National Protective Security Authority

GUIDANCE

Adopting a security-minded approach to building automation and control systems (BACS)

Table of Contents

Introduction

Building automation and control systems (BACS) are fundamental to the safety, security, and operation of most contemporary built assets. Examples of BACS include:

- Building Management Systems (BMS) that control lighting, and heating, ventilation, and air conditioning (HVAC).
- Building Energy Management Systems (BEMS) that manage energy demand, but also where applicable, local generation and energy storage. The generation and storage can be for both energy efficiency and/or business continuity purposes (e.g., UPS).
- Automatic Access Control Systems (AACS) managing access to the built asset and zones within it.
- Fire and Security Systems that detect potentially harmful or hazardous conditions and provide alarms or alerts to first responders.
- Facilities Management Systems providing functions such as room bookings, maintenance fault reporting, maintenance scheduling, etc.
- In some built assets the BACS may also be linked to, or integrated with, Industrial Automation and Control Systems (IACS), where the BACS controls the environment in which manufacturing and production lines, or process industries operate.

The scope of these systems and their level of integration can vary significantly. At the higher levels of integration this has led to terminology such as ‘Smart’ or ‘Intelligent’ buildings, for which there are many definitions.

BACS technology has rapidly evolved from essentially analogue sensors and communications connectivity to more complex digital devices operating over wired or wireless networks. This new technology, commonly referred to as the Internet-of-Things (IoT), may in part rely on use of cloud-based storage and processing hosted by a system or service provider. There may be significant differences between security measures and cloud management resources procured by your organisation compared to those bundled as part of, e.g., a BEMS system or associated energy-related service offering.

The connectivity and widespread deployment of BACS functionality creates inherent information flows extending across organizational boundaries. For example, a BEMS may process space occupancy data and externally sourced meteorology data, with its outputs used to:

- optimise the control of HVAC systems;
- achieve optimum use of energy or heat generated by the built asset; and/or
- provide information to an external energy management service.

The metrology data may be sourced from outside the built asset, via the Internet and/or from locally installed weather stations. Data from the local environment monitoring provides data on the current local conditions, while external meteorological data is used for future energy demand forecasting. These external data feeds into the BEMS may represent an exploitable vulnerability.

Organisations need to be aware of and understand the security implications concerning BACS, their reach both within and between organisations and critically, the threats and vulnerabilities BACS potentially embed into an organisation and its business operations.

Why is security and resilience of BACS an issue?

Due to convergence of technologies in BACS and enterprise IT systems, their integration and inter-connection has rapidly increased, particularly where organisations are seeking:

- to reduce their carbon footprint and overall energy consumption;
- efficiency gains from changes in the operation and maintenance of built asset plant and machinery;
- to optimise and reduce the amount of space required due to adoption of hybrid working.

Whilst the business benefits of this increased system connectivity are manifold the vulnerabilities are generally less well understood.

From a physical security perspective, BACS device and network vulnerabilities include physical access to automation equipment such as sensors, actuators, local controllers, management workstations and communication networks. Threats arising from such physical access include unauthorised creation of local and/or remote connectivity, foreign device insertion and local reprogramming. Modern building systems increasingly employ telemetry, sending data back to manufacturers or suppliers. This may be a consequence of the procurement model used, e.g., procuring an Asset-as-a-Service (AaaS) involving payment by use, or as a mechanism to support diagnostics and preventative maintenance, e.g., detecting and investigating changes in performance before a fault or failure occurs. The use of system telemetry is an inherent security vulnerability. It is important to consider how such telemetry is used, and how remote access is granted and managed.

From a personnel security perspective, BACS vulnerabilities include insider threats, poor cyber hygiene, and little or no control of online and physical access to the system. Personnel security issues are exacerbated where multiple organisations are involved in use and maintenance of the BACS, particularly if there is limited or inadequate security governance. Supply chains comprising visiting contractors and maintenance personnel are typically subject to minimal security scrutiny and may not be adequately supervised.

