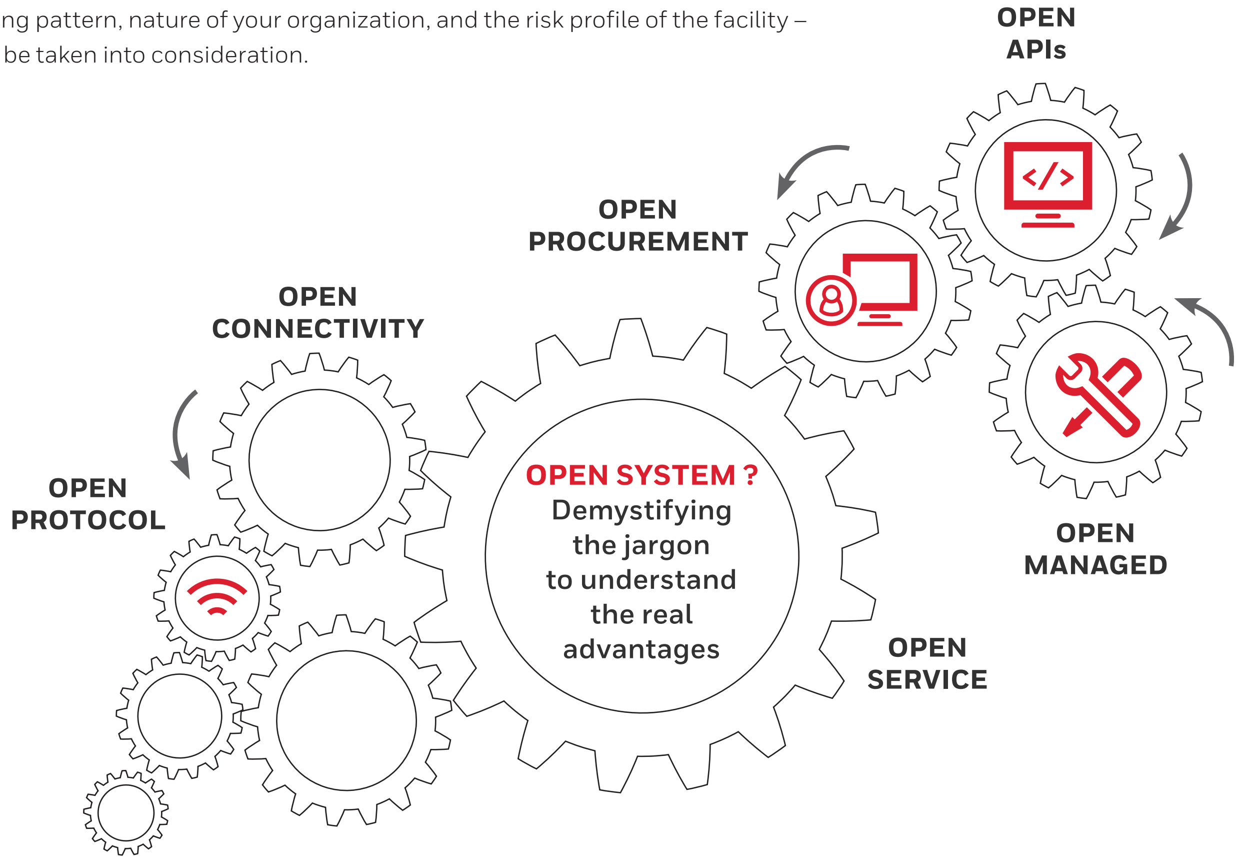
Depending on the context, variations in terminology include "open," "open system," "open service," and "open vendor" (also known as a non-proprietary system). Unfortunately, these terms are often used inconsistently or incorrectly – and worse, they can be distorted to the advantage of particular vendors.

A clear understanding of the differences between these concepts is essential for ensuring the success of the system and your facility. All stakeholders should have the opportunity to understand the business benefits and potential pitfalls associated with each of these "open" elements.

The desire for an open system often stems from the wish to avoid the perceived risk of being locked into a single service provider. Although not always the reality, a single service provider may result in high service prices and poor service levels.

