International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.8031/Y.1342

(06/2011)

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

Recommendation ITU-T G.8031/Y.1342

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
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
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.

Recommendation ITU-T G.8031/Y.1342

Ethernet linear protection switching

Summary

Recommendation ITU-T G.8031/Y.1342 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.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T G.8031/Y.1342	2006-06-06	15
1.1	ITU-T G.8031/Y.1342 (2006) Amd. 1	2007-10-07	15
1.2	ITU-T G.8031/Y.1342 (2006) Cor. 1	2008-06-06	15
2.0	ITU-T G.8031/Y.1342	2009-11-13	15
2.1	ITU-T G.8031/Y.1342 (2009) Cor. 1	2010-09-06	15
3.0	ITU-T G.8031/Y.1342	2011-06-22	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 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/.

Table of Contents

Page

Recommendation ITU-T G.8031/Y.1342

Ethernet linear protection switching

1 Scope

This Recommendation defines the APS protocol and linear protection switching mechanisms for point-to-point VLAN-based ETH subnetwork connection (SNC) in Ethernet transport networks. All other protection schemes, including point-to-multipoint and multipoint-to-multipoint, are for further study.

Linear 1+1 and 1:1 protection switching architectures with unidirectional and bidirectional switching are defined in this version of the Recommendation.

The APS protocol and protection switching operation for all other Ethernet network architectures, (for example, ring, mesh, etc.), are for further study.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T G.780] Recommendation ITU-T G.780/Y.1351 (2008), *Terms and definitions for synchronous digital hierarchy (SDH) networks*.

[ITU-T G.805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks*.

[ITU-T G.806] Recommendation ITU-T G.806 (2009), *Characteristics of transport equipment – Description methodology and generic functionality*.

[ITU-T G.808.1] Recommendation ITU-T G.808.1 (2006), *Generic protection switching – Linear trail and subnetwork protection*.

[ITU-T G.841] Recommendation ITU-T G.841 (1998), *Types and characteristics of SDH network protection architectures.*

[ITU-T G.870] Recommendation ITU-T G.870/Y.1352 (2008), *Terms and definitions for optical transport networks (OTN).*

[ITU-T G.8010] Recommendation ITU-T G.8010/Y.1306 (2004), *Architecture of Ethernet layer networks*.

[ITU-T G.8021] Recommendation ITU-T G.8021/Y.1341 (2007), *Characteristics of Ethernet transport network equipment functional blocks*.

[ITU-T M.495] Recommendation ITU-T M.495 (1988), *Transmission restoration and transmission route diversity: Terminology and general principles*.

[ITU-T Y.1731] Recommendation ITU-T Y.1731 (2008), *OAM functions and mechanisms for Ethernet based networks*.

[IEEE 802] IEEE Std 802-2001, *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*.

[IEEE 802.1D] IEEE Std 802.1D-2004, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*.

[IEEE 802.1Q] IEEE Std 802.1Q-2005, *IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

Terms defined in [ITU-T G.780]:

3.1.1 bidirectional protection switching

3.1.2 unidirectional protection switching

Terms defined in [ITU-T G.805]:

3.1.3 adapted information

3.1.4 characteristic information

3.1.5 link

3.1.6 link connection

3.1.7 tandem connection

3.1.8 trail

3.1.9 trail termination

Terms defined in [ITU-T G.806]:

3.1.10 atomic function

3.1.11 defect

3.1.12 failure

3.1.13 server signal degrade (SSD)

3.1.14 server signal fail (SSF)

3.1.15 signal degrade (SD)

3.1.16 signal fail (SF)

3.1.17 trail signal degrade (TSD)

3.1.18 trail signal fail (TSF)

Terms defined in [ITU-T G.870]:

3.1.19 APS protocol

3.1.19.1 1-phase

3.1.20 protection class

3.1.20.1 individual

3.1.20.2 group

3.1.20.3 network connection protection

3.1.20.4 subnetwork connection protection

3.1.20.4.1 sublayer monitored (/S)

3.1.20.4.2 non-intrusive monitored

3.1.20.4.3 inherent monitored

3.1.20.4.4 test monitored (/T)

3.1.20.5 trail protection

3.1.21 switch

3.1.22 component

3.1.22.1 protected domain

3.1.22.2 bridge

3.1.22.2.1 permanent bridge

3.1.22.2.2 broadcast bridge

3.1.22.2.3 selector bridge

3.1.22.3 selector

3.1.22.3.1 selective selector

3.1.22.4 head end

3.1.22.5 tail end

3.1.22.6 sink node

3.1.22.7 source node

3.1.22.8 intermediate node

3.1.23 architecture

3.1.23.1 1+1 protection architecture

3.1.23.2 1:n protection architecture

3.1.23.3 $(1:1)^n$ protection architecture

3.1.24 signal

3.1.24.1 traffic signal

3.1.24.2 normal traffic signal

3.1.24.3 extra traffic signal

3.1.24.4 null signal

3.1.25 time

3.1.25.1 detection time

3.1.25.2 hold-off time

3.1.25.3 wait-to-restore time

3.1.25.24 switching time

3.1.26 transport entity

3.1.26.1 protection transport entity

3.1.26.2 working transport entity

3.1.26.3 active transport entity

3.1.26.4 standby transport entity

3.1.27 protection

3.1.28 impairment

3.1.29 protection ratio

3.1.30 revertive (protection) operation

3.1.31 non-revertive (protection) operation

Terms defined in [ITU-T G.8010]:

3.1.32 Ethernet characteristic information (ETH_CI)

3.1.33 Ethernet flow point (ETH_FP)

3.1.34 maintenance entity

3.1.35 maintenance entity group

3.1.36 maintenance entity group end point (MEP)

3.1.37 maintenance entity group level

Term defined in [ITU-T G.8021]:

3.1.38 Ethernet flow forwarding function (ETH_FF)

Term defined in [ITU-T M.495]:

3.1.39 transfer time (Tt)

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AI Adapted Information

APS Automatic Protection Switching

CCM Continuity Check Message

CI Characteristic Information

DNR Do Not Revert

EC Ethernet Connection

ETH Ethernet layer network

ETH-AIS Ethernet Alarm Indication Signal function

ETH-APS Ethernet Automatic Protection Switching function

ETH-CC Ethernet Continuity Check function

ETH_CI Ethernet Characteristic Information

ETH_FF Ethernet Flow Forwarding Function

ETH_FP Ethernet Flow Point

EXER Exercise

FS Forced Switch

FT Flow Termination

LCK Locked

LO Lockout of protection

LOC Loss of Continuity

LSB Least Significant Bit

MEP Maintenance Entity Group End Point

MI Management Information

MIP Maintenance Entity Group Intermediate Point

MS Manual Switch

MSB Most Significant Bit

NR No Request

OAM Operation, Administration and Maintenance

PDU Protocol Data Unit

PS Protection Switching

RR Reverse Request

RSTP Rapid Spanning-Tree Protocol

SD Signal Degrade

SDL Specification and Description Language

SF Signal Fail

SF-P Signal Fail on Protection

SNC SubNetwork Connection

SNC/I SubNetwork Connection with Inherent monitoring

SNC/N SubNetwork Connection protection with Non-intrusive monitoring

SNC/S SubNetwork Connection protection with Sublayer monitoring

SNC/T SubNetwork Connection protection with Test-trail monitoring

SSD Server Signal Degrade

SSF Server Signal Fail

STP Spanning-Tree Protocol

TCM Tandem Connection Monitoring

TSD Trail Signal Degrade

TSF Trail Signal Fail

Tt Transfer time

VID VLAN Identifier

VLAN Virtual Local Area Network

WTR Wait-To-Restore

5 Conventions

5.1 Representation of octets

Octets are represented as defined in [IEEE 802.1D].

When consecutive octets are used to represent a binary number, the lower octet number has the most significant value.

The bits in an octet are numbered from 1 to 8, where 1 is the least significant bit (LSB) and 8 is the most significant bit (MSB).

6 Introduction

This Recommendation specifies linear protection switching mechanisms to be applied to VLAN-based Ethernet networks as described in [ITU-T G.8010]. Protection switching is a fully allocated survivability mechanism. It is fully allocated in the sense that the route and bandwidth of the protection entity are reserved for a selected working entity. It provides a fast and simple survivability mechanism. It is easier for the network operator to grasp the status of the network (e.g., active network topology) with protection switching than with other survivability mechanisms, such as RSTP.

This Recommendation specifies linear 1+1 protection switching architecture and linear 1:1 protection switching architecture. The linear 1+1 protection switching architecture operates with either unidirectional or bidirectional switching. The linear 1:1 protection switching architecture operates with bidirectional switching.

In the linear 1+1 protection switching architecture, a protection transport entity is dedicated to each working transport entity. The normal traffic signal is copied and fed to both working and protection transport entities with a permanent bridge at the source of the protected domain. The traffic on working and protection transport entities is transmitted simultaneously to the sink of the protected domain, where a selection between the working and protection transport entities is made based on some predetermined criteria, such as server defect indication.

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 directions select the same entity. On the other hand, unidirectional linear 1+1 protection switching does not need APS coordination protocol.

In the linear 1:1 protection switching architecture, the protection transport entity is dedicated to the working transport entity. However, the normal traffic signal is transported either on the working transport entity or on the protection transport entity, using a selector bridge at the source of the protected domain. Alternatively, when using a broadcast bridge at the source of the protected domain, the normal traffic signal is transported on the working transport entity in normal condition, and is copied and fed to both working and protection transport entities when protection switching is triggered by any valid request. In both cases, the selector at the sink of the protected domain selects the entity which carries the normal traffic signal as indicated via the requested signal (see clause 11.8). Since source and sink need to be coordinated to ensure that the bridge at the source (either selector or broadcast) and the selector at the sink select the same entity, APS coordination protocol is necessary. (Additional details about using a selector or broadcast bridge are provided in clause 10.6.3.)

7 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 G.8021] and [ITU-T G.8010]. Other entities to be protected are for further study.

2) The protected domain should be configured such that 100% of the impaired normal traffic signal should be protected in case of failure on a single working entity.

3) Transfer time (Tt) should be less than 50 ms.

4) The ETH layer connectivity of a working transport entity and a protection transport entity should be periodically monitored.

5) Subsequent to a protection switching event, frames should be delivered in order.

   NOTE – Subsequent to a protection switching event, frames may temporarily be lost or duplicated due to differential path delay.

6) Individual and group protection switching should be supported.

7) Revertive and non-revertive switching should be provided as network operator options.

8) A mismatch between the bridge/selector positions of the near end and the far end should be detected.
   - The bridge/selector mismatch for the local network element should be detected and reported.
   - The bridge/selector mismatch should be cleared by a network operator.

9) Operator requests such as lockout–of-protection (LO), forced-switch (FS) and manual-switch (MS) commands should be supported.

10) Prioritized protection between signal fail (SF) and operator requests should be supported.

11) A provisionable "generic hold-off function" should be provided so as to delay the beginning of the protection switching action.

8 Protection characteristics

8.1 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.8021]). For the purpose of the protection switching process, a transport entity within the protected domain has a condition of OK, failed (signal fail = SF), or degraded (signal degrade = SD) if applicable.

The customary monitoring methods are as follows:

Inherent – Inherent monitoring is based on detection of defects by a trail-termination function or adaptation function at the tail end. Ethernet subnetwork protection with inherent monitoring (SNC/I) is based on inherent monitoring.

Non-intrusive – Protection switching is triggered by a non-intrusive monitor at the tail end of the protection group. This action allows protecting a segment of a trail that is not constrained by the beginning or end of the trail. An Ethernet subnetwork protection with non-intrusive monitoring (SNC/N) is a linear protection based on non-intrusive monitoring. Non-intrusive monitoring may be based on monitoring of a layer or sublayer (e.g., non-intrusive TCM).

Sublayer – Ethernet subnetwork protection with sublayer monitoring (SNC/S) is a linear protection architecture based on sublayer monitoring. Each serial compound link connection is extended with tandem connection monitoring (TCM) or segment termination/adaptation functions to derive the fault condition status independent of the traffic signal present. For network layers supporting TCM, it is attractive to instantiate a TCM-monitored segment of a trail precisely across a protected segment so that protection switching is based only on defects within the protected segment. This has a further advantage over SNC/N in that defects that occur upstream of the protected segment will not be visible for the purpose of protection switching.

Test trail – Defects are detected using an extra test trail. An extra test trail is set up between source and sink of the protected domain, which includes a protection group of subnetwork connections. Ethernet subnetwork protection with test trail monitoring (SNC/T) is based on test trail monitoring that is applicable for group protection only.

The protection switching controller does not care which monitoring method is used, as long as it can be given (OK, SF, SD if applicable) 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 the far end from declaring an SD over the APS protocol, even if the monitor at the near end cannot detect SD.

In this version of the Recommendation, SNC/S monitoring architecture is supported for point-to-point VLAN-based ETH SNC. Other monitoring methods such as SNC/I, SNC/N and SNC/T are for further study.

9 Protection group commands

9.1 End-to-end commands and states

This clause describes commands that apply to the protection group as a whole. When an APS protocol is present, these commands are signalled to the far end of the connection. In bidirectional switching, these commands affect the bridge and selector at both ends.

Lockout of protection – This command prevents a working signal from being selected from the protection transport entity. This effectively disables the protection group.

Force switch normal traffic signal-to-protection – Forces normal traffic signal to be selected from the protection transport entity.

Manual switch normal traffic signal-to-protection – In the absence of a failure of a working or protection transport entity, forces normal traffic signal to be selected from the protection transport entity.

Manual switch normal traffic signal-to-working – In the absence of a failure of a working or protection transport entity in non-revertive operation, forces normal traffic signal to be selected from the working transport entity.

Wait-to-restore normal traffic signal – In a revertive operation, after the clearing of a SF (or SD if applicable) on the working transport entity, maintains normal traffic signal as selected from the protection transport entity until a wait-to-restore timer expires. The state will be changed to NR if the timer expires prior to any other event or command. This is used to prevent frequent operation of the selector in the case of intermittent failures.

Exercise signal – Exercise of the APS protocol. The signal is chosen so as not to modify the selector.

Do-not-revert normal traffic signal – In non-revertive operation, this is used to maintain a normal traffic signal selected from the protection transport entity.

No request – No request is the state entered by the local priority under all conditions where no local protection switching requests (including Wait-to-Restore and do-not-revert requests) are active. A normal traffic signal is selected from the corresponding transport entity.

Clear – Clears the active near-end Lockout of protection, Forced switch, Manual switch, WTR state, or Exercise command.

9.2 Local commands

These commands apply only to the near end of the protection group. Even when an APS protocol is supported, they are not signalled to the far end.

Freeze – Freezes the state of the protection group. Until the freeze is cleared, additional near end commands are rejected. Condition changes and received APS information are ignored. When the Freeze command is cleared, the state of the protection group is recomputed based on the condition and received APS information.

Clear freeze

10 Protection architectures

In the linear protection architecture defined in this version of the Recommendation, protection switching occurs at the two distinct endpoints of a point-to-point VLAN-based ETH SNC. Between these endpoints, there will be both "working" and "protection" transport entities.

For a given direction of transmission, the "head end" of the protected entity is capable of performing a bridge function, which will place a copy of a normal traffic signal onto a protection transport entity when required. The "tail end" will perform a selector function, where it is capable of selecting a normal traffic signal either from its usual working transport entity, or from a protection transport entity. In the case of bidirectional transmission, where both directions of transmission are protected, both ends of the protected entity will normally provide both bridge and selector functions.

The following architectures are possible:

1+1 – In 1+1 architectures, a protection transport entity is employed to protect the normal traffic signal. At the head end, the bridge is permanent. Switching occurs exclusively at the tail end.

1:1 – In 1:1 architectures, a protection transport entity is employed to protect the normal traffic signal. At the head end, the bridge is not established until a protection switch is required.

The architecture at each end of the protected domain must match.

10.1 Unidirectional and bidirectional switching

In the case of bidirectional transmission, it is possible to choose either unidirectional or bidirectional switching. With unidirectional switching, the selectors at each end are fully independent. With bidirectional switching, an attempt is made to coordinate the two ends so that both have the same bridge and selector settings, even for a unidirectional failure. Bidirectional switching always requires APS information to coordinate the two endpoints. Unidirectional switching can protect two unidirectional failures (or degradations, if applicable) in opposite directions on different entities.

10.2 Need for APS communication

The only switching type that does not require APS communication is 1+1 unidirectional switching. With a permanent bridge at the head end and no need to coordinate selector positions at the two ends, the tail end selector can be operated entirely according to defects and commands received at the tail end.

Bidirectional switching always requires APS communication.

10.3 Revertive and non-revertive switching

In revertive operation, normal traffic signal is restored to the working transport entity after the condition(s) causing a switch has cleared. In the case of clearing a command (e.g., forced switch), this happens immediately. In the case of clearing of a defect, this generally happens after the expiry of a Wait-to-Restore (WTR) timer, which is used to avoid chattering of selectors in the case of intermittent defects.

In non-revertive operation, normal traffic signal is allowed to remain on the protection transport entity even after a switch reason has cleared. This is generally accomplished by replacing the previous switch request with a Do not Revert (DNR) request, which is low priority.

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 a 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 a revertive operation. Although it is possible to define the protocol in a way that would permit a non-revertive operation for 1:1 protection, 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, although a mismatch of this parameter does not prevent interworking, it would nonetheless be peculiar for one side to go to WTR for the 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_C_MI_PS_OperType.

10.4 Provisioning mismatches

With all of the options for provisioning of protection groups, there are opportunities for mismatches between the provisioning at the two ends. These provisioning mismatches take one of several forms:

a) Mismatches where proper operation is not possible.

b) Mismatches where one or both sides can adapt their operation to provide a degree of interworking in spite of the mismatch.

c) Mismatches that do not prevent interworking. An example is the revertive/non-revertive mismatch discussed in clauses 10.3 and 11.4.

Not all provisioning mismatches can be conveyed and detected by information passed through the APS communication. There are simply too many combinations of valid entity numbers to easily provide full visibility of all of the configuration options. What is desirable, however, is to provide visibility for the middle category, where the sides can adapt their operation to interwork in spite of the mismatch. For example, an equipment provisioned for bidirectional switching could fall back to unidirectional switching to allow interworking. An equipment provisioned for 1+1 switching with an APS communication could fall back to operate in 1+1 unidirectional switching without an APS communication. The user could still be informed of the provisioning mismatch, but a level of protection could still be provided by the equipment.

10.5 Protection switching trigger

For example, protection switching should be performed when:

a) Initiated by operator control (e.g., Forced switch, Manual switch) if it has a higher priority than any other local request or the far-end request; or

b) SF is declared on the active transport entity and is not declared on the standby transport entity, and the detected SF condition has a higher priority than any other local request or the far-end request; or

c) SD is declared on the active transport entity and is not declared on the standby transport entity, and the detected SD condition has a higher priority than any other local request or the far-end request; or

d) In the bidirectional 1+1 and 1:1 architecture, the received APS protocol requests to switch and it has a higher priority than any other local request.

Other cases are described as state transition in Annex A.

10.5.1 Signal fail declaration conditions

SF is declared when an ETH trail signal fail condition is detected. ETH trail signal fail is specified in [ITU-T G.8021].

10.5.2 Signal degrade declaration conditions

SD is declared when an ETH trail signal degrade condition is detected. ETH trail signal degrade is specified in [ITU-T G.8021].

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 connection function (ETH_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_C.

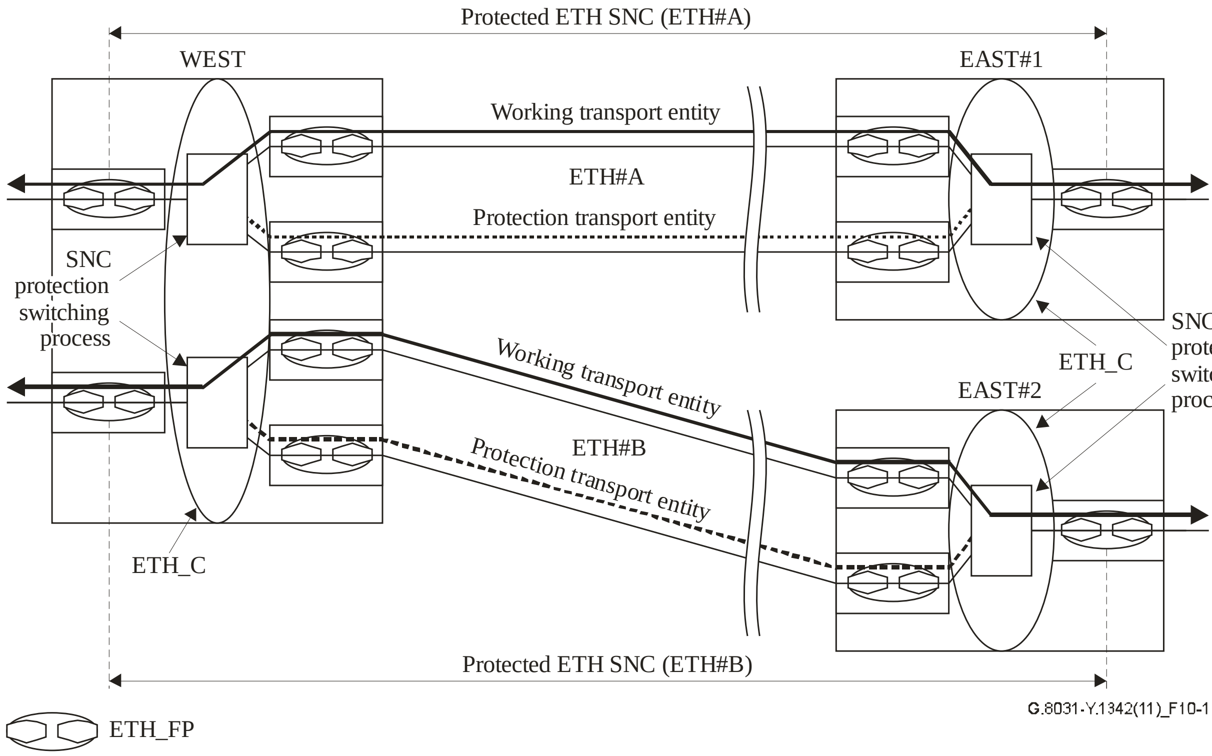


Figure 10-1 – ETH SNC/S protection switching architecture

Working and protection transport entities for an SNC protection switching process shall be configured via ETH_C_MI_PS_WorkingPortId and ETH_C_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 Y.1731], as shown in Figure 10-2.

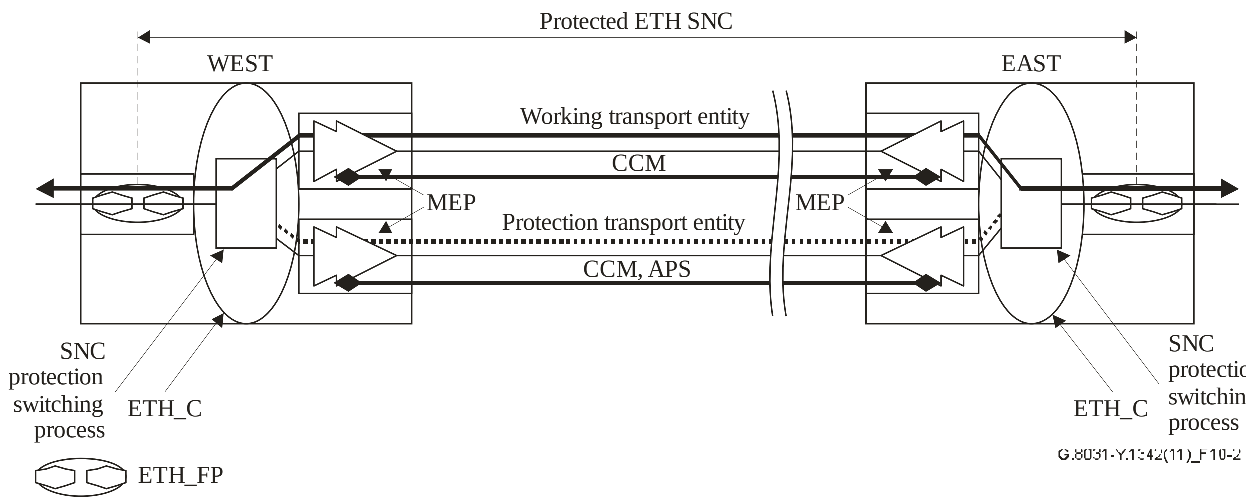


Figure 10-2 – MEPs in ETH SNC/S protection switching architecture

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

APS information and defect condition which are terminated/detected by the 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 an SF (or SD if applicable) 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 Y.1731]) is done by the ETH_FT atomic function. If the ETH_FT detects a failure condition, an ETH_AI_TSF (or ETH_AI_TSD if applicable) is signalled to the ETH(x) to ETH adaptation sink (ETH(x)/ETH_A_Sk) which subsequently generates an ETH_CI_SSF (or ETH_CI_SSD if applicable). The ETH(x)/ETH adaptation function employs this ETH_CI_SSF (or ETH_CI_SSD if applicable) to notify the ETH SNC protection switching process within ETH_C of the 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_SSD if applicable) 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.

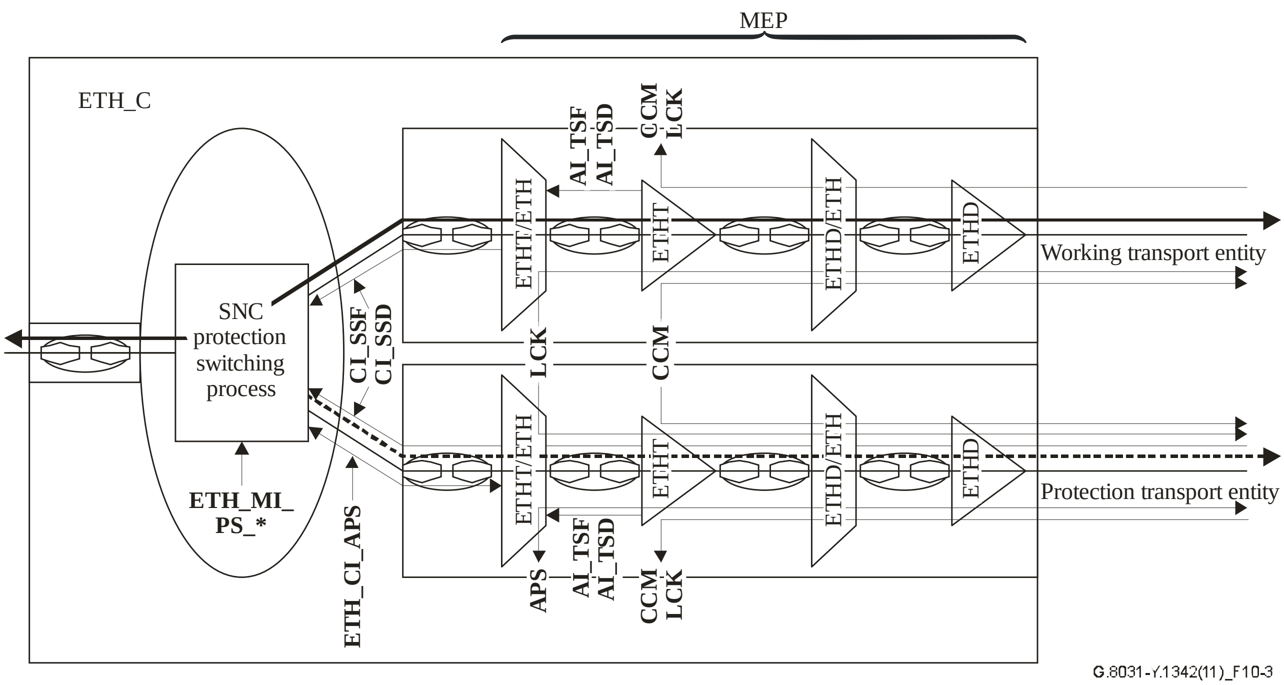


Figure 10-3 – Behaviours of both MEPs and SNC protection switching process in ETH SNC/S protection switching architecture

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_C only from the working entity. Figure 10-5 illustrates a situation where a protection switching has occurred due to a signal fail (or signal degrade) 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.

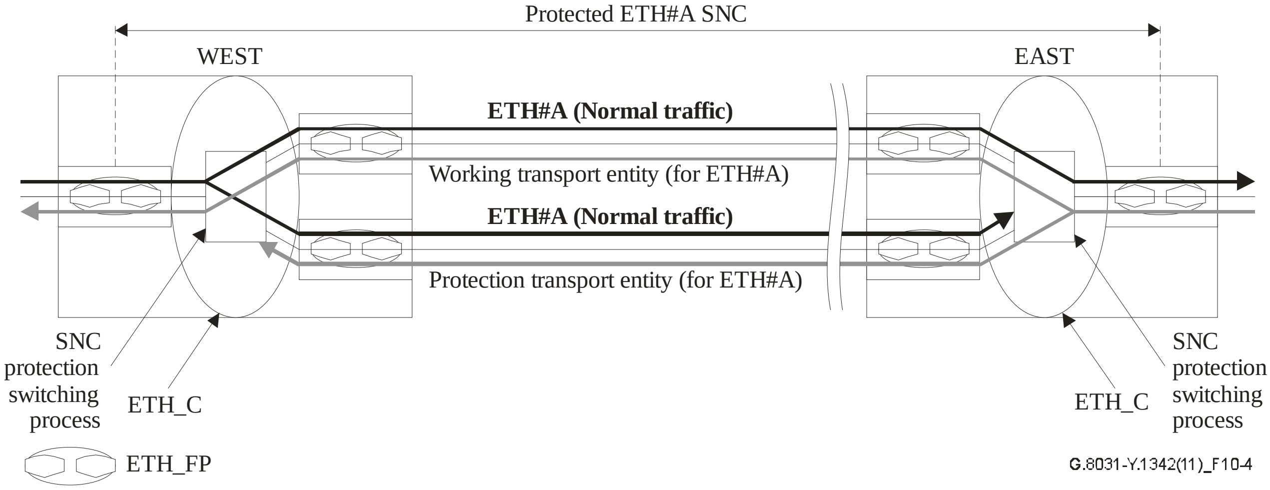


Figure 10-4 – 1+1 bidirectional protection switching architecture

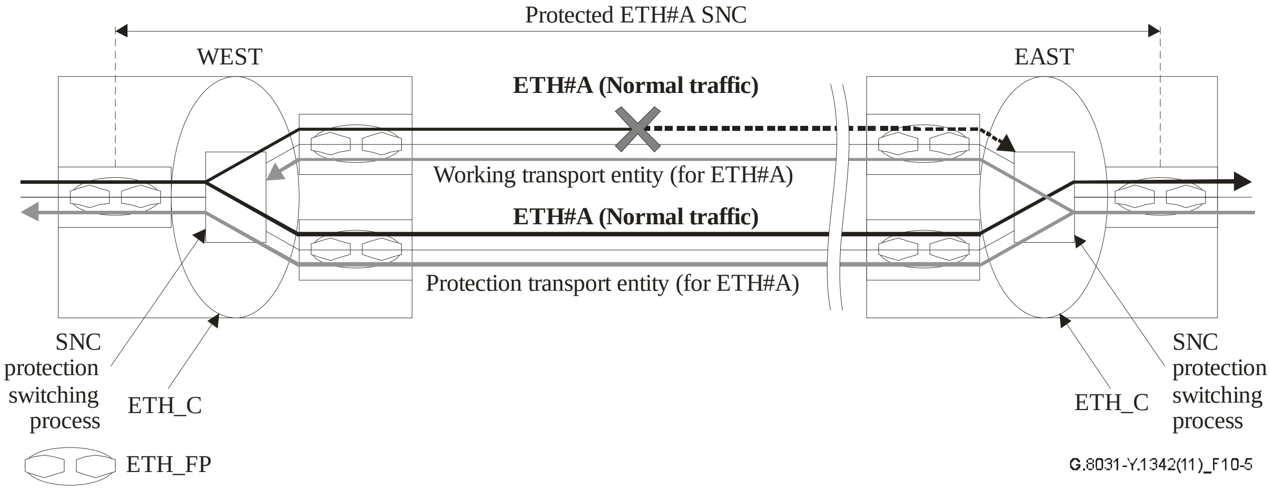


Figure 10-5 – 1+1 bidirectional protection switching architecture – Signal fail (or signal degrade) condition for a working entity

The ability of a SNC protection switching process to trigger protection switching upon SD shall be configured via ETH_C_MI_PS_SD_Protection. ETH_C_MI_PS_SD_Protection accepts the values enabled and disabled. The default value of ETH_C_MI_PS_SD_Protection shall be disabled.

NOTE – ETH_C_MI_PS_SD_Protection is recommended to be set to enabled only when both ends can trigger protection switching upon SD.

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_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 (or signal degrade) condition on the working transport entity in the west-to-east direction. The normal traffic signal 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 based only on the local information. For this purpose, APS coordination protocol is not necessary.

Figure 10-8 illustrates a case where a signal fail (or signal degrade) 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 these types of double-defect scenarios, while bidirectional protection switching cannot.

