International Telecommunication Union

ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

G.8031/Y.1342
Amendment 1
(10/2007)

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

Packet over Transport aspects – Ethernet over Transport aspects

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Internet protocol aspects – Transport

Ethernet linear protection switching
Amendment 1

ITU-T Recommendation G.8031/Y.1342 (2006) – Amendment 1

ITU-T

International Telecommunication Union

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
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
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
Ethernet over Transport aspects	**G.8000–G.8099**
MPLS over Transport aspects	G.8100–G.8199
Quality and availability targets	G.8200–G.8299
Service Management	G.8600–G.8699
ACCESS NETWORKS	G.9000–G.9999

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

ITU-T Recommendation G.8031/Y.1342

Ethernet linear protection switching

Amendment 1

Summary

Amendment 1 to ITU-T Recommendation G.8031/Y.1342 contains additional material to be incorporated into ITU-T Recommendation G.8031/Y.1342, Ethernet linear protection switching. It presents enhancements about response to EXER and DNR, and the location of protection switching process. It also presents additional descriptions about management information (MI) signals.

Source

Amendment 1 to ITU-T Recommendation G.8031/Y.1342 (2006) was approved on 7 October 2007 by ITU-T Study Group 15 (2005-2008) under the ITU-T Recommendation A.8 procedure.

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/.

CONTENTS

ITU-T Recommendation G.8031/Y.1342

Ethernet linear protection switching

Amendment 1

1) Scope

This amendment provides updated material pertaining to Ethernet linear protection switching as described in ITU-T Rec. G.8031/Y.1342. It presents enhancements about response to EXER and DNR, and the location of protection switching process. It also presents additional descriptions about management information (MI) signals.

2) References

– ITU-T Recommendation G.8031/Y.1342 (2006), *Ethernet protection switching*.

3) Conventions

This amendment contains changes to ITU-T Rec. G.8031/Y.1342.

Some of this material is new material, while some represents modifications to existing material in the original Recommendation.

4) Changes to ITU-T Rec. G.8031/Y.1342

Modify the title of G.8031/Y.1342 by:

Ethernet linear protection switching

4.1) Changes to Summary

Modify text in Summary as follows:

This Recommendation describes the specifics of linear protection switching for Ethernet VLAN signals. Included are details pertaining to ETH linear protection characteristics, architectures and the APS protocol. The protection scheme considered in this Recommendation is:

– VLAN-based Ethernet subnetwork connection linear protection with sublayer monitoring.

5) Changes to clause 4, Abbreviations

Add the following abbreviation between "MEP" and "MIP" in clause 4:

MI Management Information

6) Changes to clause 6, Introduction

Modify the fourth paragraph in clause 6 as follows:

Although selection is made only at the sink of the protected domain in linear 1+1 protection switching architecture, bidirectional linear 1+1 protection switching needs APS coordination protocol so that selectors for both direction selects the same entity. On the other hand, unidirectional linear 1+1 protection switching does not need APS coordination protocol.

7) Changes to clause 7, Requirements

Modify the title and the first item of clause 7 as follows:

7 ~~Requirements~~Network objectives

1) Ethernet linear protection switching should be applicable to Point-to-Point VLAN-based ETH SNC which provides connectivity between two ETH flow points in an ETH flow domain. VID(s) can be used to identify Point-to-Point VLAN based ETH SNC(s) within ETH links. Additional details on ETH and related atomic functions can be obtained from ITU-T Rec~~.~~s G.8021/Y.1341 and G.8010/Y.1306. Other entities to be protected are for further study.

8) Changes to clause 10, Protection architectures

8.1) Addition to clause 10.3, Revertive and non-revertive switching

Modify the third, fourth and fifth paragraphs in clause 10.3 and add a sentence to the end of clause 10.3 as follows:

1+1 protection is often provisioned as non-revertive operation, as the protection is fully dedicated in any case, and this avoids a second "glitch" to the normal traffic signal. There may, however, be reasons to provision this to be revertive operation (e.g., so that the normal traffic signal uses the "short" path except during failure conditions. Certain operator policies also dictate revertive operation even for 1+1).

1:1 protection is usually revertive operation. Although it is possible to define the protocol in a way that would permit non-revertive operation for 1:1 protection, however, since the working transport entity is typically more optimized (i.e., from a delay and resourcing perspective) than the protection transport entity, it is better to revert and glitch the normal traffic signal when the working transport entity is repaired.

In general, the choice of revertive/non-revertive operation will be the same at both ends of the protection group. However, a mismatch of this parameter does not prevent interworking; it just would be peculiar for one side to go to WTR for clearing of switches initiated from that side, while the other goes to DNR for its switches.

Revertive/non-revertive operation of a SNC/S protection switching process shall be configured via ETH_MI_PS_OperType.

8.2) Changes to clause 10.6, Protection switching models

Modify text and figures in clause 10.6, subclauses 10.6.1, 10.6.2 and 10.6.3 as follows:

10.6 Protection switching models

Figure 10-1 depicts an example of the VLAN based ETH SNC/S protection switching models defined in this Recommendation. Other network scenarios are permissible.

Within the ETH ~~Flow Forwarding~~ Connection function (ETH_~~FF~~C) an ETH SNC protection switching process is instantiated to protect the ETH Connection (EC). When protection switching is configured for an EC, i.e., the protected ETH SNC, it is defined between two ETH Flow Points (ETH_FPs) as depicted in Figure 10-1. Each instantiated SNC protection switching process determines the specific output ETH_FP over which the protected ETH_CI is transferred.

For example, in the case of 1:1 protection switching configuration, ETH_CI for the protected ETH can be forwarded to either working or protection transport entities by the instantiated ETH SNC protection switching process within the ETH_~~FF~~C.

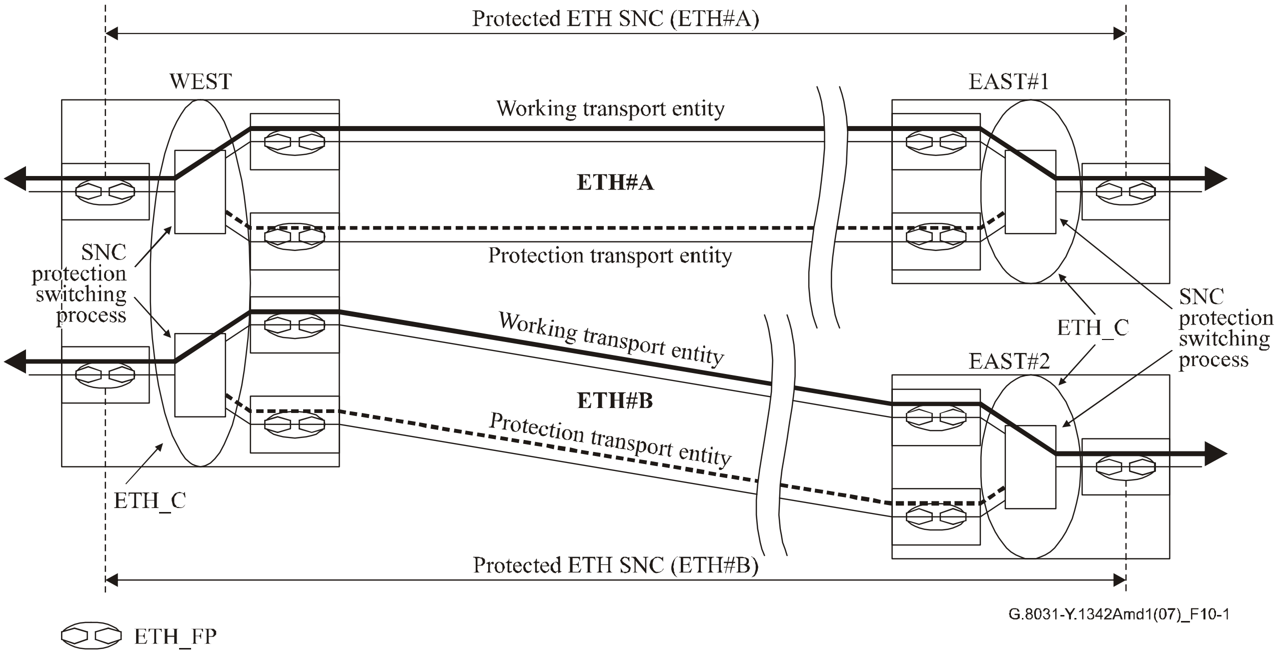


Figure 10-1 – ETH SNC/S protection switching architecture

Working and protection transport entities for a SNC protection switching process shall be configured via ETH_MI_PS_WorkingPortId and ETH_MI_PS_ProtectionPortId.

Since the protection switching mechanism requires monitoring for both working and protection transport entities, it is required that MEPs be activated for the purpose of monitoring the working and protection transport entities. Both transport entities are monitored by individually exchanging CCM defined in ITU-T Rec. Y.1731 as shown in Figure 10-2.