However, the potential disadvantages of choosing an open system or the "wrong openness" also need to be considered and avoided – such as the risk of greater complexity in multi-vendor systems, whether the integration in such systems is resilient to change, and the loss of differentiation in functionality between devices and supervisor systems.

When assessing any open strategy, critical determinants – such as the size, operating pattern, nature of your organization, and the risk profile of the facility – should be taken into consideration.



OPEN PROTOCOL

2

“Open protocols” are also referred to as “open connectivity”

> An open protocol defines how a device communicates to a supervisor system.[1] Open protocols are generally defined and maintained by industry standards organizations.

These organizations are typically formed by multiple vendors who wish to implement a common communication protocol for their hardware and systems based on a consistent, defined standard.

A consistent communication protocol gives building managers the freedom to select and match from a wide range of software systems and field devices, tailoring a building management system to their organization’s needs and budget.

> **Example**: The BACnet™ protocol for building controls was defined by the ASHRAE industry body, and has become a widespread international standard. Other open protocols often used in buildings include ONVIF®, a standard for video surveillance, and OPC, a standard for industrial automation.

Open protocols are a positive for building managers and the building control industry, but there are limitations. Because all the devices have to work via the same supervisor system, unique or advanced features may not be supported by the protocol, which can reduce system functionality to the lowest common denominator.

Thus some manufacturers support both open protocols and proprietary or extended protocols for field devices, enabling building managers to access additional functionality not supported by the base standard.

Open protocols normally only apply to real-time, day-to-day operations. Set-up, programming, and commissioning of devices is usually done with manufacturer-specific tools. These engineering tools may not be given away freely, meaning that, in effect, you are still partially restricted to a particular brand for the knowledge of setup, configuration, and access to the closed tool set. The engineering databases may be similarly restricted.

The result is that the theoretical promise of unlimited options for devices is, in practice, often deemed impractical, because facility managers can’t afford the time, cost, or hassle of maintaining multiple configuration systems. Instead, they may end up adopting products from only one or a few manufacturers.

Open protocols also need regular maintenance and modernization updates – for instance, to keep pace with cybersecurity needs.

[1] A “supervisor” system refers to the software platform that collects data and provides a user interface for the integrated building management system, or other types of systems such as a security management system. A supervisor may also be known as a “head-end” system or “host server.”

DE FACTO OPEN SYSTEMS, STANDARDS, AND PROTOCOLS

Sometimes a communications protocol owned and defined by one vendor (or a technology platform owned by one vendor) becomes perceived as “open” because of its prevailing market position.

Thus to meet customer demands, other vendors ensure their technology works with this protocol or system. Although still the intellectual property of a single vendor, such a system or protocol has arguably become “de facto open” in at least some regards.

> **Example:** The Microsoft Windows® operating system is a proprietary OS owned by Microsoft, yet it has such a prevalent market position that most developers of computer software need to make their systems compatible with Windows. Because of Microsoft’s numerous market channels, this technology is often deemed “open,” even though Windows remains proprietary to Microsoft.

Open protocols support the growth of smart buildings, which are projected to grow from USD $80.62 billion in 2022 to USD $328.62 billion by 2029, showing a CAGR of 22.2% during the forecast period.

Source: Fortune Business Insights

DEGREES OF OPENNESS

Open systems can be great tools for providing freedom of choice. However, to determine whether a system or protocol is in fact truly open, be sure to carefully investigate the openness of the engineering tools and databases, the source files for controller programming, and the BMS supervisor.

If these are locked down, then ensure you have rights to use them when specifying your system. Otherwise, you may in essence have a closed system for the purposes of engineering and maintenance – and not the fully open system you thought you'd invested in.

- 👍 **Open protocols support the growth of smart buildings** with benefits to operations, system lifecycle, and occupant experience..
- 👎 **Loss of unique and differentiated functionality** between the device and supervisor systems.
- 👍 **Flexibility to add any field device** to any manufacturer’s head-end software system.
- 👎 **Lowest common denominator of functionality.** Varying quality and reliability among manufacturer field devices may introduce inconsistent results.
- 👍 **Large range of field devices are available** enables best-of-breed selection.
- 👎 **Each field device requires its own engineering tool** to set up and commission. This increases the cost to the engineer and the complexity of maintaining multiple system configurations.