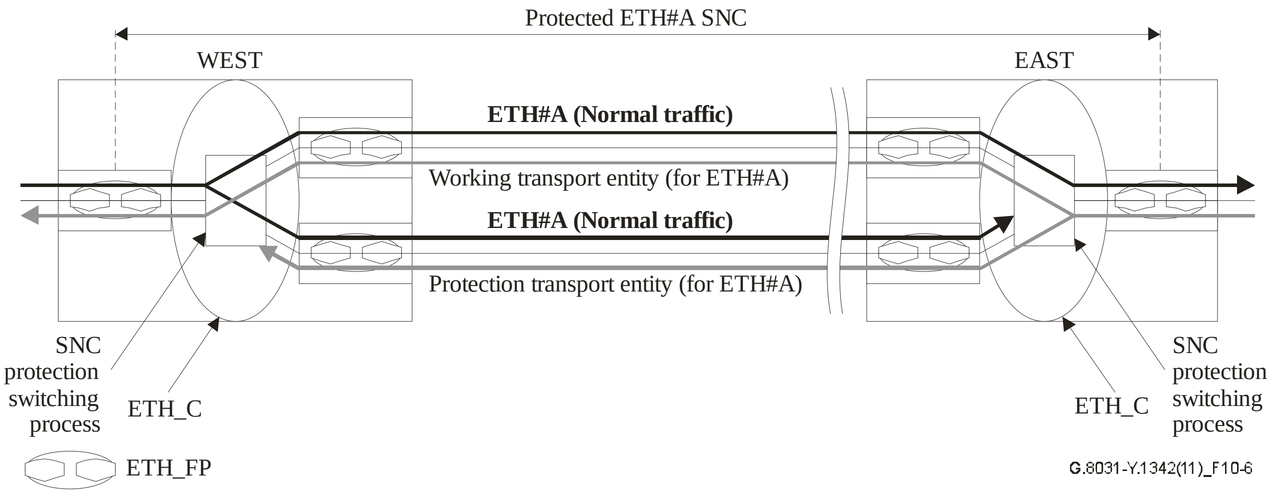


Figure 10-6 – 1+1 unidirectional protection switching architecture

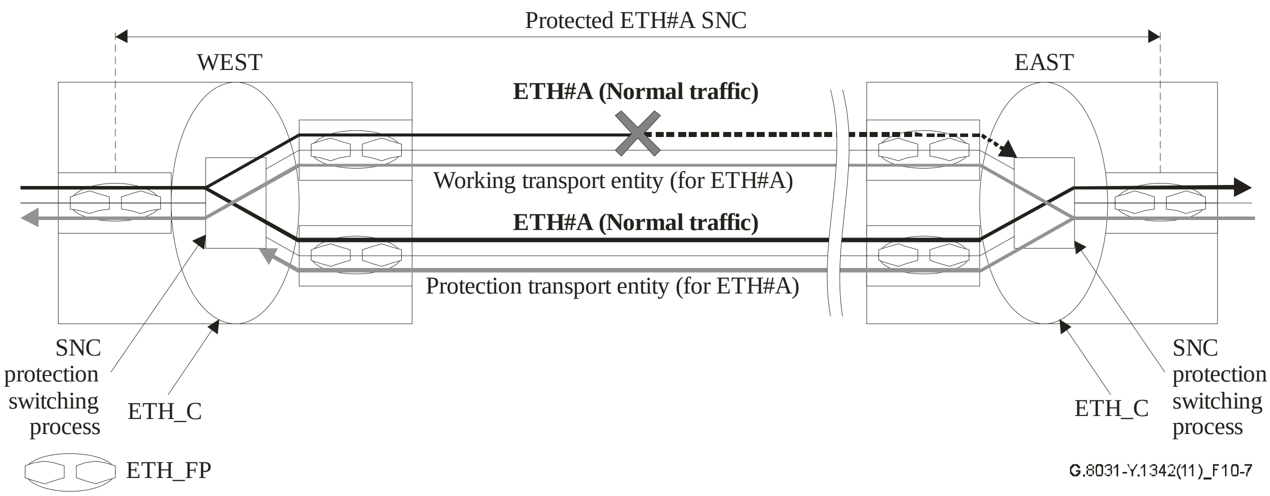


Figure 10-7 – 1+1 unidirectional protection switching architecture – signal fail (or signal degrade) condition for a working transport entity in the west-to-east direction

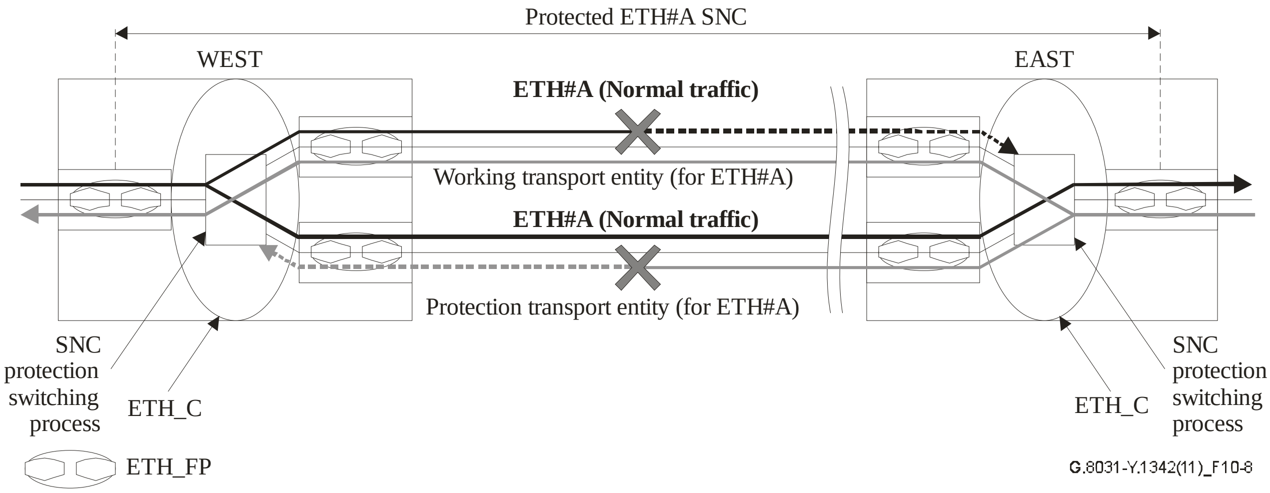


Figure 10-8 – 1+1 unidirectional protection switching architecture – signal fail (or signal degrade) condition in both directions

10.6.3 1:1 bidirectional protection switching

1:1 SNC protection switching can be supported either by a selector bridge or by a broadcast bridge. The type of bridge used for 1:1 SNC protection switching (selector or broadcast) shall be configured via ETH_C_MI_PS_BridgeType. ETH_C_MI_PS_BridgeType accepts the values 0 (selector bridge) and 1 (broadcast bridge). The default value of ETH_C_MI_PS_BridgeType shall be 0. In the current version of this Recommendation, the selector bridge does not support protection against SD while the broadcast bridge does.

NOTE – Broadcast bridge is recommended to be used in revertive mode only.

Figure 10-9 illustrates the 1:1 linear protection switching architecture, with the normal traffic signal (ETH#A) being transmitted via the working transport entity. This Figure 10-9 is applicable to both types of bridges (selector or broadcast).

Figure 10-10 illustrates a situation where a protection switch has occurred, due to a signal fail condition on the working transport entity. A selector bridge is used at the source node where the normal traffic signal (ETH#A) is forwarded to the protection transport entity. At the sink node, the normal traffic signal (ETH#A) is received from the protection transport entity.

Figure 10-11 illustrates a situation where a protection switch has occurred due to a signal degrade condition on the working transport entity, declared as specified in clause 10.5.2. As detection of the ETH trail signal degrade condition, specified in clause 10.5.2, depends on the presence of a normal traffic signal, such a condition declared on the working transport entity would be cleared following protection switching to the protection transport entity if a selector bridge is used, possibly resulting in flapping. To avoid flapping, a broadcast bridge is used at the source node where the normal traffic signal (ETH#A) is forwarded to both the working transport entity and the protection transport entity. At the sink node, the normal traffic signal (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_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_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.

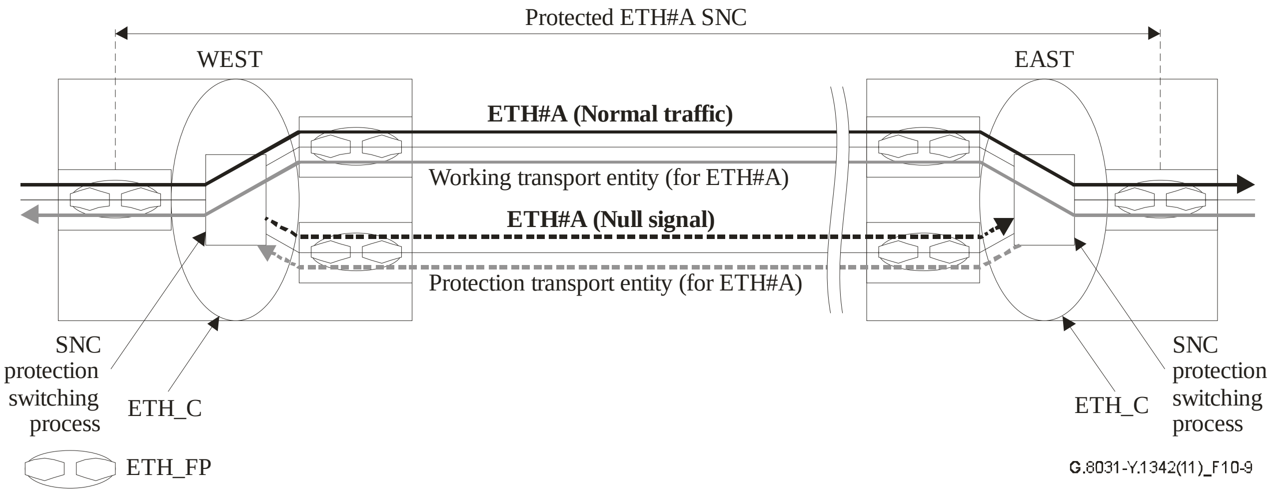


Figure 10-9 – 1:1 protection switching architecture

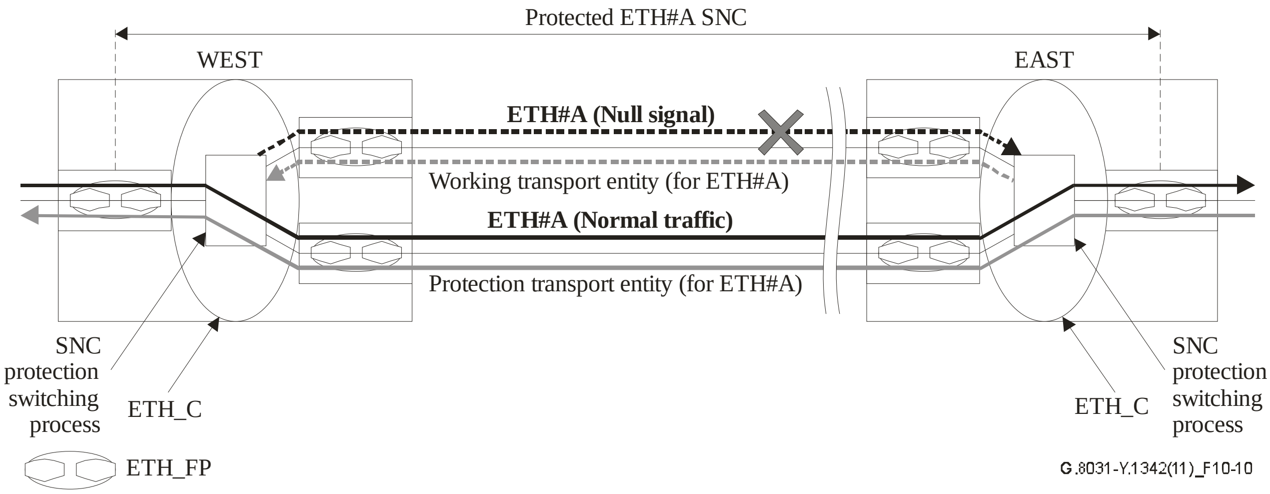


Figure 10-10 – 1:1 protection switching architecture (with selector bridge) – signal fail condition for working transport entity

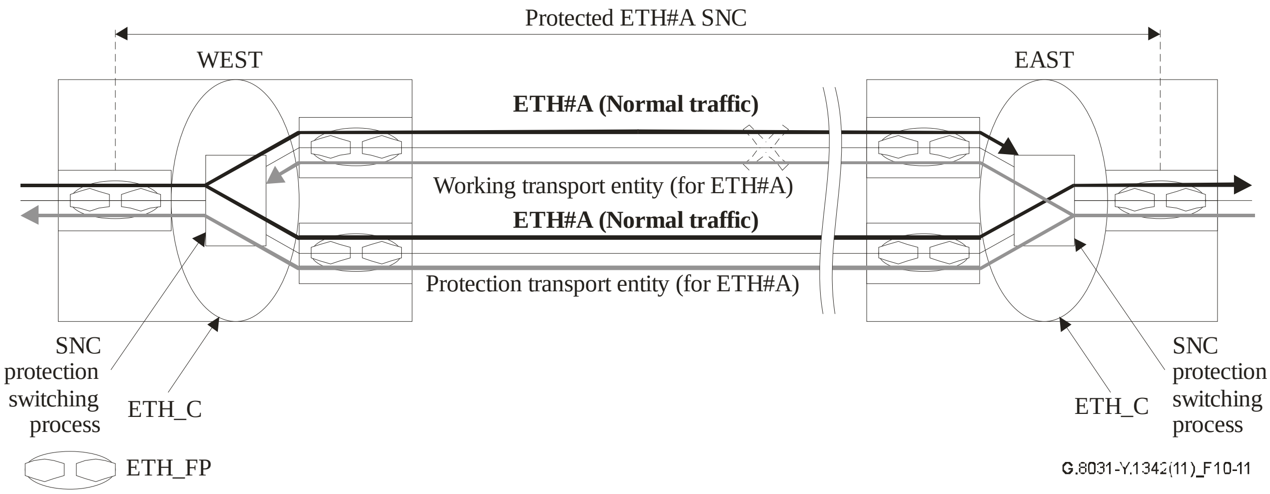


Figure 10-11 – 1:1 protection switching architecture (with broadcast bridge) – signal degrade condition for working transport entity

11 APS protocol

11.1 APS format

APS information is carried within the APS PDU which is one of a suite of Ethernet OAM PDUs. OAM PDU formats for each type of Ethernet OAM operation are defined in [ITU-T Y.1731]. APS-specific information is transmitted within specific fields in the APS PDU. The APS PDU is identified by a specific Ethernet OAM OpCode. In this version of the Recommendation, 4 octets in the APS PDU are used to carry APS-specific information. This is illustrated in Figure 11-1. In addition, it should be noted that for the current version of this Recommendation, the TLV Offset field is required to be set to 0x04.

<table>
<tr><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td><td colspan="8">4</td></tr>
<tr><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td colspan="3">MEL</td><td colspan="5">Version (0)</td><td colspan="8">OpCode (APS=39)</td><td colspan="8">Flags (0)</td><td colspan="8">TLV Offset (4)</td></tr>
<tr><td colspan="32">APS-specific information</td></tr>
<tr><td colspan="8">END TLV (0)</td></tr>
</table>

Figure 11-1 – APS PDU format

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

a) Version: 0x00

b) OpCode: 0d39 (=0x27)

c) Flags: 0x00

d) END TLV: 0x00

In the MEL field, the MEG level of the APS PDU is inserted.

The format of the APS-specific information within each APS PDU is defined as per Figure 11-2:

<table>
<tr><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td><td colspan="8">4</td></tr>
<tr><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td colspan="4" rowspan="2">Request/
State</td><td colspan="4">Prot. Type</td><td colspan="8" rowspan="2">Requested Signal</td><td colspan="8" rowspan="2">Bridged Signal</td><td rowspan="2">T</td><td colspan="7" rowspan="2">Reserved (0)</td></tr>
<tr><td>A</td><td>B</td><td>D</td><td>R</td></tr>
</table>

Figure 11-2 – APS-specific information format

All bits defined as "Reserved" in this Recommendation shall be transmitted as 0 and ignored on reception.

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

Table 11 – Code points and field values

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-W)	
		1001	Signal degrade (SD)	
		0111	Manual switch (MS)	
		0110	Depreciated	
		0101	Wait to restore (WTR)	
		0100	Exercise (EXER)	
		0010	Reverse request (RR)	
		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)	
Bridge type (for 1:1 protection switching)	T	0	Selector bridge	
		1	Broadcast bridge	

The 1-phase APS protocol shall be used for the supported protection architectures described in clause 10.

11.2 1-phase APS protocol

11.2.1 Principle of operation

Figure 11-3 illustrates the principle of the 1+1/1:1 linear protection switching algorithm. This algorithm is performed in network elements at both ends of the protected domain (locations WEST and EAST). Bidirectional switching is achieved by transmitting local switching requests to the far end via the "Request/State" in the first octet of the APS-specific information (see Figure 11-2). The transmitted "Requested Signal" and "Bridged Signal" in the second and the third octets of the

APS-specific information contain the local bridge/selector status information; a persistent mismatch between both ends may thus be detected and leads to an alarm.

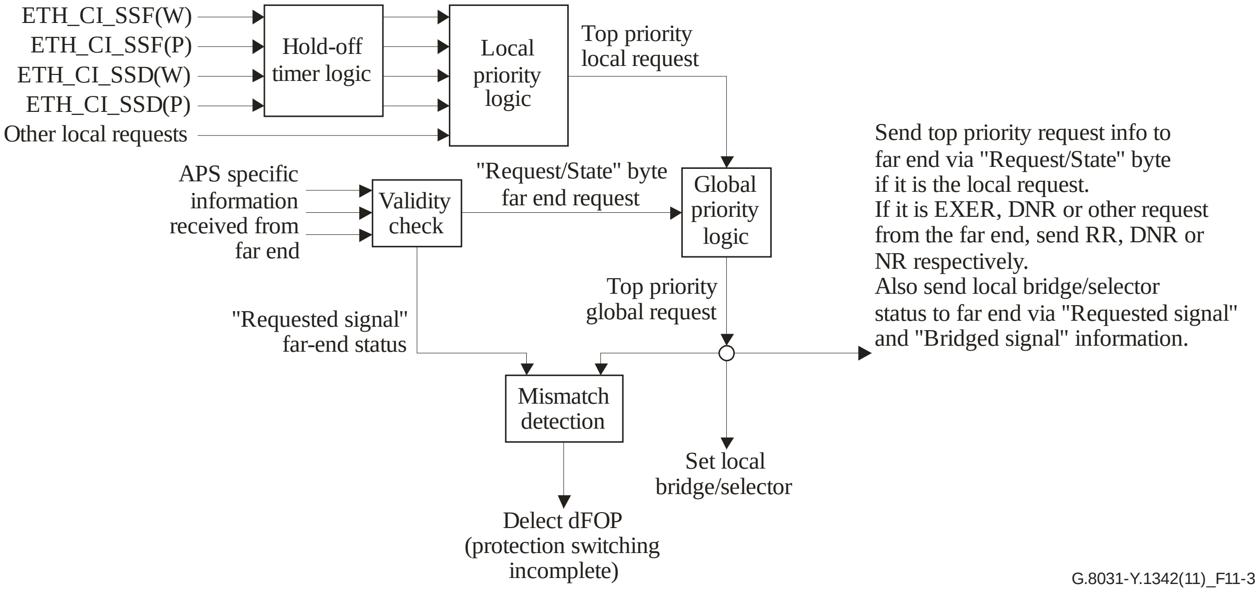


Figure 11-3 – Principle of 1+1/1:1 linear protection switching algorithm

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 clauses 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". Note that if the CLEAR command is accepted, clearance of SF(-P) (or of SD if applicable) or expiration of WTR timer shall not be processed by the local priority logic but shall be submitted to the global priority logic for processing.

If the provisioned hold-off timer value is non-zero, when the "hold-off timer logic" receives new ETH_CI_SSF (or ETH_CI_SSD if applicable) information, it does not report this information to the "local priority logic" immediately. Instead the hold-off timer will be started (see clause 11.12).

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 clause 11.2.4). The state transitions and the top priority global request are calculated in the "global priority logic" based on the top-priority local request. The request of the last received "Request/State" information, and state transition tables defined in Annex A, are as follows:

a) If the top priority local request is CLEAR, or if SF(-P) (or of SD if applicable) is cleared, or if WTR has expired, a state transition is calculated. This calculation is first based on the top-priority local request and state machine table for local requests to obtain an intermediate state. This intermediate state is the final state in the case of clearance of SF-P. Otherwise, starting at this intermediate state, the last received far-end request and the state machine table for far-end requests are used to calculate the final state[1].

[1] The intermediate state is an abstraction to determine the final state. The local network element only enters the final state, not the intermediate state. As a result, no switch and no APS exchange are performed because of the intermediate state being determined.

b) If the top-priority local request is not CLEAR, and there is neither clearance of SF(-P) (or of SD if applicable), nor expiration of WTR, the "global priority logic" compares the top priority local request with the request of the last received "Request/State" information, based on Table 11-1.

   i) if the top priority local request has higher or equal priority, it is used with the state transition table for local requests defined in Annex A to determine the final state[2]; otherwise;

   ii) the request of the last received "Request/State" information is used with the state transition table for far-end requests defined in Annex A, to determine the final state.

The final state corresponds to the "top-priority global request".

If the top-priority global request is the local request, it will be indicated in the "Request/State" field. If the top-priority global request is EXER, DNR, or another request from the far end, RR, DNR or NR will be indicated respectively. 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:

c) For 1+1 architectures, only the selector position is controlled. For 1:1 architectures, both the bridge and the selector positions are maintained to select the same position;

d) If the top-priority global request is a request for a working entity, the associated normal traffic signal is bridged/switched to/from the protection entity, i.e., the associated bridge/selector of the local network element selects the protection entity. A switching request for a working entity means a request to switch from a working entity to the protection entity.

The bridge/selector status is transmitted to the far end via the "Requested Signal" and "Bridged Signal" (with coding as described in Table 11-1). It is also compared with the bridge/selector status of the far end as indicated by the received "Requested Signal" and "Bridged Signal".

Note that every time one of the input signals changes, the linear protection switching algorithm commences immediately (see Figure 11-3), i.e., when the status of any local request changes, or when a different APS-specific information is received from the far end. The consequent actions of the algorithm are also initiated immediately, i.e., change the local bridge/selector position (if necessary), transmit a new APS-specific information (if necessary), or detect dFOP if the protection switching is not completed within a period specified in clause 11.15.

11.2.2 Revertive mode

In the revertive mode of a unidirectional protection switching operation, in conditions where a normal traffic signal is being received via the protection entity, if local protection switching requests (see Figure 11-3) have been previously active and have 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.

In the case of bidirectional protection switching, a local wait-to-restore state is entered only when there is no higher-priority 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.

[2] Note however that, as stated in clause 11.10, once a switch has been completed due to a request, it will not be overridden by another request of the same priority (first-come, first-served policy).

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.

11.2.3 Non-revertive mode

In the non-revertive mode of a unidirectional protection switching operation, in conditions where a normal traffic signal is being transmitted via the protection entity, if local protection switching requests (see Figure 11-3) have been previously active and have 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 a bidirectional protection switching operation, a local do-not-revert state is entered when there is no request of higher priority received from the far end than that of the do-not-revert state, or when both the local state and far-end state are NR with the requested signal number 1.

11.2.4 Transmission and acceptance of APS

Traffic units which carry APS PDU are called APS frames. The APS frames are transported via the protection transport entity only, being inserted by the head end of the protected domain and extracted by the tail end of the protected domain.

A new APS frame must be transmitted immediately when a change in the transmitted status (see Figure 11-3) occurs.

The first three APS frames should be transmitted as fast as possible only if the 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 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 an interval of 5 seconds.

If no valid APS-specific information is received, the last valid information that has been received remains applicable, except in case of SF condition on the protection transport entity.

If a protection end point receives APS-specific information from the working entity, it should ignore this information, and should detect the failure of protocol defect for the local network element (see clause 11.15).

11.3 Request type

The request types 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 signal a Reverse Request only in response to an EXER command from the far end.

11.4 Protection types and bridge type

The valid configurations of the protection type and bridge type are as specified in Table 11-2:

Table 11-2 – Valid configurations of the protection type and bridge type

Protection type	Bridge type	Valid configuration
000x	N/A	1+1 unidirectional, no APS communication
100x	N/A	1+1 unidirectional w/APS communication
101x	N/A	1+1 bidirectional w/APS communication
111x	0	1:1 bidirectional w/APS communication using a selector bridge
111x	1	1:1 bidirectional w/APS communication using a broadcast bridge

The protection type values are chosen such that the default value (all zeros) matches the only type of protection that can operate without APS (1+1 Unidirectional).

Note that protection type values 010x, 001x, and 011x are invalid since 1:1 and Bidirectional require an APS communication.

If the B bit mismatches, the selector is released since 1:1 and 1+1 are incompatible. This will result in a defect.

Provided the B bit matches:

a) If the A bit mismatches, the side expecting APS will fall back to 1+1 unidirectional switching without APS communication.

b) If the D bit mismatches, the bidirectional side will fall back to unidirectional switching.

c) If the R bit mismatches, one side will clear switches to WTR and the other will clear to DNR. The two sides will interwork and the traffic is protected.

d) If the "T" bit mismatches, the side using a broadcast bridge will fall back to using a selector bridge.

The protection type of an SNC protection switching process shall be configured via ETH_C_MI_PS_ProtType.

NOTE – Equipment not supporting the broadcast bridge (e.g., equipment compliant with previous versions of this Recommendation) sets the bridge type (T) bit to 0 and ignores it in reception.

11.5 Requested signal

This indicates the signal that the near-end requests be carried over the protection path. For NR, this is the null signal when the far end is not bridging the normal traffic signal to the protection entity. When the far end is bridging the normal traffic signal to the protection entity, the requested signal is the normal traffic signal for NR; for LO, this can only be the null signal. For Exercise, this can be the null signal when Exercise replaces NR or the normal traffic signal in the case where Exercise replaces DNR. For SF (or SD if applicable), this will be the normal traffic signal, or the null signal to indicate that protection has failed or has been degraded. For all other requests, this will be the normal traffic signal requested to be carried over the protection transport entity.

11.6 Bridged signal

This indicates the signal that is bridged onto the protection path. For 1+1 protection, this should always indicate the normal traffic signal, accurately reflecting the permanent bridge. For 1:1 protection, this will indicate what is actually bridged to the protection entity (either the null signal, or normal traffic signal). This will generally be the bridge requested by the far end.

11.7 Control of bridge

In 1+1 architectures, the normal traffic signal is permanently bridged to protection. The normal traffic signal will always be indicated in the bridged signal field of the APS information.

In 1:1 architectures, the bridge will be set to the one indicated by the "Requested Signal" field of the incoming APS information. Once the bridge has been established, this will be indicated in the "Bridged Signal" field of the outgoing APS information.

11.8 Control of selector

In 1+1 unidirectional architectures (with or without APS communication), the selector is set entirely according to the highest priority local request. This is a single phase switch.

In 1+1 bidirectional architectures, the normal traffic signal will be selected from the protection entity when the outgoing "Requested Signal" indicates the normal traffic signal.

In 1:1 bidirectional architectures, normal traffic signal will be selected from the protection entity when the number appears in the outgoing "Requested Signal".

11.9 Signal fail of the protection transport entity

Signal fail on the protection transport entity is higher priority than any defect that would cause a normal traffic signal to be selected from protection. If an APS signal is in use, an SF-P on the protection transport entity (over which the APS signal is routed) has priority over the Forced switch. The Lockout command has higher priority than SF-P: during failure conditions, lockout status shall be kept active.

11.10 Equal priority requests

In general, once a switch has been completed due to a request, it will not be overridden by another request of the same priority (first-come, first-served policy). Equal priority requests from both sides of a bidirectional protection group are both considered valid, as follows:

a) If the local state is NR, with the requested signal number 1, and the far-end state is NR, with the requested signal number 0, the local state transits to NR with the requested signal number 0. This applies to the case when the remote request for switching to the protection transport entity has been cleared.

b) If both the local and far-end states are NR, with the requested signal number 1, the local state transits to the appropriate new state (see clause 11.2.3 for non-revertive mode and clause 11.13 for revertive mode). This applies to the case when the old request has been cleared at both ends.

c) If both the local and far-end states are RR, with the same requested signal number, both ends transit to the appropriate new state according to the requested signal number. This applies to the case of concurrent deactivation of EXER from both ends.

d) In other cases, no state transition occurs, even if equal priority requests are activated from both ends. Note that if MSs are issued simultaneously to both working and protection transport entities, either as local or far-end requests, the MS to the working transport entity is considered as having higher priority than the MS to the protection transport entity.

11.11 Command acceptance and retention

The commands CLEAR, LO, FS, MS, and EXER are accepted or rejected in the context of previous commands, the condition of the working and protection entities in the protection group, and (in bidirectional switching only) the APS information received.

The CLEAR command is only valid if a near end LO, FS, MS, or EXER command is in effect, or if a WTR state is present at the near end and rejected otherwise. This command will remove the near-end command or WTR state, allowing the next lower-priority condition or (in bidirectional switching) APS request to be asserted.

Other commands are rejected unless they are higher priority than the previously existing command, condition, or (in bidirectional switching) APS request. If a new command is accepted, any previous, lower-priority command that is overridden is forgotten. If a higher priority command overrides a lower-priority condition or (in bidirectional switching) APS request, that other request will be reasserted if it still exists at the time the command is cleared. If a command is overridden by a condition or (in bidirectional switching) APS request, that command is forgotten.

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

11.12 Hold-off timer

In order to coordinate timing of protection switches at multiple layers or across cascaded protected domains, a hold-off timer may be required. The purpose is to allow either a server layer protection switch to have a chance to fix the problem before switching at a client layer, or to allow an upstream protected domain to switch before a downstream domain (e.g., to allow an upstream ring to switch before the downstream ring in a dual node interconnect configuration so that the switch occurs in the same ring as the failure).

Each protection group should have a provisionable hold-off timer. The suggested range of the hold-off timer is 0 to 10 seconds in steps of 100 ms (accuracy of ±5 ms).

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.

This hold-off timer mechanism shall be applied for both working and protection transport entities.

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

11.13 Wait-to-restore timer

In revertive mode of operation, to prevent frequent operation of the protection switch due to an intermittent defect, a failed working transport entity must become fault-free. After the failed working transport entity meets this criterion, a fixed period of time shall elapse before a normal traffic signal uses it again. This period, called a wait-to-restore (WTR) period, may be configured by the operator in 1 minute steps between 5 and 12 minutes; the default value is 5 minutes. An SF (or SD (W) if applicable) condition will override the WTR. To activate the WTR timer appropriately, even when both ends concurrently detect clearance of SF (or SD (W) if applicable), when the local state transits from SF (or SD (W) if applicable) to NR with the requested signal number 1, the previous local state, SF (or SD (W) if applicable), should be memorized. If both the local state and far-end state are NR with the requested signal number 1, the local state transits to WTR only when the previous local state is SF (or SD (W) if applicable). Otherwise, the local state transits to NR with the requested signal number 0.

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 (W) 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 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_C_MI_PS_WTR.

11.14 Exercise operation

Exercise is a command to test if the APS communication is operating correctly. It is lower priority than any "real" switch request. It is only valid in bidirectional switching, since this is the only place where you can get a meaningful test by looking for a response.

The 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 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 signal number is 1.

11.15 Failure of protocol defects

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

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

b) Working/protection configuration mismatch (described in clause 11.2.4)

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

NOTE – If the lack of response results from issuance at the local end of a:

  a. SD request that is unknown at the far end then it is expected that the operator would set the ETH_C_MI_PS_SD_Protection to disabled at the local end to resolve the dFOP-NR and the misalignment between the protection switching states at the two ends.

  b. MS [r/b=null] request that is unknown at the far end then it is expected that the operator would clear the MS [r/b=null] command at the local end to resolve the dFOP-NR and the misalignment between the protection switching states at the two ends.

d) No APS frame is received on the protection transport entity during at least 3.5 times the long APS interval (e.g., at least 17.5 seconds) and there is no defect on the protection transport entity.

Fully incompatible provisioning and working/protection configuration mismatches are detected by receiving only one APS frame. Detection and clearance of "failure of protocol" defects are defined in [ITU-T G.8021].

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

11.16 Signal degrade of the protection transport entity

Signal degrade on the protection transport entity has the same priority as signal degrade on the working transport entity. As a result, if an SD condition affects both transport entities, the first SD detected is not overridden by the second SD detected. If the SD is detected simultaneously, either as local or far-end requests on both working and protection transport entities, then the SD on the standby transport entity is considered as having higher priority than the SD on the active transport entity, and the normal traffic signal continues to be selected from the active transport entity (i.e., no unnecessary protection switching is performed).

NOTE – In the preceding sentence, "simultaneously" relates to the occurrence of SD on both the active and standby transport entities at input to the SNC protection switching process at the same time, or as long as a SD request has not been acknowledged by the remote end in bidirectional protection switching.

Annex A

State transition tables of protection switching

(This annex forms an integral part of this Recommendation.)

In this annex, state transition tables for the following protection switching configurations are described.

a) 1:1 bidirectional (revertive mode, non-revertive mode);

b) 1+1 bidirectional (revertive mode, non-revertive mode);

c) 1+1 unidirectional (revertive mode, non-revertive mode).

Note that any global or local request which is not described in the state transition tables does not trigger any state transition.

NOTE – Re-assertion cases in state transition tables for far-end requests are provided to facilitate understanding, and are otherwise covered by subnumeral b): i) of clause 11.2.1.

A.1 State transition for 1:1 bidirectional switching with revertive mode

A.1.1 Local requests

Table A.1 shows the state transition by a local request for the 1:1 protection switching in revertive mode.

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	k	l	m	n	o
			Lockout	Forced switch	SF on working [a]	Working recovers from SF	SF on protection [a]	Protectio n recovers from SF	SD on working [a]	Working recovers from SD	SD on protection [a]	Protection recovers from SD	Manual switch to protection	Manual switch to working	Clear	Exercise	WTR timer expires
A	No Request Working/Active Protection/Standby	NR [r/b=null]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	→K	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	→E	O	→F	N/A	→P	O	→Q	N/A	→G	→H	N/A	O	N/A
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	O	O	O	O	O	O	O	O	O	O	O	O	→A or →E[b] or →F[c] or →P[d] or →Q[e]	O	N/A
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	O	O	O	O	O	→A or →E[b] or →P[d] or →Q[e]	O	N/A
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→I or →P[d] or →Q[e]	→F	N/A	O	O	O	O	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 or →E[b] or →P[d] or →Q[e]	O	O	O	O	O	O	N/A	O	N/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**	**k**	**l**	**m**	**n**	**o**
			Lockout	**Forced switch**	**SF on working** [a)]	**Working recovers from SF**	**SF on protection** [a)]	**Protection recovers from SF**	**SD on working** [a)]	**Working recovers from SD**	**SD on protection** [a)]	**Protection recovers from SD**	**Manual switch to protection**	**Manual switch to working**	**Clear**	**Exercise**	**WTR timer expires**
P	Signal Degrade (W) Working/Standby Protection/Active	SD [r/b=normal]	→C	→D	→E	N/A	→F	N/A	N/A	→I or →Q[e)]	O	O	O	O	N/A	O	N/A
Q	Signal Degrade (P) Working/Active Protection/Standby	SD [r/b=null]	→C	→D	→E	N/A	→F	N/A	O	O	N/A	→A or →P[d)]	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	→P	N/A	→Q	N/A	O	O	→A	O	N/A
H	Manual Switch Working/Active Protection/Standby	MS [r/b=null]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	O	O	→A	O	N/A
I	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	→A	O	→A
K	Exercise Working/Active Protection/Standby	EXER [r/b=null]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	→A	O	N/A
M	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	→K	N/A

NOTE 1 – "N/A" means that the event 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 remains unchanged.

a) Signal fail (SF) or signal degrade (SD) on working or protection is input to the local priority logic only if the SF or SD still exists after hold-off timer expires.

b) If SF is reasserted.

c) If SF-P is reasserted.

d) If SD (W) is reasserted.

e) If SD (P) is reasserted.

A.1.2 Far-end requests

Table A.2 shows the state transition by a far-end request received by APS for the 1:1 bidirectional protection switching in revertive mode.

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

	State	Signalled APS	Received far-end request													
			p	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**aa**	**ab**	**ac**
			LO	**SF-P**	**FS**	**SF**	**SD**	**SD**	**MS**	**MS**	**WTR**	**EXER**	**RR**	**NR**	**NR**	**DNR**
			[r/b= null]	**[r/b= null]**	**[r/b= normal]**	**[r/b= normal]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= null]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= normal]**
A	No Request Working/Active Protection/Standby	NR [r/b=null]	(→A)	(→A)	→B	→B	→B	(→A)	→B	(→A)	→B	→M	(→A)	(→A) or →E[a)] or →F[b)] or →P[d)] or →Q[e)]	(→A)	→B
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	→A	(→B)	→A	(→B)	N/A	N/A	→A or →E[a)] or →P[d)]	→A or →I[c)]	(→B)
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	(→C)	O	O	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	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	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	O	O
P	Signal Degrade (W) Working/Standby Protection/Active	SD [r/b=normal]	→A	→A	→B	→B	(→P)	O	O	O	O	O	O	O	O	O

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

State		Signalled APS	Received far-end request													
			p	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**aa**	**ab**	**ac**
			LO	**SF-P**	**FS**	**SF**	**SD**	**SD**	**MS**	**MS**	**WTR**	**EXER**	**RR**	**NR**	**NR**	**DNR**
			[r/b= null]	**[r/b= null]**	**[r/b= normal]**	**[r/b= normal]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= null]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= normal]**
Q	Signal Degrade (P) Working/Active Protection/Standby	SD [r/b=null]	→A	→A	→B	→B	O	(→Q)	O	O	O	O	O	O	O	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→A	→A	→B	→B	→B	→A	(→G)	(→G) or →A[f)]	O	O	O	O	O	O
H	Manual Switch Working/Active Protection/Standby	MS [r/b=null]	→A	→A	→B	→B	→B	→A	O	(→H)	O	O	O	O	O	O
I	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→A	→A	→B	→B	→B	→A	→B	→A	(→I)	O	O	N/A	O	O
K	Exercise Working/Active Protection/Standby	EXER [r/b=null]	→A	→A	→B	→B	→B	→A	→B	→A	N/A	(→K)	(→K)	O	N/A	O
M	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	→A	→A	→B	→B	→B	→A	→B	→A	N/A	(→M)	→A	→A	N/A	O

NOTE 1 – "N/A" means that the event 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 remains unchanged.

a) If SF is reasserted.

b) If SF-P is reasserted.

c) If the previous local state is SF (or SD (W) if applicable, see clause 11.13).

d) If SD (W) is reasserted.

e) If SD (P) is reasserted.

f) Only if the far-end request is due to the simultaneous application of a manual switch to working command at the far end (i.e., no NR request acknowledging the local MS state received previously from the far end).

A.2 State transition for 1:1 bidirectional switching with non-revertive mode

A.2.1 Local requests

Table A.3 shows the state transition by a local request for the 1:1 bidirectional protection switching in non-revertive mode.

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	j	k	l	m	n
			Lockout	Forced switch	SF on working [a)]	Working recovers from SF	SF on protection [a)]	Protection recovers from SF	SD on working [a)]	Working recovers from SD	SD on protection [a)]	Protection recovers from SD	Manual switch to protection	Manual switch to working	Clear	Exercise
A	No Request Working/Active Protection/Standby	NR [r/b=null]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	→K
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	→E	O	→F	N/A	→P	O	→Q	N/A	→G	→H	N/A	O
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	O	O	O	O	O	O	O	O	O	O	O	O	→A or →E[b)] or →F[c)] or →P[d)] or →Q[e)]	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	O	O	O	O	O	→J or →E[b)] or →P[d)] or →Q[e)]	O
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→J or →P[d)] or →Q[e)]	→F	N/A	O	O	O	O	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 or →E[b)] or →P[d)] or →Q[e)]	O	O	O	O	O	O	N/A	O
P	Signal Degrade (W) Working/Standby Protection/Active	SD [r/b=normal]	→C	→D	→E	N/A	→F	N/A	N/A	→J or →Q[e)]	O	O	O	O	N/A	O

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	j	k	l	m	n
			Lockout	**Forced switch**	**SF on working** a)	**Working recovers from SF**	**SF on protection** a)	**Protection recovers from SF**	**SD on working** a)	**Working recovers from SD**	**SD on protection** a)	**Protection recovers from SD**	**Manual switch to protection**	**Manual switch to working**	**Clear**	**Exercise**
Q	Signal Degrade (P) Working/Active Protection/Standby	SD [r/b=null]	→C	→D	→E	N/A	→F	N/A	O	O	N/A	→A or →P[d)]	O	O	N/A	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	O	O	→J	O
H	Manual Switch Working/Active Protection/Standby	MS [r/b=null]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	O	O	→A	O
J	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	→L
K	Exercise Working/Active Protection/Standby	EXER [r/b=null]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	→A	O
L	Exercise Working/Standby Protection/Active	EXER [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	→J	O
M	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	→K
N	Reverse Request Working/Standby Protection/Active	RR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	→L

NOTE 1 – "N/A" means that the event 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 remains unchanged.

a) Signal fail (SF) or signal degrade (SD) on working or protection is input to the local priority logic only if the SF or SD still exists after hold-off timer expires.

b) If SF is reasserted.

c) If SF-P is reasserted.

d) If SD (W) is reasserted.

e) If SD (P) is reasserted.

A.2.2 Far-end requests

Table A.4 shows the state transition by a far-end request received by APS for the 1:1 bidirectional protection switching in non-revertive mode.

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

State		Signalled APS	Received far-end request															
			o	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**aa**	**ab**	**ac**	**ad**
			LO	**SF-P**	**FS**	**SF**	**SD**	**SD**	**MS**	**MS**	**WTR**	**EXER**	**EXER**	**RR**	**RR**	**NR**	**NR**	**DNR**
			[r/b= null]	**[r/b= null]**	**[r/b= normal]**	**[r/b= normal]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= normal]**
A	No Request Working/Active Protection/Standby	NR [r/b=null]	(→A)	(→A)	→B	→B	→B	(→A)	→B	(→A)	→B	→M	N/A	(→A)	N/A	(→A) or →E[a] or →F[b] or →P[c] or →Q[d]	(→A)	→J
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	→A	(→B)	→A	(→B)	N/A	N/A	N/A	N/A	→A or →E[a] or →P[c]	→J	→J
C	Lockout Working/Active Protection/Standby	LO [r/b=null]	(→C)	O	O	O	O	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	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	O	O	O	O
F	Signal Fail (P)	SF-P	→A	(→F)	O	O	O	O	O	O	O	O	O	O	O	O	O	O
P	Signal Degrade (W) Working/Standby Protection/Active	SD [r/b=normal]	→A	→A	→B	→B	(→P)	O	O	O	O	O	O	O	O	O	O	O
Q	Signal Degrade (P) Working/Active Protection/Standby	SD [r/b=null]	→A	→A	→B	→B	O	(→Q)	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	→B	→A	(→G)	(→G) or →A[e]	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															
			o	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**aa**	**ab**	**ac**	**ad**
			LO	**SF-P**	**FS**	**SF**	**SD**	**SD**	**MS**	**MS**	**WTR**	**EXER**	**EXER**	**RR**	**RR**	**NR**	**NR**	**DNR**
			[r/b= null]	**[r/b= null]**	**[r/b= normal]**	**[r/b= normal]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= null]**	**[r/b= normal]**	**[r/b= normal]**
H	Manual Switch Working/Active Protection/Standby	MS [r/b=null]	→A	→A	→B	→B	→B	→A	O	(→H)	O	O	O	O	O	O	O	O
J	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→A	→A	→B	→B	→B	→A	→B	→A	→B	N/A	→N	N/A	(→J)	O	O	(→J)
K	Exercise Working/Active Protection/Standby	EXER [r/b=null]	→A	→A	→B	→B	→B	→A	→B	→A	→B	(→K)	N/A	(→K)	N/A	O	N/A	N/A
L	Exercise Working/Standby Protection/Active	EXER [r/b=normal]	→A	→A	→B	→B	→B	→A	→B	→A	→B	N/A	(→L)	N/A	(→L)	N/A	O	O
M	Reverse Request Working/Active Protection/Standby	RR [r/b=null]	→A	→A	→B	→B	→B	→A	→B	→A	→B	(→M)	N/A	→A	N/A	→A	N/A	N/A
N	Reverse Request Working/Standby Protection/Active	RR [r/b=normal]	→A	→A	→B	→B	→B	→A	→B	→A	→B	N/A	(→N)	N/A	→J	N/A	N/A	→J

NOTE 1 – "N/A" means that the event 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 remains unchanged.

a) If SF is reasserted.

b) If SF-P is reasserted.

c) If SD (W) is reasserted.

d) If SD (P) is reasserted.

e) Only if the far-end request is due to the simultaneous application of a manual switch to working command at the far end (i.e., no NR request acknowledging the local MS state received previously from the far end).

A.3 State transition for 1+1 bidirectional switching with revertive mode

A.3.1 Local requests

Table A.5 shows the state transition by a local request for the 1+1 bidirectional protection switching in revertive mode.

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**	**k**	**l**	**m**	**n**	**o**
			Lockout	**Forced switch**	**SF on working** [a)]	**Working recovers from SF**	**SF on protection** [a)]	**Protection recovers from SF**	**SD on working** [a)]	**Working recovers from SD**	**SD on protection** [a)]	**Protection recovers from SD**	**Manual switch to protection**	**Manual switch to working**	**Clear**	**Exercise**	**WTR timer expires**
A	No Request Working/Active Protection/Standby	NR [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	→K	N/A
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	→E	O	→F	N/A	→P	O	→Q	N/A	→G	→H	N/A	O	N/A
C	Lockout Working/Active Protection/Standby	LO [r=null, b=normal]	O	O	O	O	O	O	O	O	O	O	O	O	→A or →E[b)] or →F[c)] or →P[d)] or →Q[e)]	O	N/A
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	O	O	O	O	O	→A or →E[b)] or →P[d)] or →Q[e)]	O	N/A
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→I or →P[d)] or →Q[e)]	→F	N/A	O	O	O	O	O	O	N/A	O	N/A
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r=null, b=normal]	→C	O	O	O	N/A	→A or →E[b)] or →P[d)] or →Q[e)]	O	O	O	O	O	O	N/A	O	N/A
P	Signal Degrade (W) Working/Standby Protection/Active	SD [r/b=normal]	→C	→D	→E	N/A	→F	N/A	N/A	→I or →Q[e)]	O	O	O	O	N/A	O	N/A

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	k	l	m	n	o
			Lockout	Forced switch	SF on working a)	Working recovers from SF	SF on protection a)	Protection recovers from SF	SD on working a)	Working recovers from SD	SD on protection a)	Protection recovers from SD	Manual switch to protection	Manual switch to working	Clear	Exercise	WTR timer expires
Q	Signal Degrade (P) Working/Active Protection/Standby	SD [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	O	O	N/A	→A or →P[d)]	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	→P	N/A	→Q	N/A	O	O	→A	O	N/A
H	Manual Switch Working/Active Protection/Standby	MS [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	O	O	→A	O	N/A
I	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	→A	O	→A
K	Exercise Working/Active Protection/Standby	EXER [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	→A	O	N/A
M	Reverse Request Working/Active Protection/Standby	RR [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	→K	N/A

NOTE 1 – "N/A" means that the event 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 remains unchanged.

a) Signal fail (SF) or signal degrade (SD) on working or protection is input to the local priority logic only if the SF or SD still exists after hold-off timer expires.

b) If SF is reasserted.

c) If SF-P is reasserted.

d) If SD (W) is reasserted.

e) If SD (P) is reasserted.

A.3.2 Far-end requests

Table A.6 shows the state transition by a far-end request received by APS for the 1+1 bidirectional protection switching in revertive mode.

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

State		Signalled APS	Received far-end request													
			p	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**aa**	**ab**	**ac**
			LO	**SF-P**	**FS**	**SF**	**SD**	**SD**	**MS**	**MS**	**WTR**	**EXER**	**RR**	**NR**	**NR**	**DNR**
			[r=null, b=normal]	**[r=null, b=normal]**	**[r/b= normal]**	**[r/b= normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**r=null, b=normal]**	**r=null, b=normal]**	**r=null, b=normal]**	**[r/b= normal]**	**[r/b= normal]**
A	No Request Working/Active Protection/Standby	NR [r=null, b=normal]	(→A)	(→A)	→B	→B	→B	(→A)	→B	(→A)	→B	→M	(→A)	(→A) or →E a) or →F b) or →P d) or →Q e)	(→A)	→B
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	→A	(→B)	→A	(→B)	N/A	N/A	→A or →E a) or →P d)	→A or →I c)	(→B)
C	Lockout Working/Active Protection/Standby	LO [r=null, b=normal]	(→C)	O	O	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	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	O	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r=null, b=normal]	→A	(→F)	O	O	O	O	O	O	O	O	O	O	O	O
P	Signal Degrade (W) Working/Standby Protection/Active	SD [r/b=normal]	→A	→A	→B	→B	(→P)	O	O	O	O	O	O	O	O	O
Q	Signal Degrade (P) Working/Active Protection/Standby	SD [r=null, b=normal]	→A	→A	→B	→B	O	(→Q)	O	O	O	O	O	O	O	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→A	→A	→B	→B	→B	→A	(→G)	(→G) or →A f)	O	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													
			p	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**aa**	**ab**	**ac**
			LO	**SF-P**	**FS**	**SF**	**SD**	**SD**	**MS**	**MS**	**WTR**	**EXER**	**RR**	**NR**	**NR**	**DNR**
			[r=null, b=normal]	**[r=null, b=normal]**	**[r/b= normal]**	**[r/b= normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**r=null, b=normal]**	**r=null, b=normal]**	**r=null, b=normal]**	**[r/b= normal]**	**[r/b= normal]**
H	Manual Switch Working/Active Protection/Standby	MS [r=null, b=normal]	→A	→A	→B	→B	→B	→A	O	(→H)	O	O	O	O	O	O
I	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→A	→A	→B	→B	→B	→A	→B	→A	(→I)	O	O	N/A	O	O
K	Exercise Working/Active Protection/Standby	EXER [r=null, b=normal]	→A	→A	→B	→B	→B	→A	→B	→A	N/A	(→K)	(→K)	O	N/A	O
M	Reverse Request Working/Active Protection/Standby	RR [r=null, b=normal]	→A	→A	→B	→B	→B	→A	→B	→A	N/A	(→M)	→A	→A	N/A	O

NOTE 1 – "N/A" means that the event 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 remains unchanged.

a) If SF is reasserted.

b) If SF-P is reasserted.

c) If the previous local state is SF (or SD (W) if applicable, see clause 11.13).

d) If SD (W) is reasserted.

e) If SD (P) is reasserted.

f) Only if the far-end request is due to the simultaneous application of a manual switch to working command at the far end (i.e., no NR request acknowledging the local MS state received previously from the far end).

A.4 State transition for 1+1 bidirectional switching with non-revertive mode

A.4.1 Local requests

Table A.7 shows the state transition by a local request for the 1+1 bidirectional protection switching in non-revertive mode.

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	j	k	l	m	n
			Lockout	Forced switch	SF on working [a]	Working recovers from SF	SF on protection [a]	Protection recovers from SF	SD on working [a]	Working recovers from SD	SD on protection [a]	Protection recovers from SD	Manual switch to protection	Manual switch to working	Clear	Exercise
A	No Request Working/Active Protection/Standby	NR [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	→K
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→C	→D	→E	O	→F	N/A	→P	O	→Q	N/A	→G	→H	N/A	O
C	Lockout Working/Active Protection/Standby	LO [r=null, b=normal]	O	O	O	O	O	O	O	O	O	O	O	O	→A or →E[b] or →F[c] or →P[d] or →Q[e]	O
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	O	O	O	O	O	→J or →E[b] or →P[d] or →Q[e]	O
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→J or →P[d] or →Q[e]	→F	N/A	O	O	O	O	O	O	N/A	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r=null, b=normal]	→C	O	O	O	N/A	→A or →E[b] or →P[d] or →Q[e]	O	O	O	O	O	O	N/A	O
P	Signal Degrade (W) Working/Standby Protection/Active	SD [r/b=normal]	→C	→D	→E	N/A	→F	N/A	N/A	→J or →Q[e]	O	O	O	O	N/A	O
Q	Signal Degrade (P) Working/Active Protection/Standby	SD [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	O	O	N/A	→A or →P[d]	O	O	N/A	O
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	O	O	→J	O

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	j	k	l	m	n
			Lockout	Forced switch	SF on working a)	Working recovers from SF	SF on protection a)	Protection recovers from SF	SD on working a)	Working recovers from SD	SD on protection a)	Protection recovers from SD	Manual switch to protection	Manual switch to working	Clear	Exercise
H	Manual Switch Working/Active Protection/Standby	MS [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	O	O	→A	O
J	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	→L
K	Exercise Working/Active Protection/Standby	EXER [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	→A	O
L	Exercise Working/Standby Protection/Active	EXER [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	→J	O
M	Reverse Request Working/Active Protection/Standby	RR [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	→K
N	Reverse Request Working/Standby Protection/Active	RR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	→L

NOTE 1 – "N/A" means that the event 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 remains unchanged.

a) Signal fail (SF) or signal degrade (SD) on working or protection is input to the local priority logic only if the SF or SD still exists after hold-off timer expires.

b) If SF is reasserted.

c) If SF-P is reasserted.

d) If SD (W) is reasserted.

e) If SD (P) is reasserted.

A.4.2 Far-end requests

Table A.8 shows the state transition by a far-end request received by APS for the 1+1 bidirectional protection switching in non-revertive mode.

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

State		Signalled APS	Received far-end request															
			o	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**aa**	**ab**	**ac**	**ad**
			LO	**SF-P**	**FS**	**SF**	**SD**	**SD**	**MS**	**MS**	**WTR**	**EXER**	**EXER**	**RR**	**RR**	**NR**	**NR**	**DNR**
			[r=null, b=normal]	**[r=null, b=normal]**	**[r/b= normal]**	**[r/b= normal**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r/b= normal]**
A	No Request Working/Active Protection/Standby	NR [r=null, b=normal]	(→A)	(→A)	→B	→B	→B	(→A)	→B	(→A)	→B	→M	N/A	(→A)	N/A	(→A) or →E[a)] or →F[b)] or →P[c)] or →Q[d)]	(→A)	→J
B	No Request Working/Standby Protection/Active	NR [r/b=normal]	→A	→A	(→B)	(→B)	(→B)	→A	(→B)	→A	(→B)	N/A	N/A	N/A	N/A	→A or→E[a)] or →P[c)]	→J	→J
C	Lockout Working/Active Protection/Standby	LO [r= null, b=normal]	(→C)	O	O	O	O	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	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	O	O	O	O
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r= null, b=normal]	→A	(→F)	O	O	O	O	O	O	O	O	O	O	O	O	O	O
P	Signal Degrade (W) Working/Standby Protection/Active	SD [r/b=normal]	→A	→A	→B	→B	(→P)	O	O	O	O	O	O	O	O	O	O	O

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

	State	Signalled APS	Received far-end request															
			o	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**aa**	**ab**	**ac**	**ad**
			LO	**SF-P**	**FS**	**SF**	**SD**	**SD**	**MS**	**MS**	**WTR**	**EXER**	**EXER**	**RR**	**RR**	**NR**	**NR**	**DNR**
			[r=null, b=normal]	**[r=null, b=normal]**	**[r/b= normal]**	**[r/b= normal**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r/b= normal]**
Q	Signal Degrade (P) Working/Active Protection/Standby	SD [r= null, b=normal]	→A	→A	→B	→B	O	(→Q)	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	→B	→A	(→G)	(→G) or →A[e)]	O	O	O	O	O	O	O	O
H	Manual Switch Working/Active Protection/Standby	MS [r= null, b=normal]	→A	→A	→B	→B	→B	→A	O	(→H)	O	O	O	O	O	O	O	O
J	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→A	→A	→B	→B	→B	→A	→B	→A	→B	N/A	→N	N/A	(→J)	O	O	(→J)
K	Exercise Working/Active Protection/Standby	EXER [r=null, b=normal]	→A	→A	→B	→B	→B	→A	→B	→A	→B	(→K)	N/A	(→K)	N/A	O	N/A	N/A
L	Exercise Working/Standby Protection/Active	EXER [r/b=normal]	→A	→A	→B	→B	→B	→A	→B	→A	→B	N/A	(→L)	N/A	(→L)	N/A	O	O
M	Reverse Request Working/Active Protection/Standby	RR [r=null, b=normal]	→A	→A	→B	→B	→B	→A	→B	→A	→B	(→M)	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															
			o	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**	**aa**	**ab**	**ac**	**ad**
			LO	**SF-P**	**FS**	**SF**	**SD**	**SD**	**MS**	**MS**	**WTR**	**EXER**	**EXER**	**RR**	**RR**	**NR**	**NR**	**DNR**
			[r=null, b=normal]	**[r=null, b=normal]**	**[r/b= normal]**	**[r/b= normal**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r=null, b=normal]**	**[r/b= normal]**	**[r/b= normal]**
N	Reverse Request Working/Standby Protection/Active	RR [r/b=normal]	→A	→A	→B	→B	→B	→A	→B	→A	→B	N/A	(→N)	N/A	→J	N/A	N/A	→J

NOTE 1 – "N/A" means that the event 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 remains unchanged.

a) If SF is reasserted.

b) If SF-P is reasserted.

c) If SD (W) is reasserted.

d) If SD (P) is reasserted.

e) Only if the far-end request is due to the simultaneous application of a manual switch to working command at the far end (i.e., no NR request acknowledging the local MS state received previously from the far end).

A.5 State transition for 1+1 unidirectional switching with revertive mode

A.5.1 Local requests

Table A.9 shows the state transition by a local request for the 1+1 unidirectional protection switching in revertive mode.

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

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

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

State		Signalled APS	Local request														
			a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
			Lockout	**Forced switch**	**SF on working** a)	**Working recovers from SF**	**SF on protection** a)	**Protection recovers from SF**	**SD on working** a)	**Working recovers from SD**	**SD on protection** a)	**Protection recovers from SD**	**Manual switch to protection**	**Manual switch to working**	**Clear**	**Exercise**	**WTR timer expires**
H	Manual Switch Working/Active Protection/Standby	MS [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	O	O	→A	N/A	N/A
I	Wait to Restore Working/Standby Protection/Active	WTR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	→A	N/A	→A

NOTE 1 – Signalled APS is communicated in the case of 1+1 unidirectional protection switching with APS communication but does not trigger any state transition.
NOTE 2 – "N/A" means that the event is not expected to happen for the State. However if it does happen, the event should be ignored.
NOTE 3 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.
NOTE 4 – "(→X)" represents that the state is not changed and remains the same state.
a) Signal Fail or Signal Degrade on working or protection is input to the local priority logic only if the Signal Fail or Signal Degrade still exists after hold-off timer expires.
b) If SF is reasserted.
c) If SF-P is reasserted.
d) If SD (W) is reasserted.
e) If SD (P) is reasserted.

A.6 State transition for 1+1 unidirectional switching with non-revertive mode

A.6.1 Local requests

Table A.10 shows the state transition by a local request for the 1+1 unidirectional protection switching in non-revertive mode.

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

State		Signalled APS	Local request													
			a	b	c	d	e	f	g	h	i	j	k	l	m	n
			Lockout	**Forced switch**	**SF on working** [a)]	**Working recovers from SF**	**SF on protection** [a)]	**Protection recovers from SF**	**SD on working** [a)]	**Working recovers from SD**	**SD on protection** [a)]	**Protection recovers from SD**	**Manual switch to protection**	**Manual switch to working**	**Clear**	**Exercise**
A	No Request Working/Active Protection/Standby	NR [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	N/A
C	Lockout Working/Active Protection/Standby	LO [r=null, b=normal]	O	O	O	O	O	O	O	O	O	O	O	O	→A or →E [b)] or →F [c)] or →P [d)] or →Q [e)]	N/A
D	Forced Switch Working/Standby Protection/Active	FS [r/b=normal]	→C	O	O	O	→F	N/A	O	O	O	O	O	O	→J or →E [b)] or →P [d)] or →Q [e)]	N/A
E	Signal Fail (W) Working/Standby Protection/Active	SF [r/b=normal]	→C	→D	N/A	→J or →P [d)] or →Q [e)]	→F	N/A	O	O	O	O	O	O	N/A	N/A
F	Signal Fail (P) Working/Active Protection/Standby	SF-P [r=null, b=normal]	→C	O	O	O	N/A	→A or →E [b)] or →P [d)] or →Q [e)]	O	O	O	O	O	O	N/A	N/A
P	Signal Degrade (W) Working/Standby Protection/Active	SD [r/b=normal]	→C	→D	→E	N/A	→F	N/A	N/A	→J or →Q [e)]	O	O	O	O	N/A	N/A
Q	Signal Degrade (P) Working/Active Protection/Standby	SD [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	O	O	N/A	→A or →P [d)]	O	O	N/A	N/A
G	Manual Switch Working/Standby Protection/Active	MS [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	O	O	→J	N/A

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

State		Signalled APS	Local request													
			a	b	c	d	e	f	g	h	i	j	k	l	m	n
			Lockout	Forced switch	SF on working [a]	Working recovers from SF	SF on protection [a]	Protection recovers from SF	SD on working [a]	Working recovers from SD	SD on protection [a]	Protection recovers from SD	Manual switch to protection	Manual switch to working	Clear	Exercise
H	Manual Switch Working/Active Protection/Standby	MS [r=null, b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	O	O	→A	N/A
J	Do Not Revert Working/Standby Protection/Active	DNR [r/b=normal]	→C	→D	→E	N/A	→F	N/A	→P	N/A	→Q	N/A	→G	→H	N/A	N/A

NOTE 1 – Signalled APS is communicated in the case of 1+1 unidirectional protection switching with APS communication but does not trigger any state transition.

NOTE 2 – "N/A" means that the event is not expected to happen for the State. However if it does happen, the event should be ignored.

NOTE 3 – "O" means that the request shall be overruled by the existing condition because it has an equal or a lower priority.

[a] Signal Fail or Signal Degrade on working or protection is input to the local priority logic only if the Signal Fail or Signal Degrade still exists after hold-off timer expires.

[b] If SF is reasserted.

[c] If SF-P is reasserted.

[d] If SD (W) is reasserted.

[e] If SD (P) is reasserted.

Appendix I

Example of operation of 1-phase APS protocol

(This appendix does not form an integral part of this Recommendation.)

I.1 Introduction

Examples of operation of 1-phase APS protocol (1:1, revertive and non-revertive modes) are shown here.

I.2 Example scenario

I.2.1 Revertive mode

This example assumes the scenario below.

1) The protected domain is operating without any defect (working entity is selected).
2) SF (signal fail) occurs in the West-to-East direction (switches to protection entity).
3) This defect is repaired (enters WTR state, maintains to select protection entity).
4) WTR timer expires (switches to working entity).

I.2.2 Non-revertive mode

This example assumes the scenario below.

1) The protected domain is operating without any defect (working entity is selected).
2) SF (signal fail) occurs in the West-to-East direction (switches to protection entity).
3) This defect is repaired (enters DNR state, maintains to select protection entity).

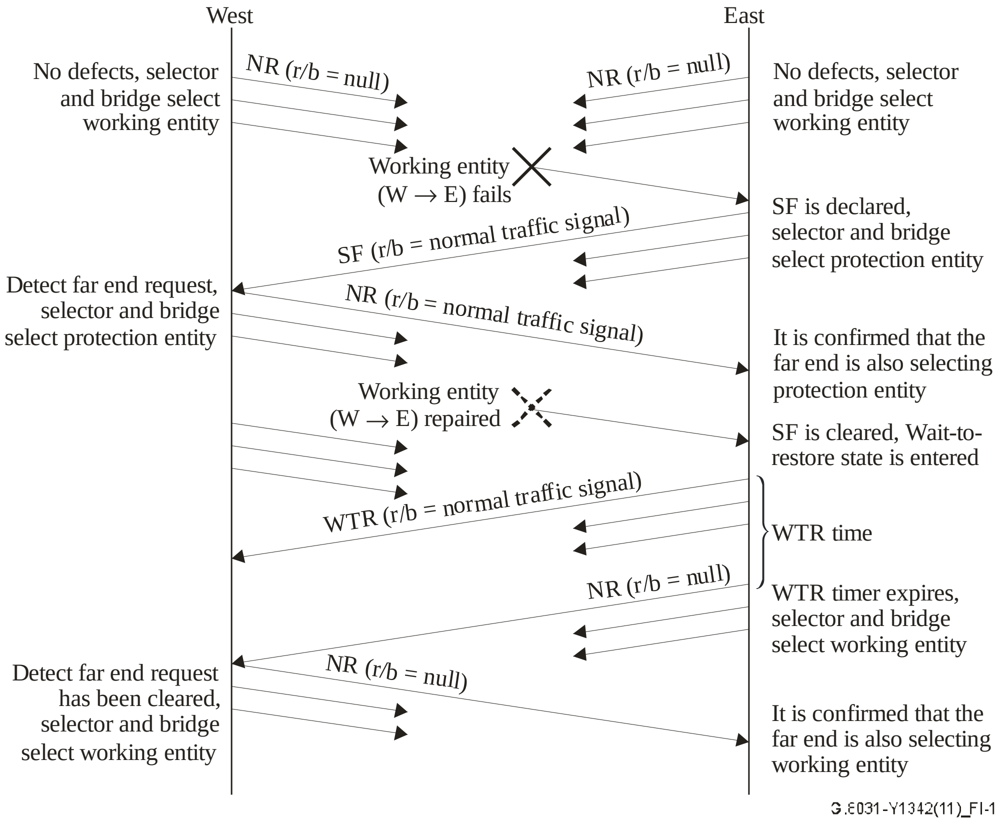
I.2.3 Signal fail and forced switch

This example assumes the scenario below.

1) SF (signal fail) occurs in the west-to-east direction (switches to protection entity).
2) FS (forced switch) command is accepted at east (enters FS state).
3) FS is cleared at east and SF is reasserted at east.

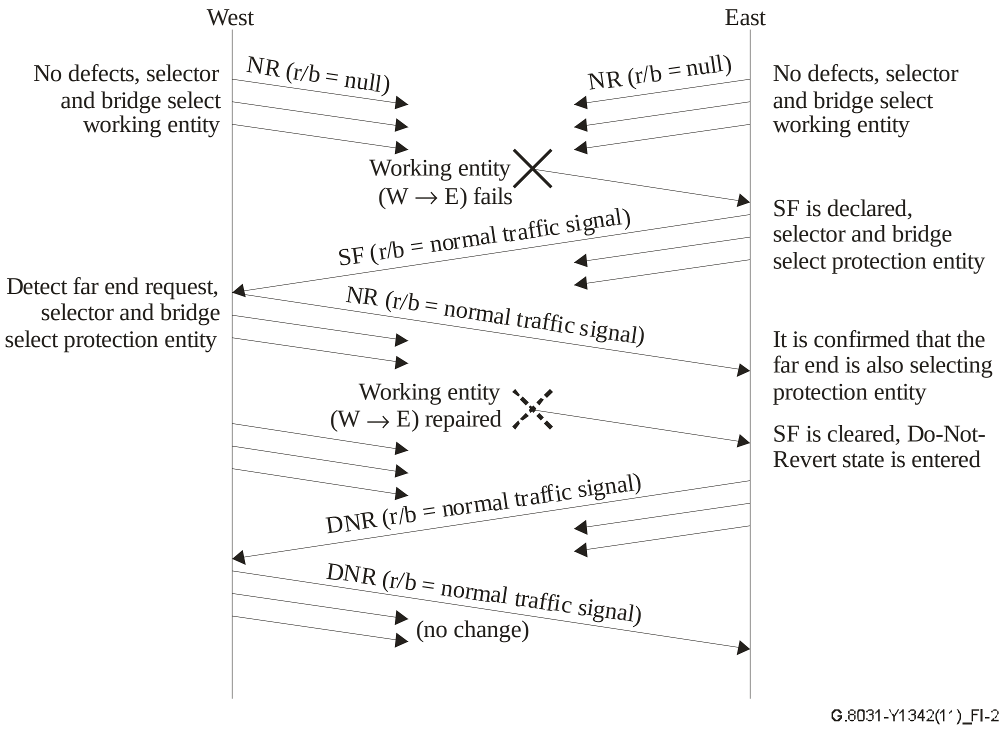
I.3 Examples of APS protocol

Examples of APS protocol are shown in Figure I.1 (revertive mode), Figure I.2 (non-revertive mode) and Figure I.3 (SF and FS).



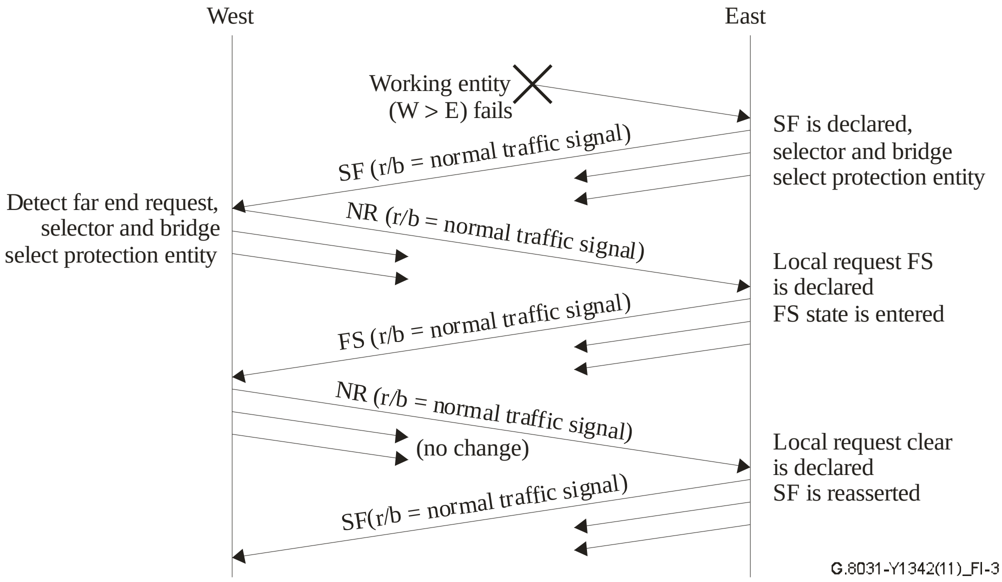
DNR	Do-Not-Revert	SF	Signal failure
NR	No request	WTR	Wait-To-Restore
r/b	Requested signal/bridged signal	W → E	West to east direction

Figure I.1 – Example of protocol (revertive mode)



NR	No request	WTR	Wait-To-Restore
r/b	Requested signal/bridged signal	DNR	Do-Not-Revert
SF	Signal failure	W → E	West to east direction

Figure I.2 – Example of protocol (non-revertive mode)



NR	No request	FS	Forced switch
r/b	Requested signal/bridged signal	$W \rightarrow E$	West to east direction
SF	Signal failure		

Figure I.3 – Example of protocol (SF and FS)

Appendix II

Interaction between Ethernet protection switching and spanning-tree protocol (STP)

(This appendix does not form an integral part of this Recommendation.)

This appendix shows that a bridge port within the protected domain must not participate in a spanning-tree protocol (STP) domain if it is to avoid undesirable interaction between STP and Ethernet protection switching. One way to ensure this is to disable the STP in the protected domain. However, domains outside of the protected domain could be STP-enabled. Another way to ensure this is for the working and protection transport entities to belong to two different STP domains. These two scenarios are discussed in this clause.

Figure II.1 shows the first way introduced above. The protected domain and STP domains (#1 and #2) are segmented vertically and do not overlap. Bridges #A and #B at the edge of the protected domain and STP domains interconnect the STP domains without any loop problem.

The second case mentioned above is shown in Figure II.2. STP domains (#1 and #2) are segmented horizontally, and provide two transport entities for Ethernet protection switching. Figure II.3 shows that the working and protection transport entities for Ethernet protection switching are provisioned separately within different STP domains. In this example, each VLAN and network resource would be used effectively.

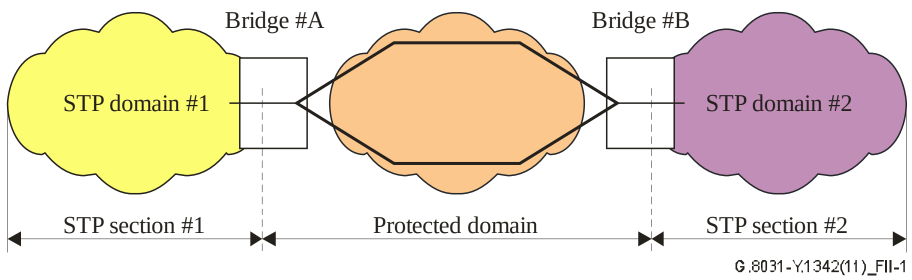


Figure II.1 – No overlapping between the protected domain and STP

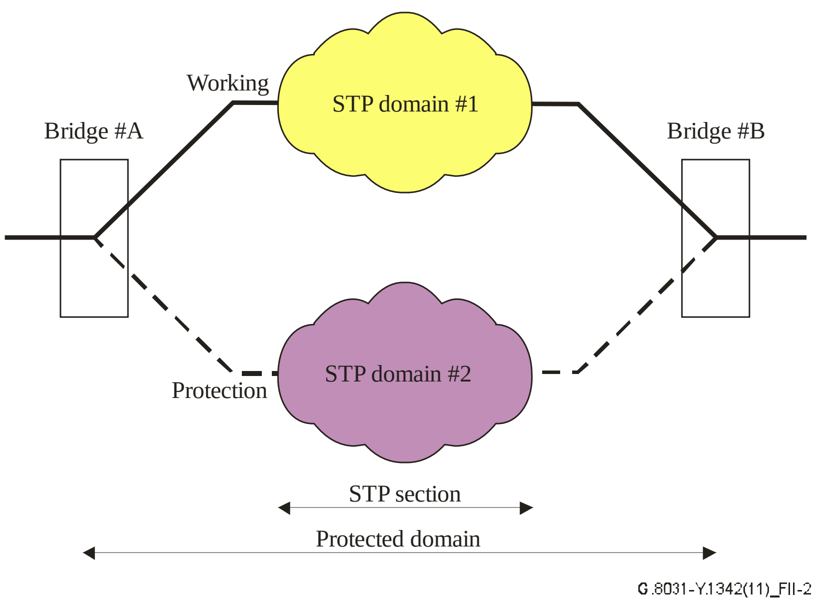


Figure II.2 – Overlapping between the protected domain and STP

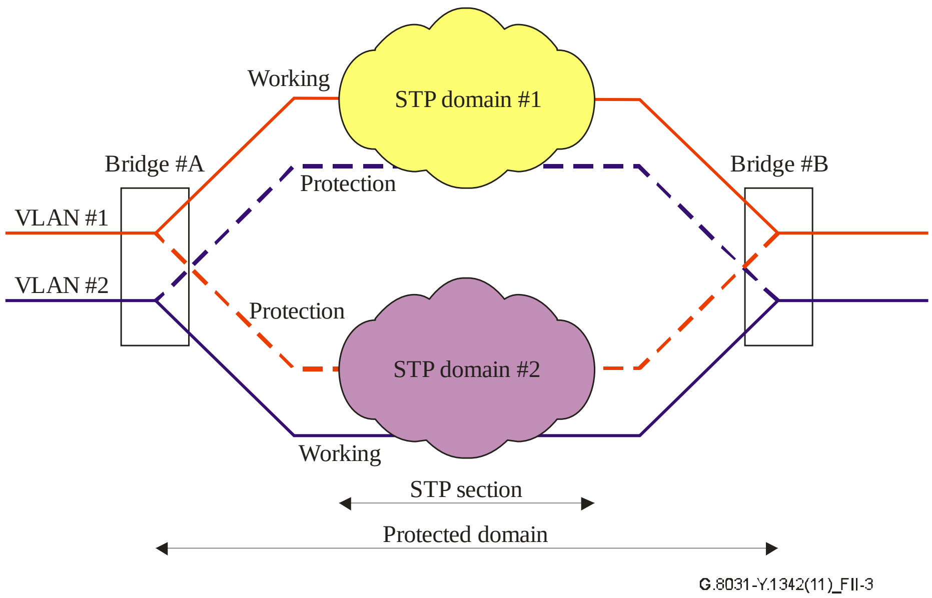


Figure II.3 – Overlapping between the protected domain and STP per VLAN

Appendix III

Maintenance entity group intermediate points for a protection switching environment

(This appendix does not form an integral part of this Recommendation.)

III.1 Introduction

In this appendix, considerations and examples of configuration of maintenance entity group intermediate points (MIPs) for a protection switching environment are shown.

III.2 Considerations

Figure III.1 shows an example of a configuration for protection switching of maintenance entity group end points (MEPs) and MIPs. In Figure III.1, two pairs of MEPs are configured to monitor both the working and protection transport entities in MEG Level N. Also, in MEG Level N+1, MEPs and MIPs are configured at each port as depicted in the figure.

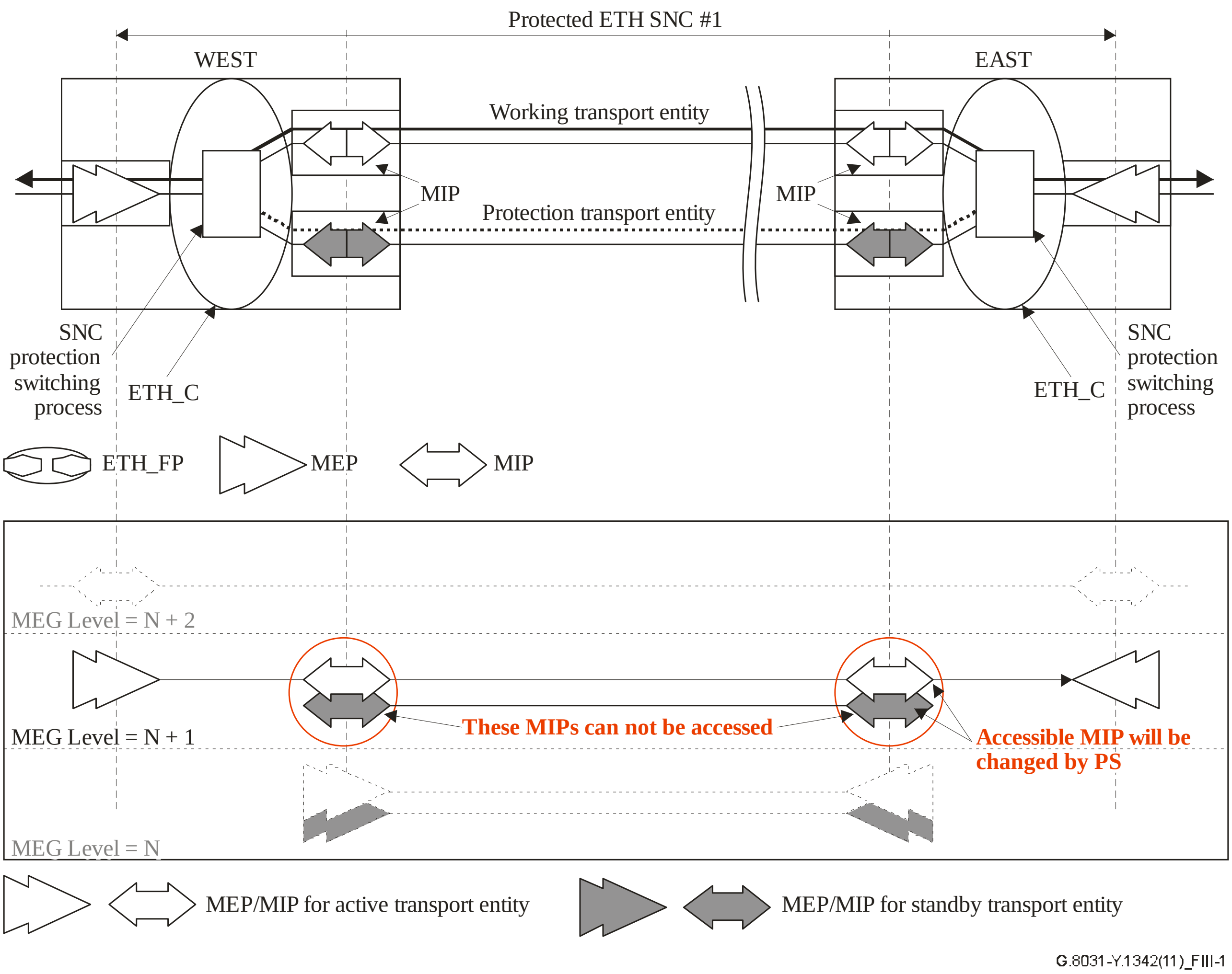


Figure III.1 – MEPs and MIPs for 1:1 bidirectional protection switching

If 1:1 protection switching is configured, MIPs in MEG Level N+1 on the standby transport entity cannot be accessed by MEPs for the same MEG, and accessible MIPs will be changed by the protection switching. Therefore, MIPs in MEG Level N+1 shown in Figure III.1, appear to be unnecessary.

Figure III.2 shows a configuration of MEPs and MIPs for a 1+1 unidirectional protection switching environment. In this case, a request/response communication between a MEP and a MIP cannot be made correctly. Therefore, MIPs in MEG Level N+1 shown in Figure III.2 also appear to be unnecessary.

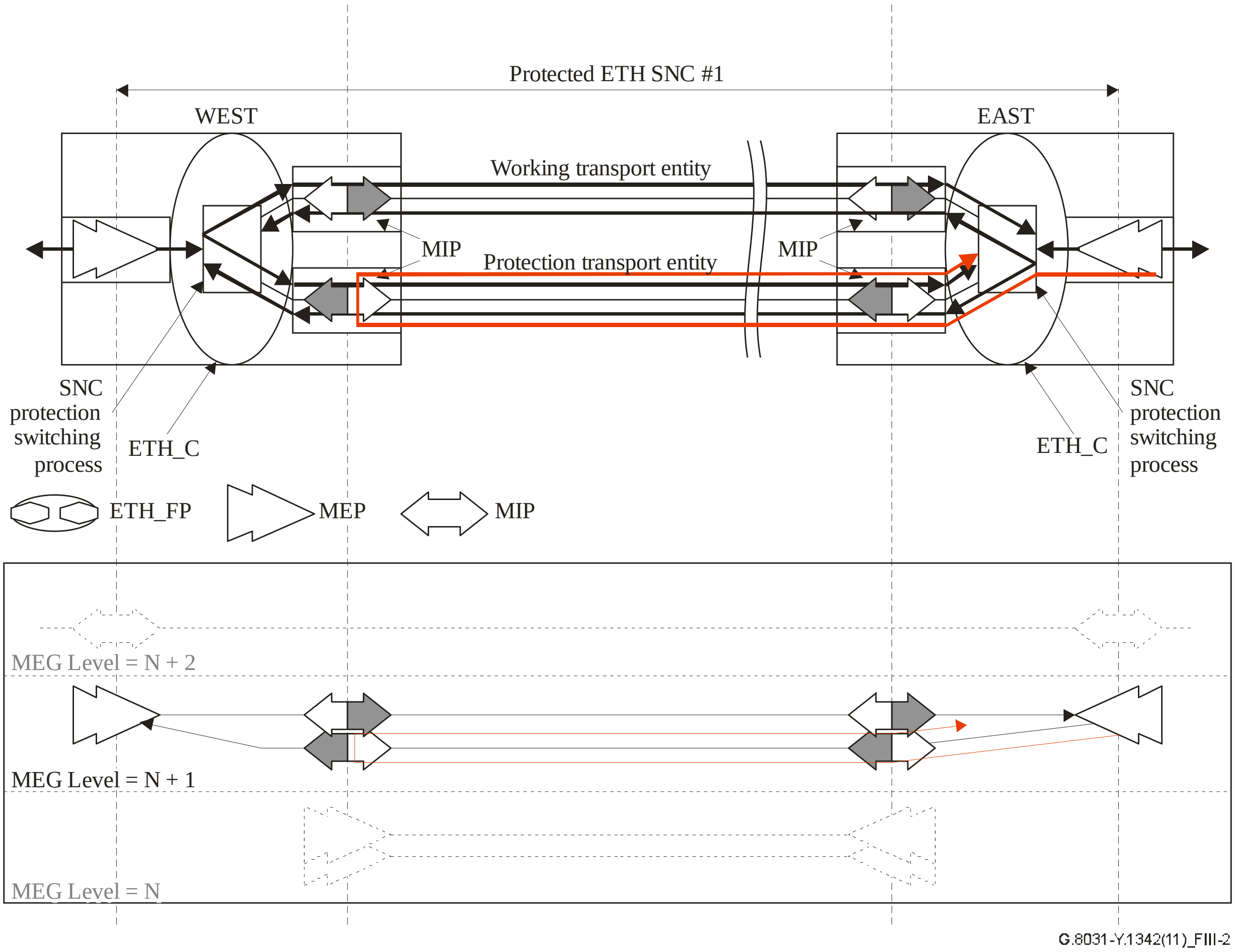


Figure III.2 – MEPs and MIPs for 1+1 unidirectional protection switching

As described above, configuring MIPs anywhere inside the protected domain, for a higher MEG Level than that of MEPs which monitors both working and protection transport entities, appears to be unnecessary.

III.3 Examples of configuration

Figure III.3 shows two examples of possible configuration of MEPs and MIPs.

In the first example, shown in the middle of Figure III.3, no MIPs are configured in MEG Level N+1, but MEPs are configured instead. In this case, the MEG in MEG Level N+1 represents the protected domain.

The second example is shown at the bottom of Figure III.3. In this configuration, MIPs are configured in MEG Level N+1 at the edge of the protected domain.

MEPs and MIPs shown in both examples are fully accessible because they are not configured inside the protected domain.

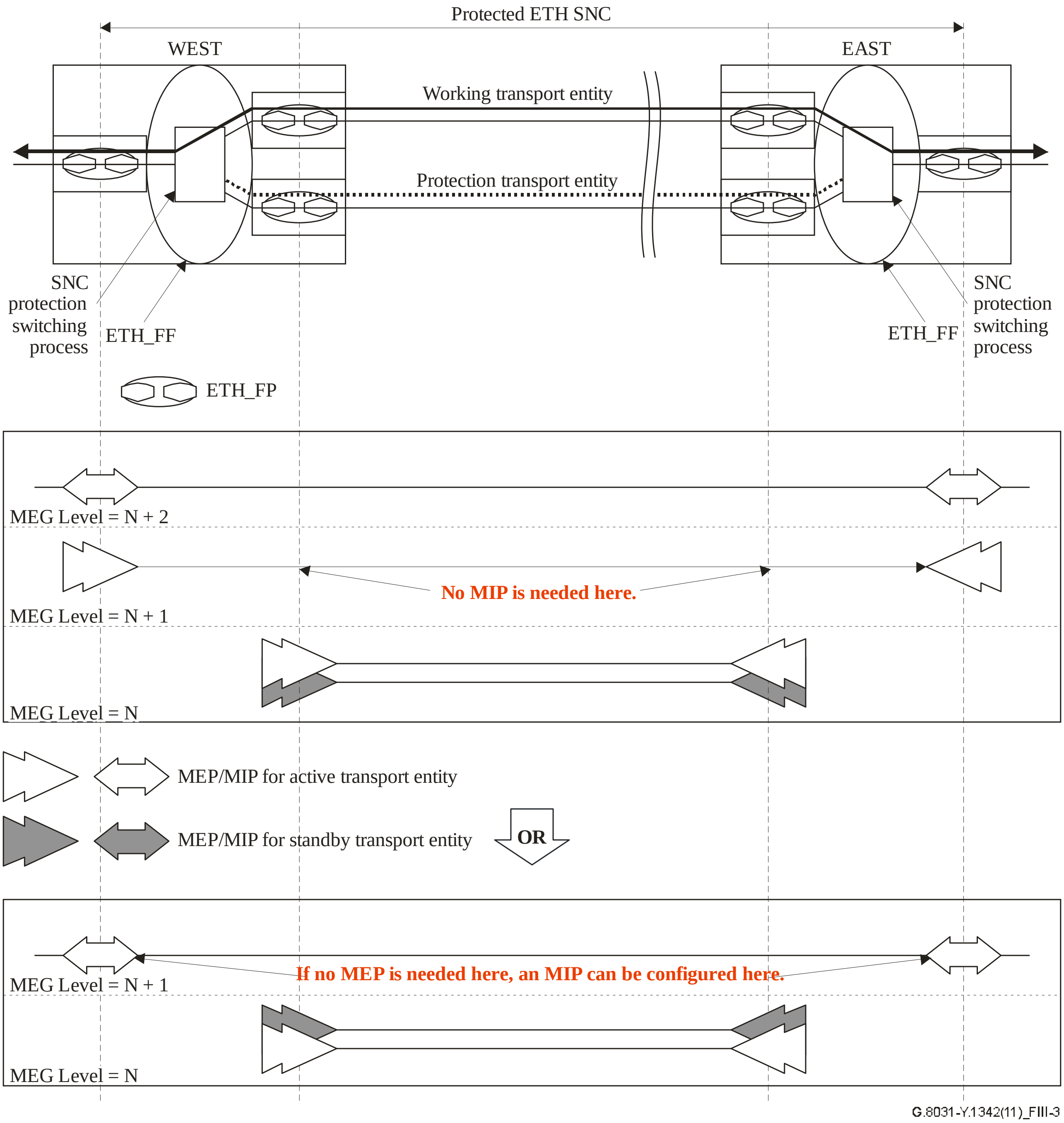


Figure III.3 – Examples of configuration of MEPs and MIPs for the protection switching environment

Appendix IV

State transition diagrams using specification and description language

(This appendix does not form an integral part of this Recommendation.)

IV.1 Introduction

In Appendix IV, diagrams using specification and description language (SDL) for state transitions defined in Annex A are provided for information.

IV.2 SDL diagrams

IV.2.1 1:1 bidirectional protection switching

The following diagrams define state transitions of 1:1 bidirectional protection switching both in revertive and non-revertive modes.

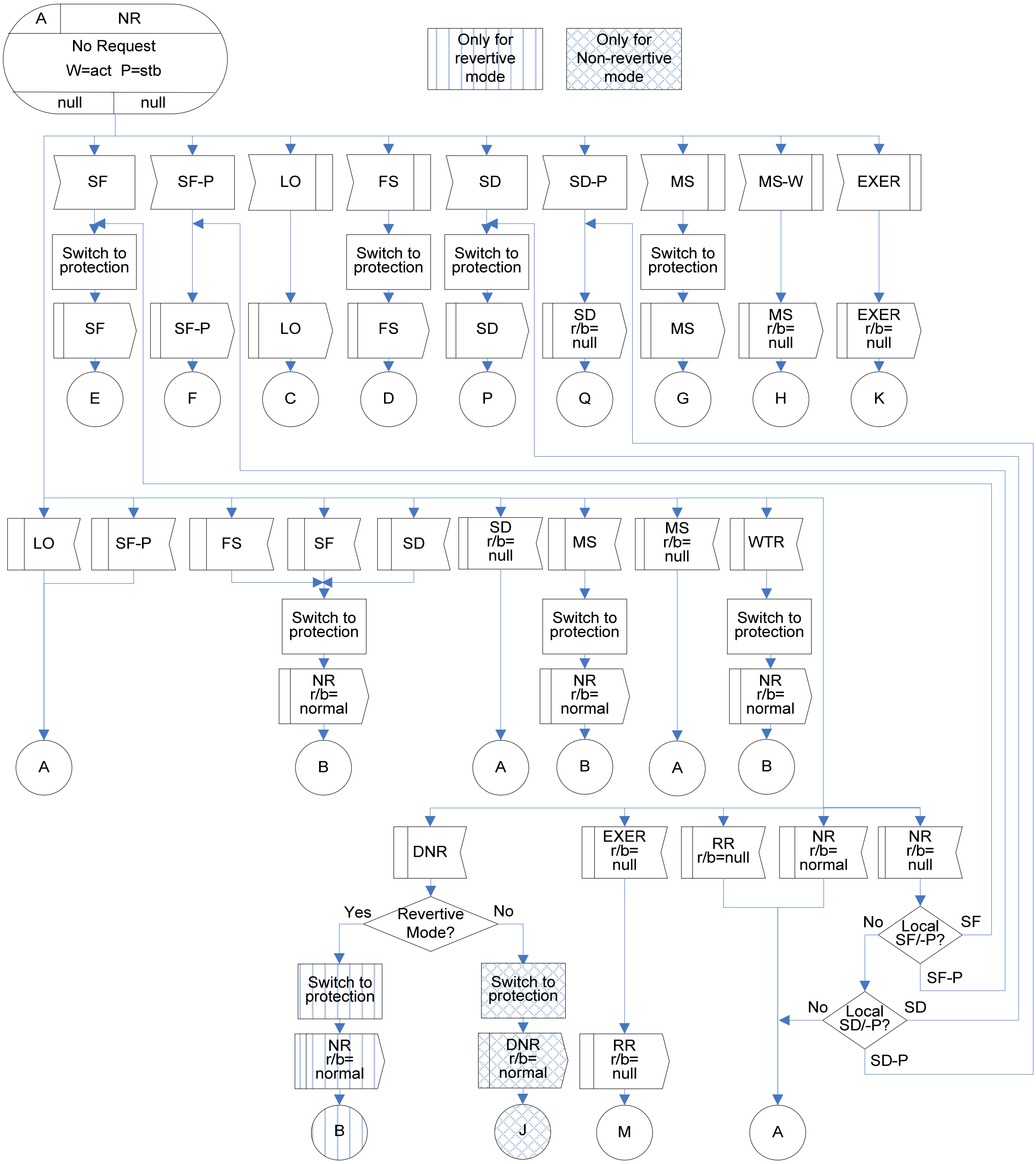


Figure IV.1 – NR(r/b=null) state for 1:1 bidirectional protection switching

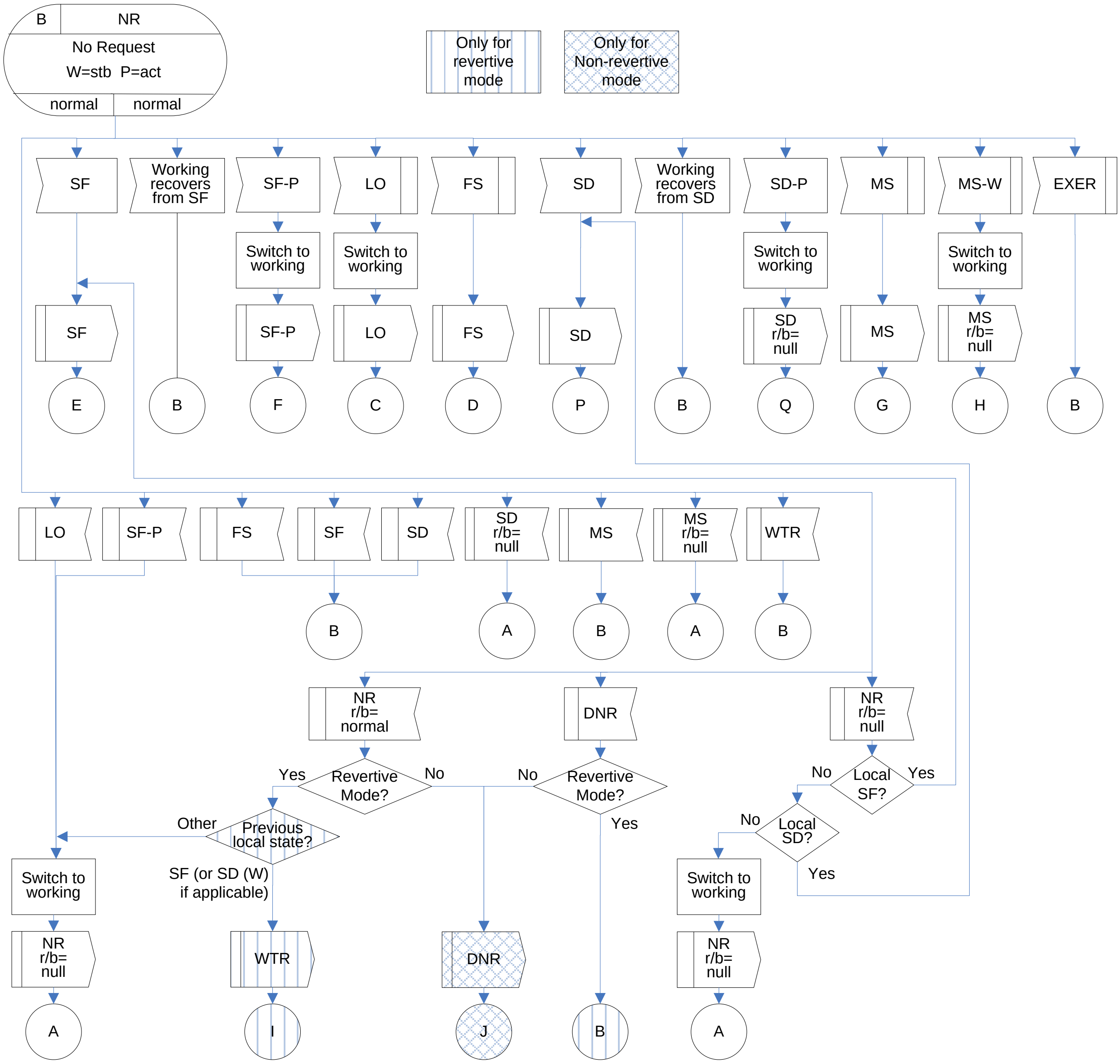


Figure IV.2 – NR(r/b=normal) state for 1:1 bidirectional protection switching

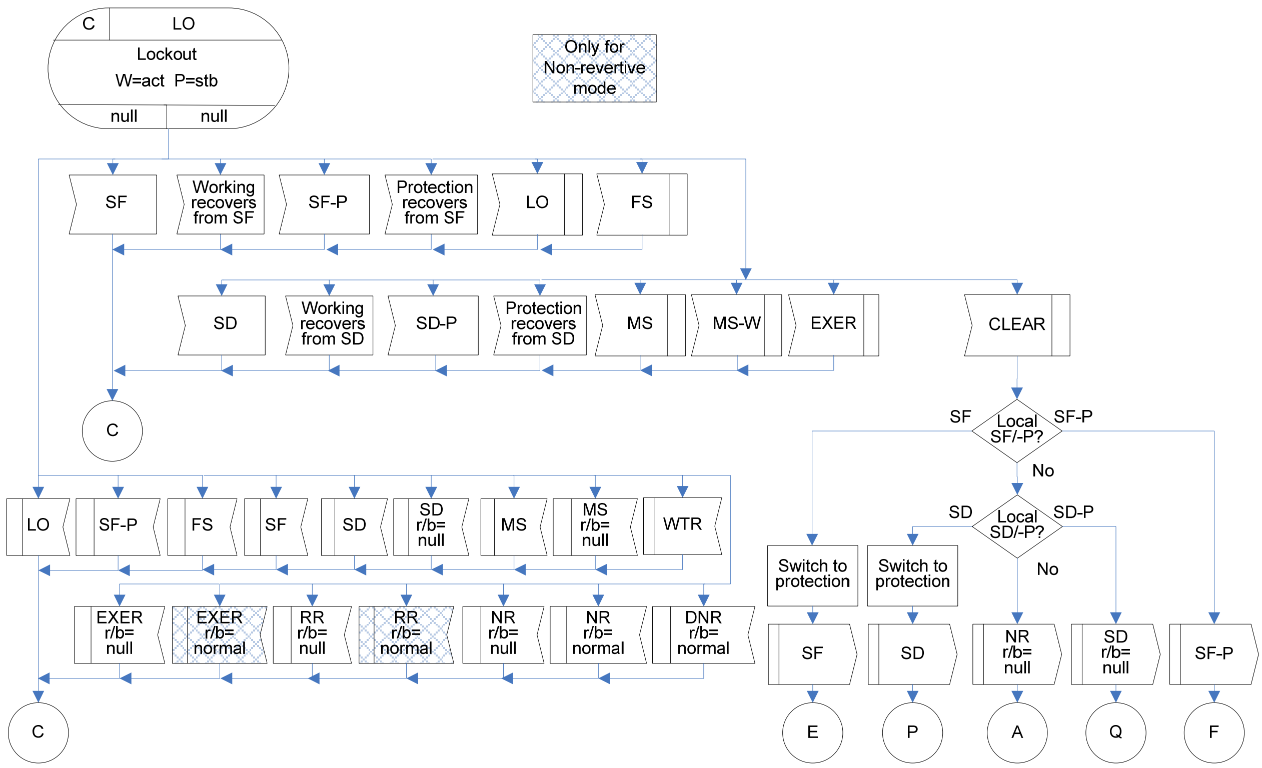


Figure IV.3 – LO(r/b=null) state for 1:1 bidirectional protection switching

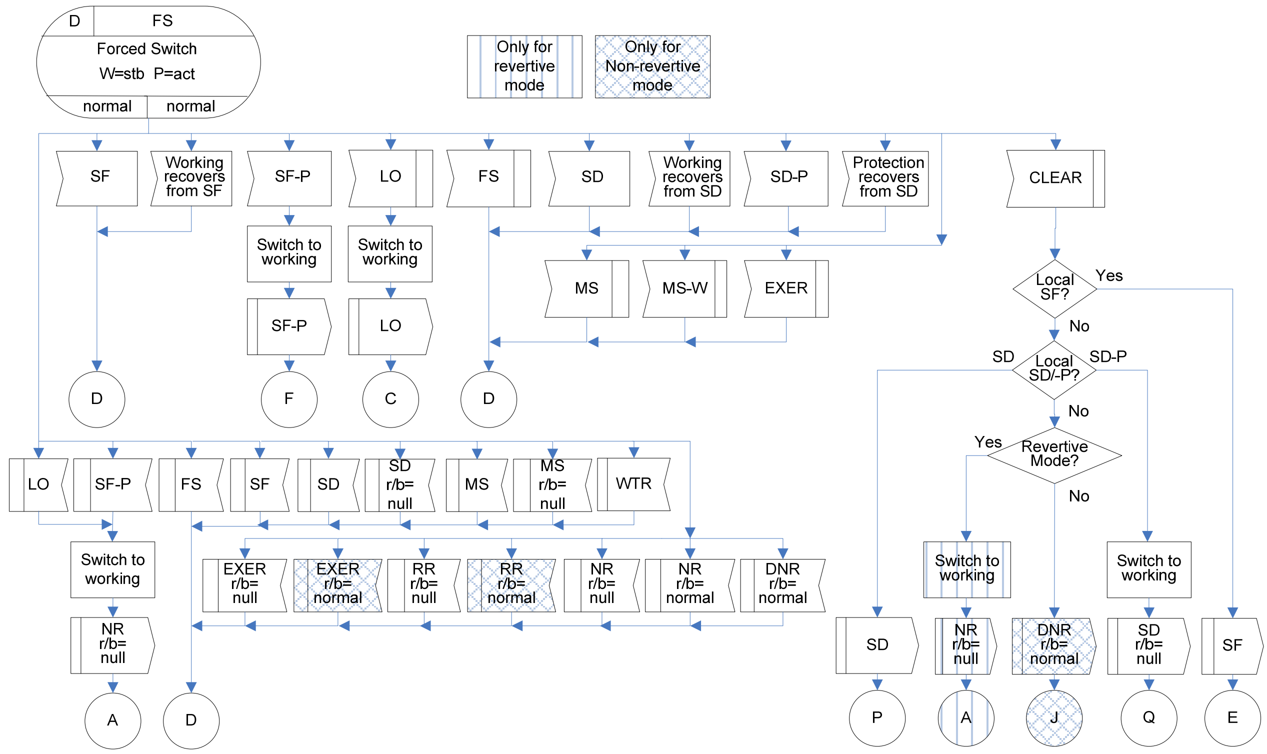


Figure IV.4 – FS(r/b=normal) state for 1:1 bidirectional protection switching

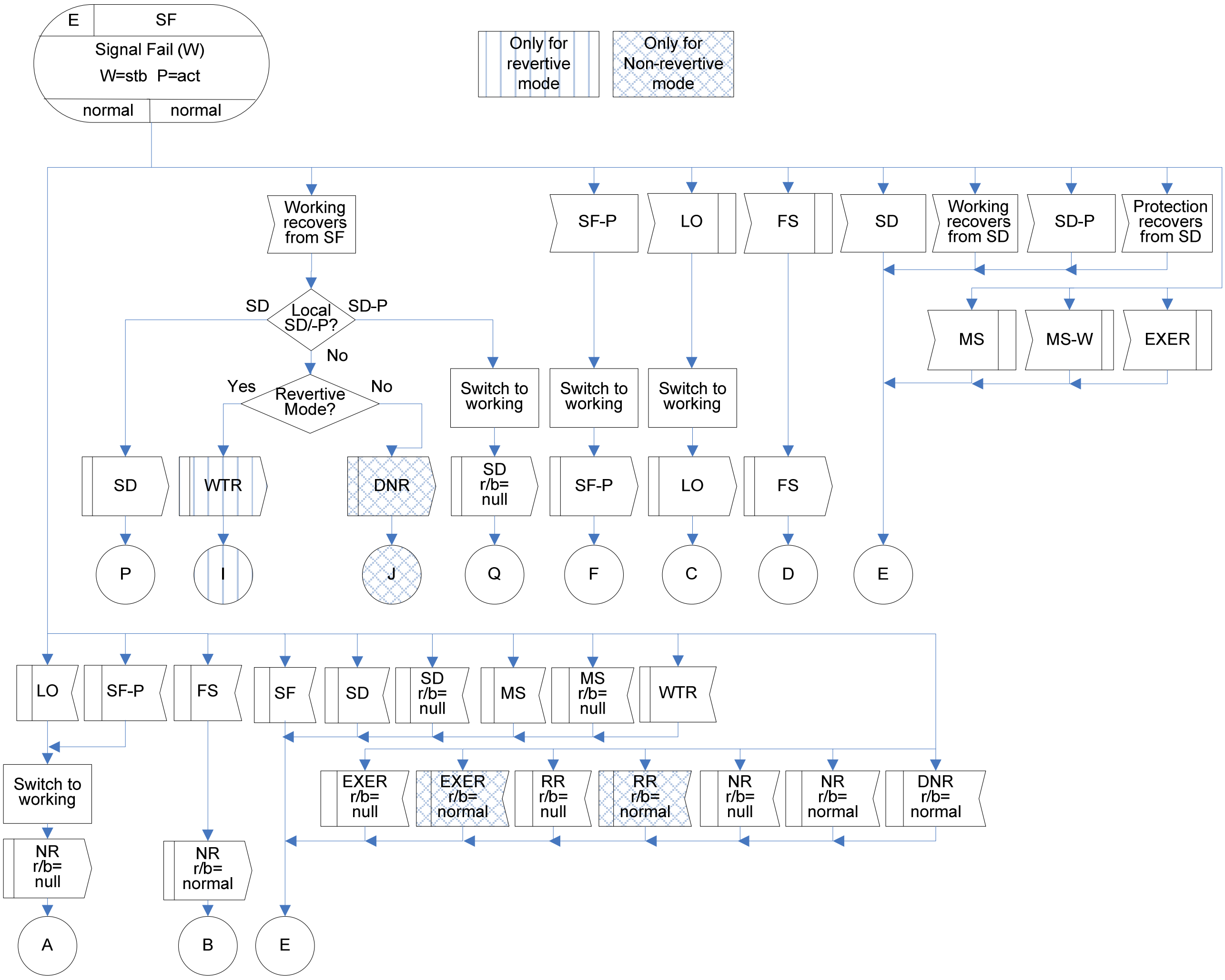


Figure IV.5 – SF(r/b=normal) state for 1:1 bidirectional protection switching

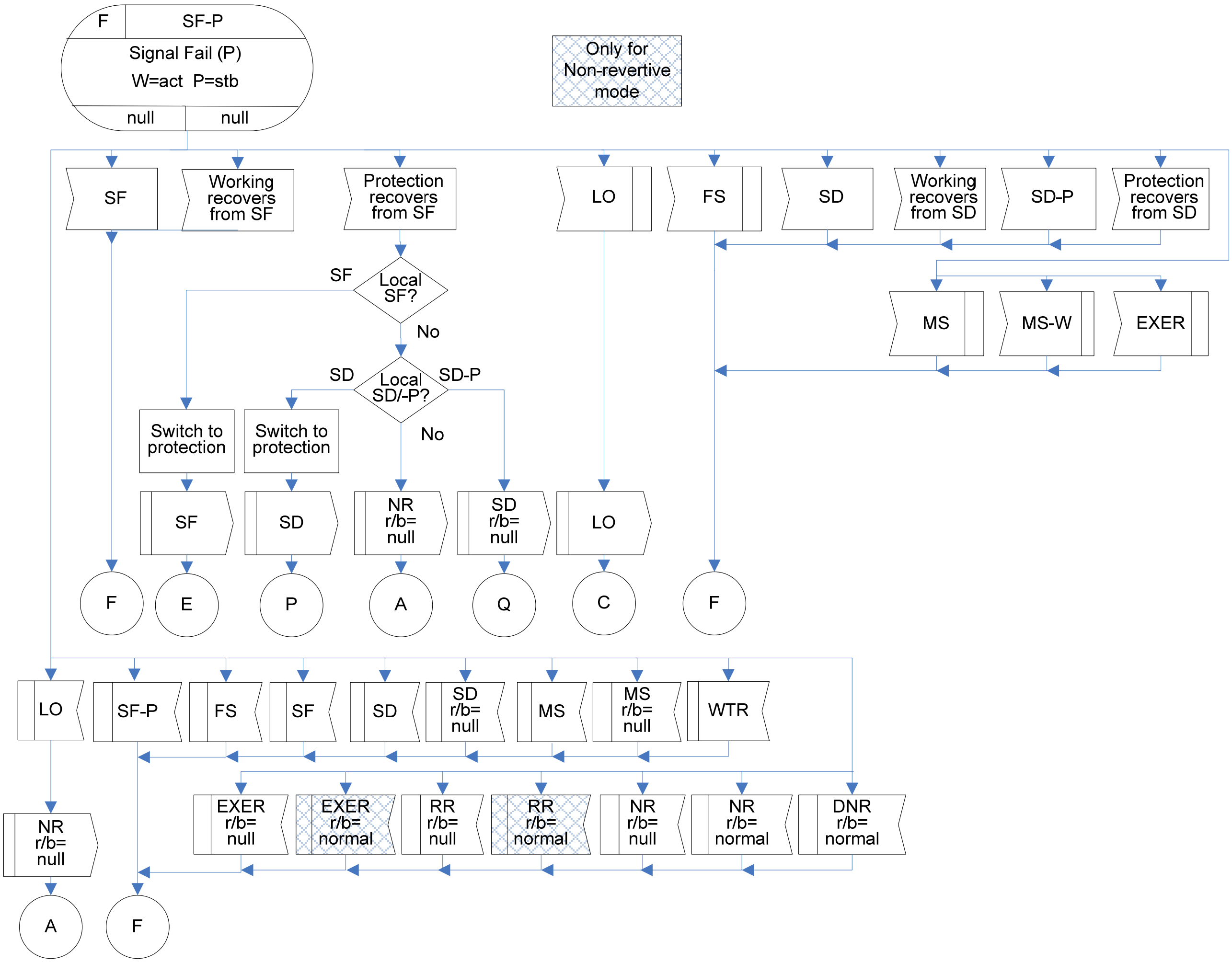


Figure IV.6 – SF-P(r/b=null) state for 1:1 bidirectional protection switching

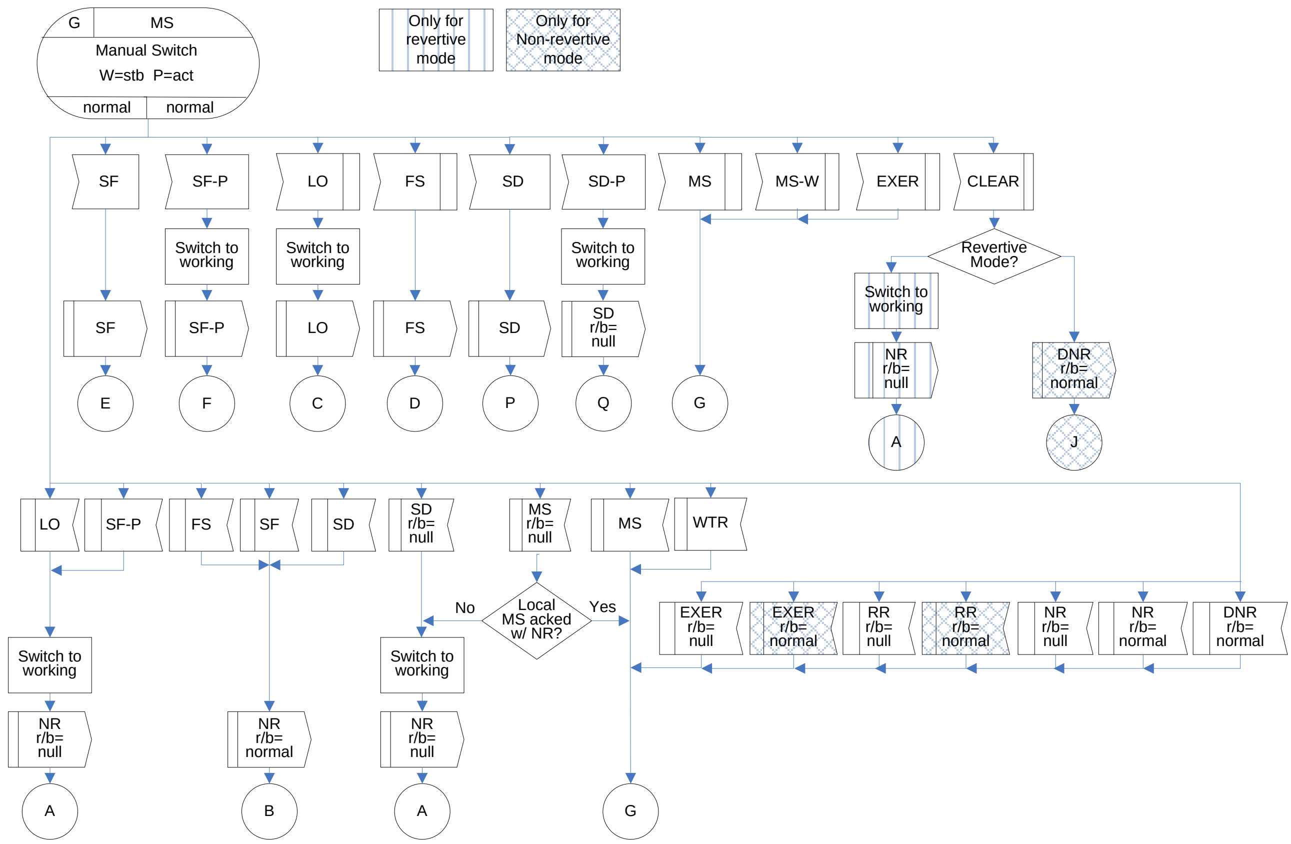


Figure IV.7 – MS(r/b=normal) state for 1:1 bidirectional protection switching

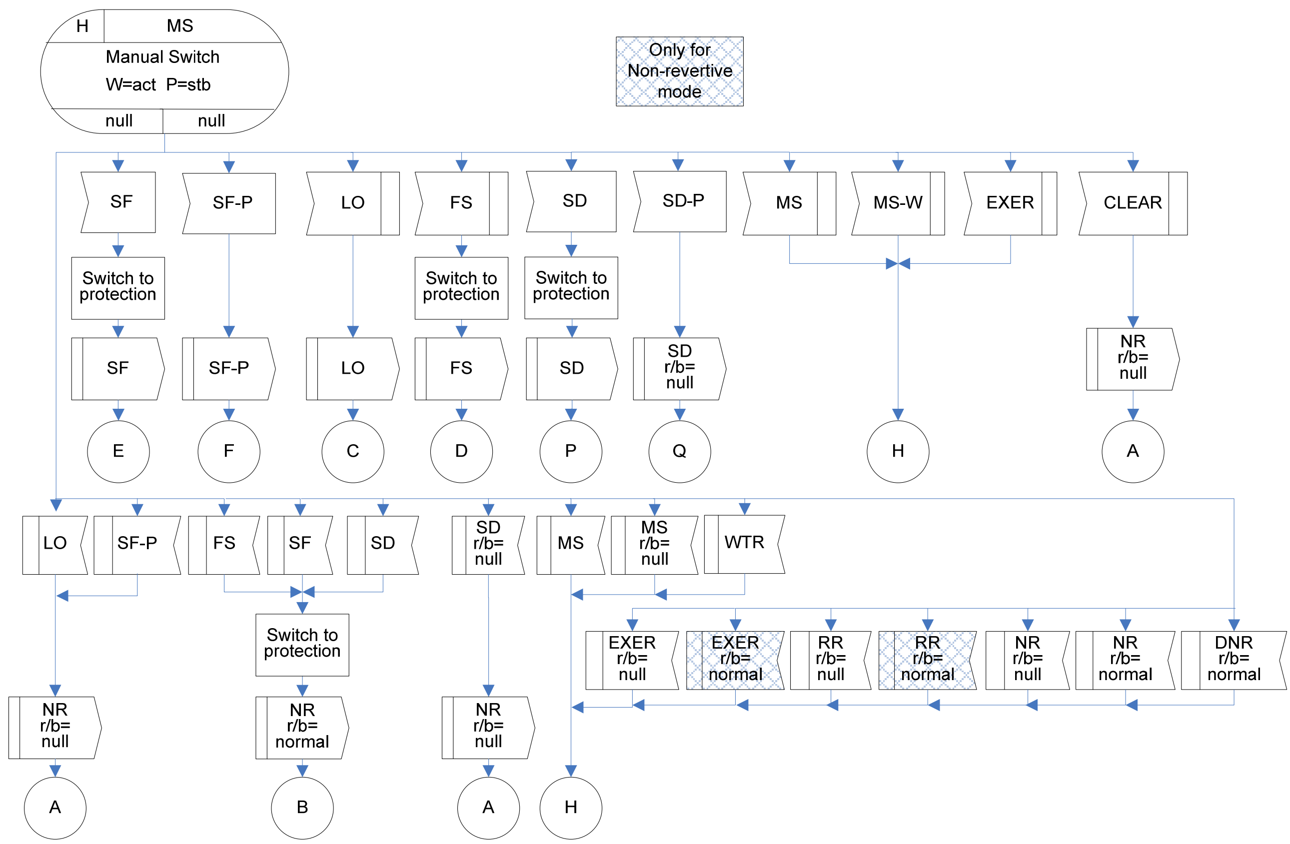


Figure IV.8 – MS(r/b=null) state for 1:1 bidirectional protection switching

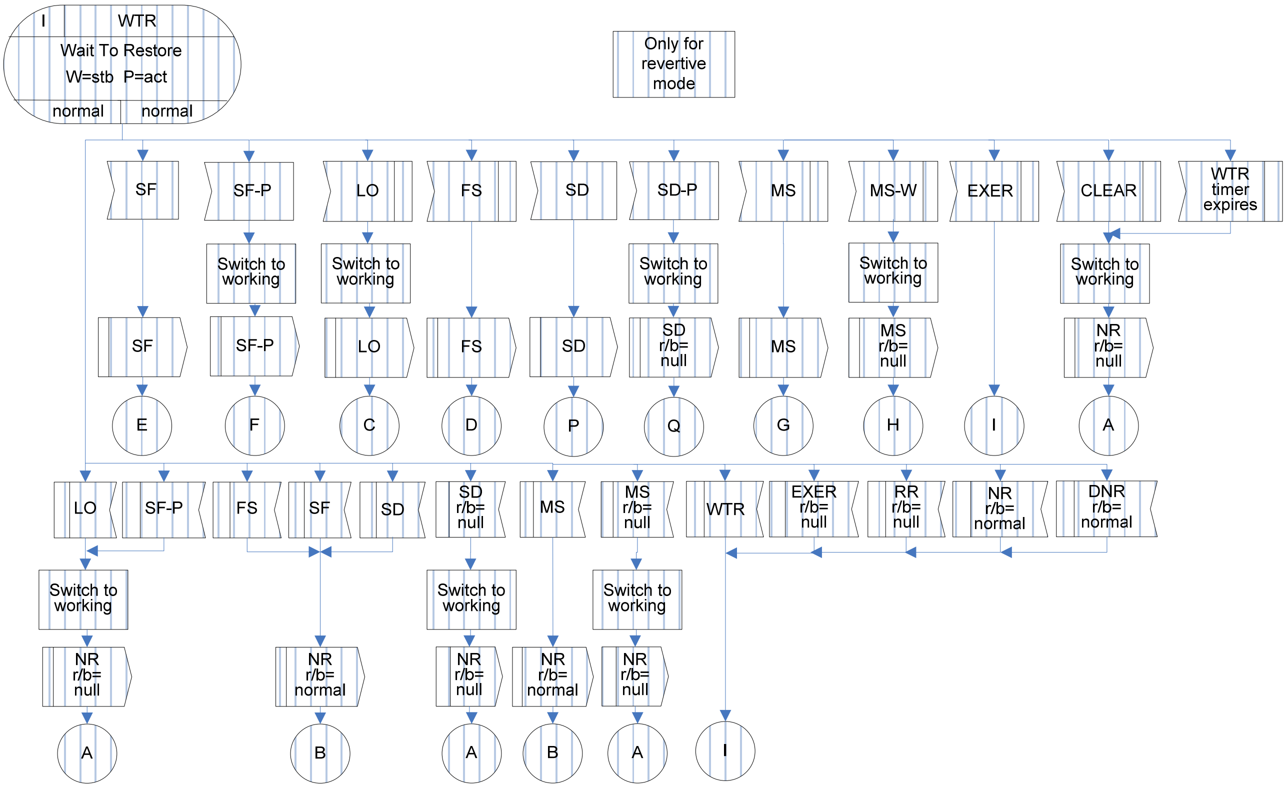


Figure IV.9 – WTR(r/b=normal) state for 1:1 bidirectional protection switching

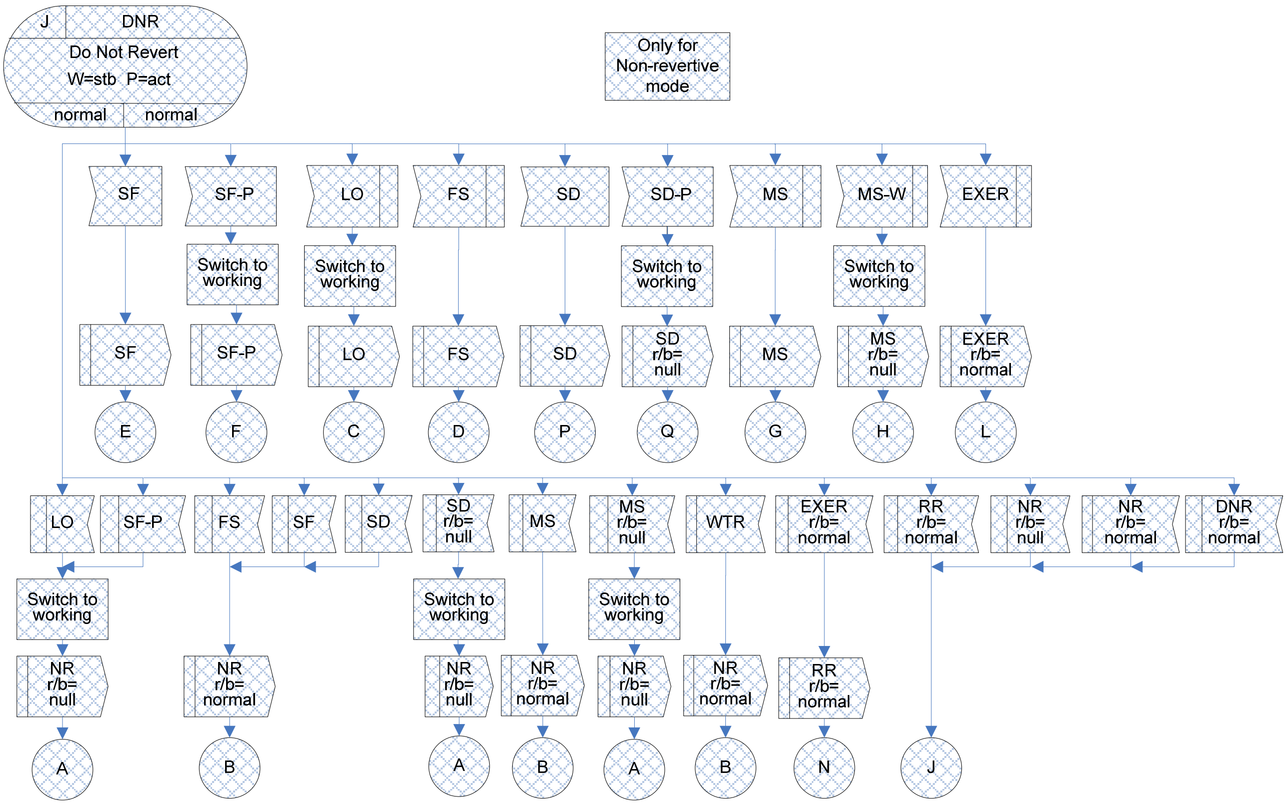


Figure IV.10 – DNR(r/b=normal) state for 1:1 bidirectional protection switching

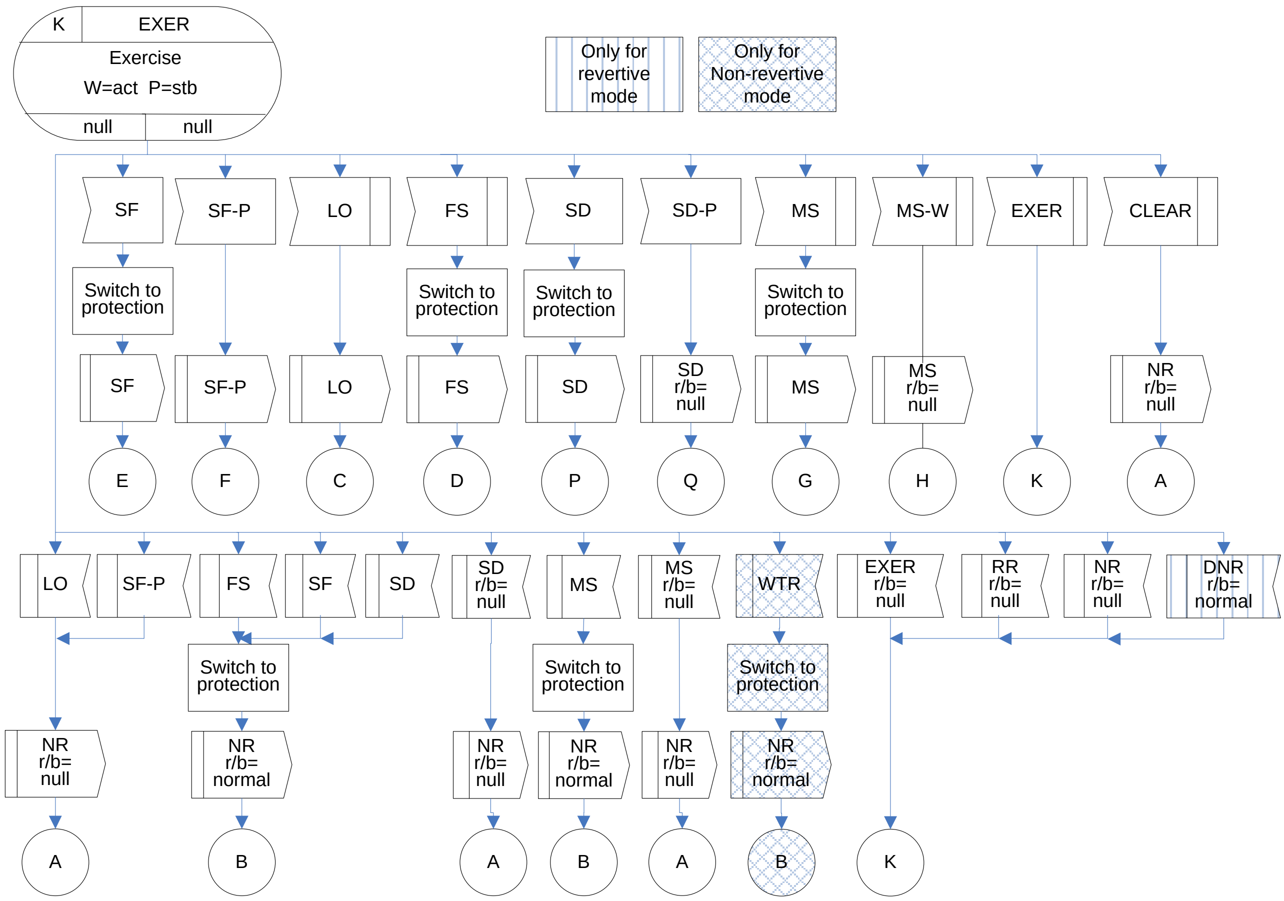


Figure IV.11 – EXER(r/b=null) state for 1:1 bidirectional protection switching

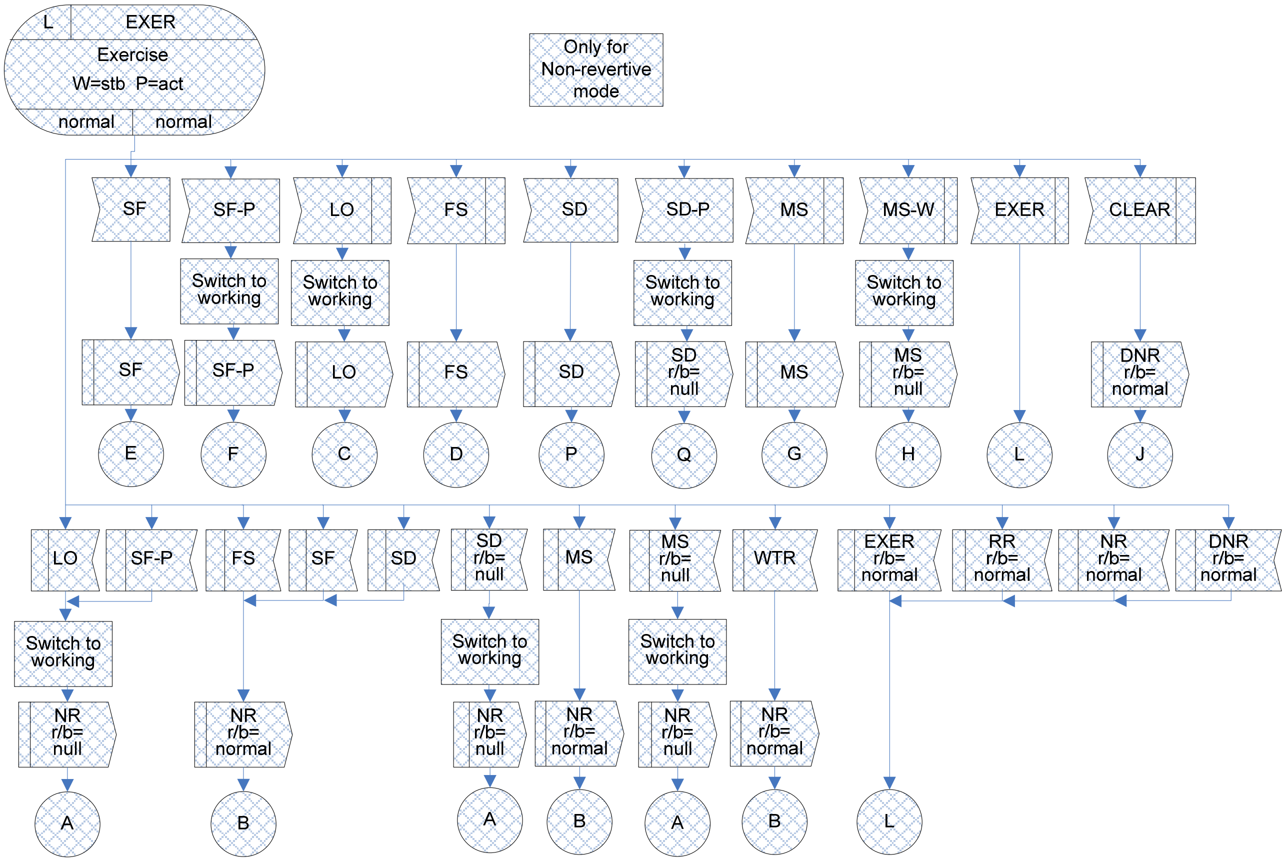


Figure IV.12 – EXER(r/b=normal) state for 1:1 bidirectional protection switching

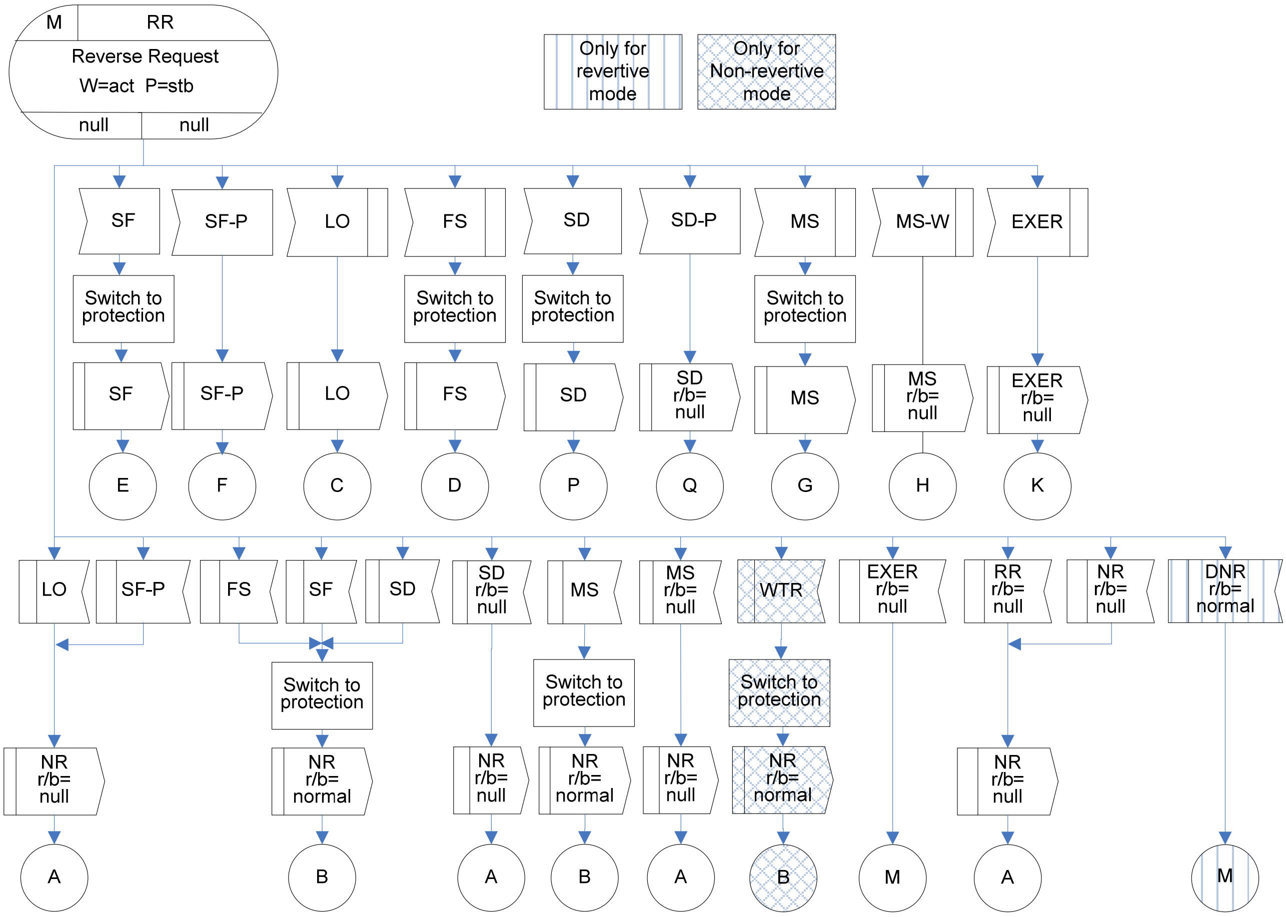


Figure IV.13 – RR(r/b=null) state for 1:1 bidirectional protection switching

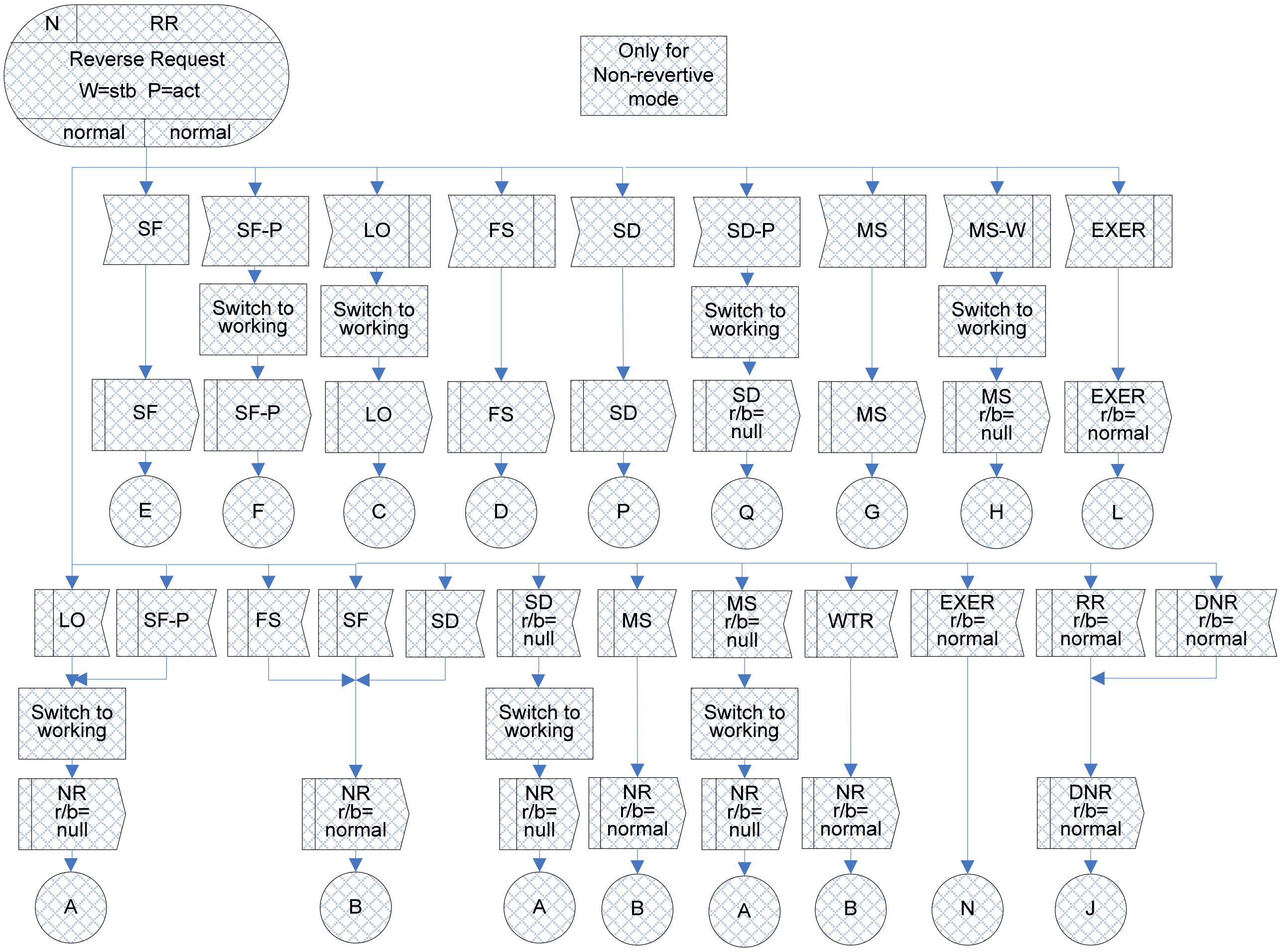


Figure IV.14 – RR(r/b=normal) state for 1:1 bidirectional protection switching

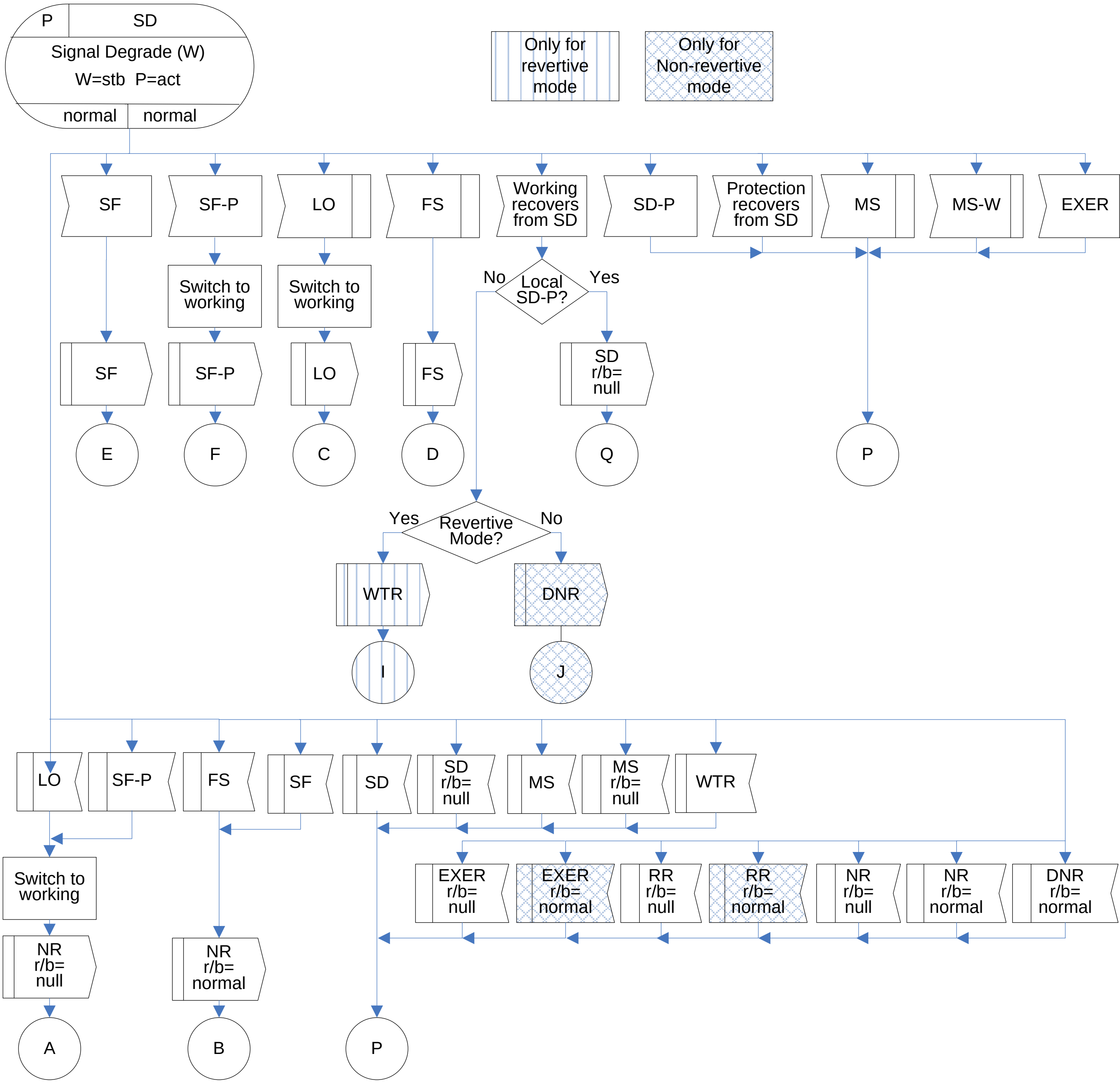


Figure IV.15 – SD(r/b=normal) state for 1:1 bidirectional protection switching

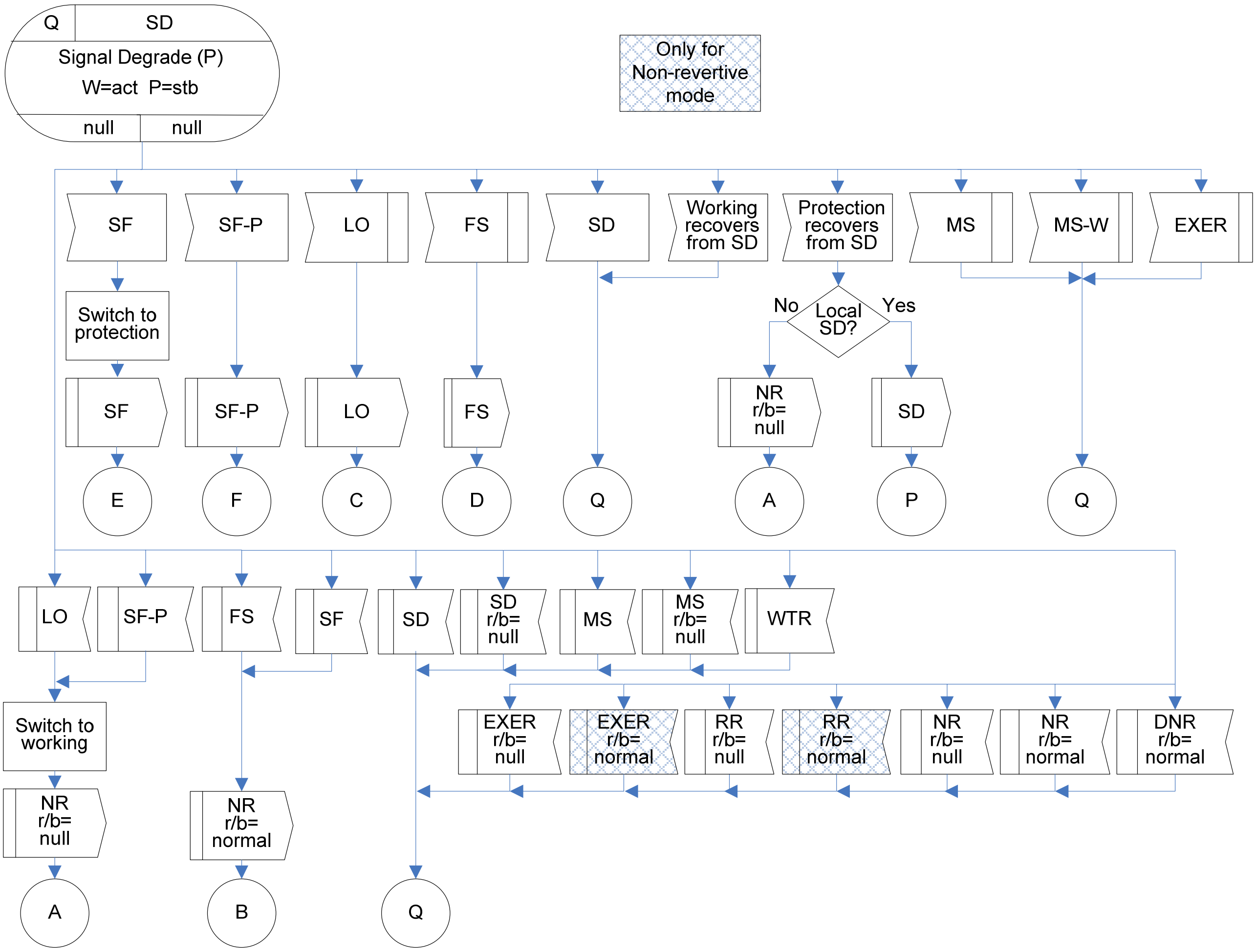


Figure IV.16 – SD(r/b=null) state for 1:1 bidirectional protection switching

IV.2.2 1+1 bidirectional protection switching

The following diagrams define state transitions of 1+1 bidirectional protection switching both in revertive and non-revertive modes.

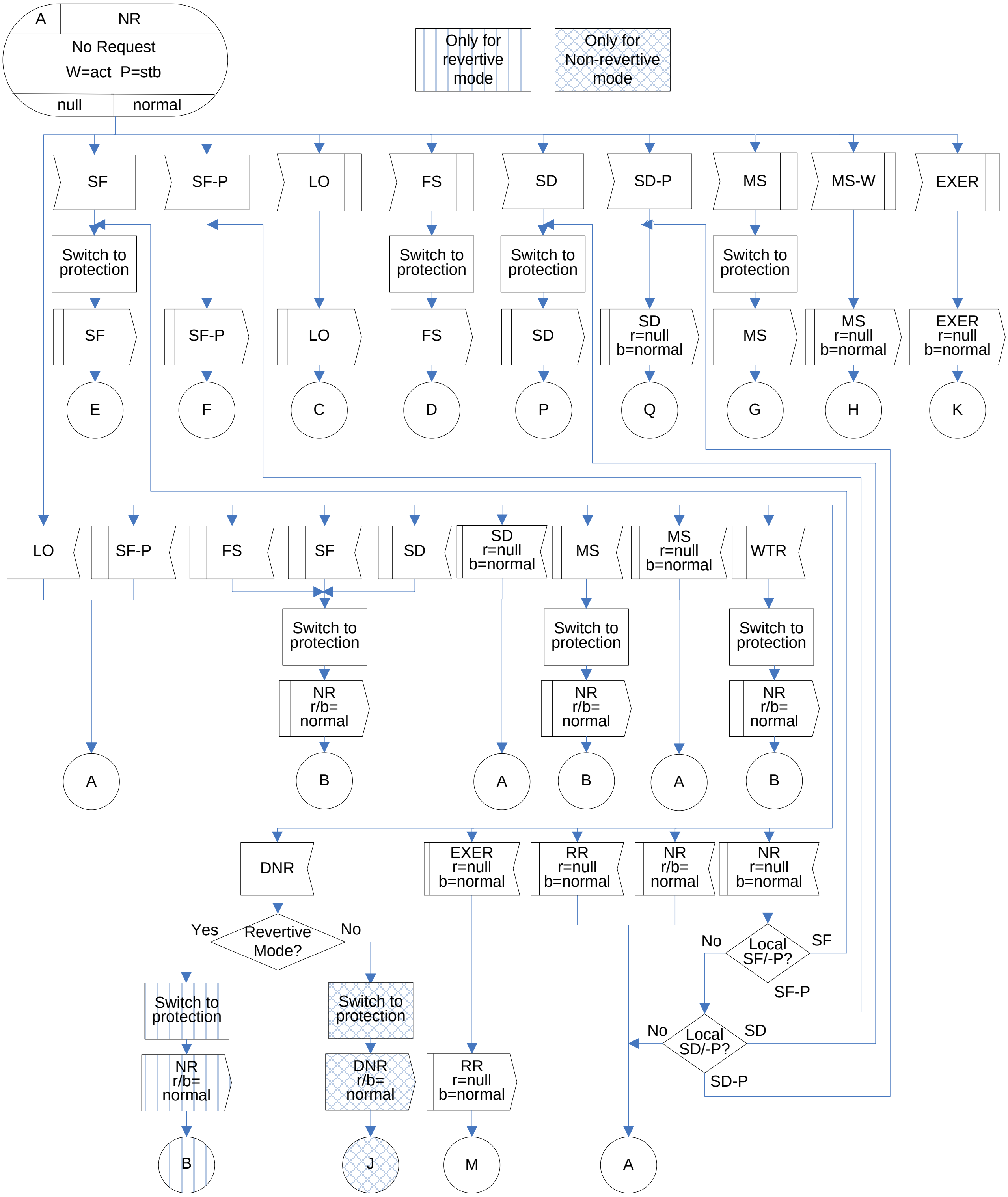


Figure IV.17 – NR(r=null, b=normal) state for 1+1 bidirectional protection switching

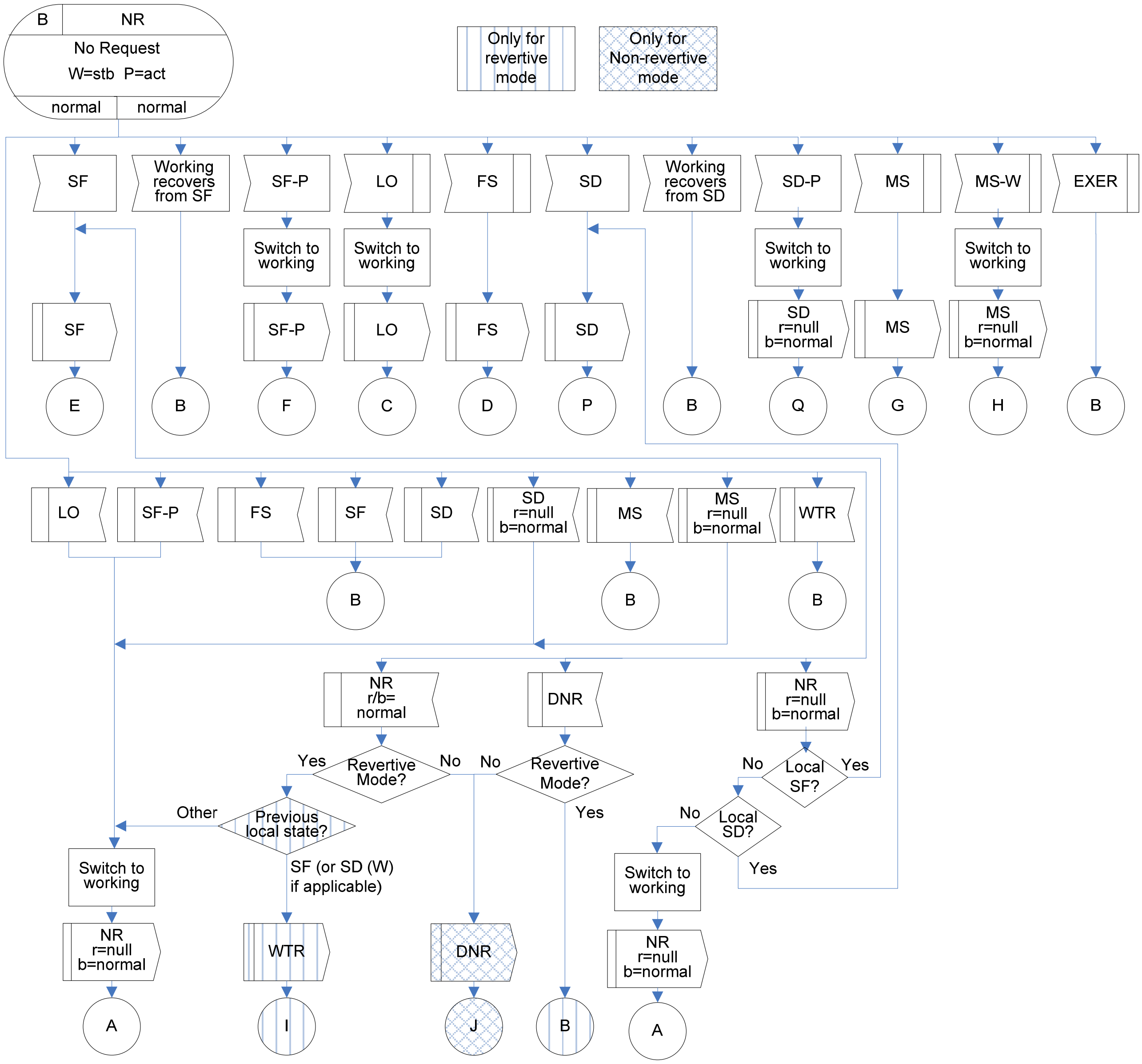


Figure IV.18 – NR(r/b=normal) state for 1+1 bidirectional protection switching

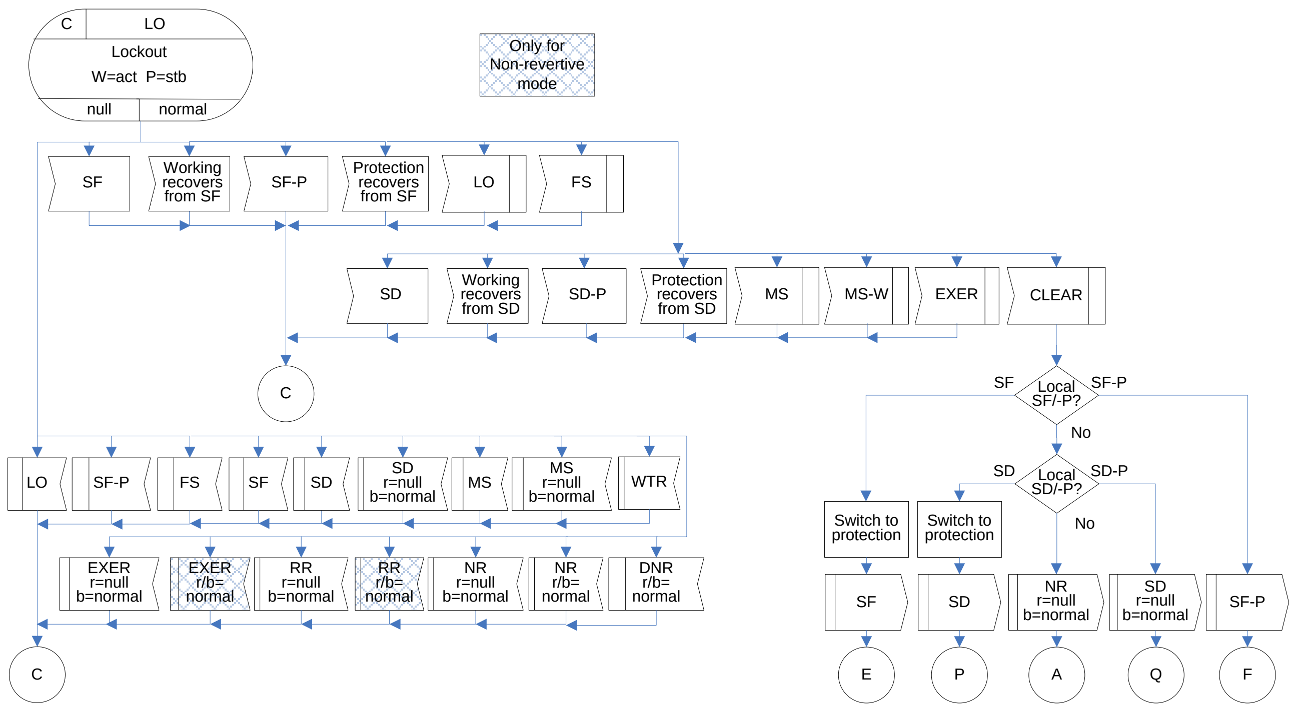


Figure IV.19 – LO(r=null, b=normal) state for 1+1 bidirectional protection switching

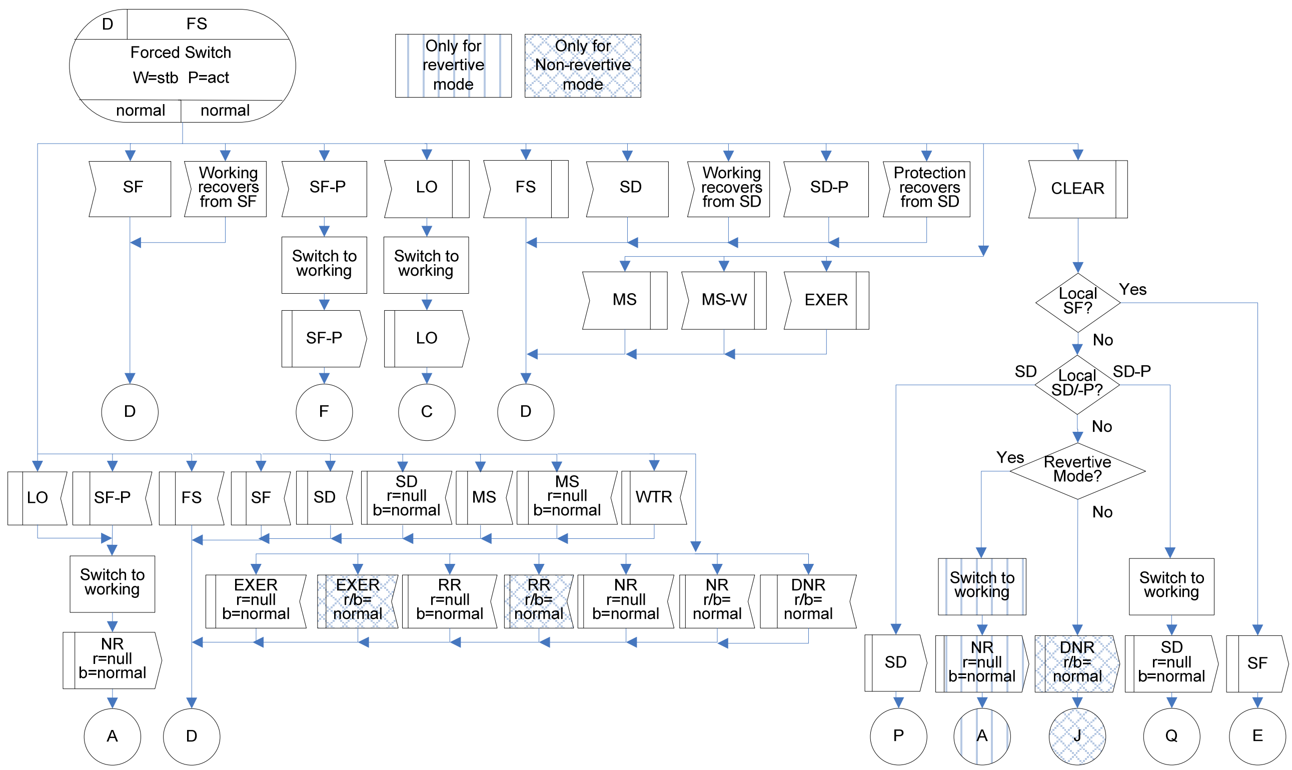


Figure IV.20 – FS(r/b=normal) state for 1+1 bidirectional protection switching

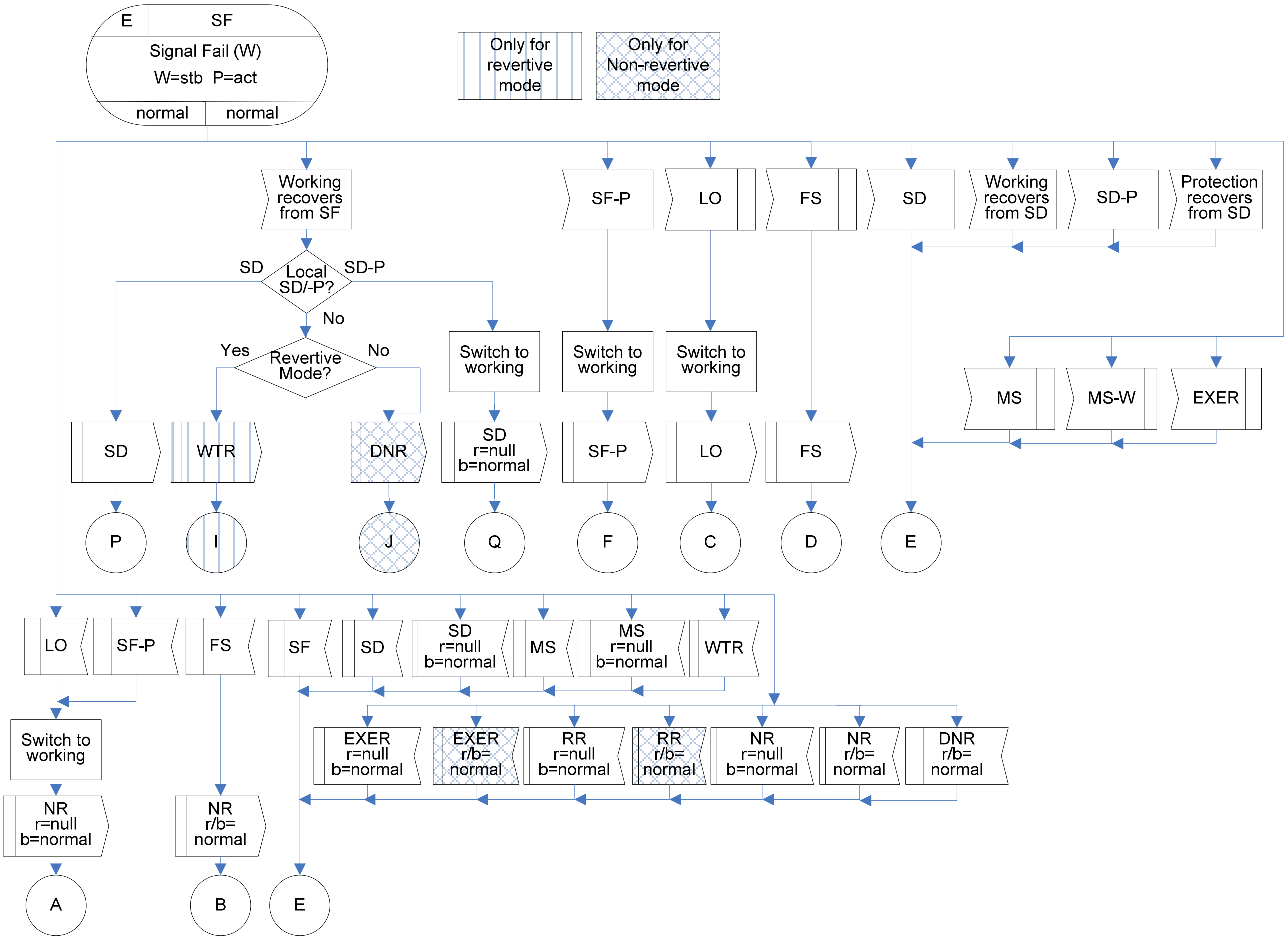


Figure IV.21 – SF(r/b=normal) state for 1+1 bidirectional protection switching

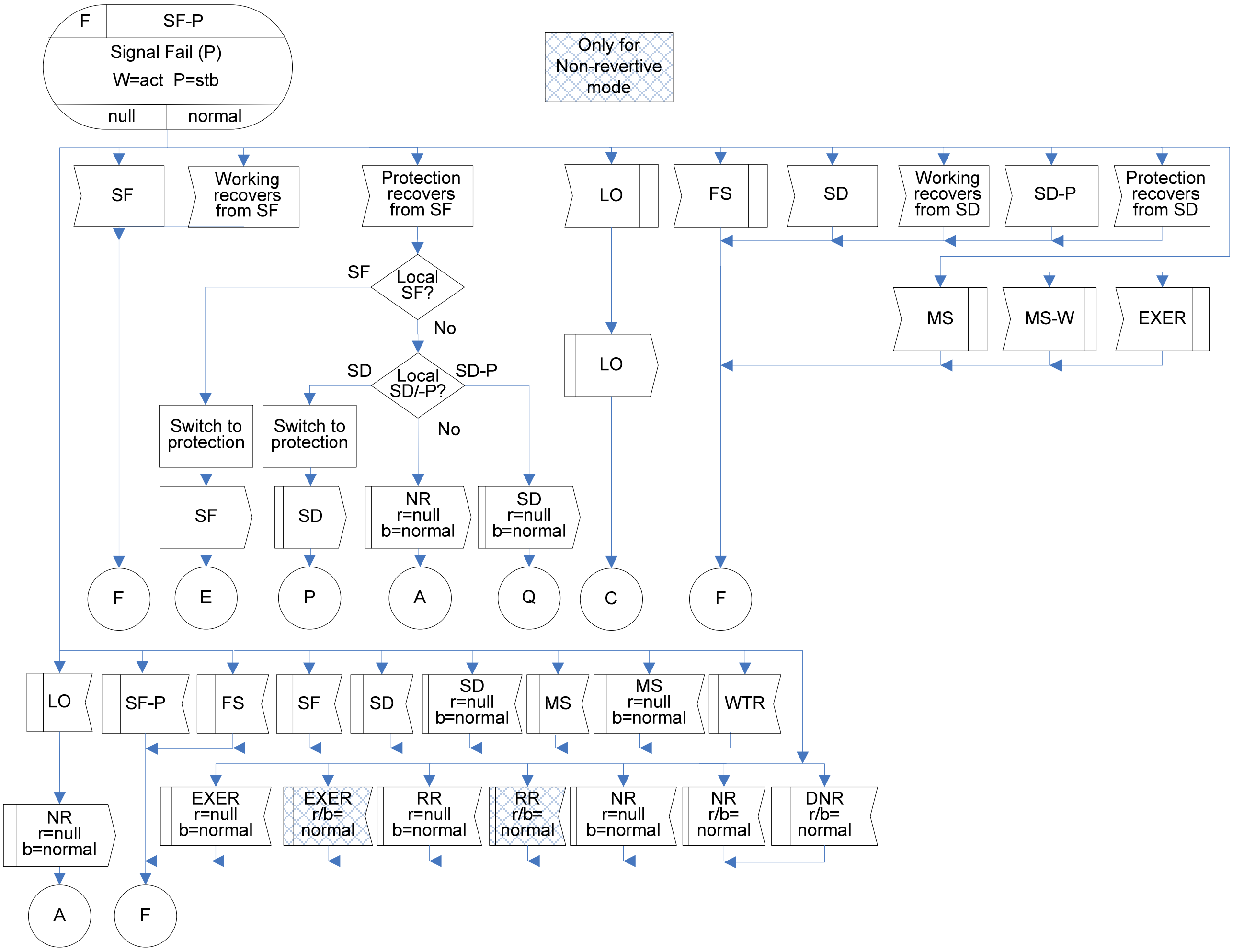


Figure IV.22 – SF-P(r=null, b=normal) state for 1+1 bidirectional protection switching

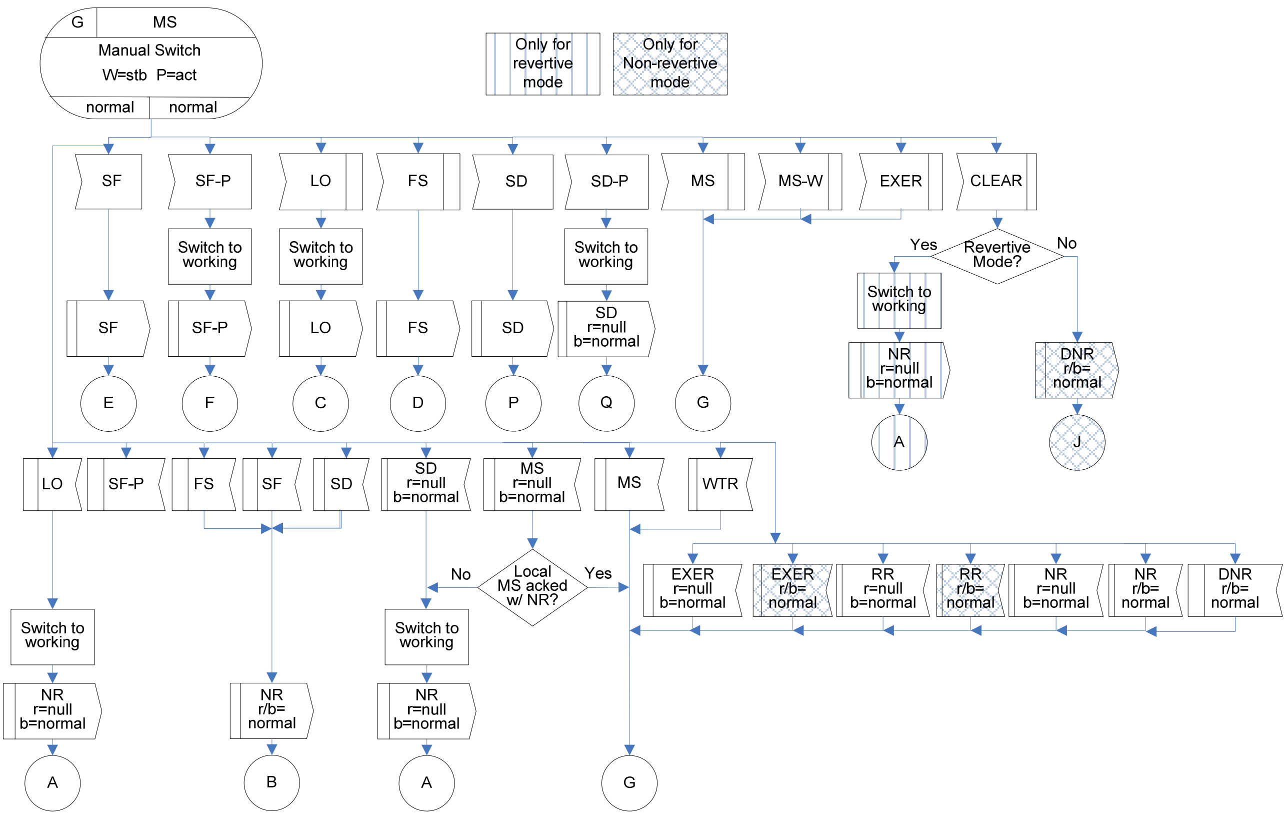


Figure IV.23 – MS(r/b=normal) state for 1+1 bidirectional protection switching

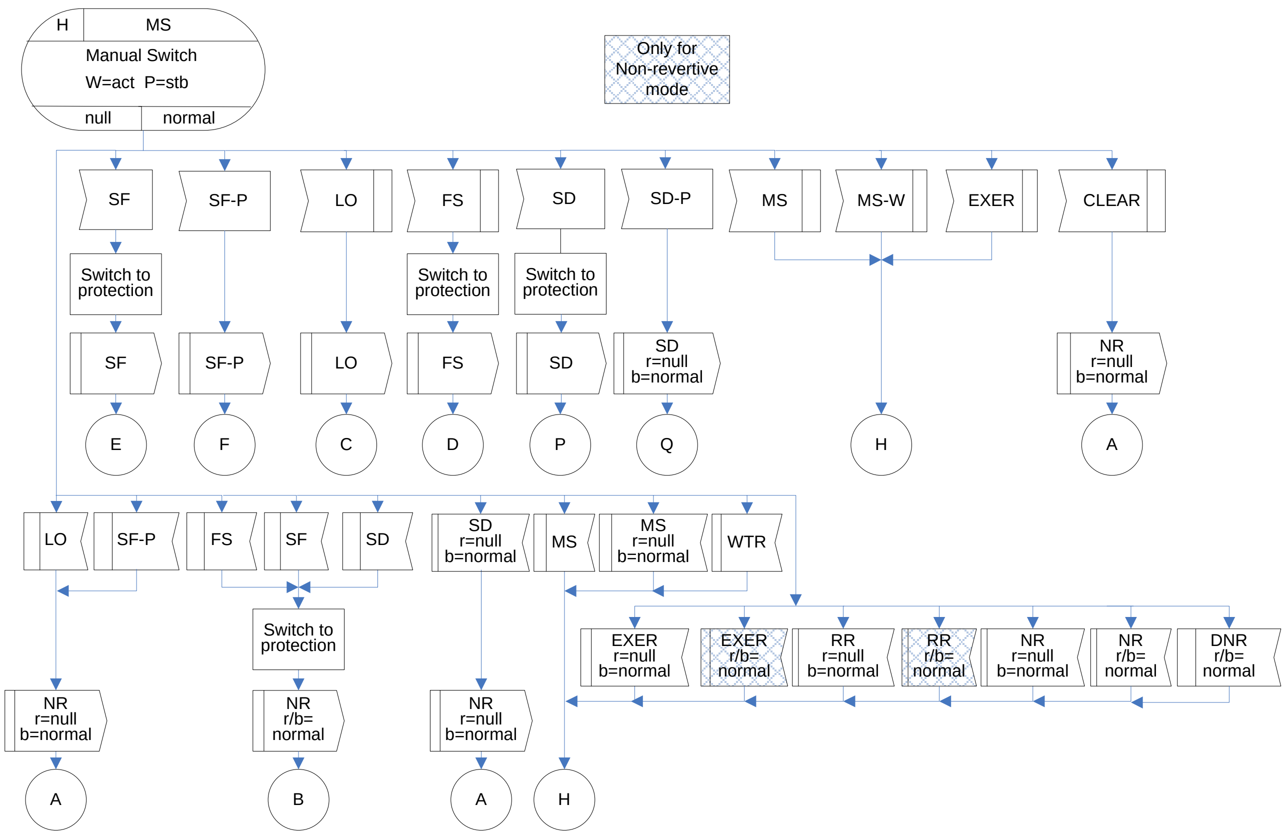


Figure IV.24 – MS(r=null, b=normal) state for 1+1 bidirectional protection switching

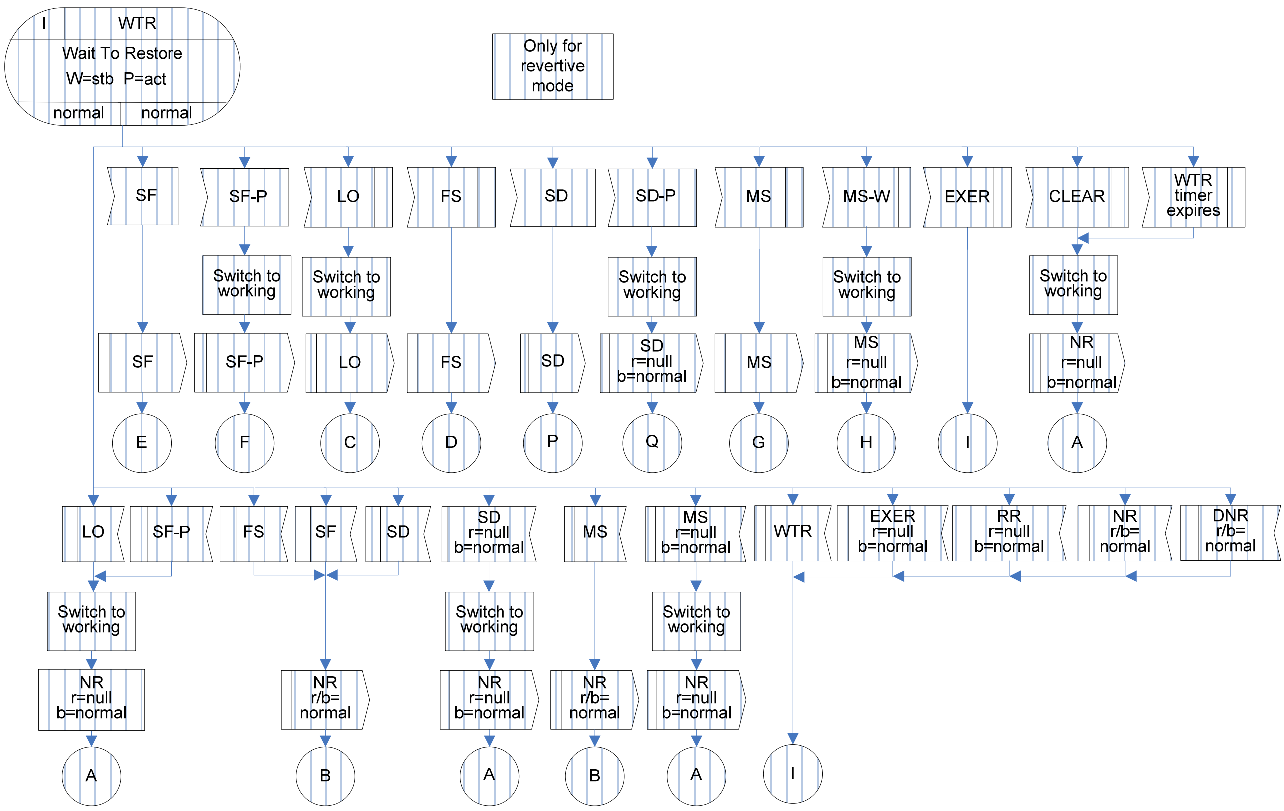


Figure IV.25 – WTR(r/b=normal) state for 1+1 bidirectional protection switching

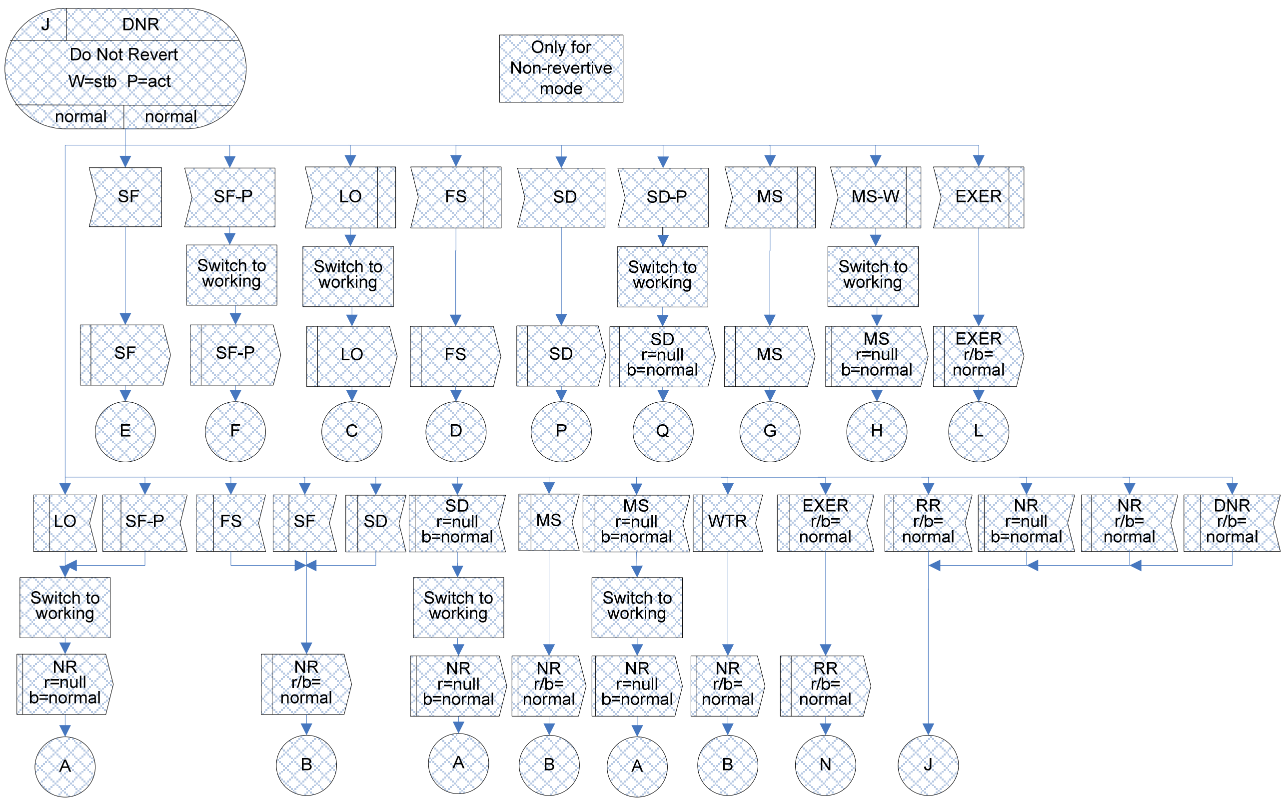


Figure IV.26 – DNR(r/b=normal) state for 1+1 bidirectional protection switching

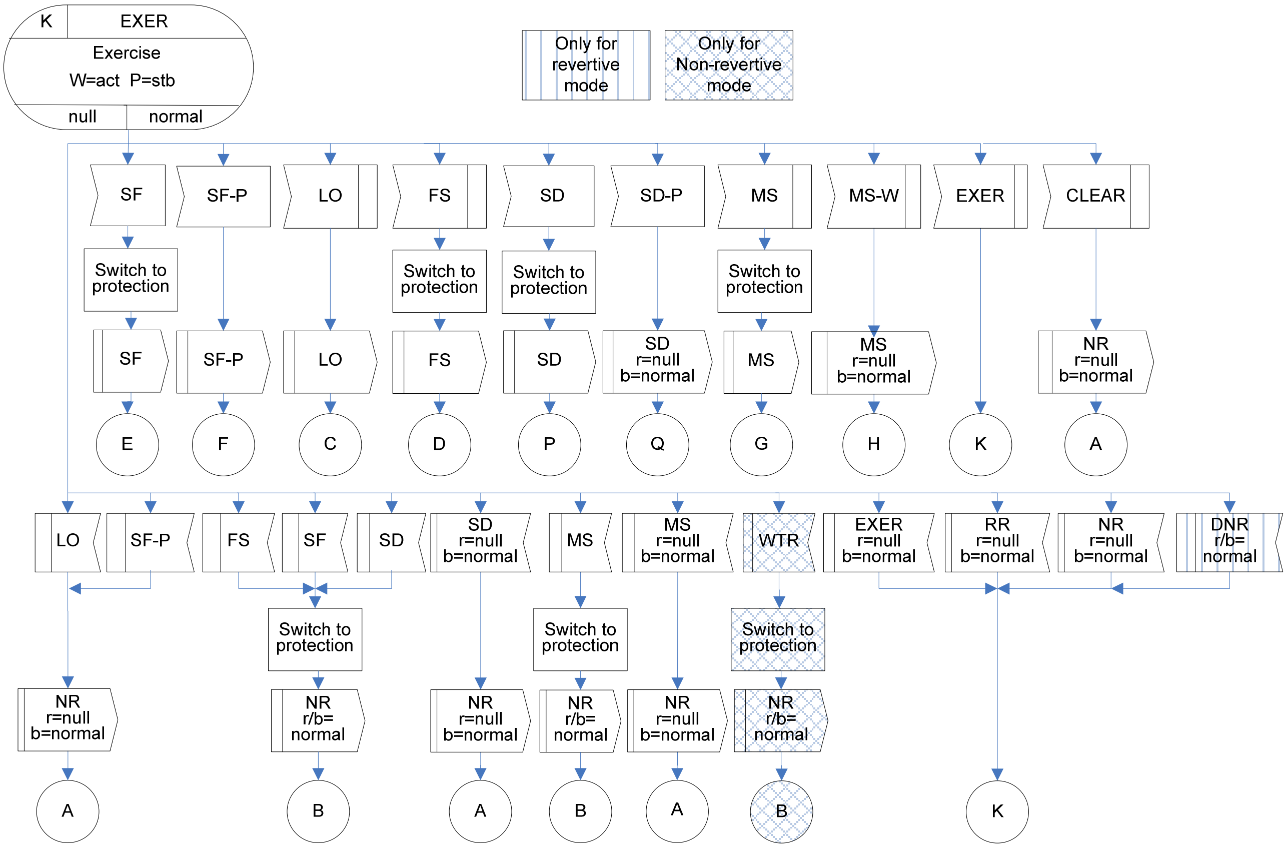


Figure IV.27 – EXER(r=null, b=normal) state for 1+1 bidirectional protection switching

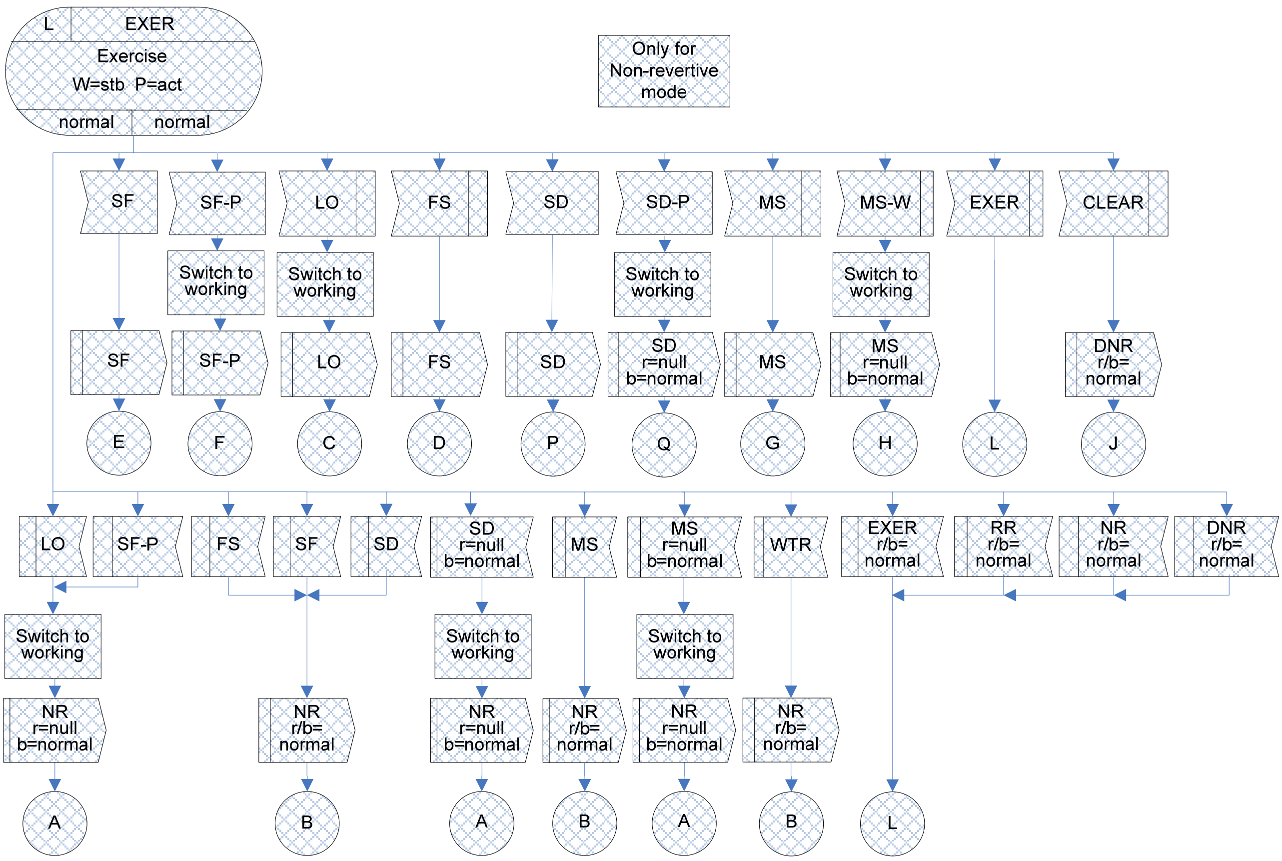


Figure IV.28 – EXER(r/b=normal) state for 1+1 bidirectional protection switching

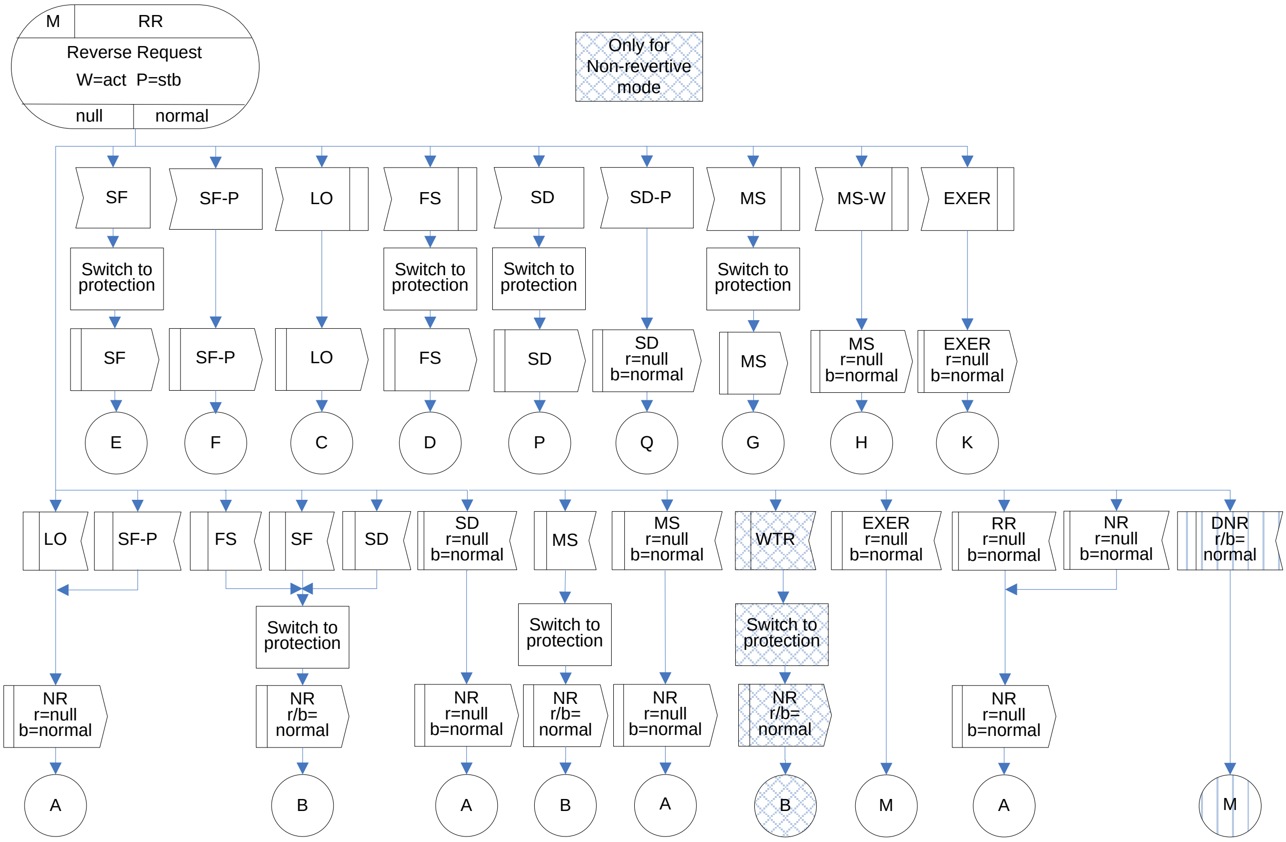


Figure IV.29 – RR(r=null, b=normal) state for 1+1 bidirectional protection switching

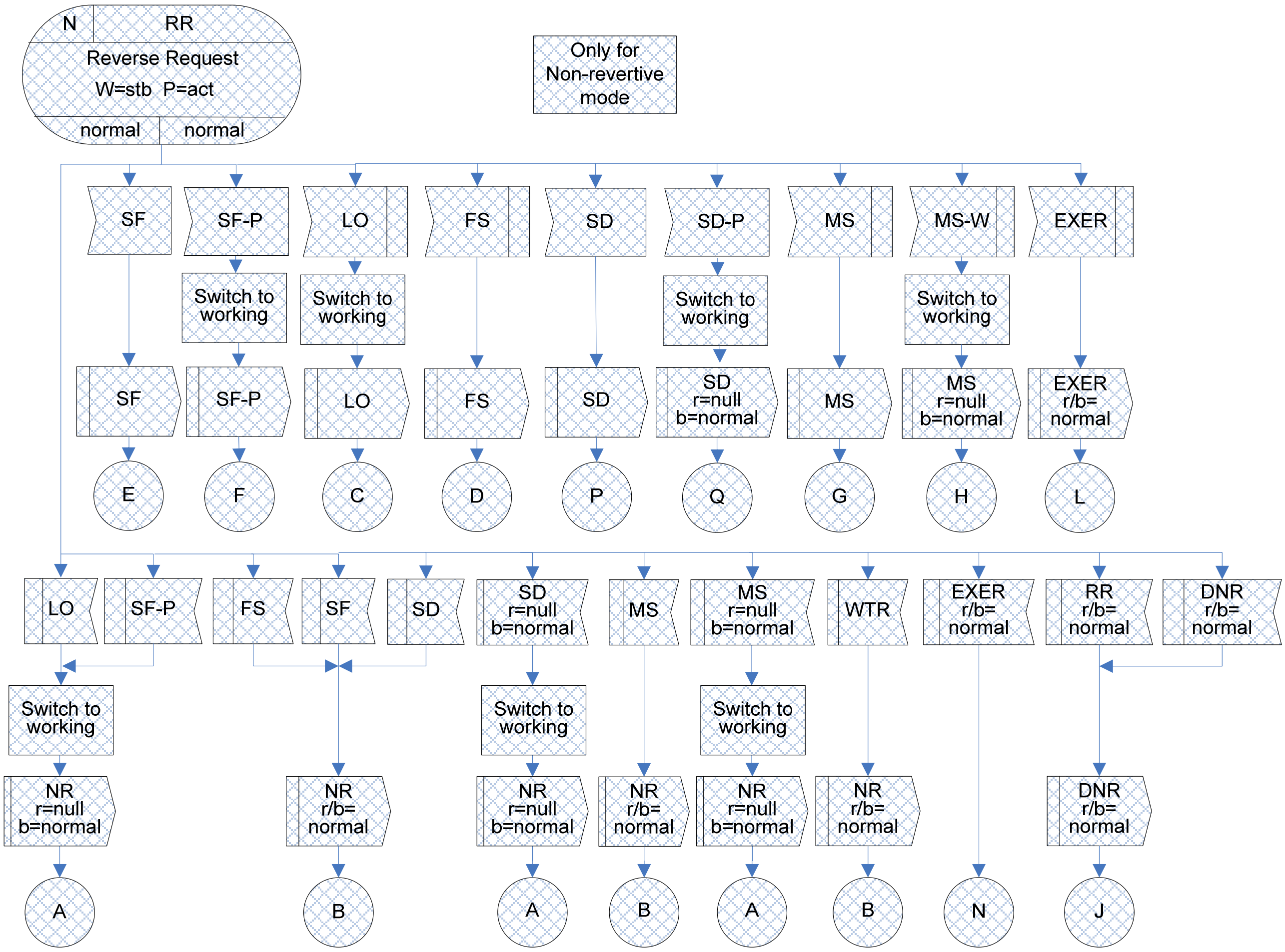


Figure IV.30 – RR(r/b=normal) state for 1+1 bidirectional protection switching

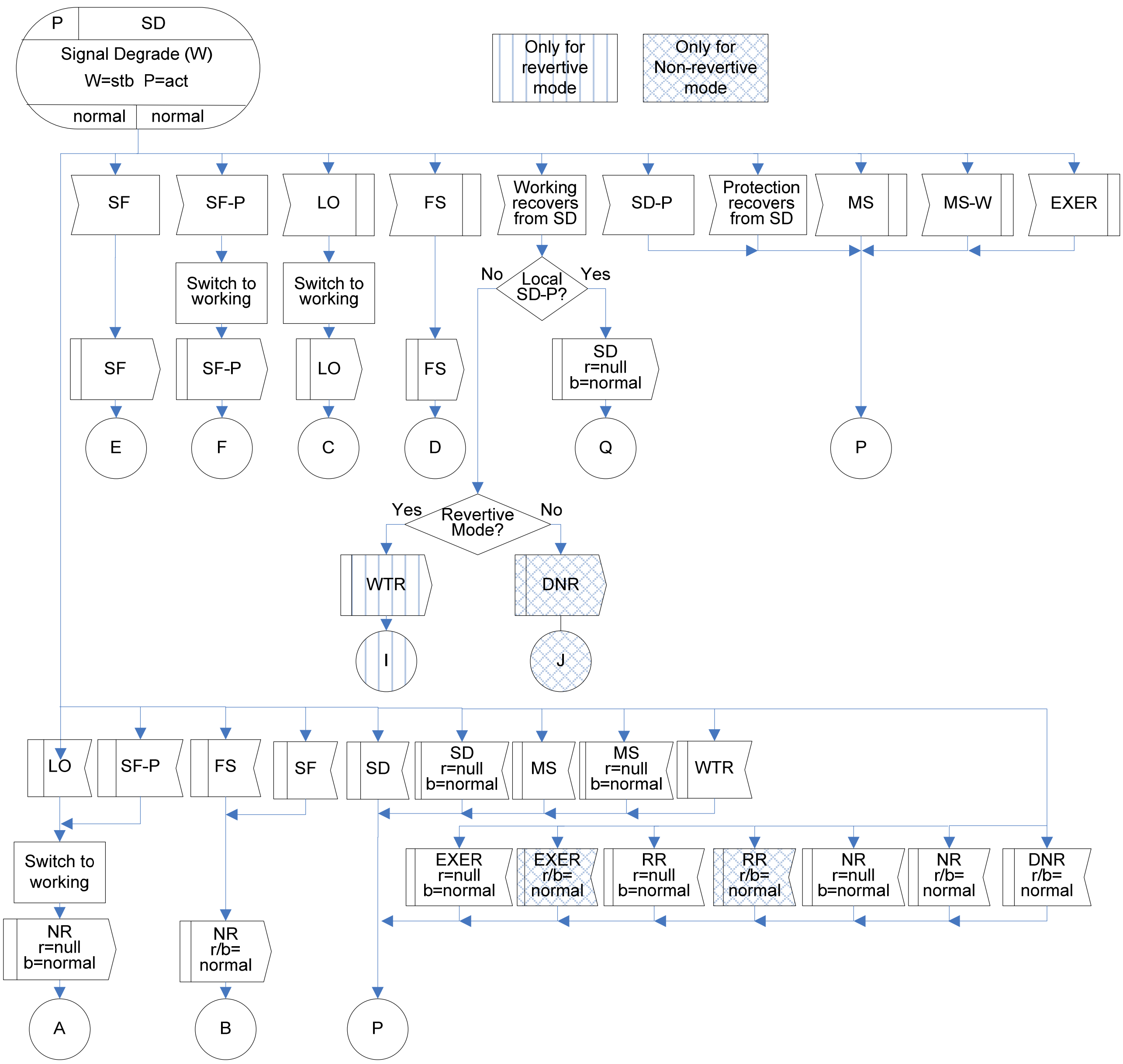


Figure IV.31 – SD(r/b=normal) state for 1+1 bidirectional protection switching

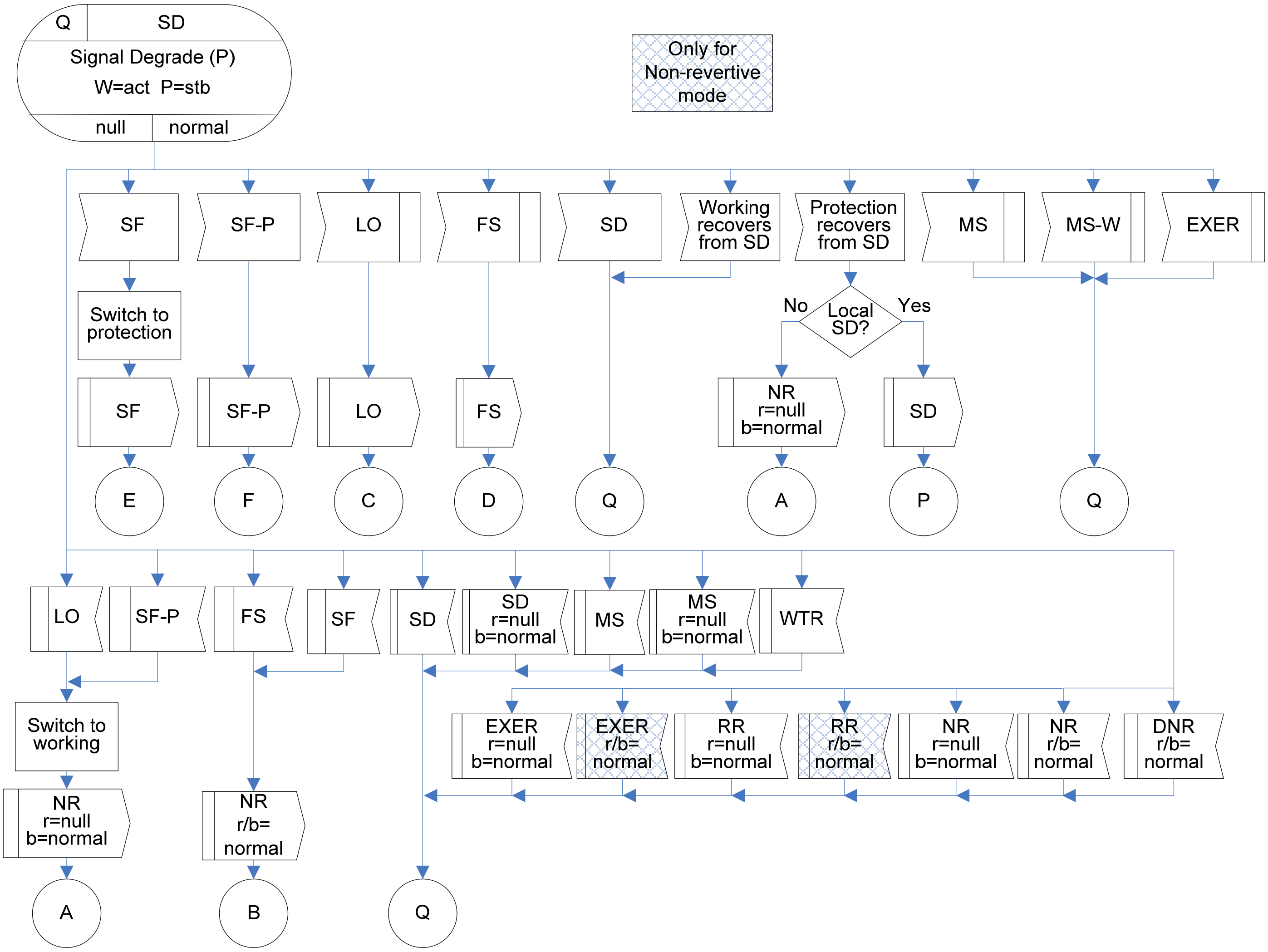


Figure IV.32 – SD(r=null, b=normal) state for 1+1 bidirectional protection switching

IV.2.3 1+1 unidirectional protection switching

The following diagrams define state transitions of 1+1 unidirectional protection switching both in revertive and non-revertive modes.

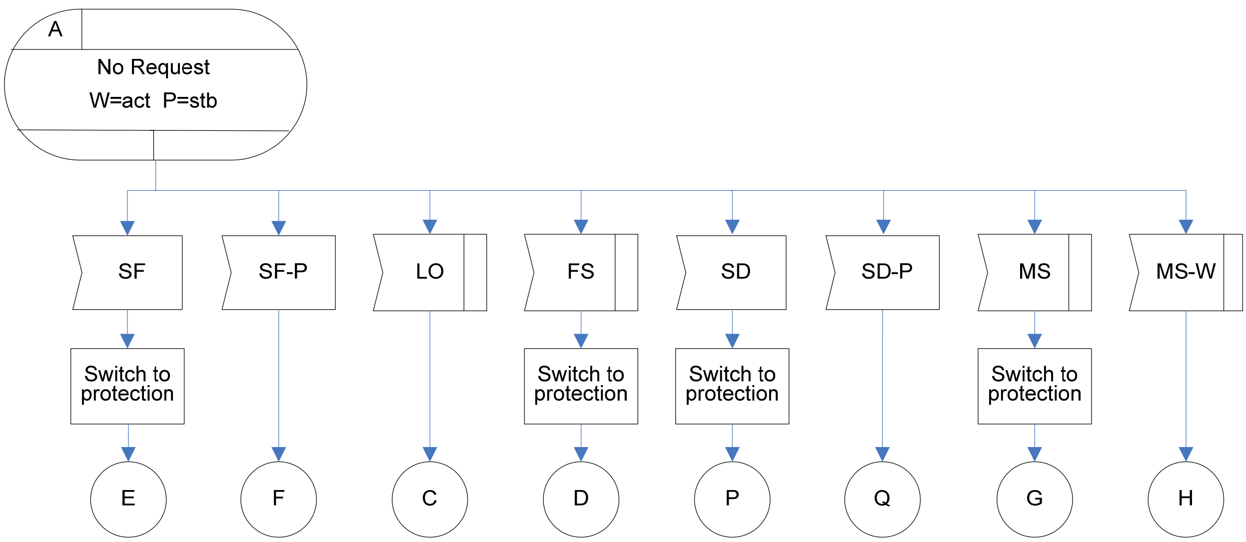


Figure IV.33 – NR(W=act/P=stb) state for 1+1 unidirectional protection switching

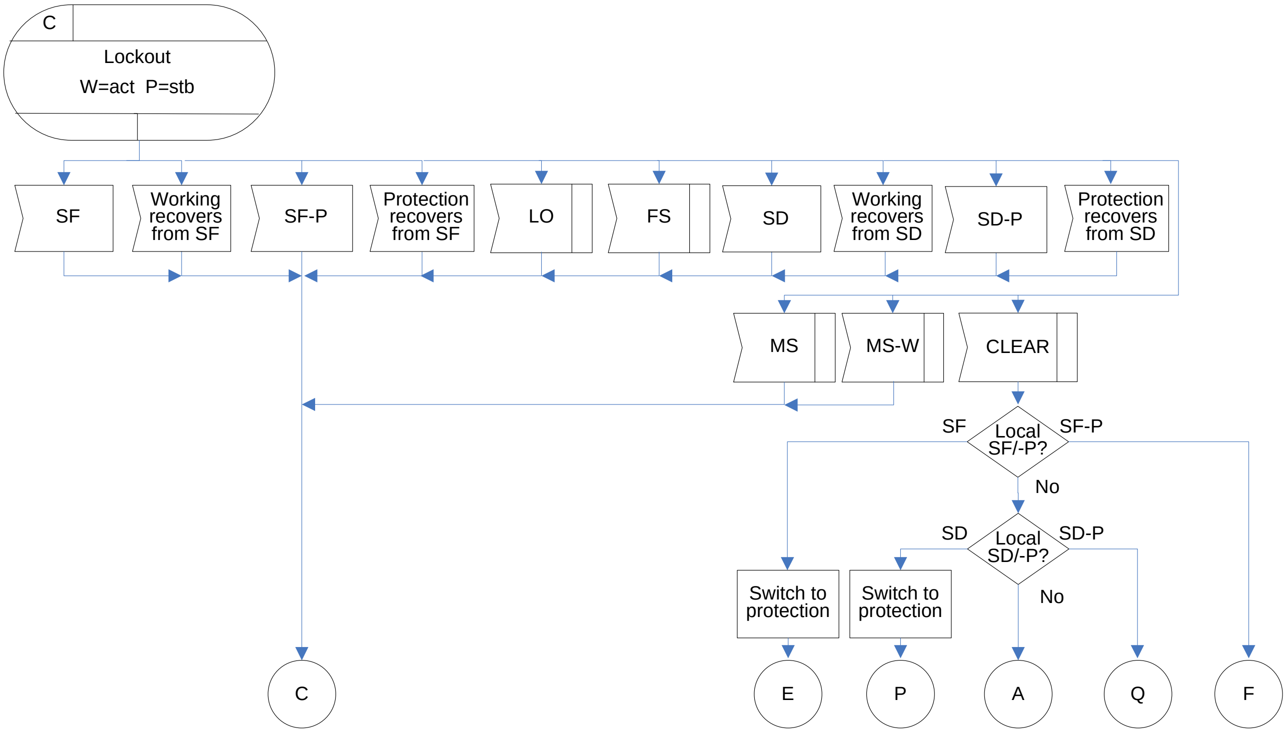


Figure IV.34 – LO(W=act/P=stb) state for 1+1 unidirectional protection switching

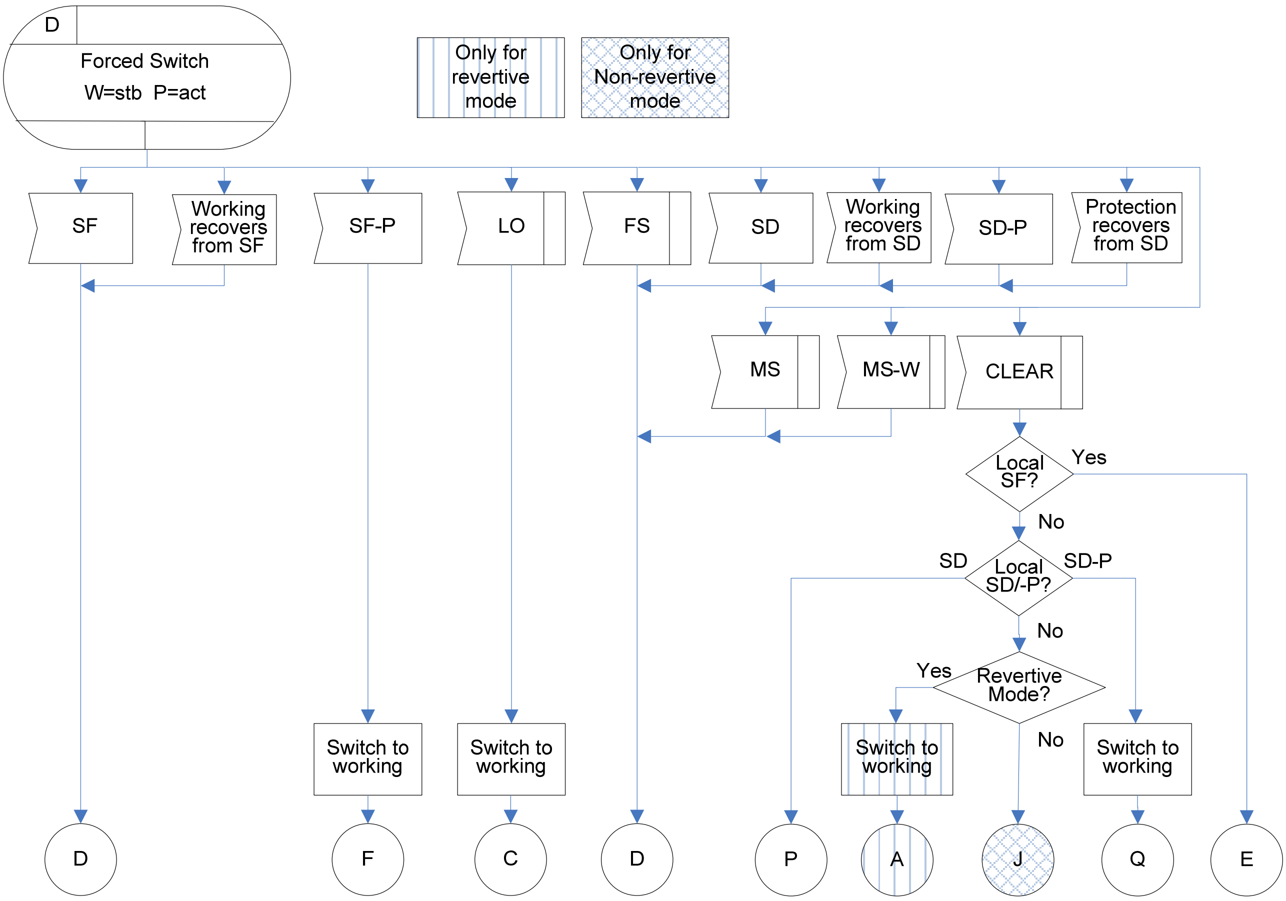


Figure IV.35 – FS(W=stb/P=act) state for 1+1 unidirectional protection switching

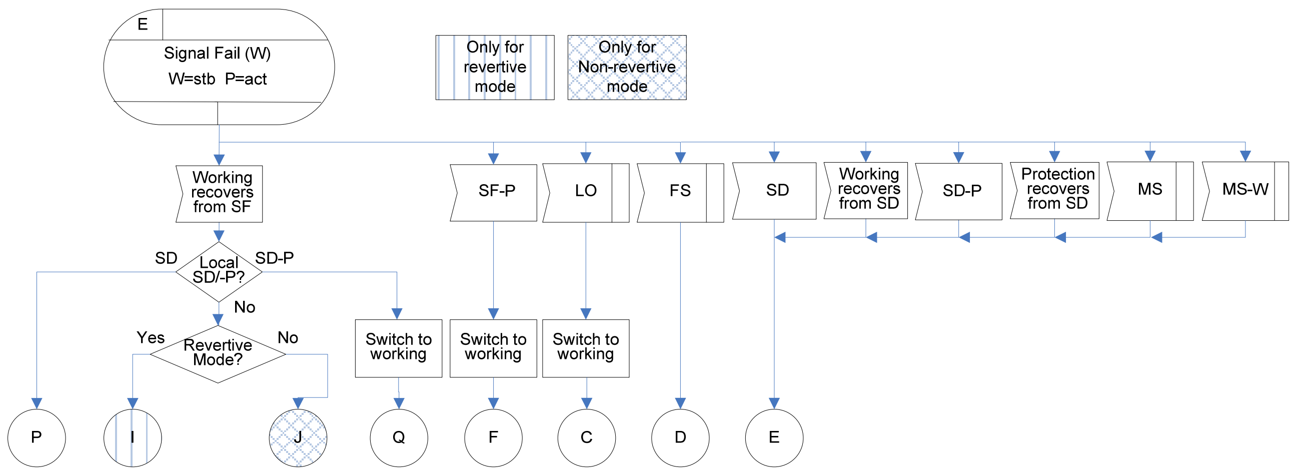


Figure IV.36 – SF(W=stb/P=act) state for 1+1 unidirectional protection switching

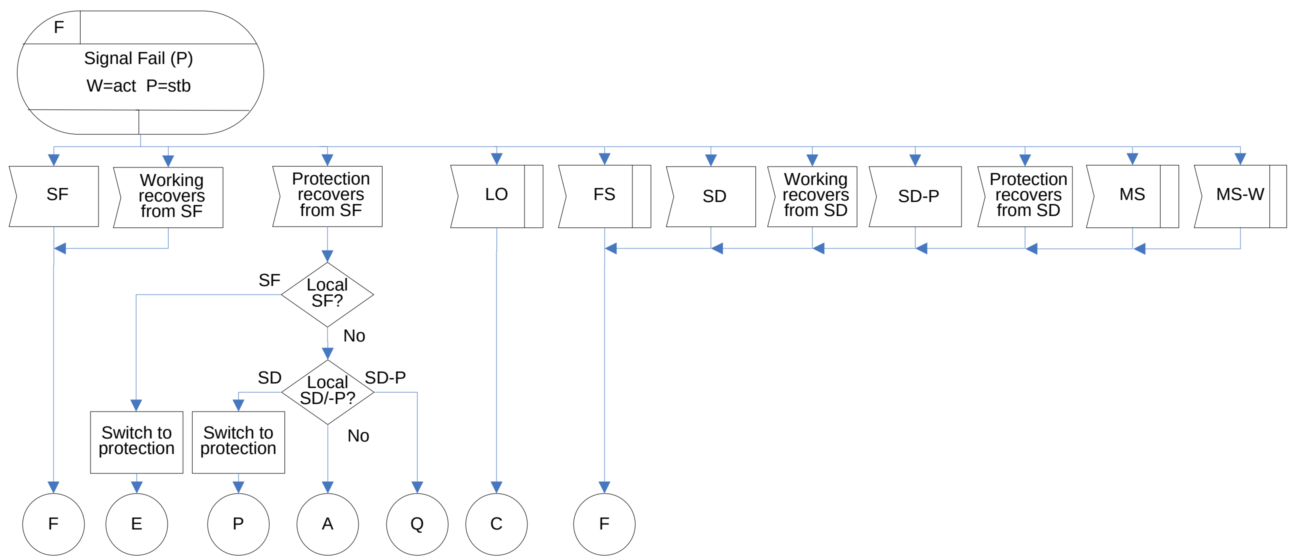


Figure IV.37 – SF-P(W=act/P=stb) state for 1+1 unidirectional protection switching

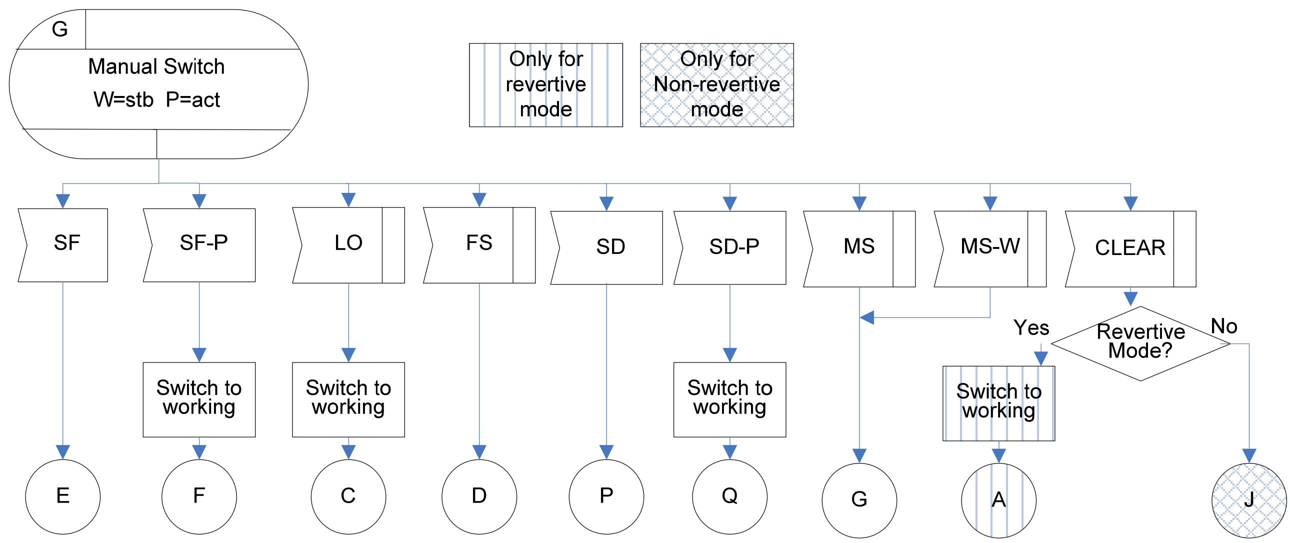


Figure IV.38 – MS(W=stb/P=act) state for 1+1 unidirectional protection switching

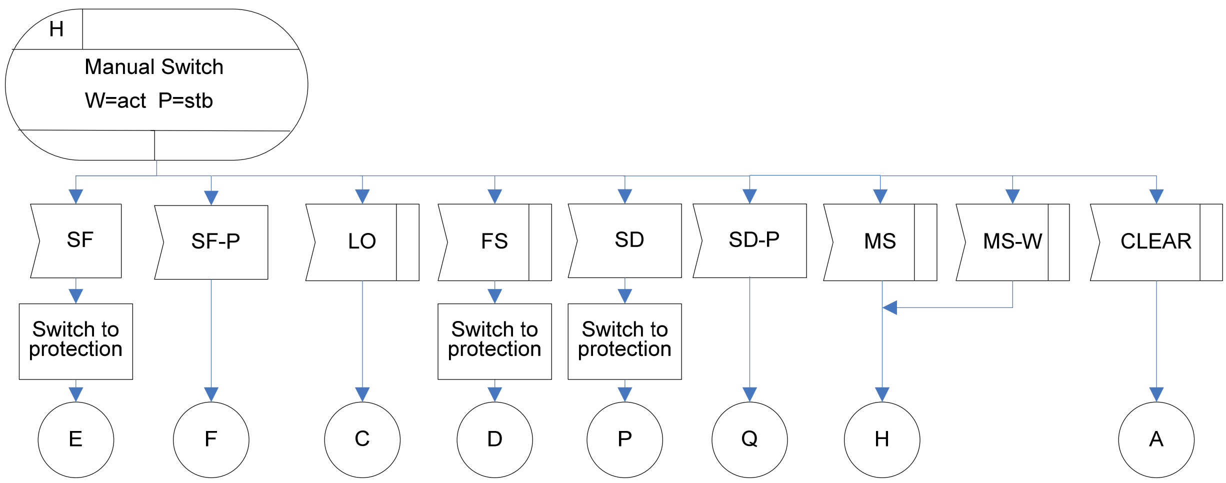


Figure IV.39 – MS(W=act/P=stb) state for 1+1 unidirectional protection switching

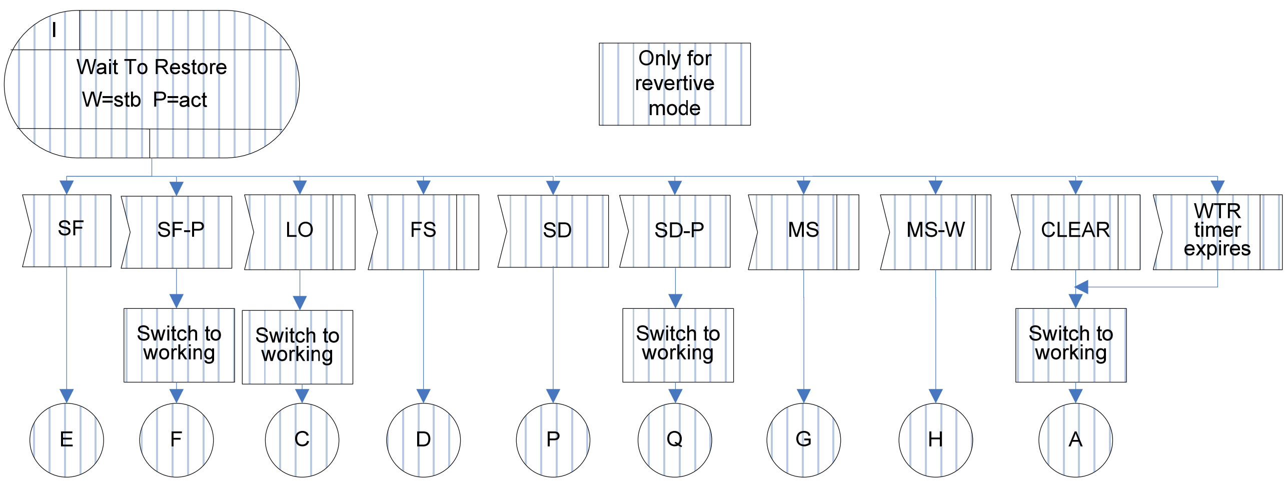


Figure IV.40 – WTR(W=stb/P=act) state for 1+1 unidirectional protection switching

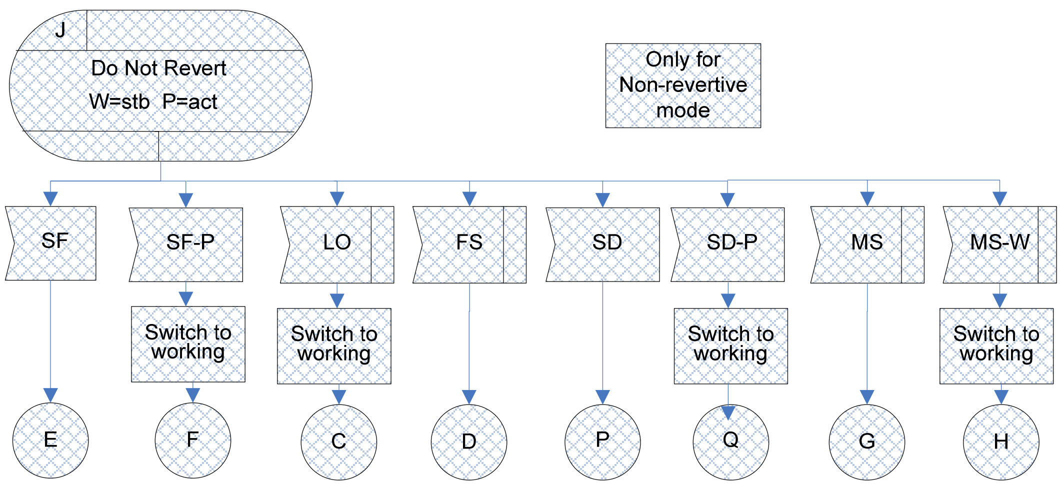


Figure IV.41 – DNR(W=stb/P=act) state for 1+1 unidirectional protection switching

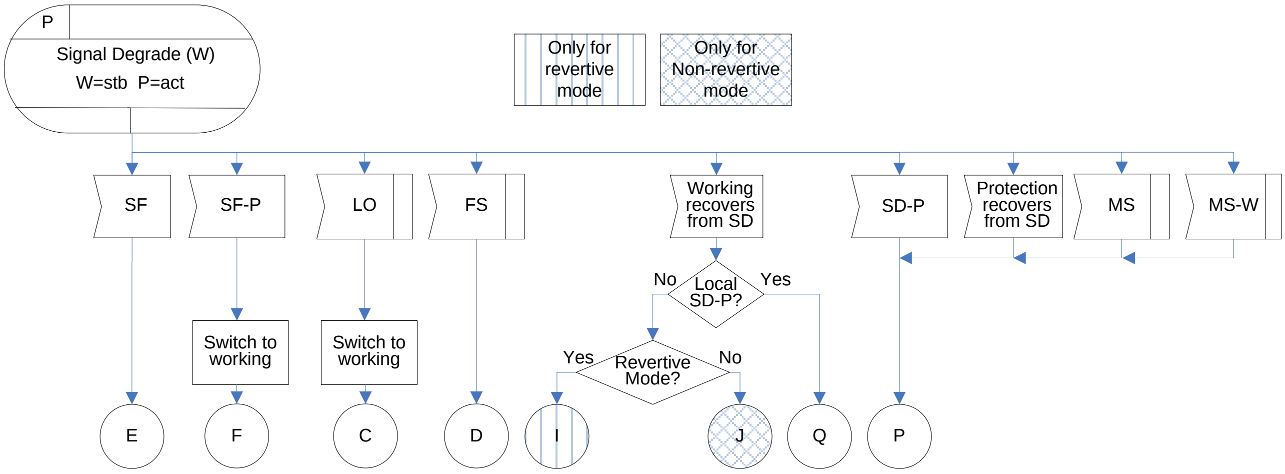


Figure IV.42 – SD(W=stb/P=act) state for 1+1 unidirectional protection switching

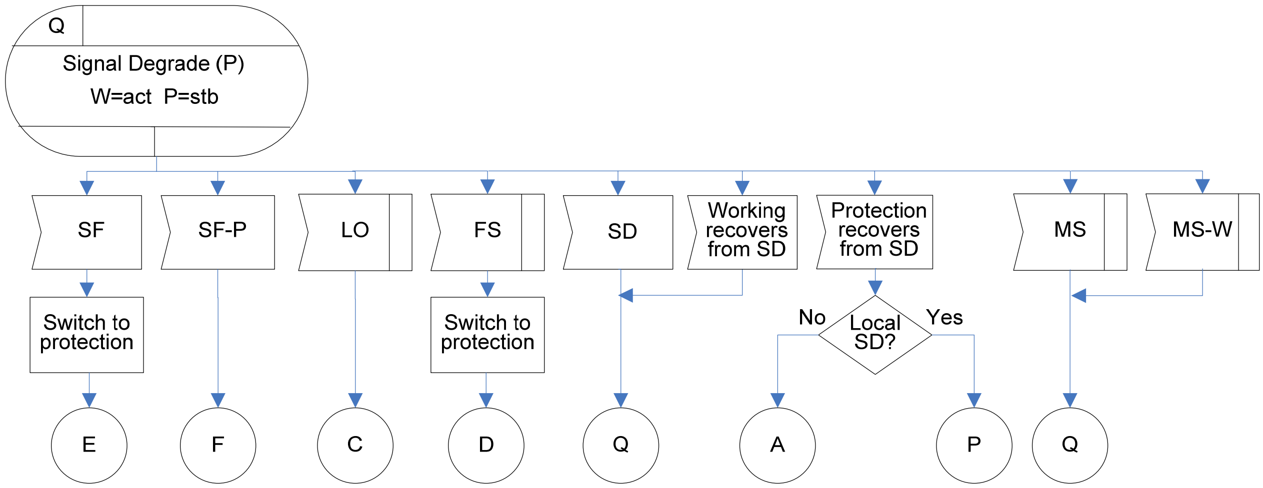


Figure IV.43 – SD(W=stb/P=act) state for 1+1 unidirectional protection switching

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
IPTV over NGN	Y.1900–Y.1999
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
Smart ubiquitous networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
Future networks	Y.3000–Y.3099

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	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, 2012