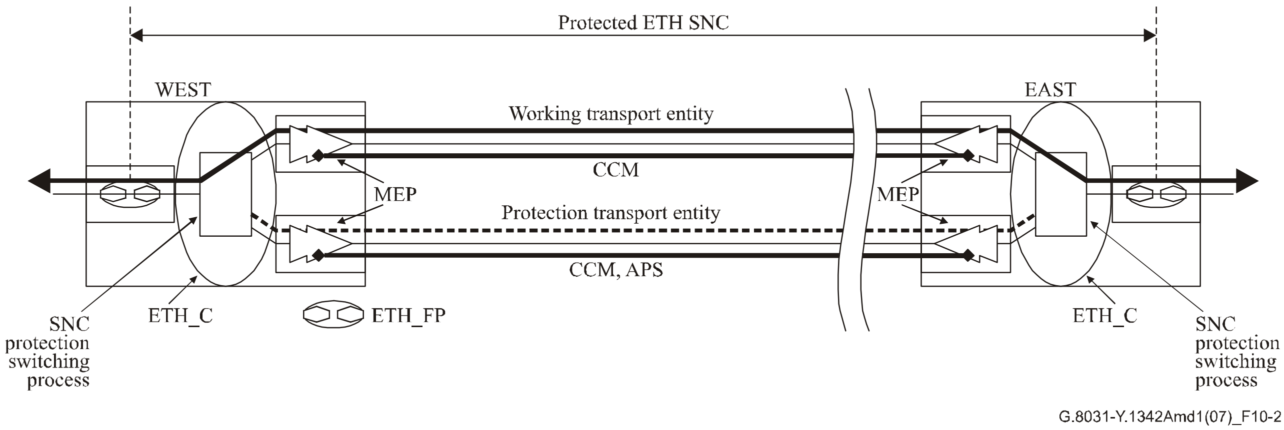


Figure 10-2 – MEPs in ETH SNC/S protection switching architecture

The protection switching process also requires APS communication in order to coordinate its switching behaviour with the other end of the protected domain if the protection switching architecture is not 1+1 unidirectional protection switching. APS PDU is transmitted and received between the same MEP pair on the protection transport entity where CCM is transmitted for the monitoring.

APS information and defect condition which are terminated/detected by MEP sink function can be input to the protection switching process as shown in Figure 10-3.

If an MEP detects an anomaly which contributes to a SF defect condition, it will inform the protection switching process that a failure condition has been detected. Termination of the CCM and LCK (which are defined in ITU-T Rec. Y.1731) is done by the ETH_FT atomic function. If the ETH_FT detects a failure condition, an ETH_AI_TSF is signalled to the ETH(x) to ETH adaptation sink (ETH(x)/ETH_A_Sk) which subsequently generates an ETH_CI_SSF. The ETH(x)/ETH adaptation function employs this ETH_CI_SSF to notify the ETH SNC protection switching process within ETH_~~FF~~C of the signal failure condition.

The APS PDU is terminated by the ETH(x)/ETH_A_Sk function within the MEP. The ETH(x)/ETH_A_Sk function then extracts the APS specific information from the received APS PDU, and then transfers it to the ETH SNC protection switching process as the APS characteristic information (ETH_CI_APS).

The protection switching process determines the new switching state after it receives ETH_CI_SSF or ETH_CI_APS, and then it determines the specific output ETH_FP over which the protected ETH_CI is transferred as necessary.

It is noted that the administrative state of the ETH(x)/ETH adaptation function for both working and protection transport entities shall not be locked.

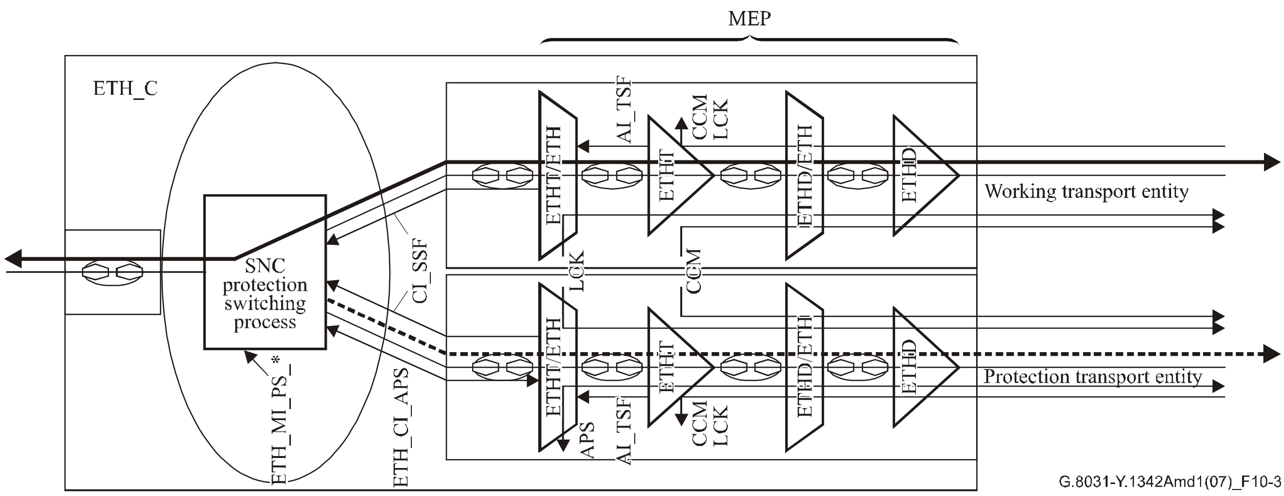


Figure 10-3 – Behaviours of both MEPs and SNC protection switching process in ETH SNC/S protection switching architecture

SNC/S protection is not only limited to subnetwork connections; it is also possible to extend this protection mechanism to support a single link connection as well as network connections.

10.6.1 1+1 bidirectional protection switching

Figure 10-4 illustrates the 1+1 bidirectional linear protection switching architecture. The protected ETH_CI traffic is permanently bridged to both the working transport entity and the protection transport entity. In this figure, the traffic is shown as being received via the ETH_~~FF~~C only from the working entity. Figure 10-5 illustrates a situation where a protection switching has occurred due to a signal fail condition on the working transport entity. It should be noted that both directions are switched even when a unidirectional defect occurs. For this purpose, APS coordination protocol is necessary.

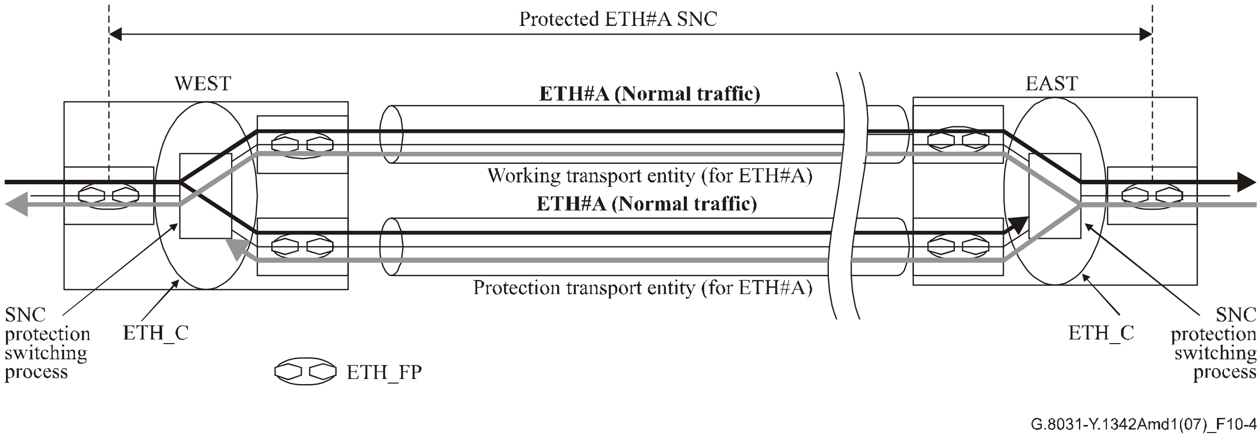


Figure 10-4 – 1+1 bidirectional protection switching architecture

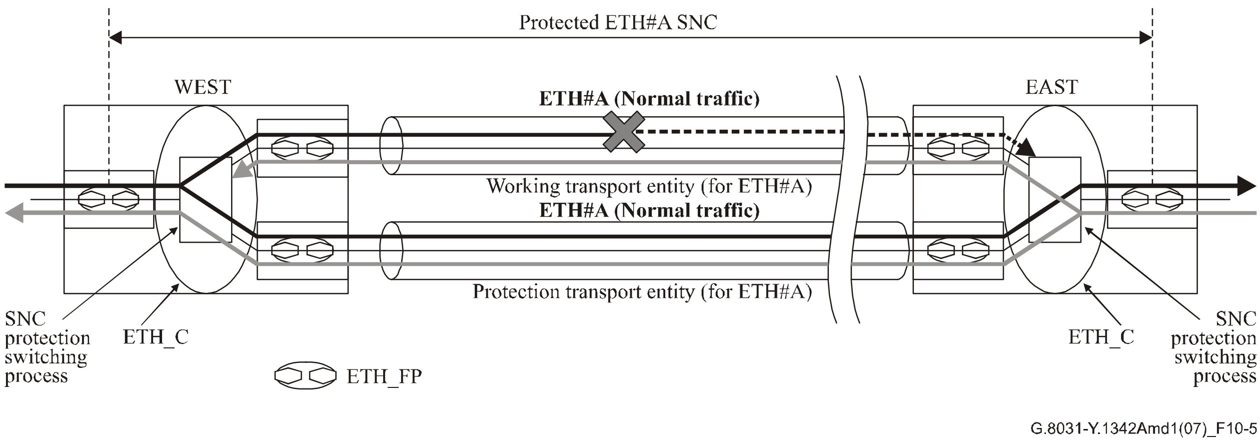


Figure 10-5 – 1+1 bidirectional protection switching architecture – Signal fail condition for working entity

10.6.2 1+1 unidirectional protection switching

Figure 10-6 illustrates the 1+1 unidirectional linear protection switching architecture. The protected ETH_CI traffic is permanently bridged to both the working transport entity and the protection transport entity. In this figure, the traffic is shown as being received via the ETH_~~FF~~C only from the working entity for both directions. Figure 10-7 illustrates a situation where a protection switching has occurred due to a signal fail condition on the working transport entity in the West-to-East direction. The normal traffic in the East-to-West direction continues to be received via the working transport entity. In unidirectional protection switching, each direction is switched independently. Selectors at the sink of the protected domain operate only based on the local information. For this purpose, APS coordination protocol is not necessary.

Figure 10-8 illustrates a case where signal fail condition exists on the working transport entity in the West-to-East direction and on the protection transport entity in the East-to-West direction. Unidirectional protection switching can protect this type of double defect scenarios while bidirectional protection switching cannot.

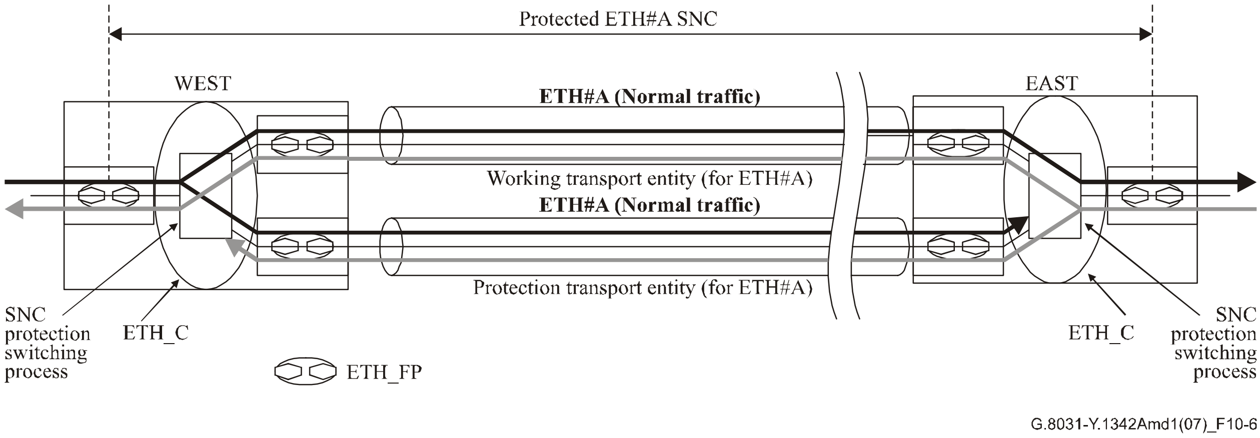


Figure 10-6 – 1+1 unidirectional protection switching architecture

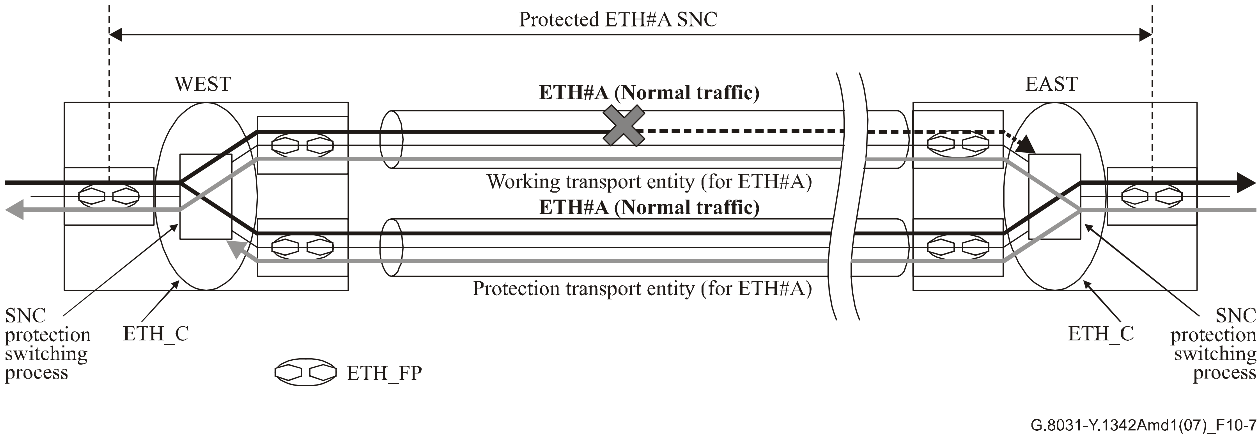


Figure 10-7 – 1+1 unidirectional protection switching architecture – Signal fail condition for working transport entity in the west-to-east direction

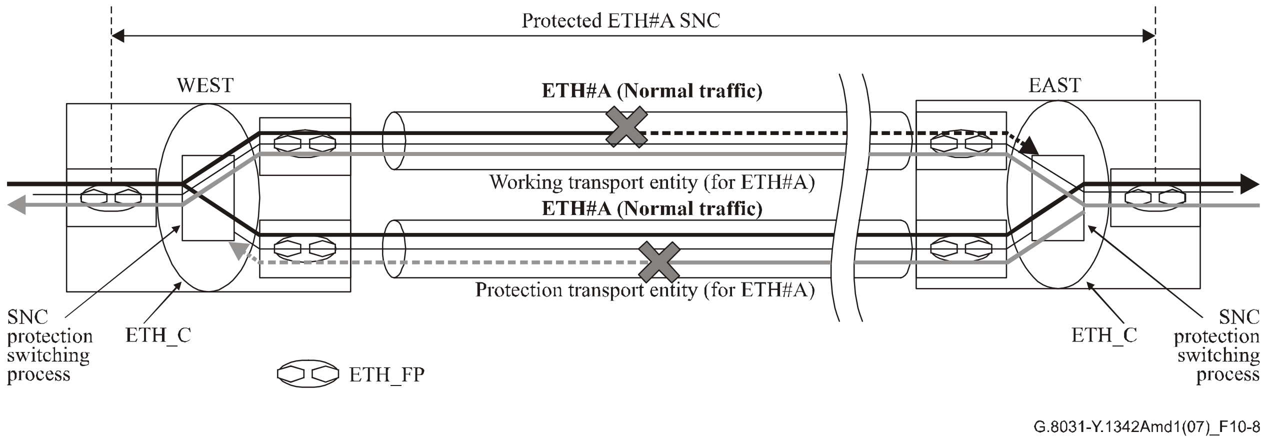


Figure 10-8 – 1+1 unidirectional protection switching architecture – Signal fail condition in both directions

10.6.3 1:1 bidirectional protection switching

Figure 10-9 illustrates the 1:1 linear protection switching architecture, with the normal traffic (ETH#A) being transmitted via the working transport entity. Although both the working and protection transport entities for ETH#A can be used by any other ETH traffic, the ETH SNC protection switching process only determines the specific output ETH_FP over which the protected ETH_CI for ETH#A is transferred if the protection switching is only established for ETH#A.

Figure 10-10 illustrates a situation where a protection switch has occurred, due to a signal fail condition on the working transport entity. At the source node, the normal traffic (ETH#A) is forwarded to the protection transport entity. At the sink node, the normal traffic (ETH#A) is received from the protection transport entity. During the protection switching operation, transient mismatch between bridge/selector positions at both ends of the protected domain is possible. However, misconnection between ETH_CI for ETH#A and other ETH_CI is not possible because traffic is always forwarded correctly through the ETH_~~FF~~C, based on the VID. Note that in order to achieve this forwarding behaviour, different VID must be configured on the protection transport entity for the protected ETH#A and the non-protected ETH traffic.

The forwarding of traffic according to the VID in the ETH_~~FF~~C function means that for 1:1 architectures, traffic misconnections are never possible. This greatly simplifies the functionality of the protection switching protocol, enabling a 1-phase protocol to be used, with only a single information exchange being required between both ends to complete a bidirectional switching.

