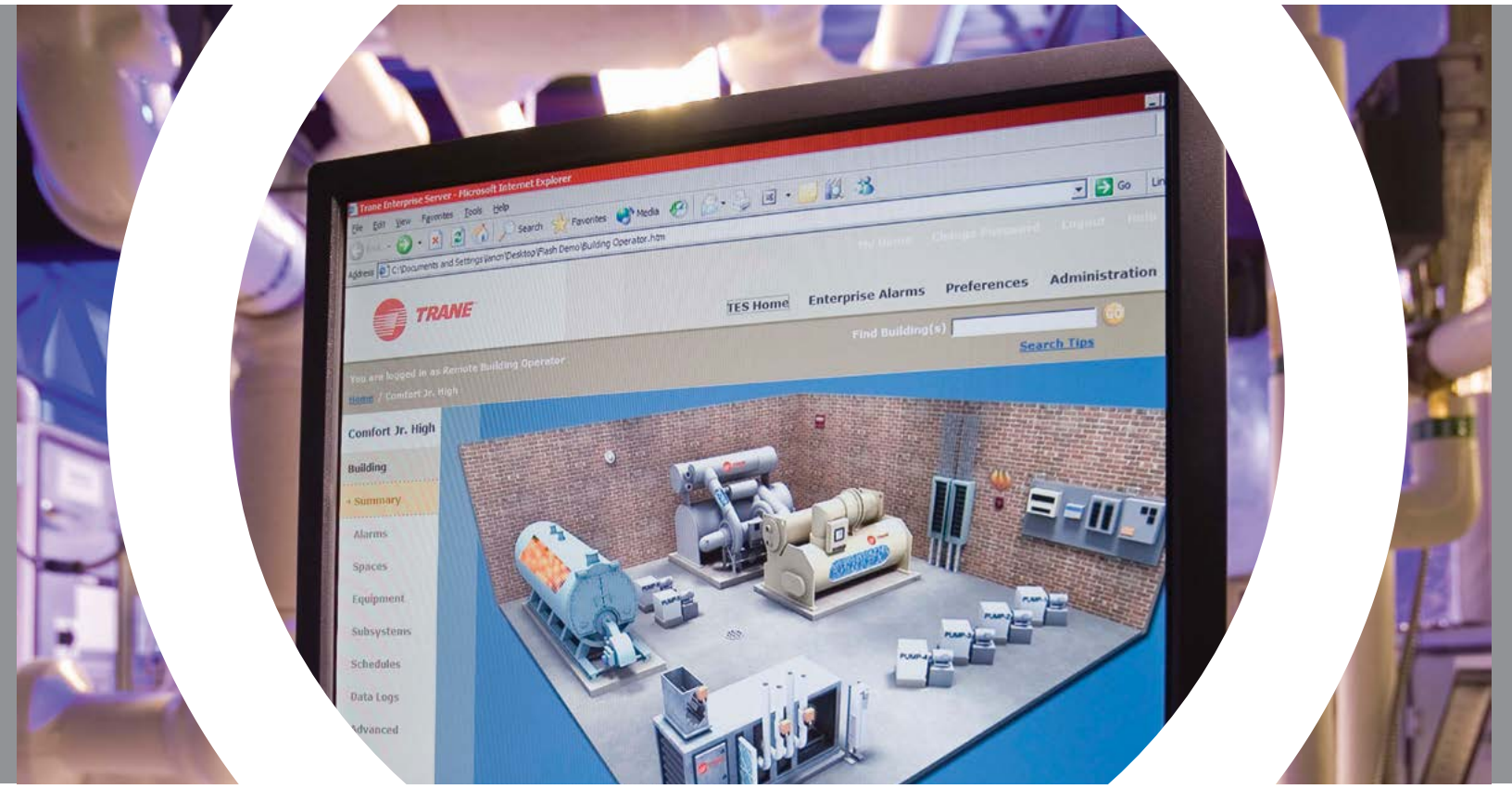
Tracer ES

Ten frequently asked IT questions about Building Automation Systems (BAS)



Ten frequently asked IT questions about Building Automation Systems (BAS)

1. What is a Building Automation System (BAS)?

A building automation system (BAS) is a generic term for devices and software applications working together to enable automated control of building environments, such as lighting, heating, air conditioning, securityand others. The scope of building automation systems can range from a single location to one spanning multiple sites around the world. The purpose of any BAS is to make building environments as energy efficient, comfortable and productive as possible.

