HBT-HBS

BMS ICT & Cybersecurity Technical Specification Guide

7 April 2020 | Revision No. 1 HBS-ICTCOE-031

DISCLAIMER

The information contained in this document is for general information and illustrative purposes only, is not intended to constitute professional advice and should not be relied on or treated as a substitute for specific advice on or treated as a substitute for specific advice relevant to particular circumstances.

The information in this document is provided “as is” and Honeywell makes no warranties, representations or undertakings with respect to the contents of this document (including, without limitation, as to the quality, accuracy, completeness, suitability, merchantability or fitness for any particular purpose of its content), or any content of any other document or source referred to herein. Honeywell makes no representations, warranties or guarantees, whether express or implied, that the content of this document is accurate, complete or up-to-date and it is subject to change without notice.

In no event is Honeywell liable, in any way or for any damages of any kind or under any theory, arising from this document, or access to or use of or reliance on the information in or accessed through this document, including but not limited to liability or damages under contract or tort theories, regardless of prior notice to Honeywell.

Table of Contents

1. Introduction

The purpose of this document is to provide general guidance with respect to technical specifications for Building Management System (BMS) - Information Communication Technology (ICT) infrastructure and prospective Cybersecurity measures related thereto.

Building Control Systems are often a critical asset for organizations worldwide and can help to optimize operations and lower facility costs, while enhancing safety, security and sustainability. This document provides guidance regarding certain core ICT / Cybersecurity considerations, while implementing IT systems for a Building Management System.

2. Scope

This document describes many key ICT and cybersecurity components of BMS and provides a breakdown of products and services to be considered in managing cybersecurity risks. Key areas of focus are as follows:

- ICT Infrastructure (Network, Server, Virtualization)
- Cybersecurity Assessments
- Secure Design
- Secure Configuration
- Cybersecurity Appliances and Software
- Monitoring and Management
- Incident Response
- QA Environment
- Policies
- Supplier Cyber practices

This specification excludes all other components, products and services, including but not limited to control system hardware and software for access control, field instrumentation, auxiliary systems, and safety systems, as well as all software configuration and installation services for the BMS.

3. BMS System

BMS is an automated system that converges, integrates and connects many different facility technologies through information flow to a monitoring point.