OPEN PROCUREMENT

3

“Open procurement” is also known as “multi-vendor procurement”

> The term “open system” is often used to describe a supervisor system that is “openly procurable” – meaning that it can be purchased through more than one vendor.

Open procurement is unrelated to support for open protocols, as both multi-vendor and single-vendor systems may support open protocols.

The supervisor itself may still be proprietary software containing intellectual property from one vendor – the original equipment manufacturer (OEM) – but it can be purchased from multiple sources, usually through a one- or two-step distribution channel.

Open procurement is attractive because customers are not locked in to one particular vendor, and can purchase the technology from their choice of vendors, including installation and ongoing support for that technology. Purchasers are, however, locked in to that technology and its associated OEM.

Single-vendor systems are considered to implicitly be synonymous with “proprietary,” which can have negative connotations for building owners, facility managers, and consultants. So selling a system through open procurement may be a way to get around this perception.

However, it can be easy to lose sight of the fact that every supervisor system (or the underlying subsystems) contains proprietary technology, which is the intellectual property of the developer. Even those systems that support open protocols and that are sourced through open procurement channels still ultimately depend on single-vendor software.

Likewise, when it is installed, a supervisor system is always custom engineered to meet the requirements of that particular site – for example, the number of points monitored and controlled, the layout of the site, and the building manager’s specific operational requirements. So a qualified service provider must design, install, engineer, commission and maintain that site-specific integrated BMS. This ultimately results in an operational system that is as unique as the site itself.

As the complexity and criticality of the engineered system increases, the tie to that service provider, who has the knowledge of how the system is set up, also increases. As such, it can become impractical to consider changing service providers, even for multi-vendor systems.

Given this, it may be useful to place a high priority on simplified, self-documenting solutions rather than a highly complex, customized system. A simpler self-documenting system can be serviced by many different technicians or providers – not just the service provider who installed it – and the amount of training required will also be less, which can translate into a reduction of time and cost to maintain.

👍 **Flexibility to purchase** a supervisor system from multiple vendors.

👎 **Loss of direct contact** with the manufacturer of the supervisor for support and special requirements.

👍 **Increased competition** between vendors to provide installation and support services.

👎 **Delays in issue resolution** can occur when it is unclear whether the issue is with the work of the integrator or with the system itself – in which case, the issue may take longer or cost more to resolve.

👍 **Ability to purchase the product** outside the geographical footprint of the manufacturer.

👎 **Lack of deep understanding** of the supervisor and how to apply it successfully, compared to single-vendor systems that are installed by the manufacturer with a local presence.

👍 **Single point of ownership** for service when issues occur, as the installer / service provider has unrivalled knowledge and expertise of the onsite configuration, passwords, and tools.

👎 **Risks may increase** when using smaller integrators whose engineering skills and record keeping may not be assured, and whose business may not be as financially secure as a larger business (such as the system's actual developer, whose longevity, skills, resources and commitment to delivering the solution are more established).

OPEN APIs

4

Open application programming interfaces (APIs) are often referred to as "open extensibility"

> Some vendors use the term "open system" to refer to a supervisor system with published APIs. These enable system integrators to develop their own software, which can extend and customize the functionality of the existing system.

APIs built and supported by a trusted technology supplier can deliver enhanced, consistent operability, and the capacity to integrate future third-party technologies as industry standards and capabilities evolve.

When referred to as "open extensibility," this may also include "open endpoints" that provide a direct point of connection for additional functionality.

An API is a documented set of software functions that can be used to add new applications to a system, to integrate multiple systems together, and to customize existing systems for specific needs.

APIs are specific to a particular system, and are often not interoperable. In other words, an application developed using an "open API" for one supervisor system is unlikely to work on a different supervisor from another manufacturer.

