10.1. Cable Management Fundamentals

Objective

10.1.1. Cable management systems are designed to support the integration of systems across government facilities, assist maintenance and engineering changes, as well as minimise the opportunity for tampering or unauthorised changes to cable systems.

Context

Scope

10.1.2. This section covers information relating to cable distribution systems used in facilities within New Zealand. When designing cable management systems, Section 10.5 - Cable Labelling and Registration and Section 10.6 - Cable Patching of this chapter also apply.

Applicability of controls within this section

10.1.3. The controls within this section are applicable only to communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside of New Zealand Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual MUST be consulted.

Common implementation scenarios

10.1.4. This section provides common requirements for non-shared facilities. Specific requirements for facilities shared between agencies and facilities shared with non-government entities can be found in subsequent sections of this chapter.

Red/Black Concept and Cable Separation

10.1.5. The **RED/BLACK** concept is the separation of electrical and electronic circuits, devices, equipment cables, connectors, components and systems that transmit store or process national security information from non-national security information. The **RED/BLACK** concept is sometimes described as **RED/BLACK** architecture or **RED/BLACK** engineering.

10.1.6. The **RED/BLACK** concept should not be confused with the generic description HIGH/LOW or HIGH SIDE/LOW SIDE. In this context, HIGH refers to systems **classified** CONFIDENTIAL and above and LOW refers to systems **classified** RESTRICTED and below. While these concepts are similar and often used interchangeably, it is important to recognise that information does not usually change classification. The signal or transmission, however, may transit both **RED** and **BLACK** systems in order to reach its intended destination. It is important to note that systems carrying a particular classification may also carry information at **ALL** lower classifications **BUT NOT** any higher classifications.

10.1.7. An example is the use of radio transmissions or Wi-Fi where the information may hold a HIGH classification and originate in **RED** equipment but once transmission occurs the **signal** is **BLACK** as radio and Wi-Fi signals can be detected by anyone within range.

10.1.8. This also leads to the situation where some equipment may have both **RED** and **BLACK** elements. Examples include Wi-Fi Access Points and encryption devices. **RED** Information in a **BLACK** environment is invariably protected by encryption and a variety of technical countermeasures.

10.1.9. All cables with metal conductors (the signal carrier, the grounding element, the strengthening member or an armoured outer covering) can act as fortuitous signal conductors allowing signals to escape or to cross-contaminate other cables and signals. This provides a path for the exploitation of signals, data and information.

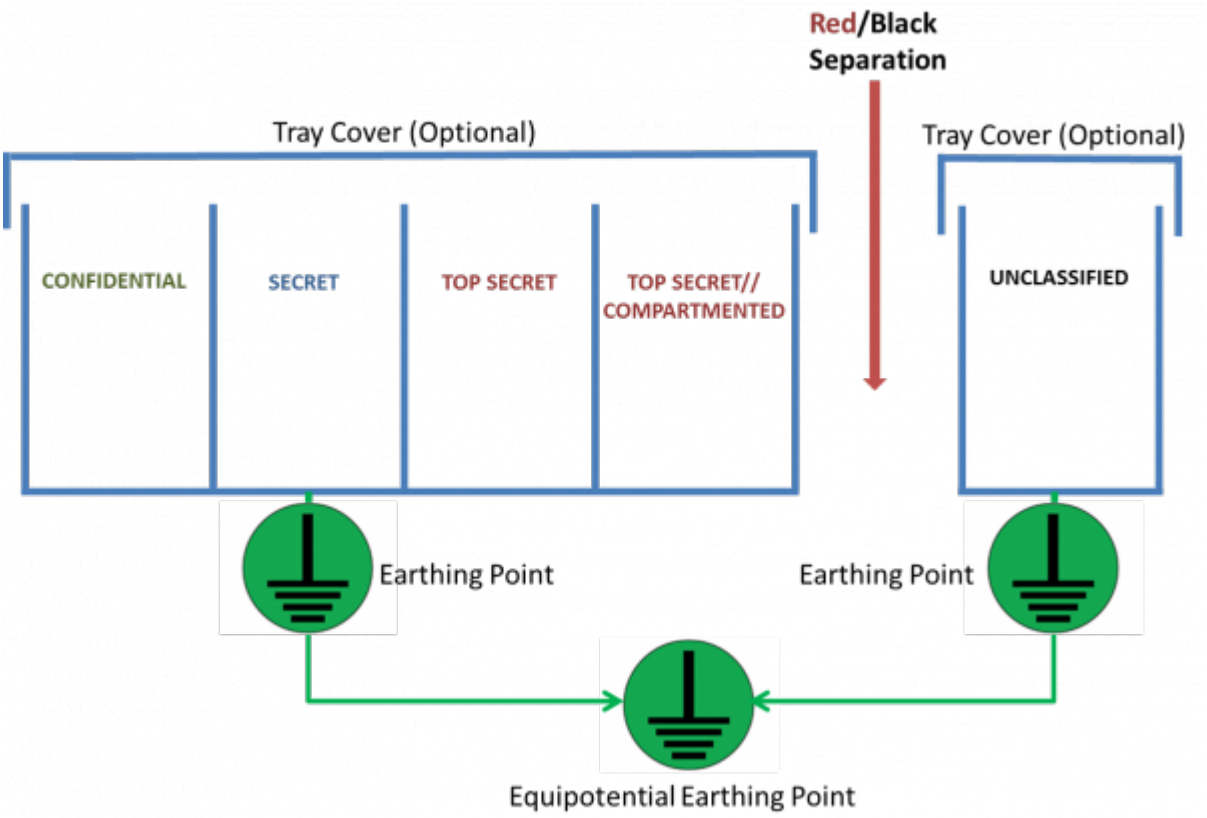
10.1.10. A fundamental control is the separation of cables and related equipment with sufficient distance between them to prevent cross-contamination.

Cable trays

10.1.11. Where copper or a combination of copper and fibre cables are used, cable trays will provide separation, assist cable management and enhance cable protection. While preferable to separate RED cables of different systems for cable management purposes, the most important element is to maintain RED/BLACK separation.

10.1.12. It is preferable that cable trays contain dividers. Some cable trays provide only a single receptacle for cables (no dividers). If dividers are not

available, multi-core fibre cables should be used. Cables of similar classifications should be bundled. A typical cable tray layout with dividers is depicted below:



Catenary

10.1.13. The use of catenary (wire, rope, nylon cord or similar cable support mechanisms) is becoming more widespread in place of cable trays. Care MUST be taken to maintain **RED/BLACK** separation if this method of cable support is used.

Earthing

10.1.14. It is important that any metal trays or metal catenary are earthed for both safety and to avoid creating any fortuitous conductors. All earthing points MUST be equipotentially bonded.

Fibre optic cabling

10.1.15. Fibre optic cabling does not produce, and is not influenced by, electromagnetic emanations; as such it offers the highest degree of protection from electromagnetic emanation effects.

10.1.16. Many more fibres can be run per cable diameter than wired cables thereby reducing cable infrastructure costs. Fibre Optic cable is usually constructed with a glass core, cladding on the core and a further, colour coded coating. Multiple cores can be bundled into a single cable and multiple cables can be bundled into a high capacity cable. This is illustrated in Figures 1 below. Cables also have a central strength member of mylar or some similar high strength, non-conductive material

10.1.17. Fibre cable is considered the best method to future proof against unforeseen threats.

10.1.18. Cable trays for fibre only cable may be of any suitable material. If metal trays are used they MUST be earthed.

Ribbon Fibre Optic Cable

10.1.19. In the context of this discussion, traditional and ribbon fibre optic cables are subject to identical controls, restrictions in installation and use and any operational caveats.

10.1.20. Unlike traditional beam optical cable, ribbon fibre optic cable is arranged into a strip. Because the ribbon contains only coated optical fibres, this type of cable takes up much less space and is generally lighter (weight) than individually buffered optical fibres. As a result, ribbon cables are denser than any other fibre cable design. They are ideal for applications where space is limited, such as in an existing conduit that has very little room left for an additional cable. Ribbon fibre optic cable is a convenient solution for space and weight challenges.

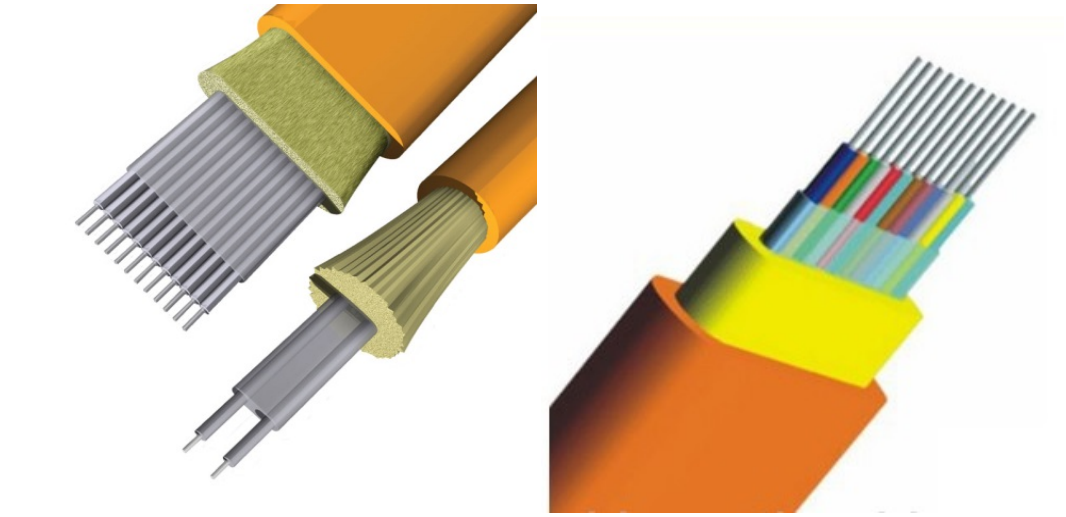


Figure 2: Typical Ribbon Cable

10.1.21. Ribbon cables enable the migration to high fibre count systems required to support high bandwidth applications including 10, 40 and 100Gb/s. Ribbon cables are rarely used in long distance fibre optic trunk cable but are typically used in data centres, campus, commercial buildings and large industrial sites. Fibre counts can range from 2 to over 1700.