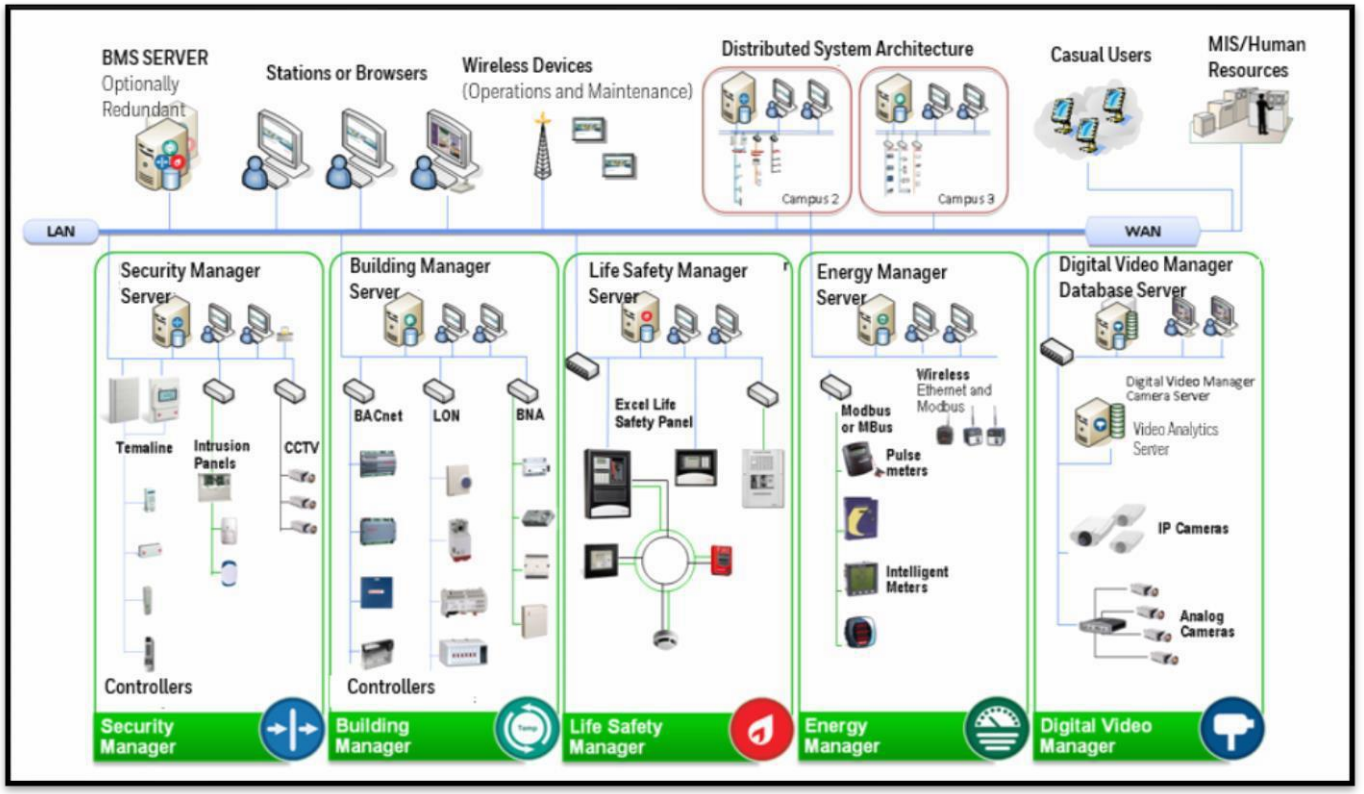
BMS is modular and often formed from the integration of products through open systems and enterprise services, providing building operators with real time or near real time facility data. This platform can help organizations to detect incidents faster, respond timely, and mitigate impact in a cost-efficient manner.

BMS technical architecture is essentially comprised of three levels consisting of management, automation and field devices.

- The management level contains the human interface, generally on the organization's enterprise network
- The automation level provides the primary control devices, connected via networked controllers
- The field device level are the physical input sensors

3.1 Basic Network Architecture

The below diagram shows a typical building network architecture for BMS.



Based on the above evolution of BMS technology, BMS now typically supports a combination of standardized Operational Technology (OT) protocols (such as Modbus and BACnet) and standard Information Technology (IT) protocols (HTTP, FTP, XML, etc.), and connectivity to Internet-based resources.

The disconnect between IT groups and OT groups is still the operational model for most buildings. Smart building technologies and connectivity often compound these challenges and can increase the potential security threats that smart building enhancements can create.

Cybersecurity configuration and design services are often utilized to apply cost-effective configuration and design principles that can help to mitigate cyber OT risks, while also enhancing the confidentiality, integrity, availability, and safety of these systems.

4. ICT Infrastructure

The ICT infrastructure consists of many assets depending upon the complexity and severity of small, medium and large projects.

4.1 Network Design

The ICT network typically provides the vital communication path and end-to-end connectivity for BMS servers, workstations and other endpoint devices. The underlying network infrastructure should be built to enable full integration with all sub systems allowing for maximum flexibility in the way the building operates over its lifespan.

The integration of BMS solutions such as HVAC, CCTV and Fire safety systems, into a single view platform often increases the value of all these systems.

A highly available building communications infrastructure should be employed to meet the required throughput and data processing capacity of all BMS endpoints and devices to be integrated.

The ICT infrastructure should be designed for future requirements and consider the various data formats to make data processing and presentation functions scalable.

