International Telecommunication Union

ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

G.873.1

Amendment 1

(10/2012)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Digital networks – Optical transport networks

Optical Transport Network (OTN): Linear protection

Amendment 1

Recommendation ITU-T G.873.1 (2011) – Amendment 1

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
General aspects	G.800–G.809
Design objectives for digital networks	G.810–G.819
Quality and availability targets	G.820–G.829
Network capabilities and functions	G.830–G.839
SDH network characteristics	G.840–G.849
Management of transport network	G.850–G.859
SDH radio and satellite systems integration	G.860–G.869
Optical transport networks	**G.870–G.879**
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T G.873.1

Optical Transport Network (OTN): Linear protection

Amendment 1

Summary

Amendment 1 to Recommendation ITU-T G.873.1 (2011) contains additional protection architectures, corrections to the protection protocol, clarification of drawings of protection architectures and references to equipment standards.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T G.873.1	2003-03-29	15
2.0	ITU-T G.873.1	2006-03-29	15
3.0	ITU-T G.873.1	2011-07-22	15
3.1	ITU-T G.873.1 (2011) Amd. 1	2012-10-29	15

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Recommendation ITU-T G.873.1

Optical Transport Network (OTN): Linear protection

Amendment 1

1) Scope

This amendment contains additional protection architectures, corrections to the protection protocol, clarification of drawings of protection architectures and references to equipment standards.

2) Clause 2 References

Insert new reference as shown below:

[ITU-T G.709] Recommendation ITU-T G.709/Y.1331 (2012), *Interfaces for the optical transport network.*

[ITU-T G.798] Recommendation ITU-T G.798 (2010), *Characteristics of optical transport network hierarchy equipment functional blocks*.

<u>[ITU-T G.798.1] Recommendation ITU-T G.798.1 (2012), *Types and characteristics of optical transport network equipment.*</u>

3) Clause 4 Abbreviations and acronyms

Add the following abbreviations:

<u>SNC/Ne Sub-Network Connection with Non-intrusive end-to-end monitoring</u>

<u>SNC/Ns Sub-Network Connection with Non-intrusive sublayer monitoring</u>

4) Clause 5.1 Monitoring methods and conditions

Modify the text as follows:

5.1 Monitoring methods and conditions

Protection switching will occur based on the detection of certain defects on the transport entities (working and protection) within the protected domain. How these defects are detected is the subject of the equipment Recommendations (e.g., [ITU-T G.806] and [ITU-T G.798]). For the purpose of the protection switching controller, an entity within the protected domain has a condition of no defect = OK, degraded (signal degrade = SD), or failed (signal fail = SF).

The customary monitoring methods are <u>specified in clauses 11.2 and 11.3 of [ITU-T G.808.1] and in clause 14.1 of [ITU-T G.798] and are supported in the OTN</u> as follows:

Inherent – Protection switching is triggered by defects detected at the ODUk link connection (e.g., server layer trail and server/ODUk adaptation function). The trail termination sink of an (OTUk[V] or ODUk~~P~~) server layer provides the TSF- and TSD-based SF and SD protection switching criteria via the OTUk[V]/ODUk_A~~, or~~ ODUkP/ODU[i]j_A or ODUkP/ODUj-21_A functions (as SSF and SSD). No defect detection is performed ~~at~~ on the protected ODUk or ODU[i]j or ODUj ~~layer~~signals itself. It can be used for individual and for compound link group protection (CL_SNCG/I).

NOTE 1 – In contrast to SDH SNC/I, ODUk SNC/I can stretch only a single link connection, as the FDI/AIS defect resulting from further upstream server layer defects is not detected in the server/ODUk adaptation function. The limitation to a single server layer trail for SNC/I protection is given by the use of signal degrade (SD) as protection switching criteria. SD is only available from the OTUk[V] or HO ODUk trail that is locally terminated and not from further upstream OTUk[V] or HO ODUk trails. Furthermore, FDI/AIS, which provides information about defects in upstream OTUk[V] or HO ODUk trails, is not detected in the OTUk[V]/ODUk_A_Sk or ODUkP/ODU[i]j_A_Sk. For details of the atomic functions for TSF TSD forwarding for the SNC protection on LO ODU refer to [ITU-T G.798].

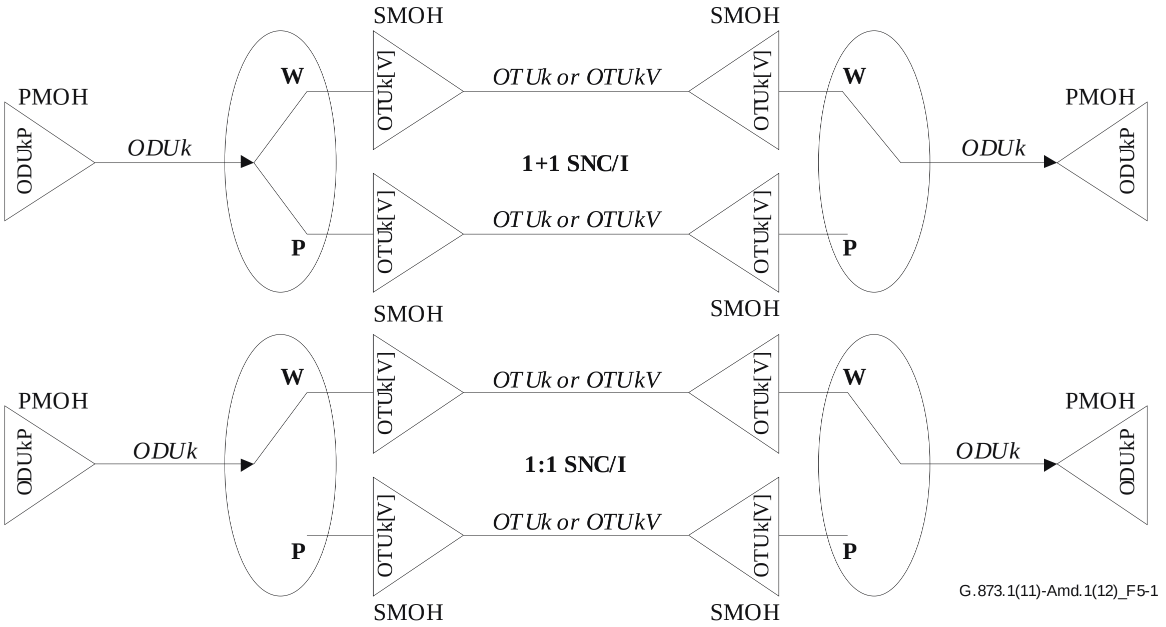

Figure 5-1 – OTUk- or OTUkV-monitored ODUk SNC/I protection configuration

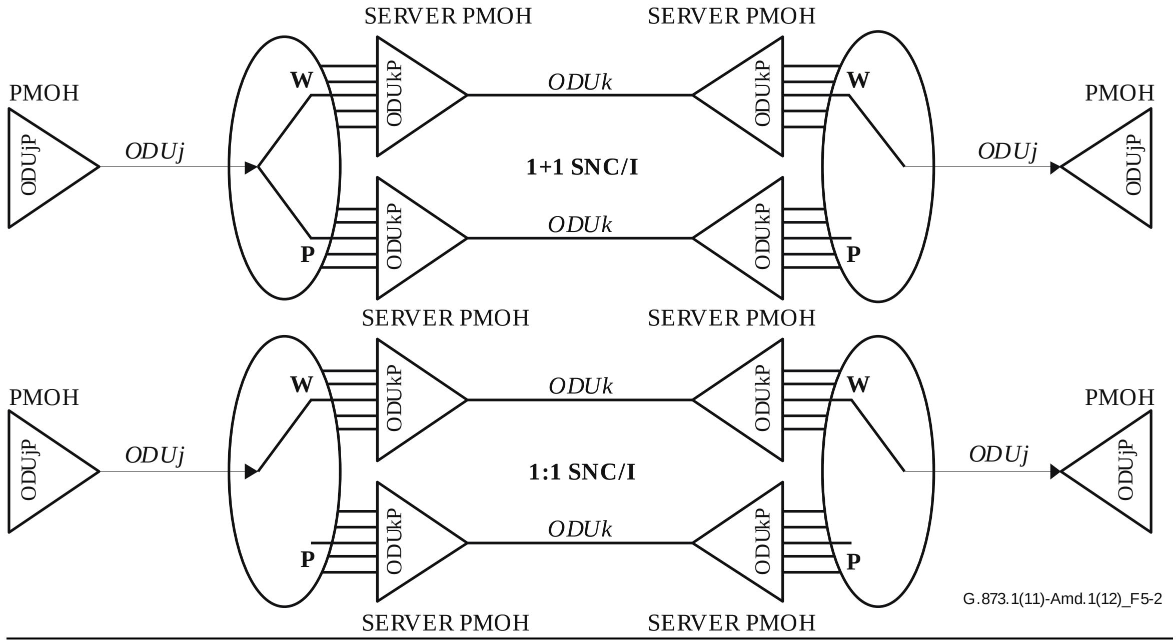

Figure 5-2 – Server ODUk-monitored ODU[i]j/ODUj SNC/I protection configuration

Non-intrusive – Protection switching is triggered by a non-intrusive monitor of the ODUkP trail or ODUkT sub-layer~~s~~ trail~~s~~ at the tail-end of the protection group.

NOTE 2 – For a SNC/N protection the criteria according to [ITU-T G.798] are taken. This ensures that ODUk-AIS as well a Locked or OCI