10.1.22. The cable ribbons are coated optical fibres placed side by side, encapsulated in Mylar tape, similar to a miniature version of wire ribbons used in computer wiring. A single ribbon many contain 4, 8, 12 or 24 optical fibres with ribbons stacked up to 22 high. At present 12-fiber ribbons are readily accessible and identifiable with ribbon identification numbers, TIA-598 compliant fibre colour coding and are available with non-flame-retardant or formulated flame-retardant outer jacket. They are also available in several configurations including all-dielectric, armoured and aerial self-supporting cables.

10.1.23. Because the cable profile is different to older round cable type, new cable strippers, cleavers, and fusion splicers are required for installation and maintenance.

10.1.24. Fibre optic ribbon cable comes in two basic configurations: loose tube ribbon cable and jacket ribbon. Loose tube cables are where fibre ribbons are stacked on top of one another inside a loose-buffered tube. This arrangement can hold several hundred fibres in close quarters. The buffer, strength members, and cable jacket carry any strain while the fibre ribbons move freely inside the buffer tube.

10.1.25. Jacket ribbon cable is similar to a regular tight-buffered cable, but it is elongated to contain a fibre ribbon. This type of cable typically features a small amount of strength member and a ripcord to tear through the jacket.

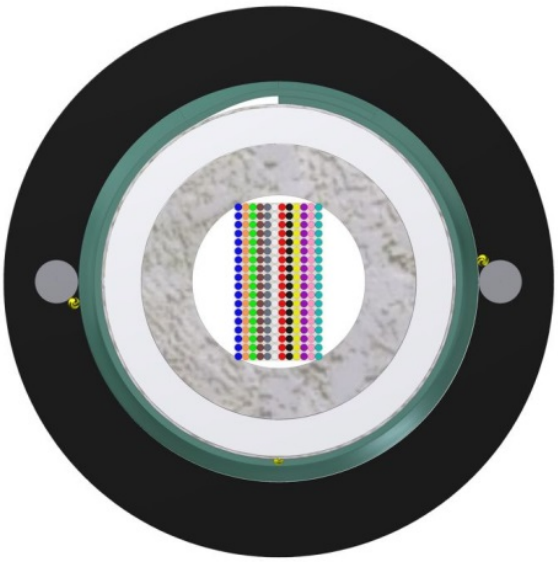


Figure 3: Jacket Cable

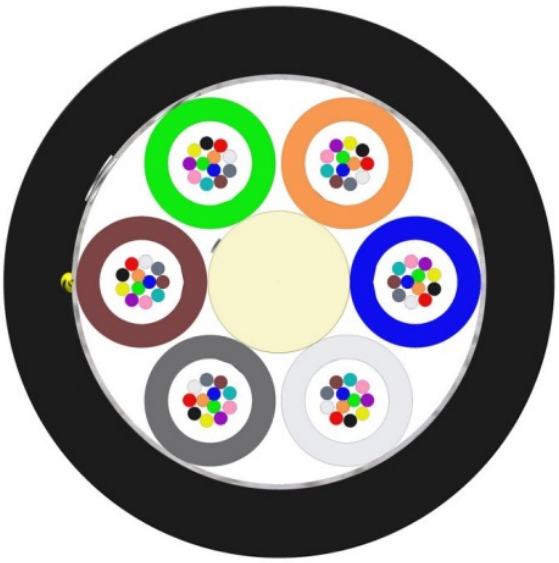


Figure 4: Loose Tube Cable

10.1.26. Infrastructure cables contain multiple fibre ribbon units inside a central tube with dielectric strength members for tensile strength and colour coded

fibres with individual ribbon unit ID numbers for clear identification. Ribbon fibre optic cables are available in configurations supporting high-speed, applications such as Gigabit Ethernet, 10 Gigabit Ethernet, Gigabit ATM and Fibre Channel.

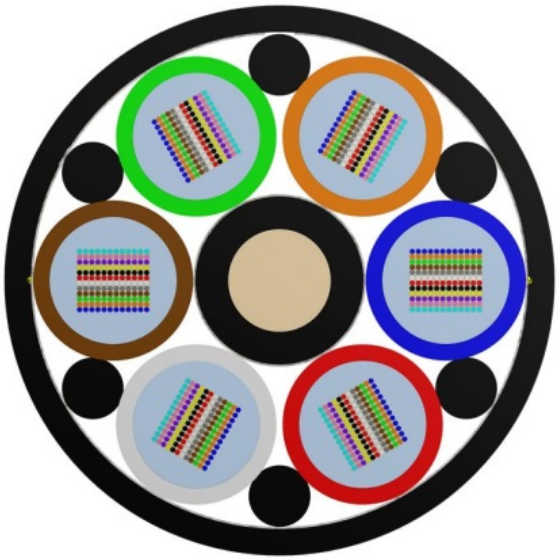


Figure 5: Infrastructure (High Cable Count) Ribbon Cable

Armoured Fibre optic cabling

10.1.27. Some fibre optic cable also includes conductive metal cable strengtheners and conductive metal armoured sheaths which may be wire-wound or stainless steel mesh for external cable protection and steel wire cores as core strength members. This strengthening and armouring is conductive and specialist advice may be needed to avoid earth loops, cross-coupling, inductive coupling or the introduction of other compromising signals and currents. Fibre optic cable with metal cable strengtheners or conductive armoured sheaths is considered *unsuitable* for secure installations.

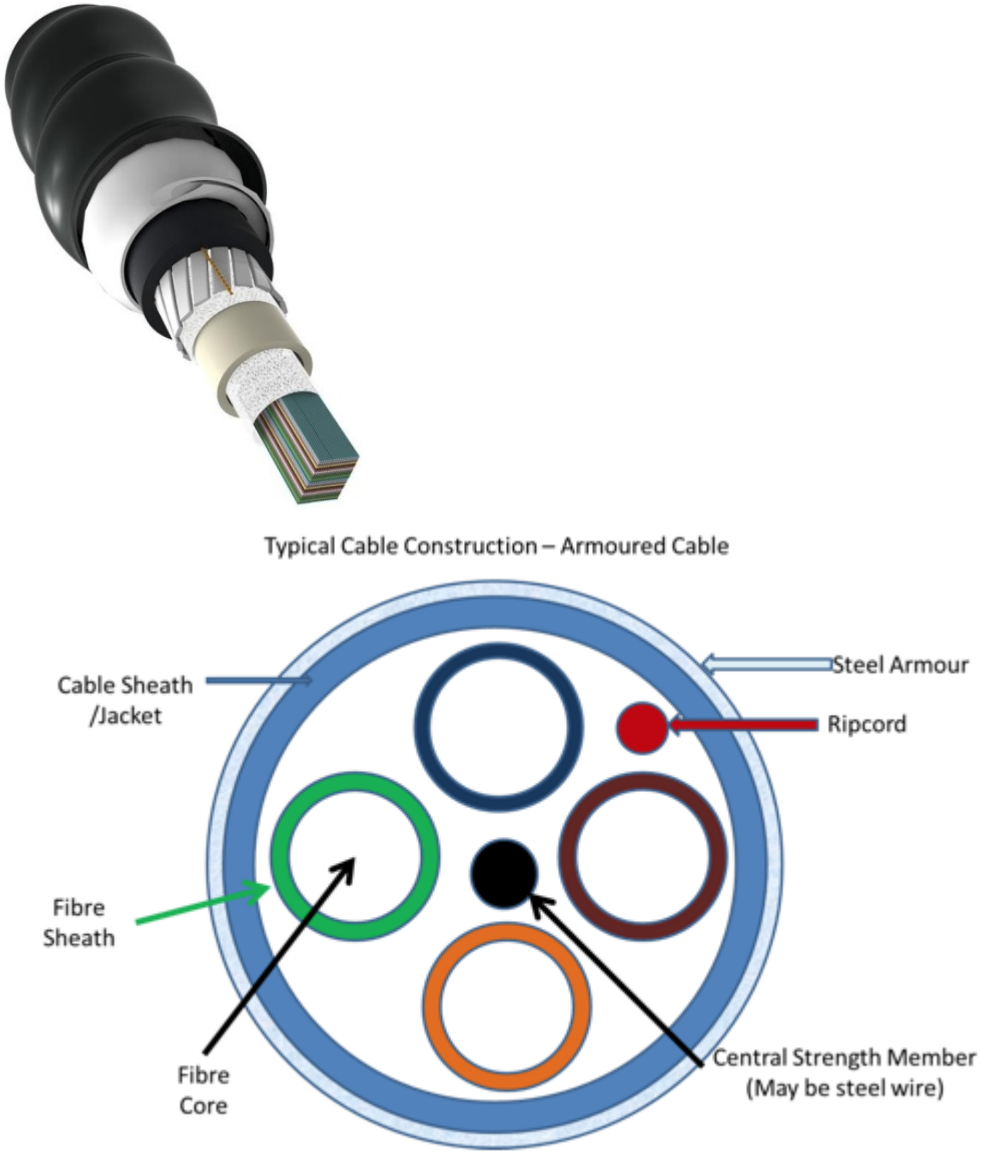


Figure 6 - Armoured Ribbon Fibre Cable

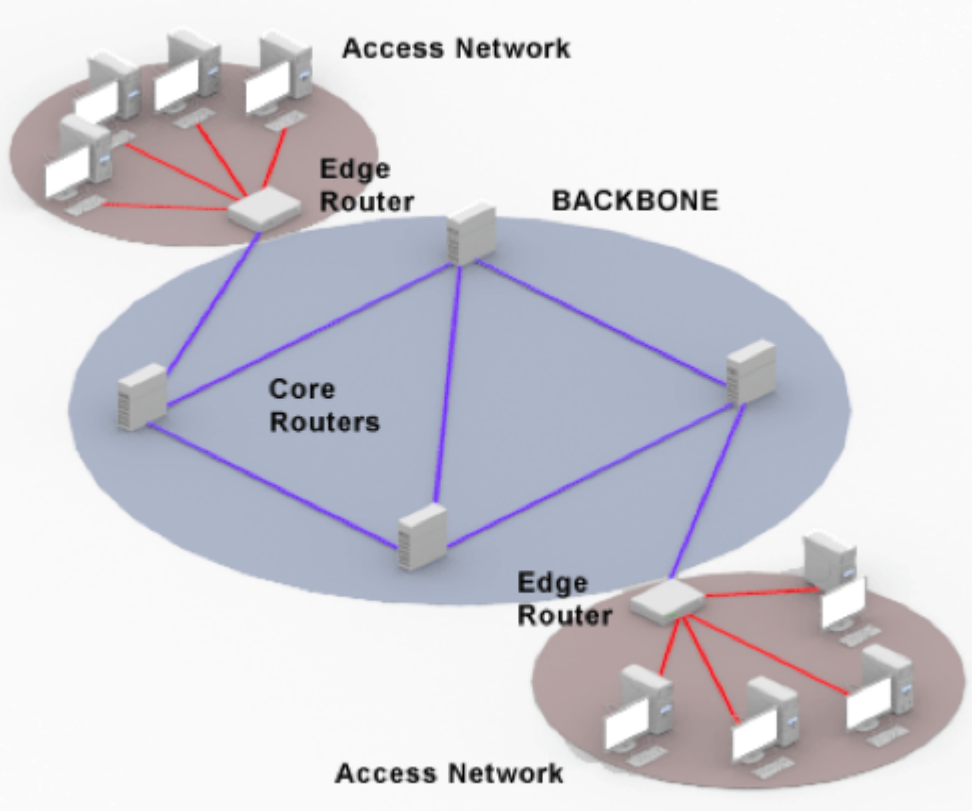
Backbone

10.1.28. A backbone or core is the central cabling that connects the infrastructure (servers, databases, gateways, equipment and telecommunication rooms etc.) to local areas networks, workstations and other devices, such as MFD's. Smaller networks may also be connected to the backbone.

10.1.29. A backbone can span a geographic area of any size including an office, a single building, multi-story buildings, campus, national and international infrastructure. In the context of the NZISM the term backbone generally refers to the central cabling within a building or a campus.

10.1.30. Backbones can be defined in terms of six criteria:

- transmission media;
- topology;
- security required;
- access control;
- transmission technique;
- transmission speed and capability.



TOP SECRET cabling

10.1.31. For TOP SECRET cabling the cable's non-conductive protective sheath IS NOT considered to be a conduit. For TOP SECRET fibre optic cables with sub-units, the cable's outer protective sheath IS considered to be a conduit.

Power Filters

10.1.32. A power filter is a device placed between an external power source and electronic devices. It is used in order to attenuate external transients, conducted radio frequencies (RF) or electromagnetic interference (EMI) between the AC or DC power line and the equipment. Filters can also reduce radiated interference to assist in managing emissions or susceptibility to interference.

10.1.33. The power lines entering an electronic device can act both as an antenna and as a low impedance conduction path for signals that exist inside the device. These signals may couple into the power line, either through inductance or capacitance, from internal circuitry, other internal wiring or from other components such as transformers, coils or adjacently routed wires. To a lesser degree, but still problematic, the power lines can also pickup induced current signals from magnetic fields inside the enclosure.

10.1.34. The purpose of power supply filters is to smooth the power supply and provide a degree of isolation from the external power supply for connected electronic devices. RF/EMI filters are designed to reduce line - to - ground (common mode) interference, EMI and anomalous RF. Best practice is to solve or suppress EMI and RF emissions at source, rather than after emission.

10.1.35. There are international and national regulations on frequencies and signal levels that a device is permitted to produce in order to minimise or prevent interference with other equipment. Practically no modern equipment, with fast digital circuits and switch-mode power supply regulators can meet electromagnetic compatibility (EMC) requirements without efficient filtering, particularly when operating in close proximity. While most devices are designed by manufacturers to meet regulation, not all devices filter EMI or RF to levels acceptable for secure environments. It may be necessary to use a power line filter to keep signals inside the enclosure as much as possible and keep any generated signals to less than the legal or required limits for conducted emissions.

10.1.36. Power filters have a variety of capabilities depending on their specification. It is important the filters are selected correctly for the power supply, expected load and required attenuation capacity. It is important to note that an Uninterruptible Power Supply (UPS) is NOT considered an RF/EMI filter.

10.1.37. Common usage of filters is for computer systems, laboratory and testing equipment, medical devices, consumer electronics, and to protect any equipment where good quality power supply and protection of the electronic devices and data is required. Devices can be within buildings, vehicle, ships, aircraft or portable.

10.1.38. Power filters often include EMC/ RFI filters which channel emissions to earth to prevent them from being conducted back down the supply cables. This can be detected as an earth leakage current which may cause Residual Current Devices (RCDs) to trip. This problem can be corrected by using the correct specification of power filter or installing low leakage current devices. Agencies should consult the GCSB if such problems occur.

References

10.1.39. Fibre Standards:

Reference	Title	Publisher	Source
AS/NZS 2967:2014	Optical fibre communication cabling systems safety. Provides rules for safe practices in the handling, installation, testing, use and disposal of optical fibre cabling and associated materials and equipment.	Standards NZ	https://www.standards.govt.nz/shop/asnzs-29672014/
ISO/IEC 11801	Information technology - Generic cabling for customer premises. Specifies general-purpose telecommunication cabling systems (structured cabling), including several classes of optical fibre interconnections.	ISO	https://www.iso.org/standard/66182.html
IEC 60793 Series	Optical fibres. A list of all parts in the IEC 60793 series, published under the general title Optical fibres, can be found on the IEC website.	ISO	https://webstore.iec.ch/home
IEC 60794 Series	Optical fibre cables. A list of all parts in the IEC 60794 series, published under the general title Optical fibre cables, can be found on the IEC website.	ISO	https://webstore.iec.ch/home
ANSI/TIA-568-C.3	Optical Fibre Cabling Components	TIA	https://webstore.ansi.org
ANSI/TIA-598-D (Revision of TIA-598-C) July 2014	Optical Fibre Cable Colour Coding This standard defines the recommended identification scheme or system for individual fibres, fibre units, and groups of fibre units within a cable structure.	TIA	https://webstore.ansi.org
ITU-T G.657 – 659 series	Optical Fibre Cables Characteristics and recommendations for selection, use and installation.	ITU-T	https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx

References - Fibre Standards

10.1.40. Further references can be found at:

Reference	Title	Publisher	Source
NZCSS 400	**New Zealand Communications Security Standard No 400 (Document classified CONFIDENTIAL)**	GCSB	CONFIDENTIAL document available on application to authorised personnel
AS/NZS 3000:2007/Amdt 2:2012	**Electrical Installations (Known as the Australia/New Zealand Wiring Rules,**	Standards NZ	https://standards.govt.nz/
ANSI/TIA-568-C.3	**Optical Fiber Cabling Components**	American National Standards Institute (ANSI)	https://www.ansi.org/
IEEE 802-2014	**Local and Metropolitan Area Networks: Overview and Architecture**	Institute of Electrical and Electronics Engineers (IEEE)	https://ieeexplore.ieee.org/document/6847097

PSR references

10.1.41. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	Home | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements/ Physical security (PHYSEC) | Protective Security Requirements

Rationale & Controls

Backbone

10.1.42.R.01. **Rationale**

The design of a backbone requires consideration of a number of criteria including the capacity of the cable to carry the predicted volume of data at acceptable speeds. An element of "future proofing" is also required as re-cabling to manage capacity issues can be costly. Fibre optic cable provides a convenient means of securing and "future proofing" backbones.

10.1.42.C.01. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must** [CID:2216]

Agencies MUST use fibre optic cable for backbone infrastructures and installations.

10.1.42.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2217]

Agencies SHOULD use fibre optic cable for backbone infrastructures and installations.

Use of Fibre Optic Cable

10.1.43.R.01. **Rationale**

Fibre optic cable is considered more secure than copper cables and provides electrical isolation of signals. Fibre will also provide higher bandwidth and speed to allow a degree of future-proofing in network design.

10.1.43.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2220]

Agencies SHOULD use fibre optic cabling.

10.1.43.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2221]

Agencies SHOULD consult with the GCSB where fibre optic cable incorporating conductive metal strengtheners or sheaths is specified.

10.1.43.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2222]

Agencies SHOULD consult with the GCSB where copper cables are specified.

10.1.43.C.04.

Control System Classifications(s): All Classifications; Compliance: Should Not [CID:2223]

Agencies SHOULD NOT use fibre optic cable incorporating conductive metal strengtheners or sheaths except where essential for cable integrity.

Cabling Standards

10.1.44.R.01. **Rationale**

Unauthorised personnel could inadvertently or deliberately access system cabling. This could result in loss or compromise of classified information. Non-detection of covert tampering or access to system cabling may result in long term unauthorised access to classified information by a hostile entity.

10.1.44.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2226]

Agencies MUST install all cabling in accordance with the relevant New Zealand standards as directed by AS/NZS 3000:2007 and NZCSS400.

Cable colours

10.1.45.R.01. **Rationale**

To facilitate cable management, maintenance and security cables and conduit should be colour-coded to indicate the classification of the data carried and/or classification of the compartmented data.

10.1.45.R.02. **Rationale**

Cables and conduit may be the distinguishing colour for their entire length or display a distinguishing label marking and colour at each end and at a maximum of two metre intervals along the cable.

10.1.45.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2230]

Agencies MUST comply with the cable and conduit colours specified in the following table.

Classification	Cable colour
Compartmented Information (SCI)	Orange/Yellow/Teal or other colour
TOP SECRET	Red
SECRET	Blue
CONFIDENTIAL	Green
RESTRICTED and all lower classifications	Black

10.1.45.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2231]

Additional colours may be used to delineate special networks and compartmented information of the same classification. These networks MUST be labelled and covered in the agency's SOPs.

Cable colours for foreign systems in New Zealand facilities

10.1.46.R.01. **Rationale**

Foreign systems should be segregated and separated from other agency systems for security purposes. Colour-coding will facilitate installation, maintenance, certification and accreditation.

10.1.46.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:2234]

The cable colour to be used for foreign systems MUST be agreed between the host agency, the foreign system owner and the Accreditation Authority.

10.1.46.C.02. **Control System Classifications(s): Top Secret; Compliance: Must Not** [CID:2235]

Agencies MUST NOT allow cable colours for foreign systems installed in New Zealand facilities to be the same colour as cables used for New Zealand systems.

10.1.46.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2236]

The cable colour to be used for foreign systems SHOULD be agreed between the host agency, the foreign system owner and the Accreditation Authority.

10.1.46.C.04. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:2237]

Agencies SHOULD NOT allow cable colours for foreign systems installed in New Zealand facilities to be the same colour as cables used for New Zealand systems.

Cable groupings

10.1.47.R.01. **Rationale**

Grouping cables provides a method of sharing conduits and cable reticulation systems in the most efficient manner. These conduits and reticulation system must be inspectable and cable separations must be obvious.

10.1.47.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2240]

Agencies MUST contact GCSB for advice when combining the cabling of special networks.

10.1.47.C.02. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:2241]

Agencies MUST NOT deviate from the approved fibre cable combinations for shared conduits and reticulation systems as indicated below.

Group	Approved combination
1	UNCLASSIFIED
	RESTRICTED
2	CONFIDENTIAL
	SECRET
3	TOP SECRET
	Other Special Networks

Fibre optic cables sharing a common conduit

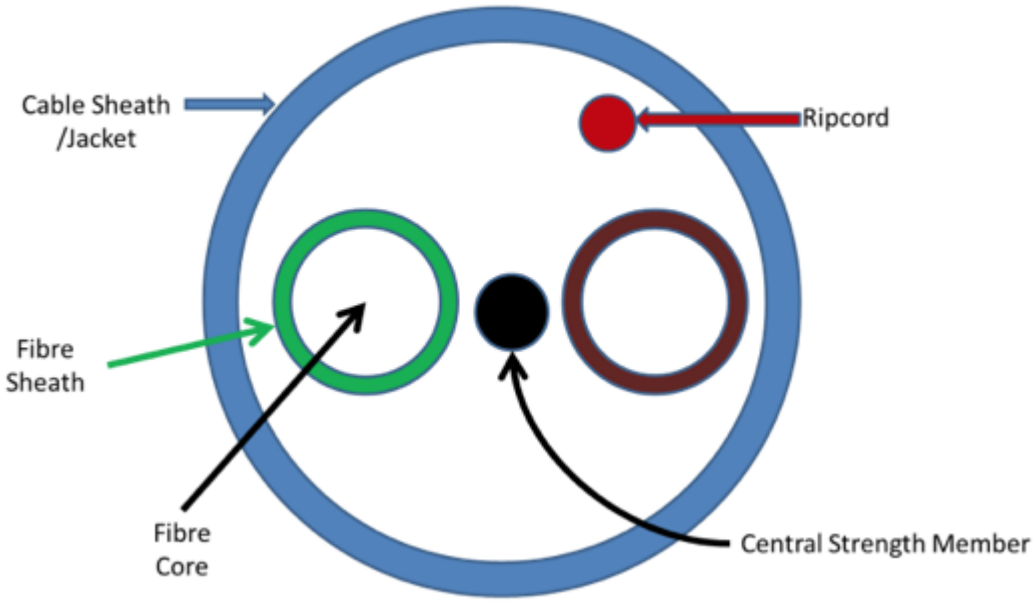
10.1.48.R.01. **Rationale**

The use of multi-core fibre optic cables can reduce installation costs. The principles of separation and containment of cross-talk and leakage must be adhered to.

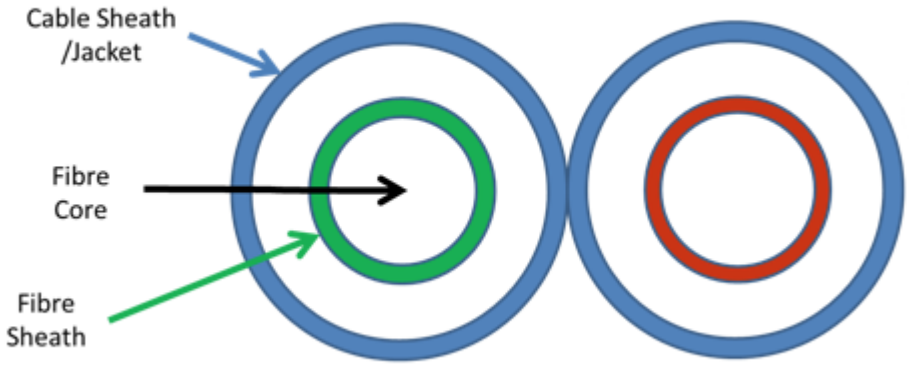
10.1.48.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2244]

With fibre optic cables the arrangements of fibres within the cable sheath, as illustrated in Figure 3, MUST carry a single classification only.