From a technical security perspective, vulnerabilities can arise from a wide range of software (application) and system components, as well as emergent risks arising from integration or interconnection of systems. The longevity of many BACS, in comparison to typical enterprise systems, means that maintaining security over an extended operational lifecycle can be challenging. Hardware and software become obsolete, unsupported or lacks the capacity to run the latest security tools. This can lead to use of second-hand or reconditioned equipment, of unknown provenance or reliability, to prolong the operational life of a BACS.

BACS exploitable vulnerabilities can be considered from several threat-facilitating aspects. The potential consequence of such threats will be determined, in part, by the level within the automation hierarchy at which a vulnerability exists, but also the potential to access higher architectural levels or move laterally between systems. Threats arising from such access include denial of service, data/information theft, covert facility entry or espionage, loss of data confidentiality, integrity or availability, and access to other business packages.

Four primary categories of adverse consequences can arise when threats to a BACS are realized:

- Loss – events causing degraded operation of BACS functionality resulting in catastrophic system failure and/or creation of hazardous or harmful situations;
- Denial – events that result in the inability of an authorised user to control the BACS or respond to alerts/alarms, whilst the system itself continues to operate 'normally';
- Manipulation – events occurring where an unauthorised party controls or influences operation of the BACS, includes presenting false information to authorised users;
- Unauthorised access – these events enable an unauthorised party to gain access to the built asset and/or information about it.

These four categories, which are described further in Appendix A, can impact different aspects of BACS functionality creating a range of consequences that affect built asset operation as well as the built asset owner/operator/users.

A sophisticated attack or combination of attacks can realise threats in multiple categories affecting different aspects of the BACS. For example, manipulation of sensor data may result in a harmful loss of control of a BACS, with the illicit activity being concealed by a denial of control and monitoring (i.e., an authorised operator is unable to access the control workstation to view or change system operation).

Establishing a security baseline for a BACS

Unlike corporate IT systems that are generally managed by a corporate IT team, responsibility for BACS often spreads across multiple organisational units or organisations. Typically the operation of BACS are managed by a facilities manager, who may work for the built asset owner, occupier, or for a contractor providing facilities management service (e.g., cleaning, reception, catering, manned guarding, etc.). For example, in a tenanted or multi-tenanted building the landlord or their supplier may have responsibility for some systems and/or services, and tenants for others. Security becomes more complicated when multiple organisations are responsible for a group of interconnected systems.

To establish a security-minded approach to BACS it is advisable to take the following five steps:

1. establish the current deployment of BACS in the built asset(s);
2. assess criticality of each BACS sub-system to your business operations;
3. perform a BACS risk assessment;
4. develop the BACS security strategy; and
5. implement the BACS security strategy.

NOTE: If you are planning the design and construction of a new built asset that will include one or more BACS the process set out in the Appendix C details specific considerations that should be addressed. This Appendix is also relevant when planning significant changes to an existing built asset that affect the configuration, integration or operation of existing BACS.

1. Establish the current deployment of BACS in your built asset(s)

This is essentially a stocktake of the systems providing BACS functionality in the built asset(s). A set of questions is provided in Appendix B to identify essential information about each of the identified BACS.

2. Assess criticality of each BACS sub-system to your business operations

Working with the built asset owner/operator and the business users/occupiers of the built asset(s) determine the criticality of each system, in terms of:

a) built asset safety & security;

b) business continuity (e.g., necessity in respect of built asset continuity of use);

c) business goals (e.g., energy efficiency, carbon footprint, etc);

d) built asset operations and maintenance (e.g., facilities management).

Where the BACS is creating and maintaining a controlled environment to support storage, manufacturing, or regulated processes (e.g., chemical, biological, radiological or nuclear processing) the impact of BACS failure or malfunction should be assessed.

3. Perform a BACS risk assessment

Using your organisation's risk assessment guidance for each BACS, taking into consideration criticality of the system(s), systematically assess the impact arising from events materialising in each of the four threat categories listed in Appendix A. For each risk, identify whether there are any appropriate and proportionate mitigation measures that may be applied and how they would affect the potential impact. Mitigations may involve both security and operational measures. For example, a security measure to reduce the likelihood of the risk occurring and operational measures to mitigate the impact can improve the resilience of the built asset and help to maintain business continuity. The importance of uninterruptible power should not be ignored, just as with corporate systems, loss of power can be very disruptive as loss of some safety and security systems can make a built asset unusable.

Your understanding of the likelihood of an adverse event occurring will be influenced in part by information you collected in the first step. It will also depend on the attractiveness as targets of your organisation, the built asset(s), and your neighbours – both in the built asset(s) and in neighbouring built assets or sites. For example, if you occupy a high-profile building or have a high-profile neighbour this may increase the attractiveness of the BACS as a target for a malicious or hostile actor.

Where two or more BACS are interconnected, or integrated, you should also consider the potential impact of combinations and cascading effects, and again how mitigations may moderate their impact. These effects occur where a malicious or hostile act on one system results in adverse effects in other systems. For example, for energy management and efficiency purposes the BEMS could be connected to the AACS, allowing the HVAC settings to be optimised to achieve the most energy efficient settings whilst an area, floor or building is unoccupied. This interconnection could provide a route between the two systems enabling lateral movement between system. This in turn could allow an attacker to gain unauthorised access or make changes to AACS settings, thus compromising the control of physical access to the built asset or part(s) of it.

Note: If your organisation does not have guidance on security risk management then use the guidance available on the NPSA1, 2 and NCSC 3 websites. In addition, Appendix D outlines some consideration regarding security goals that are relevant to built assets and cyber-physical systems such as BACS.

4. Develop the BACS security strategy

Based on the risk assessment conducted in the previous step, systematically review the BACS risk portfolio. Determine the acceptability of each risk and where applicable any identified combinations or cascading risks. If an unmitigated risk is unacceptable, then:

- mitigation measures should be identified and addressed in the security strategy; and
- where applicable, any associated operational measures addressed in a business continuity plan.

The security strategy should specify how the BACS are to be monitored and managed. For example, for larger organisations, consideration should be given as to whether the BACS are subject to monitoring by the organisation's operations centres (security/network/facilities management) so that a coordinated response can be provided to potential security and/or safety related incidents.

In developing the BACS security strategy consider how frequently the strategy should be reviewed on a routine basis and what triggers may be appropriate for ad hoc reviews. The strategy should also provide direction on how changes to (including introduction of new) BACS should be assessed.

Depending on the nature of the built asset and the organisation's relationship to it, development of the BACS security strategy may require collaboration with third parties, e.g., the built asset owner, operator/facilities manager, and other tenants or occupiers. This may require sensitive information to be shared; if so, appropriate data sharing agreements should be put in place to protect sensitive information.

5. Implement the BACS security strategy

Once the security strategy has been developed there is likely to be a programme of work to implement the security measures and, where applicable, any business continuity measures. It is important to maintain accountability for these implementation activities and their ongoing monitoring and maintenance.

An important general measure that should be implemented as part of the strategy is the raising of security awareness among built asset users. For example, those who monitor and manage the physical security of the building, should also be aware of, and trained how to, recognise and react to attacks on building systems as well as physical intrusion. This can provide an effective deterrence to hostile or malicious individuals who are seeking to damage or disrupt the operation of the BACS.

[1] https://www.npsa.gov.uk/content/adopt-risk-management-approach
[2] https://www.npsa.gov.uk/insider-risk-assessment
[3] https://www.ncsc.gov.uk/collection/risk-management-collection

Sources of further guidance

- For guidance on cyber security tailored to the built environment see:

  IET Code of Practice for Cyber Security in the Built Environment – 2nd Edition. Available: https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-in-the-built-environment-revised-second-edition/

- For guidance on physical and personnel security, and security-mindedness, see also: National Protective Security Authority (NPSA) website – http://www.npsa.gov.uk

- For guidance on cyber security see also:

  National Cyber Security Centre (NCSC) website – http://www.ncsc.gov.uk

- For information about the security of sensors and sensor networks, the approach set out in this PAS is equally applicable to built asset systems:

  PAS 7040:2019 Digital manufacturing – Trustworthiness and precision of networked sensors – Guide. Available: http://shop.bsigroup.com/PAS7040

Appendix A – Explanation of BACS Threat Categories

The table below provides illustrative examples of how the realisation of threats can affect aspects of a BACS resulting in harm, damage, financial or reputational losses.

Threat Category	Aspect	Consequence examples
Loss	Control	May result in catastrophic systems failure, e.g., BACS becomes infected with malware, ceasing to operate correctly and resulting in damage to building services plant and machinery.
	Function	Impact on business operation & stakeholders, e.g., during construction work BMS cables in another area are damaged resulting in a loss of HVAC in an operations centre which is evacuated due to an unacceptable temperature rise.
	Monitoring & Information	Loss of visibility and potential loss of control, e.g., an event requiring human intervention occurs out-of-hours and the duty responder is unable to remotely access the system due to a broadband outage.
	Safety/Security	Increased risk of harm to people, assets & environment, e.g., through incorrect or inappropriate system operation.
Denial	Control	Unable to change system state, e.g., a disgruntled now ex-employee changed the BMS start-up password, the users are unable to access the control workstation following a power outage.
	Monitoring & Information	Unable to view system state, may impact other systems or processes, e.g., an operator had used the BACS control workstation to read and answer social media posts. A malware infection of the workstation encrypts the disk drive preventing use of the workstation.
	Safety/Security	May be compromised by loss of alerts or alarms, e.g., electrical interference jams the video feed from a wireless CCTV camera preventing security personnel from responding to an incident.
Manipulation	Control	Unauthorised system actions disrupting business operations, e.g., a hacker gains remote access to the BMS and modifies the temperature set-points in a refrigerated storage area leading to the spoiling of a large amount of perishable stock.
	Sensors and/or Actuators	Malfunction of system, e.g., physical interference with the sensors on a bulk liquid storage facility result in the overfilling of a toxic waste tank resulting in pollution of a local waterway.
	Monitoring & Information	Malfunction or compromise of system, e.g., unauthorised changes to firewall rules allowing exfiltration of commercially sensitive energy use data.
	Safety/Security	False alarms or alerts diverting resources and/or causing disruption, e.g., by gaining remote access to a fire alarm system, a disgruntled employee triggers false alarms severely disrupting the business for several weeks.
Unauthorised access	Security	Unauthorised access to built assets or parts of them, e.g., vulnerability exploited to allow cloning of security access token permitting unauthorised access to secure areas.
	Modification	Compromised system integrity, e.g., data exfiltration, e.g., installation of a compromised counterfeit component (i.e., sensor/actuator) providing a backdoor into system.
	Monitoring & Information	Hostile reconnaissance (pattern-of-life/pattern-of-use), e.g., an organised criminal gang gains access to BACS systems at a site handling valuable materials, they use the information to successfully plan a raid without needing to physically reconnoitre the site.

Appendix B – Questions to determine baseline information for a BACS

Ideally all the information listed below would be readily available to the relevant managers but given the nature of BACS it may be necessary to gather up-to-date information from several organisational units or organisations.

For the BACS portfolio associated with a built asset:

a) identify all the systems providing building automation and control functionality.

Note: from a configuration management perspective is it beneficial to create a configuration management database to hold both this high-level information and the more detailed information listed in (b) to (d) below.

b) for each BACS establish:

a. the scope of the system, i.e., its function and the physical distribution of its component parts;

Note: from an asset management perspective, it is beneficial to capture and maintain data such as component location, serial number, model and version numbers along with any software versions and variants. This data should be catalogued to enable for future monitoring of vulnerabilities, i.e., the BACS equivalent to the Common Vulnerabilities & Exploits (CVE) Database use by corporate systems.

b. who is responsible for:
    i. operating the system;
    ii. maintaining the system;

c. for all system software:
    i. whether it is up-to-date;
    ii. how often it is updated;
    iii. whether the update process is manual or automatic; and
    iv. who is responsible for ensuring updates are installed and tested;

d. what other systems does it connect to, both in and outside (remote) to the built asset;

e. whether the system has remote access capabilities, and if so the:
    i. nature of the access;
    ii. systems, organisations and/or personnel with access; and
    iii. what arrangements are in place for granting, reviewing and revoking access;

f. whether there is a system security policy and if so when it was last reviewed and/or updated;

g. whether it is subject to any periodic security testing, and if so:

i. the scope/nature of the testing;
ii. the frequency of tests;
iii. when the system was last tested; and
iv. the arrangements for addressing any identified vulnerabilities.

c) Who has responsibility for approving the addition of new BACS, modification of existing BACS, and interconnections or integration of the BACS;

d) What BACS information is shared and how sensitive it is:
   a. automatically or semi-automatically between the BACS and other systems; and
   b. manually obtained and passed to other parties or systems.

Note: For guidance on assessing the sensitivity of data see the NPSA publications - https://www.npsa.gov.uk/security-minded-approach-open-and-shared-data &

https://www.npsa.gov.uk/security-minded-approach-information-management

Appendix C – Addressing security of BACS during design and construction

This Appendix is focused on the first three stages of the five-stage lifecycle (conception, pre-implementation, implementation, operation and disposal) described in the IET/NCSC Code of Practice for Cyber Security in the Built Environment[4]. Figure 4.2 in the Code of Practice illustrates how these stages relate to those commonly used in various industry plans of work (e.g. the RIBA stages).

C.1 Conception

At this stage there are strategic considerations regarding the future operation and support of the built asset, e.g., the need for automated control over the built asset's environment and the monitoring management of energy use. For built asset owners, or operators, of a portfolio of built assets, a further consideration may be whether the BACS in any new or modified build asset should be integrated into a central monitoring and control facility.

The following plain language questions that should be considered at this stage:

1. What BACS are likely to be required or modified in the built asset?
2. How will the BACS be monitored and managed?
3. Will any BACS data be electronically shared or accessible by third parties?

It is prudent to develop, or for an existing built asset review and update, the security strategy to ensure that security risks associated with the BACS are appropriately addressed.

C.2 Pre-implementation

During the pre-implementation stage the design will be progressively developed. The built asset owner and/or operator should develop the concept of operations (CONOP) for the buildings considering the building systems that form part of the emerging design. The CONOP will need to address how building systems are monitored and managed, and the provision of connectivity to them by third parties. The means by which connectivity is provided have implications for the security of the building systems, the BACS and potentially the enterprise systems within the built asset.

For example, in a multi-storey built asset, to comply with disability discrimination a vertical transportation system may be needed for wheelchair access. These systems are generally monitored not only through a central call centre linked to an emergency call button but also through the flow of condition monitoring data to the supplier who provides a preventative maintenance service. Operation of the vertical transport system would therefore need the provision of connectivity for the emergency call button as well as digital connectivity for transmission of the condition monitoring data.

[4] Free download: https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-in-the-built-environment-revised-second-edition/

The following plain language questions that should be considered at this stage:

1. What building systems are going to be installed/modified in the built asset?
2. For each building system where will, or is, the BACS located?
3. For each BACS who will, or has, access to it and is such access within the built environment or remotely?
4. What are the proposed, or current, maintenance arrangements for each building systems and what access to the BACS is required by the maintainer?
5. What BACS connectivity infrastructure is likely to be required, or modified, in the built asset?
6. How will the BACS be monitored and managed?
7. What BACS data, if any, will be electronically shared or accessible by third parties?
8. For any BACS data that is to be shared has the sensitivity[5] of the data been assessed?
9. What integration of building systems is required, or currently exists, and how does this affect the respective BACS?
10. Where there is currently or is proposed to be integration, or interconnectivity, between BACS, what are the separability requirements and the requirements regarding separate operability?

Based on answers to these questions and the security strategy, during this stage the following documentation should be developed:

a) The security policy/policies covering the building systems and BACS. Depending on the nature of the building systems and the level of integration of the BACS, one overarching policy may be suitable or individual policies required for separate systems.

b) A security architecture addressing the physical and cyber security of the building systems and their associated BACS.

c) The security requirements for each building system and associated BACS. These requirements should be included in the tender pack for the procurement, installation, delivery, commissioning, and handover of new or modified building systems and BACS.

C.3 Implementation

During this stage there are numerous opportunities for security vulnerabilities to materialise. These range across the spectrum from deliberate and potentially hostile acts to errors and/or omissions in the procurement, installation and configuration of the building systems and BACS.

The following plain language questions that should be considered at this stage:

1. Are the building systems and BACS installations delivered in accordance with the approved security architecture?
2. Have any “as built” variations from the approved security architecture been reviewed and approved by the security manager?
3. How is compliance with the security requirements being verified and validated?

[5] Triage process – see https://www.npsa.gov.uk/security-minded-approach-open-and-shared-data

4. Have the security operating procedures (SYOPS) for the BACS been developed and approved by the security manager?
5. Has appropriate security training been developed for those using the BACS and maintaining the building systems?
6. What are the arrangements for updating/patching BACS software to address security vulnerabilities?
7. How will end-of-life/end-of-support for BACS be communicated to the built asset owner/operator?
8. What is the incident response plan if a security breach or suspected breach occurs that affects the building systems and/or BACS?
9. What is the business continuity plan regarding building systems and BACS?
10. What are the arrangements for periodic security testing, audits and reviews of building systems and BACS?

During the commissioning of the building systems and BACS and prior to handover/hand back of the systems to the built asset owner/operator the implementation team should complete the security verification and validation, and deliver the operation and security training to the personnel that will operate/maintain the systems.

C.4 Handover to Operations

During the handover, or in the case of an existing built asset the hand back, to the built asset owner/operator there are several essential security related tasks that should be completed. For example, all default passwords should be replaced with built asset/operator specific passwords, all test accounts should be disabled and/or removed, all external/remote access that is not part of the approved security strategy should be disabled and/or removed.

The following plain language questions that should be considered at this stage:

1. Has the security and user training been completed for BACS users and building systems maintainers?
2. Are all required security operating procedures (SYOPS) approved and in use?
3. Have any approved “as built” variations been incorporated into the approved security architecture?
4. Has the physical security of the building systems and BACS installations been verified and validated?
5. Has the cyber security of the building systems and BACS installations been verified and validated?
6. How is compliance with the security requirements being verified and validated?
7. Are documented and tested arrangements in place for updating/patching BACS software to address security vulnerabilities?
8. Has the incident response plan been tested for building systems and BACS?
9. Has the business continuity plan been tested regarding failure or loss of service from building systems and BACS?

10. Are arrangements in place for periodic security testing, audits and reviews of building systems and BACS?

C.5 Maintaining security

Over time, changes will inevitably occur to the built assets, the building systems, and the BACS. It is essential that a security minded approach is adopted to ensure that these often-incremental changes do not progressively degrade the original security strategy, policies and architecture. As threats change and vulnerabilities emerge it is important that the security is periodically reviewed and where appropriate and proportionate changes made to maintain the security risks within acceptable bounds.

Appendix D – Security goals for built assets and cyber-physical systems

Security requirements are typically created in response to specific security goals. For example, in respect of enterprise IT the concept of the "CIA Triad" refers to the security goals of confidentiality, integrity, and availability. This is a narrow set of goals. In practice, where the security of complex built assets and/or cyber-physical systems is to be addressed, a wider set is required. When specifying, designing and implementing a BACS, organisations should consider how the security goals illustrated in Figure D-1 impact and are affected by the technical, information and/or business architectures.

