Advisory Note

A Service to A.G. Coombs Group Clients.

Are you in Control of your BMCS?

In modern buildings, Building Management and Control Systems (BMCS) are responsible for the operation of critical systems including air conditioning, ventilation, lighting, backup power supplies and, often, building security and access. These critical systems can be let down by a substandard computer, communications and power supply infrastructure, or by poor management and maintenance practices.

Computer Hardware and Power Supplies:

A 'normal' desktop computer is typically used for a BMCS. These systems should be selected, maintained and managed in the same way as any commercial computer system. File servers should be selected with an appropriate level of computing power, memory and data storage. Depending on the criticality of the facility, disk arrays and redundant servers can also be considered.

Resilience strategies should incorporate a sufficient level of Uninterruptable Power Supply backup to ensure continuity of the facility operations. This also applies to communications network infrastructure equipment including gateways, routers, switches and hubs. The system should be able to recover without human intervention.

As with many computer systems, the computer hardware has an expected life cycle of around three years and replacement should be planned accordingly.

BMCS software:

The BMCS software application should be maintained to ensure correct operation; noting the difference between maintaining software and upgrading. Maintaining will correct bugs with minor improvements while an upgrade will usually include new features and functionality. It is recommended that a software maintenance program be included within the BMCS maintenance contract.

The BMCS vendor should inform the system owner of software upgrade releases and if the upgrade requires any field hardware upgrades or if previous versions of software will no longer be supported.

The BMCS software database should, ideally, be automatically backed up on a regular basis. This should include all configuration data as well as performance data such as trend history. This is particularly important with metering data used for NABERS assessments. An off-site copy of the database backup should be kept by both the building owner and the BMCS maintenance provider.

Computer Operating Systems:

Outside the BMCS software, the computer operating systems and core software applications should also be commercial or professional grade. These should be selected based on the size and configuration of BMCS and the facility. Basic or freeware versions of applications may work but typically do not have the capacity to support the complete BMCS functionality requirements.

Anti-virus software application should be installed on all BMCS file servers and workstations.

It is important that the software is maintained with any upgrades and patches as and when they become available.

It should be noted that Microsoft ends support for Windows Server® 2008 and Windows® 7 operating systems on January 14, 2020.

Release of software patches and support for security and performance issues for these operating systems will end.

If your operating system is affected, your BMCS platform could be at risk for cyber-attacks, malware, and other threats. To keep your building secure, it is important to act.

All software and upgrades should be certified by the BMCS system vendor for compatibility with their system.

Communications Networks:

BMCS communications networks are typically broken into backbone infrastructure (based on high speed Ethernet data networks) and controller sub-networks (based on the RS485 Communications Protocol). The network infrastructure architecture should be well documented and the documentation maintained for the life of the system.

The high speed backbone should be installed to a recognised commercial data infrastructure standard and be tested and certified to the relevant technology standards. Again, commercial grade communications network equipment should be used that will support the required network management. Domestic grade equipment is not adequate. The design should also include capacity for future expansion.

Whether BMCS communication networks are standalone or integrated into a facility's enterprise communications network, configuration should carefully consider factors including system criticality, capacity, redundancy, and power supplies.

Field controller sub-networks should be designed to meet the standards for both the technology used as well as the installation requirements of the BMCS hardware supplier. All field sub-networks should be installed to support future expansion. This should include sub-networks for third party devices over High Level Interfaces (HLI).

For more information on BMCS Management, please contact:

Andrew Smith
Leader Building Technologies
P: +61 3 9248 2700
E: asmith@agcoombs.com.au