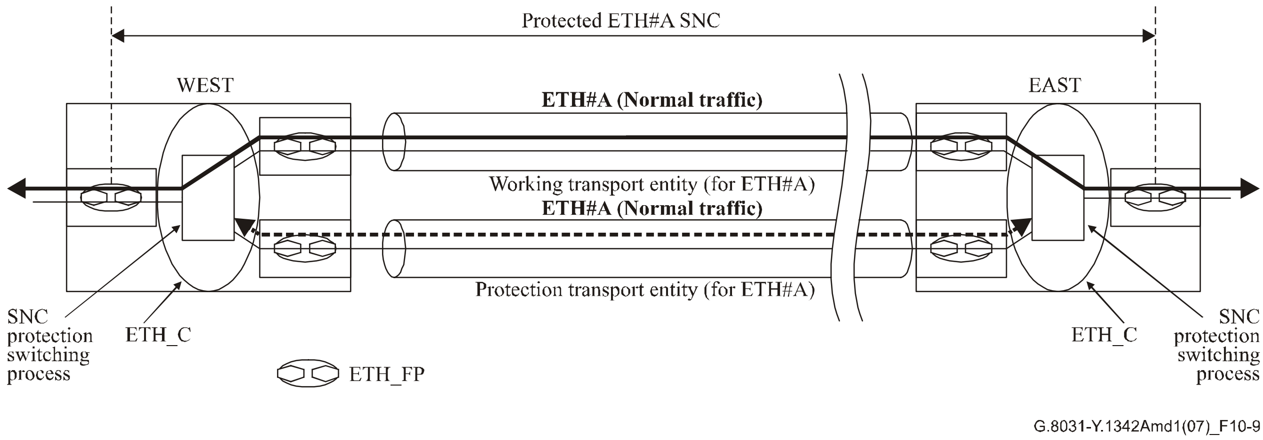


Figure 10-9 – 1:1 protection switching architecture

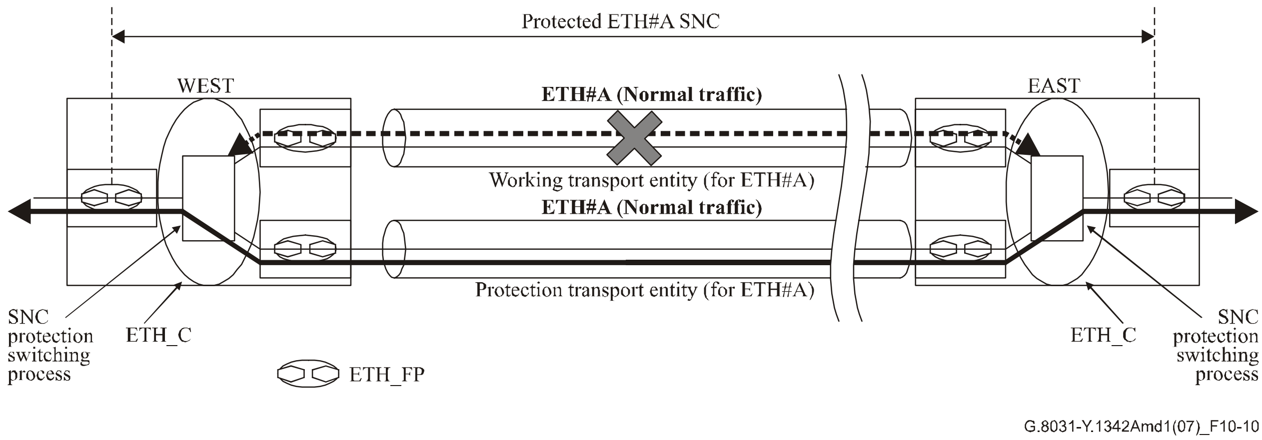


Figure 10-10 – 1:1 protection switching architecture – Signal Fail condition for working transport entity

9) Changes to clause 11, APS Protocol

9.1) Changes to clause 11.1, APS format

Modify the second bullet of the second paragraph and Table 11-1 as follows:

For other fields such as Version, OpCode, Flags and END TLV, the following values shall be used as defined in ITU-T Rec. Y.1731.

– **Version**: 0x00
– **OpCode**: 0x27 (=0d39)
– **Flags**: 0x00
– **END TLV**: 0x00

…

Table 11-1 describes code points and values for APS-specific information.

Table 11-1 – Code points and field values for APS-specific information

Request/State		1111	Lockout of Protection (LO)	Priority
		1110	Signal Fail for Protection (SF-P)	highest
		1101	Forced Switch (FS)	
		1011	Signal Fail for Working (SF)	
		1001	Signal Degrade (SD) (Note ~~1~~)	
		0111	Manual Switch (MS)	
		0101	Wait to Restore (WTR)	
		0100	Exercise (EXER)	
		0010	Reverse Request (RR) ~~(Note 2)~~	
		0001	Do Not Revert (DNR)	
		0000	No Request (NR)	lowest
		Others	Reserved for future international standardization	
Protection Type	A	0	No APS Channel	
		1	APS Channel	
	B	0	1+1 (Permanent Bridge)	
		1	1:1 (no Permanent Bridge)	
	D	0	Unidirectional switching	
		1	Bidirectional switching	
	R	0	Non-revertive operation	
		1	Revertive operation	
Requested Signal		0	Null Signal	
		1	Normal Traffic Signal	
		2-255	(Reserved for future use)	
Bridged Signal		0	Null Signal	
		1	Normal Traffic Signal	
		2-255	(Reserved for future use)	
NOTE ~~1~~ – SD is for further study. ~~NOTE 2 – RR is reserved for future standardization by ITU-T.~~				

9.2) Changes to clause 11.2, 1-phase APS protocol

9.2.1) Changes to clause 11.2.1, Principle of operation

Modify the fourth paragraph and Figure 11-3 as follows:

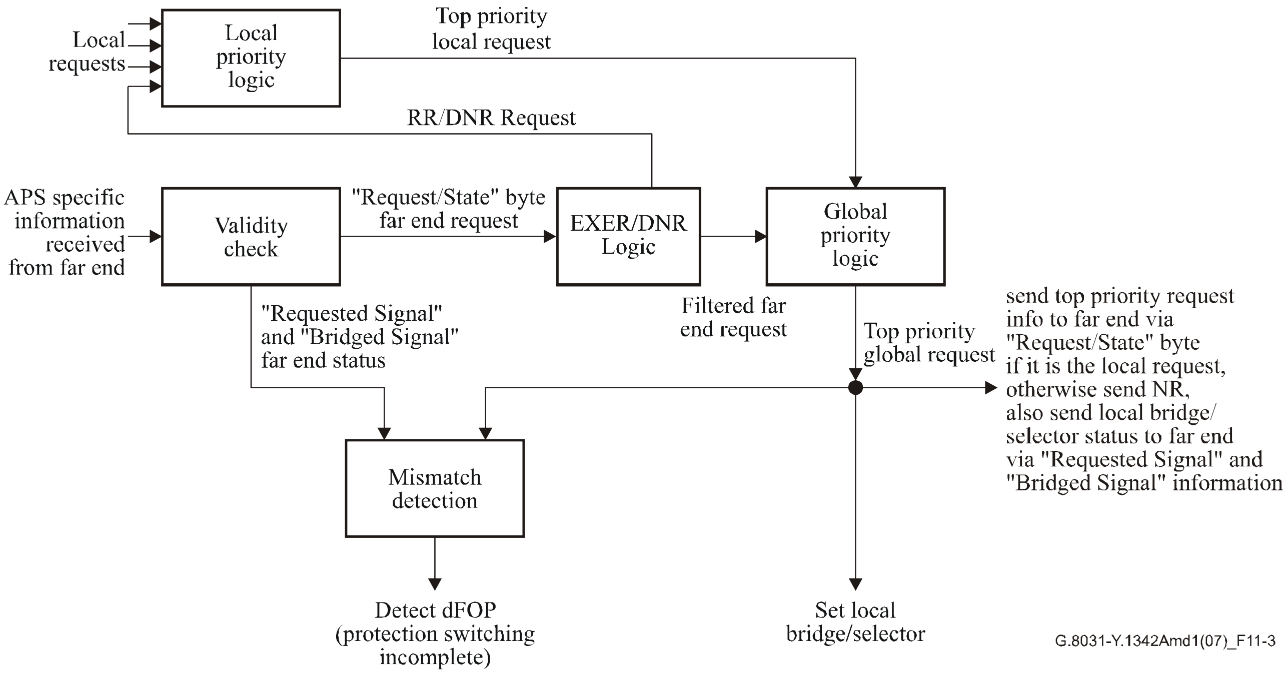


Figure 11-3 – Principle of 1+1/1:1 linear protection switching algorithm

In detail, the functionality is as follows (see Figure 11-3):

At the local network element, one or more local protection switching requests (as listed in 9.1 and 9.2) may be active. The "local priority logic" determines which of these requests is of top priority, using the order of priority given in Table 11-1. This top priority local request information is passed on to the "global priority logic".

The local network element receives information from the network element of the far end via the APS-specific information. The received APS-specific information is subjected to a validity check (see 11.2.4). The information of the received "Request/State" information (which indicates the top priority local request of the far end) is then passed on to the "EXER/DNR logic". If the received "Request/State" information is EXER, DNR or RR, then it is filtered by "EXER/DNR logic". "EXER/DNR logic" then generates RR local request if the received "Request/State" information is EXER, or generates DNR if the received "Request/State" information is DNR. The generated local request is then passed to "local priority logic". If the received "Request/State" information is none of EXER, DNR and RR, it is simply passed to the "global priority logic". The "global priority logic" compares the top priority local request with the request of the received "Request/State" information (according to the order of priority of Table 11-1) to determine the top priority global request. If the top priority global request is the local request, it will be indicated in "Request/State" field, otherwise "NR" will be indicated. The top priority global request will be exactly the same as the top priority local request in the case of unidirectional protection switching because the received "Request/State" information should not affect the operation of the unidirectional protection switching. This request then determines the bridge/selector position (or status) of the local network element as follows:

9.2.2) Changes to clause 11.2.2, Revertive mode

Modify all paragraphs in clause 11.2.2 as follows:

In revertive mode of unidirectional protection switching operation, in conditions where working traffic is being received via the protection entity, if local protection switching requests (see

Figure 11-3) have been previously active and now become inactive, a local wait-to-restore state is entered. Since this state now represents the highest priority local request, it is indicated on the transmitted "Request/State" information and maintains the switch.

~~This state normally times out and becomes a no request state after the wait-~~In the case of bidirectional protection switching, a local wait-to-~~restore timer has expired. The wait-~~restore state is entered only when there is no higher priority of request received from the far end than that of the wait-to-restore state.

This state normally times out and becomes a no request state after the wait-to-restore timer has expired. The wait-to-restore timer is deactivated earlier if any local request of higher priority pre-empts this state.

~~Note that for the decision of whether or not to enter the wait-to-restore state, only local requests are considered.~~ A switch to the protection entity may be maintained by a local wait-to-restore state or by a remote request (wait-to-restore or other) received via the "Request/State" information. Therefore, in a case where a bidirectional failure for a working entity has occurred and subsequent repair has taken place, the bidirectional reversion back to the working entity does not take place until both wait-to-restore timers at both ends have expired.

9.2.3) Changes to clause 11.2.3, Non-revertive mode

Modify text in clause 11.2.3 as follows:

In non-revertive mode of unidirectional protection switching operation, in conditions where working traffic is being transmitted via the protection entity, if local protection switching requests (see Figure 11-3) have been previously active and now become inactive, a local "do not revert state" is entered. Since this state now represents the highest priority local request, it is indicated on the transmitted "Request/State" information and maintains the switch, thus preventing reversion back to the released bridge/selector position in non-revertive mode under no request conditions.

In the case of bidirectional protection switching operation, a local do not revert state is entered only when there is no higher priority of request received from the far end than that of the do not revert state.

9.2.4) Changes to clause 11.2.4, Transmission and acceptance of APS

Modify the third paragraph in clause 11.2.4 as follows:

The first three APS frames should be transmitted as fast as possible ~~after~~ only if ~~the status change of the protection end point~~APS information to be transmitted has been changed so that fast protection switching is possible even if one or two APS frames are lost or corrupted. For the fast protection switching in 50 ms, the interval of the first three APS frames ~~is desirable to~~ should be 3.3 ms, which is the same interval as CCM frames for fast defect detection. APS frames after the first three frames should be transmitted with the interval of 5 seconds.

9.3) Changes to clause 11.3, Request type

Modify text in clause 11.3 as follows:

The request types ~~that may be reflected in the APS-specific information are the "standard" types traditionally supported by protection switching for SONET and SDH. These requests~~ reflect the highest priority condition, command, or state. 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 communication, otherwise NR will be indicated. In 1-phase APS protocol, the near end will ~~never~~ signal Reverse Request ~~even when~~only in response to an EXER command from the far end ~~request has the highest priority~~.

9.4) Changes to clause 11.4, Protection types

Add the following sentence at the end of clause 11.4:

The Protection Type of a SNC protection switching process shall be configured via ETH_MI_PS_ProtType.

9.5) Changes to clause 11.11, Command acceptance and retention

Add the following sentence at the end of clause 11.11:

Each external command shall be input to a SNC protection switching process via ETH_MI_PS_ExtCMD.

9.6) Changes to clause 11.12, Hold-off timer

Modify the last paragraph and add a sentence at the end of clause 11.12 as follows:

~~The operation of the hold-off timer uses the "peek twice" method specified in SDH standards. Specifically, w~~When a new defect or more severe defect occurs (new SF (or SD if applicable)), this event will not be reported immediately to protection switching if the provisioned hold-off timer value is non-zero. Instead, the hold-off timer will be started. When the hold-off timer expires, it will be checked whether a defect still exists on the trail that started the timer. If it does, that defect will be reported to protection switching. The defect need not be the same one that started the timer.

The hold-off timer of a SNC protection switching process shall be configured via ETH_MI_PS_HoTime.

9.7) Changes to clause 11.13, Wait-to-restore timer

Modify the last paragraph and add a sentence at the end of clause 11.13 as follows:

In revertive mode of operation, when the protection is no longer requested, i.e., the failed working transport entity is no longer in SF (or SD if applicable) condition (and assuming no other requesting transport entities), a local wait-to-restore state will be activated. Since this state becomes the highest in priority, it is indicated on the APS signal (if applicable), and maintains the normal traffic signal from the previously failed working transport entity on the protection transport entity. This state shall normally time out and become a no request ~~null signal~~ state. The wait-to-restore timer deactivates earlier when any request of higher priority pre-empts this state.

The wait-to-restore timer of a SNC protection switching process shall be configured via ETH_MI_PS_WTR.

9.8) Changes to clause 11.14, Exercise operation

Modify the second paragraph in clause 11.14 as follows:

Exercise command shall issue the command with the same requested and bridged signal numbers of the NR, RR or DNR request that it replaces. In 1-phase APS protocol, the valid response will be an ~~NR~~ RR with the corresponding requested and bridged signal numbers. When Exercise commands are input at both ends, an EXER, instead of RR, is transmitted from both ends. The standard response to DNR should be DNR rather than NR. When the exercise command is cleared, it will be replaced with NR or RR if the requested signal number is 0, and DNR or RR if the requested~~for normal traffic~~ signal number is 1.

9.9) Changes to clause 11.15, Failure of protocol defects

Modify clause 11.15 as follows:

~~Entry and exit criteria for Failure of Protocol defects (dFOP) for APS protocol defined in this Recommendation are described in Table 11-2.~~

~~Table 11-2/G.8031/Y.1342 – Entry/Exit criteria for dFOP~~

~~Fully incompatible provisioning (the "B" bit mismatch)~~	
~~Entry criteria~~	~~Reception of three APS frames with the incompatible "B" bit value during the period of 22.5 seconds.~~
~~Exit criteria~~	~~Reception of the first APS frame with a compatible "B" bit value.~~
~~Protection switching incomplete~~	
~~Entry criteria~~	~~If the transmitted "Requested Signal" and received "Bridged Requested Signal" do not match for a period of 50 ms or longer.~~
~~Exit criteria~~	~~Reception of the first APS frame which indicates the same "BridgedRequested Signal" value with the transmitted "Requested Signal" value.~~
~~Working/Protection configuration mismatch~~	
~~Entry criteria~~	~~Reception of three APS frames from the working transport entity during the period of 22.5 seconds.~~
~~Exit criteria~~	~~If no APS frame is received from the working transport entity during the period of 22.5 seconds.~~
~~NOTE – 22.5 seconds enables the reception of three APS frames even if two APS frames are lost.~~	

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

– Fully incompatible provisioning (the "B" bit mismatch, described in clause 11.4).

– Working/Protection configuration mismatch (described in clause 11.2.4).

– Lack of response to a bridge request (i.e., no match in sent "Requested Signal" and received "Requested Signal") for > 50 ms.

Fully incompatible provisioning and working/protection configuration mismatch are detected by receiving only one APS frame. Detection and clearance of "Failure of Protocol" defects are defined in ITU-T Rec. G.8021/Y.1341.

If an unknown request or a request for an invalid signal number is received, it will be ignored.

10) Changes to Annex A, State transition tables of protection switching

10.1) Changes to Annex A.1.1, Local requests

Modify Table A.1 as follows:

Table A.1 – State transition by local requests (1:1 bidirectional, revertive mode)

State		Signalled APS	Local request a	b	c	d	e	f	g	h	i	j
			Lockout	**Forced switch**	**~~Signal~~F ~~fail~~ on working**	**Working recovers from SF**	**~~Signal~~F ~~fail~~ on protection**	**Protection recovers from SF**	**Manual switch**	**Clear**	**Exercise**	**WTR timer expires**
A	No Request Working/Active Protection/Standby	NR [r/b=null]	→C	→D	→E[a)]	N/A	→F	N/A	→G	~~O~~N/A	→I	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	(→B)[b)] or →E	O	→F	N/A	→G	~~O~~N/A	O	N/A
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	O	O	O	O	O	O	O	→A or →E[c)] →F[d)]	O	N/A
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→A or →E[c)]	O	N/A
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	~~O~~N/A	O	N/A
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b=null]	→C	O	O	O	N/A	→A	O	~~O~~N/A	O	N/A
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	O	→A	O	N/A
H	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	→A	O	→A

Table A.1 – State transition by local requests (1:1 bidirectional, revertive mode)

State		Signalled APS	Local request									
			a	b	c	d	e	f	g	h	i	j
			Lockout	Forced switch	S~~ignal~~F ~~fail~~ on working	Working recovers from SF	S~~ignal~~F ~~fail~~ on protection	Protection recovers from SF	Manual switch	Clear	Exercise	WTR timer expires
I	Exercise Working/Active Protection/Standby	EXER [r/b=null]	→C	→D	→E	N/A	→F	N/A	→G	→A	O	N/A
J	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→I	N/A

NOTE 1 – "N/A" means that the event ~~can~~ is not expected to happen for the State. However if it does happen, the event should be ignored.

NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.

NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.

a) It transits to the state E if the Signal Fail still exists after hold-off timer expires.

b) If FS is indicated in the received APS from the far end.

c) If SF is reasserted.

d) If SF-P is reasserted.

10.2) Changes to Annex A.1.2, Far end requests

Modify Table A.2 as follows:

Table A.2 – State transition by far end requests (1:1 bidirectional, revertive mode)

State		Signalled APS	Received far end request									
			k	l	m	n	o	p	q	r	s	t
			LO [r/b=null]	SF-P [r/b=null]	FS [r/b= normal]	SF [r/b= normal]	MS [r/b= normal]	WTR [r/b= normal]	EXER [r/b=null]	RR [r/b=null]	NR [r/b=null]	NR [r/b= normal]
A	No Request Working/Active Protection/Standby	NR [r/b=null]	(→A)	(→A)	→B	→B	→B	N/A	~~(~~→~~A~~J~~)~~	(→A)	(→A) or →E a) or →F b)	(→A)
B	No Request Working/Standby	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	(→B)	N/A	N/A	→A or →E a)	~~N/A~~→A

Table A.2 – State transition by far end requests (1:1 bidirectional, revertive mode)

State		Signalled APS	Received far end request									
			k	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**
			LO [r/b=null]	**SF-P [r/b=null]**	**FS [r/b= normal]**	**SF [r/b= normal]**	**MS [r/b= normal]**	**WTR [r/b= normal]**	**EXER [r/b=null]**	**RR [r/b=null]**	**NR [r/b=null]**	**NR [r/b= normal]**
	Protection/Active											
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	(→C)	O	O	O	O	O	O	O	O	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O	O
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b=null]	→A	(→F)	O	O	O	O	O	O	O	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O	O
H	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→A	→A	→B	→B	→B	(→H)	O	O	N/A	O
I	Exercise Working/Active Protection/Standby	EXER [r/b=null]	→A	→A	→B	→B	→B	N/A	(→I)	(→I)	O	N/A
J	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	→A	→A	→B	→B	→B	N/A	(→J)	→A	→A	N/A

NOTE 1 – "N/A" means that the event ~~can~~ is not expected to happen for the State. However if it does happen, the event should be ignored.

NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.

NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.

[a] If SF is reasserted.

[b] If SF-P is reasserted.

10.3) Changes to Annex A.2.1, Local requests

Modify Table A.3 as follows:

Table A.3 – State transition by local requests (1:1 bidirectional, non-revertive mode)

State		Signalled APS	Local request								
			a	b	c	d	e	f	g	h	i
			Lockout	Forced switch	SF~~ignal fail~~ on working	Working recovers from SF	SF~~ignal fail~~ on protection	Protection recovers from SF	Manual switch	Clear	Exercise
A	No Request Working/Active Protection/Standby	NR [r/b=null]	→C	→D	→E[a)]	N/A	→F	N/A	→G	~~O~~N/A	→I
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	(→B)[b)] or →E	N/A	→F	N/A	→G	~~O~~N/A	O
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	O	O	O	O	O	O	O	→A or →E[c)] →F[d)]	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→~~J~~H or →E[c)]	O
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	~~O~~N/A	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b=null]	→C	O	O	O	N/A	→A	O	~~O~~N/A	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	O	→H	O
H	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	~~O~~N/A	→J
I	Exercise Working/Active Protection/Standby	EXER [r/b=null]	→C	→D	→E	N/A	→F	N/A	→G	→A	O
J	Exercise Working/Standby Protection/Active	EXER [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	→H	O
K	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→I

Table A.3 – State transition by local requests (1:1 bidirectional, non-revertive mode)

State		Signalled APS	Local request a Lockout	b Forced switch	c SF~~ignal fail~~ on working	d Working recovers from SF	e SF~~ignal fail~~ on protection	f Protection recovers from SF	g Manual switch	h Clear	i Exercise
L	Reverse Request Working/Standby Protection/Active	RR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→J

NOTE 1 – "N/A" means that the event ~~can~~is not expected to happen for the State. However if it does happen, the event should be ignored.
NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.
NOTE 3 – "(→**X**)" represents that the state is not changed and remains the same state.
a) It transits to the state E if the Signal Fail still exists after hold-off timer expires.
b) If FS is indicated in the received APS from the far end.
c) If SF is reasserted.
d) If SF-P is reasserted.

10.4) Changes to Annex A.2.2, Far end requests

Modify Table A.4 as follows:

Table A.4 – State transition by far end requests (1:1 bidirectional, non-revertive mode)

State		Signalled APS	Received far end request ~~k~~j LO [r/b=null]	~~l~~k SF-P [r/b=null]	~~m~~l FS [r/b=normal]	~~n~~m SF [r/b=normal]	~~o~~n MS [r/b=normal]	~~q~~o EXER [r/b=null]	~~r~~p EXER [r/b=normal]	q RR [r/b= null]	r RR [r/b=normal]	s NR [r/b=null]	t NR [r/b=normal]	u DNR [r/b=normal]
A	No Request Working/Active Protection/Standby	NR [r/b=null]	(→A)	(→A)	→B	→B	→B	~~(→A~~K~~)~~	N/A	(→A)	N/A	(→A) or →E[a)] or →F[b)]	(→A)	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	N/A	~~(→B)~~N/A	N/A	N/A	→A or →E[a)]	N/A	~~(→B~~H~~)~~
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	(→C)	O	O	O	O	O	O	O	O	O	O	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O	O	O	O

Table A.4 – State transition by far end requests (1:1 bidirectional, non-revertive mode)

State		Signalled APS	Received far end request											
			~~k~~j	~~l~~k	~~m~~l	~~n~~m	~~o~~n	~~q~~o	~~r~~p	q	r	s	t	u
			LO [r/b=null]	**SF-P [r/b=null]**	**FS [r/b= normal]**	**SF [r/b= normal]**	**MS [r/b= normal]**	**EXER [r/b=null]**	**EXER [r/b= normal]**	**RR [r/b= null]**	**RR [r/b= normal]**	**NR [r/b=null]**	**NR [r/b= normal]**	**DNR [r/b= normal]**
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O	O	O	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/b=null]	→A	(→F)	O	O	O	O	O	O	O	O	O	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O	O	O	O
H	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→A	→A	→B	→B	→B	N/A	~~(→H~~L~~)~~	N/A	(→H)	O	O	(→H)
I	Exercise Working/Active Protection/Standby	EXER [r/b=null]	→A	→A	→B	→B	→B	(→I)	N/A	(→I)	N/A	O	~~O~~N/A	N/A
J	Exercise Working/Standby Protection/Active	EXER [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→J)	N/A	(→J)	~~O~~N/A	O	O
K	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	→A	→A	→B	→B	→B	(→K)	N/A	→A	N/A	→A	N/A	N/A
L	Reverse Request Working/Standby Protection/Active	RR [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→L)	N/A	→H	N/A	N/A	→H

NOTE 1 – "N/A" means that the event ~~can~~is not expected to happen for the State. However if it does happen, the event should be ignored.

NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.

NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.

a) If SF is reasserted.

b) If SF-P is reasserted.

10.5) Changes to Annex A.3.1, Local requests

Modify Table A.5 as follows:

Table A.5 – State transition by local requests (1+1 bidirectional, revertive mode)

	State	Signalled APS	Local request									
			a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**
			Lockout	**Forced switch**	**SF on working**	**Working recovers from SF**	**~~SD~~ SF on protection**	**Protection recovers from SF**	**Manual switch**	**Clear**	**Exercise**	**WTR timer expires**
A	No Request Working/Active Protection/Standby	NR [r~~/b~~=null, b=~~/~~normal]	→C	→D	→E[a)]	N/A	→F	N/A	→G	~~O~~N/A	→I	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	(→B)[b)] or →E	O	→F	N/A	→G	~~O~~N/A	O	N/A
C	Lockout Working/Active Protection/Standby	LO [r~~/b~~=null, b=~~/~~normal]	O	O	O	O	O	O	O	→A or → E[c)] →F[d)]	O	N/A
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→A or →E[c)]	O	N/A
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	~~O~~N/A	O	N/A
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r~~/b~~=null, b=~~/~~normal]	→C	O	O	O	N/A	→A	O	~~O~~N/A	O	N/A
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	O	→A	O	N/A
H	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	→A	O	→A
I	Exercise Working/Active Protection/Standby	EXER [r~~/b~~=null, b=~~/~~normal]	→C	→D	→E	N/A	→F	N/A	→G	→A	O	N/A
L	Reverse Request Working/Active Protection/Standby	RR [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→I	N/A

Table A.5 – State transition by local requests (1+1 bidirectional, revertive mode)

NOTE 1 – "N/A" means that the event ~~can~~is not expected to happen for the State. However if it does happen, the event should be ignored. NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority. NOTE 3 – "(→X)" represents that the state is not changed and remains the same state. a) It transits to the state E if the Signal Fail still exists after hold-off timer expires. b) If FS is indicated in the received APS from the far end. c) If SF is reasserted. d) If SF-P is reasserted.

