

5.1.3.6 Hardware security for software process identity credentials.

5.1.4 Passwords

As an organisation, TfL must ensure that for control systems utilising password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.

The project must ensure that any system can support the following minimum baseline requirements:

If an OT system does not have the capabilities to meet all the password requirements, a concession must be raised.

5.1.4.1 The system shall provide a configurable password management facility to allow passwords to be selected according to the requirements in 5.1.4.2.

5.1.4.2 Passwords must meet the following requirements:

- Minimum 13 characters long when set by a human.
- Minimum 13 characters long minimum when set by a system/service.
- The system must support a password of at least 64 characters maximum length.
- All ASCII characters (including space) shall be supported for passwords.
- The password shall not be truncated when processed.
- The chosen password shall be checked with known password dictionaries.
- The system shall allow the number of password attempts before lockout to be set (5.1.2.8 refers).
- The system shall deny the repeated use or recycling of the last five passwords.
- There shall be no complexity requirements for passwords.
- There shall be no password expiration period.
- There shall be no password hints.
- There shall be no knowledge-based authentication (e.g. who was your best friend in high school?).

5.1.4.3 Passwords shall not be stored, electronically or hard copy, in plain text. The exception to this requirement is the sharing of an initial or recovery password with an authorised user, which must be in a separate communication to the user identification.

5.1.4.4 Copies of root, administrator, and system account details, retained for emergency use, must be stored separately from the system and in a secure storage.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.1.4.5 Password generation and lifetime restrictions for human users

5.1.4.6 Password lifetime restrictions for all users



5.1.5 Wireless Access Management

As an organisation, TfL must ensure that the control system provides the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

The project must ensure that any system can support the following minimum baseline requirements:

- 5.1.5.1 The control system shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.
- 5.1.5.2 Wireless networks shall have MAC Address filtering enabled.
- 5.1.5.3 The system shall provide the capability to authorise, monitor and enforce usage restrictions for wireless connectivity to the control system.
- 5.1.5.4 Wireless systems shall employ a key management system.
- 5.1.5.5 Wireless encryption requirements are contained Section 5.5.5 (Encryption).
- 5.1.5.6 Wireless devices shall be protected with security controls, such as access control and encryption, to protect the devices from unauthorised access, modification, or use.
- 5.1.5.7 Where Public Key Infrastructure (PKI) is utilised, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.

Requirements 5.1.5.8, 5.1.5.9, 5.1.5.10 and 5.1.5.11 are only applicable to systems that provide open public WIFI networks at Stations and on passenger trains or trams.

- 5.1.5.8 The system shall be designed so that open public WIFI networks can be disabled within 15 minutes.
- 5.1.5.9 The system shall be designed so that disabling open public WIFI networks does not affect the operational railway system.
- 5.1.5.10 The project shall document and test a process to disable open public WIFI networks within 15 minutes of being requested.
- 5.1.5.11 The project shall document and test a process to reenable open public WIFI networks

Note: For safety critical and service critical systems the following additional requirements shall apply:

- 5.1.5.10 Hardware security for public key authentication

5.1.6 User Change Management and Access Review

As an organisation, TfL must ensure they are able to track joiners, movers and leavers in order to ensure that each individual user is only granted minimum required access rights for their role, that these rights are reviewed when they change role and revoked on leaving TfL.



It is essential that access to any OT system which supports the delivery of TfL services is authorised by the system owner or a delegated deputy (Section 5.1.1.1 refers).

System owners should conduct a regular review of user access rights for the system(s) they are responsible for and ensure those which are no longer required are revoked (Sections 5.1.1.3 and 5.1.1.4 refer).

Projects must provide the capabilities within the systems they are delivering to support these user change management and access review activities through the following minimum baseline requirements:

- 5.1.6.1 The system shall provide the capability to uniquely identify and authenticate all human users.
- 5.1.6.2 The system shall provide the capability to uniquely identify and authenticate all non-human users.
- 5.1.6.3 This identification and authentication shall be enforced on all interfaces which provide access to the control system to support the verification of the principle of least privilege.
- 5.1.6.4 The system shall provide the capability to support the management of all accounts by authorised users, including adding, activating, modifying, disabling, and removing accounts.
- 5.1.6.5 The system shall provide the capability to support the management of identifiers by user, group, role, or control system interface.
- 5.1.6.6 The system shall provide the capability to:
 - change all default authenticators upon control system installation.
 - change/refresh all authenticators; and
 - protect all authenticators from unauthorised disclosure and modification when stored and transmitted.

5.1.7 Monitor Access

As an organisation, TfL must provide the capability to log and monitor all user access to any OT system, which will form an integral element of system monitoring.

The project must ensure that any system can support the following minimum baseline requirements:

- 5.1.7.1 The system shall provide the capability to obscure feedback on authentication information during the authentication process. (For example, responding to a failed login attempt with a “login failed” message rather than “your password was incorrect” which shows an attacker they have used a valid user ID).
- 5.1.7.2 The system shall provide the capability to enforce a configurable number, currently three (Section 5.1.2.8 refers), of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period, which is recommended to be set at thirty minutes.



- 5.1.7.3 The system shall provide the capability to deny access for three hours or until unlocked by an administrator when the consecutive invalid access attempts limit has been exceeded (Section 5.1.2.8 refers).
- 5.1.7.4 The system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorised personnel.
- 5.1.7.5 The system shall provide the capability to enforce authorisations assigned to all users (humans, software processes and devices) for controlling use of the system to support Segregation of duties and least privilege.
- 5.1.7.6 The system shall provide the capability for an authorised user or role to define and modify the mapping of permissions to roles for all human users, software processes and devices.
- 5.1.7.7 The system shall provide the capability to automatically enforce configurable usage restrictions that include:
- preventing the use of portable and mobile devices
 - restricting code and data transfer to/from authorised portable and mobile devices.
- 5.1.7.8 The system shall provide the capability to log, including but not limited to:
- Failed log in attempts
 - Automatic account reset
 - Administrative account reset
 - Successful logins out of normal working patterns
 - Password changes
 - Permission changes
 - Failed attempts to connect unauthorised portable and mobile devices
 - Connection of authorised portable and mobile devices.
- 5.1.7.9 The system shall provide the capability to forward user logging securely to a central log collector (Section 6 refers).

5.2 Data Security

TfL must protect data which is stored or transmitted electronically from actions such as unauthorised access, modification or deletion that may cause an adverse impact on essential functions.

This protection must be underpinned by a good understanding of the data that is important to the delivery of the TfL services, where it is stored, where it travels, and how unavailability or unauthorised access, modification or deletion would impact the service. This also applies to any third parties storing or accessing data important to the delivery of TfL services.

5.2.1 Identify and Understand Critical Data (Information and Documents)

As an organisation, TfL must ensure that for each OT system, there is a record of the location, type, quantity, and quality of data important to the delivery of TfL services. In addition, this record must include the context, limitations and dependencies of the data that is critical to TfL services.

Much of the information about the OT system may be stored electronically or in hardcopy outside the system and is not protected by OT authorisation controls. Unauthorised access and use of this information are a threat to OT security and this information needs to be appropriately controlled and managed.

The project must provide the following minimum baseline requirements:

- 5.2.1.1 A document management process shall be developed and maintained for OT information which supports the system.
- 5.2.1.2 Information classification levels, commensurate with [S1782](#) Information Security Classification, shall be defined for access and control, including sharing, copying, transmitting, and distributing of OT information.
- 5.2.1.3 All logical assets within the scope of the project (including, but not limited to, system design information, vulnerability assessments and network diagrams) shall be classified to indicate the protection required commensurate with the consequence of compromise. ([S1782](#) – Information Security Classification refers).
- 5.2.1.4 Policies and procedures, commensurate with [S1782](#) Information Security Classification, should be developed for retention, physical and integrity protection, destruction, and disposal of all assets based on their classification, including written and electronic records, equipment and other media containing information, with consideration for legal or regulatory requirements.
- 5.2.1.5 Measures shall be employed to ensure long-term records can be retrieved. This could include converting the data to a newer format or retaining older equipment that can read the data.
- 5.2.1.6 Information that requires special control or handling shall be reviewed on a periodic, at least annual, basis to validate that special handling is still required.
- 5.2.1.7 Annual reviews of compliance to [S1782](#) Information Security Classification shall be performed.

5.2.2 Understand Data Links

As an organisation, TfL must ensure that for each OT system, there is a documented and up to date understanding of the data links used to transmit data that is critical or important to the delivery of TfL services.

The project must provide the following minimum baseline requirements:

- 5.2.2.1 A documented record of all the data links that transfer data into or out of the system.
- 5.2.2.2 The record must include the context, limitations and dependencies of the data links that are critical to TfL services.
- 5.2.2.3 The record shall support and inform the capability to protect the integrity of transmitted information (Section 5.5.2 refers).



5.2.3 Identify Mobile Devices and Portable Media

As an organisation, TfL must ensure that all mobile devices and media that may hold data important to the delivery of the TfL services and are used to support the OT system must be identified and recorded.

Mobile devices include but is not limited to laptop computers and handheld programmers. Media assets include removable media and devices such as floppy disks, CDs, DVDs, and USB memory sticks, as well as printed reports and documents.

If an adversary gains access to backup media associated with an OT system, it could provide valuable data for launching an attack. Recovering an authentication file from the backups might allow an adversary to run password cracking tools and extract usable passwords. In addition, the backups typically contain machine names, IP addresses, software version numbers, usernames, and other data useful in planning an attack.

The project must provide the following minimum baseline requirements:

- 5.2.3.1 The use of any unauthorised mobile device or portable media on any node that is part of or connected to the OT system shall not be permitted in order to prevent the introduction of malware or the inadvertent loss or theft of data.
- 5.2.3.2 Systems shall only use removable media and mobile devices where absolutely necessary and must undergo business justification and further risk assessment to provide justification for all enabled USB ports, CD/DVD drives and other removable media devices.
- 5.2.3.3 Where the use of a mobile device or portable media is permitted, this must be a dedicated device which is subject to an equivalent level of protective controls to the OT system that it is used to support.
- 5.2.3.4 There shall be a documented process to verify that a mobile device is free from malware before it is connected to the system (Section 5.7.1 refers).
- 5.2.3.5 A documented record of all authorised mobile devices and portable media which are associated with the system must be maintained/created.
- 5.2.3.6 The number of authorised removable media and mobile devices shall be kept to the absolute minimum required for system operation.
- 5.2.3.7 Mobile devices and portable media that will be transported between physically secure locations is to employ data at rest encryption.
- 5.2.3.8 Where the use of removable media is authorised and the system supports it, software can be used to enforce removable media processes.

5.2.4 Manage Data Holdings

As an organisation, TfL must ensure that data holdings relating to OT are managed throughout the life of the system.

The project must provide or ensure the following minimum baseline requirements:

- 5.2.4.1 A documented record of data holdings relating to the system which will include, but not be limited to, design documentation, operational data, system logs and backups.

- 5.2.4.2 The system shall provide the capability to review and then remove or minimise unnecessary copies or unneeded historic data.
- 5.2.4.3 Data retention must be aligned to regulation, system operating requirements and security monitoring requirements. For example, if system logs are ingested into a centralised logging system, they do not need to be retained in perpetuity on the system, but only for local fault finding or recovery purposes, which would require up to a months' worth of data.

5.3 Personnel Security

TfL must closely manage privileged user access to networks and information systems supporting the TfL services.

Personnel security has three related aspects. From an organisational HR perspective, it involves looking at new and current personnel to determine if they will maintain the OT security for the organisation. For new personnel, the personnel security process evaluates them prior to their entry into the organisation making sure they demonstrate behaviours consistent with their future security responsibility. For current personnel, the personnel security process establishes that they continue to demonstrate behaviour consistent with their current security responsibilities.

Personnel security requirements are also driven by concerns about training, approved staff, awareness of the system, awareness of safety and in some instances malicious activity (generally referred to as Insider Threats). For more information on Insider Threats refer to [G1134: Personnel Security – Insider Threat](#).

From a project perspective, the approach is ensuring that the system has the required capabilities to support the minimum baseline controls for personnel security and builds on the baseline identity and access control requirements in Section 5.1.

5.3.1 Privileged User Access

TfL must ensure that individuals who require privileged levels of user access receive additional validation and authentication.

The project must provide the following minimum baseline requirements:

- 5.3.1.1 Privileged access shall be granted, changed, or terminated on the authority of an appropriate senior manager or system owner.
- 5.3.1.2 Privileged access accounts should be dedicated to a specific function and must not be used for general administrative tasks.
- 5.3.1.3 Privileged access accounts must use MFA.
- 5.3.1.4 A non-privileged user must not be able to gain privileged access rights without proper authorisation and such authorisation should only be temporary to support an urgent business need.
- 5.3.1.5 On all interfaces, the system shall provide the capability to enforce authorisations assigned to all users (humans, software processes and devices) for controlling use of the system to support Segregation of duties and least privilege.
- 5.3.1.6 The system shall provide the capability for an authorised user or role to define and modify the mapping of permissions to roles for all human users.



5.3.2 User Management

TfL must ensure that the identities of the individuals, whether employees or partners, with privileged access to networks and information systems to support the TfL services systems are known and managed.

The project must provide the following minimum baseline requirements:

- 5.3.2.1 A record shall be maintained of all privileged access accounts, including details of the individual(s) and devices authorised to use the account, their permissions, and the authorising manager.
- 5.3.2.2 Privileged access accounts shall be suspended or removed immediately when they are no longer needed, for example in the event of a job change.
- 5.3.2.3 The system shall provide the capability to automatically enforce configurable usage restrictions for users that include:
 - preventing the use of portable and mobile devices
 - requiring context specific authorisation; and
 - restricting code and data transfer to/from portable and mobile devices.

Note: For safety critical and service critical systems the following additional requirements shall apply:

- 5.3.2.4 Supervisor override
- 5.3.2.5 Hardware security for public key authentication.

5.3.3 Role Based Access

TfL should ensure that privileged users are granted only specific privileged permissions which are essential to their business role or function.

The project must provide the following minimum baseline requirements:

- 5.3.3.1 Duties should be segregated amongst personnel to maintain appropriate checks and balances, so that no single individual has total control over actions that change the functional operation of the OT.
- 5.3.3.2 Personnel should be assessed for the critical positions controlling and maintaining the OT.

5.3.4 Privileged Access Review

TfL must conduct a regular review and validation of activity by privileged and standard users to identify any unauthorised or unusual activities.

The project must provide the following minimum baseline requirements:

- 5.3.4.1 All established privileged access accounts shall be reviewed monthly to ensure that the accounts only provide the minimum required permissions and remain a valid requirement for operating the system.
- 5.3.4.2 The system shall provide the capability to generate audit records relevant to privileged account security for the following categories:
 - access control



- request errors
- operating system events
- system events
- configuration changes
- potential reconnaissance activity and audit log events.

5.3.4.3 Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.

5.3.4.4 The system shall allocate sufficient audit record storage capacity for log management and system configuration. This shall be to a minimum of one year's worth of records.

5.3.4.5 The system shall provide timestamps for use in audit record generation.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.3.4.6 Supervisor override

5.3.4.7 Hardware security for public key authentication.

5.4 Physical Security

TfL must ensure that physical security arrangements compliment OT cyber security and protect the OT supporting the TfL services from direct attack.

This will create a secure environment for the protection of OT assets.

This section should be read in conjunction with established physical security standards (Listed or linked in Section 13) and in consultation with the physical security team. The intention is to ensure that physical and cyber security arrangements are complementary and considered properly at each stage of design, development and delivery. This section is not intended to replace established physical security standards, but rather to highlight to TfL staff and partners where particular physical security considerations are relevant to OT systems.

Surveillance and security systems, in particular CCTV, access control systems and intruder detection systems shall comply with [S1147](#) Surveillance and Security Systems.

An asset is any physical or logical object owned by, or operated by, TfL having either a perceived or actual value to the organisation for delivery of TfL services. OT assets are those assets that are a part of the OT, either physical or cyber or that can affect the operation of the OT.

IT assets used in support of or as part of OT systems shall comply with [S1747](#) Physical Security of IT Equipment.

Physical security measures ensure that all assets, specifically those related to the OT of an organisation, are protected physically from unauthorised access, loss, damage, misuse, and the like. Environmental security measures ensure that the assets of an organisation are protected against environmental conditions that would make them unusable or damage the information they contain.



Physical and environmental security measures should be designed to complement the cyber security measures taken to protect assets that are part of the OT and coordinated with the physical security of the remainder of the infrastructure.

It is important to include all systems in the scope and not just limit the effort to traditional computer room facilities and equipment rooms. Practical engineering judgment should be used to balance the risks when determining physical security procedures.

Physical segmentation is a key security countermeasure designed to compartmentalise devices into security Zones where identified security practices are employed to achieve the desired target security level.

The physical protection of the cyber components and data associated with the system must be addressed as part of the overall security of a system. Security at many OT facilities is closely tied to site safety. A primary goal is to keep people out of hazardous situations without preventing them from doing their job or carrying out emergency procedures. Physical security controls are any physical measures, either active or passive, that limit physical access to any information assets in the OT environment.

These measures are employed to prevent many types of undesirable effects, including:

- Unauthorised physical access to sensitive locations
- Physical modification, manipulation, theft or other removal, or destruction of existing systems, infrastructure, communications interfaces, personnel, or physical locations
- Unauthorised observation of sensitive informational assets through visual observation, note taking, photographs, or other means
- Prevention of unauthorised introduction of new systems, infrastructure, communications interfaces, or other hardware
- Prevention of unauthorised introduction of devices intentionally designed to cause hardware manipulation, communications eavesdropping, or other harmful impact.

The project must provide the following minimum baseline requirements:

- 5.4.1.1 Security procedures that address the physical security in the protection of assets shall be established for the system
- 5.4.1.2 At least one physical security perimeter shall be established to provide barriers to unauthorised access to protected assets. Critical components and systems must have at least two physical perimeters.
- 5.4.1.3 There must be entry controls at each physical barrier or boundary.
- 5.4.1.4 There shall be an auditable record of access to equipment via a security barrier or boundary.
- 5.4.1.5 All connections under the control of the project shall be adequately protected from tampering or damage.



- 5.4.1.6 Arrangements must be established to protect assets against environmental damage from threats such as fire, water, smoke, dust, radiation, corrosion, and impact.
- 5.4.1.7 Maintenance procedures must be established for all equipment assets, including auxiliary environmental equipment, to ensure proper operation through correct maintenance.
- 5.4.1.8 Procedures shall be established for monitoring and alarming when physical or environmental security is compromised.
- 5.4.1.9 Procedures should be established and audited with respect to the addition, removal, and disposal of all assets.
- 5.4.1.10 Procedures shall be established to ensure the protection of critical components during the interruption of operations, for example, due to fire, water ingress, security breach, interruption, natural or any other type of disaster.

5.5 Network Security

TfL must ensure that the transit of data important or critical to the delivery of TfL services is protected. This includes the transfer of data to third parties.

5.5.1 Data Transfer

The project must ensure that:

- 5.5.1.1 All Conduits for data transfer have been identified according to Section 5.2.2.
- 5.5.1.2 Conduits shall be designed to protect the data they are transferring. Options to protect the data include, but are not limited to:
 - Encryption (See Section 5.5.5)
 - Secure Tunnelling, such as VPNs (See Section 5.5.6)
 - Data Diodes
 - Inbound and outbound boundary (firewall) rules.

5.5.2 Data Protection

TfL must ensure that the system has the capability to protect the integrity of transmitted information.

The project must provide the following minimum baseline requirements:

- 5.5.2.1 The system shall provide the capability to protect the confidentiality of information for which explicit read authorisation is supported, whether at rest or in transit.

The project should pay particular attention to the information confidentiality relating to portable and mobile devices (for example engineering laptops and USB sticks).

- 5.5.2.2 Authentication information, such as passwords, should be considered confidential, and never be sent in a readable format. The exception to this requirement is the sharing of an initial or recovery password with an authorised user, which must be in a separate communication to the user identification.



- 5.5.2.3 The system shall provide the capability to protect the confidentiality of information at rest.
- 5.5.2.4 Communications over untrusted or open networks shall be encrypted (See Section 5.5.5 Encryption for details).
- 5.5.2.5 The system shall provide the capability to protect the confidentiality of remote access sessions traversing an untrusted network.

Note: Encryption is a common mechanism for ensuring information confidentiality.

5.5.3 Single Points of Failure

TfL must ensure that the system has been designed to eliminate single points of failure where possible.

The project must deliver the following minimum baseline requirements:

- 5.5.3.1 As part of the design process, the project must identify single points where, due to failure, there is a significant risk of impact on the delivery of the TfL services.
- 5.5.3.2 Where possible, these single points of failure should be eliminated during the design stages, but if this is not achievable, this should be recorded in the project risk register and incorporated into any response plans for the system.

5.5.4 Resilient Communications

TfL must ensure there are alternative communication paths where there is a significant risk of impact on the delivery of TfL services if a primary communication path is lost or interrupted.

The project must provide the following minimum baseline requirements:

- 5.5.4.1 As part of the design process, the project must identify communication paths where, due to failure, there is a significant risk of impact on the delivery of the TfL services.
- 5.5.4.2 The project should incorporate alternative communication paths to eliminate the risk to service delivery in the primary path is lost or interrupted. If an alternative path cannot be found, this should be recorded in the project risk register and incorporated into any response plans for the system.

5.5.5 Encryption

TfL must ensure that the system has capability to protect the integrity of transmitted information.

This section provides the specific requirements for different methods of encryption, but it should also be noted that depending on the location or design of the system in question, alternative controls could be adopted.

The selected encryption method must provide a commensurate level of protection for the data, both at rest and in transit. This protection must be in line with the impact on TfL services if the data is compromised and will most likely be informed by a risk or impact assessment.

Depending on the type of encryption, the project must adopt the following minimum baseline requirements:



- 5.5.5.1 For Private Key Encryption (Symmetric Key Cipher), a minimum of AES-256 must be used.
- 5.5.5.2 For stream ciphers, RC4 and algorithms derived from that shall not be used. AES may be used in a cryptographic mode that allows streaming provided that the key is changed in accordance with the limitations of the cryptographic mode chosen. Keys for streaming cipher modes of operation must only be used for one stream and shall not be reused.
- 5.5.5.3 The Electronic Codebook (ECB) and Cypher Block Chaining (CBC) block cipher mode of operation must not be used.
- 5.5.5.4 For key exchange, the DH (Diffie-Hellmann) algorithm must be used with a key length of at least 3072-bit (Group 15). Ephemeral Diffie-Hellmann is preferred.
- 5.5.5.5 For Public Key Infrastructure (Asymmetric Key Ciphers) encryption, the RSA algorithm with a key length of at least 3072-bit must be used.
- 5.5.5.6 For Public Key Infrastructure (Asymmetric Key Ciphers) authentication, RSA or DSA algorithms with a key length of at least 3072-bit must be used.

DSA was originally designed for digital signatures and not for general encryption, although it can be used for general encryption purposes. NIST is trying to deprecate DSA in favour of Elliptic-Curve DSA (ECDSA) and Edwards Curve DSA (EdDSA).

Consideration should be given to Elliptic Curve Cryptography (ECC) instead of RSA, such as Elliptic Curve Diffie Hellmann, since for a given approved curve, the key length is roughly halved to get the same strength of encryption.

- 5.5.5.7 For data hashing, SHA-256 must be used as minimum. SHA3 shall also be allowed as well as SHA2, with more than 256 bits (FIPS 202).
- 5.5.5.8 For file integrity checking, SHA-2 must be used as a minimum. SHA3 shall also be allowed as well as SHA2, with more than 256 bits (FIPS 202).
- 5.5.5.9 For 802.11-based infrastructure, WPA2 Enterprise with AES CCMP encryption and EAP-TLS 1.2 must be used as a minimum.
- 5.5.5.10 All encryption keys must be changed from their default value before use.
- 5.5.5.11 All encryption keys must be randomly generated, not human-specified; except for file-level encryption passwords specified by individual users.
- 5.5.5.12 Cryptographically Secure Pseudorandom Number Generators (CSPRNGs) must be used to generate encryption keys and the following CSPRNGs should be used where possible:
- RNGCryptoServiceProvider, CryptGenRandom, FIPSGenRandom or RtlGenRandom (Microsoft Windows XP Service Pack 3 or later only).
 - /dev/random, /dev/urandom or /dev/arandom (preferred) (*nix-based systems).
 - Any other Evaluation Assurance Level (EAL) 4+ accredited CSPRNGs.
 - Any other Federal Information Processing Standard (FIPS) 186-2 compliant CSPRNGs.
- 5.5.5.13 CSPRNGs based on the following functions are deemed insecure and must not be used:

- Rand()
- Math.Random()

5.5.5.14 Symmetric and Private keys must be stored securely at rest using PKCS#11 or PKCS#12.

5.5.5.15 Encryption hardware should be certified to FIPS 140-2 (tamper evident) as a minimum.

5.5.5.16 Encryption hardware should be protected from physical tampering and uncontrolled electronic connections.

Cryptography also introduces key management issues since robust security policies require periodic key changes. This process becomes more difficult as the geographic size of the OT increases, with extensive OT systems being the most severe example. As site visits to change keys can be costly and slow, it is useful to be able to change keys remotely.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.5.5.17 Cryptographic integrity protection.

5.5.6 Virtual Private Networks (VPN)

TfL must ensure that any VPN used to encrypt communications is configured securely.

The project must meet the following minimum baseline requirements:

5.5.6.1 When a VPN is implemented, a solution which uses one of the following protocols must be used:

- Internet Protocol Security (IPsec)
- Transport Layer Security (TLS).

5.5.6.2 For remote access connections, the VPN shall include a logical break point (jump server) at an OT De-Militarised Zone (DMZ) to allow the link to be monitored.

5.5.6.3 The project must ensure that VPN devices used to protect systems are thoroughly tested to verify that the VPN technology is compatible with the application or system and that implementation of the VPN devices does not unacceptably affect network traffic characteristics.

5.5.7 Backups

TfL must ensure that there are backups of the data required to restore systems to normal operational capability (See also Section 7.2).

The project must meet the following minimum baseline requirements:

5.5.7.1 The project must ensure that the system can provide suitable, secured backups of the data (systems, software, licenses, configurations, data, and other relevant information) required to allow the TfL services to operate or to restore the TfL



services to an operational state within agreed recovery objectives (Section 7.1.1 refers).

Note: Automated backups are recommended to ensure that all required files are captured with reduced operator overhead.

- 5.5.7.2 The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the system without affecting normal operations.
- 5.5.7.3 Although not usually required for system recovery, information required for post-incident forensic activity (for example, audit logs) should be specifically included in the backup.
- 5.5.7.4 Where a backup contains confidential information, encryption should be considered where this will not affect any recovery operations, or the backup should be secured in a suitable lockable storage or safe.
- 5.5.7.5 The system shall provide the capability for backups to be extracted and stored securely in a separate location.
- 5.5.7.6 Full-bit images shall be recorded as configuration baselines for operational systems and assets. These images must be stored securely.
- 5.5.7.7 The system shall provide the capability to verify the reliability of backup mechanisms, including the capability to conduct routine tests to ensure the backup process is functioning correctly and that the backups are usable.
- 5.5.7.8 The backups shall be accessible if an extreme event occurs.

5.6 System Security

TfL must ensure that security is designed into the network and information systems that support the delivery of TfL services from the outset.

The project should adopt secure design principles to minimise the attack surface and ensure that the delivery of the TfL services should not be impacted by the exploitation of any single vulnerability.

5.6.1 Secure by Design

TfL must employ appropriate expertise to design secure networks and information systems supporting the TfL services.

The project must meet the following minimum baseline requirements:

- 5.6.1.1 The system shall provide the capability to protect the integrity of transmitted information (Section 5.5 refers).
- 5.6.1.2 Only permitted, verified, and tested software from authorised sources shall be installed.
- 5.6.1.3 The system shall have port security implemented on network devices to prevent the use of unused ports.

- 5.6.1.4 There shall be no unmanaged network devices on the system
- 5.6.1.5 The system shall employ protection mechanisms to prevent, detect, report, and mitigate the effects of malicious code or unauthorised software.
- 5.6.1.6 The system shall provide the capability to update the protection mechanisms.
- 5.6.1.7 The system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT, and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.
- 5.6.1.8 The system shall provide the capability to detect, record, report and protect against unauthorised changes to software and information at rest.
- 5.6.1.9 The system shall validate the syntax and content of any input which is used as an input that directly impacts the action of the system.
- 5.6.1.10 The system shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained because of an attack.
- 5.6.1.11 The system shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the OT unless revealing this information is necessary for the timely troubleshooting of problems.
- 5.6.1.12 The system shall provide the capability to protect the integrity of sessions.
- 5.6.1.13 The system shall reject any usage of invalid session IDs.
- 5.6.1.14 The system shall protect audit information and audit tools (if present) from unauthorised access, modification, and deletion.
- 5.6.1.15 The system shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device) to a configurable number of sessions.
- 5.6.1.16 The system shall provide the capability to employ malicious code protection mechanisms at all entry and exit points.
- 5.6.1.17 The system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model (Section 5.6.5 and supporting guidance refers).
- 5.6.1.18 The system shall provide the capability to operate in a degraded mode during a Denial of Service (DoS) event.
- 5.6.1.19 The system shall provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of information flooding types of DoS events.
- 5.6.1.20 The system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.

Note: For safety critical and service critical systems the following additional requirements shall apply:

- 5.6.1.21 Central management and reporting for malicious code protection.
- 5.6.1.22 Automated mechanisms for security functionality verification.

Printed copies of this document are uncontrolled.
Page 33 of 51



- | | |
|----------|--|
| 5.6.1.23 | Security functionality verification during normal operation. |
| 5.6.1.24 | Automated notification about integrity violations. |
| 5.6.1.25 | Hardware and software inventory. |
| 5.6.1.26 | Discovery tooling. |

5.6.2 Configuration Management / Change Control

TfL must implement configuration management processes to control modifications to hardware, firmware, software, and documentation to ensure that the system is protected against improper modifications prior to, during, and after system implementation.

The project must meet the following minimum baseline requirements:

- 5.6.2.1 The current OT network configuration and device configurations must always be known and documented.
- 5.6.2.2 A formal change management process should be established to ensure that all modifications to an OT network meet, or exceed, the security requirements as defined in the system specifications or low-level design.
- 5.6.2.3 Risk assessment must be performed on all changes to the OT network that could affect security, including configuration changes, the addition of network components, and installation of software.
- 5.6.2.4 There should be restricted access to configuration settings of OT components.

5.6.3 System and Information Integrity

TfL must maintain system and information integrity to ensure that sensitive data has not been modified or deleted in an unauthorised and undetected manner.

The project must meet the following minimum baseline requirements:

- 5.6.3.1 There shall be controls implemented for malware detection, spam and spyware protection and intrusion detection.
- 5.6.3.2 An alert should be raised if these controls are triggered.

5.6.4 Malware Detection

TfL must ensure that malware detection products are deployed as widely as possible.

Malware detection products evaluate files on a computer's storage devices against an inventory of known malware signature files.

Anti-malware software can be deployed on workstations, servers, firewalls, and handheld devices, but may not be appropriate for operational devices.

Anti-malware tools only function effectively when installed, configured, running full-time, and maintained properly against the state of known attack methods and payloads.

The project must meet the following minimum baseline requirements:



- 5.6.4.1 Anti-malware products must be installed on all devices that can support it. This includes, but is not limited to, Windows, Unix, Linux systems, etc. used as consoles, engineering workstations, data historians, HMIs and general-purpose SCADA and backup servers.
- 5.6.4.2 Malware detection shall be implemented with anti-malware protection and / or whitelisting. Whitelisting must:
- Prevent the execution of all unauthorised software.
 - Provide an alert when unauthorised software attempts to run.
 - Report the list of authorised software and versions that are on the OT assets.
- 5.6.4.3 Updates for anti-malware products installed on the OT Network must only be obtained from secure sources (i.e. a dedicated anti-malware distribution server, located within a DMZ outside the OT network (Section 5.6.5 refers)).
- 5.6.4.4 Anti-malware tools shall be the subject of a dedicated compatibility testing routine to ensure their use does not impact system performance.
- 5.6.4.5 Malware protection shall be in place at all physical and logical network entry and exit points (e.g. Which may also need the use of ‘Sheep Dips’).

5.6.5 Network Segmentation

TfL must ensure that the networks and information systems supporting the TfL services are segregated into appropriate security Zones as defined in the Zone and Conduit model (See Section 4.6 of the supporting Guidance document).

Network segmentation and the level of protection it provides will vary greatly depending on the overall network architecture. Logically segmenting networks based on their functionality provides some measure of protection but may still lead to single-points-of-failure if a network device is compromised. Physically segmenting networks provides another level of protection by removing that single-point-of-failure case but will lead to a more complex and costly network design.

The project must meet the following minimum baseline requirements:

- 5.6.5.1 The system design shall group key OT devices into separate Zones with common security levels to manage security risks and to achieve a desired target security level for each Zone.
- 5.6.5.2 The system shall be separated into Zones and each Zone shall have a clearly defined security level.
- 5.6.5.3 There shall be enforced Conduits between Zones.
- 5.6.5.4 There shall be firewalls between Zones of differing security levels.
- 5.6.5.5 There shall be Access Control Lists (ACLs) between Zones of common security levels.
- 5.6.5.6 There shall be a DMZ between the IT and OT Networks.
- 5.6.5.7 There shall be no direct Internet access to or from the OT Network.
- 5.6.5.8 An OT DMZ shall be used for all outbound connectivity.



- 5.6.5.9 There shall be Virtual Local Area Networks (VLANs) to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.
- 5.6.5.10 The design shall ensure there are simple data flows between systems, devices, and interfaces to enable effective monitoring.
- 5.6.5.11 Any connections to external networks or other systems must occur through managed interfaces consisting of appropriate boundary protection devices (for example, proxies, gateways, routers, firewalls, unidirectional gateways, guards and encrypted tunnels) arranged in an effective architecture (for example, firewalls protecting application gateways residing in a DMZ). These connections must be necessary for operational and business purposes and subject to risk assessment.
- 5.6.5.12 High-risk or critical systems shall be subject to a risk assessment to determine if they should be isolated from or employ a barrier device to separate them from other Zones with different security levels or risks i.e. unidirectional gateways.
- 5.6.5.13 The system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate the zoning model. This may require that some servers may need to be duplicated on the control system network to support normal network features, for example Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS) or local Certificate Authorities (CAs).
- 5.6.5.14 Systems shall only be connected to external networks where absolutely necessary and must undergo business justification and further risk assessment to provide justification.

Note: For safety critical and service critical systems the following additional requirements shall apply:

- 5.6.5.15 Independence from non-control system networks.
- 5.6.5.16 Greater logical and physical isolation of critical networks.
- 5.6.5.17 Island mode (physical isolation of critical networks).
- 5.6.5.18 Fail close operation.
- 5.6.5.19 Uni-directional gateways or data diodes.

5.6.6 Zone boundary protection

TfL must ensure that the system shall provide the capability to monitor and control communications at Zone or segmentation boundaries to enforce the compartmentalisation defined in the Zone and Conduits model.

The project must meet the following minimum baseline requirements:

- 5.6.6.1 The system shall provide the capability to monitor and control communications at Zone boundaries.
- 5.6.6.2 The system shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).
- 5.6.6.3 In response to an incident, it may be necessary to break the connections between different network segments. In that event, the services necessary to support essential operations should be designed and maintained in such a way that the devices can continue to operate properly and/or shutdown in an orderly manner.

Printed copies of this document are uncontrolled.
Page 36 of 51



5.6.6.4 System boundary protections at any designated alternate location should provide the same levels of protection as that of the primary site.

5.6.7 General purpose person-to-person communication restrictions

TfL shall ensure that the system shall provide the capability to restrict or prevent general purpose person-to-person messages from being received from users or systems external to the system.

The project must meet the following minimum baseline requirements:

5.6.7.1 The system shall restrict email or other messaging solutions that provide internal computer-to-external computer communications using outbound messages.

These internal-to external communications may be limited to the purpose of sending system alerts or other computer-generated information messages to users or systems external to the system.

5.6.7.2 The system shall utilise preconfigured messages to transmit alert or status information.

5.6.7.3 The system shall not allow users to attach files or other information to these outbound-only messages at the time the messages are created by the system.

Note: For safety critical and service critical systems the following additional mitigations shall apply:

5.6.7.4 Prohibit all general-purpose person-to-person communication.

5.6.8 Security configuration settings

TfL shall ensure that the system has the capability to be configured according to recommended security configurations (See Section 5.6.9).

The project must meet the following minimum baseline requirements:

5.6.8.1 The system shall provide an interface to support the management of network and security configuration settings.

5.6.8.2 The system shall be able to support monitoring and control of changes to the configuration settings.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.6.8.4 Implementation of an automated check process where the current security settings are automatically collected by an agent and compared to approved settings, with changes being alerted.

5.6.9 Secure Configurations

TfL shall ensure that the system has been configured according to recommended network and security configurations, aka system hardening.

If the manufacturer's recommended configurations are different to any configurations required by this standard, the differences must be reviewed and the most restrictive configuration applied, unless this would impact the safe and reliable operation of the system.



The project must meet the following minimum baseline requirements:

- 5.6.9.1 There shall be documentation detailing all applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including revisions and/or patch levels for each of the computer systems associated with the system.
- 5.6.9.2 There shall be a documented list of services required for any computer system running control system applications or required to interface the control system applications. The list must include:
- All ports and services required for normal operation as well as any other ports and services required for emergency operation.
 - Justification as to why each service is necessary for operation.
- 5.6.9.3 All software components that are not required for the operation and maintenance of the control system must be removed prior to FAT. This must include, but is not limited to:
- Games
 - Device drivers for network devices not in use
 - Instant messaging services
 - Servers or clients for unused Internet services
 - Software compilers in all user workstations and servers except for development workstations and servers
 - Software compilers for languages that are not used in the control system
 - Unused networking and communications protocols
 - Unused administrative utilities, diagnostics, network management, and system management functions
 - Backups of files, databases, and programs used only during system development
 - All unused data and configuration files
 - Sample programs and scripts
 - Unused document processing utilities (Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice, etc.).
- 5.6.9.4 Unnecessary credentials shall be removed (preferred option) or disabled.
- 5.6.9.5 Unnecessary communication ports and media drives shall be disabled by logical (software) or physical (disconnection) means or secured with an engineered barrier.
- 5.6.9.6 The system BIOS shall be password protected to prevent unauthorised configuration changes, unless this is not technically possible, which must be recorded in the system risk register.
- 5.6.9.7 There shall be documentation covering components that have been removed and/or disabled, and justification for components that remain enabled.



5.6.10 Remote Access

TfL must ensure that the system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.

The project must meet the following minimum baseline requirements:

- 5.6.10.1 Remote access services shall use secure methods such as VPN and SSH.
- 5.6.10.2 Remote access services must route through an OT DMZ.
- 5.6.10.3 An OT DMZ shall be the preferred means of controlled remote access to OT systems.
- 5.6.10.4 The system shall provide the capability to deny access requests via untrusted networks unless approved by an assigned role.
- 5.6.10.5 Telnet sessions shall not be permitted.
- 5.6.10.6 Dial up and line modems shall not be permitted.
- 5.6.10.7 The system shall provide the capability to terminate a remote session either automatically after a configurable period of inactivity or manually by the user who initiated the session (Section 5.1.2 refers).
- 5.6.10.8 The system shall employ a multifactor authentication scheme with an appropriate level of strength to positively identify a remote interactive user.

5.6.11 Vulnerability Management

TfL must ensure that there is the capability to manage vulnerabilities in the network and information systems to prevent disruption of TfL services.

It would be expected that vulnerability management would be a pan-TfL service, since a vulnerability could affect a component which is used in multiple systems or services and therefore required a coordinated approach across TfL, but individual projects must ensure that systems are designed to comply with the principles of vulnerability management and can be kept secure through life.

The project must meet the following minimum baseline requirements:

- 5.6.11.1 The system must be free of known vulnerabilities on handover to operational service. Where a vulnerability cannot be resolved, suitable alternative controls must be implemented and the vulnerability, with mitigating controls and a long-term resolution plan, recorded in the project risk register.
- 5.6.11.2 The system shall not be handed over with obsolete technology in place.
- 5.6.11.3 There shall be a process to monitor and analyse publicly known vulnerabilities relevant to the system to understand the risk. This will require access to documents covering the system and network configuration, high level design and asset register.
- 5.6.11.4 There shall be a process to ensure that both publicly announced and privately notified vulnerabilities in the system are tracked. Tracked vulnerabilities must be clearly tagged with both the OT system affected and the TfL services which could be impacted if the vulnerability was exploited.



- 5.6.11.5 There shall be a process to ensure that vulnerabilities being tracked can be assessed, prioritised, and mitigated.
- 5.6.11.6 There shall be a process to implement a temporary mitigation solution for a vulnerability which is not exposed outside the system boundary/security Zone of the system.
- 5.6.11.7 There shall be a process to implement a temporary mitigation solution for obsolete and/or unsupported technology while pursuing migration to supported technology.
- 5.6.11.8 Any temporary mitigation, whether for a vulnerability or obsolete technology, must be risk assessed and recorded in the system risk register. The project should consider that the vulnerability or obsolete technology could have a wider impact across TfL than the immediate system in question.
- 5.6.11.9 The system shall be capable of supporting regular tests or assessments undertaken to check for previously unknown vulnerabilities within the constituent components.

Due to the sensitive nature of OT networks and systems, operators need to carefully consider their approach to the testing of live OT, as system operation, availability and safety could be affected. Assurance could be gained without this additional risk by testing against non-operational environments or by testing individual components in a laboratory environment.

- 5.6.11.10 Vulnerabilities shall be rated according to the Common Vulnerability Scoring System (CVSS)

5.6.12 Patch Management

TfL must ensure that there is the capability to deploy patches in the network and information systems to prevent disruption of TfL services.

Patches are additional pieces of code that have been developed to address specific problems or flaws in existing software. They can be part of a general service improvement plan from the manufacturer or can be in response to a specific vulnerability.

It would be expected that patch management would be a pan-TfL service, since a patch could affect a component which is used in multiple systems or services and therefore required a coordinated approach across TfL, but individual projects must ensure that systems are designed to comply with the principles of patch management and can be kept secure through life.

Applying patches to Operating System (OS) components creates another situation where significant care should be exercised in the OT environment.

The project must meet the following minimum baseline requirements:

- 5.6.12.1 Systems are to be handed over into operation with the latest approved and validated software version and patch revision applied.
- 5.6.12.2 There shall be a systematic and documented patch management process which must operate throughout the operating life of the system.



- 5.6.12.3 Patches must be thoroughly tested to determine they do not impact the safe operation of the system and do not introduce unexpected side effects. Regression testing is advised.
- 5.6.12.4 Patches must only be deployed from known secure sources. The preferred source shall be a patch management server within the DMZ which should act as a repository for patches from external sources for planned or scheduled deployment.
- 5.6.12.5 Any patches which cannot be applied must be captured with the system risk register.

5.6.13 Time Synchronisation

TfL must ensure that time is synchronised across all systems and services.

The project must meet the following minimum baseline requirements:

- 5.6.13.1 The system shall synchronise with a dedicated time source through a secure interface.
- 5.6.13.2 The dedicated time source shall be protected from unauthorised modification.

5.7 Secure Management:

TfL must ensure that network and information systems that support the delivery of TfL services can be managed, operated, and maintained securely.

5.7.1 Secure Management

Systems shall be managed, operated, and maintained in a secure manner.

The project must meet the following minimum baseline requirements:

- 5.7.1.1 Dedicated devices shall be used for the maintenance and security management of OT systems.
- 5.7.1.2 Devices which will be used to manage and maintain systems shall be verified as free from unauthorised software and malware before being connected to conduct management or maintenance activities.
- 5.7.1.3 Systems shall only be administered and maintained by authorised privileged users.
- 5.7.1.4 Secure management processes and supporting technical information shall be documented as part of the system development process and handed over with the system into operational service.
- 5.7.1.5 Documents which support the system shall be stored and secured according to the criticality of the system or the impact of the loss of that system on the delivery of TfL services.

6 Detecting cyber security events

The following controls and considerations will contribute to detecting cyber security incidents within TfL's OT and establish the minimum baseline of cyber security measures for all new projects and upgrades to existing systems.

Safety and service critical systems must also be risk assessed and are expected to require additional controls above the minimum baseline, for which suggestions are shown in the notes and guidance.



6.1 Security Monitoring

TfL must ensure that systems have effective cyber security defences and the capability to detect cyber security events which affect, or have the potential to affect, the delivery of TfL services.

6.1.1 Monitoring coverage

TfL must ensure that data sources have been identified to support the timely identification of security events in the system.

The project must have the capability to meet the following minimum baseline requirements:

- 6.1.1.1 Security monitoring data shall be collected from identified data sources (Section 6.1.3 refers) to detect and identify security events in the system.
- 6.1.1.2 The monitoring shall detect the presence of known indicators of compromise on the essential components of the system.
- 6.1.1.3 Monitoring shall be conducted of all privileged activity on the system for suspicious or undesirable activity.
- 6.1.1.4 There shall be monitoring in place on all network gateways and critical devices, where possible.
- 6.1.1.5 There shall be network taps installed at the network choke point boundary between the OT system and any external systems.
- 6.1.1.6 There shall be network taps installed at the network choke point boundary between the OT control system and its subordinate Zones.
- 6.1.1.7 There shall be monitoring in place to collect essential information against critical services or applications (such as key servers).
- 6.1.1.8 There shall be monitoring in place to detect the connection of unauthorised devices to the system.
- 6.1.1.9 There shall be documented reporting mechanisms such that any monitoring alert can allow for a timely response to events.
- 6.1.1.10 There shall be a centralised logging server.
- 6.1.1.11 System logs shall be capable of being read locally and forwarded to the centralised logging server.

6.1.2 Securing Logs

TfL must ensure that logging data be held securely and read access to it should be granted only to accounts with a business need.

The project must meet the following minimum baseline requirements:

- 6.1.2.1 Only authorised personnel can view logging information.
- 6.1.2.2 There shall be no ability to modify or delete logging data within the specified retention period, after which it can be deleted.
- 6.1.2.3 The system shall protect audit information and audit tools (if present) from unauthorised access, modification, and deletion.

Printed copies of this document are uncontrolled.
Page 42 of 51



- 6.1.2.4 The system shall provide the capability for authorised humans and/or tools to access audit logs on a read-only basis.
- 6.1.2.5 The system shall allocate sufficient audit record storage capacity according to commonly recognised recommendations for log management and system configuration.
- 6.1.2.6 The system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.
- 6.1.2.7 The system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure.
- 6.1.2.8 The system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.

It should be noted that either overwriting the oldest audit records or halting audit log generation are possible responses to audit storage capacity being exceeded but imply the loss of potentially essential forensic information.

Note: For safety critical and service critical systems, the following additional requirements shall apply:

- 6.1.2.9 Audit records on write once media.

6.1.3 Generating Alerts and Audit Records

TfL must ensure that data relating to potential security alerts is captured in the monitoring data and that alerts are triggered.

The project must meet the following minimum baseline requirements:

- 6.1.3.1 The system shall generate audit records about events occurring in the system.
- 6.1.3.2 Audit records should be sufficient in detail to monitor the effectiveness and proper operation of the security mechanisms in place on the system.
- 6.1.3.3 The system shall provide the capability to generate audit records relevant to security for the following categories:
 - Access control
 - User activity
 - Request errors
 - Operating system (System, User and Security) events
 - Control system events
 - Use or attempts to use mobile devices
 - Connection of unauthorised devices
 - Backup and restore events
 - Configuration changes
 - Potential reconnaissance activity



- Audit log events
- Anti-malware events
- Boundary device logs
- FTP Logs
- Proxy Logs
- VPN Logs.

6.1.3.4 The system shall provide timestamps for use in audit record generation.

6.1.3.5 Individual audit records shall include:

- Timestamp
- Source (originating device, software process or human user account)
- Category
- Type
- Event ID
- Event result.

6.1.3.6 Alerts shall be resolved to individual assets.

6.1.3.7 Actions shall be attributed to a specific human user.

6.1.3.8 Alerts shall be generated on suspicious activity linked to known indicators of compromise.

6.1.3.9 Security logs shall be reviewed regularly and, if possible, alerts should be reviewed almost continuously, in real time.

6.1.3.10 Security alerts shall be prioritised, investigated and appropriate action taken.

Note: For safety critical and service critical systems, the following additional requirements shall apply:

- 6.1.3.11 Internal time synchronisation.
- 6.1.3.12 Protection of time source integrity.
- 6.1.3.13 Non-repudiation for all users.

6.1.4 Identifying Security Incidents

TfL must ensure that security alerts are contextualised with knowledge of the threat and the systems, to identify those security incidents that require some form of response.

The project must meet the following minimum baseline requirements:

6.1.4.1 Updates for all signature based protective technologies are received at least monthly.

6.1.4.2 The system shall have the capability for updates to be implemented at least monthly.

6.1.4.3 There shall be a recognised source of threat information to support the identification of security issues.



6.1.4.4 Security alerts shall be prioritised, investigated and appropriate action taken.

6.1.5 Monitoring Tools and Skills

TfL must ensure that monitoring staff skills, tools, and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they protect.

The project must meet the following minimum baseline requirements:

6.1.5.1 The system shall meet the requirements for monitoring coverage (Section 6) and incident response (Section 7) are defined, with appropriate tools and techniques identified.

Consideration should be given to aligning these tools and techniques with other systems for a more consistent and coordinated approach.

6.1.5.2 There shall be personnel in place who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and system performance.

This could involve additional personnel to create additional capacity or require existing personnel to be updated on the new system.

6.1.5.3 There shall be defined roles and skills/competence requirements to ensure that monitoring personnel, together with other personnel such as operators, system administrators and third parties, are able to cover all parts of the monitoring and investigation process.

6.1.5.4 There shall be documentation to inform monitoring personnel which TfL services are supported by the assets being monitored so that alerts or investigations can be prioritised appropriately.

6.1.5.5 There shall be documented processes, procedures, and workflows for monitoring personnel to follow for the analysis, investigation and reporting of alerts.

The project may have to update existing process for the new system or create new processes to support the new system.

6.1.6 Incident Reporting

TfL must ensure that the reporting requirements for cyber security incidents are clearly articulated and understood to ensure that the right information is provided to the right people in a timely manner to allow incidents to be resolved effectively.

The project must develop reporting processes and ensure that the system can generate the information required, reporting at the first available opportunity, to meet the following minimum baseline reporting requirements:

6.1.6.1 The theft or unexplained loss of cyber systems or assets, asset data which an attacker could use to improve the chances of a successful attack or circumvent installed security measures.

6.1.6.2 The unauthorised physical or electronic access to cyber systems.

6.1.6.3 The compromise of a Cyber Assurance of Physical Security Systems (CAPSS) verified system protecting a Railway Asset.

- 6.1.6.4 The occurrence of successful or suspected attempted jamming of radio communication systems such as (but not limited to) mobile phones, portable credit/debit card payment systems, radios, Global Positioning System (GPS) radio navigation systems or Global System for Mobile Communications-Railway (GSM-R).
- 6.1.6.5 The unauthorised addition or modification of software or data on cyber systems.
- 6.1.6.6 The unauthorised destruction or disruption of software or data.
- 6.1.6.7 The malware infection of assets or attempted cyber intrusion.
- 6.1.6.8 The unauthorised physical access to secure rooms.
- 6.1.6.9 All incident reports must be made to the TfL Security Operations Centre (SOC) at the earliest opportunity.
- 6.1.6.10 All incident reports relating to NIS systems must be made within 72 hours to the competent authority.

7 Minimising the impact of cyber security incidents

The following controls will contribute to minimising the impact of a cyber security incident on TfL's OT and establish the minimum baseline of cyber security measures for all new projects and upgrades to existing systems.

Safety and service critical systems must also be risk assessed and are expected to require additional controls above the minimum baseline, for which suggestions are shown in the notes.

7.1 Incident response and recovery planning

TfL must be prepared to restore TfL services following disruption as a result of a cyber incident and must ensure that there are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure.

Mitigation activities designed to contain or limit the impact of compromise are also in place.

An incident response plan is the documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against an organisation's information systems. Response should be measured first and foremost against the "service being provided," not just the system that was compromised.

7.1.1 Business Continuity Plan

TfL must ensure that new systems and upgrades are included in the Business Continuity Plan, which will identify procedures for maintaining and/or re-establishing essential business operations while recovering from a significant disruption.

The project must meet the following minimum baseline requirements:

- 7.1.1.1 Recovery objectives shall be determined for the systems involved, based on business needs.



- 7.1.1.2 An assessment shall be conducted to determine the impact to TfL services because of significant disruption or system loss.
- 7.1.1.3 Continuity plans shall be developed and implemented to ensure that business processes can be restored in accordance with recovery objectives.
- 7.1.1.4 The business continuity plan shall be updated with any specific roles and responsibilities for the new system.
- 7.1.1.5 There shall be backup and restore procedures that support the business continuity plan.

7.1.2 Response and Recovery Plan

TfL must ensure that cyber incident response plans are updated with new and updated systems.

The project must meet the following minimum baseline requirements:

- 7.1.2.1 The overall cyber incident response plan that identifies responsible personnel and defines actions to be performed by designated individuals shall be updated.
- 7.1.2.2 The various types of OT incidents should be identified and classified as to potential impact so that a proper response can be formulated for each potential incident.
- 7.1.2.3 The systems and supporting technologies required to restore operations are known, documented and in line with TfL business continuity, disaster recovery and risk management processes.
- 7.1.2.4 The incident response plan shall be communicated to all appropriate organisations.
- 7.1.2.5 The response plan shall be tested during system development, at least during FAT and SAT and shall be capable of being repeated at regular intervals once handed over to operations.
- 7.1.2.6 Develop procedures to support the activities as determined by the cyber elements of an incident response plan or dedicated cyber incident response plan. The procedures must document the actions to be taken in the event of a cyber security incident and those listed in Section 6.1.6.
- 7.1.2.7 Create offline and hardcopies of incident response plans and procedures.

7.1.3 System recovery

TfL must ensure that the system provides the capability to recover and reconstitute to a known secure state after a disruption or failure.

System recovery and reconstitution to a known secure state means that all system parameters (either default or configurable) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are re-established, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded and the system is fully tested and functional.



The project must meet the following minimum baseline requirements:

- 7.1.3.1 The sequence in which systems, networks and supporting technologies are recovered to restore the systems supporting the delivery of TfL services shall be known, documented, and shared when the system is handed over to operations.
- 7.1.3.2 The interdependencies between the systems and the supporting technologies shall be understood, documented, and shared when the system is handed over to operations.
- 7.1.3.3 The system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or enter a documented degraded mode.
- 7.1.3.4 There may be instances where compensating countermeasures such as physical door access control may be affected by loss of base power supply, in which case the emergency power supply should cover those associated systems. If this is not possible, other compensating countermeasures may be needed during such an emergency situation.

7.2 Backups:

TfL must ensure that there are accessible and secured current backups of data and information needed to recover network and information systems which support the TfL services.

7.2.1 Backups

TfL must ensure that there are backups of all systems, software, licenses, configurations, data, and other relevant information required to enable recovery of individual devices or entire networks and systems supporting the delivery of TfL services.

The project must meet the following minimum baseline requirements for backups from Section 5.5.7.

7.3 Incident lessons learned

TfL must ensure that following an incident or exercise, a root cause analysis shall be conducted to identify measures to prevent reoccurrence based upon incident or exercise.

7.3.1 Lessons Learned

TfL must ensure that lessons are learned from any incident or exercise and that documentation and processes are updated to reflect those lessons.

The project must meet the following minimum baseline requirements:



- 7.3.1.1 The details of an identified incident shall be documented to record the incident, the response and the lessons learned to update system documentation and response processes considering the incident or exercise.
- 7.3.1.2 Exercise scenarios should be developed and tested to ensure that different aspects of the response plan can be tested on a periodic, at least annual, basis. Lessons learnt from exercise tests shall be remediated prior to handover into operation.

8 Supporting Information

8.1 Background

Cyber security should be considered as an integral part of any review for any OT and where possible should be integrated into existing safety, environmental, operational or risk considerations. This should reflect that cyber could be a potential cause of a failure and needs to be captured as part of the response or recovery process, rather than a separate consideration.

8.2 Customer Considerations

Whilst cyber security for OT should not be at the forefront of customer considerations, it should form part of the wider safe, secure and reliable message.

9 Guidance

For further advice and guidance in support of this Standard contact the Cyber Security team CyberSecurityGRC@tfl.gov.uk

10 Person accountable for this document

Name	Job title
Paul Richardson	Cyber Security Assurance Manager

11 Definitions

Term	Definition	Source
Operational Technology	A collection of personnel, processes, hardware and software that can affect or influence the safe, secure and reliable operation of a physical process or asset.	Jargon Buster
Conduit	Security groupings for the communications of information into, out of and within the security Zones/networks	Jargon Buster
Internet	This public data network is considered hostile in the context of the ICS.	Jargon Buster
Protection Systems	Protection systems, Safety-Instrumented System and Emergency Shutdown Systems	Jargon Buster
Segregation	Physically or logically separating different Zones	Jargon Buster



Term	Definition	Source
Zone	A grouping of electronic assets that share common cyber security requirements	Jargon Buster

12 Abbreviations

Abbreviation	Meaning
CCTV	Closed Circuit Television
CPNI	Centre for the Protection of National Infrastructure
DMZ	De-Militarised Zone
FAT	Factory Acceptance Testing
HMI	Human Machine Interface
HR	Human Resources
ICS	Industrial Control System
IT	Information Technology
LAN	Local Area Network
OS	Operating System
OT	Operational Technology
PLC	Programmable Logic Controllers
RTU	Remote Terminal Units
SAT	Site Acceptance Testing
SCADA	Supervisory Control and Data Acquisition
SIS	Safety-Instrumented System
SMS	Short Message Service
SOC	Security Operations Centre
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

13 References

Document no.	Title or URL
R1770	Operational Technology Cyber Security - Framework
S1147	Surveillance and Security Systems
S1747	Physical Security of IT Equipment
S1770	Operational Technology Cyber Security - Governance
S1772	Operational Technology Cyber Security – Operations and Maintenance
S1782	Information Security Classification
G1771	Operational Technology Cyber Security – Projects and Upgrades Guidance
G1134	Personnel Security – Insider Threats
N/A	NIS CAF
HSE OG86v2	Cyber Security for Industrial Automation and Control Systems (IACS) Edition 2
IEC 62443-2-1	Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security

Printed copies of this document are uncontrolled.
Page 50 of 51



Document no.	Title or URL
	program
IEC 62443-3-3	Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels
N/A	CPNI Good Practice Guide – Process Control and SCADA Security
NIST SP800-82	Guide to Industrial Control System (ICS) Security
EN50128	Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems
EN50129	Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling
EN50519	Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

14 Document history

Issue no.	Date	Changes	Author
A1	December 2021	New guidance document published in accordance with Change Request CR-15043.	Tim Parker



Standard

S1772 A1

Operational Technology Cyber Security - Operations and Maintenance

Contents

1	Purpose	3
2	Scope	3
2.1	Operational Technology (OT) definition	3
2.2	Examples	4
3	Requirements	5
3.1	Protecting against cyber attack	6
3.2	Detecting Cyber Security events	7
3.3	Minimising the impact of Cyber Security incidents	7
4	OT Lifecycle	7
4.1	Good Practice Principles	8
4.2	OT Project Lifecycle Requirements	9
4.3	The Purdue model and Secure OT Design	12
5	Protecting against cyber attack	12
5.1	Identity and access control	12
5.2	Data Security	19
5.3	Personnel Security	21
5.4	Physical Security	24
5.5	Network Security	26
5.6	System Security	30
5.7	Providing Secure Management	40
6	Detecting Cyber Security events	41
6.1	Security Monitoring	41
7	Minimising the impact of Cyber Security incidents	46
7.1	Incident response and recovery planning	47
7.2	Backups	48
7.3	Incident lessons learned	49
8	Supporting Information	49
8.1	Background	49
8.2	Customer Considerations	49



9	Guidance	49
10	Person accountable for this document	50
11	Definitions	50
12	Abbreviations.....	50
13	References	51
14	Document history	52



1 Purpose

This standard describes the Cyber Security requirements for operating and maintaining in a secure manner all Operational Technology (OT) which is used to support services within Transport for London (TfL).

2 Scope

This standard applies to TfL staff and partners with responsibility for operating and maintaining OT. It applies at all times when operating or maintaining OT.

2.1 Operational Technology (OT) definition

Operational Technology is a collection of personnel, processes, hardware, and software that can affect or influence the safe, secure, and reliable operation of a physical process or asset.

These include, but are not limited to:

- Signalling for rail, road and marine transport, train management, Supervisory Control and Data Acquisition (SCADA), building management and access control, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), intelligent electronic devices, networked electronic sensing and control, and monitoring and diagnostic systems.

In this context, process control systems include basic process control system and Safety-Instrumented System (SIS) functions, whether they are physically separate or integrated.

- Associated information systems such as advanced control, dedicated equipment monitors, graphical interfaces, process historians, and plant information management systems.
- Associated internal, human, network, or machine interfaces used to provide monitoring, control, and safety operations functionality.

As an owner and operator of physical transport assets, TfL has an extensive estate of OT systems and devices across a wide range of its underground and surface operations.

There are OT systems which are clearly OT such as traction power, tunnel ventilation, fire detection, and systems which are clearly Information Technology (IT) such as Human Resources (HR) and email. However, there are systems where the distinction is not as clear, such as CCTV and ticket barriers.

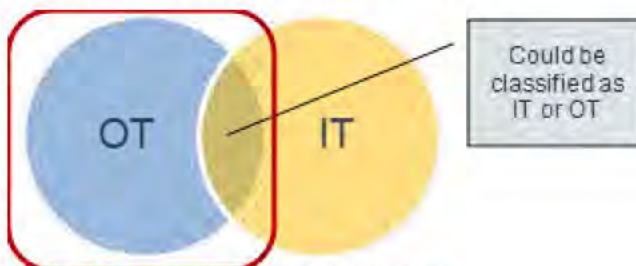


Figure 1 Operational Technology systems scope

2.2 Examples

In this section we provide some examples of systems which may or may not be considered or recognised as OT.

2.2.1 Example OT systems

Examples of OT systems installed in London Underground and Surface Transport that are clearly OT include, but is not limited to:

- Power management systems (traction and general power)
- Energy monitoring
- Signalling systems
- Road traffic signals
- Rolling stock
- Communication networks used by OT (e.g. Surface WAN/Connect/Station LAN)
- Control and information systems
- Track systems
- Station systems (e.g. escalator and elevator control)
- Fire detection and suppression systems
- Civil Systems / Tunnel Systems
- Building management systems and building automation systems
- Heating, ventilation and air conditioning (HVAC) systems
- Security and access control systems (e.g. swipe card or key fob)

2.2.2 Example of systems which can be OT or IT

Some systems may be defined as OT or IT, which is usually dependent on the context. To determine if the system is OT or IT, refer to the definition in section 2.1 above and apply the test of whether the systems “can affect or influence the safe, secure, and reliable operation of a physical process or asset.” If the answer to this is “Yes”, then the system is OT, otherwise it is IT. If the answer is not clear, then refer to the supporting bullet points in the definition to for tests, such as whether the system provides “sensing” or “control”, for example.

Some common edge cases which may be classified as OT or IT are given below:

CCTV and One Person Operation (OPO) CCTV – If the CCTV system (cameras and recorders) are networked then they would come under the definition as “networked electronic sensing” and “monitoring” in the definition above. CCTV which is monitoring an area (e.g. an underground station platform) controlled by other OT (e.g. BMS or signalling) should be classified as OT. CCTV which is not used directly to deliver or support delivering a service (e.g. Head Office CCTV for security monitoring) should be classified as IT.



Lighting controls – Simple manual lighting controls are unlikely to be OT. Automated, remotely controlled or monitored lighting control systems for stations, road and rail tunnels, ferry terminals, are likely to be OT as they can affect the reliable operation of the lighting and of services.

HVAC – Reasonably modern HVAC systems in stations, tunnels and buildings (e.g. Victoria coach station) will have a control system which may be linked into a BMS. They may also have remote access from a facilities management and/or maintenance company.

Ticket barriers – A particular physical access control system which not only has card readers and controllers (OT) but will also link to ticketing systems which will be in the IT network.