Once a correctly designed cabling infrastructure is in place, the active network equipment can be overlaid. Important characteristics of the communications infrastructure include the following:

- Room for expansion, considering future requirements
- Infrastructure resilience
- Physical security measures in place
- Highly available, scalable wired and wireless network supporting high bandwidth and time sensitive data
- Supporting monitoring and management
- Supporting open systems and standards - IT industry Institute of Electrical and Electronics Engineers (IEEE), International Organization for Standardization (ISO), Request for Comment (RFC)
- Seamlessly resilient to power or backbone link failure

4.1.1 Capacity

The network should have sufficient capacity to support normal usage and, ideally, additional ability to support intermittent heavy loads or 'burst' traffic as well as future expansions desired.

Capacity or bandwidth of a network is normally measured in Mbps. Network capacity can be reduced by latency, often attributable to delays in processing network data usually introduced at routers and bridges. The greater the latency on a network, the slower it will typically be perceived to be performing with respect to processing capability. Another factor in network capacity is the number of computers connected to a network, as the greater the number and the busier they are the slower the network will again be perceived to be performing with respect to processing capability.

Measuring usage on a network is not a simple task and often requires monitoring the network using dedication-related tools and software over a sufficient period of time. This provides a baseline profile of network usage and an objective indication if capacity is inadequate for the needs of the system. Software vendors may also be able to give indications of network usage through their software.

Quality of Service (QoS) should be used to impose restrictions or to provide preferential delivery of service for specific applications or types of network traffic. For example, IP video services might be given preference on a network, reducing the capacity for data traffic. If preferential levels of services are required, the network's capacity and its capability to support the required levels should be considered. It is important to note that not all network infrastructures can support all types of QoS control.

4.1.2 Wired

In addition to the points raised in section 4.1.1, the network should also include:

- Enough network ports for the number of devices and for future expansion
- Cabling of sufficient standard to support the required network speeds

Ethernet cables are typically CAT 6 and support speeds of up to 10Gb. Total length is limited 100m or less between devices. (Note that maximum speeds are usually only obtainable over cable runs significantly shorter than the maximum run.) Cabling should be implemented to support the

capabilities of current and/or near-term network device needs. Note that it is often more cost effective to install the best quality cabling once, than to have to replace inferior quality cabling later.

It is typically recommended to use a wired ethernet network for end point devices. If a wired network is not feasible, a wireless ethernet configuration as shown below should be considered.

4.1.3 Wireless

In addition to the points raised in section 4.1.1, also consider the following:

- The network should be secured so only authorized devices can connect
- Signal coverage should extend to required areas only
- The wireless network, if configured, should not leak outside of the building
- Strong authentication and encryption on wireless should be implemented

Typical power deployment for wireless configurations utilize Power Over-Ethernet Technology (POE), eliminating the need for a power outlet at the access point. The requirements for wireless service can vary depending upon the planned use of the system and the exact system requirements. Surveys must be conducted to confirm that the requirements for a wireless system can be met.

4.1.4 Mobile

Mobile network communications are often used via devices such as mobile phones or other devices with SIM card capabilities. While different network types are available, at the time of publication of this writing 4G/LTE is the most prevalent. However, the next generation (5G) is being rolled out and is expected to offer higher connectivity speeds and better latency.

If wired or wireless ethernet solutions are not viable for every point of presence, then mobile networks can often provide viable connectivity solutions for devices deployed within an integrated BMS solution.

It is important to note that establishing connections to mobile networks can be limited by the building fabric itself and the location of network infrastructure within it. Low Power Wide Area (LPWA) networking technology like NB-IoT often helps to provide greater penetration within the building fabric and can extend the reach of mobile connectivity.

4.1.5 Active Network Components

All active network components such as switches, firewalls, and routers should have the ability to provide administrative access to allow maintenance and troubleshooting abilities. All devices should support SNMP v3 agents to allow full monitoring. The use of unmanaged devices should not be permitted.

The use of layer 2 and layer 3 capable devices enable network segmentation technologies, such as Virtual Local Area Network (VLAN) and Access Control List (ACL), and should be configured. Network devices should be logically grouped into segments with devices of a specific purpose. This should be used in conjunction with virtual and/or physical firewalls. Firewall solutions should have a central management platform to enable monitoring, management and fast patching capabilities so as to provide optimal protection from emerging cybersecurity threats.