condition is contributing to switch criteria of a ODU SNC/N protection. For details refer to clause 14.2 of [ITU-T G.798].

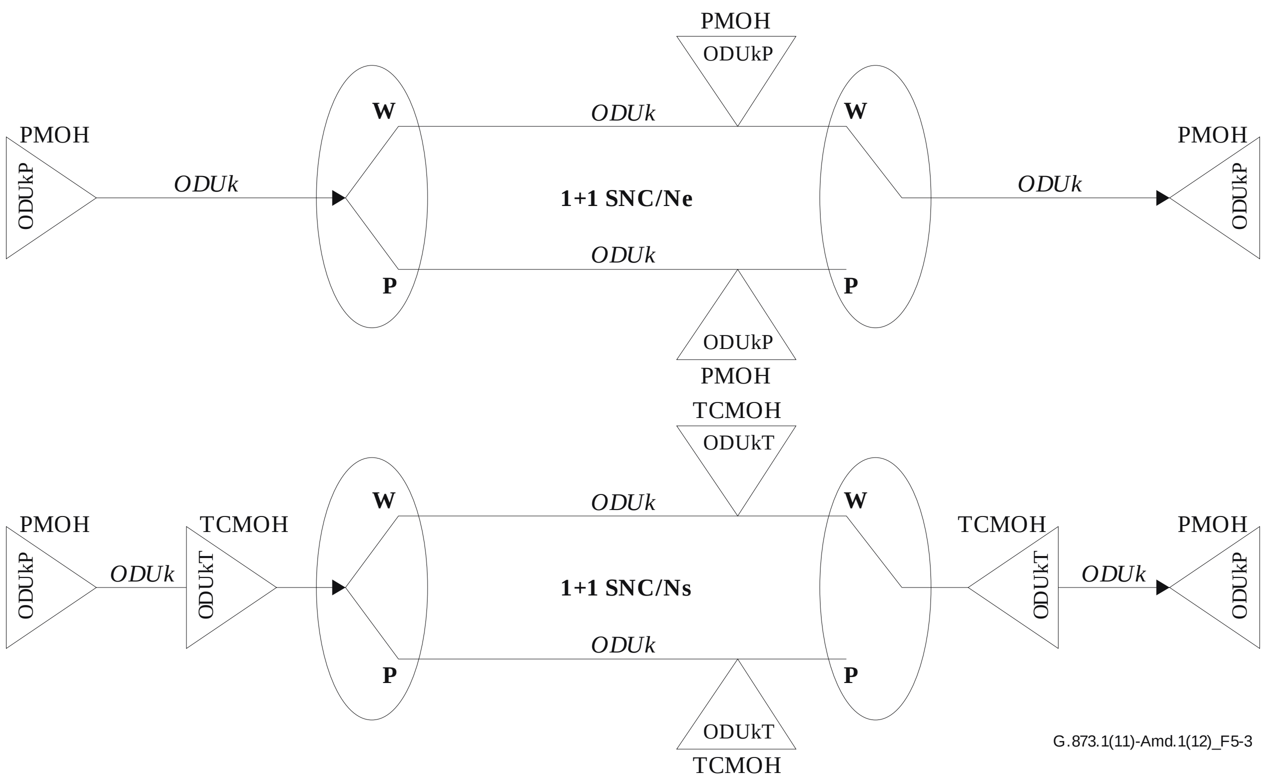

Figure 5-3 – ODUkP non-intrusively monitored ODUk SNC/Ne and ODUkT-monitored ODUk SNC/Ns protection configurations

Sublayer – Protection switching is triggered by defects detected at the ODUkT sublayer trail (TCM). An ODUkT sublayer trail is established for each working and protection entity. Protection switching is therefore triggered only on defects of the protected domain.

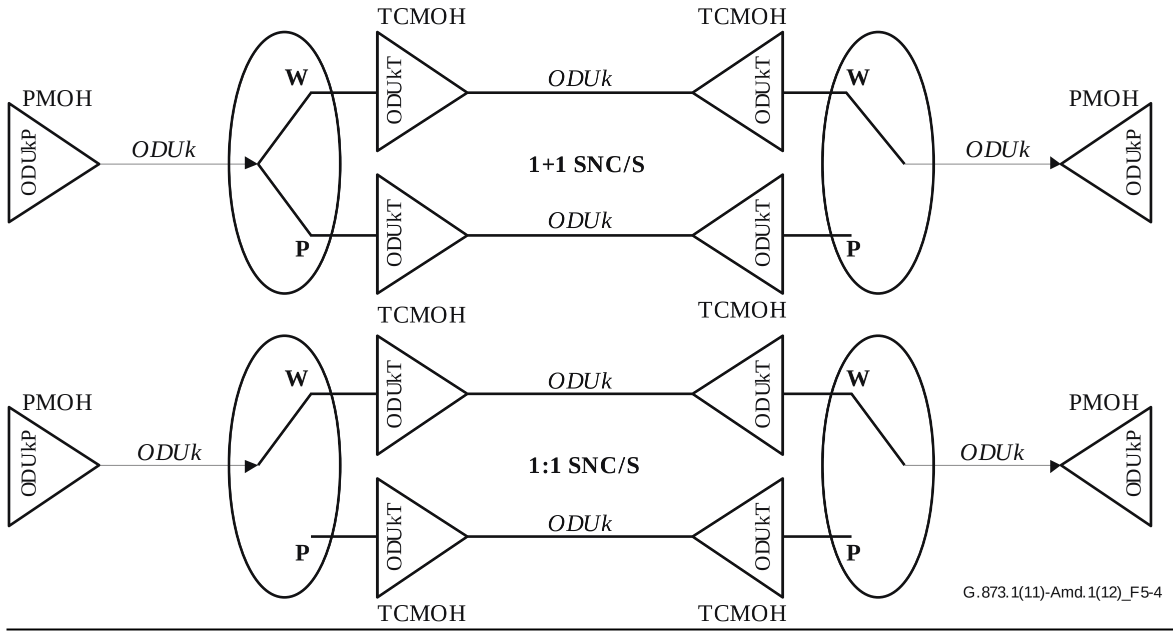

Figure 5-4 – ODUkT-monitored SNC/S protection configuration

The protection switching controller does not care which monitoring method is used, as long as it can be given (OK, SD, SF) information for the transport entities within the protected domain. Some monitors or network layers may not have an SD detection method. Where this is the case, there is no need to use a different APS protocol – it would simply happen that an SD would not be issued from equipment that cannot detect it. Where an APS protocol is used, the implementation should not preclude that the far end declares an SD over the APS channel, even if the monitor at the near-end cannot detect SD.

NOTE 3 – In accordance with [ITU-T G.709], for sublayer monitoring, nesting and cascading are the default operational configurations. Overlapping is an additional configuration for testing purposes only. Overlapped monitored connections must be operated in a non-intrusive mode and not used for protection. Maintenance signals ODUk-AIS and ODUk-LCK must not be generated for overlapped monitored connections.~~Overlapped monitored connections must be operated in a non-intrusive mode and not used for protection, in which the maintenance signals ODUk-AIS and ODUk-LCK are not generated~~. For the case where one of the endpoints in an overlapping monitored connection is located inside a SNC protected domain while the other endpoint is located outside the protected domain, the SNC protection should be forced to working when the endpoint of the overlapping monitored connection is located on the working connection, and forced to protection when the endpoint is located on the protection connection.

5) Clause 5.2, Protection switching performance

Add following new clause 5.2.

5.2 Protection switching performance

The protection switching performance is given in clause 14.1.1.1 of [ITU-T G.798] for a related reference configuration.

6) Clause 7.5 Overview of protection architectures for OTN linear protection

Add the indicated entries and text to Table 7-1 of clause 7.5 as follows:

Table 7-1 – Overview of linear OTN protection architectures and related monitoring

Protection architecture	Switching type	Protection subclass and monitoring	ODU entities for protection switching, individual/ group	APS channel used and MFAS in bits 6-8	Server layer of protected entity	Protection switched entity	Trigger criteria used
1+1	Unidir	SNC/I	Individual	No	One HO ODUk or one OTUk	ODUkP or ODUkT	ODU SSF/SSD
1+1	Bidir	SNC/I	Individual	111	One OTUk or one HO ODUk	ODUkP or ODUkT	ODU SSF/SSD
1:n	Bidir	SNC/I	Individual	111	One OTUk or one HO ODUk	ODUkP or ODUkT	ODU SSF/SSD
1+1	Unidir	SNC/Ne	Individual	No	One or more HO ODUk and/or OTUk	ODUkP	ODU TSF/TSD
1+1	Bidir	SNC/Ne	Individual	000	One or more HO ODUk and/or OTUk	ODUkP	ODU TSF/TSD
1+1	Unidir	SNC/Ns	Individual[4]	No	One or more HO ODUk and/or OTUk	ODUkT	ODU TSF/TSD
1+1	Bidir	SNC/Ns	Individual[4]	001-110	One or more HO ODUk and/or OTUk	ODUkT	ODU TSF/TSD
1+1	Unidir	SNC/S	Individual[4]	No	One or more HO ODUk and/or OTUk	ODUkT or ODUkP	ODUkT SSF/SSD
1+1	Bidir	SNC/S	Individual[4]	001-110	One or more HO ODUk and/or OTUk	ODUkT or ODUkP	ODUkT SSF/SSD
1:n	Bidir	SNC/S	Individual[4]	001-110	One or more HO ODUk and/or OTUk	ODUkT or ODUkP	ODUkT SSF/SSD

Table 7-1 – Overview of linear OTN protection architectures and related monitoring

Protection architecture	Switching type	Protection subclass and monitoring	ODU entities for protection switching, individual/ group	APS channel used and MFAS in bits 6-8	Server layer of protected entity	Protection switched entity	Trigger criteria used
1+1	Unidir	CL-SNCG/Ie	Group	No	One HO ODUk	LO ODU	HO ODUkP SSF/SSD ~~and HO ODUdPLM~~
1+1	Bidir	CL-SNCG/Ie	Group	HO 000	One HO ODUk	LO ODU	HO ODUkP SSF/SSD ~~and HO ODUdPLM~~
1:1	Bidir	CL-SNCG/Ie	Group	HO 000	One HO ODUk	LO ODU	HO ODUkP SSF/SSD ~~and HO ODUdPLM~~
~~1+1~~	~~unidir~~	~~CL-SNCG/Is~~	~~group~~	~~no~~	~~one HO ODUk~~	~~LO ODU~~	~~ODUkT SSF/SSD~~
~~1+1~~	~~bidir~~	~~CL-SNCG/Is~~	~~group~~	~~001-110~~	~~one HO ODUk~~	~~LO ODU~~	~~ODUkT SSF/SSD~~
~~1:N~~	~~bidir~~	~~CL-SNCG/Is~~	~~group~~	~~001-110~~	~~one HO ODUk~~	~~LO ODU~~	~~ODUkT SSF/SSD~~

NOTE 1~~2~~ – Bidir SNC/N, is ~~not~~ supported ~~because it requires the transport of an APS signal between the head-end and the tail-end. This APS signal is to be inserted on the ODUk signal which may contain AIS OCI or LCK signal. This ODUk AIS/OCI/LCK signal with APS cannot be distinguished from a ODUk AIS/OCI/LCK signal without APS inserted at an intermediate point of the protection connection at the tail-end.~~but care should be taken in case of nested protection schemes as an APS channel may be used by more than one protection scheme and/or protection scheme instance. It is recommended to use 1+1 bidir SNC/S instead.

NOTE ~~3~~ 2 – CL-SNCG/I~~E~~ can assign all Normal signal to the Na subgroup and leave the Nb subgroup empty.

NOTE 3 – The equipment models and required processes of the various architectures are given in the related subclauses of clause 14.1 of [ITU-T G.798].

NOTE 4 – The SNC/S architecture may be implemented when there is HO/LO muxing with "emulation" of line switching by switching all contained LO ODU connections. Examples are given in [ITU-T G.798.1].

7) Clause 8.3 Request type

Modify the text of clause 8.3 as indicated below:

8.3 Request type

The request types that may be reflected in the APS bytes are the "standard" types traditionally supported by protection switching for SONET and SDH. These requests reflect the highest priority condition, command, or state (see Tables 8-2 and 8-3). In the case of unidirectional switching, this is the highest priority value determined from the near-end only.

In bidirectional switching, ~~the local request will be indicated only in the case where it is as high as or higher than any request received from the far end over the APS channel. In bidirectional switching, when the far end request has the highest priority, the near-end will signal Reverse Request.~~the sent Request/State shall indicate:

a) a reverse request if;

I. the remote request is of higher priority,

II. or if the requests are of the same level (and are higher priority than a no request/do not revert) and the sent Request/State already indicates reverse request, or if

III. the requests are of the same level (and are higher priority than a no request/do not revert) and the sent Request/State byte does not indicate reverse request and the remote request indicates a lower entity ID;

b) the local request in all other cases

Table 8-2 – Request/state priorities with APS protocol

Request/state	Priority
Lockout for Protection (LoP)	1 (highest)
Signal Fail (SF) – protection	2 (see clause 8.9)
Forced Switch (FS)	3
Signal Fail (SF) – working	4
Signal Degrade (SD)	5
Manual Switch (MS)	6
Wait-to-Restore (WTR)	7
Exercise (EXER)	8
Reverse Request (RR)	9
Do Not Revert (DNR)	10
No Request (NR)	11 (lowest)

Table 8-3 – Request/state priorities without APS protocol

Request/state	Priority
Lockout for Protection (LoP)	1 (highest)
Forced Switch (FS)	2
Signal Fail (SF)	3
Signal Degrade (SD)	4
Manual Switch (MS)	5
Wait-to-Restore (WTR)	6
Do Not Revert (DNR)	7
No Request (NR)	8 (lowest)

8) Clause 8.6 Bridged signal

Add the following text to clause 8.6 as indicated:

8.6 Bridged signal

This indicates the signal that is bridged onto the protection entity. For 1+1 protection, this should always indicate Normal traffic Signal 1, accurately reflecting the permanent bridge. This allows a 1-phase rather than a 2 or 3-phase switch in the case of 1+1 architecture. For 1:n protection, this will indicate what is actually bridged to the protection entity (either the Null Signal (0), Extra Traffic (255), or the number of a normal traffic signal). This will generally be the bridge requested by the far end.

If for the 1:N bidirectional architecture for the protection transport entity a local SF condition is present the bridge is released.

If for a 1:N unidirectional architecture, the protection transport entity is found in a local SF condition, the bridge is frozen.

9) Clause 8.14 APS channel alarming

Modify the bullet item list in clause 8.14 as indicated below:

8.14 APS channel alarming

"Failure of Protocol" situations for groups requiring APS are as follows:

– Fully incompatible provisioning (the "B" bit mismatch), described in clause 8.4.

– Lack of response to a bridge request for > ~~50 m~~1 s as defined for dFOP-NR in clause 6.2.7.1.2 of [ITU-T G.798] for the following protection types.
  - For 1+1 bidirectional, mismatch in sent *"Requested Entity"* and received *"Requested Entity"*.
  - For 1:n unidirectional, mismatch in sent *"Requested Entity"* and received *"Bridged Entity"*.
  - For 1:n bidirectional, mismatch in sent *"Requested Entity"* and received *"Bridged Entity"* as well as in sent *"Requested Entity"* and received *"Requested Entity"*.

If an unknown request or a request for an invalid entity number is received, it will be ignored. It will be up to the far end to alarm the non-response from the near-end.

If for a 1:N unidirectional architecture a SF request for the Null signal is received via the APS channel, a mismatch in sent "Requested Entity" and received "Bridged Entity" shall not result in a "Failure of Protocol".

10) Appendix II – clause II.3 Model of client SNC/I protection architectures of OTN linear client protection

Add the indicated entries and text to clause II.3.

II.3 Model of client SNC/I protection architectures of OTN linear client protection

Figure II.2 provides the model overview of the client SNC/I schemes as listed in Table II.1. The protection uses the client connection function external to the OTN and the OPU-CSF transport of the OTN as input to the protection.

SNC/I client protection requires that the client signal be split between two different ports in the client-to-network direction. Each port maps the client into an ODUk, and the two ODUk are carried across the OTN as if they were unrelated, unprotected signals. At the far end, the two ODUks are each terminated and the client signals are recovered. One or the other client signal is transmitted, based on monitoring of the ODUk overhead (including OPU-CSF). Two different selection mechanisms are possible, as shown in Figure II.2. Option (a) uses a Y-cable and a control process that monitors the ODUkP trail termination functions to determine which one provides the better signal and controls the client termination function (srv_TT) such that only one of the two transmitters is active. Option (b) uses an external optical switch with a selector that is controlled by the ODUkP trail termination functions. The client's APS information is transported over the ODUk PM APS channel. Access to this channel is provided via an extended version of the ODUkP/CBR adaptation functions specified in [ITU-T G.798]. The extension contains support for ODUk PM APS insertion and extraction processes as illustrated in Figures II.3 and II.4.