10.6) Changes to Annex A.3.2, Far end requests

Modify Table A.6 as follows:

Table A.6 – State transition by far end requests (1+1 bidirectional, revertive mode)

State		Signalled APS	Received far end request									
			k	l	m	n	o	p	q	r	~~r~~s	~~s~~t
			LO [r~~/b~~=-null, b=~~/~~normal]	SF-P [r~~/b~~=-null, b=~~/~~normal]	FS [r/b=normal]	SF [r/b=normal]	MS [r/b=normal]	WTR [r/b=normal]	EXER [r~~/b~~=-null, b=~~/~~normal]	RR [r~~/b~~=-null, b=~~/~~normal]	NR [r~~/b~~=-null, b=~~/~~normal]	NR [r/b=normal]
A	No Request Working/Active Protection/Standby	NR [r~~/b~~=null, b=~~/~~normal]	(→A)	(→A)	→B	→B	→B	N/A	(→A)	(→A)	(→A) or →E a) or →F b)	(→A)
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	~~(→A)~~	(→B)	(→B)	(→B)	(→B)	N/A	N/A	→ A or →E a)	~~N/A~~→A
C	Lockout Working/Active Protection/Standby	LO [r~~/b~~=null, b=~~/~~normal]	(→C)	O	O	O	O	O	O	O	O	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O	O
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r~~/b~~=null, b=~~/~~normal]	→A	(→F)	O	O	O	O	O	O	O	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O	O

Table A.6 – State transition by far end requests (1+1 bidirectional, revertive mode)

State		Signalled APS	Received far end request									
			k	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**~~r~~s**	**~~s~~t**
			LO [r~~/b~~=null, b=~~/~~normal]	**SF-P [r~~/b~~=null, b=~~/~~normal]**	**FS [r/b=normal]**	**SF [r/b=normal]**	**MS [r/b=normal]**	**WTR [r/b=normal]**	**EXER [r~~/b~~=null, b=~~/~~normal]**	**RR [r~~/b~~=null, b=~~/~~normal]**	**NR [r~~/b~~=null, b=~~/~~normal]**	**NR [r/b=normal]**
H	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→A	→A	→B	→B	→B	(→H)	O	O	N/A	O
I	Exercise Working/Active Protection/Standby	EXER [r~~/b~~=null, b=~~/~~normal]	→A	→A	→B	→B	→B	N/A	(→I)	(→I)	O	N/A
J	Reverse Request Working/Active Protection/Standby	RR [r=null, b=normal]	→A	→A	→B	→B	→B	N/A	(→J)	→A	→A	N/A

NOTE 1 – "N/A" means that the event ~~can~~is not expected to happen for the State. However if it does happen, the event should be ignored.

NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.

NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.

a) If SF is reasserted.

b) If SF-P is reasserted.

10.7) Changes to Annex A.4.1, Local requests

Modify Table A.7 as follows:

Table A.7 – State transition by local requests (1+1 bidirectional, non-revertive mode)

State		Signalled APS	Local request								
			a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**
			Lockout	**Forced switch**	**SF~~ignal fail~~ on working**	**Working recovers from SF**	**SF~~ignal fail~~ on protection**	**Protection recovers from SF**	**Manual switch**	**Clear**	**Exercise**
A	No Request Working/Active Protection/Standby	NR [r~~/b~~=null, b=~~/~~normal]	→C	→D	→E a)	N/A	→F	N/A	→G	~~O~~N/A	→I
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	(→B) b) or →E	N/A	→F	N/A	→G	~~O~~N/A	O
C	Lockout Working/Active Protection/Standby	LO [r~~/b~~= null, b=~~/~~normal]	O	O	O	O	O	O	O	→A or →E c) →F d)	O

Table A.7 – State transition by local requests (1+1 bidirectional, non-revertive mode)

State		Signalled APS	Local request a Lockout	b Forced switch	c S~~ignal~~F ~~fail~~ on working	d Working recovers from SF	e S~~ignal~~F ~~fail~~ on protection	f Protection recovers from SF	g Manual switch	h Clear	i Exercise
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	→H or →E[c)]	O
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→H	→F	N/A	O	~~O~~N/A	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r~~/b~~= null, b=~~/~~normal]	→C	O	O	O	N/A	→A	O	~~O~~N/A	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	O	→H	O
H	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→J
I	Exercise Working/Active Protection/Standby	EXER [r~~/b~~=null, b=~~/~~normal]	→C	→D	→E	N/A	→F	N/A	→G	→A	O
J	Exercise Working/Standby Protection/Active	EXER [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	→H	O
K	Reverse Request Working/Active Protection/Standby	RR [r/b=null/normal]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→I
L	Reverse Request Working/Standby Protection/Active	RR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→G	N/A	→J

NOTE 1 – "N/A" means that the event ~~can~~is not expected to happen for the State. However if it does happen, the event should be ignored.

NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.

NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.

a) It transits to the state E if the Signal Fail still exists after hold-off timer expires.

b) If FS is indicated in the received APS from the far end.

c) If SF is reasserted.

d) If SF-P is reasserted.

10.8) Changes to Annex A.4.2, Far end requests

Modify Table A.8 as follows:

Table A.8 – State transition by far end requests (1+1 bidirectional, non-revertive mode)

State		Signalled APS	Received far end request											
			~~k~~j	~~l~~k	~~m~~l	~~n~~m	~~o~~n	~~q~~o	~~r~~p	q	r	s	t	u
			LO [r/~~b~~= null~~,~~ b=~~/~~normal]	SF-P [r/~~b~~= null~~,~~ b=~~/~~normal]	FS [r/b= normal]	SF [r/b= normal	MS [r/b= normal]	EXER [r/~~b~~= null~~,~~ b=~~/~~normal]	EXER [r/b= normal]	RR [r=null, b=normal]	RR [r/b= normal]	NR [r/~~b~~= null~~,~~ b=~~/~~normal]	NR [r/b= normal]	DNR [r/b= normal]
A	No Request Working/Active Protection/Standby	NR [r/~~b~~=null~~,~~ b=~~/~~normal]	(→A)	(→A)	→B	→B	→B	~~(→A~~K~~)~~	N/A	(→A)	N/A	(→A) or →E[a)] or →F[b)]	(→A)	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	N/A	~~(→B~~N/A~~)~~	N/A	N/A	→A or→E[a)]	N/A	~~(→B~~H~~)~~
C	Lockout Working/Active Protection/Standby	LO [r/~~b~~= null~~,~~ b=~~/~~normal]	(→C)	O	O	O	O	O	O	O	O	O	O	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→A	→A	(→D)	O	O	O	O	O	O	O	O	O
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→A	→A	→B	(→E)	O	O	O	O	O	O	O	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r/~~b~~= null~~,~~ b=~~/~~normal]	→A	(→F)	O	O	O	O	O	O	O	O	O	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→A	→A	→B	→B	(→G)	O	O	O	O	O	O	O
H	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→A	→A	→B	→B	→B	N/A	~~(→H~~L~~)~~	N/A	(→H)	O	O	(→H)
I	Exercise Working/Active Protection/Standby	EXER [r/~~b~~=null~~,~~ b=~~/~~normal]	→A	→A	→B	→B	→B	(→I)	N/A	(→I)	N/A	O	~~O~~N/A	N/A
J	Exercise Working/Standby Protection/Active	EXER [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→J)	N/A	(→J)	~~O~~N/A	O	O
K	Reverse Request Working/Active Protection/Standby	RR [r/b=null/normal]	→A	→A	→B	→B	→B	(→K)	N/A	→A	N/A	→A	N/A	N/A

Table A.8 – State transition by far end requests (1+1 bidirectional, non-revertive mode)

State		Signalled APS	Received far end request											
			~~k~~j	~~l~~k	~~m~~l	~~n~~m	~~o~~n	~~q~~o	~~r~~p	q	r	s	t	u
			LO [r~~/b~~= null~~,~~ b=~~/~~normal]	**SF-P [r~~/b~~= null~~,~~ b=~~/~~normal]**	**FS [r/b= normal]**	**SF [r/b= normal**	**MS [r/b= normal]**	**EXER [r~~/b~~= null~~,~~ b=~~/~~normal]**	**EXER [r/b= normal]**	**RR [r=null, b=normal]**	**RR [r/b= normal]**	**NR [r~~/b~~= null~~,~~ b=~~/~~normal]**	**NR [r/b= normal]**	**DNR [r/b= normal]**
L	Reverse Request Working/Standby Protection/Active	RR [r/b=normal]	→A	→A	→B	→B	→B	N/A	(→L)	N/A	→H	N/A	N/A	→H

NOTE 1 – "N/A" means that the event ~~can~~ is not expected to happen for the State. However if it does happen, the event should be ignored.
NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.
NOTE 3 – "(→X)" represents that the state is not changed and remains the same state.
a) If SF is reasserted.
b) If SF-P is reasserted.

