TS 00031.1:1.1

Standard

OT10 Threat-Based Cyber Security Controls

Part 1: Controls and Implementation Requirements

Issue date: 29 April 2026

Effective date: 29 April 2026

Disclaimer

This document has been prepared by Transport for NSW (TfNSW) specifically for its own use and is also available for use by NSW public transport agencies for transport assets.

Any third parties considering use of this document should obtain their own independent professional advice about the appropriateness of using this document and the accuracy of its contents. TfNSW disclaims all responsibility and liability arising whether directly or indirectly out of or in connection with the contents or use of this document.

TfNSW makes no warranty or representation in relation to the accuracy, currency or adequacy of this document or that the document is fit for purpose.

The inclusion of any third party material in this document, does not represent an endorsement by TfNSW of any third party product or service.

For queries regarding this document, please email Transport for NSW Prioritisation and Asset Management
At standards@transport.nsw.gov.au or visit www.transport.nsw.gov.au

Document information

Owner:	Professional Head of Telecom & Op Tech Prioritisation and Asset Management Planning, Integration and Passenger
Mode:	Multimodal
Discipline:	Security

Document history

Revision	Effective date	Summary of changes
1.0	24 January 2023	First issue.
1.1	29 April 2026	Minor revision to update the due dates for concessions when crown jewel systems do not meet the compliance to this document

Preface

This standard is a minor revision v1.1 of the first issue, to support concessions compliance.

This document describes threat-based cyber security controls and details implementation requirements that address common tactics and techniques used against OT. These controls are known as the OT10.

Under the *NSW Cyber Security Policy* NSW Government departments and public service agencies are required to implement the ACSC Essential Eight.

According to the Australian Signals Directorate *ACSC Essential Eight maturity model* “the Essential Eight are designed to protect Microsoft Windows-based internet-connected networks. While the Essential Eight may be applied to cloud services and enterprise mobility, or other operating systems, it was not primarily designed for such purposes and alternative mitigation strategies may be more appropriate to mitigate unique cyber threats to these environments”. (Source: Australian Cyber Security Centre, © Commonwealth of Australia 2022)

TfNSW manages a diverse portfolio of OT systems and products many of which fall outside of the stated design intent of the ACSC Essential Eight. In accordance with ACSC guidance TfNSW has developed the OT10 as alternative mitigation strategies that address the unique cyber threats faced by OT environments.

This document is one part in a proposed series on threat-based cyber security controls for operational technology.

The OT10 has been developed with reference to version 11 of the MITRE ATT&CK® industrial control systems matrix.

Mitre Corporation allows the use of its contents under the following terms:

> The MITRE Corporation (MITRE) hereby grants you a non-exclusive, royalty-free license to use ATT&CK® for research, development, and commercial purposes. Any copy you make for such purposes is authorized provided that you reproduce MITRE's copyright designation and this license in any such copy.
>
> "© 2021 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation."

This document includes definitions from IEC. IEC allows the use of these definitions under the following terms:

> The author thanks the International Electrotechnical Commission (IEC) for permission to reproduce Information from its International Standards. All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and

context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy therein.

The terms ‘normative’ and ‘informative’ are used in asset standards to define the application of the appendices to which they apply. A ‘normative’ appendix is an integral part of an asset standard, whereas an ‘informative’ appendix is only for information and guidance. Appendix A and Appendix B are both normative appendices. Appendix C is informative.

Table of contents

1 Scope

This standard sets out the requirements for the implementation of the OT10 to applicable OT systems.

This document covers OT systems including assets and services at functional hierarchy level zero to level three within the operations and control domain of IEC 62264-1.

This document does not cover IT systems including assets or services that are at functional hierarchy level four within the enterprise domain of IEC 62264-1.

2 Application

This document applies to new and altered systems that have been classified during delivery as crown jewels under the *NSW Cyber Security Policy* or otherwise have been directed to apply this document.

This document also applies retrospectively to existing systems that have been classified as crown jewels under the *NSW Cyber Security Policy* or otherwise have been directed to apply this document.

For existing systems, this document applies from the date when a system has been classified as a crown jewel or otherwise directed to apply this document (date of application).

> Note: The implementation of the OT10 on existing systems is not intended to trigger full compliance to the Transport OT cyber security standards, unless the resultant configuration change is assessed as level 1 significant.

This document applies to asset custodians, asset stewards, delivery partners and service providers who are accountable or responsible for OT systems.

It applies to all modes of transport and all asset life cycle stages.

3 Referenced documents

The following documents are cited in the text. For dated references, only the cited edition applies. For undated references, the latest edition of the referenced document applies.