4.1.6 Network Protocols

There are several network protocols that different services and software packages use to communicate. The most common are typically Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) over Internet Protocols (IP) in IT networks.

For OT networks, specific protocols should be required to communicate with different controllers.

Controllers should support standard protocols such as BACnet and LONWork protocols, and these controllers should allow integration with other manufacturers products on different communication protocols.

Due to the converged nature of buildings, ICT networks should make use of open protocols allowing increased flexibility when designing operational and maintenance approaches due to the potential for enhanced cause and effect integrations.

4.2 Power

The building should have enough power to support the number of devices that will operate at the same time. In the case of a power disruption, devices that are required to be online should be supplied via Uninterruptable Power Supply (UPS), so that their ability to continue operating during an outage is appropriately furthered. It should be noted that a UPS is only intended to cover short duration power interruptions, such as 20 minutes depending on the load. Longer power interruptions typically require transition to backup power, for example a generator.

Calculating power requirements is often a case of identifying the power consumption of each device in Watts and aggregating the total the amount required. Consultation with the local electricity provider may then be required to determine if the power supply to the building is sufficient.

When determining UPS needs, it should be ascertained whether devices need to run just long enough to be shut down properly or if they need to run for an extended amount of time. The longer a UPS needs to run and the more devices it needs to support, the larger the UPS should be. UPS needs are also typically governed by the business continuity and disaster recovery plans in place.

BMS should have monitoring capabilities on UPS systems, such that all alerts and information of UPS are received.

4.3 Servers

Servers are often categorized in terms of their purpose. Examples of server types available in BMS networks are:

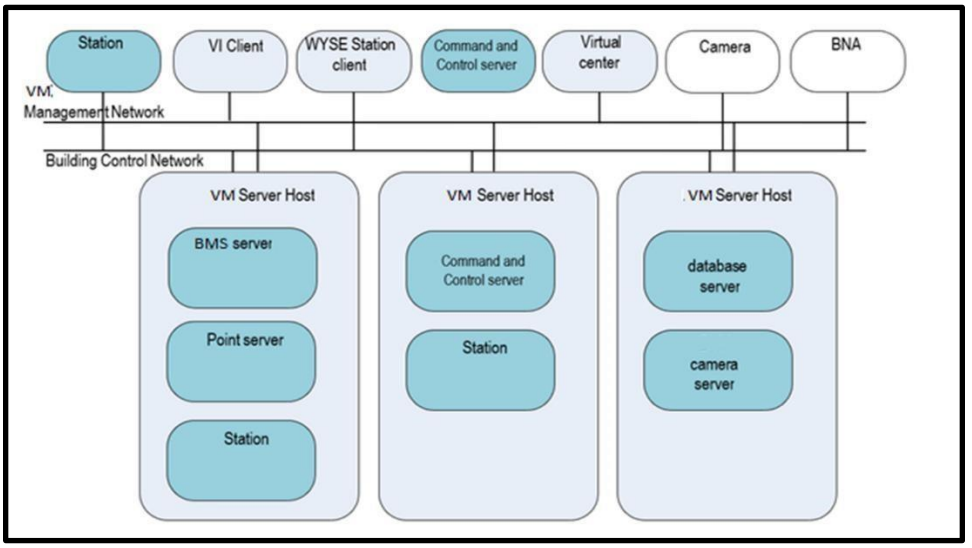
- BMS Server
- BMS Point Server
- CCTV Server
- Lighting Server
- Key Safe Server
- Backup Server
- Proxy Server
- Antivirus/Anti Malware Server
- Infrastructure Monitoring server
- Network services such as Directory Services (AD), Authentication, DHCP, DNS

Many BMS servers provide mission critical insight for building operators, helping them to minimize system downtime. Server and application resiliency should be configured to mitigate risks associated with system availability.

4.3.1 Virtualization

Virtualized infrastructure for all servers should be utilized to optimize hardware consumption and energy efficiency. Multiple virtual servers can often be hosted on a few physical hosts, reducing overall capital expenses such as required rack space and power and cooling demands. Additional virtualization benefits typically include point in time snapshots, speed of provisioning new machines and quick roll back and recovery from system changes and disaster recovery.

The figure below illustrates a BMS server, Point server and Station server virtualized on a single VM host, a Command and Control server and Station on a separate VM host, and a database and camera server virtualized on a separate Virtual host. This type of architecture removes the need for six separate physical computers.



4.4 Clients

Workstations can include physical PCs or Virtual Desktop Infrastructure (VDI) thin clients. The configuration of workstations often depends upon the application running on the system and needs to be considered carefully so that system performance corresponds to end user expectations. In most cases, this involves higher than normal work requirements.

4.5 Commercial Off The Shelf (COTS) Hardware Supplier

The core principal for determining hardware requirements starts with consulting the vendors of the software running on the system and implementing their recommendations with respect to hardware size.

In addition, you should determine the applications that need to be run using manufacturer sizing tools to scope and implement adequate hardware requirements.

Changes to hardware configurations after purchase can often be more expensive than purchasing systems with additional capability in the first instance. As such, wherever possible, systems should be purchased to allow for future growth. Growth is most often required in the amount of Random Access Memory (RAM) installed. Disk Space and processor speeds are often less likely to require growth, however, if given the option, for a minimal price differential, faster processors (or more 'cores') should be considered.

5. Cybersecurity – BMS

For BMS ICT Networks, the International Electrotechnical Commission (IEC) 62443 standard provides cybersecurity framework considerations that are useful in following ways:

- Leverage the focus on risk assessment to evaluate and identify potential threats to existing and legacy building control systems and design an enhanced cyber secure system and management protocol to better protect and maintain those systems.
- IEC 62443 defines concepts of secure OT network segmentation intended to enhance protection from both internal and external threats.

The solutions should contain expert knowledge of OT systems and industry expertise to help reduce cyber risk exposure and increase cyber resilience, including the use of key people, process and technology; this includes Defense in Depth strategies.

In addition to the below IEC 62443 OT Cyber Standards, National Institute of Standards and Technology (NIST) Guidelines and ISO27000 Framework protocols should be adopted, as per the relevant cyber requirements.

- IEC 62443-3-2: Security assessment and system design
- IEC 62443-3-3: System security requirements and security levels
- IEC 62443-4-2: Component alignment to technical security requirements

5.1 Cybersecurity Assessments

A formal threat and risk assessment are typically the essential 'first step' to determine potential vulnerabilities in BMS cyber defense profile, and typically underpins the processes and procedures for holistic go-forward risk mitigation. Areas of focus should include:

- Asset inventories
- Network baselines
- Vulnerability identification
- Remediation confirmation
- Security posture insight reporting

The assessment should identify all system gaps and seek to enhance the security level by including secure configuration considerations such as system hardening, patch management, firmware update on devices and new security solutions required.

These Cyber Assessments should be conducted at a minimum annually, to promote proactive identification and addressing of security gaps and new vulnerabilities.

5.2 Secure Configuration and Design

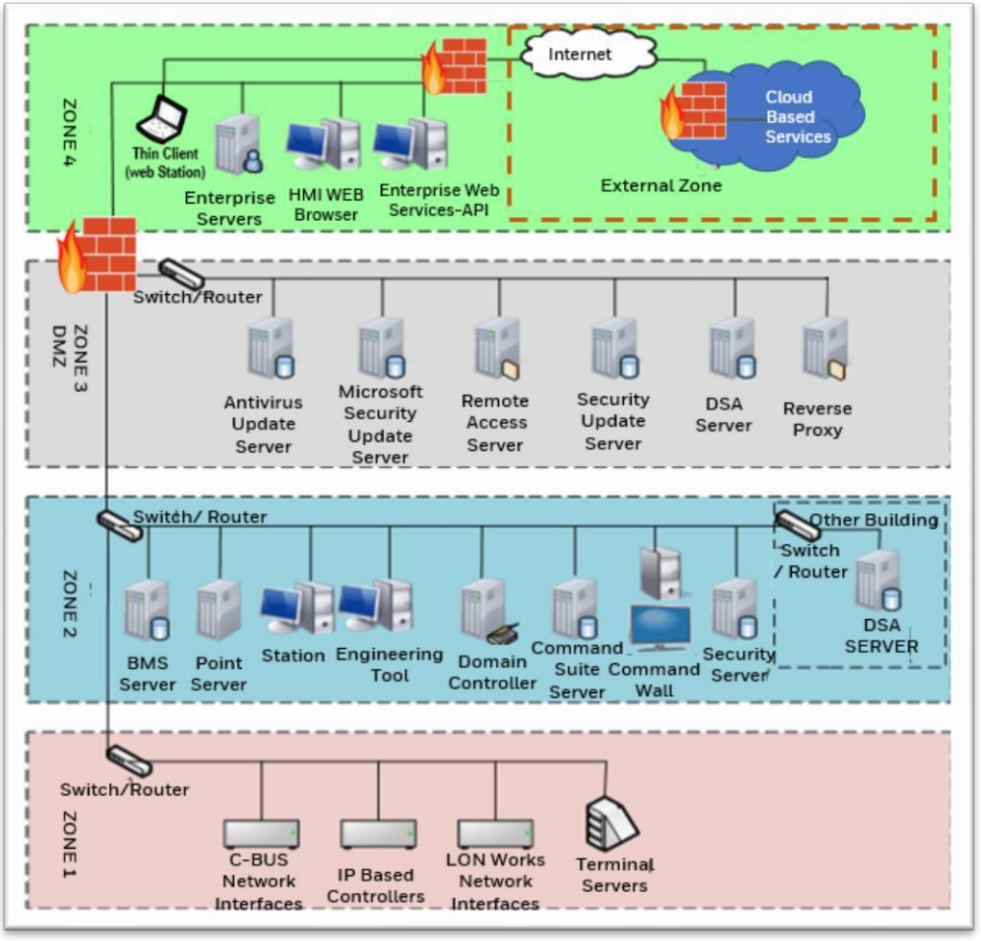
BMS network architecture should be secure and reliable utilizing ethernet-based systems. It should comprise a tiered network architecture of switches, routers, and firewalls to more effectively protect and isolate critical building operational levels from less secure network levels.

At a high level, the IEC 62443 standard recommends that control systems (i.e., ICT network) should be organized into segments or zones. This typically allows devices of similar trust levels to be grouped together, and access is restricted to help mitigate threat exposure.

Security zones should be formed for physical or logical grouping of assets that share common security requirements, with isolation of critical control systems components. A special type of security zone should be the Demilitarized Zone (DMZ), which segments the external network with the internal (ICT) network with help of security components such as a Firewall with Advanced Gateway Security. This architecture should provide a layered security approach with Defense-in-Depth.
In combination with a comprehensive defense in depth approach and complementary adoption of the NIST Framework and ISO 27000 standards, new architecture should facilitate secure interactions with valuable cloud services and ultimately smarter and more effective buildings.

Communication between zones should be restricted through a specific conduit, with the principle of least privilege, used as a configuration baseline. Conduit controls the access to the zone by often helping to resist several attacks like denial of service, malware attacks and protects the integrity and confidentiality of the network traffic.

An illustrative example of a potentially secure network design is shown in the below figure. However, secure configuration and design can be based on cyber assessment results and adopted cybersecurity standards recommendations for BMS Systems.



- Zone 1: Building, access and security controller busses connect to the Level 1 network switches via network interfaces and terminal servers. Mostly field controllers, sensors, actuators are placed in this level.

- Zone 2: BMS Servers (BMS management and point servers) connect to Level 2 switches. There are also uplink connections from Level 1 switches. If the nodes at Level 2 are part of a Microsoft Windows domain, these nodes will likely have to communicate with the domain controller.

- Zone 3: A DMZ serves as a buffer zone between the Building Control Network (BCN) and the business network. It is a separate network segment connected directly to the firewall.

- Zone 4: The business network, this is generally managed and administered by the corporate IT department and is outside the scope of these guidelines.

5.2.1 Network Security

Network security is the practice of preventing and protecting against unauthorized intrusion into networks. For securing a network, an organization should be aware of the devices connected and types of software running on the network. A detailed hardware and software inventory asset management list will help to address this concern.

Network monitoring tools and control software should be deployed to help identify real time threats and to automatically help minimize those threats. A proxy server often helps to keep users and the internal network better protected from potential cyberthreats. Proxy servers can also provide a higher level of privacy.

A RADIUS server should be deployed for secure configuration and management of all Network elements across the ICT Network. Deployment of RADIUS with active directory can be applicable for the network with maximum number of nodes to implement policies and best practices.

All switches should be managed in the network to avoid access of unused ports and promote secure switch configuration. Firewall devices should be used to segregate the network and control the access as per approved ACL. Different types of firewalls can often be used for IT and OT networks depending on the nature of network data traffic.

Firewall with advanced gateway security at the OT and IT perimeter, will often enhance protection of ICT Network (OT systems) from threats by utilizing deep packet inspection, IPS and anti-malware advanced features.

Critical data should be encrypted in the network to help avoid data leakage by packet capturing of plain texts communication.

5.3 Cybersecurity Appliances and Software

BMS System ICT network should be protected by deep packet inspection tools and Endpoint protection tools with machine learning capabilities for advanced threat detection.

5.3.1 Endpoint Protection

Endpoint security is typically vital, as threat actors often utilize endpoint vulnerabilities as entry points to corporate or OT network. Different types of endpoint security mechanisms should be considered and implemented as indicated below:

- **Next Generation Endpoint Security** – Uses advanced artificial intelligence or deep learning capabilities with behavioral analysis enhancing protection from ransomware using light weight and low touch agents. Management and reporting should be available from a central console.
- **Application Whitelisting** – Allows only authorized files to execute and run. Management and reporting should be available from a central console.
- **Data Loss Prevention –** Helps prevent leak of Intellectual property (IP) from OT systems. Management and reporting should be available from a central console.

- **Removable Media Protection** – Helps identify and quarantine destructive malware on USB with advanced threat intelligence for detecting cyber threat indicators. . Protected machines configured to explicitly require the user to confirm the identity and use of an inserted USB device.

5.3.2 Server and Client Hardening

ICT servers and client hardening should follow standards such as those provided by the Center for Internet Security (CIS) hardening and Microsoft security hardening. In addition, the following services and processes are required to establish a more secure ICT architecture for system components.

- Secure Policy Configuration
- BIOS Hardening
- Remote Management onboard (such as ILO)

5.4 Monitoring and Management

A cloud-based analytics platform should be implemented to monitor and analyze critical OT servers, workstations, virtual machines, and applications 24/7. This level of visibility often helps to plan and monitor critical site activities. The system should centrally capture and analyze key event information relating to servers and workstation assets, helping to provide an overall health status of the system, and direct the assigned technicians to perform reactive and preventative maintenance activities in an efficient way.

The ongoing network monitoring should ensure system availability and cybersecurity, thus alerting technicians to problems even before they cause an outage. A key benefit of the system sought should be early identification of actual and potential server and workstation problems, and integration to service management system to auto create work orders for technicians.

5.4.1 Remote Access

Remote access to resources (on premises) is typically a key requirement to promoting the best applicable support model. It should follow strict cyber controls to permit access only by authorized users and be carefully audited and tracked.