10.9) Changes to Annex A.5.1, Local requests

Modify Table A.9 as follows:

Table A.9 – State transition by local requests (1+1 unidirectional, revertive mode)

State		Local request									
		a	b	c	d	e	f	g	h	i	j
		Lockout	**Forced switch**	**Signal fail on working**	**Working recovers from SF**	**Signal fail on protection**	**Protection recovers from SF**	**Manual switch**	**Clear**	**Exercise**	**WTR timer expired**
A	No Request Working/Active Protection/Standby	→B	→C	→D a)	N/A	→E	N/A	→F	O	N/A	N/A
B	Lockout Working/Active Protection/Standby	O	O	O	O	O	O	O	→A or →D b) →E c)	N/A	N/A
C	Forced Switch Working/Standby Protection/Active	→B	O	O	O	→E	N/A	O	→A or →D c)	N/A	N/A
D	Signal Fail (W) Working/Standby Protection/Active	→B	→C	N/A	→G	→E	N/A	O	O	N/A	N/A

Table A.9 – State transition by local requests (1+1 unidirectional, revertive mode)

State		Local request									
		a	b	c	d	e	f	g	h	i	j
		Lockout	**Forced switch**	**Signal fail on working**	**Working recovers from SF**	**Signal fail on protection**	**Protection recovers from SF**	**Manual switch**	**Clear**	**Exercise**	**WTR timer expired**
E	Signal Fail (P) Working/Active Protection/Standby	→B	O	O	O	N/A	→A	O	O	N/A	N/A
F	Manual Switch Working/Standby Protection/Active	→B	→C	→D	N/A	→E	N/A	O	→A	N/A	N/A
G	Wait to Restore Working/Standby Protection/Active	→B	→C	→D	N/A	→E	N/A	→F	→A	N/A	→A

NOTE 1 – "N/A" means that the event ~~can~~ is not expected to happen for the State. However if it does happen, the event should be ignored.

NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.

[a] It transits to the state D if the Signal Fail still exists after hold-off timer expires.

[b] If SF is reasserted.

[c] If SF-P is reasserted.

10.10) Changes to Annex A.6, Local requests

Modify Table A.10 as follows:

Table A.10 – State transition by local requests (1+1 unidirectional, non-revertive mode)

State		Local request								
		a	**b**	**c**	**d**	**e**	**f**	**g**	**i**	**j**
		Lockout	**Forced switch**	**SF on working**	**Working recovers from SF**	**SF on protection**	**Protection recovers from SF**	**Manual switch**	**Clear**	**Exercise**
A	No Request Working/Active Protection/Standby	→B	→C	→D[a]	N/A	→E	N/A	→F	O	N/A
B	Lockout Working/Active Protection/Standby	O	O	O	O	O	O	O	→A or →D[b] →E[c]	N/A
C	Forced Switch Working/Standby Protection/Active	→B	O	O	O	→E	N/A	O	→G or →D[b]	N/A
D	Signal Fail (W) Working/Standby Protection/Active	→B	→C	N/A	→G	→E	N/A	O	O	N/A
E	Signal Fail (P) Working/Active Protection/Standby	→B	O	O	O	N/A	→A	O	O	N/A
F	Manual Switch Working/Standby Protection/Active	→B	→C	→D	N/A	→E	N/A	O	→G	N/A
G	Do Not Revert Working/Standby Protection/Active	→B	→C	→D	N/A	→E	N/A	→F	O	N/A

NOTE 1 – "N/A" means that the event ~~can~~is not expected to happen for the State. However if it does happen, the event should be ignored.

NOTE 2 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.

[a] It transits to the state D if the Signal Fail still exists after hold-off timer expires.

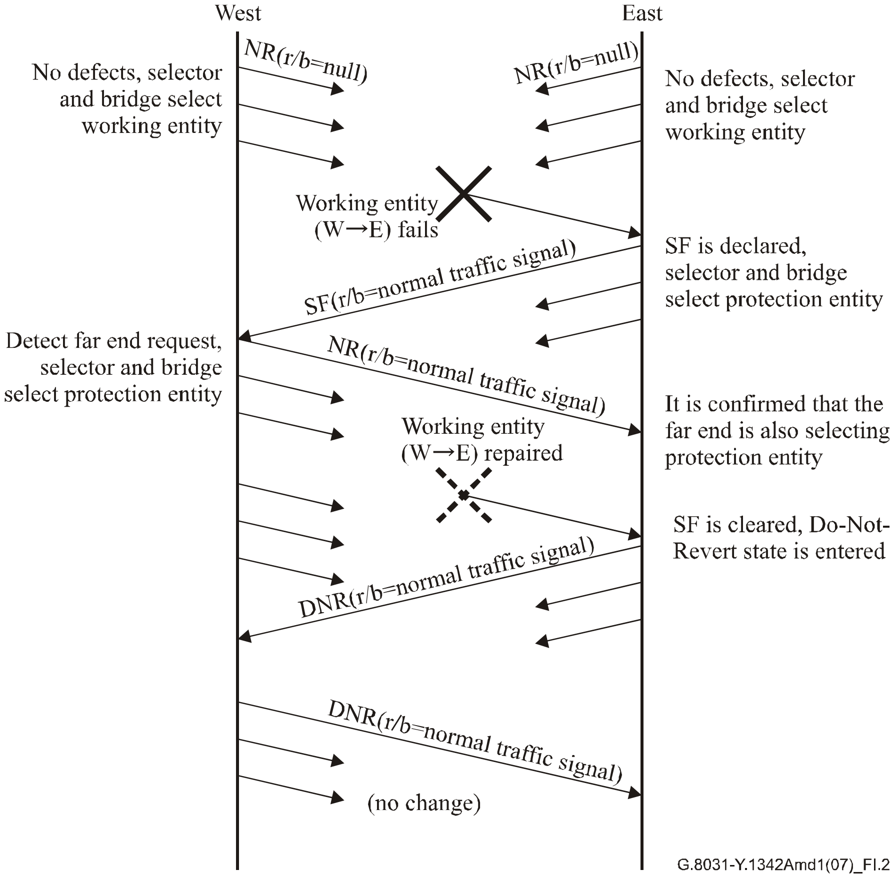
[b] If SF is reasserted.

[c] If SF-P is reasserted.

11) Changes to Appendix I, Operation example of 1-phase APS protocol

11.1) Changes to Figure I.2

Replace Figure I.2 as follows:



NR	No Request
r/b	requested signal/bridged signal
SF	Signal Failure
WTR	Wait-To-Restore
DNR	Do-Not-Revert
W→E	West to East direction

Figure I.2 – Protocol example (non-revertive mode)

11.2) Changes to Figure I.3

Replace Figure I.3 as follows:

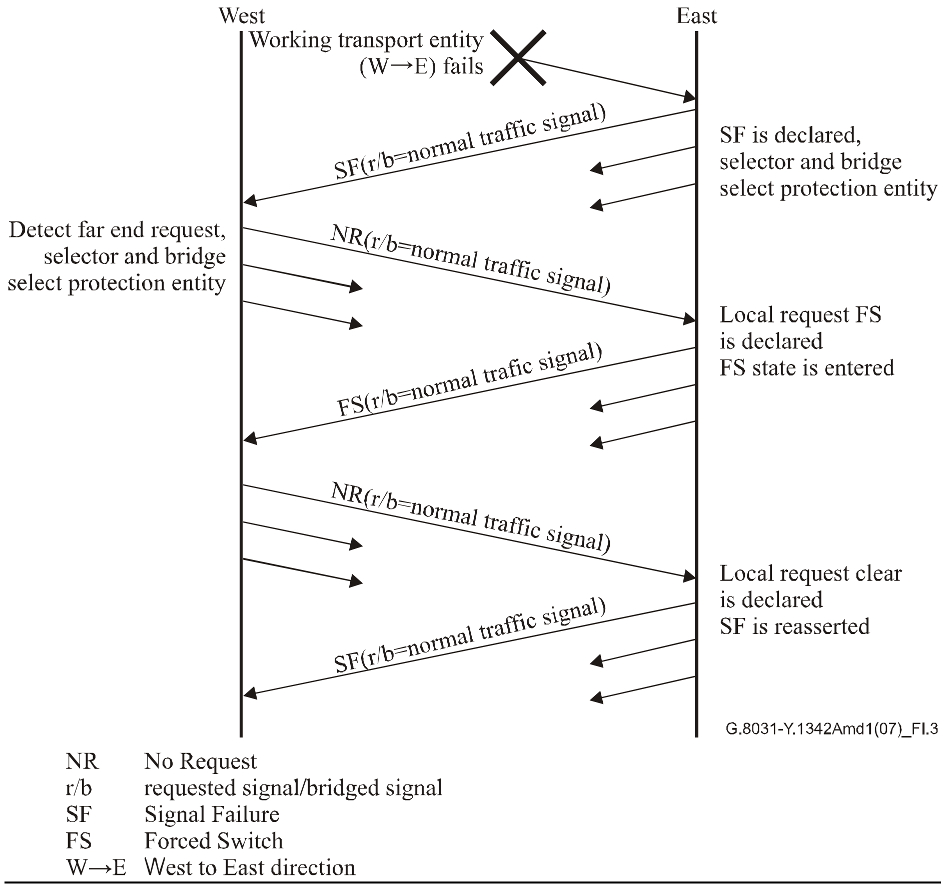


Figure I.3 – Protocol example (SF and FS)

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	**Y.1300–Y.1399**
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

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

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	Telephone transmission quality, telephone installations, local line networks
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, 2008