International standards

IEC 62264-1 *Enterprise-control system integration – Part 1: Models and terminology*

IEC 62443-2-1:2010 *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

IEC 62443-2-4:2015 *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*

IEC 62443-3-3:2013 *Industrial communication networks – Network and system security – Part 3–3: System security requirements and security levels*

Transport for NSW standards

TS 00003.1 *Concessions to Transport Standards Part 1 – Concession Process*

TS 04982 *TfNSW Risk Criteria for External Organisations*

Other referenced documents

Australian Signals Directorate, *ACSC Industrial control systems: Remote access protocol*

State of New South Wales *NSW Cyber Security Policy*

4 Terms, definitions and abbreviations

The following terms, definitions and abbreviations apply in this document:

access control protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy (Source: IEC/TS 62443-1-1 ed.1.0, Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

ACSC Australian Cyber Security Centre

asset custodian the TfNSW Division accountable for the end-to-end lifecycle management and performance of assets (including asset condition, risk and reporting) on behalf of the asset owner to achieve agreed customer and community outcomes

asset steward the entity given the responsibility by an asset custodian to oversee part of the lifecycle process for an asset

authentication security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (Source: IEC/TS 62443-1-1 ed.1.0, Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

change management process of controlling and documenting any change in a system to maintain the proper operation of the equipment under control (Source: IEC 62443-2-1, ed.1.0, Copyright © 2010 IEC Geneva, Switzerland. www.iec.ch)

conduit logical grouping of communication assets that protects the security of the channels it contains (Source: IEC/TS 62443-1-1 ed.1.0, Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

CSMS cyber security management system

decryption process of changing cipher text into plaintext using a cryptographic algorithm and key (Source: IEC/TS 62443-1-1 ed.1.0, Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

digital signature origin authentication, data integrity, and signer non-repudiation (Source: IEC/TS 62443-1-1 ed.1.0, Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

domain environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources (Source: IEC/TS 62443-1-1 ed.1.0, Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

encryption cryptographic transformation of plaintext into ciphertext that conceals the data's original meaning to prevent it from being known or used (Source: IEC/TS 62443-1-1 ed.1.0, Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

essential functions function or capability that is required to maintain health, safety, the environment and availability for the equipment under control (Source: IEC 62443-3-3, ed.1.0, Copyright © 2013 IEC Geneva, Switzerland. www.iec.ch)

IACS industrial automation and control systems

incident event that is not part of the expected operation of a system or service that causes or may cause, an interruption to, or a reduction in, the quality of the service provided by the system (Source: IEC 62443-2-1, ed.1.0, Copyright © 2010 IEC Geneva, Switzerland. www.iec.ch)

IT information technology

integration service provider service provider that provides integration activities for an Automation Solution including design, installation, configuration, testing, commissioning, and handover (Source: IEC 62443-2-4, ed.1.0, Copyright © 2015 IEC Geneva, Switzerland. www.iec.ch)

least privilege basic principle that holds that users (humans, software processes or devices) should be assigned the fewest privileges consistent with their assigned duties and functions (Source: IEC 62443-3-3, ed.1.0, Copyright © 2013 IEC Geneva, Switzerland. www.iec.ch)

local area network communications network designed to connect computers and other intelligent devices in a limited geographic area (typically less than 10 km) (Source: IEC/TS 62443-1-1 ed.1.0, Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

maintenance service provider service provider that provides support activities for an Automation Solution after handover (Source: IEC 62443-2-4, ed.1.0, Copyright © 2015 IEC Geneva, Switzerland. www.iec.ch)

multifactor authentication an authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed

using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are. (Source: Natl. Inst. Stand. Technol. Spec. Publ. 800-63-3, (June 2017)))

OT operational technology; technology-based assets and services directly involved in the context of Transport's operations that can affect or influence safety, security, reliability, operational efficiency, service quality, and regulatory compliance

portable media portable devices that contain data storage capabilities that can be used to physically copy data from one piece of equipment and transfer it to another (Source: IEC 62443-2-4, ed.1.0, Copyright © 2015 IEC Geneva, Switzerland. www.iec.ch)

privilege authorization or set of authorizations to perform specific functions, especially in the context of a computer operating system (Source: IEC/TS 62443-1-1 ed.1.0, Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

remote access communication with, or use of, assets or systems within a defined perimeter from any location outside that perimeter (Source: IEC/TS 62443-1-1 ed.1.0, Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

safety instrumented system system used to implement one or more safety-instrumented functions (Source: IEC/TS 62443-1-1 ed.1.0, Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

security zone grouping of logical or physical assets that share common security requirements (Source: IEC/TS 62443-1-1 ed.1.0, Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch)

service provider a party external or internal to an organisation providing a service on behalf of an accountable party either directly or through a supply chain

SIS safety instrumented system

system integrator person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications (Source: IEC 62443-3-3, ed.1.0, Copyright © 2013 IEC Geneva, Switzerland. www.iec.ch)

TAO Technically Assured Organisation

TfNSW Transport for NSW

5 OT10 threat-based controls

TfNSW has developed the OT10 threat-based controls to assist asset stewards to implement effective risk treatments. The OT10 comprise ten controls that have been specifically designed to treat common attack tactics and techniques used against OT is provided in Appendix A. The ATT&CK® mitigations achieved by each OT10 control is provided in Appendix B.

Note: The OT10 is intended to direct cyber security continuous improvement programs to address common threats to OT systems. It does not replace compliance to standards or comprehensive risk management programs. TfNSW intends to revise this document every three years to reflect changes in the threat environment and technological advances in protective and detective controls.

The OT10 controls shown in Table 1 shall be fully implemented unless a concession is first obtained in accordance with TS 00003.1 for alternative risk treatment decisions such as compensating controls or risk acceptance.

Note: The focus of the OT10 is on information and cyber security controls. In this context, physical and personnel security are considered compensating controls.

Table 1 – OT10 controls

No.	Control name	Control description
1	Authentication of human users	Implement multi-factor authentication for human user remote access, access from laptops, and remote privileged access.
2	Authentication of devices	Enforce usage restrictions to prevent the use of unauthorised devices.
3	Authorised applications and portable media	Allow only authorised applications and portable media on laptops, workstations, and servers.
4	Third-party software provenance	Verify the provenance of third-party software.
5	Independent network services	Implement independent network services for essential functions.
6	Authorised network traffic flows	Allow only authorised network traffic flows. Deny inbound emails, social media, and messaging that permit the transfer of executables files.
7	Event and incident management	Centrally monitor, detect, characterise, and report on security anomalies and events.
8	Least functionality	Remove, disable, or restrict unnecessary functions, ports, protocols, certificates, and services.
9	Backup	Centrally automate the backup of component configuration settings.
10	Patch management	Test and install patches or implement compensating controls to address security vulnerabilities.

The OT10 controls are achieved by implementing the management system requirements, security capability requirements, and technical system security capability requirements given in Table 2, Table 3, and Table 4 respectively.

Risk assessments of alternate risk treatment decisions shall analyse and evaluate the common attack techniques shown in Appendix A and OT10 control mitigations shown in Appendix B.

Risk assessments shall use the risk criteria defined in TS 04982 unless a concession is obtained in accordance with TS 00003.1.

For new and altered systems, full implementation of risk treatments shall be achieved prior to handover in the operate and maintain asset life cycle stage.

For existing systems, asset stewards shall complete an initial control assessment against the OT10 and develop a risk treatment plan not later than six months from the date of application of this document.

For existing systems, asset stewards shall fully implement risk treatments not later than three years from the date of application of this document. For existing systems where OT10 controls are not implemented by the specified due dates, a concession shall be obtained no later than January 2027.

6 OT10 management system requirements

To implement the OT10 controls, the asset custodian or asset steward shall develop, implement, and maintain policies, procedures, practices, and the like as part of a CSMS in accordance with Table 2.

The CSMS requirements are specified in IEC 62443-2-1:2010.

Table 2 – Management system requirements

No.	Control name	IEC 62443-2-1: 2010 requirements	Description
1	Authentication of human users	Element: Access control – Account administration policy • 4.3.3.5.1 to 4.3.3.5.6 Element: Access control – Authentication policy • 4.3.3.6.4 to 4.3.3.6.8 Element: Access control – Authorisation policy • 4.3.3.7.3	Account administration, authentication, and authorisation policies includes multi-factor authentication and remote access.
2	Authentication of devices	Element: Access control – Authentication policy • 4.3.3.6.9 Employ authentication for task-to-task communication Element: Physical and environmental security • 4.3.3.3.6 Protect connections	Account authentication policy includes authentication of trusted devices.

No.	Control name	IEC 62443-2-1: 2010 requirements	Description
3	Authorised applications and portable media	Element: System development and maintenance procedures • 4.3.4.3.8 Establish and document antivirus/malware management procedure	Antivirus/malware management procedure includes application control mechanisms.
4	Third-party software provenance	Element: System development and maintenance procedures • 4.3.4.3.7 Establish and document a patch management procedure	Patch management procedure includes verification of supply chain provenance. Refer to IEC TR 62443-2-3 for informative guidance on patch file authenticity.
5	Independent network services	Element: Network segmentation architecture • 4.3.3.4.1 Develop the network segmentation architecture • 4.3.3.4.2 Employ isolation or segmentation on high-risk IACS	Network segmentation architecture specifies independent network services.
6	Authorised network traffic flows	Element: Network segmentation architecture • 4.3.3.4.1 Develop the network segmentation architecture • 4.3.3.4.2 Employ isolation or segmentation on high-risk IACS • 4.3.3.4.3 Block non-essential communications with barrier devices	Network segmentation architecture specifies network security zones, conduits, and authorised traffic flows.
7	Event and incident management	Element: Incident planning and response procedures – all requirements of 4.3.4.5	Incident planning and response plans and procedures.
8	Least functionality	Element: System development and maintenance procedures • 4.3.4.3.1 Define and test security functions and capabilities	Configuration baselines incorporates least functionality principles.
9	Backup	Element: System development and maintenance procedures • 4.3.4.3.9 Establish backup and restoration procedure	Backup and restoration procedure.

No.	Control name	IEC 62443-2-1: 2010 requirements	Description
10	Patch management	Element: System development and maintenance procedures • 4.3.4.3.7 Establish and document a patch management procedure	Patch management procedure includes information gathering, project planning and implementation, monitoring and evaluation, patch testing, and patch deployment and installation.

7 OT10 security capability requirements

To implement the OT10 controls the service provider shall provide evidence of security capabilities and deliverable documentation in accordance with Table 3.

> Note: If the system is in the create/acquire asset life cycle stage, the service provider refers to the integration system provider. If the system is in the operate/maintain asset life cycle stage, the service provider refers to the maintenance service provider.

The security capability requirements are specified in IEC 62443-2-4: 2015.

Unless otherwise specified, the service provider shall meet the base requirements as specified in IEC 62443-2-4: 2015.

Table 3 – Security capability requirements

#	Control name	IEC 62443-2-4: 2015 requirements	Description
1	Authentication of human users	Architecture • SP.03.07 RE(1) SIS • SP.05.05 Remote access • SP.07.01 to SP.07.04 • SP.07.04 RE(1) Account management • SP.09.01 • SP.09.04	Architecture – workstation access control. SIS – workstation communications. Remote access – security tools and software, and data protection. Account management – user and service accounts.
2	Authentication of devices	Assurance • SP.02.02 Architecture • SP.03.05 Wireless • SP.04.02	Assurance – security tools and software. Architecture – least functionality. Wireless – network design.

#	Control name	IEC 62443-2-4: 2015 requirements	Description
3	Authorised applications and portable media	Malware protection • SP.10.02 • SP.10.05 RE(1), RE(2)	Malware protection – mechanisms and portable media.
4	Third-party software provenance	Patch management • SP.11.03	Patch management – delivery.
5	Independent network services	Architecture • SP.03.02 BR, RE(1), RE(2) • SP.03.07 SIS • SP.05.03	Architecture – network design and connectivity, workstation access control. SIS – workstation communications.
6	Authorised network traffic flows	Architecture • SP.03.02 BR, RE(1), RE(2) • SP.03.07 SIS • SP.05.05	Architecture – network design and connectivity, workstation access control. SIS – workstation communications.
7	Event and incident management	Event management • SP.08.01 to SP.08.02	Event management – reporting and logging.
8	Least functionality	Architecture • SP.03.05 Assurance • SP.02.03	Architecture – least functionality. Assurance – hardening guidelines.
9	Backup	Configuration management • SP.06.02 Backup/Restore • SP.12.01 to SP.12.09	Configuration management – inventory register. Backup and restoration – processes, verification, and disaster recovery.
10	Patch management	Architecture • SP.03.01 and SP.03.03 Configuration management • SP.06.02 Patch management • SP.11.01 to SP.11.06	Architecture – vulnerabilities. Configuration management – inventory register. Patch management – processes, qualification, and installation.

8 OT10 technical system security capability requirements

To implement the OT10 controls, the service provider shall provide a technical system that achieves the security capabilities in accordance with Table 4.

The technical system requirements are specified in IEC 62443-3-3: 2013.

Table 4 – Technical system security requirements

No.	Control name	IEC 62443-3-3: 2013 requirements	Description
1	Authentication of human users	SR 1.1 RE 2 Multifactor authentication for untrusted networks SR 1.13 Access via untrusted networks	Technology associated with multi-factor authentication and remote access.
2	Authentication of devices	SR 2.2 Wireless use control SR 2.3 Use control for portable and mobile devices	Technology associated with network access control.
3	Authorised applications and portable media	SR 2.3 Use control for portable and mobile devices SR 3.2 Malicious code protection SR 3.2 RE 2 Central management and reporting for malicious code protection	Technology associated with application control and portable media policy enforcement.
4	Third-party software provenance	N/A – refer to IEC TR 62443–2–3 for informative guidance.	Technology associated with determining third party software authenticity and integrity.
5	Independent network services	SR 5.1 Network segmentation SR 5.1 RE 1 Physical network segmentation SR 5.1 RE 2 Independence from non-control system networks	Technology associated with network segmentation from external domains, and independent network services.
6	Authorised network traffic flows	SR 5.2 Zone boundary protection SR 5.2 RE 1 Deny by default, allow by exception SR 5.3 General purpose person-to-person communication restriction SR 5.4 Application partitioning	Technology associated with network segmentation between security zones and conduits, and authorised traffic flows.
7	Event and incident management	SR 2.8 Auditable events SR 2.8 RE 1 Centrally managed, system-wide audit trail SR 6.1 Audit log accessibility SR 6.2 Continuous monitoring	Technology associated with event and incident management.
8	Least functionality	SR 7.7 Least functionality	Technology associated with the development, operations, and maintenance of standard operating environments.

No.	Control name	IEC 62443-3-3: 2013 requirements	Description
9	Backup	SR 7.3 Control system backup SR 7.3 RE 1 Backup verification SR 7.3 RE 2 Backup automation SR 7.4 Control system recovery and reconstitution SR 7.8 Control system component inventory	Technology associated with inventory, backup, and restoration. Technology associated with permanent test environment.
10	Patch management	N/A – refer to IEC TR 62443–2–3 for informative guidance.	Technology associated with information gathering, project planning and implementation, monitoring and evaluation, patch testing, and patch deployment and installation. Technology associated with permanent test environment.

Appendix A Common attack techniques (normative)

Risk assessments that support alternate risk treatment decisions shall analyse and evaluate the common attack techniques shown in Figure 1 and Table 5, and OT10 control mitigations shown in Appendix B.

For the purpose of this document common attack techniques are those that are known to have been used by malware variants as recorded within the global ATT&CK® industrial control systems matrix.

Figure 1 shows a heatmap of known ATT&CK® tactics and techniques used to attack OT.

> Note: The heatmap does not represent tactics and techniques used against TfNSW or cyber security incidents experienced by TfNSW.

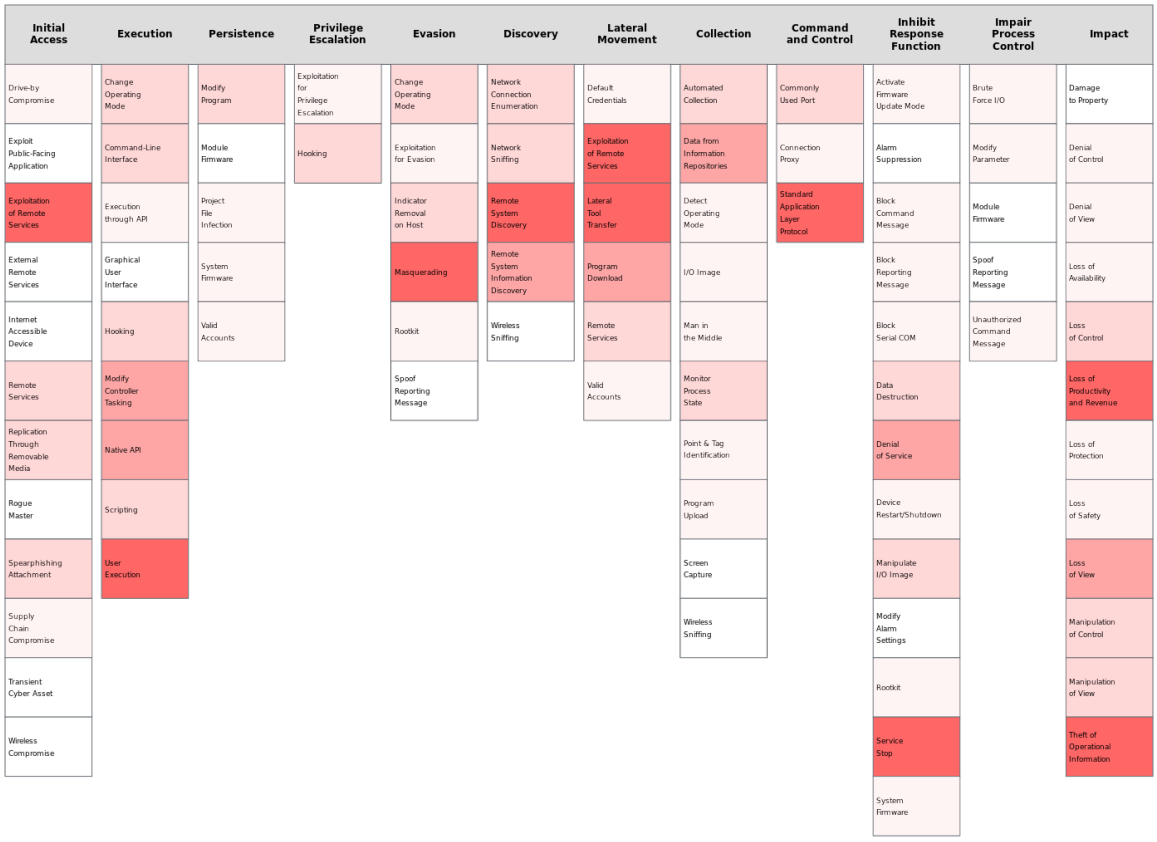

Figure 1 Heatmap of ATT&CK® tactics and techniques used to attack OT

Table 5 shows the number of known occurrences of ATT&CK® tactics and techniques used to attack OT.

Table 5 – Number of occurrences of ATT&CK® tactics and techniques used to attack OT

ATT&CK® tactic	ATT&CK® technique	Number of occurrences
TA0105: Impact	T0828: Loss of Productivity and Revenue	7
TA0108: Initial Access	T0866: Exploitation of Remote Services	4
TA0104: Execution	T0863: User Execution	4
TA0103: Evasion	T0849: Masquerading	4
TA0102: Discovery	T0846: Remote System Discovery	4
TA0109: Lateral Movement	T0866: Exploitation of Remote Services	4
TA0109: Lateral Movement	T0867: Lateral Tool Transfer	4
TA0101: Command and Control	T0869: Standard Application Layer Protocol	4
TA0107: Inhibit Response Function	T0881: Service Stop	4
TA0105: Impact	T0882: Theft of Operational Information	4
TA0104: Execution	T0821: Modify Controller Tasking	3
TA0104: Execution	T0834: Native API	3
TA0102: Discovery	T0888: Remote System Information Discovery	3
TA0109: Lateral Movement	T0843: Program Download	3
TA0100: Collection	T0811: Data from Information Repositories	3
TA0107: Inhibit Response Function	T0814: Denial of Service	3
TA0105: Impact	T0829: Loss of View	3
TA0108: Initial Access	T0886: Remote Services	2
TA0108: Initial Access	T0847: Replication Through Removable Media	2
TA0108: Initial Access	T0865: Spearphishing Attachment	2
TA0104: Execution	T0858: Change Operating Mode	2
TA0104: Execution	T0807: Command-Line Interface	2
TA0104: Execution	T0874: Hooking	2
TA0104: Execution	T0853: Scripting	2
TA0110: Persistence	T0889: Modify Program	2
TA0111: Privilege Escalation	T0874: Hooking	2
TA0103: Evasion	T0858: Change Operating Mode	2
TA0103: Evasion	T0872: Indicator Removal on Host	2
TA0102: Discovery	T0840: Network Connection Enumeration	2
TA0102: Discovery	T0842: Network Sniffing	2

ATT&CK® tactic	ATT&CK® technique	Number of occurrences
TA0109: Lateral Movement	T0886: Remote Services	2
TA0100: Collection	T0802: Automated Collection	2
TA0100: Collection	T0801: Monitor Process State	2
TA0101: Command and Control	T0885: Commonly Used Port	2
TA0107: Inhibit Response Function	T0809: Data Destruction	2
TA0107: Inhibit Response Function	T0835: Manipulate I/O Image	2
TA0105: Impact	T0827: Loss of Control	2
TA0105: Impact	T0831: Manipulation of Control	2
TA0105: Impact	T0832: Manipulation of View	2
TA0108: Initial Access	T0817: Drive-by Compromise	1
TA0108: Initial Access	T0862: Supply Chain Compromise	1
TA0104: Execution	T0871: Execution through API	1
TA0110: Persistence	T0873: Project File Infection	1
TA0110: Persistence	T0857: System Firmware	1
TA0110: Persistence	T0859: Valid Accounts	1
TA0111: Privilege Escalation	T0890: Exploitation for Privilege Escalation	1
TA0103: Evasion	T0820: Exploitation for Evasion	1
TA0103: Evasion	T0851: Rootkit	1
TA0109: Lateral Movement	T0812: Default Credentials	1
TA0109: Lateral Movement	T0859: Valid Accounts	1
TA0100: Collection	T0868: Detect Operating Mode	1
TA0100: Collection	T0877: I/O Image	1
TA0100: Collection	T0830: Man in the Middle	1
TA0100: Collection	T0861: Point & Tag Identification	1
TA0100: Collection	T0845: Program Upload	1
TA0101: Command and Control	T0884: Connection Proxy	1
TA0107: Inhibit Response Function	T0800: Activate Firmware Update Mode	1
TA0107: Inhibit Response Function	T0803: Block Command Message	1
TA0107: Inhibit Response Function	T0804: Block Reporting Message	1

ATT&CK® tactic	ATT&CK® technique	Number of occurrences
TA0107: Inhibit Response Function	T0805: Block Serial COM	1
TA0107: Inhibit Response Function	T0816: Device Restart/Shutdown	1
TA0107: Inhibit Response Function	T0851: Rootkit	1
TA0107: Inhibit Response Function	T0857: System Firmware	1
TA0106: Impair Process Control	T0806: Brute Force I/O	1
TA0106: Impair Process Control	T0836: Modify Parameter	1
TA0106: Impair Process Control	T0855: Unauthorized Command Message	1
TA0105: Impact	T0813: Denial of Control	1
TA0105: Impact	T0815: Denial of View	1
TA0105: Impact	T0826: Loss of Availability	1
TA0105: Impact	T0837: Loss of Protection	1
TA0105: Impact	T0880: Loss of Safety	1

Appendix B OT10 control mitigations (normative)

Risk assessments that support alternate risk treatment decisions shall analyse and evaluate the common attack techniques provided in Appendix A and OT10 control mitigations provided in appendix Section B.1 to Section B.10.

B.1 OT10 control 1: authentication of human users

The OT10 control achieves the following ATT&CK® mitigations:

- M0932 Multi-factor Authentication
- M0936 Account Use Policies
- M0926 Privileged Account Management.

B.2 OT10 control 2: authentication of devices

The OT10 control achieves the following ATT&CK® mitigations:

- M0934 Limit Hardware Installation
- M0813 Software Process and Device Authentication.

B.3 OT10 control 3: authorised applications and portable media

The OT10 control achieves the following ATT&CK® mitigations:

- M0938 Execution Prevention
- M0945 Code Signing
- M0949 Antivirus/Antimalware
- M0934 Limit Hardware Installation
- M0928 Operating System Configuration.

B.4 OT10 control 4: third-party software provenance

The OT10 control achieves the following ATT&CK® mitigations:

- M0817 Supply Chain Management
- M0945 Code Signing.

B.5 OT10 control 5: independent network services

The OT10 control achieves the following ATT&CK® mitigations:

- M0930 Network Segmentation
- M0935 Limit Access to Resource Over Network.

B.6 OT10 control 6: authorised network traffic flows

The OT10 control achieves the following ATT&CK® mitigations:

- M0802 Communication Authenticity
- M0937 Filter Network Traffic
- M0807 Network Allowlists
- M0931 Network Intrusion Prevention.

B.7 OT10 control 7: event and incident management

MITRE ATT&CK does not show event and incident monitoring as a discrete mitigation; instead individual mitigations have preventative and detective controls.

B.8 OT10 control 8: least functionality

The OT10 control achieves the following ATT&CK® mitigations:

- M0942 Disable or Remove Feature or Program
- M0928 Operating System Configuration
- M0922 Restrict File and Directory Permissions
- M0924 Restrict Registry Permissions
- M0954 Software Configuration
- M0814 Static Network Configuration.

B.9 OT10 control 9: backup

The OT10 control achieves M0953 Data Backup ATT&CK® mitigation.

B.10 OT10 control 10: patch management

The OT10 control achieves the following ATT&CK® mitigations:

- M0951 Update Software
- M0916 Vulnerability Scanning.

Appendix C Control implementation guidance

C.1 OT10 control 1: authentication of human users

Depending on the criticality of the system the remote access procedure should align to the *ACSC Industrial control systems remote access protocol.* This protocol describes an invitational model where remote access is normally unavailable and prior approval is necessary to establish a connection.

In the context of remote access, SP.03.07 RE(1) requires a multi-factor authentication service is provided and is used for human user access from uncontrolled spaces such a remote or field locations.

In the context of remote access, SP.09.01 requires the use of a central authentication service or database that meets the following conditions:

- part of the control system, rather than an enterprise shared service
- allows central management and configuration of remote access accounts, as opposed to multiple remote access solutions using local authentication.

C.2 OT10 control 2: authentication of devices

OT data communications equipment should implement pre-connect network access control to authenticate trusted devices and prevent untrusted devices from accessing OT networks and services.

Wired and wireless local area network equipment should implement network access control on all network access interfaces, except those used by equipment that performs essential functions.

Network access control should use industry standard extensible authentication protocols that supports certificate-based and mutual authentication.

As an alternative to pre-connect network access control, post-connect network access control methods may be used to detect, quarantine, and enforce access policies on connected devices.

In cases where the implementation of network access control is not reasonably practicable, security analysis tools should be used to detect unauthorised connected devices. The effectiveness of this method is dependent on the event and incident management capability.

C.3 OT10 control 3: authorised applications and portable media

Individual applications should be explicitly approved.

> Note: A ‘blanket’ approval of all installed applications on a device is not considered to be an effective control.

Once commissioned, application control should prevent the execution of unapproved applications.

> Note: Running application control in ‘audit’ mode or ‘blacklist enforcement’ which blocks execution of blacklisted items only is not considered to be an effective control.

Application control should use a combination of cryptographic hash and either digital signature or publisher whitelisting. If these techniques are not reasonably practicable, then file path whitelisting may be used provided that the listed directory or folder is subject to strict access controls.

> Note: Application control based on file name or file size alone is not considered an effective control.

To support application control, a configuration baseline of required applications, software libraries, scripts, installers, and firmware should be established for servers, workstations and laptops. These should be subject to change management.

The default configuration for all workstations, laptops and servers should prohibit the attachment of portable media.

Where the attachment of portable media is necessary for system functionality, authorised portable media devices should be limited to pre-approved devices.

Where supported, portable media should be uniquely identified, encrypted, and authenticated.

Controls for authorised portable media may consist of a combination of administrative and technical methods such as:

- administrative including documented work instructions and specially marked devices
- technical including scanning and sanitisation, group policy settings, and decryption.

C.4 OT10 control 4: third-party software provenance

The provenance of third-party software is cryptographically verified to establish its authenticity and integrity.

Where the provenance of third party is unable to be adequately verified the software is not used and a cyber security incident raised for further investigation.

The provenance of third-party software should be verified against the manufacturer's supplied digital signature.

Where digitally signed software is not available, the integrity of third-party software should be verified against the manufacturer's supplied cryptographic checksum.

Where supported, devices should be configured with digitally signed firmware and device drivers.

Where supported, devices should automatically verify the checksum or digital signature of firmware prior to load and execution.

C.5 OT10 control 5: independent network services

OT systems should not depend on external network services for the performance of essential functions, such as safety protection, control, visibility, or remote access necessary for critical maintenance or support functions.

Network services that may be considered necessary for essential functions include the following:

- access control
- licence management
- remote login
- file transfer
- domain name translation
- local certificate authority
- host initialisation
- network management of local area networks
- network time dissemination.

In the event of a cyber security incident affecting the enterprise domain or other external domains, OT systems should have the capability to run in island mode.

OT system should implement independent network services to ensure that essential functions continue to operate when connectivity to the external domains is broken or lost.

> Note: Running in island mode may result in the loss or degradation of non-essential functions.

C.6 OT10 control 6: authorised network traffic flows

Devices should be compartmentalised by asset class, function, or type.

> Note: Network segmentation is designed to group devices with the common security requirements into security zones where rules restricting traffic flows between zones can then be implemented. The network segmentation architecture is influenced by several factors including risk, criticality, function, and location.

The criteria to group devices into security zones should be as granular as reasonably practicable.

An example network segmentation architecture may define the following groups:

- operator workstations
- support workstations
- management devices
- wireless devices (if applicable)
- SCADA front-end processors
- SCADA application servers
- historians
- gateway devices
- jump servers
- SIS workstations
- SIS devices.

Networks may be further segmented to individual devices (known as ‘micro-segmentation’) provided this does not introduce an administrative burden.

The network segmentation architecture should allow traffic flows between the enterprise domain and operations and control domain only using a gateway, proxy, bastion host, jump server, or the like located within level three.

The network segmentation architecture should deny traffic flows between levels two or one of the operations and control domain and the enterprise domain.

The network segmentation architecture should allow traffic flows between SIS and levels two or one only.

All traffic flows between security zones and domains should be denied by default and allowed by exception only.

Traffic rules should not allow general purpose person-to-person communication such as email, instant messaging, and telephony between the operations and control domain and the enterprise domain.

Traffic rules should not allow general purpose access to the Internet from within the control system. Traffic rules should allow access to authorised sites necessary for business use cases such as to permit the download of patches from specified vendor sites.

Allowed traffic flow rules should be as specific and complete as reasonably practicable such as addresses, ports, and protocols between communicating hosts or security zones.

Allowed traffic flow rules for transmission control protocol flows should be stateful, defining the source and destination hosts or security zones.

Traffic flow rules within the operations and control domain, and between the operations and control domain and the enterprise domain should be maintained as part of the control system. For example, it should not be allowed to alter the traffic flow rules of the control system from the enterprise domain.

To preserve authenticity, integrity, and confidentiality, safety-related network traffic should be cryptographically secured.

C.7 OT10 control 7: event and incident management

Incident management principles should align to AS ISO/IEC 27035.1.

Plans and preparation for incident response should align to the guidance within AS ISO/IEC 27035.2.

Incident response plans should be tested at least annually.

Procedures for cyber security incident reporting to government bodies should meet enterprise obligations, such as to the Australian Cyber Security Centre, Cyber Security NSW, and Office of the Australian Information Commissioner.

Product supplier configuration guides should be considered in conjunction with industry best practices to ensure that event logging does not degrade system performance.

Event filtering, analysis, and reporting mechanisms should be performed on a separate system that is independent of the control system.

Events should be recorded at redundant and geographically diverse central locations as soon as reasonably practicable without degrading system performance.

Note: The central locations need not be the same for all OT systems.

Security information and event management technology should be implemented to correlate individual events from sub-systems.

C.8 OT10 control 8: least functionality

Standard operating environments should represent the least privilege baseline configuration necessary to meet operational safety, efficiency, and reliability objectives.

Standard operating environments should not be shared between enterprise and operational domains.

Standard operating environments should be specific to the asset class, function, or type.

Service provider and product supplier hardening guidelines should be followed.

C.9 OT10 control 9: backup

Backups should be stored at redundant and geographically diverse central locations in addition to any on-site backups.

Note: The central locations do not need to be the same for all OT systems.

Backups should be retained for the last four configuration changes for a period of at least six months.

Restoration from backups should be tested at least annually and as part of a configuration change.

Automatic backups should be performed on the following events:

- routinely in accordance with a defined periodic schedule
- immediately before and after a configuration change.

Backups should contain at least the following for each component:

- as-built configuration data
- running configuration data and operating state
- logs and audit events.

C.10 OT10 control 10: patch management

Patch management should comply with IEC TR 62443-2-3:2015.

Where software tools are used to discover assets, they should use passive discovery methods only.

A permanent test environment should be established and maintained to support functional and non-functional testing.

The test environment should consist of hardware, software, applications, and data configured to represent the operational environment so far as is reasonably practicable.

A test management tool should be implemented to manage test process and documentation.

Other software tools for automation, performance, and security testing should be implemented as necessary.

Requirements in Transport standards apply to testing processes and documentation.