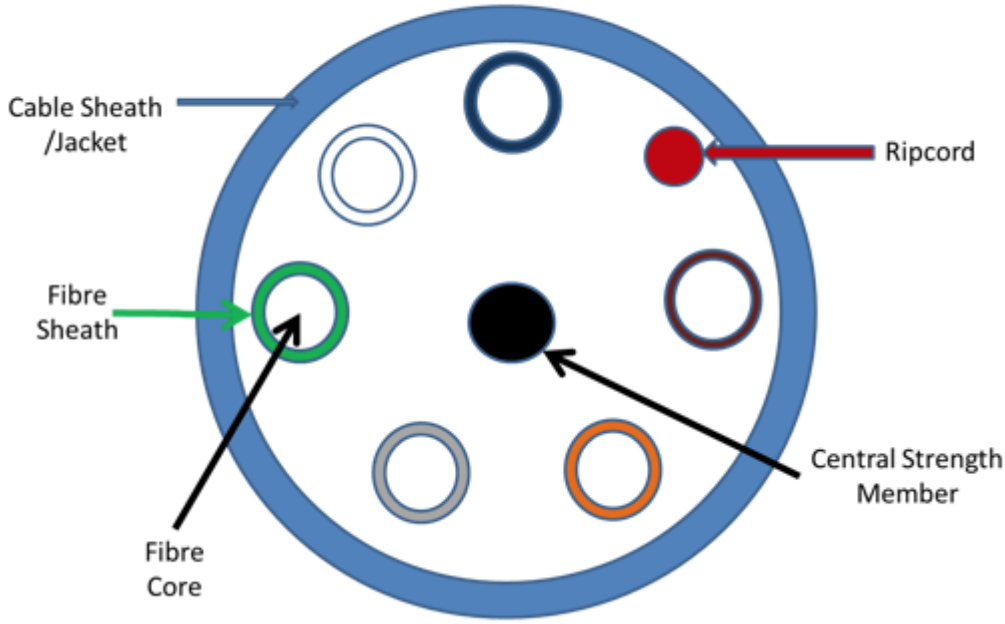
Typical Cable Construction - Duplex



Typical Cable Construction - TwinFlex

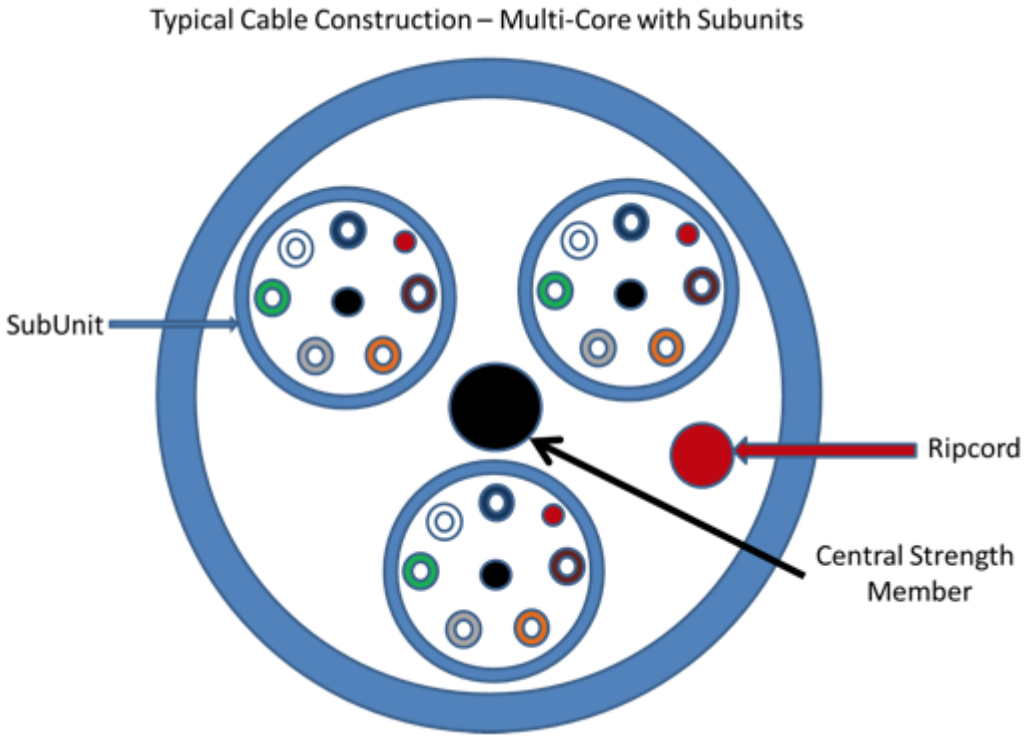


Typical Cable Construction – Multi-Core Cable



10.1.48.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2245]

If a fibre optic cable contains subunits, as shown in Figure 4, each subunit MUST carry only a single classification.



10.1.48.C.03. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:2246]

Agencies MUST NOT mix classifications up to RESTRICTED with classifications of CONFIDENTIAL and above in a single cable.

Audio secure areas

10.1.49.R.01. **Rationale**

Audio secure areas are designed to prevent audio conversation from being heard outside the walls. Penetrating an audio secure area for cables in an unapproved manner can degrade this. Consultation with GCSB needs to be undertaken before any modifications are made to audio secure areas.

10.1.49.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:2249]

When penetrating an audio secure area for cables, agencies MUST comply with all directions provided by GCSB.

Wall outlet terminations

10.1.50.R.01. **Rationale**

Wall outlet boxes are the preferred method of connecting cable infrastructure to workstations and other equipment. They allow the management of cabling and can utilise a variety of connector types for allocation to different classifications.

10.1.50.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2253]

Cable groups sharing a wall outlet MUST use different connectors for systems of different classifications.

10.1.50.C.02. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:2254]

In areas containing outlets for both TOP SECRET systems and systems of other classifications, agencies MUST ensure that the connectors for the TOP SECRET systems are different to those of the other systems.

10.1.50.C.03. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:2255]

Cable outlets MUST be labelled with the system classification and connector type.

10.1.50.C.04.

Control System Classifications(s): All Classifications; Compliance: Should [CID:2256]

Cable outlets SHOULD be labelled with the system classification and connector type.

Power Filters

10.1.51.R.01. **Rationale**

Power filters are used to provide a filtered (clean) power supply and reduce opportunity for technical attacks. See also 10.1.32.

10.1.51.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:5899]

Power filters SHOULD be used to provide a filtered power supply and reduce opportunity for technical attacks.