2. Why should the BAS be integrated into the existing infrastructure?

A BAS can operate within an existing business computing network infrastructure, and use existing IT support groups. This helps increase associated efficiencies by preventing the duplication of resources. The sharing of these resources reduces installation cost and improves speed of implementation, technical support and security.

A BAS is essentially a business computing system like any other business system the IT department may support. As such, it can be plugged into the IT support structure and operate within currently accepted standards and best practices.

Using an existing network and support infrastructure also decreases implementation cost. IT involvement can make implementation easier, and can provide continuing support for building automation systems.

3. How will the BAS use the network infrastructure to operate?

The ability to implement a BAS using an existing business computing network infrastructure depends on the technology that the network utilizes. A BAS can operate over the existing network infrastructure, regardless of topology (LAN/WAN, satellite, wireless, VLAN, etc.), as long as it supports IEEE Ethernet and IP routing. Most building automation systems use HTTP, SNMP, UDP, BACnet and SMTP Internet standard protocols.

Newer building automation systems can run using the Windows network operating system. Within that operating system, BAS workstations and file servers can exist as domain members or in Active Directory. Those building systems can support Windows-based workstations and network logon authentication. Downstream devices will use application-specific proprietary forms of security authentication.

With regard to impact on the network, BAS bandwidth requirements are generally very small. Network traffic is primarily generated by polling or alarming events. When the BAS network is designed, great care is taken to minimize network broadcasts. Traffic may be heavier when the system is being installed and configured, or in the case of a building emergency. Otherwise, experience has shown bandwidth impact is generally less than five percent.

As with any typical IP network-supported application, network services like DHCP and DNS are considerations, as are standard directory services like Active Directory and LDAP. BAS will use these services as any other application would, although some BAS devices may require static IP addresses. The PC's "hosts" file may need to be used to enable the use of static IP. If DHCP is used, it is often best to define long-term or "permanent" leases for the IP addresses used in the BAS system.

4. What network support is required from the organization's IT group?

A BAS network requires available connectivity, IP addresses, specific open TCP and UDP ports and, in most cases, remote access capability. BAS computing resources, like file servers and workstations, require

standard IT support. Specific BAS components such as BACnet controllers and downstream devices would likely be supported by facility management or the BAS vendor.

5. Does the BAS require access to the Internet?

No. A BAS generally resides on the intranet behind the corporate firewall, isolated from the Internet. Multi-site connectivity is supported via the existing WAN, or site-specific remote access services like VPN.

This being stated, access to the BAS, or vendor support access to the BAS, will most likely be from the Internet. Remote access (for remote support or management purposes) is typically supported via existing IT-approved methods, such as VPN. BAS applications primarily use UDP instead of TCP.

6. What is BACnet and how does it affect the network?

BACnet is a communications protocol that is used by the BAS controller and provides a standardized data transfer mechanism for the HVAC industry. BACnet data packets are embedded within the IP data packets and are evaluated by the BACnet controller after the NIC card accepts the packet.

BACnet utilizes the UDP stack for network layer traffic and is port specific. BACnet device communication requires a static IP address, passive NAT will prevent proper communications between BACnet devices. Besides this requirement, BACnet traffic will blend into our network like all other UDP packets.

7. Does the BAS require remote access?

Some form of remote access is generally desirable to provide offsite management for facility or IT personnel. Remote access is usually required if BAS vendor support is provided.

Remote access can take any form the organization supports, but Virtual Private Networking (VPN) is the recommended approach. Also, workstation remote control software (VNC, PCAnywhere, Dameware, etc.) may also be used. These applications allow remote control of BAS workstations or file servers, from which the entire BAS can be controlled to the extent security permits.

Using the existing organizational approach to remote access allows the control of that access within current best practices, making remote BAS support standardized and secure.

8. How does BAS implement security?

Usually BAS system access is only needed by a relatively small group. Typically comprised of facility management, IT support and the BAS vendor, some form of remote access is often needed as well.

A well-designed BAS is not likely to be the source of internal attacks. Trane BAS systems also support data encryption. BAS downstream equipment is often very specialized with industry-specific protocols, so it is very unlikely that a security breach will occur.

BAS workstations and networked controllers support standard network interfaces and are fully securable like any other standard networked device. Virus-scanning software is compatible and recommended for BAS workstations and servers. BAS workstations and file servers are as vulnerable as any other similar device already supported by IT. However, virus threats are rare against the proprietary software running the downstream BAS components.

BAS security is implemented as with any other application. Most existing standards and best practices can be followed. The BAS application security, which is built into the BAS system itself, can be maintained by either IT or facility management as organizational guidelines dictate.

Additionally, many building automation systems use encryption to protect any data being transmitted from being hacked. BAS data encryption is generally supported to 128 bit SSL.

9. What maintenance does the BAS require?

Periodic maintenance requirements are the same for a BAS as for any other computing system. BAS software

does get updated and software upgrades can be issued periodically. BAS vendor support is typically available and very comprehensive, and a good BAS vendor will be committed to customer success.

The ongoing support of the BAS includes applying system fixes, application software upgrades, and operating system fixes and upgrades. Operations scheduling, system backup/restore, and system hardware maintenance are also required. BAS data that is accumulated on a PC workstation or file server should be saved and protected as any other application date. If a server is a BAS component, it should be located with the other business servers and maintained accordingly.

Server and workstation support would usually be provided by IT, but typically most of the devices operating in a BAS do not require IT maintenance. They are specialized devices that are supported by the BAS vendor or facilities manager. In supporting BAS servers and workstations, standard system management tools can be used. BAS can also be supported by widely implemented network management tools such as OpenView, Unicenter and Tivoli.

Building automation systems are very specialized applications and generally completely compatible with the other business computing applications found in an organization. However, some BAS devices may use vendor-specific applications.

Generally, the IT group will not need specific training to support the server and workstation components of the BAS implementation. However, further investigation of downstream BAS components may be required to better understand how the overall BAS works. Trane will offer all training necessary to successfully support its BAS solution.

10. What are the Disaster Recovery implications of the BAS?

When a BAS PC workstation (a PC running BAS management software) or file server (a server that allows centralized running of programs, and the accumulation and sharing of data) is lost, the BAS is not as susceptible to failure as other business systems might be. BAS network nodes can usually function independently, each controlling devices possessing the intelligence needs to perform their particular duties within the system. These devices often support their own event logging and that data may be recovered when a failed BAS workstation or server is brought back online.

Devices that are downstream from workstations or file servers tend to be less susceptible to failure. Equipment controllers are very reliable devices, but if they do fail the devices they control will generally still continue to function. Most core BAS devices allow manual intervention (in fact, before building automation systems were conceived, everything was manually controlled).

Each organization is unique; therefore a good disaster plan will identify and prioritize critical applications. To facilitate actual disaster recovery planning (DRP), a specific BAS disaster plan should be created when the BAS is installed. If desired, this plan can then be merged into the enterprise disaster recovery plan.

Learn more at trane.com

TRANE

Trane – by Trane Technologies (NYSE: TT), a global climate innovator – creates comfortable, energy efficient indoor environments through a broad portfolio of heating, ventilating and air conditioning systems and controls, services, parts and supply. For more information, please visit *trane.com* or *tranetechnologies.com*.

BAS-SLB014-EN
07/16/2020