Timetabling – Scheduling bus and train services with the timetabling system (IT) may need to interface to other OT systems, such as train management systems. The timetabling system could be considered as OT because it can “affect or influence the safe, secure, and reliable operation” of services.

2.2.3 Alignment to Purdue Model

A complimentary approach to determining if a system should be defined as OT or IT is to refer to the Purdue Model, [G1772](#) Section 4 refers, where OT systems and services sit in Levels 0 to 3 in the Model and IT systems and services sit in Levels 4 and 5 of the Model.

3 Requirements

This standard states the mandatory requirements for OT Cyber Security during operations and maintenance and is aligned to the Network and Information Systems (NIS) Regulations (2018) and the International Electrotechnical Commission IEC 62443 series of standards for OT Cyber Security, in particular IEC 62443-3-3 system security requirements and security levels. It forms part of a wider framework of standards and guidance ([R1770](#)) for Operational Technology Cyber Security in TfL. The standard should be read in tandem with the associated guidance ([G1772](#)).

Each system will have been subject to a risk assessment during development to determine the cyber risk and to identify any additional controls required above that of the established minimum-security baseline or concessions which might be necessary where the minimum baseline cannot be met. This risk assessment and associated risk register will form part of the handover document set before the system is taken into live service, however the risk assessment will have to be revisited regularly throughout the operational life of the system.

Notwithstanding this, the minimum Cyber Security baseline established within this standard is the set of minimum Cyber Security requirements for ALL new or upgraded OT which support TfL services. It should also be considered as best practise for protecting legacy or established services during operations and maintenance activities, whilst recognising that these systems may not have been designed to incorporate Cyber Security controls and therefore alternative mitigation measures may have to be adopted.



The baseline is intended to prevent the unauthorised disclosure of information to an entity actively searching for it using simple means with low resources, generic skills, and low motivation. These requirements are applicable to all OT assets including, but not limited to, Intelligent End Devices, Remote Terminal Units, Microcontrollers, Programmable Logic Controllers, Sensors, Actuators, Servers, Workstations, and Network Devices.

Concessions or non-compliance to the requirements established within this standard must have appropriate mitigating controls implemented and follow the formal engineering concession process. Any risks arising from the concession must have been registered in the project risk register, which is then transferred to the system owner and maintained as the system risk register.

The standard is intended to direct staff and partners working for TfL to understand and adopt the necessary steps to protect against cyber threats, detect a cyber incident and respond to a cyber incident when operating and maintaining OT which supports the delivery of TfL services safely and reliably.

Not all elements of the standard are solely the responsibility of the staff and partners responsible for the respective OT system; in some areas, TfL will have to have organisational processes or shared services, such as monitoring, in place to support these requirements and the OT systems will have to have the capabilities to apply the requirements.

For example, if an individual moves role, there needs to be recognition at an organisational level that their access privileges must be reviewed, but the system must have appropriate mechanisms to ensure access controls can be enforced and updated.

It is important to note that this standard closely mirrors Operational Technology Cyber Security – Projects and Upgrades ([S1771](#)) and the two documents have been written in parallel, since the Cyber Security requirements are carried forward from design into operation.

The key difference is that for Operations and Maintenance the emphasis is on **operating** and **supporting** the OT securely and according to established process to limit the likelihood and impact of a cyber incident, so the broader guidance remains to give context and build understanding of why the security controls are important. For Projects and Upgrades, the emphasis is more focused on **designing** and **implementing** the OT in a secure way, such that the cyber risk is mitigated as far as practicable and that the controls are appropriate to the risk.

Cyber Security considerations or controls are grouped according to the following security principles and the components are explained in the following sections.

3.1 Protecting against cyber attack

The requirement is that TfL will have proportionate security measures in place to protect TfL services and systems from cyber-attack.



The underlying principle is that TfL defines, implements, communicates, and enforces appropriate policies, standards, processes and procedures that direct its overall approach to securing systems and data that support delivery of TfL services.

3.2 Detecting Cyber Security events

The requirement is that TfL will have the capabilities to ensure security defences remain effective and to detect Cyber Security events affecting, or with the potential to affect, TfL services.

The underlying principle is that TfL monitors the security status of the networks and systems supporting the delivery of TfL services to detect potential security problems and to track the ongoing effectiveness of protective security measures.

3.3 Minimising the impact of Cyber Security incidents

The requirement is that TfL will have the capabilities to minimise the impact of a Cyber Security incident on TfL services, including the restoration of those services where necessary.

The underlying principle is that TfL has well-defined and tested Cyber Security incident management processes in place, that aim to ensure continuity of essential services in the event of an incident affecting systems or services.

4 OT Lifecycle

All OT projects and operational systems must undertake Cyber Security activities and implement Cyber Security controls throughout both the project lifecycle as well as the operational lifecycle. For the purposes of this standard, the focus is on operating and maintaining OT systems securely during the operations phase, but the overall lifecycle is shown in Figure 1 to highlight that the operations phase is part of a much wider development process.

As such, lifecycle phases for which projects are responsible are summarised in this standard and only the Operations phase retained in full. For a full description of the OT Lifecycle, refer to [S1771](#) Operational Technology Cyber Security – Projects and Upgrades, Section 4.

For staff and partners who are responsible for operating OT systems, they should understand that the project will deliver an OT system which is secure by design and capable of being operated in a “cyber-secure” manner and there will be end-of-life activities necessary to dispose of the system securely.

Figure 1 below details the OT Lifecycle.

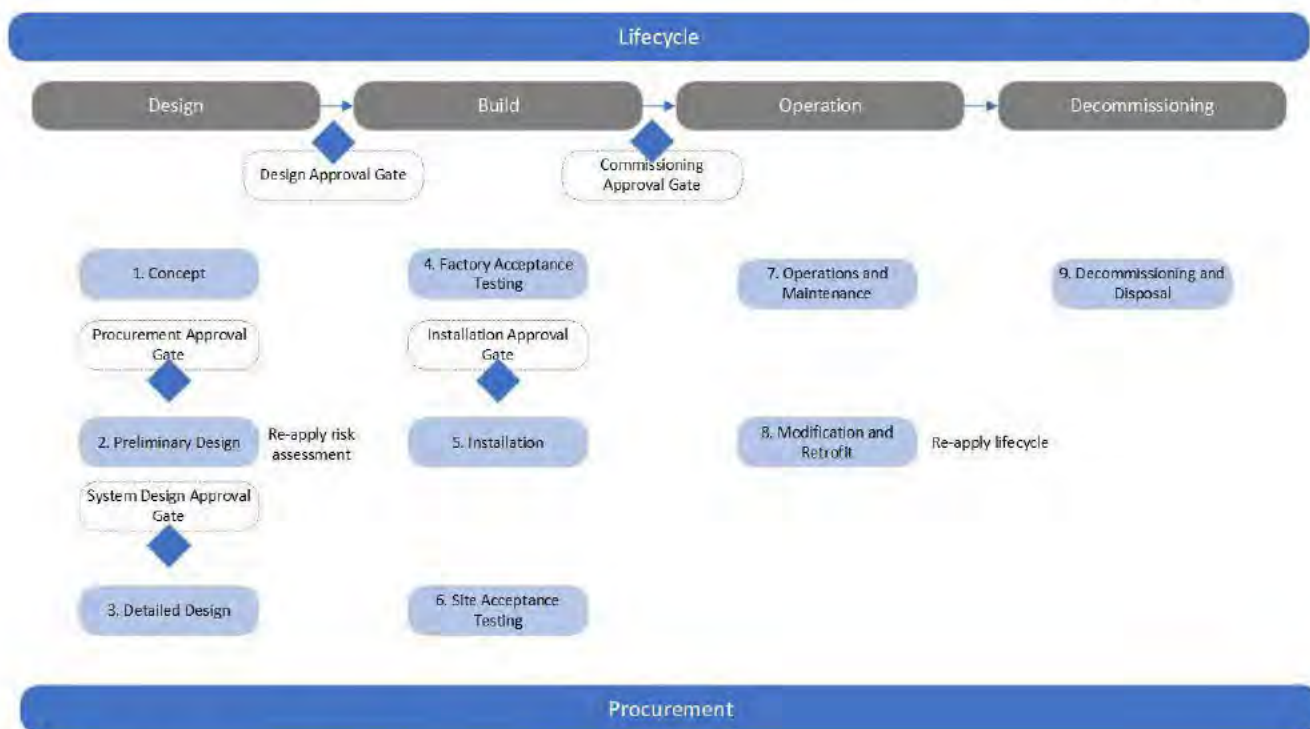


Figure 1 - OT Lifecycle

Implementing security protection measures into OT can be more difficult and costly once systems have been built and deployed. Even more important is that bolting on security measures to either in-service OT, or late in the development cycle of that OT, is often less effective than building them in at the beginning. Dealing with security risks by integrating protection measures into the OT early in its lifecycle is more effective, avoids overruns, is usually less costly and can often be a business enabler.

4.1 Good Practice Principles

To effectively manage the OT lifecycle within the organisation there are five good practice principles which bridge the gap between the lifecycle and Cyber Security frameworks and bring manageable actions to supporting the lifecycle.

The good practice principles are to:

- Ensure regulatory and security requirements are included in procurement and penalties are flowed down
- Ensure OT systems are secure by design
- Manage security through OT system construction
- Manage operational security
- Managing security risks during decommissioning and disposal.