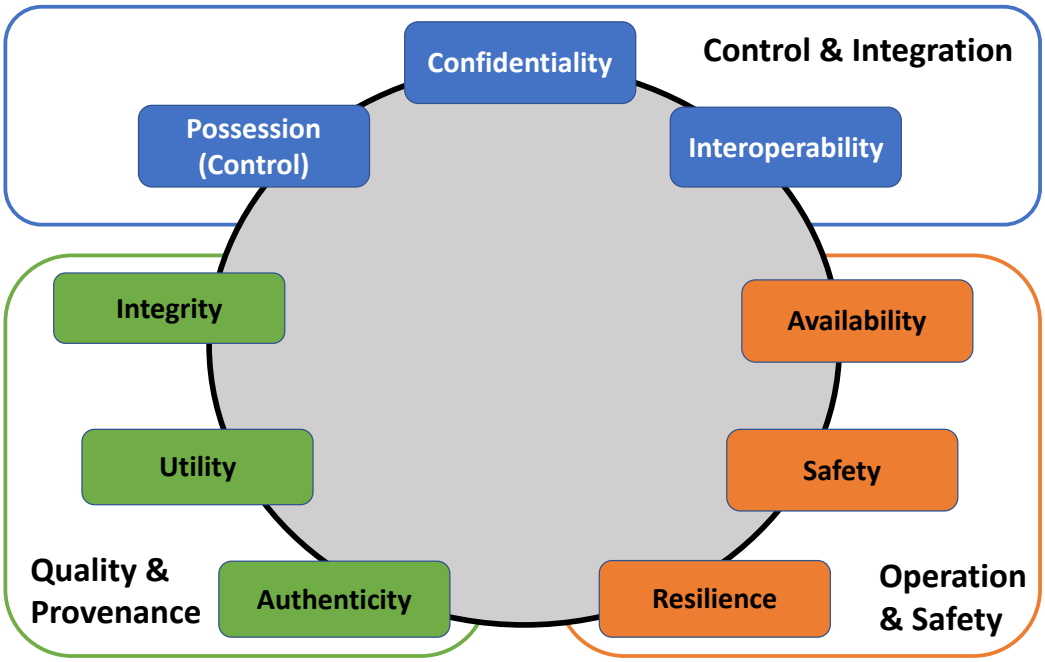

Figure D-1 - Security Goals

When considering security goals, it is necessary to recognise that affected asset(s) may be sensitive or valuable in isolation, or in aggregate, or through their role in delivery of a service. In respect of the security of BACS, multiple assets are potentially involved:

a) Physical assets such as the BACS, the physical entities it controls or manages, and physical items within the space managed by the BACS;

b) Intangible assets, i.e., information that

   a. the BACS collects about the use and performance of the built asset,

   b. it may use regarding the organisational structure and/or location of business units or functions.

It is important to understand the interaction between different assets, whether physical or intangible, and their potential value to the organisation and its stakeholders.

In general, the security goals can be interpreted as follows:

a) Confidentiality, i.e., the control of access, and prevention of unauthorized access to assets. The concept of confidentiality is applicable to privacy, where access is granted

for limited to specific purposes and the extent of any access is proportionate to the reason for which it was granted;

b) Possession, i.e., prevention of unauthorized control, manipulation, or interference with the asset.

c) Interoperability, i.e., the ability of assets (e.g., systems) to operate together in an appropriately integrated fashion, without unwanted situations occurring due to mishandling and/or misunderstanding, of any data and/or information shared between them.

d) Availability, i.e., the assets and any associated processes are consistently/reliably discoverable, accessible, and usable/operable.

e) Safety, i.e., assets and related processes are designed, implemented, operated, and maintained to prevent the creation of harmful states, which might lead to injury or loss of life, unintentional environmental damage, or damage to assets.

f) Resilience, i.e., the ability of assets and any associated processes or services to transform, renew and recover in a timely way in response to adverse events.

g) Integrity, i.e., maintaining the completeness, accuracy, consistency, coherence and configuration of assets and any associated processes.

h) Utility, i.e., assets should remain usable and useful across both their life cycle, and of any associated asset or process.

i) Authenticity, i.e., assets, the state of the assets, and any associated processes, should be verified and certified as genuine.

Governance

To support the achievement of the required security goals, an overall governance regime should be employed to establish appropriate accountability and responsibility. The accountability should rest at a senior level in an organisation, for example, the board or senior management team. Whereas responsibility should lie with those managers or individuals who are charged with delivering the goals. This governance regime should address the actions, behaviour and culture of the organisation, its personnel and relevant supply chains.

The governance regime for BACS should encompass the assets, management of the security domains (physical, people, process, technical and information) and the specification and fulfilment of security goals. Whilst the assets may be physical or intangible, it is important to recognise that there will be intangible assets (e.g., information and/or intellectual property), which may be more sensitive than the physical assets themselves. Understanding the value of such intangible assets is a key part of the information management that supports all security domains.