Any interface, application, or functionality derived from an API is essentially custom software or site-specific software, and needs to be treated as such for ongoing support, upgrades and updates, and cybersecurity adaptations. This typically necessitates a support tie to whichever software provider created this custom functionality.

There are also varying degrees of "openness" when it comes to APIs.

For example, one approach is to provide APIs directly to end customers only, so that they have the option to modify and evolve the supervisor system in-house as needed, without relying on the manufacturer.

> **Example:** The Niagara Framework® from Tridium is an open platform that enables extensive development of new functionality on top of the base system. Many system integrators even build their own Niagara supervisor using the toolkit that the Niagara platform provides.

To ensure a wider degree of openness and flexibility throughout the life of your system, look for platforms with well-documented, publicly available collections of extensible APIs.

DEGREES OF OPENNESS

In addition to APIs, you may also want to seek systems with "open endpoints."

An endpoint is a connection that enables you to configure additional functionality by connecting to it, rather than needing to develop custom software.

> **Example:** Connecting a cellphone to a car via a standard Bluetooth® connection is much easier than writing a custom app for a wireless phone-to-car connection.

A platform that gives you access to both open APIs and open endpoints is an optimal way to gain a range of options for adding and modifying system functionality over time.

👍 **Any organization or contractor can adapt software or hardware functionality** without the manufacturer needing to be involved.

👎 **Any added functionality is custom software** or site-specific software, which may not be supported by the manufacturer or OEM. In this case, you may be dependent upon the developer for support of that custom functionality.

👍 **Anyone with sufficient software skills can write code** to add functionality via an API. You are not dependent upon the original manufacturer.

👎 **No quality control** is guaranteed for custom code, unless it is specified and audited.

👎 **Ongoing support needs to be planned** for in advance. This includes agreement on who can access the source code and any associated intellectual property.

👎 **API user experiences may have an inconsistent look and feel,** depending on who developed the application and its integration.

👍 **APIs and open standards** are available to anyone.

👎 **Interpretation and understanding of API documentation may vary by provider.** Most documents are written with an assumed knowledge on behalf of the manufacturer and OEM.

OPEN MANAGED

5

An “open-managed” system may also be referred to as “user-managed”

> Some supervisor systems can only be engineered by the manufacturer or an approved system integrator, whereas others can also be engineered by the end-user – such as adding new open-protocol components.

This added flexibility is known as an “open-managed” or “user-managed” system.

User-managed systems arguably give building managers the greatest long-term flexibility, since they always have the option to engineer the supervisor themselves and use in-house resources to apply system changes (supplemented by appropriate training), or to engage the original system provider to make these changes for them.

In either case, engineering-configuration work is required for devices and other system components, even if they use open protocols. Specific engineering tools may be required, and these software tools are generally restricted to the manufacturer and its licensed system integrators.

Some manufacturers do provide such licenses to their customers or their customers’ delegated service providers, but some do not – so if you’re seeking an open-managed system, inquire about this form of licensing in advance.

However, the risk of a system engineered by the user is that it may not follow the latest best practices for engineering and configuration – especially with systems or capabilities that are highly complex – which could lead to issues with overall system efficiency, functionality, or maintenance. And if issues do arise, they may be outside the scope of manufacturer support. Conversely, vendor-managed systems typically do follow industry best practices with functionality that is fully supported.

👍 **User-managed systems are not dependent upon the manufacturer** or installer for engineering and adding devices.

👎 **User-managed systems may not follow best practices** for engineering or configuration.

👎 **Issues could prove costly and time-consuming to diagnose and resolve,** unless you also have a service-level agreement with the manufacturer.

OPEN SERVICE

6

An “open service” contract lets you retain your installed technology while changing service providers

> At first glance, open service looks similar to open procurement in the sense that you are not contractually limited to a single vendor. However, in practice, changing service providers for an installed system tends to be much more complex than selecting a procurement vendor.

It may be natural to assume that “open service” should translate into potential cost savings, given the option of engaging a low-cost service provider. However, low-cost service providers often lack the specific domain knowledge and technical expertise to best service and optimize a system they did not install.