Controls include those in the form of:

- Two factor authentications (e.g., using tokens or mobile app authenticators)
- Fully encrypted communication– minimum standard of 256-bit AES encryption
- Secured VPN access
- May also be limited to specific devices (users may not connect from internet café or home machines but only managed devices by their respective organizations)
- Least privilege access and permissions

The solution should be designed to allow advanced features such as secure file transfers, chat messaging and collaboration to help enrich remote support capabilities.

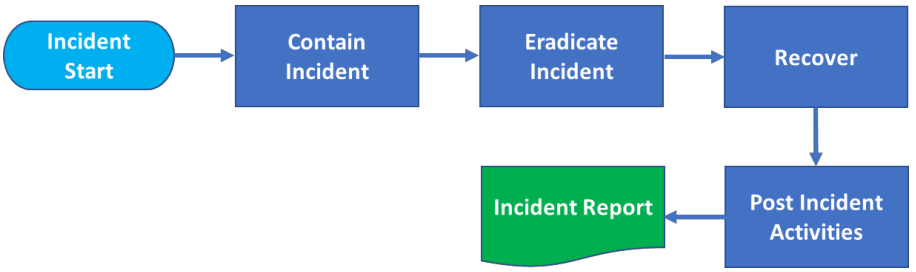
5.5 Incident Response

BMS or OT environments managers and owners should be prepared to take the right steps quickly and be ready to respond to cybersecurity incidents.

Incident response plans should provide a clear process following an incident for the response team to restore systems to a minimal-viable operating level, while seeking to address the containment and eventual eradication of the threat. Post incident activities should take place including digital

forensics

This process, done incorrectly, may lower some security controls, so it is important to follow a predefined set of protocols. This will help to contain, eradicate and recover from cybersecurity Incidents. A high-level incident response flow diagram is shown below:



5.5.1 Business Continuity and Disaster Recovery Plan (BCP)

A BCP should be in place to appropriately size the BMS system to support the services required. Business critical systems should have plans in place in the event of system or component failure, such that the business operations can continue or, in the worst case, recover within a desired time period from any significant disaster.

This should include, but not limited to:

- Provision for offsite back up or storage of data
- Supply of an identical replacement system within a specified time
- Fail-over or High Availability of servers and applications

Virtualization platforms and cloud-based solutions should be implemented for business continuity and disaster recovery of the BMS solution.

5.5.1.1 Backup

Backup strategy and policies should be clearly defined and deemed to be the most efficient based on the physical and virtual solutions deployed.

Backups should be in place, so that any data with the need to be preserved is covered by backup agreements with the relevant service providers. Backups should be kept securely and for specified periods of time as required (e.g., as required by law or by company policies).

Backup data should be treated with the same confidentiality as live system data and should be protected against tampering with the use of an auditable solution.

If data is backed up and stored off site system implementations should provide that, in the event of need, it can be restored or retrieved in line with business requirements.

6. Policies

ICT and Cybersecurity polices should be created, maintained and reviewed annually. Polices include, but are not limited to: Password management, Access control management, Patch management, Backup and recovery, Acceptable use of information, Change control, Logging and monitoring, Risk management, Media handling.

7. Quality Assurance (QA) Environment

There should be a QA environment setup and maintained at site level. This environment should be capable of testing all changes to BMS systems, prior to deploying in the production environment.

The QA environment should be running identical versions of hardware and software as the production environment. Production environment data should not be copied to the QA environment.

8. Supplier

There should be established processes in place to evaluate products and vendors. Strong cybersecurity maturity should be demonstrated as part of the organization's culture.

Key areas may include, but are not limited to:

- Secure Development Lifecycle (SDL) processes of vendors, based on CIS, NIST and IEC 62443 standards
- Strong security controls defined by cybersecurity team in their supplier specifications, as part of the supplier vetting process
- Agreed security arrangements with external suppliers
- Documented process to govern the selection and management of outsourced vendors
- Maintaining appropriate contacts with relevant authorities
- General Data Protection Regulation (GDPR) compliance
- Information security policy
- Information security incident management process
- Information classification scheme
- Information security risk identification and remediation
- Security awareness curriculum to create security positive behavior