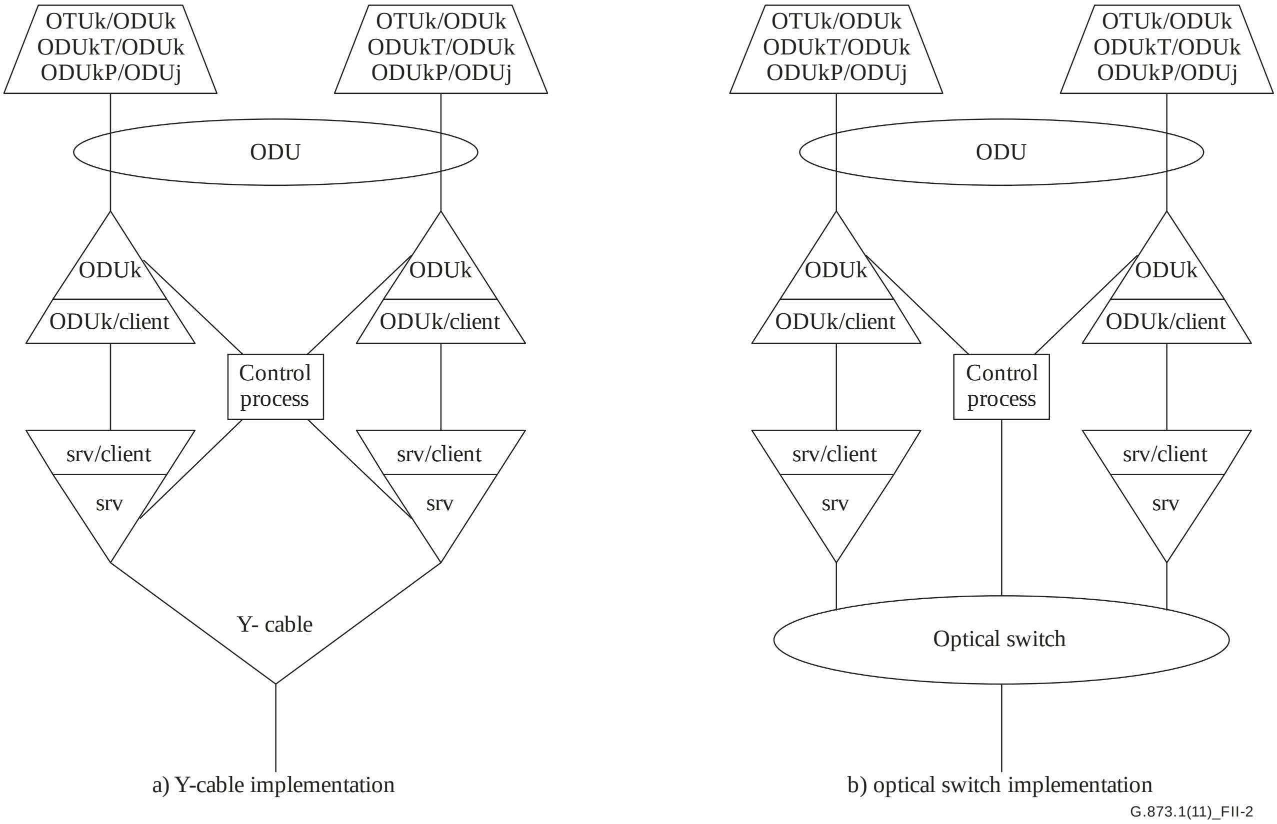

Figure II.2 – OTN client SNC/I protection models

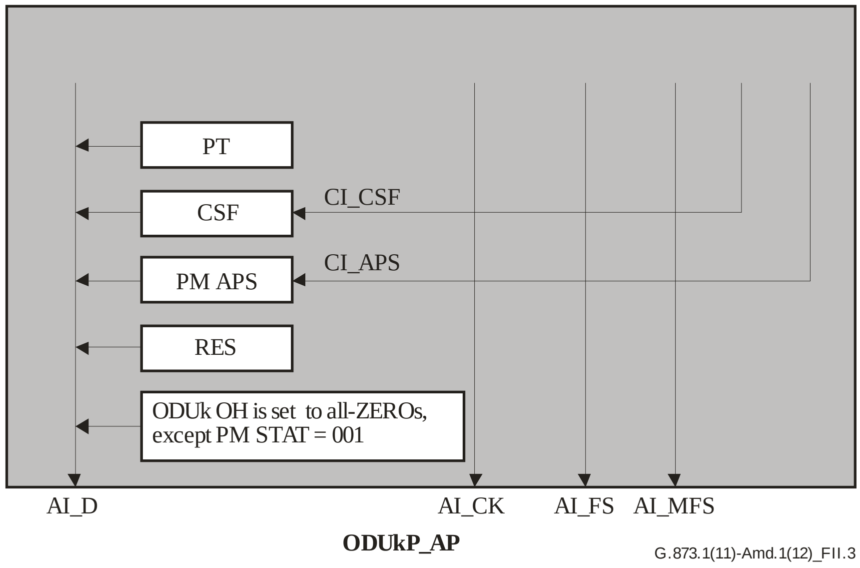

Figure II.3 – Supporting ODUk PM APS access in ODUkP/CBR adaptation source functions

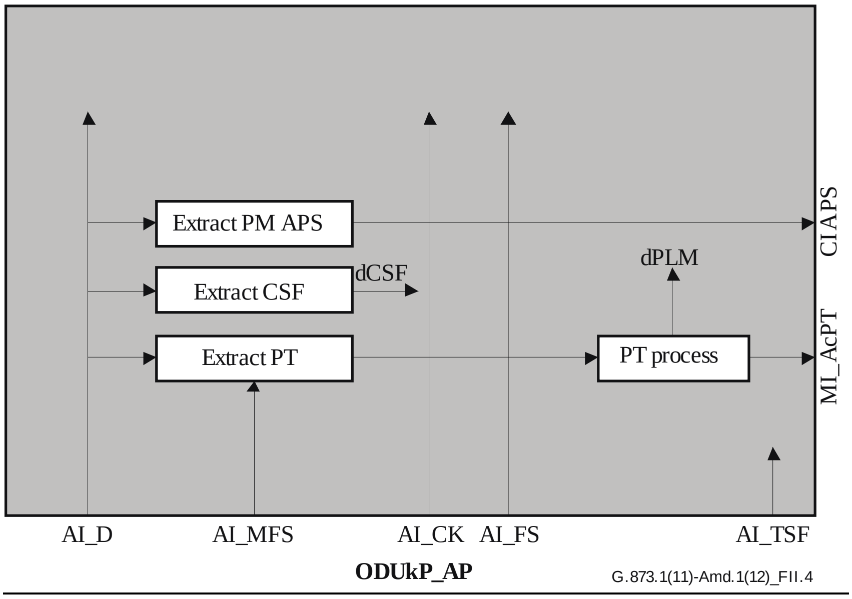

Figure II.4 – Supporting ODUk PM APS access in ODUkP/CBR adaptation sink functions

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013