Moreover, purchasing an “open procurement” supervisor does not guarantee open service, because the engineering tools may not be included with the supervisor system.

To service an integrated BMS, any potential service provider needs to have access to all the tools and documentation that have been used to set up and configure the supervisor, including all the passwords. They also need the tools to set up and configure all connected devices, such as controllers or cameras.

So changing service providers can become challenging if a new provider cannot easily find or get access to all the information and tools that they need.

Ultimately, the complexity of engineering and customizing a supervisor to a site’s unique requirements often makes changing service providers impractical and cost prohibitive – even if all the tools are available.

If you hope to take advantage of an open-service contract to change service providers, then ensure your installer and any subsequent servicers maintain thorough, transparent documentation of all system components, configurations, passwords, and other essential details – and ensure that you have the rights to this information, so that you can pass it on when needed.

- 👍 **Choice of service providers.**
- 👎 **A new service provider must have access** to all configuration tools, documentation, and passwords to service the system.
- 👍 **Some service providers have the support** of the OEM or the manufacturer.
- 👎 **Issues could take weeks or months to resolve** if the service provider does not have the manufacturer’s support.
- 👎 **Pinning down the responsibility for a system issue** (and its resolution) can become difficult to distinguish between the installer, the manufacturer, and service providers.

HOW TO CHOOSE AN INTEGRATION PARTNER YOU CAN RELY ON

7

> Choosing a reliable, capable BMS ultimately requires a wide variety of expertise: Specifying the right capabilities and the technologies to achieve them. Ensuring the compatibility of all technologies. Integrating them all into a single platform. Assessing and mitigating any risks your building operations may face throughout the life of the system. Planning for ongoing support and maintenance.

These needs are usually easier to manage with expert help – which means that choosing the right partner may be even more important than the technology choices.

Critical factors such as the size, operating pattern, the nature of your business or organization, and the risk profile of your facility should be taken into consideration when planning any open strategy.

With the right building integration partner, you don't have to navigate all these factors on your own. But that raises another question: How do you identify the right partner?

These are some key questions to ask when assessing potential building integrators.

QUESTIONS TO ASK

- Which system will best meet the needs and complexities of my site? How and why did the vendor or integrator arrive at that recommendation over other options?
- How will this system be delivered, maintained, and upgraded over time? Does this include future concerns such as cybersecurity?
- How fast is technology evolving in my industry, and what effects will that have on my system's lifecycle? How future-ready and adaptable is the proposed system?
- How will the return on investment (ROI) be assessed, and how do I show value to my stakeholders in system continuity?
- Who will be the most cost-effective and technically expert provider for service and support over the long term?
- How important is this system in achieving our organization's goals, and maintaining a competitive advantage in the marketplace?
- Can I be assured that my service provider will maintain the system and documentation to a level that will enable me to change technology providers in the future?
- Does my service provider offer the tools, information, and transparency necessary for me to monitor and validate the quality and reliability of their service?

Over a 40-year lifespan, 85% of a building's total cost of ownership will consist of operations and maintenance costs. Significant opportunities exist to maximize return on investment with the right supplier and technology mix.

Source: Statista

THE NAME BUILDINGS TRUST HONEYWELL

Helping buildings achieve safer, smarter, and more efficient operations has been the bedrock of our business for generations – which is why today, Honeywell technologies are in more than 10 million buildings worldwide.

How? Because we've established expertise in each part of the job – from developing the software and equipment, to integrating open systems, and engineering the performance that a complex site depends on to get results.

All Honeywell supervisors work on the Microsoft Windows operating system, with support for a variety of open protocols and de facto open protocols. Since Honeywell supervisors also support any "commercially off the shelf" hardware (COTS), your deployment and configuration options are highly versatile and adaptable.

Find out what your building can achieve

Honeywell knows buildings –
and we're always ready to help

hwll.co/WEBsN4

For more information
buildings.honeywell.com

Honeywell Building Technologies
715 Peachtree St NE
Atlanta, Georgia 30308

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell